

Biblioteka Operaciona istraživanja  
i informacijski sistemi

24

Mirjana Drakulić

---

## **Osnovi Kompjuterskog prava**

**Mirjana Drakulić**

***Osnovi Kompjuterskog prava***

**Društvo operacionih istraživača Jugoslavije - DOPIS  
Beograd, 1996.**

dr Mirjana Drakulić, vanredni profesor Fakulteta organizacionih nauka

### ***Osnovi Kompjuterskog prava***

© Drakulić dr Mirjana, 1996.

*Umnožavanje, promena i distribuiranje nije dozvoljeno bez saglasnosti autora i izdavača*

Izdavač: *Društvo operacionih istraživača Jugoslavije - DOPIS*  
Volgina 15, Beograd 11000

Glavni i odgovorni urednik: *Slobodan Guberinić*

Lektor: *Vera Lebović*

Kompjuterska obrada teksta: *Ratimir Drakulić*

CIP - Katalogizacija u publikaciji  
Narodna biblioteka Srbije, Beograd  
Drakulić, Mirjana  
Osnovi kompjuterskog prava / Mirjana  
Drakulić. - Beograd : Društvo operacionih  
istraživača Jugoslavije - DOPIS, 1996  
(Beograd : Udruženje Nauka i društvo Srbije).  
- 499 str. ; 24 cm

Tiraž 300. - Beleške uz tekst. -  
Bibliografija: str. 491-499.

ISBN 86-7172-012-8

659.2.000.34

a) Računarska tehnologija - Pravni aspekt

b) Informaciona tehnologija - Pravni aspekt

ID=48872972

Štampa: *Udruženje Nauka i društvo Srbije*

**Izdavanje ove knjige finansiralo je  
Ministarstvo za nauku i tehnologiju Republike Srbije**

*"Nobody can ever imagine just how many problems lurk inside a computer. Computer problems wait patiently for the most inconvenient moment, then strike without mercy"*

*"Niko ne može zamisliti koliko mnogo problema vreba u unutrašnjosti kompjutera. Kompjuterski problemi pažljivo čekaju najnepogodniji trenutak da udare bez milosti."*

***Murphy's Computer Law, 1990.***

# PREDGOVOR

*Pravo je uvek težilo da normama ne samo obuhvati postojeće stanje, odnose i događaje, već i da predvidi i reguliše ono što se može dogoditi. Donedavno je naše pozitivno pravo bilo zatečeno i bez odgovora na pitanja koja postavlja razvoj kompjuterske tehnologije. Jutanje prava dovelo je danas do mnogobrojnih negativnih posledica, sa tendencijom njihovog nagomilavanja i usložnjavanja. Sve veći broj ljudi koristi ovu tehnologiju, pa su im potrebna i znanja iz mnogih područja - a jedno od njih je i pravno. Pravo se može posmatrati i kao kontrolni mehanizam za zaštitu individualnih prava, čime pravni aspekti korišćenja kompjuterske tehnologije postaju jedno od krucijalnih problema svakog pojedinca.*

*Ova knjiga teži da ukaže i, onoliko koliko je to u ovom trenutku moguće, osvetli one tačke u kojima se pravo i kompjuterska tehnologija sreću i dodiruju. To nije lako i jednostavno jer se tehnologija brzo menja, a neke oblasti i grane prava izuzetno sporo.*

*Pošto je ova materija kod nas nedovoljno obradjena, kao i da manjkaju naša iskustva, pa su mnoga rešenja, uz odgovarajuća prilagođavanja, preuzeta iz strane literature, zakonodavstava i prakse sudova drugih zemalja. Poseban problem bila je terminologija, naročito da li koristiti termin kompjuter ili računar. S obzirom da nema nikakvih posebnih razloga za negiranje ni jednog od njih koriste se naizmenično. Jedna od dilema bile su i trenutne izmene u našem zakonodavstvu. Opređenje je bilo za trenutna važeća rešenja, a u fusnotama objašnjenje predloženih, ali neusvojenih. Izuzetak je samo Predlog zakona o autorskom i srođnim pravima čije donošenje je u poslednjoj fazi, te su rešenja uneta u prikaz stanja. Naravno, po predaji rukopisa izdavaču, krajem prošle godine, najveći izazov, kome se nije moglo odoleti, nastao je pristupom Internetu, od proleća 1996., i dostupnošću dokumentima koja su u prethodnim fazama rada na knjizi bila samo želja. Najteže je bilo zaustaviti se. Doradjivala sam knjigu do samog momenta predaje, svesna da su neki praznine i slovne greške ipak ostale.*

*Knjiga je prevashodno namenjena onima koji se u svom radu sreću sa ovom problematikom. Materija je podeljena u dve celine. U prvom delu obradjen je uticaj kompjuterske tehnologije na pravo. Drugi deo je posvećen pravnoj zaštiti kompjuterskih sistema i obuhvata: zaštitu podataka, zaštitu kompjuterskih programa i softvera, zaštitu baza podataka, zaštitu topografije integrisanih kola i zaštitu od kompjuterskog kriminaliteta.*

*Bez pretenzija da se mogu obuhvatiti svi pravni aspekti i da se mogu dati odgovori na sva pitanja koja se postavljaju, cilj ove knjige je da se njihova kompleksnost i značaj pokažu.*

*Sugestije i mišljenja prof. dr Dragoljuba Kavrana, redovnog profesora Pravnog fakulteta u Beogradu, i prof. dr Branislava Lazarevića, redovnog profesora Fakulteta organizacionih nauka u Beogradu, bile su mi od izuzetne pomoći.*

*Na kraju, žalela bih se zahvaliti g-dji Bratislavi Petrović za pomoć u uobličavanju konačne verzije teksta, g-djama Branki Totić i Dušanki Dudić iz Saveznog zavoda za intelektualnu svojinu, kao i g-dji Mariji Djermanović iz Ministarstva za pravosudje Republike Srbije na dokumentima i materijalima, takodje i g-dinu Nikoli Markoviću iz Saveznog zavoda za informatiku. Traganje za literaturom bilo mi je lakše zbog pomoći g-djice Tatjane Dadić iz Biblioteke britanskog saveta, g-dje Vere Sekulić iz Instituta za međunarodnu privredu i politiku i g-dja Dušice Semenčenko i Suzane Stamatović iz Instituta "Mihajlo Pupin". Naravno, želela bih da se posebno zahvalim g-dinu Chris Reed-u, Stephan Saxsby-u i Ian Walden-u na prijemu, literaturi i sugestijama.*

*Posebnu zahvalnost dugujem svojoj porodici koja je istrpila sve što pisanje ovakve knjige zahteva.*

*Zemun, septembra, 1996.*

*Autor*

# UVOD

Poslednjih dvadesetak godina stepen razvoja jednog društva počeo se meriti, pored ostalog, i stepenom razvoja informatike, kompjuterske tehnologije (**KT**)<sup>1</sup>, informacionih sistema (**IS**) i mogućnostima njihove primene. Oni se danas pojavljuju kao jedan od činilaca razvoja, čiji uticaj sve više raste ukoliko su savršeni i ukoliko je društvo spremno da im ubrza razvoj. Informaciono razvijene zemlje, mada sa različitim pozicijama i sa različitim ciljevima, svoju dominaciju i razvoj informatike zasnovala<sup>2</sup> su na: **a**) tesnoj povezanosti vlade i industrije; **b**) promeni stava prema inovacijama; c) izradi strateških programa istraživanja, dugoročnom planiranju i velikim ulaganjima u razvoj. Odnos vlade i KT-industrije ostvarivao se, u prvim danima razvoja KT u: preduzimanju odgovarajućih političkih i administrativnih mera u homogenizaciji nacionalnog tržišta, regeneraciji privrednih delatnosti usmeravanjem ka proizvodnji produkata KT i njihovih usluga, kao i postavljanjem trgovinskih i drugih barijera za sopstvene proizvode i uvoz tuđjih proizvoda (tako su u V. Britaniji te rane godine kompjuterskih tehnologija ocenjene kao period tesne saradnje Vlade, industrijskih kompanija i sindikata da se gotovo brišu uobičajene suprotnosti i "bela usijanja" koja su dugo među njima vladala). Tome je doprinela i promena stava o značaju inovacija za nacionalnu privredu i komercijalno poslovanje. Kako su Amerikanci, u većini slučajeva, bili skloni brzom reagovanju na inovacije to su i vlade Francuske, V. Britanije i Nemačke, svaka za sebe, odlučile da preduzmu mere koje bi podspešile kreativnost i stvaralačke sposobnosti svojih stručnjaka i smanjile protok vremena između ideje i eksploatacije, osobito u kompjuterskoj industriji<sup>3</sup>. Time su želele da onenoguće dominaciju SAD i podignu barijere u čuvanju svojih ideja i proizvoda. Treća značajna aktivnost bila je vezana za izradu strateških programa istraživanja i donošenja dugoročnih planova razvoja koji bi znatno izmenili stav mnogih zemalja tržišne ekonomije u odnosu na nacionalne ekonomske planove. Njihova izrada poverena je grupama eksperata. Tako je u Francuskoj šezdeseti godina nacionalni ekonomski plan obuhvatio i "Plan Calcul" kojim su planirane aktivnosti vezane za KT-industriju i njenu primenu i u javnom, ali i u privatnom sektoru. Nemačka izrađuje "Prvi program podrške obradi podataka" kojim obezbeđuje sumu od 140 miliona maraka, za period 1967-1970, za ekonomski razvoj računara. "Drugi program" je povećao sumu na 1.300 miliona, a treći na 1.576 miliona maraka. Po ovim programima firme kao što je Siemens dobile su finansijsku pomoć, za razvoj, uz niz drugih beneficija za i ostvarenje.

<sup>1</sup> Mada se u literaturi više spominju informacione tehnologije (IT), ipak je termin kompjuterske tehnologije, iako donekle už, primereniji termin sadržaju ove knjige.

<sup>2</sup> Murphy B., The International Politics of New Information Technology, London, Crom Helm, 1986., str. 50.

<sup>3</sup> Norton H., Informatics In Europe, Manchester, NCC Blackwell, 1991., str. 35-61.

Zahvaljujući ovom programu *Simens* danas spada među 100 najrazvijenijih firmi u svetu<sup>4</sup>. Od ovih aktivnosti nisu ostali imuni ni Japanci. U 1978. godini donosi se "Projekat japanske kompjuterske pete generacije" po kome se predviđaju potrebe za određenim kompjuterskim sistemima u 1990. godini. Prognoza i ulaganje u taj razvoj omogućili su ostvarenje zadatog cilja - obezbedjenje Japanu glavnine profita od svetske KT-industrije. To se u dobroj meri i ostvaruje (treće mesto *Fujitsu*, peto *Hitachi*, trinaesto *Toshiba*, petnaesto *Machushita* i dr. na svetskoj listi 100 najuspešnijih firmi). Kao odgovor ovom projektu, u V. Britaniji se 1982. godine objavljuje "*Alvely project*"<sup>5</sup> u kome se predviđaju pravci razvoja, kao i sredstva koja će biti uložena u istraživanja (oko 352 miliona funti za programe razvoja komunikacija, demonstratorske projekate i obrazovanje).

Razvoj informatike, kompjuterske tehnologije i informacionih sistema odražava se i na društvenu osnovicu i na nadgradnju, jer ukazuje na propuste zbog kojih bazu i nadgradnju treba menjati. Između ostalog, neophodna je i promena svesti o njihovom značaju u privrednom i društvenom razvoju i posledicama koje nastaju usled okamenjenih ili pogrešnih shvatanja. U informaciono razvijenim društvima uveliko se već govori o post-industrijskom (post-buržoaskom, super-industrijskom, tehnotronskom, organizacijskom, programskom i sl.) društvu, a koncepcija počiva na teoretskom znanju, kao osnovi, na kojoj će se nova tehnologija, ekonomski rast i stratifikacija društva organizovati<sup>6</sup>. U suštini ideja o post-industrijskom društvu identifikuje nove osnove i principe organizacije i definiše zajedničko jezgro problema sa kojima će se takva društva boriti. Poredeći promene koje su bile u industrijskim i post-industrijskim društvima, može se konstatovati da su razlike ne samo velike nego i suštinske. Tako se ekonomija u industrijskim zemljama (Evropske Unije, Japana) bazira na proizvodnji robe (industrijskoj proizvodnji i preradi), dok u post-industrijskim (SAD) na tercijalnim (transport i usluge) i kvartalnim delatnostima; profesionalna usmerenost u industrijskom društvu okupirana je polukvalifikovanim radnicima i inženjerima, a u post-industrijskom profesionalizovanim i tehnički orijentisanim naučnicima; tehnologija je u industrijskom društvu bazirana na energiji, a post-industrijskog na informaciji; metodologija je u prvom zaokupljena empirizmom i eksperimentima, a u drugom se zasniva na apstraktnim teorijama (modelima, simulaciji, teoriji odlučivanja, sistemskoj analizi); ako se, pak, gleda vremenska perspektiva, onda se u industrijskim društvima ona sagledava kroz ad hoc prilagođavanja i projekcije, dok je u post-industrijskim okrenuta budućnosti i prognozama. Osnovni principi industrijskog društva vezani su za ekonomski rast, državnu i privatnu kontrolu investicionih odluka, a u post-industrijskom

<sup>4</sup> Datamation, june 1994.

<sup>5</sup> Murphy B., op. cit., str. 80-84.

<sup>6</sup> Bell D., The post-industrial society: a conceptual scheme, edicija Evolution of an Information Society, London, Aslib, 1987., str. 60.

za centralizovana i kodifikovana teorijska znanja<sup>7</sup>. Struktura i problemi koje post-industrijsko društvo nosi, u odnosu na osnovne principe na kojima treba izgradjivati kodifikovana znanja, su:

| Osnovni principi       | Centralizovano i kodifikovano teoretsko znanje                |
|------------------------|---|
| Primarne institucije:  | Univerziteti<br>Naučni instituti<br>Istraživačke organizacije |
| Ekonomska podloga:     | Industrija bazirana na nauci                                  |
| Primarni resurs:       | Ljudski   |
| Politički problem:     | Politika razvoja nauke<br>Obrazovna politika                  |
| Strukturalni problemi: | Ravnoteža između privatnog i javnog sektora                   |
| Stratifikacija:        | Iskustvo<br>Obrazovanje                                       |
| Teorijski problem:     | Kohezija "nove klase"   |
| Sociološke reakcije:   | Otpor birokratizmu<br>Nepovoljna kultura                      |

Znači, društvo koje pokušava da se osloni na nauku, znanje i informacije, čija se privreda od proizvodnje orijentiše ka uslugama, a tehnologija ka novim industrijama baziranim na nauci i informatici postaje prioritetno, kao što i države u kojima se to realizuje postaju vodeće u međunarodnom poretku. Kolike razmere to poprima vidi se u sve češće korišćenom terminu informaciono društvo, koji se između ostalog, našao i u zvaničnim dokumentima Evropske Unije (prvi put korišćen u *White Paper Growth Competitiveness, Employment - the Challenges and Ways Forward into the Twenty-first Century*)<sup>8</sup>. Post-industrijsko, odnosno informaciono društvo, takodje, unosi promene u vladajućoj klasi i izvoru njene moći. "Nova vladajuća klasa" postaje "profesionalna klasa", odnosno, klasa koja svoju moć zasniva na znanju, prevashodno informatičkom, više nego na imovini<sup>9</sup>.

<sup>7</sup> Bell D., op. cit., str. 61.

<sup>8</sup> Group on the Information Society to the Corfu European Council, Brussels, 1994.

<sup>9</sup> Greenop D., Shaping the European Information Society, British Telecommunications Engineering, vol. 14., 3/95., str. 186 - 198.

Medjutim, te se promene još uvek ne dešavaju u većini dojučerašnjih socijalističkih zemalja danas nazvanih "zemlje u tranziciji", u kojima se<sup>10</sup> značaj informatike, KT i IS dovodi u kontekst ukupnog privrednog i društvenog razvoja, dirigovanog "novim ciljevima", koji su isto toliko nedefinisani i magloviti koliko su i ovi sistemi neefikasni. Mnogi principi, pa, čak, i instituti koji su nastali sa razvojem informatike, KT i IS u razvijenim zemljama dobili su sasvim drugačija značenja ili su negirani. To najbolje pokazuje nesposobnost ovih društava da prihvate činjenicu da ukupni društveni i privredni razvoj umnogome zavisi od razvoja ovih fenomena. Naime, izuzetan prirodni i ljudski potencijal koji je postojao u nekadašnjem SSSR-u (računa se da je oko milion ljudi bilo uključeno u istraživanje i razvoj) nije značio i postojanje odgovarajućeg nivoa razvoja u odnosu na KT. Po proceni nekih zapadnih zemalja jer pouzdanih podataka iz primarnog izvora nema, "Sovjeti" zaostaju za dve ili tri godine u srednjim kompjuterskim sistemima, a između pet i sedam u mikro<sup>11</sup>. I druge zemlje Istočne Evrope koje imaju heterogene kulture, ekonomije, prava, tehnički razvoj i sl. imaju nešto zajedničko - nizak nivo primene kompjuterske tehnologije (sve zajedno imale su 1991. godine instaliranih oko 1 milion DOS personalnih računara, što je svakako zanemarljivo u odnosu na 40 miliona samo u SAD<sup>12</sup>). Istovremeno, lokalno tržište softvera im je relativno malo, a ideja o pravljenju profita od programiranja i distribucije softvera im je još uvek strana. Tek je u poslednjih nekoliko godina, nekoliko preduzeća počelo je sa prodajom softverskih paketa<sup>13</sup>. Za sada najpoznatiji program nastao u tlu nekadašnjeg Sovjetskog saveza je igra *Tetris*<sup>TM</sup>, koji je na Zapad stigao preko Madjarske. Osim ovog, poznati su i bugarski virusoliki programi, pa je ova zemlja postala jedan od glavnih "rasadnika" virusa uopšte. Uzrok ovakvog stanja je, svakako, činjenica što su u ovakvim zemljama donošene rezolucije, strategije tehnološkog razvoja, srednjoročni ili dugoročni planovi društveno-ekonomskog razvoja i slični dokumenti koji su u prvi plan stavljali "sopstveni pravci razvoja" i počinjali "stvari" iz početka. Drugim rečima, otkrili su ono što je već bili poznato i time gubilo i vreme i sredstva, kao i ljudske potencijale (sopstveni razvoj hardvera bio je često predmet ovih dokumenata). Zatvorenost u sopstvene ili neke interesne granice, dovodila je do niza pogrešnih poteza u tekućoj ili perspektivnoj politici i rezultirala pogrešnim merama i akcijama. Kao ilustraciju ovakvih shvatanja može da posluži i naša zemlja koja je dugo usmeravala razvoj KT ka domaćim doprinosima, pri čemu je zatvorila granice za strane proizvođače, dajući prioritet "sopstvenim" proizvođačima i kadrovima sa veoma niskim znanjem i informatičarskom kulturom, kao i vrlo uskim tehnološkim mogućnostima. Istovremeno egzistiraju visoke carinske kvote za uvoz opreme, destimulativni uvoz stručne literature (koja je zbog vrednosti dinara vrlo skupa i

<sup>10</sup> Besarović V., Pravo industrijske svojine i autorsko pravo, Beograd, NIO Poslovna politika, 1984., str. 33.

<sup>11</sup> Murphy B., op. cit., str. 119.

<sup>12</sup> Kotov V., Project Start, Communications of the ACM, vol. 34., no. 6/91., str30 i 31.

<sup>13</sup> Krčevinac S., Informacione tehnologije u centralnoj i istočnoj Evropi, zbornik radova sa XI Info -Teh, Donji Milanovac, 1996., str. 8 - 13.

opterećena carinama, porezima i sličnim nametima), neodgovarajući finansijski stimulansi naučno-istraživačkih, stručnih kadrova i inovatora, kao lociranje naučno-istraživačkog rada, mahom na fakultete i institute i njihovim tretmanom kao potrošnje. Takvim merama i akcijama treba dodati i izmene suštine prava intelektualne svojine, koje od klasičnog prava pojedinca postaje pravo organizacije, kao i niz "sopstvenih" rešenja koja samo otežavaju umesto da ubrzavaju razvoj. Zaštita informacionih sistema, podataka, tehnologije ostaju otvorena pitanja koja će se kasnije rešavati. Razvoj mreže između pojedinih IS-a je prepušteno dogovorima i konsensusima pojedinih subjekata, a utvrđivanje i postojanje jedinstvenih standarda i metodologije pretvoreno je u "bojno polje" zbog različitih interesenata sa različitim stepenom uticaja, pri čemu, prevaga ne počiva na kvalitetu već na jačini političke moći koju su pojedini predlagali imali. Na žalost, ovakvo stanje, još uvek, prevladava kod nas. U drugim zemaljama istočnog bloka, od nedavno počinje prevazilaženje ovakvog stanja što se može videti i izborom Japanaca da jedan mađarski logički programski jezik bude osnova za razvoj projekta pete generacije ili što je *Digital* u 1989. godini počeo investiranje u Mađarskoj i ^eškoslovačkoj, kao i prihvatanjem akcije IBM da se na univerzitetu ^eškoslovačke, Mađarske, Poljske i Jugoslavije instaliraju, po niskoj ceni, računari srednje veličine i da se na tri fakulteta u Budimpešti koriste fiber-optic mrežu. Isto tako, rastu i ulaganja u kompjutersku tehnologiju, kao što se one sve više okreću njihovim visokim kvalitetima i boljim uslugama<sup>14</sup>. To je, svakako, trebalo da donese određene promene u shvatanjima i akcijama koje je potrebno preduzimati. Ali, sankcije koje su nas zadesile prekinule su ovu akciju, te smo upravo mi, iako najkonkurentniji, prepustili mesto Bugarskoj.

Pored zemalja u tranziciji izuzetno je značajna pojava zemalja u razvoju, kao posebne i organizovane grupacije koja se pedesetih godina ovog veka pojavljuje kao legitimni član međunarodne zajednice. One, tražeći sopstvene puteve i pravce razvoja, čine čitav niz naprednih, ali i pogrešnih koraka. U početku, mnoge od njih, kao bivše kolonije, prihvatile su rešenja (pravna, razvojna, i dr.) svojih nekadašnjih kolonista, koja preslikana u nerazvijene uslove više štete nego što koriste, jer takva rešenja nisu bila predviđena za nerazvijene društveno-ekonomske, pravne, tehnološke uslove u kojima su se primenjivala. Među zemljama u razvoju polarizuju se dve grupe u odnosu na usvojene pravce razvoja. **Prva grupa** zemalja, Indija, Maroko, Iran, Meksiko, Panama, počinje korišćenje IS, između 1954. i 1970, ali su oni bili centralizovani administrativni sistemi u javnom sektoru, zasnovani na hardveru i softveru dizajniranom i proizvedenom u informaciono razvijenim zemljama. S obzirom da su ovi sistemi predstavljali izvor moći i kontrole nad sopstvenim stanovništvom nastavljena je centralizacija daljeg razvoja KT, uglavnom, na vrlo niskom nivou i bez nekih posebnih vizija. Sopstveni razvoj, kroz nacionalnu politiku, jedini je u tom periodu objavio Brazil. Kako su ove zemlje uglavnom komunicirale i saradjivale sa svojim ex-

<sup>14</sup> Information Technology Trends in Central and Eastern Europe, Deloitte Touche Tohmatsu International, IDOM, 1994/1995.

kolonijalistima, to je predstavljalo osnovicu jedne nove pojave - tehnološkog neokolonijalizma. Neokolonijalizam<sup>15</sup> je postao izvor političke nadmoći i paternizma informaciono razvijenih zemalja nad zemljama u razvoju. Uočivši opasnost, vlade ovih zemalja počinju intenzivno da rade na utvrđivanju pravaca sopstvenog razvoja pospešujući ga protekcionizmom, beneficijama i nacionalnim administrativnim merama zaštite. Potom, nakon nastajanja negativnih posledica, ova rešenja se zamenjuju, opet nekritički, novim, koja u većini slučajeva negiraju sve postojeće, i koja značajno odstupaju od pozitivnih rešenja koja bi mogla biti prihvaćena. Počinje utvrđivanje osnovnih aksioma sopstvenog informaciono-tehnološkog razvoja koji se nije pokazao baš u najboljem svetlu jer se, s jedne strane, zasnivao na paralelnom razvoju svih komponenti kompjuterske tehnologije, a s druge, precenjivanju sopstvenih snaga što dovodi do "erozije razvoja". Situacija se, npr., Indiji, unekoliko menja pojavom PC i pokušajima da se uoče sopstveni pravci razvoja, proizvodnje i prodaje. Da bi se svladale teškoće nasledjene iz perioda velikih sistema, Indija je odredila pravce strategije koju će realizovati i koja se, u suštini, sastoji u stvaranju ugleda na proizvodnji softvera za tržište (a ne za poznatog kupca) jer se time omogućuje veći prodor na svetsko tržište (od ukupnog izvoza softvera svega 1% su bili softverski paketi koji nisu bili prilagođeni određenoj potrebi); vraćanju servisiranja Indiji (jer su ga preuzele druge zemlje iz kojih su PC dolazili); pomeranju težišta sa niske cene na visoki kvalitet; i sl. Za to im je potreban veoma veliki broj programera (oko 250.000 do 1995.) kojih nemaju (imaju negde oko 50.000) i istraživača, kao i decentralizacija razvoja ka organizacijama. **Druga grupa** zemalja, Singapur, Tajvan, Hong Kong, Južna Koreja, Filipini, Tajland, Indonezija, Vijetnam<sup>16</sup>, inače nazvanih "azijskim tigrovima" svoj razvoj usmeravaju ka elektronskim komponentama koje su značajne u KT-proizvodnji. Parcijalnim razvojem samo nekih komponenti, ove zemlje su postepeno počele da zauzimaju značajno mesto na međunarodnoj informaciono-tehnološkoj sceni. Koliko su ove zemlje napravile intenzivan prodor na svetsko tržište hardvera isto toliko su imale i ozbiljnih problema u prodoru na svetsko tržište softvera. Ovo izgleda protivurečno iz jednostavnog razloga što je softverska industrija u ovim zemljama zabeležila izuzetno brz rast u poslednjih nekoliko godina i izuzetno slab plasman van svog tržišta. Razloga za to ima više: pritisak kompanija iz SAD da samo za njih razvijaju ekskluzivne softvere, npr. IBM je pre pet godina u strateškom savezu sa Tajvanskim državnim Institutom za informacione tehnologije obezbedio razvoj oko 100 programa. Ovi su programi i dokumentacija bili paralelno izradjeni na orijentalnim jezicima i na engleskom. S obzirom na slabosti autorskog prava ove zemlje i propusta u ugovorima, IBM je ove programe dvostruko iskoristio - za plasman na dalekoistočnom tržištu i za

<sup>15</sup> Marohy B., op. cit., str. 52.

<sup>16</sup> Goodman S. E., Press L. I., Computing in Vietnam: An Asian Tiger in the Rough, Communication of the ACM, vol.38., no.1/95., str. 11 - 17.

prodaju na drugim tržištima<sup>17</sup>. Kad se ovi problemi budu rešili više je nego sigurno da će ove zemlje zauzeti posebno mesto i u razvoju softvera, kao što ga imaju u razvoju drugih komponenti komjuterske tehnologije<sup>18</sup>.

Cilj iznošenja ovih primera i pravaca je da ukratko ukaže da su društveno-socijalne implikacije raznolike, a kao osnovne pojavljuju se sledeće: **1)** promena društvene dinamike i razlika između informaciono razvijenih i nerazvijenih zemalja; **2)** pojava tehnološkog neokolonijalizma; **3)** pojava nove klase - klase profesionalaca u post-industrijskom društvu; **4)** erozija državne suverenosti, internacionalizacija i globalizacija svetske zajednice. Sve ove implikacije dešavaju se na širem planu, a posledice nastaju za konkretnu državu, organizaciju i/ili pojedinca. Svako od ovih "polja" na različite načine reaguje na promene koje nosi informaciona revolucija, stvarajući različite odbrambene mehanizme. Nikako ne treba zaboraviti pravo, kao jednog od njih.

<sup>17</sup> Press L., Personnel Computers and the World Software Market, Communications of the ACM, vol.34., no. 34/91., str. 28.

<sup>18</sup> Tako je, npr. Vijetnam, u svojoj strategiji razvoja u oblasti IT, odn. KT, objavljenoj avgusta 1994. godine potencirao tri bazne oblasti u nacionalnom programu: izgradnju infrastrukture za KT; primenu KT u državnom menadžmentu i socio - ekonomskim aktivnostima; kao i podsticanju razvoja i primene KT u svim domenima. Značajne pretpostavke ovog programa su: obezbedjenje razvoja mreža, međunarodna koordinacija i transfer tehnologije, zaštita intelektualne svojine, kao i obezbedjenje uslova da se do kraja decade osposobi 20.000 informatičara koji će program realizovati.

# **PRVI DEO**

**KOMPJUTERSKA TEHNOLOGIJA**

**I**

**NOVA GRANA PRAVA**

**Uvod**

**Glava 1: Kompjutersko pravo**

# GLAVA 1

## KOMPJUTERSKO PRAVO

|      |   |    |
|------|---|----|
| 1.   | <b>Pravo i kompjuterska tehnologija</b>                               | 12 |
| 2.   | <b>Odredjivanje problema</b>  | 13 |
| 3.   | <b>Uredjivanje pravnih osnova korišćenja kompjuterske tehnologije</b> | 15 |
| 4.   | <b>Može li se govoriti o novoj grani prava?</b>                       | 18 |
| 5.   | <b>Šta je Kompjutersko pravo?</b>                                     | 20 |
| 6.   | <b>Predmet Kompjuterskog prava</b>                                    | 22 |
| 7.   | <b>Istorijski razvoj Kompjuterskog prava</b>                          | 29 |
| 8.   | <b>Izvori Kompjuterskog prava</b>                                     | 32 |
| 9.   | <b>Odnos Kompjuterskog prava sa drugim granama prava</b>              | 38 |
| 9.1. | <i>Kompjutersko pravo i Pravo informacione tehnologije</i>            | 38 |
| 9.2. | <i>Kompjutersko pravo i Informatičko pravo</i>                        | 40 |
| 9.3. | <i>Kompjutersko pravo i Informaciono pravo</i>                        | 43 |
| 9.4. | <i>Kompjutersko pravo i Telekomunikaciono pravo</i>                   | 47 |

## 1. Pravo i kompjuterska tehnologija

Moderno društvo skoro da se ne može zamisliti bez korišćenja računara, i ne samo njih, već i drugih dostignuća visokih tehnologija sa kojima se srećemo u svakodnevnom životu, radu, obrazovanju i drugim sferama. Može se reći da smo postali zavisni od ovih tehnologija, jer se na njima baziraju mnogi poslovni sistemi, uprava, odbrana, pa i naše zdravlje. Međutim, ne sme se zaboraviti ni činjenica da sigurnost tih sistema predstavlja jedno od najvažnijih pitanja i naše sopstvene sigurnosti. Mnoge poslovne, službene, vojne i lične tajne čuvaju se u računaru. Istovremeno i perfidni, teško predvidljivi i izuzetno teško odgonetljivi ataci mogu ugroziti ne samo pojedinca, već i organizaciju, državu, društvo. Da bi se napadi sprečili, počinioci kaznili i osujetili neophodno je predvideti i preduzeti čitav niz mera i akcija. Mere se sve više izgrađuju i unapred ugrađuju u informacione sisteme i što opasnost više raste, postaju sve kompleksnije i potrebnije. Posebnu grupu čine pravne mera.

U razvijenim zemljama pravne mere postaju ravnopravne sa tehničkim i organizacionim. Sigurnost informacija i podataka, IS, telekomunikacija, postaje jedan od prioriteta zadatka pravnih sistema. A kako se kompjuterska tehnologija sve više razvija, to se sigurnost prenosi sa nacionalnog na međunarodni plan. Međunarodne organizacije i asocijacije postepeno, u okviru svojih redovnih aktivnosti, počinju da se bave i ovim problemima, da bi u određenim situacijama i slučajevima formirale posebna tela za praćenje i rešavanje narastajućih opasnosti i mogućnosti koje sa sobom nose nove tehnologije. Rešenja se, potom, manje ili više, ugrađuju u zakonodavstva zemalja članica. Pravni aspekti sigurnosti tako dobijaju i međunarodni značaj. Ma koliko to prirodno izgledalo to nije, baš, uvek i svuda, tako. Pre svega, samo pravo, često vrlo inertno, teško je prihvatilo novine kojima su se remetile njegove tradicionalne postavke. Mnogi pravni instituti nastali još u Rimskom pravu svakako nisu mogli da asimiliraju takve novine kakve su npr. softver, mikročip, telekomunikacije. To znači da tradicionalne grane prava (gradjansko, obligaciono, krivično, privredno, upravno i dr.) nisu mogle da se prilagode promenama, pa su i ostajale bez odgovora na pitanja kojim su ih obasipali novi trendovi razvoja.

S druge strane, radjanje novih grana prava predstavlja mukotrpan i relativno dugotrajan proces koji ne mora uvek da rezultira pozitivnim efektima. Tim više što mu obično prethodi dugotrajno stvaranje i izgrađivanje moralnih normi.

Teškoće koje su se pojavile u samom početku, a vremenom su postajale sve veće i pretile da osujete i ono malo što je uspelo da se izgradi. Srećom, narastanjem zahteva, ubrzanom izgradnjom etičkih normi od strane velikih proizvođača hardvera i

softvera, izuzetnoj zainteresovanosti moderne civilizacije i država za zaštitu prava i slobode pojedinaca i ličnosti, kao i razlike koje su oduvek postojale između anglo-saksonske (anglo-saksonski pravni sistemi su fleksibilniji i lakše podložni promenama) i kontinentalnih pravnih sistema (baziranih na Rimskom pravu) stvorile su mogućnosti za nastajanje novih grana prava i inovaciju postojećih. Tako u SAD-u, V. Britaniji, Australiji, Kanadi, početkom sedamdesetih godina ovog veka, nastaju koreni Kompjuterskog prava, Informacionog prava ili Prava informacione tehnologije. Ove nove grane prava predstavljaju značajan pomak ka kompleksnom rešavanju najznačajnijih pitanja koja se pred pravo postavlja vezano za KT. Pod pritiskom naraslih potreba i nadjenim rešenjima u novim granama prava određenih zemalja i tradicionalno pravo počinje da se otvara, a one zemlje koje u početku nisu pravom regulisale ova pitanja, postepeno su to počele da čine.

Iako u početku, Kompjutersko pravo postaje deo informacionog veka i potreba od kojih se, ma koliko to hteli i želeli, ne može pobeći.

## 2. Odredjivanje problema

Prihvatajući tvrdnju<sup>1</sup> da su informacioni sistemi stari onoliko koliko i ljudsko društvo, može se reći, da su se izuzetno značajne promene počele da dešavaju tek sredinom ovog veka, kada je dominacija "papira, olovke i činovnika" zamenjena kompjuterima i novim profilom stručnjaka. Mnogo se starog izmenilo, ali i mnogo novog pojavilo. Između ostalog, pojavili su se i prvi stručnjaci koji se profesionalno bave informatikom, kao i prvi veliki i mnogobrojni problemi. Kompjuteri nisu uvek dobro radili, rukovodioci su bili protivnici promena, a stručnjaci nisu imali niti veliko znanje, ni veliko iskustvo. Kasnih 60-ih i ranih 70-ih godina sistemi za obradu podataka postepeno prerastaju u sisteme stvaranja informacija. Računski centri rastu i dobijaju sve više poslova i sve veći značaj. Centralizacija kompjuterskih, informacionih i komunikacionih usluga postupno postaje nužnost. Sredinom 70-ih prvi mini i mikro kompjuteri nagoveštavaju promene koje će imati dalekosežne posledice. Brže, jeftine i korisnički orjentisane mašine obezbeđuju efikasna rešenja mnogih problema, koji u 80im godinama dobijaju i nove aspekte. Komunikacije između mašina ne samo što su postale tehnički moguće nego su prerasle u svakodnevnu nužnost. Rukovodioci, a i drugi zaposleni, sve se više interesuju za IS jer im oni, kao izvor - resurs rada i rukovodjenja, obezbeđuju podatke za stvaranje relevantnih slika o organizaciji i njenom okruženju,

---

<sup>1</sup> Edwards C., Savage N., Walden I., Information Technology & The Law, Basingstoke, MacMillan Publishers LTD, 1990., str. 2.

prošlosti, budućnosti<sup>2</sup> i tako postaju neophodna komponenta poslovanja. Istovremeno, mnogi rutinski poslovi, kao što su kancelarijski, postaju područje sve veće primene KT. Takođe, mnoga područja uprave (naročito vojna) postaju pogodno tle za sve veću primenu ovih tehnologija (ne sme se zanemariti činjenica da su baš vojne potrebe bile pionirska oblast korišćenja KT, te da su upravo iz njih krenule i prve aplikacije za poslovne procese). Sve faze razvoja kroz koje je prošla KT<sup>3</sup>, bile su brze, a promene koje je izazvala gotovo munjevit, što je karakteristika veka u kome živimo. Sve ono što je nekad bilo nezamislivo postaje stvarnost i svakodnevica. Ali problemi, takođe, postaju deo svakodnevnih ili, bar, čestih glavobolja. F. Lobel je još 1984. godine naveo da je samo u SAD-u prodato kompjuterskog hardvera za oko \$65 biliona, a softvera za \$16.2 biliona<sup>4</sup>. Oko 1.000 kompanija je pravilo programe, a niko nije tačno znao koliko je programa postojalo, procene su se kretale između 8.000 - 40.000. Istovremeno se isticalo, da programeri mogu postati milioneri u 20-oj godini jer mogu lako ukrasti softver i uz malu modifikaciju zaraditi više miliona dolara. A kako je tek danas?

Problemi postaju sve ozbiljniji i zahtevaju sve češću pomoć pravnika i sve veću potrebu za pravnim regulisanjem. Međutim, ni pravnici ih neće moći da reše bez pomoći informatičara. Otuda bi svi oni koji se bave obradom podataka ili se služe KT trebalo da imaju osnovno znanje iz oblasti prava, kako bi mogli da definišu problem i procene kolika i kakva im je pomoć pravnika neophodna.

Potrebno<sup>5</sup> je znati:

1. kako, ukoliko je to moguće, izbeći pravne probleme?
2. kako ih, ukoliko su već nastali, identifikovati?
3. koliko će vremena, ljudi i novaca biti potrebno za otklanjanje njihovih posledica?
4. ko, kakvu i u kojim rokovima može pružiti pomoć i kakva se naknada i od koga može očekivati?
5. kakve su šanse za uspešno rešavanje problema?

Naravno, sve ovo je moguće rešiti ukoliko postoji pravni sistem koji je slične probleme, odnose i pojave već obuhvatio, kao i društvo u kome pravo besprekorno funkcioniše. Kako to, na žalost, nije slučaj sa našom zemljom, postoji samo jedno

<sup>2</sup> Everest G., Database Management, Objectives, System Functions, and Administration, New York, McGraw-Hill Book Company, 1986., str. 2.

<sup>3</sup> Eaton J., Smithers J., Curran S., This is IT, A Manager's Guide to Information Technology, Oxford, Philip Allan, 1988., str. 14.

<sup>4</sup> Lobel F., Foiling The System Breakers, New York, McGraw Hill Book Company, 1986., str. 12.

<sup>5</sup> Mawrey R., Salmon K., Computers and the Law, Oxford, BSP Professional Books, 1988., str. XI.

pitanje koje se kod nas može postaviti - da li uopšte pravo može da odgovori na bilo koje od definisanih problema? S obzirom, na postojeće stanje, na odgovore ćemo još dugo čekati, samo da ne bude prekaasno, jer se tada negativne posledice teško moći otkloniti. Jedna se već pojavila - Jugoslavija je posle Hong Konga i Kine najveći softverski pirat.

Ipak, nekih pionirskih pokušaja na ovom planu ima. Jedino nam ostaje nada da će se u skoroj budućnosti ove teškoće savladati.

Znači, da bi pravo moglo da se izbori sa problemima koji nastaju razvojem informatike neophodno je da se zadovolje određeni preduslovi; da se obezbedi povoljno dejstvo odgovarajućih činilaca, odnosno, da se obezbede takve mehanizme koji će omogućiti paralelni razvoj informatike i prava.

### **3. Uredjivanje pravnih osnova korišćenja kompjuterske tehnologije**

Pravni aspekti sigurnosti IS i zaokupljenost pravnika i informatičara kako pravno rešiti probleme korišćenja KT novijeg su datuma. U stvari, samo četvrt veka je prošlo od donošenja prvih zakona o zaštiti podataka, dvadeset sedam godina od prve presude za kradju učinjenu pomoću računara<sup>6</sup>, dvadeset četiri godine od unošenja u jedan pravni akt autorskog prava na računarskim programima.

Istovremeno sa prvim zakonima koji su za predmet imali neko od ključnih pitanja iz oblasti primene KT ili funkcionisanja IS počelo je i osnivanje nacionalnih, državnih ili profesionalnih, komiteta, udruženja, komisija, biroa i drugih tela koja će se kontinuirano baviti pravnim problemima iz ovog područja. To je, npr., američko Udruženje za Kompjutersko pravo (*Computer Law Association*)<sup>7</sup>.

Razvijene zemlje sveta danas ova pitanja i probleme stavljaju u žižu interesovanja angažujući svoje najbolje pravnike kako bi pronašli najpogodnija rešenja za zaštitu pojedinaca, ali i nacionalne privrede jer shvataju značaj informatike za porast nacionalnog dohotka i ukupnog razvoja. Osnivaju se profesionalne asocijacije i instituti

<sup>6</sup> McKnight G., *Computer Crime*, London, Michael Joseph, 1973., str. 13.

<sup>7</sup> Erdelez., S., *Kompjutersko pravo, informatičko pravo ili informacijsko pravo*, Pravni vjesnik, br. 6/90., str. 174.

koji treba da prate ovu problematiku i izradjuju odgovarajuće studije na osnovu kojih će se zakonodavna tela moći oglasiti odgovarajućim pravnim aktima<sup>8</sup>.

Pored toga, na spremnost da se pravno reše ovi specifični problemi svakako je uticao i razvoj **međunarodnog prava**. Naime, kako IS i KT sve više poprimaju "anacionalnu" prirodu jer se njima zadovoljavaju potrebe međunarodnog tehnološkog razvoja i prometa specifične robe i usluga, kao i zbog toga što se razvojem telekomunikacija i EDI omogućuje prekogranični tok podataka, tako oni sve više dobijaju elemente inostranosti. Rešenja su se razlikovala od zemlje do zemlje, a te razlike su dovele do neophodnosti donošenja međunarodnih normi o pravnoj zaštiti KT i IS.

U početku to su bili **bilateralni sporazumi** između zemalja koje su realizovale pravni promet tehnologije, informacija, softvera i usluga. Ovim sporazumima regulisala su se pitanja iz oblasti tehničko-tehnološke i informatičke saradnje, sa po nekim problemom vezanim za konkretne podatke i ICC usluge (npr. SAD i Japan su sklopili sporazum o zaštiti mikročipova u međusobnoj trgovini, ali i u odnosu na treće zemlje).

Ubrzo posle prvih bilateralnih ugovora počeli su da se sklapaju i **regionalni sporazumi**, kojima se obezbeđuje odgovarajuća integracija i harmonizacija pravnih poredaka zemalja sa jednog geografskog područja. Tako, Komitet za pravnu saradnju EEZ-a 1976. godine osniva Komisiju za izradu evropske konvencije vezane za međunarodne tokove podataka, koja je 1980. predala tekst nacrtu. Ministarski savet, samo sa jednim uzdržanim glasom, prihvatio je ovu Konvenciju.

Kako ni to nije bilo dovoljno, donete su međunarodne konvencije, deklaracije, rezolucije, preporuke u okviru pojedinih **međunarodnih organizacija**. Ovi **multilateralni sporazumi** predstavljali su pravni okvir za izgradnju i primenu odgovarajućih principa, unifikaciju pravnih sistema zemalja potpisnica i regulisanje pojedinih pitanja od zajedničkog interesa (npr. klasifikacije, standardizacije). Tako, na primer, Svetska organizacija za intelektualnu svojinu osniva posebni Komitet eksperata koji izradjuje Model zakona za zaštitu kompjuterskog softvera još 1977. godine. Svetska unija za zaštitu autorskih prava na kongresu u Londonu 1986. godine donosi Rezoluciju o zaštiti kompjuterskog softvera i integrisanih kola. GATT 1994. godine, u okviru Urugvajске runde pregovora, donosi poseban Sporazum o trgovinskim aspektima prava intelektualne svojine obuhvatajući i zaštitu računarskih programa, baza podataka i

<sup>8</sup> Tako je, npr., u Velikoj Britaniji rešavanju pitanja neautorizovanog pristupa podacima, kao posebnom krivičnom delu, prethodila obimna studija posebnog Komiteta (Fraud Trials Committee Report).

topografije integrisanih kola. Pored ovih specijalizovanih i druge medjunarodne organizacije osnivaju posebne savete, komitete, komisije koje treba da: na osnovu studija stanja u zakonodavstvima zemalja članica, pronadju i predlože univerzalna rešenja za rešavanje određenih pitanja. OECD preduzima intenzivne akcije u praćenju i analizi kompjuterskog kriminala, a i posebna grupa eksperata (Komitet za politiku u informacijama, kompjuterima i komunikacijama - *ICCP Committee*) izrađuje studiju o zaštiti privatnosti u medjunarodnim tokovima podataka na osnovu koje se donosi i posebna preporuka 1980. godine. ISO 1986. i 1987. godine prihvata OSI standarde kao skup standarda vezanih za sigurnost otvorenih, medjusobno povezanih, sistema.

Neka od pitanja (zaštite podataka, privatnosti, ICC usluge i sl.) našla su se i u Univerzalnoj deklaraciji o ljudskim pravima UN, Evropskoj konvenciji o ljudskim pravima, Univerzalnoj poštanskoj konvenciji, Medjunarodnoj konvenciji o telekomunikacijama, itd.

Tako su medjunarodnim normama, takodje, stvorene realne mogućnosti da se pravo prilagodi potrebama, promenama i zahtevima savremenog informacionog razvoja.

Sve ove aktivnosti predstavljaju značajne korake u pravnom, nacionalnom i medjunarodnom, regulisanju vitalnih ili gorućih pitanja vezanih za pravne osnove KT. Istovremeno, one ukazuju i na značaj koji ovaj aspekt ima. Iako na prvi pogled izgleda da su pravni aspekti IS i KT novijeg datuma, to i nije baš tako jer su se odmah ili neznatno nakon pojavljivanja prvih ozbiljnijih problema, manje ili više, rešavali uspešno. Naravno, ovakvi pokušaji činjeni su u zemljama razvijenih tehnologija, kao i u onim koje su na vreme shvatile značaj ove problematike.

Kod nas to teče veoma sporo, mada se neka najelementarnija pitanja već polako počinju ugradjivati u pravne propise. To je slučaj sa Zakonom o izmenama i dopunama Zakona o autorskom pravu, sa početka 90-ih, koji je kao novinu uveo autorskopravnu zaštitu računarskih programa. Medjutim, za druge probleme još uvek nisu nadjeni odgovori. Tako je, npr., pre nešto više od desetak godina (1981.) uradjena studija za Izvršno veće Skupštine SR. Srbije o obezbedjenju i zaštiti podataka sa stanovišta informacionog sistema SR Srbije van pokrajina, nakon koje je usledio i nacrt zakona. Medjutim, na tome se stalo. Republički zakon nije donet, kao što nije donet ni savezni. Propuštena je izuzetna prilika i izgubljeno je dragoceno vreme. Ništa bolje nije ni sa zaštitom mikročipova, mada se ono postavilo i kao delegatsko pitanje u Skupštini Jugoslavije (1989.). Zakon o obligacionim odnosima, takodje, nije obuhvatio ni jednu specifičnost ugovora vezanih za softver, podatke, hardver i njihovo osiguranje i sl. Krivični zakon SRJ je bio nekoliko puta menjan, ali o uključivanju kompjuterskog

kriminaliteta u njega još uvek se ne vode diskusije. Ista je situacija i sa republičkim zakonima.

Ako se tome dodaju još i konstatacije: da se usled pravne nesigurnosti i stalnih promena pravnih normi ne mogu uneti kompetentne izmene, kao i da ne postoje kompletni pravni IS koji bi obuhvatali, ne samo norme nego i sudsku praksu i tako olakšali izradu odgovarajućih analiza i studija, na osnovu kojih bi se mogla formirati i neka rešenja i da se o tome ne mogu oformiti ni etičke norme. Na žalost, našim organizacijama pogoduje ovakvo stanje jer mogu da rade kako hoće i da nikome ne odgovaraju pošto je inertnost sistema tolika da se još verovatno dugo vremena neće ništa promeniti. Onda je jasno zašto mi zaostajemo i na ovom planu za drugima.

#### 4. Može li se govoriti o novoj grani prava?

Paralelno sa reagovanjem pravnih sistema na zahteve koje su pred njih postavili razvoj i primena KT i IS i na koje je trebalo odgovoriti nekakvim rešenjima, u odgovarajućim normama nazire se i ideja o neophodnosti postojanja nove grane prava. Naime, pravo je na novonastale zahteve moglo reagovati na nekoliko načina: ćutanjem, analogijom i stvaranjem nove, sui generis, grane prava.

**Ćutanje prava** je u početku bio najčešći odgovor na mnogobrojna pitanja koja su se mu postavljala, a koja su bila vezana za razvoj KT i IS. Na primer, u mnogim doskorašnjim socijalističkim i nerazvijenim zemljama u kojima se ovaj razvoj nije odvijao u razmerama kao u informaciono razvijenim zemljama, problemi vezani za moderne KT nisu se ni postavljali. S jedne strane, to je posledica nedostupnosti ovih tehnologija (ili malog broja njihovih aplikacija) čije sporadično i pojedinačno primenjivanje nije zahtevalo neke posebne aktivnosti vezane za promenu prava. S druge strane, naročito u nerazvijenim, a u početku i u razvijenim zemljama, nije se shvatalo da ove tehnologije menjaju tradicionalne načine postupanja sa podacima i informacijama<sup>9</sup>. Naime, pre nastajanja KT obrada podataka je uvek bila vezana za njihove materijalizovane oblike tako da se u svakom momentu znalo: šta neki medijum nosi i kako sa njim postupati. Primera radi, svaki dokument u pravnom prometu morao je biti uredno potpisan u nekoliko primeraka. Pojavom računara i EDI postavilo se pitanje pravne valjanosti faksimila umesto potpisa i sl. Takodje, postavljalo se pitanje dokazne snage kompjuterskih zapisa umesto uobičajenog zapisa na papiru. Kako tek reagovati na telekomunikacije i mogućnosti transfera ogromnih novčanih suma, bez opipljivih, zvečećih moneta? Kao moguće rešenje, u početku, najlakše je bilo ignorisati njihovo

<sup>9</sup> Erdelez S., op. cit., str. 172.

postojanje i držati se poznatih stvari. U takvim okolnostima pravo je oćutalo postojanje ovih promena i dugo bilo nepripremljeno i zbunjeno i nije imalo ništa značajno da kaže, na postavljena pitanja od strane informatike <sup>10</sup>.

Sledeći način bio je primena **analogije**. To je bilo moguće u situaciji kad su IS počeli tek da se razvijaju i kad posledice njihove primene nisu izazivale korenite promene u postojećoj praksi. Na osnovu analogije zaštita ličnosti koja je mogla biti ugrožena postojanjem i korišćenjem podataka (automatski obradjenih) mogla se vršiti primenom prava privatnosti, poznatog još od kraja prošlog veka. Znači, nije bilo neophodno ništa menjati, već analogijom primeniti postojeća rešenja, na nove slučajeve. Isto je bilo i sa zaštitom softvera, odnosno računarskog programa koji se podvodio pod književna dela i uživao istu autorskopravnu zaštitu, kao i roman. Analogija je mnogo duže korišćena za krivična dela u kojima je predmet "napada" ili sredstvo bio računar. Podvodjenjem kradja u kojima se računar pojavljuje kao objekat ili sredstvo pod isti tretman kao i klasično izvršenih kradja predstavljalo je prvobitni odgovor prava na sve specifičnosti kompjuterskog kriminaliteta. Drugim rečima, primenom analogije trebalo je popuni sve one pravne praznine koje su nastale pojavom KT. Pravo, u početku, nije moglo, ali, nije ni htelo da odgovori na ovaj izazov jer ga nije evidentiralo, kao veliki i konstantan problem, pa otuda nije ni znalo da nadje rešenja.

Treći način rešavanja mnogobrojnih problema proisteklih iz razvoja KT i IS je **stvaranje nove, posebne, grane prava**, odn., radjanje nove pravne discipline. Ta nova disciplina trebalo bi da se bavi teorijskom obradom ove oblasti prava kako bi se moglo rešiti mnoštvo pitanja koje kompjuterizacija postavlja. Ova pravna disciplina ima i svoje posebnosti. Isto tako, Kompjutersko pravo je i nova grana prava koja obuhvata skup pravnih normi koje se bave odnosima nastalim upotrebom kompjuterske tehnologije. Nove propise trebalo ubrzano donositi kako bi mogli da prate razvoj i regulišu mnoga pitanja vezana za KT i IS. Opasnosti koje nastaju u slučajevima prebrzog donošenja novih propisa, gotovo su veće od onih ako se propisi uopšte i ne donose. Naime, kako se broj problema skoro svakodnevno povećava, kako su raznovrsni subjekti kojima je u interesu da se ovi problemi regulišu, kako oni postaju sve uznemireniji i nestrpljiviji u čekanju da se nadju odgovarajuća rešenja za njihove probleme, kako su i države sve zainteresovanije da se oni stvarno i reše gledajući u njihovom rešavanju izbegavanje višestrukih dilema i ostvarivanje sopstvenih interesa (npr. prevlast nad drugim zemljama, novi oblik kolonijalizma, osvajanje novih tržišta, redukcije cena u odnosu na vodeće zemlje - SAD i Japan, postavljanje ili savladavanje raznih barijera) to se i nastajanje novih propisa i nove pravne discipline može vezati za relativno brzoplete, nategnute i iznudjene aktivnosti koje se brzo mogu osvetiti njihovim

<sup>10</sup> Kirby M., Access to information and privacy: the ten information commandments, Government Information Quarterly, no. 3/86, str. 333.

tvorcima. Ipak, apstrahujući ove, ali i mnoge druge opasnosti i manjkavosti, može se konstatovati da sve, iole, informaciono razvijene zemlje ubrzano rade na donošenju novih propisa, a njih prati i razvoj nove pravne discipline. Nova pravna disciplina koja je na pomolu, izazvala je mnoge nesuglasice i razmimoilaženja među pravnicima - da li se uopšte može govoriti o novoj disciplini, kako da se zove i šta bi sve trebalo da obuhvati?

## 5. Šta je Kompjutersko pravo?

Kompjutersko pravo nastaje kao odgovor prava na kvalitativno nove odnose proistekle iz kompjuterizacije svih domena ljudskog života i rada. Ono je novonastajuće, kompleksno, područje savremenog prava koje nosi sve osobenosti novih pravnih disciplina za koje pojedini strani<sup>11</sup> i jugoslovenski<sup>12</sup> teoretičari navode da su:

- sa nadnacionalnom dimenzijom i globalnim rešavanjima;
- sa nizom specifičnosti u zaštiti prava, naročito ličnih i imovinskih;
- u pitanju pravni odnosi koji se odvijaju u okvirima "zatvorenih" kompjuterskih sistema, ali zato međusobno tako povezanih i isprepletanijih da čine finu mrežu kojom se obavijaju svi ostali;
- sa izuzetno burnim razvojem i takvom dinamikom koja ukazuje da će se stalno pomerati granice ka novim područjima;
- sve više interdisciplinarnog sastava u koji pored pravnih mogu ući i "nepravni" odnosi kako bi se bolje sagledali odnosi koji nastaju razvojem i primenom kompjuterske tehnologije.

Što je ono u stvari? Može se reći da je Kompjutersko pravo, u suštini, nova, samostalna grana prava i nova naučna disciplina koja se u pravnoj nauci pokušava оформiti u toku poslednjih nekoliko dekada. S obzirom da su pojave koja ona treba da reguliše nove još uvek postoji nesuglasje oko njene prirode i predmeta. Pogotovo što pravnici "proizašli" iz škole evropskog kontinentalnog prava još uvek u nedoumici oko postojanja ovog prava, kao i njegovog predmeta i mesta. Tim više što se pojavilo i Informatičko pravo (poreklo mu je u Francuskoj), Informaciono pravo (najveći broj

<sup>11</sup> Saxby S., The role of law in the development of the information society, Pravni vijesnik., str. 6/90, str. 163 - 167; Seipel P., Computing Law: perspectives on the new legal discipline, Stockholm, Liberfoerlag, 1977., str. 110; Mylott T., Computer Law for Computer Professionals, New York, Prentice Hall, 1984., str. 8.

<sup>12</sup> Mecanović I., Informatičko pravo - nova grana prava u nastajanju, Pravni vjesnik, br. 6/90, str. 203.

zagovornika ima u nemačkom i norveškom pravu<sup>13</sup>) i Pravo informacione tehnologije (postojbina mu je Velika Britanija u kojoj i ima najveći broj pristalica<sup>14</sup>, mada je u poslednjih nekoliko godina sve veći broj pristalica i u drugim zemljama<sup>15</sup>). Situacija je nešto bolja u zemljama Common Law sistema u kojima se priznaje sva kompleksnost materija, kao i postojanje još uvek velikih nedoumica, ali se, ipak, insistira na činjenici da je Kompjutersko pravo već "nešto" što je evidentno prisutno i čemu ne treba postavljati "zamke" u diskusijama oko postojanja nego dalje rešavati pitanja koja se nameću razvojem KT. Naročito što se predstavnici ove "škole" manje bave rešavanjem teorijskih konverzi, već više pragmatičnim konstrukcijama realnih problema.

Znači, sve je sigurnije da je nova pravna disciplina nastala i pored svih razlika i razmimoilaženja u njenom definisanju. Za mnoga pitanja vezana za nju još uvek nema adekvatnih odgovora. Među njima svakako su najvažnija vezana za njeno odredjenje, obim, pa i naziv. Ovim se pitanjima, uglavnom, pristupa sa **dva različita stanovišta**. Predstavnici *prvog stanovišta* polazeći od uticaja kompjuterske tehnologije prihvataju postojanje Kompjuterskog prava kao nove pravne discipline i ukazuju da njegov predmet i obim tek treba postepeno i sistematski odrediti. To zahtevati veliki "intelektualni napor" mnogih ljudi. Pristalice *drugog stanovišta* polaze od preklapanja ove discipline sa informacionom politikom i problemima koje nameće "proizvodnja, širenje i upotreba informacija, a što ne zavisi od pojedinačne tehnologije"<sup>16</sup>. Iako je, na prvi pogled, drugo odredjenje prihvatljivije ono to ipak nije iz jednostavnog razloga zato što su to dve različite stvari. Kompjutersko pravo nije isto što i Informaciono pravo, prvo je vezano za razvoj i uticaj posebne tehnologije, a drugo za mnogo šire odnose - političke (informacione politike) čime se ono više vezuje za subjektivna prava i slobode pojedinaca. Kako rasprave još uvek traju, što je sasvim normalno, i kako "ne postoji jednostavan način da se stvori nova pravna disciplina, niti je to put kojim se brzo prolazi"<sup>17</sup>, jasno je da ovu posebnu pravnu disciplinu tek treba izgradjivati i razvijati. To je težak, neizvesan i mračan tunel kojim treba proći.

<sup>13</sup> Najeminentniji predstavnici su: norvežanin Jon Bing, nemaci Herbert Bukert i Herbert Fiedler, mada se pojavio i amerikanac Peter Marx koji najviše razvija ideju da ova nova grana prava nije vezana za informacionu tehnologiju već za informacije, o čemu više kod: Erdelaz S., op. cit., str. 176.

<sup>14</sup> Rodonačelnik je Stephen Saxby koji je, čak, bio editor Encyclopedia of Information Technology Law 1990 godine.

<sup>15</sup> Npr. u Australiji, Holandiji

<sup>16</sup> Tumačenje Sandre Erdelez definicije Informacionog prava Peter Marx-a

<sup>17</sup> Erdelaz S., op. cit., str. 177.

## 6. Predmet Kompjuterskog prava

Različita stanovišta o Kompjuterskom pravu reflektuju se i na pitanja definisanja njegovog predmeta. Svaki autor ima svoju definiciju, tako da postoji onoliko definicija koliko i autora (mada je njihov broj za sada nevelik). Ipak, iskristalisala su se **dva osnovna pristupa: po jednom**, predmet Kompjuterskog prava definiše se široko<sup>18</sup>, tako da postoji opasnost da se ne vidi njegova suština i predmet, odnosno "stvara se utisak da Kompjutersko pravo ne predstavlja jasno definiranu cijelinu"<sup>19</sup>; **po drugom**, ovo se pravo i njegov predmet definišu nabranjem pojedinačnih problema koje ono treba da reši i reguliše, a što predstavlja subjektivno viđenje svakog pojedinog autora i što, po pravilu, po mišljenima drugih, uvek postoji nešto što je namerno ili slučajno izostavljeno i što u kasnijem razvoju može predstavljati ozbiljan problem i izazivati sumnje u opravdanost i sistematičnost takvog pristupa. Među najizrazitijim predstavnicima drugog pristupa su i Lipner, Kalman, Scott, Reed, Tapper.

**S. Lipner i S. Kalman**<sup>20</sup> smatraju da je Kompjutersko pravo ne samo nova materija, već i materija u razvoju. Ono nije jedinstveno kao što je to slučaj, npr., sa Radnim ili Ustavnim pravom, **već oblast koja dodiruje druge, upravo onako kao što i kompjuteri, danas, zadiru u sve vitalne aspekte života i upliću se u svaku oblast prava**. Kompjuterska industrija nametnula je nova kompleksna pitanja društvu, vladama, poslovanju i međunarodnoj trgovini. Oni određuju predmet ove grane prava, ali se ogradjuju od teorijski raspravlja o njegovoj suštini, ističu **da su oblasti koje se njime "pokrivaju" amalgam prava i tehnologije**, pa često, sa neformiranim pravnim mišljenjima i rešenjima. Kao ključne **probleme koji čine okosnicu ovog prava** oni navode:

**a) zaštitu softvera i hardvera** - autorskopravna, patentnopravna, zaštita institutom poslovne tajne, zaštita ugovorima - opštim i pojedinačnim, o pravima raspolaganja računarskim programima koje razvijaju zaposleni;

**b) ugovore o sticanju prava na kompjuterskim sistemima** - prodaja "roba" i usluga;

**c) "licenciranje" kompjuterske tehnologije** - obuhvata dve različite vrste ugovora. Prvi se odnosi na klasične "prave" ugovore o naručivanju softvera koji će biti obuhvaćen licencom. Ovim se ugovorima regulišu međusobni

<sup>18</sup> Maylott, op. cit., str. 6; Fakes A., Choosing your computer law counsel, Information Management Review, vol. 15, no. 4/88, str. 23.

<sup>19</sup> Erdelez S., op. cit., str. 174.

<sup>20</sup> Lipner S., Kalman S., Computer Law, Cases and Materials, Columbus, Merrill Publishing Company, 1989., str. V.

odnosi nosioca prava intelektualne svojine i korisnika i daje dozvola za njegovo korišćenje. Druga vrsta ugovora su novi, "moderni", ugovori kojima se ugovorne strane dogovaraju o masovnoj prodaji softvera. To je, na primer, "licenca o prikupljanju omotača" (*shrink-wrap licensing*), odnosno ostvarivanje tzv. "doktrine prve prodaje" (*first sale doctrine*). Ove licence, u suštini, obezbeđuju trgovcima pravo da prikupljaju takse, garancije i sl. u prodajnim transakcijama;

**d) odgovornosti za greške koje nastaju korišćenjem kompjutera, pri programiranju i osiguranje od takvih slučajeva** - osiguranje od povreda i šteta obuhvata dva različita tipa: prve su fizičke i ekonomske koje se lako utvrđuju i na koje se jednostavno primenjuju tradicionalno pravo. Druga vrsta, koja je rezultat upravo informacione ere, označava konflikt između želje za podizanjem nivoa znanja i potrebe za zaštitom pojedinaca od zloupotreba drugih. Ovaj drugi tip povreda (šteta) pojavljuje se obično u kontekstu povreda ustavnih prava, prava privatnosti, povreda ugleda i sl.;

**e) kompjuterski kriminal** - uspešna prevencija, otkrivanje i kažnjavanje predstavljaju prvorazredni pravni problem sa kojim se treba suočiti, jer se pravo teško privikava na kompjutersku tehnologiju, a što istovremeno poslovi kompjuterske sigurnosti prerastaju u multimilionsku - dolarsku industriju.

S. Lipner i S. Kalman, na osnovu odgovora na postavljena, određena pitanja prognoziraju da će Kompjutersko pravo svojim sadržajem obuhvatiti i razvijati povećanje vrednosti tehnologije, obezbediti razumevanje neophodnih prinuda pravnog sistema, kao i osigurati zadovoljenje potreba društva.

**M. Scott<sup>21</sup>**, kao jedan od najpoznatijih autora koji se ovom problematikom bavi, određuje **Kompjutersko pravo kao skup pravnih doktrina koje su nastale ili su izmenjene pojavom kompjuterske tehnologije**. Kompjuterska tehnologija stvara niz problema koje treba pravno rešiti. **Najznačajniji problemi su:**

**a) zaštita softvera** - autorskopravna zaštita, patentnopravna zaštita, zaštita softvera javnim i običajnim pravom, zaštita ugovorima vezanim za zaposlene;

**b) kompjuterski ugovori** - ugovori koji za predmet imaju kompjutersku tehnologiju i kojima se definišu prava i obaveze ugovornih strana vezanih za njihov pravni promet, od garancija do provizija, od pravnih lekova do arbitraže;

**c) štete** - nehati u dizajnu i proizvodnji koji izazivaju štete, nehati u korišćenju i/ili nekorisćenju, namerne štete, krađe, napadi na privatnost, ucene, korupcije i sl.;

---

<sup>21</sup> Scott M., Computer Law, New York, John Wiley & Sons, 1987., str. 1-1.

**d) krivična dela vezana za kompjutersku tehnologiju** - aktivnosti koje mogu predstavljati krivična dela su: kradja, neautorizovani pristup, unos, korišćenje, programiranje, fizičko uništenje i sl.;

**e) prava pojedinaca** - koja su ugrožena kompjuterskom tehnologijom ili nova koja sa njom nastaju;

**f) dokazi** - legitimitet i dokazna snaga kompjuterizovanih informacija i sl.;

**g) takse** - uvozne i prodajne takse, carine, takse za korišćenje, porezi i sl.;

**h) zaštita mikročipova** - tehnologija proizvodnje i piratstvo, tretman, formalnosti za obezbeđenje zaštite, međunarodna zaštita i sl.

**C. Reed<sup>22</sup>**, Kompjutersko pravo definiše **kao granu prava koja reguliše informacionu tehnologiju**. Mada se ova tehnologija, pre svega, odnosi na kompjutere ona potencijalno označava i sredstva pomoću kojih se informacije prenose, kao što su telekomunikacije ili radiodifuzija. **Kompjutersko pravo ima objedinjavajuću ulogu.**

Reed navodi neka teorijska shvatanja po kojima nije neophodno da se Kompjutersko pravo izdvoji kao posebna oblast i da je ono, u stvari, samo primena već postojećih principa na novi set činjenica. Međutim, nove činjenice koje nastaju primenom KT su potpuno različite od novih setova činjenica vezanih za druge oblasti tehnologije. Objašnjavajući razliku između KT i klasične industrije, kao i ulogu prava vezanu za svaku od njih navodi da KT, u suštini, obezbeđuje informacije koje su, formalno gledajući, nešto kratkotrajno i koje treba da se pretvore u nešto što ima bilo kakav pa i, kvazi-fizički oblik. Ako je u pitanju trgovina, ona je moguća samo ukoliko se informacija pretvori u neki oblik robe. Tako, usluge koje vezane za baze podataka predstavljaju prodaju "čistih" informacija, kao što i softverske kuće prodaju odgovarajuće informacije u obliku softvera. Tradicionalna uloga prava je mnogo više nego samo regulisanje ovih aktivnosti, pošto pravo u procesu dopunjavanja postojećeg rešava sve ove aktivnosti i specifičnosti.

Kao **predmet Kompjuterskog prava** Chris Reed navodi:

**a) hardverski ugovori** - prodaja, licence i lizing, pregovaranje i zaključivanje ugovora, isporuka i plaćanje, prenos svojine i rizik, obaveze prodavca, obaveze kupca, posebne klauzule i sl.;

**b) softverski ugovori** - licence softvera, garancije, ograničenja i isključenja odgovornosti, "licenca o prikupljanju omotača" i sl.;

<sup>22</sup> Reed C., Computer Law, London, Blekstone Press Limited, 1993., str. 1.

**c) odgovornost za kompjuterski softver** - proizvođača i korisnika, ugovorene odgovornosti, uobičajene odgovornosti, nemarnosti, propusti u dizajnu, propusti u radu, nehat u vezi sa sistemskim izlazom, propusti u korišćenju kompjuterskog sistema, posebni problemi vezani za ekspertne sisteme i sl.;

**d) autorskopravna i patentnopravna zaštita softvera** - karakteristike autorskopravne i patentnopravne zaštite, patentibilnost i "autoribilnost" kompjuterskog softvera, razvoj u SAD, V. Britaniji i Evropskoj zajednici, prava tvorca i sl.;

**e) dizajn i zaštita mikročipova** - zaštita mikročipova pomoću modela i uzoraka;

**f) zaštita poverljivih informacija** - kategorije poverljivih informacija, obaveze koje nastaju zbog poverljivosti, javni interes za objavljivanje određenih informacija, posebni problemi poverljivih informacija i dolaženje do njih na nedozvoljen način, krivično pravo i sl.;

**g) kompjuterski kriminal** - prevare vezane za računar, neautorizovan pristup ili brisanje podataka, krađe informacija, budućnost kompjuterskog kriminala i sl.;

**h) dokazi;**

**i) zaštita podataka** - zaštita podataka i privatnosti, međunarodna aktivnost i razvoj nacionalnih prava i sl.;

**j) ekspertni sistemi** - pravni ekspertni sistemi i problemi vezani za njih;

i

**k) Kompjutersko pravo Evropske zajednice.**

**C. Tapper** je jedan od najjemenitnijih autora više knjiga o Kompjuterskom pravu. On polazi od činjenice da je specifičnost ovog prava upravo vezana za način na koji kompjuteri rade, tim više, što upravo kompjuteri od svih mašina najbolje, za sada, imitiraju čoveka<sup>23</sup> i što su rad ljudskog mozga mnogo više transformisali nego rad ruku<sup>24</sup>. Efekti koji se postižu njihovom primenom dovode do tehnoloških i komercijalnih promena. Međutim, nisu ništa manje značajne ni implikacije kompjutera na pravo. U kratkim vremenskim intervalima menjaju se uobičajena pravila i principi i stvaraju posebna, kako se pravo ne bi našlo u "mračnom tunelu" ignorisano integracijom kompjutera u, strogo zaokruženom i zatvorenom,

<sup>23</sup> Tapper C., Computer Law, London, Longman, 1989., str. 1.

<sup>24</sup> Tapper C., Legal Problems Posed by Computers International Consideration, edicija: Essays on Computer Law, Melbourne, Longman Professional, 1990., str. 5.

području prava. Tako, u odnosu na imovinu, pojava mas-tržišta računara donela je značajne promene u konceptu intelektualne svojine. Uvode se novine u odnosu na potrebe formiranja i unificiranja standarda radi olakćavanja prenosa podataka između raznih aplikacija. U oblasti odgovornosti naročito su značajna pitanja kriminala i privatnosti u novim konceptima i problemima vezanim za potrošačku, ugovornu i prekršajnu dimenziju. I na kraju, značajne su i promene koje nastaju u odnosu na postupke koji se menjaju zahvaljujući sve većoj primeni kompjutera, u raznim fazama (npr. upravnom ili krivičnom postupku) ali i sve većem broju parnica i njihovoj vrednosti, a koje se vode zbog mnoštva različitih problema vezanih za kompjutere.

Nabrajajući najznačajnije oblasti prava koje su pretrpele i najveće promene primenom kompjuterske tehnologije C. Tapper u suštini markira najznačajnija i ključna područja Kompjuterskog prava. Po njemu to su *sledeća područja* (mada ne isključuje i druga):

**a) svojina:** patent - primena na kompjutere, teorijske i praktične pogodnosti; autorsko pravo - osnove zaštite, nivoi primene na programe, audio-vizuelna sredstva, baze podataka, vlasništvo, prava trećih lica i sl.; poslovna tajna i nelojalna konkurencija - odnosi sa drugim oblastima, interesi podnosilaca žalbi ili tužbi, ponašanje tuženog, pravni lekovi i sl.; modeli i uzorci, žigovi; monopol i anti-trust; režimi po meri i sl;

**b) odgovornost:** ugovori - hardverski; softverski (sistemski i aplikativni) provizije, osiguranje i sl.; održavanje - softvera, hardvera; posebnih subjekata - trećih lica, personala; programerske usluge i konsultantske usluge; razne druge usluge - biroa, prodaje, lizinga, licence, pravni lekovi (posebne odredbe) i sl.; prekršaje, prevare, nehat, klevete i sl.; kriminal - problem kompjuterskog kriminala, klasifikacija dela, poseban kriminal, reforma sistema itd.; privatnost - značenje i nova rešenja, preventivne mere, pravni lekovi, zakonodavstvo;

**c) postupci:** dokazi - tehnička i pravna priroda problema, značenje, dokazna snaga i sl.; praksa - pre sudjenja, sudjenje.

Ukazujući na specifičnosti, kompleksnost, nedovoljnu konceptualnu zaokruženost, teškoće oko definisanja i određivanja same prirode ove nove grane prava, Colin Tapper ističe da još uvek postoji konfuzija o njegovom konceptu, a tamo gde vlada konceptualna konfuzija i što se više o nečem raspravlja to ono postaje sve sumnjivije. Cena razlika, a i rasprava su anomalije<sup>25</sup>.

---

<sup>25</sup> Tapper C., op. cit., str. 8.

Analizirajući izneta mišljenja o pojmu i predmetu Kompjuterskog prava može se konstatovati:

**Prvo.** Sve je manje sporno da je nastala *nova grana prava* i, da se vrlo brzo razvija menjajući ustaljena pravila i postulate prava. Ubrzani razvoj kompjuterske tehnologije i nastajanje njenog globalnog mas-tržišta će izazvati promene koje će, s jedne strane, primoravati ovu granu prava da ih rešava, a s druge, zahtevati određene promene u pozitivnim pravnim sistemima.

**Drugo.** Mada se gotovo svi slažu da je *Kompjutersko pravo, u suštini, skup pravnih normi, institucija i principa kojima se regulišu odnosi koji nastaju razvojem i primenom kompjuterske tehnologije*, ipak još uvek ne postoji jedinstvena definicija ovog prava. Pogotovo što ne postoji ni jedinstveno mišljenje šta se pod kompjuterskom tehnologijom podrazumeva. Uočljiva su dva tipična shvatanja: po užem, to je tehnologija koja je isključivo vezana za kompjutere, tehnike i principe po kojima oni funkcionišu<sup>26</sup>, dok bi po *širem* shvatanju pored kompjutera, ona obuhvatala i sredstva koja se na njima baziraju (ali ne telekomunikaciona) pomoću kojih se informacije prenose, kao i metode i tehnike koje za taj prenos služe<sup>27</sup>. Za sada ne postoje posebni razlozi da se ne prihvati prošireno shvatanje pojma kompjuterske tehnologije i isto tako proširenog predmeta ove grane prava. Naravno, ostaje pitanje da li će ovakvim određivanjem nastati nejasnoće i novi problemi i da li će to dovesti do prihvatanja drugih termina i sadržaja. Međutim, svi koji se ovom problematikom bave slažu se da postoji specifičnost pravnih pitanja koja proizlaze iz korišćenja i nastajanja ove tehnologije. Ceneći postojeće razlike mislim da je celishodnije **definisati Kompjutersko pravo na opšti način i tako izbeći da se neki problemi zanemare**, a što je još važnije, i da se ostavi prostor za one koje se ne mogu predvideti. Tim više, što su razvoj i promene koje izaziva kompjuterska tehnologija ne samo brze, teško predvidljive i sa širokom disperzijom u razna područja, već i zato što se mora voditi računa o osobenostima prava i njegovoj potrebi za koherentnošću, a često i o konfliktnim ciljevima koje treba da realizuje.

**Treće.** Zajednički imenitelj svim dosadašnjim shvatanjima koja se pojavljuju oko definisanja Kompjuterskog prava je: da je ono vezano za kompjutere, odnosno primenu kompjuterske tehnologije. Otuda kao *predmet regulisanja ovog prava se pojavlju odnosi koji sadrže prava i obaveze subjekata povodom razvoja i primene*

<sup>26</sup> Ovo shvatanje zastupa relativno velik broj informatičara, naročito onih starije generacije, i svi ono pravници koji su orijentisani ka drugim nazivima nove grane prava.

<sup>27</sup> Mnogobrojni su autori koji preferiraju ovom širem shvatanju, gotovo poistovećujući kompjutersku i informacionu tehnologiju, od informatičara to su R. Schware, T. Warner, J. D. Bolter, a od pravnikā ovakvom shvatanju skloni su C. Reed i donekle C. Tapper.

**kompjuterske tehnologije.** Ovi odnosi su, kao i KT, veoma rasprostranjeni, raznovrsni i sreću se u svim oblastima života. Pojedini su vezani za moralna prava i obaveze, a drugi su imovinski. U ove odnose stupaju i različiti subjekti međusobno od pojedinaca, preko organizacija do državnih organa.

**Četvrto. Predmet Kompjuterskog prava** (u objektivnom smislu<sup>28</sup>), kao skup normi obuhvata (ali ne i samo to):

- **zaštitu računarskih programa**, softvera, korisničkog interfejsa, produkata reverzibilnog programiranja, kompjuterski generisanih dela, naziva (patentnopravna, autorskopravna, zaštita žigom - roba i usluga, know-how, pravo suzbijanja nelojalne utakmice, srodnim pravima, sui generis i ostalim pravnim institutima);
- **zaštitu topografije integrisanih kola** (sui generis pravom);
- **zaštitu baza podataka** (pravom intelektualne svojine, sui generis pravom);
- **kompjuterske ugovore** (licenci, kupoprodajni, lizing, franšizing i ostali koji za predmet imaju kompjutersku tehnologiju i kojima se definišu prava i obaveze ugovornih strana vezanih za njihov pravni promet od garancija do provizija, od pravnih lekova do arbitraže);
- **zaštitu podataka, informacija i prava pojedinaca ugroženih kompjuterskom tehnologijom** (privatnost, informaciona privatnost, privatnost e-pošte i sl.);
- **kompjuterski kriminalitet**, odn. krivična dela vezana za kompjutersku tehnologiju (kod kojih kompjuteri imaju ulogu: objekta, subjekta, instrumenta, simbola);
- **odgovornost** (za štete i greške koje nastaju korišćenjem kompjutera, u programiranju, zaštiti podataka u organizacijama, prekograničnim tokovima, EDI okruženju i sl.);
- **osiguranje** (od raznih oblika rizika);
- **tehničke norme** kojima se regulišu razna pitanja softvera, hardvera, standarda;<sup>29</sup>
- **metodologiju** prikupljanja, obrade, čuvanja, transfera i korišćenja podataka i informacija;<sup>30</sup>
- **legitimitet i autentičnost** dokumenata i informacija dobijenih primenom kompjuterske tehnologije (dokazna snaga i sl.); i

<sup>28</sup> Pored Kompjuterskog prava u objektivnom smislu kao skupa pravnih normi kojima se regulišu odnosi koji nastaju usled razvoja i primene kompjuterske tehnologije, pojavljuje se i Kompjutersko pravo u subjektivnom smislu kao pravna vlast koju subjekt prava crpi iz normi ovog prava u objektivnom smislu.

<sup>29</sup> Mecanović I., op. cit., str. 205.

<sup>30</sup> Mecanović I., op. cit., str. 205.

- drugi problemi koje treba pravno rešiti.

Ovaj predmet je u razvoju sa tendencijom stalne promene i dopune, onako kako se menja kompjuterska tehnologija i odnosi koji njenim razvojem i primenom nastaju.

**Peto. Kompjutersko pravo je savremena, posebna, samostalna, grana prava, ali i deo jedinstvenog,** po karakteru i nameni, **nacionalnog sistema prava**, tako da se sva načela i pojmovi ovog sistema protežu i na njega. Ono je tesno povezano sa drugim granama. Medjutim, ono se tesno povezuje i sa medjunarodnim normama i granama prava koje regulišu odgovarajuće medjunarodne (naročito ekonomske, poslovne) odnose.

**Šesto. Kompjutersko pravo je i kompleksno pravo.** Sva njegova kompleksnost proističe iz složenosti predmeta koji je podložan brzim promenama i intenzivnom razvoju, s jedne strane, i sve složenijim odnosima koji nastaju razvojem i primenom kompjuterske tehnologije. Naravno da delovi ovako složenog predmeta mogu biti, svaki za sebe i deo predmeta nekog drugog prava, odnosno pravne discipline, to znači i gubitak sve specifičnosti i složenosti, s obzirom da bi se rešenja davala primenom načela i metoda koja važe za te discipline i grane. To nije dovoljno i ne odgovara novonastalim zahtevima. Isto tako, prosto zbrajanje pojedinačnih rešenja datih u različitim disciplinama i granama, ma koliko srodne bile, ne može zadovoljiti svrhu njihovog povezivanja i rešavanja kompleksnog problema. I pored dinamičnosti koja zahvata sve veći broj grana i pravnih disciplina, pitanje da li su i koje od njih spremene da se brzo menjaju koliko to zahteva ovaj specifičan predmet, te rešenja koja one nude obiluju tradicionalnošću, konvencionalnošću, a često inertnošću i tvrdokornošću. Sve je to znatno ispod potreba koje se u razvoju i primeni kompjuterske tehnologije pojavljuju.

Na kraju, neophodno je istaći da je Kompjutersko pravo nastalo, ali da još mora mnogo da se uradi i na teorijskom i na praktičnom planu, da bi se afirmisalo, konceptualizovalo i dalje izgradjivalo. Ovo se, svakako, odnosi i na nas.

## 7. Istorijski razvoj Kompjuterskog prava

Izučavanje razvoja Kompjuterskog prava vezuje se za razvoj kompjuterske tehnologije i uređjivanje pravnih osnova njene primene. Postoje određene teškoće u tom izučavanju izmedju ostalog i zbog tradicionalnih metoda kod obrade ovih pitanja u oblasti pravnih nauka, što je posledica “primene pravila da se u pravnoj literaturi

izučava razvoj doktrine i pravne teorije”<sup>31</sup> za koje se vezuju momenti nastanka jedne grane prava. Kako je ovo sasvim nova grana prava to i nije izgrađena njena doktrina i teorija, što bi značilo da o njenom razvoju ne bi moglo biti reči. Međutim, odnosi koji primenom kompjuterske tehnologije nastaju postoje, kao što postoji i njihovo regulisanje, te se može konstatovati da u tom smislu postoji i ova grana prava i pravna disciplina. Njeno nastajanje vezuje se za SAD, kao zemlju u kojoj se kompjuterska tehnologija najrasprostranjenija. Negde šezdesetih godina R. Freed, ukazujući na pravne posledice koje mogu nastati korišćenjem kompjutera, naglašava da, upravo pravnici moraju biti veoma ooprezni “kako im roboti ne bi pobjegli iz ruku”<sup>32</sup>. Ubrzo, posle toga, se javljaju i prvi radovi u kojima razmatra pravna problematika vezana za računare, stidljivo nazivane imenom: **Kompjutersko pravo**. Pored R. Freed-a, B. Bigelow, H. Marks, F. Lafer, S. Nycum i nekoliko drugih američkih pravnika, mahom praktičara, sve intenzivnije koristi termin Kompjutersko pravo podrazumevajući pod njim različite stvari. Naime, kako ističu R. Bernacchi, P. Frenk i N. Statland<sup>33</sup> sa Kompjuterskim pravom se dešava isto što i sa mnogim drugim pravnim terminima i konceptima - svaki autor ima svoju definiciju i otuda ih je mnogo različitih. Ono što je bitno je da se sadržaj vezan za IS i KT postavi kao segment koji povezuje, na svoj način, ove probleme i stavlja posledice u kontekst komercijalnog sveta<sup>34</sup>. Naročito je bilo, i još uvek je, mnogo konfuzije oko određivanja predmeta, komponenti i područja koje ono obuhvata. Tako se, po njima, preteče ovog prava nalaze u nekim ugovorima o obradi podataka (npr. *Data Processing Contracts*). Pod tim nazivom objavljena je i knjiga 1974. godine u kojoj je dat koncept oblasti prava poznate pod nazivom "Kompjutersko pravo" koje je obuhvata sledeće: pravne i praktične aspekte upotrebljavanja IS i KT; razvoj, zaštitu i promet proizvoda visoke tehnologije i druge predmete vezane za njih.

Prve rasprave, kao i pojavljivu Kompjuterskog prava pratile su mnoge nedorečenosti, manjkavosti i nejasnoće, ali istovremeno i sve veći broj radova i po neka knjiga<sup>35</sup>.

<sup>31</sup> Sličan problem pojavio se i kod prikaza istorijskog razvoja Međunarodnog privrednog prava, te su prihvatljivi stavovi prof Radomira Djurovića koji u raspravljanju oko va'njih momenata razvitka ove grane prava iznosi upravo ovu konstataciju. Videti: Djurović R., Međunarodno privredno pravo, Beograd, Savremena administracija, 1991., str. 13.

<sup>32</sup> Freed R., A lawyer's guide through the computer maze, The Practical Lawyer, no. 7/60, str. 16.

<sup>33</sup> Breach R., Frank P., Statland N., Bernacchi On Computer Law, A Guide to the Legal and Management Aspects of Computer Technology, Boston, Little, Brown and Company, 1986., str. XXVI i XXVII.

<sup>34</sup> Bernacchi R., Frenk P., Statland N., op. cit., str. 1-1.

<sup>35</sup> Bender C., Computer Law: Evidence and Procedure, 1978.; Bigelow, Computers and Law: An Introductory Handbook, 1966.; Tapper C., Computer Law, 1978.; i dr.

Pravi razvoj Kompjutersko pravo doživljava početkom 80-ih, a procvat početkom 90-ih. I ne samo da su pravnici-praktičari bili zaokupljeni ovim pravom i problemima koji se njime rešavaju (npr. u predgovoru četvrtog izdanja svoje knjige Colin Tapper<sup>36</sup> ističe: "kad se prvo izdanje moje knjige Kompjutersko pravo pojavilo - 1978. godine - bilo je samo nekoliko opštih monografija o ovom predmetu na engleskom jeziku. Pri pretraživanju pravne baze podataka LEXIS po ključnoj reči **kompjuter** za 1977. godinu u SAD, na federalnom nivou, bilo je 201 sudski slučaj i 246 na nivou federalnih država, dok je 1987. broj slučajeva porastao na 963 na federalnom nivou i 873 na nivou federalnih država, odnosno, za 479% i 355%. U Velikoj Britaniji 1977. bilo je svega 20 ovakvih slučajeva, a 1987. već 102, odnosno za 510% više"), već se pojavio i veliki broj radova, knjiga, enciklopedija, monografija i specijalizovanih časopisa u kojima se i teorijski raspravlja, kao i veliki broj objavljenih radova vezanih za kompjuterske ugovore, informacionu privatnost, intelektualnu svojinu nad proizvodima KT, kriminal, poreze, prekršaje, EDI i prekogranične tokove podataka i sl.

U poslednjih nekoliko godina sve su intenzivnije aktivnosti i u pravima koja su manje bila u žiži interesovanja zbog uloge koju imaju. Tako se Kompjutersko pravo sve više proširuje na zemlje dalekog istoka: Japan, Maleziju, Singapur, kao i pojedine afričke zemlje<sup>37</sup>.

Što se Jugoslavije tiče, kod nas se uočavaju dve faze u razvoju: **prva**, inicijalna faza započinje početkom 70-ih i najveći domet ima početkom 80-ih kad se pojavljuju prvi radovi kojima se obuhvataju neka parcijalna pitanja<sup>38</sup>. Ovu fazu karakteriše raznorodnost pristupa i pokušaj da se markiraju određeni pravni problemi kompjuterizacije kod nas, kao i da se ovi problemi rešavaju više u sklopu već postojećih grana prava i pravnih disciplina. **Druga faza** započinje u vreme najrazvijeneg dela prethodne faze i teče paralelno sa njom, pri čemu svoj glavni zamajac ima od početka 90-ih. U ovoj fazi pokušavaju se dati osnove Kompjuterskog prava, raspravljati o tome kako se pravo prilagođava novom, dinamičnom i zabrinjavajućem kompjuterskom okruženju i razmišlja o potrebnim promenama koje predstoje pravu uopšte. Vodeću ulogu u ovoj fazi imaju Sandra Erdelez, Stevan Lilić, Ivan Mekanović i drugi autori koji

<sup>36</sup> Tapper C., op. cit., str.XLIV.

<sup>37</sup> videti: Miller J., Recent Developments in Computer Law in New Zeland, edicija: Essays on Computer Law, Melbourne, Longman Professional, 1990., str. 535 - 548; Kang A., Current Developments in Computer Law in Singapur and Malasia, ista edicija, str. 548 - 558; Konyn I., South African Computer Law, ista edicija, str. 660 - 681.

<sup>38</sup> Videti radove: Živka Anzulovića, Alojzija Fin'gara, Milice Gačić, Borut Justina, Dragoljuba Kavrana, Vide Kočevar, Slavice Krmeta, Dragana Medvedovića, Gabrijele Mikulec, Borislava Milića, Kreše Puharića, Alenke Šelih, Lovre Šturma, Vladimira Vodinića.

pokušavaju da daju odgovore na mnogobrojna pitanja<sup>39</sup>. Pravi razvoj tek treba očekivati.

## 8. Izvori Kompjuterskog prava

Izvori prava, te i Kompjuterskog, proističu iz specifičnosti odnosa koji se stvaraju i vezani su za određenu oblast prava. Kao izvori Kompjuterskog prava, s obzirom na već stvorene relacije u regulisanju konkretnih odnosa<sup>40</sup>, a bez obzira na njihovu neizgradjenost i nedefinisanost, pojavljuju se opšti (zajednički) i posebni (autonomni, specifični) izvori. Oni istovremeno mogu biti na nacionalnom i/ili na međunarodnom planu. **Opšti izvori** proističu iz opšte prihvaćenih izvora prava i vezani su, u nacionalnim okvirima, za pozitivne propise, običaje, sudsku praksu i pravnu nauku. No, pored sagledavanja izvora prava u pravnom sistemu jedne zemlje (i našem, takodje) za Kompjutersko pravo je od izuzetnog značaja obuhvatiti i šire pravne okvire u koje se uklapa strategija i politika nacionalnog razvoja kompjuterske oblasti, kao i pojedini segmenti vezani za njih (npr. intelektualna svojina).

Naravno, kompjuterska tehnologija stvara mnogobrojne i raznovrsne odnose koji široko prevazilaze nacionalne okvire i koji dovode do efekta “globalnog sela”, te su međunarodni izvori od izuzetnog značaja jer u mnogim slučajevima predstavljaju i izvor rešenja koja će se naći u nacionalnim propisima.

Pored ovih opštih izvora pojavljuju se i **posebni izvori**, koji, takodje, mogu biti u nacionalnim i međunarodnim okvirima. Oni predstavljaju pravni osnov za stvaranje autonomnog Kompjuterskog prava, a baziraju se na tehničkim normama i standardima, s jedne strane, i autonomnim voljama ugovornih strana, odnosno subjekata u poslovnim odnosima vezanim za kompjutersku tehnologiju, s druge.

### **Kao opšti nacionalni izvori Kompjuterskog prava pojavljuju se:**

**1. Ustavi<sup>41</sup>** - s obzirom da mnoga pitanja vezana za kompjutersku tehnologiju duboko zadiru u prava i slobode čoveka, to su ustavne odredbe od izuzetnog

<sup>39</sup> Videti pored radova navedenih autora i radove: Janka Araha, Zorana Arsića, Katarine Benedikt, Vesne Besarević, Sonje Dobrić, Mirjane Drakulić, Nelke Fikeys - Krnić, Mirka Ilesića, Mihe Juharta, Dušana Nikolića, Ivana Padjena, Zorana Paraća, Rajka Pirnata, Vladimira Popovića.

<sup>40</sup> Mecanović I., op. cit., str. 204.

<sup>41</sup> Mada se pod **zakonom u formalnom smislu** (u širem smislu) obuhvata i ustav, ali se zbog značaja koji ustavne odredbe imaju u odnosu na KT, one izdvajaju kao poseban izvor.

značaja za privatnost, informacionu privatnost i mnoga druga pitanja. Ustavne odredbe mogu predstavljati okvir ili barijeru za određene aktivnosti i odnose vezane za primenu i/ili razvoj KT. Tako je, npr., za zaštitu podataka i informacija veoma važan ustavni status i pozicija uprave u regulisanju pojedinih segmenata, kao i povezivanje pojedinih subjekata u prikupljanju, obradi, memorisanju, transmisiji i korišćenju podataka i informacija, zaštitu prava i sloboda i sl. Znači, ne retko, ustavne odredbe predstavljaju osnov za regulaciju određenih odnosa.

**2. Zakoni<sup>42</sup>** - pojavljuju se u dvostrukoj ulozi. Njima se reguliše određena materija vezana za pojedina područja Kompjuterskog prava (npr. Zakon o zaštiti topografije integrisanih kola) kao odredbama *lex specialis*-a ili regulišu druga područja, a uz njih i određena pitanja vezana za KT (npr. Zakonom o autorskom i srodnim pravima regulišu se kao autorska dela i računarski programi i baze podataka). U poslednjih desetak godina sve je veći broj podzakonskih akata kojima se regulišu konkretni odnosi i problemi. Podzakonski akti postaju nezaobilazni, naročito, u slučajevima kad nema osnova niti razloga za donošenje zakona. Tada države pribegavaju ovim aktima za uređivanje pitanja kakva su i, npr., tehničke i organizacione mere zaštite, postupak podnošenja patentne prijave i sl. Naravno, svi ovi akti zajedno trebalo bi da čine odgovarajuću pravnu mrežu kojom se štite odnosi, prava i obaveze, koje nastaju na osnovu i povodom razvoja i primene KT. Bilo bi izuzetno dobro kad bi se u okviru jedne zemlje, s obzirom na specifičnosti, pojavila i odgovarajuća kodifikacija kompletne materije koja čini ovo pravo (kao što je to slučaj sa kodifikacijama građanskog prava). Ipak, kako je ova materija u mnogim zemljama još uvek bez posebnog identiteta, to bi kodifikacija bila preuranjena, čak i u kompjuterski najrazvijenijim zemljama.

**3. Običaji** - za sada još uvek nisu u dovoljnoj meri izgrađeni kao izvor Kompjuterskog prava, jer se nije оформio ni poseban društveni odnos vezan za razvoj i korišćenje kompjuterske tehnologije. U ono malo radova koji su obuhvatali izvore Kompjuterskog prava izostao je ovaj izvor upravo iz navedenog razloga. Međutim, ako se i za ovo pravo prihvati, u savremenom poimanju izvora sve češće korišćena, objektivna teorija<sup>43</sup> po kojoj je dovoljno utvrditi da neki običaj postoji i da se primenjuje, onda bi se u tom kontekstu oni mogli pojaviti kao izvor. Tome bi trebalo dodati i činjenicu da se pod običajima više ne podrazumevaju samo nepisana pravila već "i ono na šta zakon koji reguliše određene odnose (npr. obligacione) upućuje u pojedinim slučajevima"<sup>44</sup>. Tim više, što bi se određena sistematizovana pravila, kao što

<sup>42</sup> Pod **zakonom**, u **formalnom smislu**, podrazumevaju se svi normativni akti kojima se regulišu odnosi vezani za KT, od akata koji se i zovu zakonima, pa do normativnih akata izvršne i upravne vlasti (uredbe, pravilnici, naredbe, i sl.).

<sup>43</sup> Vasiljević M., Trgovinsko pravo, Beograd, ABC Glas, 1992., str. 19, ističe da je napuštena subjektivna teorija po kojoj je za primenu običaja nužno dugotrajno vršenje i izričita ili prećutna volja stranaka.

<sup>44</sup> Djordjević Ž., Stanković V., Obligaciono pravo, Beograd, Naučna knjiga, 1987., str. 38.

su uzanse, naročito posebne, mogle odnositi na promet ili trgovinu kompjuterskim proizvoda i komponentama, kao posebnom vrstom poslovanja. Ove posebne uzanse bi se mogle naći kao izvor Kompjuterskog prava.

**4. Sudska praksa** - mada u našem pravu preovladava shvatanje da sudska praksa nije formalni izvor prava počinju da se pojavljuju i suprotna shvatanja po kojima u slučajevima kad ne postoje drugi formalni izvori, ona može dobiti ovu ulogu. Mada kod nas ne postoji tradicija anglosaksonskog prava u kojoj tumačenje norme najvišeg suda formalno obavezuje sve niže sudove, ipak tvrd stav o potpunom negiranju sudske prakse, kao izvora, izgleda posebno nepodesnim kad je u pitanju Kompjutersko pravo. Pogotovo što mnoga pitanja iz oblasti razvoja i primene kompjuterske tehnologije nisu rešena u zakonima ili drugim formalnim izvorima prava, a takva praznina može predstavljati ozbiljnu kočnicu daljeg razvoja, s jedne, i ograničavanja prava subjekata, s druge strane. U takvoj situaciji sudska praksa, odnosno sudske odluke kojima bi se ta praznina popunjavala mogla bi imati "stvaralačku ulogu."<sup>45</sup> Neke osnove za ovakav stav postoje i u običajenom prihvatanju pravnih shvatanja viših sudova od strane nižih. U svakom slučaju, nužno bi bilo preispitivanje postojećih shvatanja i fleksibilniji pristup ovom izvoru.

**5. Pravna nauka** - nije formalni izvor ni jednog, te ni Kompjuterskog prava, jer mišljenja izražena u pravnoj teoriji ne mogu obavezivati sudove u rešavanju konkretnih sporova. Iako na prvi pogled nema posebnog razloga da se mišljenje nekog posebno značajnog pravnika ne prihvati kao osnova za rešavanje (sudsko) određenog slučaja, to ipak nije, za sada, moguće. Ona može biti korisna i značajna, ali ne može biti izvor prava. Njen se značaj može ogledati kroz uticaj na zakonodavnu i sudsku praksu, ali nije obavezujući<sup>46</sup>.

Kao međunarodni izvori prava pojavljuju se međunarodni ugovori, bilo da su bilateralni ili multilateralni. Za sada, nužno je istaći, posebno značajnih bilateralnih sporazuma nema jer su zemlje prihvatile da pitanja vezana za KT rešavaju na nacionalnom planu, a kad je u pitanju međunarodna scena to su, zbog značaja, prepustile multilateralnim aktima.

Dakle, kao *opšti međunarodni izvori* pojavljuju se, prevashodno, multilateralni akti i to:

<sup>45</sup> Videti: Vasiljević M., op. cit., str. 17; Djordjević Ž., Stanković V., op. cit., str. 39.

<sup>46</sup> Videti: Vasiljević M., op. cit., str. 18; Djordjević Ž., Stanković V., op. cit., str. 40.

**6. Medjunarodne konvencije i preporuke**<sup>47</sup> - su jedan od najvažnijih izvora medjunarodnog prava vezanog za KT. Od medjunarodnih konvencija posebno su bitne one koje se odnose na zaštitu prava intelektualne svojine, naročito na patentnopravnu i autorskopravnu zaštitu, kao i zaštitu žigom ili od nelojalne konkurencije određenih produkata KT (npr. računarskih programa, čipova). Ove konvencije se donose kao **univerzalne** (Pariska konvencija za zaštitu industrijske svojine, Bernska konvencija za zaštitu književnih i umetničkih dela, Sporazum o trgovinskim aspektima prava intelektualne svojine, i sl.) ili **regionalne** (Konvencija o evropskom patentu, Panamerička konvencija o patentima, i sl.). Neke od njih potpisala je i ratifikovala i naša zemlja, dok je druge samo potpisala, ali ih nije ratifikovala, tako da će izvor prava kod nas postati tek kada se steknu uslovi za ratifikaciju. Naravno, mnoge medjunarodne konvencije za nas neće predstavljati izvor prava jer ih nismo (iz teritorijalnih, formalnih ili drugih razloga) potpisali ni ratifikovali. Na medjunarodnoj sceni su sve učestalije i aktivnosti vezane za donošenje medjunarodnih preporuka, pa i rezolucija, deklaracija. Ovim aktima regulišu se određena pitanja u okviru medjunarodnih organizacija opšteg (UN, UNESCO, WIPO, i sl.) ili regionalnog karaktera (EU, OECD, EFTA, LAFTA). Posebno značajne postaju preporuke koje se donose u okviru Evropske Unije i kojima se regulišu pitanja vezana za zaštitu podataka, informacionih sistema, računarskih programa, baza podataka, nelojalne konkurencije i mnoga druga, a koje postaju putokaz za nacionalna zakonodavstva ne samo zemalja članica.

**7. Medjunarodno običajno pravo** - je izvor Kompjuterskog prava koji bi tek trebalo da dobije u značaju, kao što bi i običajno pravo na nacionalnom planu trebalo da postane sve uticajnije i da poprma sve šire razmere. Naročito značajni medjunarodni običaji biće u sferi trgovine produktima KT i pravila koja će se formirati u pojedinim pravima pri toj trgovini.

Osim opštih izvora prava Kompjutersko pravo ima i svoje autonomne izvore. Mada njih nema baš neki impozantan broj sigurno je da će daljim razvojem postati, kao i kod drugih prava, veoma značajni i brojni. Od tih autonomnih izvora posebno se ističu:

**8. Tehničke norme i standardi** - predstavljaju posebna pravila koja se odnose na tehničke, ekonomske i pravne okvire za stvaranje globalnog sistema primene KT. Nastaju kao posledica savremene mas-proizvodnje i trgovine produktima KT, sa ciljem zadovoljenja određenih potreba (kvaliteta, potrošača, trgovine i sl.). Tehničkim normama regulišu se, prvenstveno, hardverska i softverska rešenja koja potom prerastaju u standarde. Standardizacija je do skoro bila vezana, mahom, za

<sup>47</sup> Pojedini autori (npr. Vasiljević) u formalnom smislu **medjunarodne konvencije** svrstavaju u zakone jer ratifikacijom dobijaju njegovu snagu, dok ih drugi (npr. Djurović) tretiraju kao sopstvene izvore određenog prava (npr. Medjunarodnog privrednog) opšteg karaktera. S obzirom da su to pitanja iz domena opšte teorije prava nije celishodno se ovde njima baviti.

okruženje jedne organizacije ili za jedan tip proizvoda, dok joj danas i nacionalne granice postaju tesne. Sve je značajniji međunarodni oblik regulisanja i globalni prilaz standardizaciji razvoja, a naročito korišćenja KT. Posebno važna postaje standardna metodologija razvoja (npr. kao ona za **ESPRIT** - *European Strategic Programme for Research and Development in Information Technology*) pojedinih softverskih sistema, pošto oni treba da objedine standarde za specifikaciju i standarde za implementaciju sistema u različitim tehnološkim okruženjima. Gotovi paketi treba da zadovolje određene standarde. Prenosivost i transparentnost programskih sistema, kao i komunikacija programa sa podacima ostvaruje se preko međunarodno prihvaćenih standardnih jezika za rukovanje podacima. Struktura rečnika podataka treba da bude izvedena iz određenih standarda (to su, uglavnom, **ANSI** standardi nazvani **IRDS** - *Information Resource Dictionary System*). Isti slučaj je i sa razmenom podataka između računarskih sistema (npr. **ODA** - *Office Document Architecture* predstavlja standardni format za procesiranje teksta i "desktop publishing" fajlova, koji dozvoljavaju da se dokumenat iz jednog "kancelarijskog sistema" prebaci u drugi zajedno sa kodovima za formatiranje, opisom fontova, grafikom i sl.). Zatim, **EDI** (*Electronic Data Interchange*), odnosno **EDIFACT** (*Electronic Data Interchange For Administration, Commerce and Transport*) standardi postaju od posebnog značaja za poslovne komunikacije ili **UNIMARC** za razmenu bibliografskih podataka. U suštini, **standardizacija** olakšava komunikaciju između različitih sistema i obuhvata gotovo sve sfere poslovanja, te se mnogobrojne međunarodne organizacije, asocijacije i udruženja međusobno povezuju ne bi li obezbedili njihovu unifikaciju i harmonizaciju (npr. nosioci međunarodne standardizacije o EDI i EDIFACT su: Ekonomska komisija UN za Evropu - UN/ECE, Međunarodna organizacija za standardizaciju - ISO, Međunarodna ekonomska komisija - IEC, Međunarodna telekomunikaciona unija - ITU, kao i odgovarajuće regionalne i nacionalne institucije). Pri tom se mora imati u vidu da je:

- osnovni cilj njihovog postojanja **jednoobrazna** međusobna (interorganizaciona, nacionalna i/ili međunarodna) komunikacija u određenoj oblasti;
- to **stvaranje i primena jednoobraznih** pravila o određenim pitanjima i aspektima;
- veliko očekivanje od **implikacija na kvalitet**;
- veliko očekivanje od **ekonomskih implikacija**; i
- postojanje određenih **nedostataka** i manjkavosti dopušteno, ali ne i nužno.

Ukoliko se nastave široko započete aktivnosti vezane za standardizaciju KT onda će, svakako, njena pravila prerasti u izvor Kompjuterskog prava, kao što se desilo sa poslovnim i proizvodnim standardima u Međunarodnom privrednom pravu<sup>48</sup>.

**9. Autonomne volje ugovornih strana** - postaju sve značajnije za regulisanje ponašanja u određenim situacijama za konkretne odnose. Njima se prenose i uređuju određena prava i odgovornosti. Među ugovorima značajno mesto pripada, ili će pripadati, **tipskim ugovorima** koje, obično, donose međunarodna (npr. Međunarodna trgovinska komora u Parizu je donela jednoobrazna pravila za ugovore za razmenu trgovačkih podataka pomoću teletransmisije - UNCID) ili nacionalna profesionalna udruženja, savezi, asocijacije ili druge institucije (npr. britanski Institut za kupoprodaju i snabdevanje štampao je krajem 80-ih model ugovora nabavke kompjutera, koji je kasnije poslužio kao tipski ugovor za slične pravne poslove<sup>49</sup>), mada ni udeo odgovarajućih komisija i tela OUN ili EU, nije zanemarljiv. Specifičnih tipskih kompjuterskih ugovora još uvek nema mnogo, ali se njihov broj stalno umnožava, naročito kad je u pitanju<sup>50</sup>:

- isporuka računarske opreme i pružanje usluga;
- pružanje usluga programiranja i izrade kompletnih softvera;
- održavanje isporučenog hardvera i softvera;
- ustupanje prava na korišćenje računarskih programa i softvera;
- pružanje konsultantskih usluga u vezi sa isporukom, uvodjenjem i korišćenjem računara;
- pružanje usluga klijentima na sopstvenoj opremi; i sl.

I na kraju, trebalo bi istaći da naše pravo, kao i mnoga druga, nije izričito utvrdilo formalnu hijerarhiju izvora, između ostalog, zbog nerazvijenosti ovog prava, ali i zbog nerazvijenosti samih izvora. Ipak, to je potrebno učiniti vodeći računa da najjaču snagu imaju ustavne odredbe, zakonski propisi i ratifikovane međunarodne konvencije, potom da slede standardi, za njima običaji (na oba plana), sudska praksa, pa sve do pravne nauke. Nikako ne treba zanemariti ni nepravne izvore, koji bez obzira što nemaju snagu formalnih izvora mogu imati poseban uticaj na njih. To bi bile, npr., određene moralne norme, čija izgradnja nesumljivo tek treba da usledi.

<sup>48</sup> Djurović R., op. cit., str. 29 i 30.

<sup>49</sup> Edwards C., Savage N., Walden I., op. cit., str. 24.

<sup>50</sup> Lazarević B., Drakulić M., Razvoj informacionog sistema kao inovativna delatnost, edicija: Menadžment u funkciji inovacija, Beograd, Centar za menadžment Univerziteta u Beogradu, 1995., str. 296.

## 9. Odnos Kompjuterskog prava sa drugim granama prava

Kompjutersko pravo, kao posebna samostalna grana prava, povezano je sa drugim granama prava, a naročito su važne veze i ispreplitanja ove grane prava sa Ustavnim, Obligacionim, Upravnim, Gradjanskim i Poslovnim pravom, kao i Pravom intelektualne svojine. Ove grane prava predstavljaju pravno okruženje Kompjuterskog prava dajući mu osnovu za dalji razvoj. Posebno značajan postaje odnos Kompjuterskog prava sa srodnim granama prava kao što su Pravo informacione tehnologije, Informatičko pravo, Informaciono pravo i Telekomunikaciono pravo. Svaka od ovih grana prava ne samo da ima dodirnih tačaka sa Kompjuterskim pravom, već se još uvek vode rasprave da li je u pitanju ista grana prava ali sa različitim nazivima.

### 9.1. *Kompjutersko pravo i Pravo informacione tehnologije*

Postojanje različitih shvatanja o pojmu i sadržaju Kompjuterskog prava doveli su i do vrlo čestog poistovećivanja sa Pravom informacione tehnologije. Poistovećivanje je nastalo zbog neshvatanja razlike između kompjuterske i informacione tehnologije i zbog uočavanja preuskosti Kompjuterskog prava. Zato u V. Britaniji počinje postepeni razvoj nove grane prava - **Prava informacione tehnologije koje obuhvata skup pravnih normi, institucija i principa kojima se regulišu razni aspekti informacione tehnologije**. Ovo pravo po mišljenju svog rodonačelnika S. Saxby<sup>51</sup> ima višestruke zadatke. Ti zadaci se pojavljuju na makro i mikro planu.

Tako na *makro planu* Pravo informacione tehnologije bi trebalo da:

- a) **ispita postojeće pravne principe i utvrdi njihove nedostatke** i njihovu zastarelost u odnosu na novo okruženje;
- b) **prouči međunarodnu dimenziju postavljenih problema** i pronadje najbolje načine saradnje među zemljama kako bi se nacionalni zakoni mogli primenjivati uz međunarodnu podršku; i
- c) **da komparativni prikaz razvoja i razlika** koje postoje u nacionalnim zakonima pri rešavanju pravnih problema izazvanih razvojem informacionih tehnologija.

---

<sup>51</sup> Saxby S., op. cit., str. 159 - 169.

Na mikro planu osnovni zadatak ovog prava je da obezbedi adekvatne odgovore za praktično rešavanje raznih sporova koji povodom ovih tehnologija nastaju. Mada se to činilo najlakšim zadatkom pokazalo se da i nije baš tako jer se, upravo na ovom nivou "ruši celi okvir postojećeg prava baziranog na opipljivim predmetima ili uslugama, a predmeti i usluge bazirane na informacionoj tehnologiji niti su opipljive, niti su vezane za fizičko okruženje"<sup>52</sup>.

S obzirom na zadatke i tendencije daljeg razvoja ono najčešće obuhvata:

- a) privatnost, zaštitu podataka i obaveze zaposlenih;
- b) kompjuterski sačinjena dokumenta i njihova validnost u sudskim postupcima (npr. građanskim parnicama);
- c) pravne mehanizme zaštite fenomena vezanih za informacionu tehnologiju;
- d) ugovore;
- e) kompjuterski kriminal;
- f) telekomunikacije;
- g) pravne aspekte EDI;
- h) pravne probleme automatizacije kancelarijskog poslovanja; i dr.

Teorijske rasprave i rešavanje praktičnih problema iz domena Prava informacione tehnologije uticali su na povećanje interesa pravnika ne samo u V. Britaniji, već i u Evropskoj Uniji koja danas sve više rešava konkretne probleme u okviru svog posebnog prava. Tako je i došlo do harmonizacije nacionalnih zakonodavstava zemalja članica donošenjem brojnih smernica, preporuka i drugih akata. Posebno su značajne aktivnosti na određivanju pravila pri zaključivanju ugovora vezanih za patente, licence, know-how, franšizin i sl. proizvoda informacione industrije, kao i telekomunikacija, i ostalih usluga koje se mogu obavljati. Pri tome se, svakako, ne smeju zanemariti dve činjenice: **1)** informacione tehnologije su ključ za sve ostale sektore industrije, pa se u okviru EU vrlo mnogo pažnje poklanja njihovoj pravnoj zaštiti, i **2)** EU, pored harmonizacije različitih nacionalnih tržišta, teži da obezbedi i komparativnu prednost ujedinjenog tržišta prema konkurentnim tržištima drugih zemalja nečlanica (naročito SAD-a, Japana).

Intersovanje za Pravo informacione tehnologije počelo je prevazilaziti granice V. Britanije i Evropske Unije i polako dobija svoje mesto u drugim sistemima i literaturi. Čini se da je ovo pravo, u suštini, upravo ta nova grana prava koja tek treba da se razvija i stiče svoj identitet. Medjutim, još uvek je isuviše malo učinjeno na njegovoj konceptualizaciji i utvrđivanju pojma i predmeta. Sigurno da to ne znači da se razvojem ovog prava neće moći dalje razvijati Kompjutersko i Informaciono pravo, ali je nužno

---

<sup>52</sup> Saxby S., op. cit., str. 162.

vrlo brzo definisati njihov međusobni odnos i razgraničiti predmete. Ono što je u ovom trenutku nesporno je: **prvo**, Pravo informacione tehnologije nastaje kao nova grana prava koja predstavlja skup pravnih normi, institucija i principa koji se mogu primenjivati na činjenice, radnje i aktivnosti koje se odnose na informacionu tehnologiju, odnosno, kompjuterizaciju, telekomunikacije, automatizaciju kancelarijskog poslovanja, elektronski prenos podataka; **drugo**, po svojoj prirodi ovo je pravo *šire od Kompjuterskog, a uže od Informacionog prava* - drugim rečima to znači, da je Kompjutersko pravo deo Prava informacione tehnologije, a da su zajedno oni deo Informacionog prava; **treće, to je grana prava koja je tek u povoju** i kojoj predstoji razvoj u narednim periodima. Značajnu podršku tom razvoju imaće pravo EU. Međusobni uticaj i povezanost ovih prava predstavlja pouzdanu garanciju brze konceptualizacije, razvoja i formiranja Prava informacione tehnologije bez velikih konfuzija i praznina. Ne treba zaboraviti da su u EU nacije čija pravna tradicija neće moći zaobići ni ovu granu prava. Ujedinjenje tradicije, sistematičnost i interes za rešavanje postojećih i potencijalnih problema dopuniće i zajednički interes da njihova informaciona industrija postane konkurentna razvijenijoj informacionoj industriji Japana, SAD, zemalja dalekog istoka; i **četvrto**, Pravo informacione tehnologije postaje kompleksno pravo.

Jasno je da Pravo informacione tehnologije treba da bude okvir oko Kompjuterskog, ali i drugih sličnih, grana prava.

## 9.2. *Kompjutersko pravo i Informatičko pravo*

Informatičko pravo nastalo je na tlu Evrope. Među prvima pojam "Informatičko pravo" dao je Medjuvladin biro za informatiku (**IBI - Intergovernmental Bureau of Informatics** - je međunarodna organizacija koja je nastala pod okriljem UN i UNESCO-a, sa ciljem da "na području informatike neposredno pomaže ljudima kako bi živeli u okruženju stvorenom od strane te discipline, te da pomaže ljudima da bolje razumeju uticaj informatike na društvo kako bi ostvarili maksimalnu korist iz mogućnosti koje ta disciplina pruža"<sup>53</sup>). Po dokumentima ove organizacije **Informatičko pravo predstavlja skup pravnih normi, instituta i principa koji se mogu primenjivati na činjenice, radnje i aktivnosti u vezi sa obradom informacija i informatikom**. Pri tome je neophodno odrediti šta se pod informatikom podrazumeva. Po odredjenju Francuske akademije nauka (ne treba zaboraviti da je i sama reč informatika potekla iz francuskog<sup>54</sup>) informatika predstavlja nauku racionalnog

<sup>53</sup> Convention of IBI, article II.

<sup>54</sup> Reč "informatique" postala je od kombinacije reči "information" i "automatique"

postupanja sa informacijama, naročito uz pomoć automatskih mašina, a koja je podloga za znanje i komunikacije u tehničkim, ekonomskim i društvenim oblastima. Drugim rečima, ono bi *trebalo bi da obuhvati*:

**a) Činjenice, radnje i aktivnosti u vezi sa obradom podataka** (informacija), odnosno sve one činjenice vezane za sistematske operacije na podacima pri prikupljanju, reviziji postojećih ili njihovo pretvaranje u informacije. S obzirom da se pod obradom podataka ne podrazumeva bilo koja obrada već automatska obrada podataka, neophodno je regulisanje svih operacija, radnji i činjenica koje se odnose na prikupljanje (odn. na određivanje potrebnih podataka, zaštitu subjekata na koje se ti podaci odnose, pojedinci i organizacije, nadležnost subjekata koji prikupljanje sprovode i sl.) i skladištenje podataka što pretpostavlja postojanje odgovarajućih sistema, najčešće baziranih na četiri osnovne komponente (mašini - kompjuteru, programima, podacima i ljudima) koje, takodje, treba pravno regulisati. Naime, ovim normama bi se trebalo regulisati imovinskopравни odnosi koji nastaju u vezi sa kompjuterima i sličnim mašinama, sa moralnim i materijalnim pravima tvoraca, sa pravima koja proističu iz pravnog prometa ovih proizvoda i odgovornostima vezanim za taj promet, potom to su norme koje se odnose na programe i povezane su sa njihovim nastajanjem, korišćenjem i prometom. Poseban predmet su ljudi i njihove razne aktivnosti vezane za komponente sistema. Iako ovako određena obrada podataka predstavlja vrlo široko područje koje Informatičko pravo treba da obuhvati ipak se u literaturi ono sužava na automatsku obradu podataka ili, još uže, samo na određene probleme koji njome nastaju. Tako se predmet ovog prava uglavnom odnosi na prekogranični tok podataka, zaštitu podataka, kompjuterski kriminal vezan za podatke i zaštitu informacione privatnosti<sup>55</sup>.

**b) Činjenice, radnje i odgovornosti vezane za racionalno postupanje sa informacijama** koje su podloga za znanje i komunikacije u tehničkim, ekonomskim i društvenim oblastima. Drugim rečima, racionalno postupanje pretpostavlja izbor kriterijuma po kojima će se podaci prikupljati, memorisati, prikazivati i dostavljati odgovarajućim subjektima. Kriterijume treba odabrati i regulisati što predstavlja poseban problem sa kojim se mora izboriti ovo pravo. Tako su, npr., utvrđivani principi za zaštitu privatnosti koja može biti ugrožena samom činjenicom postojanja ličnih podataka ili zbog nezakonitog i neodgovarajućeg postupanja sa njima. Principi, kao što su princip kvaliteta podataka, zakonitosti, neposrednog prikupljanja ličnih podataka, restriktivnosti korišćenja, slobodnog prenosa podataka preko državnih granica i drugi, već su ugrađeni u Smernice OECD, Konvenciju Evropskog saveta i mnoge zakone o zaštiti ličnih podataka i privatnosti. Pored principa posebno značajni postaju standardi (nacionalni i međunarodni) na osnovu kojih se obezbeđuje ispunjenje minimuma zahteva vezanih za racionalizaciju procesa i sredstva obrade podataka. Tako se standardima obuhvataju definicije, klasifikacije, nomenklature i identifikacije, tehnike i

<sup>55</sup> Erdelez S., op. cit., str. 175.

tehnologije čuvanja, prenosa i obrade podataka, dokumentacija informacionih sistema<sup>56</sup> i sl.

Vrlo slično kod nas se izdvaja mišljenje, za sada i najpotpunije, **Ivana Mekanovića**<sup>57</sup> koji smatra da je **Informatičko pravo grana prava koja definiše odnose koji nastaju u okviru prikupljanja i obrade podataka, njihovog čuvanja, prenosa i korišćenja, a odnosi se na tehničke, informatičke i društvene odnose vezane za informacije**. Međutim, Mekanović unekoliko sužava ovo pravo jer ga vezuje za kompjutersku tehnologiju i organizaciju koja se uspostavlja za korišćenje ove tehnologije. Određujući sadržaj (razlikujući predmet regulisanja i sadržaja) ovog prava isti autor *smatra da se to postiže*<sup>58</sup>:

- a) **definisanjem subjekata i realizacijom prava pojedinih subjekata** - subjekti su razni, od građana do privrednih preduzeća;
- b) **stvaranjem sistema i njihovim funkcionisanjem**;
- c) **definisanjem odgovornosti** u sistemu sa jasno utvrđenim elementima;
- d) **regulisanjem poslovnih pravnih odnosa** i uzusa u ekonomskom korišćenju informacija; i sl.

Na osnovu određenja predmeta Informatičkog prava, iako još uvek ne postoji dovoljan broj radova niti velika zainteresovanost pravnika za njega, mogu se ipak dati neke karakteristike kao što su: **prvo**, ***Informatičko pravo još uvek predstavlja maglovitu i nedovoljno oformljenu granu prava***, a s obzirom da je veće interesovanje za pojedine njegove oblasti nego za njega samog kao celovitu disciplinu<sup>59</sup>, nagoveštava da se da je dalji razvoj ovog prava veoma problematičan; i **drugo**, iako na prvi pogled Informatičko i Kompjutersko pravo izgledaju gotovo istovetno ili bar veoma slično, to ipak nije slučaj pošto je ***Informatičko pravo šire od Kompjuterskog***, jer obuhvata pravne norme kojima se uređuje automatska obrada podataka koja u osnovi ima i kompjutersku tehnologiju, ali ne samo nju. Međutim, ono istovremeno ima i ***uži okvir od Informacionog prava***.

<sup>56</sup> To je npr. predvideo jugoslovenski Zakon o društvenom sistemu informisanja i informacionom sistemu federacije, čl. 12., st. 1., tč. 2.

<sup>57</sup> Mekanović I., op. cit., str. 204.

<sup>58</sup> Mekanović I., op. cit., str. 206.

<sup>59</sup> Erdelez S., op. cit., str. 175.

### 9.3. *Kompjutersko pravo i Informaciono pravo*

Konstituisanje i razvoj Kompjuterskog prava, Prava informacione tehnologije i Informatičkog prava omogućuje da se pravni problemi vezani za kompjutersku i informacionu tehnologiju počnu postepeno i postupno rešavati. Medjutim, ponudjena rešenja nisu bila kompletna jer nisu obuhvatala i karakteristike<sup>60</sup> postupanja sa informacijama koje su u elektronskom obliku. Tako, npr., informatizacijom uprave i sudstva nastaje poseban problem oko valjanosti (autentičnosti) javne isprave prilagodjene elektronskoj obradi podataka, kao i mnogobrojna pitanja vezana za mogućnosti izjednačavanja mikrofilmskih kopija javnih isprava sa ispravama u klasičnom pismenom obliku, tretmana rešenje koje umesto potpisa ima faksimil, priznavanja dokazne snage kompjuterskog zapisa i sl. To je stvorilo potrebu da se ovi problemi reše, a kako je to prevailazilo prirodu i koncepciju postojećih novih grana prava bilo je moguće ili da se promene te koncepcije, što je teško, ili da se konstituiše nova grana prava, što je bilo nešto lakše. Iako se u početku činilo da nema neakvih posebnih problema oko definisanja predmeta i suštine Informacionog prava<sup>61</sup>, to je bilo samo delimično tačno. Vrlo brzo se shvatilo da je nastao još jedan problem, doduše ništa osobito drugačiji nego kad je u pitanju bilo koja druga grana prava, ili definisanje bilo koje druge činjenice, pojma i instituta. Pojavila su se, u relativno oskudnoj literaturi, različita shvatanja prouzrokovana različitošću pristupa pri definisanju pojma i predmeta. Postepeno su se iskristalisale **tri grupe shvatanja**: *prva* su ona koja su polazište imala u nabranju izvora ovog prava; *drugu grupu* čine ona koja su kao njen okvir istakla opšte političke osnove i odredjenja uloge koje ovo pravo treba da ima; i *treća* su ona koja su ga definisala sa pozicija pojedinačnih, subjektivnih prava. Svako od ovih polazišta imalo je određene nedostatke i prednosti, ali im je zajedničko jedno - **polaze od činjenice da Informaciono pravo postoji**.

Kao predstavnik *prve grupe* shvatanja pojavljuje se **Peter Marx** koji smatra da Informaciono pravo čine "norme, principi i postupci koji nastaju u sudovima, donose ih zakonodavni organi ili organi uprave pri rešavanju sporova ili usmeravanju ponašanja različitih subjekata vezanih za informacije u elektronskom obliku"<sup>62</sup>. Ovakvo polazište i odredjenje, u suštini, ne definiše svojstvenost ovog prava, jer se i druga prava baziraju na istim izvorima, a opet nisu ista.

<sup>60</sup> Erdelez S., op. cit., str. 175.

<sup>61</sup> Neki autori ga nazivaju Pravom informacija: npr., Nikolić D., Pravo, informacija, Novi Sad, Narodna tehnika Vojvodine, 1990., str. 11.

<sup>62</sup> Marx P., The legal risk of using information as a comparative weapon, Information Management Review, br. 8/87, str. 11 - 12.

Nešto precizniji pripadnik ove grupe shvatanja je **Jake Knoppers**. Po njemu Informaciono pravo čini svaki zakon, podzakonski akt, politički program ili kodifikacija (kao i njihovi pojedini elementi) koji zahteva stvaranje, proizvodnju, pribavljanje, dostavljanje ili uništavanje podataka, odnosno ograničavanje uslova za pristup, korišćenje, poverljivost, umnožavanje, širenje, zajedničku upotrebu ili postupanje sa informacijama<sup>63</sup>.

U *drugoj grupi* shvatanja pojavljuju se uglavnom predstavnici nemačke škole prava<sup>64</sup> bazirane, između ostalog, i na sociološkim pogledima i političkim uslovima koji predstavljaju pravno okruženje realizovanja neke grane prava. Polazeći od toga **Herbert Burket** ovo pravo određuje “kao sredstvo informacione politike i obuhvata subjekte normiranja, kao i pravne materijale kojima se uređuju informacije i njihova obrada”<sup>65</sup>. Ako bi se dublje analiziralo ovakvo definisanje moglo bi se uočiti da ono ne daje gotovo nikakve osnove za uočavanje specifičnog predmeta ovog prava, pa ni njegove suštine, već samo potencira uslove u kojima ono nastaje. Time ne samo da ostavlja kompletnu prazninu u odnosu na definiciju Informacionog prava nego i isključuje mogućnosti njegovog postojanja i realizovanja u drugačijim okruženjima i nivoima razvoja, kao što i neprecizno uslovljava postojanje ovog prava postojanjem određene informacione politike. Zar svako pravo nije i sredstvo neke politike? Određena informaciona politika može biti samo preduslov za ostvarivanje višeg ili nižeg nivoa razvoja ovog prava, ali ne i njegova karakteristika po kojoj se razlikuje od drugih prava, npr., Prava informacione tehnologije, Informatičkog ili Kompjuterskog prava.

Neposrednu razradu ovog polazišta i markiranje uloga koje Informaciono pravo ima dao je **Herbert Fiedler** koji je posebno istakao dve osnovne uloge ovog prava smatrajući da ono<sup>66</sup>: **1)** služi **kao uređjujući okvir** za korišćenje informacione tehnologije i različite načine postupanja sa informacijama, a za čije ostvarivanje je neophodno normativno regulisanje raznih informacionih aktivnosti i procesa od zaštite do obrade i korišćenja informacija; i **2)** predstavlja potporu za obezbedjenje pravne infrastrukture za korišćenje informacione tehnologije i postupanja sa informacijama. Tako se kao oblici u kojima se to ostvaruje pojavljuju norme obligacionog prava o informacionoj tehnologiji, pravni instrumenti kojima se obezbedjuju telekomunikacije,

<sup>63</sup> Knoppers J., Information law and information management, Information Management Review, br. 1/86, str. 64, 66, 73.

<sup>64</sup> Erdelez S., op. cit., str. 176.

<sup>65</sup> Burket H., Theories of information in the law, Journal of Law and Information Science, br. 2/82, str. 121, 125.

<sup>66</sup> Fiedler H., A structured approach to the teaching of information policy and information law, edicija: Computer and Law, Rome, Council of Europe, 1985., str. 80.

pravne norme kojima se obezbeđuje zaštita produkata informacione tehnologije, kao intelektualne svojine, krivičnog prava i sl. Mada je ovakva dopuna nešto povoljnija u odnosu na druga definisanja Informacionog prava ona još uvek nije potpuna.

*Treća grupa* shvatanja bazira se na subjektivnim pravima vezanim za pravilno postupanje sa informacijama i određuje, po tumačenju **Pierre Catala** Informaciono pravo kao pravo koje ima zadatak da utvrdi pravilan odnos između legitimnog prava na pristup informacijama i legitimnog prava da se taj pristup onemogući<sup>67</sup>. Međutim, ni to nije dovoljno jer Informaciono pravo ne obuhvata samo subjektivno pravo, već i objektivno, a ono u ovom slučaju nije definisano.

Postojanje različitosti u definisanju Informacionog prava, u stvari, ne negira njegovo postojanje i potrebu za razvojem. Pri tome je neophodno istaći da je **Informaciono pravo skup pravnih normi, principa i instituta kojima se reguliše postupanje sa informacijama koje su u određenom (elektronskom) obliku**. S obzirom da iz ovih normi nastaju određena subjektivna prava na legitimno pravo sopstvenog pristupa informacijama i legitimno pravo da se drugima pristup onemogući, to je i ono deo Informacionog prava. Međutim, kako se i sam pojam informacija različito određuje to će i dalje postojati problemi određenja predmeta ovog prava.

No, bez obzira na te probleme može se reći da su *karakteristike Informacionog prava sledeće*: **Prvo**, Informaciono pravo treba da predstavlja granu prava koja se tek formira i razvija. Za razliku od Kompjuterskog prava, Prava informacione tehnologije i donekle Informatičkog prava, oko postojanja, predmeta i prirode ovog prava postoji mnogo više nesuglasica. One se protežu od različitosti koje postoje u polazištima na osnovu kojih se definiše, do dileme da li ovo pravo zavisi od informacione tehnologije ili ne? Tako se može reći da su netačna shvatanja (S. Erdelez, P. Marx i dr.) da ono nije vezano za postojanje informacione tehnologije i da ne zavisi ni od jedne tehnologije. Naime, ako ovo pravo pretenduje da bude opštije od drugih srodnih novih grana, a čini se da je tako, onda ono obuhvatajući i te grane mora imati nekih dodirnih tačaka sa njima. Te dodirne tačke su informaciona tehnologija jer je ona promenila mnoge karakteristike, i ranije postojećih, informacija, kao što je promenila i način postupanja sa njima. Osobenost ovog prava, reklo bi se, otuda, leži u promenama koje nastaju u odnosu na postupanje sa informacijama u određenom obliku. Danas je to elektronski, sutra će to možda biti neki drugi, a kako je i to deo razvoja informacione tehnologije, bitno je istaći da bilo koji oblik je u pitanju on se razlikuje od doskorašnjeg "klasičnog". Isto kao što se razlikuje i klasični normativizam, kao dogmatski i

<sup>67</sup> Catala P., Answers five questions, Agora, br. 6/83, str. 14.

"zatvoren" način razmišljanja od savremene naučne metodologije<sup>68</sup>. Zbog toga se informaciona tehnologija pojavljuje kao prekretnica i pokretač znatnih promena koje u pravu nastaju (od metoda do sadržaja) čiji uticaj na pravo, uopšte, ne može da se negira, a još manje na informaciono pravo. **Drugo, Informaciono pravo je skup pravnih normi, principa i instituta, koji se mogu primenjivati na činjenice, radnje i aktivnosti vezane za primenu informacione tehnologije i specifičnosti postupanja sa informacijama u elektronskom obliku.** Pri tom se mora istaći da zahvaljujući specifičnosti ovakvog oblika informacija nastaju mnogi pravni problemi jer pravo nije bilo u stanju da se blagovremeno prilagodi tim specifičnostima, te je pravo odbilo da prizna takav oblik informacija zahtevajući da se on vrati "klasičnom, papirnom" ili kada ga je počelo priznavati podvodilo pod isti pravni režim i tretman kakav su imale "uobičajene" informacije. Tek u novije vreme elektronskom obliku informacija priznaje se svojevrsna posebnost čime se stvaraju i uslovi za nastajanje nove grane prava. Takođe, ova grana prava treba da reši i probleme koji proističu iz specifičnosti i oprečnosti dva subjektivna prava - prava na pristup informacijama i prava na onemogućavanje takvog pristupa, pa, s toga, ovo pravo treba da nadje ravnotežu između ova dva subjektivna prava. **Treće, ova grana prava je šira od Informatičkog,** a samim tim i **Kompjuterskog prava** i po svojoj prirodi ih obuhvata, ali i prevazilazi jer joj je predmet širi. Tendencije koje se u razvoju IT pojavljuju stvaraju mogućnosti da se pod okriljem Informacionog prava nadju i Komunikaciono pravo i slične nove, specijalizovane pravne grane. To znači da informaciono pravo nije zatvoren sistem, već deo "realnog kompleksa okruženja" koji treba da pulsira zajedno sa njim. Promene u okruženju odražavaju se na pravo, pa i nastajanje novog kompleksa specifičnih problema koji, ako prevazilaze postojeće pravne discipline i grane, radjaju nove. **Četvrto,** čini se da će sa **konceptualizacijom Informacionog prava biti mnogo više teškoća nego sa drugim granama prava vezanim za informacione tehnologije.** To je posledica postojanja nesigurnosti oko sadržaja i prirode ovog prava i još uvek većom preokupiranošću rešavanja prektičnih i operativnih nego konceptijskih i teorijskih problema. Teško je predvideti kako će dalje teći proces nastajanja i razvoja ovog prava, ali je sigurno da će zavisiti, kako ističe I. Mekanović<sup>69</sup>, od postojanja određenih kvantitativnih odnosa koji nisu ranije postojali, a koji su postali dominantni u rada i ljudskim komunikacijama. To može stvoriti realne mogućnosti za njegov dalji razvoj mada će, po svemu sudeći, on biti usmeren ka razvoju autonomnih delova ovog prava, kao što se za sada više i brže razvija autonomno nego sistemsko regulisanje odnosa vezanih za pojedine njegove segmente. Otuda, postoje relativno velike mogućnosti za ubrzanijim razvojem Kompjuterskog, Prava informacione tehnologije i Informatičkog prava nego Informacionog prava. **Razloga** za to ima više, ali je neophodno istaći:

<sup>68</sup> Lilić S., Izazov pravne informatike, Informatika, privreda, pravo, br. 1/90, str. 12.

<sup>69</sup> Mekanović I., op. cit., str. 204.

- **veća zaokupljenost razvijenih zemalja sa razvojem informacione tehnologije** i sistema nego sa informacionim procesima, koji su, izmedju ostalog, bitan stožer Informacionog prava i problema koje ono treba da reguliše;
- **nagomilavanje mnogih problema vezanih za rešavanje operativih i praktičnih činjenica**, stanja i odnosa vezanih za IT i IS koje je potrebno rešavati brzo i "u hodu";
- **teško i mukotrpno koncipiranje i formiranje opštih pravnih disciplina** kakvo bi trebalo da bude Informaciono pravo;
- **nadnacionalni karakter ovog prava** koji proizlazi iz globalnog karaktera IT i teškoća koje nastaju u uspostavljanju ravnoteže izmedju različitih nacionalnih pravnih sistema i interesa, pogotovo kad su u pitanju interesi koji predstavljaju osnovu nacionalnog bogatstva i prestiža, a što je lakše postići u delovima nego u celini i sl.

#### 9.4. *Kompjutersko pravo i Telekomunikaciono pravo*

Zahvaljujući određivanju pojma i sadržaja Kompjuterskog prava, kao skupa pravnih normi koje se bave kompjuterskom tehnologijom, bilo je moguće, zbog razvoja telekomunikacija, da se postepeno i paralelno razvije još jedna grana prava - **Telekomunikaciono pravo**. Postojanje obe ove grane prava omogućuje da se pravnim normama regulišu problemi, odnosi i dve ključne pojave vezane za nove tehnologije - kompjuteri i komunikacije. Razvoj telekomunikacija i mreža doveo je do velike zainteresovanosti država da se propišu pravila koja će obezbeđivati izvesnu kontrolu nad njihovim radom ne ometajući dalji razvoj. Licence vezane za opremu, servisiranje, privatne mreže, zaštitu javnih PTT i drugih sistema i slični problemi doveli su do donošenja niza zakona u mnogim zemljama (npr. u V. Britaniji je 1984. godine donet Zakon o telekomunikacijama), ali i do neophodnosti teorijskog uobličavanja pravila po kojima bi se takvi problemi rešavali. Istovremeno, počela je i postepena regulacija telekomunikacija na međunarodnom planu u okviru Poštanske unije i sličnih međunarodnih asocijacija, kao i intenzivni rad Evropske Unije. Izgrađuju se strategije daljeg razvoja telekomunikacija i standardi njihove izrade i primene. Tako su 1988. godine donete Smernice o standardima EU kojima treba obezbediti konkurentnost zemalja članica u odnosu na druge zemlje i rešavati pitanja harmonizacije tehničkih i drugih standarda u izradi i korišćenju telekomunikacija i mreža kako bi se uklonile tehničke i fizičke barijere medju njima. Sve to je zahtevalo i postojanje odgovarajućih pravila i grane prava, posebne ili u okviru neke postojeće, koja bi se ovom problematikom bavila. Pitanje celishodnosti postojanja posebne grane prava ili uključivanja ove materije u neku postojeću je dilema koja zavisi od mnogih faktora, ali

je nesporno da pravne probleme telekomunikacija treba rešavati<sup>70</sup>. Tako je nastajalo Telekomunikaciono pravo, kao posebna grana prava koja je tesno vezana za Kompjutersko pravo. Pri tom, obe ove grane prava imaće mnogo zajedničkih i dodirnih tačaka, i u nekim situacijama biće teško napraviti jasnu granicu medju njima koja će ih potpuno odvajati.

---

<sup>70</sup> Chance C., Information Technology 1992, Amsterdam, Chliford Chance Publication, 1990., str. 11 - 54.

# **DRUGI DEO**

## **PRAVNA ZAŠTITA KOMPJUTERSKIH SISTEMA**

**Glava 2: Zaštita podataka**

**Glava 3: Zaštita kompjuterskih programa i softvera**

**Glava 4: Zaštita baza podataka**

**Glava 5: Zaštita topografije integriranih kola**

**Glava 6: Zaštita od kompjuterskog kriminaliteta**

# GLAVA 2

## ZAŠTITA PODATAKA

|           |  |            |
|-----------|--|------------|
| <b>1.</b> | <b>Uvodne napomene o zaštiti podataka</b>  | <b>54</b>  |
| <b>2.</b> | <b>Objekti zaštite</b>   | <b>54</b>  |
| 2.1.      | <i>Zaštita privatnosti i podataka o ličnosti</i>   | 60         |
| 2.1.1.    | <i>Zaštita privatnosti i informacione privatnosti</i>  | 62         |
| 2.1.2.    | <i>Zaštita podataka o ličnosti</i>   | 86         |
| 2.2.      | <i>Zaštita organizacija i poverljivih podataka</i>   | 100        |
| 2.2.1.    | <i>Zaštita organizacija</i>  | 100        |
| 2.2.2.    | <i>Zaštita poverljivih podataka</i>  | 102        |
| 2.3.      | <i>Zaštita podataka u prekograničnom toku podataka</i>   | 106        |
| 2.4.      | <i>Zaštita podataka u elektronskoj razmeni podataka</i>  | 110        |
| <b>3.</b> | <b>Instrumenti zaštite</b>   | <b>118</b> |
| 3.1.      | <i>Medjunarodni instrumenti</i>  | 123        |
| 3.1.1.    | <i>Zaključci Medjunarodne komisije pravnika</i>  | 125        |
| 3.1.2.    | <i>Izveštaji Generalnog sekretara UN</i>   | 126        |
| 3.1.3.    | <i>Konvencija o zaštiti pojedinaca s obzirom na automatizovanu obradu podataka o ličnosti</i>                    | 127        |
| 3.1.4.    | <i>Smernice za zaštitu privatnosti i prekograničnih tokova podataka o ličnosti</i>                               | 129        |
| 3.1.5.    | <i>Deklaracija o prekograničnim tokovima podataka</i>  | 132        |
| 3.1.6.    | <i>Smernice koje se odnose na kompjuterizovana dosijea podataka</i>  | 134        |
| 3.1.7.    | <i>Direktiva o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i slobodnom kretanju takvih podataka</i> | 136        |
| 3.1.8.    | <i>Evropski Model EDI Sporazuma</i>  | 140        |
| 3.2.      | <i>Nacionalni instrumenti</i>  | 142        |
| 3.3.      | <i>Instrumenti našeg prava</i>   | 148        |
| 3.3.1.    | <i>Savezni pravni instrumenti</i>  | 149        |
| 3.3.2.    | <i>Pravni instrumenti Republike Srbije</i>   | 155        |
| 3.3.3.    | <i>Zaključna razmatranja o pravnim instrumentima našeg prava</i>   | 157        |

## 1. Uvodne napomene o zaštiti podataka

Nema bezopasnih podataka. Svaki, pa i najbezazleniji podatak, može da predstavlja potencijalnu opasnost za fizička i/ili pravna lica, određenu društvenu, porodičnu zajednicu i/ili neku drugu skupinu. Opasnost je postojala i ranije. Mnogobrojni primeri govore da su u svim vremenima i svim društvenim uređenjima pojedinci ili institucije strahovali od postojanja određenih podataka ili od njihovog gubljenja, menjanja, zloupotrebe. Na primer između 450. i 31. godine p. n. e. postojale su tzv. senatorske liste u koje su se, pored ostalih, unosili i ukori (note) koji su izricani senatorima. Sama pretpostavka o postojanju takvih podataka predstavljala je svojevrsnu pretnju za senatore i istovremeno budilo strah od njihove zloupotrebe. Slično se događja i sa poreskim listama u koje su se unosili podaci o katastarskim prihodima i na osnovu kojih se određivala visina stope poreza. Neznatne greške u podacima, namerno ili slučajno načinjene, mogle su da imaju značajne posledice za poreskog obveznika i u nekim slučajevima dolazilo je do oduzimanja imovine, zbog neplaćanja poreza. Pored ovih i mnogi drugi primeri ukazuju na značaj i opasnost od postojanja nekih, odn. određenih podataka. Taj značaj i opasnost postali su još izraženiji primenom kompjuterske tehnologije. Istovremeno pojavljuju se i mnogobrojna upozorenja na negativne uticaje koje je primena KT sa sobom donela. Tako lista uticaja novih tehnologija sve više raste, a i sve veći broj autora počinje da se bavi ovom problematikom. Sve ove odlike revolucije koja nastaje i evolucije koja traje stvorili su "dešperatnog optimistu" i navode da se, bar, o nekim od ovih uticaja malo više pozabavimo i u našem, relativno informaciono nerazvijenom, društvu.

## 2. Objekti zaštite

Da bi se nešto moglo štititi neophodno je prevashodno definisati šta se štiti, pa na osnovu toga odrediti i način na koji će se zaštita sprovesti.

Iako odgovori na ova pitanja izgledaju jednostavani oni to svakako nisu, jer štititi treba višestruki objekat, pri čemu se akcenat stavlja na onaj koji odgovara interesu zbog koga se zaštita i preduzima. Interesi mogu biti različiti, često međusobno suprotstavljeni. Interes može biti lični, pojedinačni i/ili grupni, kolektivni. Dok kolektivni interesi mogu biti interesi užih i širih zajednica ili celog društva, dotle lični, pojedinačni, interesi se vezuju za pojedinca (najčešće građanina). Pri tome, treba praviti razliku između ličnog i kolektivnog i javnog i privatnog interesa. Pravom se uvek štiti javni interes, dok se privatni štiti samo onda kad je to izričito određeno i ukoliko je u skladu sa javnim interesom. Mada izgleda vrlo jednostavno odrediti razliku između javnog i privatnog interesa, to u praksi i nije baš tako lako te se često ostavlja nadležnom organu da to utvrdi.

U početku funkcionisanja prvih komjuterizovanih IS, javni interes se uglavnom poklapao sa kolektivnim i zaštita se mahom orjentisala na njih. Razvojem IS, sve više se pored zaštite kolektivnog, a brzo i ispred njega, počinje da se često postavlja, kao centralno pitanje, zaštita interesa pojedinaca, zaštitita privatnosti. Kako se razvoj IS vezuje za SAD, V. Britaniju, SR Nemačku, Francusku, Japan to nije ni čudno što se pitanje zaštite privatnosti u ovim zemljama postavlja kao pitanje koje zaokuplja i naučnu i stručnu pažnju, kao i pažnju javnosti. Iako je privatnost prevashodno političko pitanje ono sve više postaje ekonomsko i etičko. Mogli bi se složiti sa stavovima<sup>1</sup> koji ističu da je ne tako davno jedna od osnovnih razlika između "Zapadnih društava" i "Socijalističkog bloka" bio pristup privatnosti, otuda se kao osnovno pitanje zaštite podataka, postavlja pitanje zaštite pojedinaca i njihove privatnosti od "skroziranja" koja su moguća, zahvaljujući podacima. Pored pojedinaca neophodno je zaštititi i druge subjekte, od kojih su najbrojnija preduzeća, odn. razna pravna lica<sup>2</sup>. Predmet zaštite su: njihove poslovne, službene i druge tajne, kao i specifičnosti njihovog poslovanja, tehnološkog i proizvodnog ciklusa i sl.

Posebni objekti zaštite su i prekogranični tokovi podataka, kao i elektronska razmena podataka u kojima se pojavljuju razni subjekti, te se, otuda, ne mogu ni za jedan odredjeni vezati.

Iz spiska objekata zaštite nikako ne smeju biti izostavljene mreže<sup>3</sup>, smart kartice<sup>4</sup>, elektronska pošta<sup>5</sup>.

Svakako da ovo ne predstavlja konačnu listu objekata zaštite, jer će razvoj i napredak verovatno postaviti pred zaštitne mehanizme nove zahteve i formirati nove objekte. Istovremeno to ne znači, da postojanje svakog od ovih objekata isključuje druge, već postoji međusobna povezanost i uslovljenost jednih drugima i teško je vršiti strogo razgraničenje (jednih u odnosu na druge). Oni se tako međusobno prepliću, pa se

<sup>1</sup> Eaton J., Smithers J., Curan S., This is IT, A Manager's Guide to Information Technology, Oxford, Philip Allan, 1988., str. 246.

<sup>2</sup> Shirey R., Security Requirements for network management data, Computer Standards & Interfaces, no. 17/95, str. 321 - 331.

<sup>3</sup> Frankel Y., Herzberg A., Karger P., Krawczyk H., Kunzinger C., Yung M., Security Issues in a CDOD Wireless Network, IEEE Personal Communications, vol. 2., no. 4/95, str. 16 - 28.

<sup>4</sup> Arazi B., Interleaving security and efficiency considerations in the design of inexpensive IC cards, IEE Proceedings Computers and Digital Technologies, vol. 141., no. 5/94, str. 22; Clark P., Hoffman L., BITS: A Smartcard Protected Operating System, Communications of the ACM, vol. 37., no. 11/94, str. 66 - 70.

<sup>5</sup> Smith D., Simon S., Cautilli L., Trials of Wireless, Secure Electronic Mail, IEEE Personal Communications, vol. 2., no. 4/95, str. 28 - 34.

efikasnost zaštite ostvaruje tek onda kad se obezbedi i povezanost objekata, mehanizama i instrumenata.

Odredjivanjem predmeta zaštite donekle je nagovešten problem koji je neophodno rešiti, jer pored njega treba odrediti od čega određeni predmet treba nužno zaštititi, kao i na koji način.

**Subjekte i podatke** neophodno je **zaštititi** od:

- **fizičkih hazarda** (požar, poplava, eksplozije);
- neispravnosti opreme;
- **grešaka** - ljudskih grešaka (korišćenje pogrešnih verzija programa, greške u kucanju, neispravno montirani medijumi) ili softverske (slabo testiran operativni sistem, i sl.);
- **zlomamernih povreda** podataka i sistema (modifikovanje, unošenje netačnih podataka, falsifikovanja, brisanje, upadi, krađe i sl.) i napadi na subjekte (na privatnost, poverljivost, integritet).

Iako se ovaj predmet mahom odnosi na pravnu zaštitu i pravne mehanizme ipak je nužno istaći da pored njih postoje i primenjuju se i druge mere zaštite.

Šta je zaštita podataka, u stvari?

Radi lakšeg definisanja ovog vida zaštite nužno je praviti razliku između zaštite podataka i zaštite uopšte (IS, ili kompjuterskog sistema). Ne ulazeći u rasprave oko definisanja pojma zaštite upošte čini se najprihvatljivije određenje<sup>6</sup> po kome sama zaštita (protection) predstavlja, u užem smislu, "skup metoda i tehnika kojima se kontroliše pristup pojedincima od strane programa koji se izvršavaju". U širem smislu, zaštita obuhvata "skup metoda, tehnika i pravnih normi kojima se kontroliše pristup podacima od strane programa i ljudi, i štiti fizički integritet celokupnog računarskog sistema, bio on distribuiran ili ne, centralizovan ili decentralizovan".

**Zaštita podataka** (data protection), pak, predstavlja skup međusobno povezanih aktivnosti, metoda, tehnika i normi kojima se **obezbedjuje privatnost**,

---

<sup>6</sup> Velašević D., Osnovni pojmovi i struktura zaštite podataka u računarskim sistemima, I stručni skup: Zaštita podataka u računarskim sistemima, Beograd, 1995., str. 2; Velašević D., Problemi i analiza zaštite podataka u računarskim sistemima; XI naučno - stručni skup Info - Teh '96, Donji Milanovac, 1996. str. 16.

*sigurnost, poverljivost, raspoloživost i integritet podataka od svih opasnosti koje im prete*<sup>7</sup>.

**Privatnost** (*privacy*) se pojavljuje kao višeznačna kategorija: kao pravo pojedinca koji se pojavljuje kao subjekt podataka i kao privatnost korisnika<sup>8</sup>. Privatnost korisnika obuhvata: **1)** privatnost tzv. "informacija za uključivanje određenog terminala u sistem" (npr. pozivni broj, broj pozivne karice, tip zahtevane usluge, i sl.); **2)** privatnost govora (onemogućavanje presretanja usmenih komunikacija); **3)** privatnost podataka (onemogućavanje presretanja podataka u bilo kom obliku oni bili); **4)** privatnost korisnikove lokacije; **5)** privatnost korisnikove identifikacije; **6)** privatnost posebnih načina uključivanja; i **7)** privatnost njegovih finansijskih transakcija (naročito transmisije informacija o kreditnim karticama).

**Sigurnost podataka** (*security*)<sup>9</sup> obuhvata obezbeđenje podataka od slučajnog ili namernog otkrivanja neovlašćenim korisnicima ili zaštitu od neovlašćenog menjanja, brisanja i korišćenja od strane ovlašćenih korisnika<sup>10</sup>.

**Poverljivost podataka** (*confidentiality*) proističe iz svojinskih odnosa i značaja podataka za određene subjekte, a pretpostavlja da se poverljivi podaci ne smenju otkriti od strane neautorizovanih pojedinaca i drugih entiteta ili u neovlašćenim procesima<sup>11</sup>. Kad su u pitanju mreže poverljivost postaje osobito veliki problem u "saobraćaju" podataka obuhvatajući i eksterne karakteristike tog saobraćaja (npr. frekvencije, izvor, destinacije).

<sup>7</sup> Parker D., Demonstrating the Elements of Information Security with Treats, National Computer Security Conference, Baltimore, 1995; Heinlein E., Principles of Information System Security, Computer & Security, no. 14/95, str. 197 - 199; Wolfe H., Computer Security: For Fun and Profit, Computer & Security, no. 14/95, str. 113 - 115.

<sup>8</sup> Wilkes J., Privacy and Authentication Needs of PCs, IEEE Personal Communications, vol. 2. no. 4/95, str. 12.

<sup>9</sup> Pojedini naši autori (npr. Velašević) prave razliku između sigurnosti i bezbednosti, međutim, više su u pitanju razlike u varijanti reči koja je prihvaćena nego o različitosti pojmovima.

<sup>10</sup> Martin J., Information Engineering, Washington, Prentice Hall, 1990., str. 583; Edwards E., Savage N., Walden I., Information Technology & The Law, Basingstoke, Macmillan Publicers LTD., 1990., str. 190. - 198; Kavran D., Laws And Regulations Of Informations Systems Development And Operation, UN, 1987., str. 25 - -27; Petrović S., Jirić V., Zaštita podataka u automatizovanim informacionim sistemima, Beograd, Naučna knjiga, 1986., str. 25; i dr.

<sup>11</sup> Shirey R., op. cit., str. 325.

**Raspoloživost podataka** (*availability*) pretpostavlja da samo ovlašćeni korisnik može blagovremeno doći do podataka, i to određenih, a bez barijera ili drugih oblika ometanja i sprečavanja.

**Integritet** (*integrity*) ima više različitih značenja. On obuhvata: integritet podataka (integritet u užem smislu); integritet izvora i tačnost. Integritet podataka pretpostavlja da se podaci neautorizovano ne manjaju ili uništavaju. Integritet izvora (tzv. Biba integrity) prirodni je nastavak prethodnog oblika integriteta i znači obezbedjenje takvog stepena poverljivosti koji omogućava puno poverenje "izvora" uključujući i poverenje u sve procese rukovanja podacima. Naravno, kao treći oblik integriteta pojavljuje se tačnost, koju mnogi autori smatraju i jedinim oblikom. Ona se prevashodno i tesno vezuje za odgovornost za greške u rukovanju<sup>12</sup>.

Svakako da je obezbedjenje sigurnosti podataka jedno od najznačajnijih i najdelikatnijih pitanja sa kojim se sreću sva društva i svi IS. Dostupnost podacima osigurava: prikupljanje, protok i dotok svih podataka neophodnih za preduzimanje, u datom trenutku, određenih akcija i donošenju određenih odluka. Njihova sigurnost pretpostavlja, da su u tim procesima i korisnicima dostupni samo oni podaci koji to mogu, i treba, da budu. Sve veća potreba za podacima i sve veći strah od njihove zloupotrebe doveli su do neophodnosti njihovog posebnog tretmana. Tim više što su, s jedne strane, rasle tehničke mogućnosti čuvanja, obrade, prenosa i korišćenja podataka, a, s druge, što se stalno proširuje krug subjekata kojima su ovi podaci potrebni i dostupni, kao i krug subjekata o kojima se i od kojih se podaci prikupljaju. Narastanje ovih mogućnosti nametnulo je neophodnost preduzimanja niza društvenih, pravnih, tehničkih, organizacionih i drugih mera, kao i primenu raznih metoda kako bi se obezbedila njihova sigurnost. Da bi primena mera i metoda bila efikasna, mora biti sinhronizovana i međusobno tako povezana da ni jedna karika u lancu ne izostane.

**Društvene mere zaštite** obuhvataju one mere kojima se štiti društvo od neovlašćenog korišćenja i zloupotrebe, naročito, poverljivih podataka. Njima je cilj da eliminišu ili smanje sve uzroke "ranjivosti" jednog sistema koje bi mogle da tangiraju društvo i svakog ili većinu pojedinaca u njemu. Ove mere realizuju se kroz koncipiranje ukupne politike informativne delatnosti i politike funkcionisanja i razvoja "javnih" baza podataka, kao i politike zaštite podataka u graničnim i prekograničnim tokovima, kojima se osigurava suverenost, nacionalna sigurnost, privatnost i lične slobode, a onemogućuju sve one aktivnosti vezane za podatke u kojima se pojavljuju bilo koji oblici kriminala ili ugrožavanja društvenih (državnih) i privatnih interesa. U većini zemalja, kao osnovni postulati u koncipiranju društvenih mera, pojavljuju se otvorenost, stabilnost, sigurnost,

<sup>12</sup> Shirey R., op. cit., str. 325.

nezavisnost i sprečavanje raznih političkih implikacija koje mogu ugroziti ili ugrožavaju jedno društvo.

Društvenim merama, pored zaštite podataka, teži se zaštititi i IS i cele nacionalne informacione delatnosti. Da bi se to postiglo donose se odgovarajući programi i planovi razvoja kojima se obuhvataju politika, kao osnova i pravci razvoja vezani za informatiku. Ovo poprima i međunarodne razmere, na primer, planovi i programi razvoja EU<sup>13</sup>. Praćenjem njihovog ostvarivanja preduzimaju se i odgovarajuće mere kojima se koriguju postojeća stanja, uskladjuju i koordiniraju aktivnosti, pokreću inicijative i uspostavljaju, održavaju i razvijaju veze svih nadležnih subjekata unutar i izvan zemlje<sup>14</sup>.

**Pravne mere zaštite** su mere kojima se odgovarajućim pravnim mehanizmima, prvenstveno, štite podaci i procesi vezani za njih, a u određenim slučajevima i subjekti koji se pojavljuju. Razvojem KT objekti zaštite postaju kompleksniji, a pravne mere konkretnije. Tako se pored podataka i subjekata, zaštita proširuje na softver, hardver, kao i trgovinu kompjuterizovanih informacija, kompjuterskih i telekomunikacionih usluga tzv. **ICC usluge** (*Informations, Computers, Communications*).

Obezbedjenje pravne zaštite sigurnosti podataka često se odnosi na zaštitu njihove **tajnosti**, koja je u ovoj dekadi u mnogim zemljama dobila šire razmere i oblike. Pored toga, promenio se i pojam, koji se od tradicionalnog pojma tajnosti i ograničenosti u dostavljanju i korišćenju podataka proširio na poseban tretman u prikupljanju, upotrebi, objavljivanju i prenosu podataka. Posebno je značajno poštovanje "poštenih" postupaka u prikupljanju podataka, njihovoj upotrebi i objavljivanju. Po zakonima nekih zemalja (npr. SAD - Zakon o pravu na finansijsku tajnost.) ili kodeksima predviđaju se osnovni principi na osnovu kojih se mora poštovati tajnost određenih podataka koji se u bazama mogu naći. Ove principe trebalo bi da znaju svi oni o kojima se podaci prikupljaju, kao i oni subjekti koji ih prikupljaju, obrađuju i koriste. Nepoštovanje predviđenih principa povlači pravne i moralne sankcije za prekršioce<sup>15</sup>.

<sup>13</sup> Norton H., *Informatics In Europe, Preparing for the Global Market*, Oxford, NCC Blackwell, 1991., str. 1 - 21.

<sup>14</sup> Muftić S., *Sigurnost kompjuterskih sistema*, Sarajevo, Zavod za ekonomsko planiranje, 1979., str. 24.

<sup>15</sup> Daler T., Gulbrandsen R., Melgard B., Sjolstad T., *Security Of Information And Data*, Chichester, Ellis Horwood Limited, 1989., str. 60 - 64.

Pored tajnosti, pravne mere zaštite posebno se odnose na izgradnju i **primenu principa** na kojima treba da se bazira funkcionisanje IS, bez obzira kakvi se podaci u njima nalaze. To su oni principi koje su prihvatile međunarodne organizacije i nacionalna zakonodavstva. Među njima najznačajniji su oni koji se odnose na ograničavanje prikupljanja podataka, navodjenje svrhe, ograničavanje upotrebe, sudelovanja i odgovornosti. Dopunjeni još i principom zabrane postojanja tajnih sistema za prikupljanje i čuvanje podataka, pravima subjekata o kojima se i od kojih se podaci prikupljaju, kao i obavezama i odgovornostima subjekata koji prikupljanje, obradu, memorisanje i dostavljanje obavljaju, ovi principi, prava, obaveze i odgovornosti predstavljaju okosnicu na kojoj počiva zaštita podataka. Njih je nužno upotpuniti i principima kao što su: korisnost, autentičnost i svojina podataka. Ovaj poslednji princip treba da omogući razlike u obezbeđenju sigurnosti u vojnim, vladinim, milicijskim i sličnim IS, od onih koji su u "rukama" poslovnih organizacija<sup>16</sup>.

**Tehničke mere zaštite** su treća vrsta mera kojima se štite podaci i imaju za cilj da obezbede, mahom, fizičku zaštitu. Ove mere<sup>17</sup> se odnose na "fizičku zaštitu objekta u kome je smeštena računarska oprema (raspored instalacija i opreme) i protivpožarnu zaštitu; obezbeđivanje i zaštitu računarske opreme (izbor adekvatne i pouzdane opreme, obezbeđenje tokom njene eksploatacije, redovno servisiranje i snabdevanje rezervnim delovima) i računarskih nosioca podataka (pri korišćenju i čuvanju); zaštitu programske podrške (u fazi projektovanja, razvoja i korišćenja programskih sistema); zaštitu računarskih mreža (prilikom projektovanja i realizacije).

**Organizacione mere** podrazumevaju: "organizaciju tehnologije rada u IS pri njegovom projektovanju (izrada preliminarne studije o razvoju IS, idejnog, glavnog, izvodjačkog projekta IS i uvođenja projektovanih rešenja) i pri operativnom radu (planiranje rada i vođenje evidencije o izvršavanju svih postupaka u radu i kreiranju dokumentacije), utvrđivanju postupaka u slučaju vanrednih okolnosti, ostale uslove za uspešno funkcionisanje IS (kontrola ljudi pri zapošljavanju, definisanje poslova i zadataka učesnika u radu IS, stručno usavršavanje)"<sup>18</sup>.

### *2.1. Zaštita privatnosti i podataka o ličnosti*

<sup>16</sup> Parker D., op. cit., 18.

<sup>17</sup> Po ranije važećoj Uredbi o obezbeđenju i zaštiti informacionih sistema državnih organa, čl. 4., Službeni glasnik SRS, br. 41/90.

<sup>18</sup> Daler T., Gulbrandsen R., Melgard B., Sjolstad T., op. cit., str. 55.

Pojedinac može biti na razne načine ugrožen, između ostalog, i podacima. Retki su oni koji znaju koji se sve podaci i informacije, gde, od strane koga i zbog čega se prikupljaju, obrađuju, memorišu i koriste.

Od samog rođenja se vode podaci o nama kod raznih organizacija, institucija, drugih organa. Počev od datuma i mesta rođenja, roditeljima, državljanstvu, kao prvih, pa preko podataka o ponašanju u obdaništima, školama, zdravstvenom stanju, sve do onih koji se vode iz posebnih razloga - izdavanja vozačkih dozvola, dozvola za nošenje oružja, pasoša, utvrđivanja raznih prekršaja, kupovine robe, stambenim prilikama, imovini, radnim mestima, i sl. Imena, sa manjim ili većim brojem podataka, mogu se naći u telefonskim imenicima, popisu stanovništva, raznim registrima, poznatim ili nepoznatim evidencijama, katalozima itd.. Pored običnih (opštih) podataka o pojedincima se vode i mnogi osetljivi podaci (npr. o zdravlju, finansijskim transakcijama, ličnim vezama i odnosima, kriminalnom ili antisocijalnom ponašanju)<sup>19</sup>. Često nismo ni svesni da se podaci o nama negde vode ili da oni uopšte postoje. Ma koliko da su, iz raznih razloga, takvi podaci neophodni oni danas postaju i mnogo veći problem nego što je to na prvi pogled izgledalo.

Kompjuteri u kojima su podaci smešteni mogu se povezati pa postaju tehnički moguće da se podaci prikupljeni za jednu, koriste u druge svrhe. Primer je IS biblioteka u SR Nemačkoj u kojima su, pored podataka o knjigama, smešteni i podaci o čitaocima. Mada, na izgled, vrlo bezazleni, ovi se podaci mogu koristiti i u druge svrhe, nego što to na prvi pogled i po prirodi stvari, izgleda. Takav slučaj je bio i sa hvatanjem članova terorističkih Crvenih brigada koji su posle jedne uspele akcije otkriveni na osnovu podataka o čitaocima literature u kojoj su terorističke akcije i ideje bile dobro razradjivane, kao i literature o Trockom i drugim autorima sličnih ideja. Dobijanjem ovih podataka i njihovim ukrštanjem sa podacima u odgovarajućim službama bezbednosti i policije bilo je moguće sačiniti spisak potencijalnih počinioaca - pripadnika neke terorističke organizacije. Nakon sprovedenih ispitivanja eliminisani su oni koji nisu, iz raznih razloga, mogli biti počinioци. Krug lica se suzio, pa nije bilo osobito teško izdvojiti lica koja su ušla u najuži izbor i za koje je trebalo odgovarajućim metodama utvrditi krivicu. U suštini, do ovakvih podataka nije naročito teško doći pa nije nemoguće da korisnici, koji imaju pristup do određenih podataka, ove podatke koriste za svrhe koje nam nisu poznate. Zbog toga stižu sa svih strana - od pravnika, novinara, informatičara upozorenja na opasnost, a u poslednje vreme ta upozorenja postaju alarmantnija.

---

<sup>19</sup> Eaton J., Smithers J., Curan S., op. cit., str. 247.

Mi i sami postajemo sve više postajemo svesni da sa postojanjem velikog broja raznovrsnih podataka o nama, koji se mogu lako povezati, postajemo sve više "ogoljeni i prozirni". Drugim rečima, ono što je najčešće i najžešće ugroženo - to je naša privatnost.

Još tada je u centru pažnje bila dilema: šta sve obuhvata privatnost i koje su njene granice, a, takodje, kolike su i gde granice javnosti, odnosno koja od njih, ima veću i jaču snagu. Međutim za rešavanje ove dileme prethodno neophodno je utvrditi šta, u stvari, privatnost predstavlja i obuhvata i zašto je uopšte važno da se ona odredi.

Polazeći od toga da se određivanjem sadržaja ovog pojma, u suštini, mogu definisati podaci, koji bi o pojedincima mogli a ne bi smeli da se prikupljaju. Osobito je važna preciznost za definisanje ove druge grupe podataka, jer njih subjekti (pravna i/ili fizička lica) ne bi smeli da prikupljaju, obrađuju i koriste, kao što i pojedinac (od koga ili o kome se takvi podaci prikupljaju) može, bez ikakvih pravnih i drugih sankcija, odbiti da ih da. Ukoliko se ovakvi podaci nadju u nekoj bazi, svi subjekti koji su to omogućili moraju odgovarati i protiv njih se moraju, po pravilu *ex officio*, pokrenuti odgovarajući postupci i izreći odgovarajuće sankcije. Istovremeno, pored pravnih za ove subjekte važe i etičke sankcije, koje su često efikasnije.

U suštini, određivanjem privatnosti omogućuje će sprečavanje problema pre njihovog nastajanja ili njihovo lakše otkrivanje, ukoliko već nastanu. Mada ovo izgleda vrlo jednostavno, to ipak nije tako, jer je definisanje privatnosti vrlo složeno i zavisi od niza faktora (primera radi i od stepena demokratičnosti jednog društva - što je društvo demokratičnije to je privatnost šira, i obrnuto). Često ovo pravo je mnogo lakše prepoznati nego definisati, jer privatnost je različita stvari za različite ljude i ima uticaja na druga osnovna prava<sup>20</sup>.

### 2.1.1. *Zaštita privatnosti i informacione privatnosti*

O pojmu privatnosti ne postoji jedinstveno mišljenje i njegova suština razlikuje se od autora do autora i od koncepcije do koncepcije. To se reflektuje na praksu i na pravne instrumente kojima se privatnost želi da zaštiti. Razlike koje postoje, prevashodno, su posledica različitosti sistema (ekonomskog, pravnog) u kojima se privatnost pojavljuje; nivoa društvene, ekonomske, naučno-tehnološke razvijenosti, a naročito razvijenosti KT, jer se zbog njega najčešće može dovesti u pitanje

<sup>20</sup> Chalton S., Gaskill, S., Data Protection Law, London, Sweet & Maxwell, 1988., str. 1-001.

obezbedjenje i sigurnost privatnosti. Naime, razvojem i primenom nove KT privatnost ne samo da dobija nova odredjenja i značaj, već postaje jedno od vitalnih problema koje treba rešiti raznim mehanizmima. Upravo zahvaljujući usavršavanju KT, privatnost dobija nove sadržaje time što se, kao ljudsko pravo dopunjuje skupom prava koja se odnose na podatke vezane za ličnosti i koji, ukoliko ne uživaju poseban tretman i zaštitu, mogu pravo da ugroze.

**Pravo na privatnost** (*privacy right*) *je jedno od osnovnih, neotudjivih i apsolutnih ljudskih prava svakog pojedinca kojim se obezbedjuje integritet i dignitet ljudske ličnosti, a radi očuvanja tajnosti i slobode njegovog privatnog života.*

Otuda, ako se žele sagledati **karakteristike i sadržaj privatnosti** može se uočiti sledeće:

**Prvo.** Privatnost je jedno od *osnovnih ljudskih prava* što znači da se odnosi na ona prava koja su vezana za ličnost čoveka i predmete koji su neposredno vezani za nju<sup>21</sup>. Iako na prvi pogled izgleda da je nepotrebno isticati vezanost prava privatnosti za fizičko lice, njegovu ličnost i život, ono je ipak neophodno jer predstavlja osnovu ovog prava. Kao lično pravo, *pravo privatnosti je neotudjivo pravo svakog pojedinca* i ne može se preneti na drugog pojedinca ili instituciju.

**Drugo.** To je *pravo kojim se obezbedjuje ljudskoj ličnosti integritet i dignitet*, odn. to je pravo koje se vezuje za: **a) život, b) telesni i fizički integritet, c) čast i ugled, d) privatni (lični i porodični) život, e) identitet, i f) ime.** Ovo pravo, drugim rečima, znači takav tretman jedne ličnosti od strane drugih (fizičkih lica, organizacija, ustanova, države i sl.) koji obezbedjuje poštovanje njene kompleksnosti (u fizičkom i psihofizičkom smislu), časti, dostojanstva, kao i želje da se u određenom stepenu izoluje i povuče iz javnosti, od pojedinaca ili grupa. To je, u stvari, pravo pojedinca da bude ostavljen na miru (iz američke doktrine poznato "*the right to be alone*")<sup>22</sup>. Međutim, ovo pravo se proširuje i na **g) tajnost pisma i druga sredstva**

<sup>21</sup> Kandić-Popović Z., Krivično-pravna zaštita privatnog života, Beograd, Anali Pravnog fakulteta u Beogradu, br. 4/88., str. 369 - 365.

<sup>22</sup> Inače, samo pravo na privatnost potiče iz američkog prava i korene vuče iz XIX veka, mada neki autori smatraju da su koreni privatnosti u Grčkoj u vreme Perika. Ono je, u stvari, pravo da je jedna ličnost nezavisna fizički i psihički, kao da je prostor (teritorija i imovina) oko nje nedodirljiva. Više o raznim shvatanjima ovog prava kod: Sipior J. C., Burke T. W., The Ethical and Legal Quandary of Email Privacy, Communication of the ACM, vol. 38, no. 12/95, str. 48 - 54; Weisband S. P., Reinig B. A., Managing Users Perceptions of Email Privacy, Communication of the ACM, vol. 38, no. 12/95, str. 40 - 47; Milberg S. J., Burke S. J., Smith H. J., Kalman E. A., Values, Personal Information Privacy, and Regulatory Approaches, Communication of the ACM, vol. 38, no. 12/95, str. 65 - 74; Drakulić R.,

**komuniciranja**, kao i na **h) nepovredivost stana**, koja su konstitutivni deo prava privatnosti, ali nisu apsolutnog karaktera (što znači da mogu u strogo predviđenim slučajevima i okolnostima, od strane unapred određenih subjekata, biti "narušena") kao što su integritet ljudske ličnosti, čast, dostojanstvo.

**Treće.** To je pravo koje *zahteva očuvanje tajnosti i slobode privatnog života*<sup>23</sup> što znači da se, s jedne strane, predviđa i obezbeđuje poštovanje privatnosti, a, s druge strane se, predviđaju i sankcionišu svi oblici indiskrecije. Oblici indiskrecije mogu biti različiti i razlikuju se od slučaja do slučaja, ali i od sistema do sistema. Sigurno da su mogućnosti indiskrecije bile drugačije kada se privatnost pojavila, pa su i sankcije bile (ukoliko su i postojale) primerene takvim uslovima. Istovremeno i poimanja određenih stvari bila su drugačija. Na primer, u početku privatnost nije obuhvatala pravo na glas, pravo na tajnost pošiljki i ličnih zapisa, pravo na sopstvenu sliku.

**Četvrto.** *Ovo je pravo apsolutnog karaktera*, što znači da ga ničimi niko ne sme ograničiti, pa makar to bili i "viši interesi države". Naravno, da su velika "iskušenja" da se ono ograniči, ali ovo pravo ta ograničenja ne prihvata. Pri tome, treba ponovo naglasiti da su pridodata prava relativnog karaktera.

Danas, u uslovima kad se lako i gotovo neprimetno ova prava mogu ugroziti zahvaljujući razvoju nauke i tehnike, oblici indiskrecije mogu biti ne samo raznovrsni nego i veoma opasni za pojedinca i njegovu želju da "bude sam" i da svoj privatni život odvoji od pogleda i uvida drugih, bez obzira ko su drugi: država, organizacija, pojedinci njemu znani ili neznani. Zahvaljujući tome, privatnost dobija nove sadržaje i počinje sve više da ukazuje na opasnost koja pretila pojedincu i njegovom pravu na privatnost postojanjem određenih podataka. Ukoliko, ti podaci postanu dostupne javnosti ili drugim licima mogu privatnost ozbiljno da ugroze. Naime, pravo na privatnost je danas najviše ugroženo prikupljanjem, obradom, memorisanjem i dostavljanjem podataka o određenoj ličnosti.

Zbog toga sve veći broj autora i sve veći broj koncepcija, a na osnovu njih i sve veći broj zakona, počinju da tretiraju **privatnost kao pravo pojedinca da kontroliše koji, za koga i kako podaci o njemu mogu postati dostupni drugima**. Ovaj vid privatnosti dobija i posebno ime - **informaciona privatnost** (*information privacy*).

---

Drakulić M., Mogućnost IT prismotre - uzrok tehnostera, I naučni skup: Tehnologija, kultura, razvoj, Beograd, 1995., str. 168 - 176; Drakulić M., Kompiutersko pravo, Beograd, MST Gajić, 1992., str. 84 - 95.

<sup>23</sup> Kandić-Popović Z., op. cit., str. 371.

Otuda se mogu prihvatiti ona shvatanja koja privatnost proširuju i pravima pojedinaca, koja se odnose na podatke o ličnosti, a po kojima je **suština privatnosti u uskladjivanju različitih interesa koji se povodom podataka pojavljuju**<sup>24</sup>.

**Interes društva i države** je da spreči neovlašćeno ili nedozvoljeno prikupljanje podataka; da spreči pristup podacima koji predstavljaju neku tajnu ili su u domenu privatnosti i koji, inače, ne bi, po zakonu, bili dostupni svakome ili nekome; da spreči neautorizovano i nasilno korišćenje ili brisanje onih BP koje sadrže podatke o pojedincima; i da omogućiti samo ona korišćenja koja su pravno dozvoljena i delotvorna. Osim toga u interesu društva i države je i da obezbedi uvid u određene podatke, naročito one koji mogu da doprinesu nacionalnoj sigurnosti i bezbednosti, zaštiti zdravlja stanovništva (na celoj teritoriji), kao i zbog daljeg napretka. Mada izgleda da su ova dva interesa protivurečna, ipak to nije tako, naprotiv, oni se međusobno dopunjuju time što se javnost uključuje samo onda kad za to postoje posebni razlozi. Ti razlozi se moraju jasno definisati, po mogućstvu, definisati slučajeve kad je potrebno praviti izuzetke i decidirano navesti u odgovarajućim pravnim aktima, svima dostupnim.

**Interes pojedinca** je da sazna: da se podaci o njemu prikupljaju i čuvaju, zašto su neophodni, kako će se koristiti i od (strane) koga, u koje svrhe i koliko dugo, kao i, da li su podaci ažurni, relevantni, kompletni i tačni. Isto tako, interes svakog pojedinca je da se podaci o njemu prikupljaju u fer i dozvoljenim postupcima, kao i da se ovi postupci poštuju u njihovom dostavljanju i korišćenju.

**Interes korisnika** ogleda se u potrebi i obavezi da korišćenje podataka o pojedincima ili organizaciji, odgovara njegovim zahtevima i potrebama, a ako je moguće da budu autorizovani i zakonski, odn. pravno dozvoljeni. Pri tome se ne sme zaboraviti činjenica da korisnik stavlja svoj interes u prvi plan, pa tek onda sagledava da li se on poklapa sa pravom. Ukoliko se pojavi raskorak između prava i ovlašćenja i interesa društva, pojedinca i korisnika, pravo na privatnost će biti ozbiljno ugroženo.

Postojanje različitih interesa, manje ili više uskladenih, dovelo je do proširenja sadržine prava na privatnost, informacionom privatnošću ("privatnost" podataka o pojedincima) koja pretpostavlja postojanje prava, ovlašćenja i odgovornosti drugih subjekata u prikupljanju, obradi, raspolaganju, korišćenju i zaštiti podataka o ličnosti.

---

<sup>24</sup> Kavran D, op. cit., str. 36 - 45.

S obzirom, da pravo na privatnost dobija novu dimenziju - novim **pravom na informacionu privatnost**<sup>25</sup>, neophodno je istaći sledeće:

**P r v o.** Pravo na informacionu privatnost je novo, kompleksno, lično pravo kojim se dopunjuje pravo na privatnost. To znači, ***pravo na informacionu privatnost predstavlja novi sadržaj prava na privatnost i njegov konstitutivni deo.*** S obzirom na njegovu kompleksnost, može se učiniti da je pravo na informacionu privatnost posebno pravo, ali nije celishodno, konstituisati ga kao takvog upravo zbog njihove međusobne nedeljivosti. U suštini, to je samo nova generacija prava na privatnost.

**D r u g o.** ***Pravo na informacionu privatnost je pravo pojedinca da kontroliše koji, za koga i kako podaci o njemu mogu da postanu dostupni drugima: odnosi se na podatke o ličnosti***<sup>26</sup> pod kojima se mogu podrazumevati svi oni podaci koji se odnose na neko određeno i određivo fizičko lice, na osnovu kojih može ono biti identifikovano, ali kojima se može ugroziti njegova privatnost. Takodje, ***ovo pravo obuhvata i postojanje definisanih i eksplicitno određenih ovlašćenja i odgovornosti drugih subjekata*** da poštuje informacionu privatnost svakog pojedinca, pošto ni ovo, kao ni bilo koje drugo pravo, ne bi imalo smisla ako ovlašćenja i odgovornosti ne bi bile predviđene. Naime, pravo bi predstavljalo "mrtvo slovo na papiru" i proklamatorno pravo ukoliko mu, kao pandan, ne postoje i obaveze i odgovornosti drugih da ga poštuju. Da bi se ovlašćenja i odgovornosti mogle pojaviti kao sastavni deo ovog prava, mnogi pravni akti predviđjali principe o kojima moraju da vode računa drugi subjekti koji sa podacima o ličnosti dolaze u dodir.

**T r e ć e.** ***Pravo na informacionu privatnost, kao i većina prava nove generacije, je relativnog karaktera*** što znači da može, u strogo predviđenim slučajevima i okolnostima, od strane unapred određenih subjekata, biti "narušeno". To je npr. slučaj kad je u pitanju nacionalna bezbednost, otkrivanje i krivično gonjenje počinioca zločina ili kada, po posebnoj proceduri, podaci o ličnosti učiniti mogu biti dostupnim javnosti.

Pravo na informacionu privatnost predstavlja kompleksno pravo (mada postoje razlike u shvatanjima od kojih se prava ono sastoji) koje obuhvata: **a)** pravo na

<sup>25</sup> Drakulić M., op. cit., str. 85 - 89.

<sup>26</sup> Veoma slično informacionu privatnost definiše Westin (Legislation for Data Privacy, Data Processing and the Law, 1984.) kao "potrebu pojedinaca, grupa i institucija da definišu koje, kada, kako i do koje granice informacije o njima mogu da budu dostupne drugima" ili Kavran (Pravo i regulacija zaštite podataka u informacionim sistemima, 1995.) koji navodi da je to "mogućnost individue da kontroliše prikupljanje, kretanje i upotrebu informacija koje se odnose na nju".

obaveštenost, odn. pravo pojedinca da bude upoznat koji se podaci o njemu prikupljaju, obrađuju i čuvaju, za koje se svrhe i od strane koga se koriste; **b)** pravo na odgovarajuće korišćenje podataka; **c)** pravo pristupa i uvida (pravo kontrole); **d)** pravo ispravke; i **e)** pravo na pravna sredstva<sup>27</sup>.

*a) Pravo na obaveštenost*

**Pravo na obaveštenost predstavlja osnovnu pretpostavku za ostvarivanje drugih prava vezanih za pravo na informacionu privatnost.** Naime, da bi mogao da traži ispravku svojih podataka ili da utvrdi da li se oni koriste u predviđene svrhe, pojedinac mora biti obavešten da se određeni podaci njemu vode, od strane kojih subjekata i za koje potrebe<sup>28</sup>. Često se ovo **pravo realizuje na dva načina: objavljivanjem u odgovarajućim glasilima** o postojanju određene baze podataka ili **direktnim obaveštavanjem svakog pojedinca** o podacima koji se o njemu vode.

U prvom slučaju, po pravilu, obaveštavanje se vrši objavljivanjem određenih pravnih akata (najčešće zakona) koji sadrže obavezu postojanja određenih podataka o ličnosti (npr. vrste i sadržaj evidencija koje se vode po Zakonu o evidencijama u oblasti rada - u Službenom listu SRJ) i kroz popis (prikaz, katalog, i sl.) baza podataka. U zakonima mnogih zemalja predviđeno je stvaranje registra baza podataka, u kojima se nalaze podaci o ličnosti, ali i obaveze korisnika (u nekim zemljama svih, u nekim samo određenih) da subjekta podataka obavesti, na odgovarajući način, o postojanju podataka o njemu (čl. 31 - 40 Zakona o zaštiti podataka SR Nemačke; čl. 3. Zakona o informatici, evidencijama i slobodama Francuske; čl. 8 Zakona o zaštiti podataka Austrije; i sl.). Popis obuhvata specifikaciju o kojim podacima se tačno radi, odn. sadrži podatke o: tačnom nazivu subjekta koji je vodi (ponekad, ukoliko postoji razlika i subjektu koji podatke prikuplja), mestu gde je baza smeštena (gradu, pojedinom telu, i sl.), medijumu na kojem se podaci nalaze, vrsti podataka i njihovom broju (npr. zdravstveni podaci koji se vode po svim bolnicama i zdravstvenim institucijama su opšte generalije, kategorija pacijenta, dijagnostički kod, dužina lečenja i sl.), broju terminalskih mesta, kao i načinu na koji on (pojedinaac) može ostvariti uvid u svoje podatke. Pokatkad ovo obaveštenje obuhvata i naznaku korisnika i visinu naknade koja se mora platiti da bi se podaci prepisali. Tako, npr. po čl. 21. Zakona o informatici, evidencijama i slobodama Francuske, Nacionalna komisija za informatiku i slobode, pri stavljanju podataka iz evidencija na uvid javnosti, prikazuje za svaku od njih: zakonski ili podzakonski akt na osnovu koga se evidencija uspostavlja, i podatke o njihovom

<sup>27</sup> Kavran D., Pravo i regulacija zaštite podataka u informacionim sistemima, I stručni skup: Zaštita podataka u računarskim sistemima, Beograd, 1995., str. 215., smatra da su to: pravo na kontrolu; pravo na notifikaciju, pravo na odgovarajuće korišćenje, pravo na verifikaciju, i pravo na otklanjanje grešaka.

<sup>28</sup> Predlog Savezne Vlade Zakona o zaštiti podataka o ličnosti, septembar 1995., čl. 11.

službenom objavljivanju (tako da se dobija i informacija gde se može naći kompletan tekst zakonskog ili podzakonskog akta); oznaku evidencije i svrhu; službu pred kojom ostvaruje pravo pristupa; vrste podataka o ličnosti o kojima se evidencija vodi, odn. korisnika koji su ovlašćeni da sa podacima raspolažu i sl. Češće podaci o korisnicima, svrsi korišćenja, zaštiti i sl., pojedincu postaju poznati u momentu kad on zatraži uvid u svoje podatke po posebnom zahtevu, ukoliko se podaci o njemu ne skupljaju na osnovu nekog posebnog propisa u kome je ta svrha naznačena. Znači, predviđanjem ovog prava u zakonima o zaštiti podataka i sadržaj registra BP predstavlja jedan od načina da se pojedinac obavesti o postojanju podataka o njegovoj ličnosti.

U drugom slučaju pojedinac se lično obaveštava o postojanju baze u kojoj se nalaze i njegovi podaci, kao i o svim ostalim činjenicama koje su relevantne za njega. Ovaj se način obaveštavanja, u principu, sprovodi za privatne baze podataka za koje ne postoji propisana obaveza vođenja. Postojanje ovih baza dugo je bilo nekontrolisano i gotovo ilegalno zbog malog kruga njihovih korisnika i specijalne svrhe zbog koje su se uspostavljale. Kako se ovim bazama veoma jednostavno moglo ugrožavati pravo na informacionu privatnost to su one postale jedna od ozbiljnih pretnji jer su bile prepuštene *bona fides* korisnika i zaposlenih da se prava pojedinaca poštuju kao i na koji način se to realizuje. Međutim, upravo kod ovih baza podataka trebalo bi voditi računa da se takvom bazom može ugroziti informaciona privatnost. O postojanju takve vrste baze mora se obavestiti pojedinac na koga se podaci odnose, dok se u većini zemalja ova obaveza ne odnosi na baze u kojima postoje podaci o ličnosti, ali oni nisu takvi da ugrožavaju ova prava. Doduše, veoma je teško praviti razliku između takvih baza (podsetimo se da nema bezopasnih podataka). Takve su, primera radi, baze u kojima se formiraju na osnovu nekakvog teksta u kome se kao deo nalaze i neki podaci o pojedincu. Vrlo je očigledan primer koji se za ovakve baze navodi<sup>29</sup>: kad god je unosio rezultate prodaje X je pisao klijentu koristeći termine koje su bili dogovoreni i to u standardnoj formi. Takva pisma X je unosio u PC sa podacima o imovini, ceni i imenima i adresama osoba koje su se u tim poslovima pojavljivale. Kad je pismo hteo da dostavi klijentu X bi u standardno pismo unosio neophodne podatke i štampao ih kao odgovarajući formular. S obzirom da nije bilo obrade podataka ovakva baza nije se smatrala kao baza kojom se ugrožava privatnost. Ona bi to postala u momentu kad bi X formirao bazu sa podacima o klijentima, a ne bazu sa formama pisama, i pojedinac na koga se odnose podaci morao bi biti obavešten o njenom postojanju. Upravo, ovaj primer pokazuje koliko je teško razgraničiti jednu od drugih baza. Mada se čini da je mnogo celishodnije da se sve one nadju u popisu baza, sa obavezom obaveštavanja pojedinaca, ali je to veoma teško ostvarljivo i skupo u slučaju postojanja velikog broja raznovrsnih baza. Zato mnogi zakoni definišu šta se pod podacima o ličnosti, koji treba da uživaju zaštitu, podrazumeva kako bi se moglo znati i da li postoji obaveza

<sup>29</sup> Edwards E., Savage N., Walden I., op. cit., str. 81.

obaveštavanja o njima. Obavezu obaveštavanja imaju, pre svega, pružaoci informacionih usluga koji su fizička ili pravna lica koja snabdevaju druge (korisnike podataka) odgovarajućim podacima. Znači, davaoci usluga su subjekti kod kojih se BP o pojedincima nalaze. Ponekad ti subjekti istovremeno prikupljaju podatke, ali ne mora uvek tako da bude. Dešava se da jedni subjekti podatke skupljaju, a drugi pružaju informacione usluge, odn. obrađuju ih, memorišu i dostavljaju. U takvoj situaciji može se predvideti da oni koji podatke prikupljaju, takodje, imaju obavezu obaveštavanja, mada se ta obaveza, po pravilu, prepušta pružaocu usluga, s tim da subjekta podataka obaveste ko je nadležan za prikupljanje. Te usluge mogu se pružati tako što se korisniku dostavljaju već obrađeni podaci u obliku u kom su dogovoreni ili da se korisnik direktno koristi opremom pružaoca usluga<sup>30</sup>. Oba subjekta dužna su da obaveste pojedinca o postojanju podataka o njegovoj ličnosti.

Pravo na obaveštenost trebalo bi poštovati, čak, i u slučaju kad postoje "opravdani razlozi" (nacionalna sigurnost i sl.) da se o podacima malo zna. Takvi podaci trebalo bi, ipak, da budu poznati (ne konkretni podaci, već činjenica o njihovom postojanju) pojedincu na koga se odnose. Iako o ovome ne postoji jedinstveno mišljenje čini se da je mnogo celishodnije obaveštavati pojedinca o postojanju takvih podataka nego držati u tajnosti koja njihovo postojanje ili nepostojanje prati. Jednostavnije je obavestiti o postojanju razloga za poseban tretman ovih podataka nego javno negirati njihovo postojanje. I minimalna sumnja može da bude štetna, pogotovo ako na neki način to procuri u javnost. U obaveštenju o postojanju ovakvih podataka poželjno je navesti razloge, zbog kojih pojedinac nema pravo na uvid u podatke o njemu.

Ovo pravo istovremeno se obezbeđuje i kad su u pitanju korisnici, jer i oni imaju određene obaveze u odnosu na subjekte podataka. Pod korisnicima podataka obično se podrazumevaju subjekti koji raspolažu podacima. Pokatkad, ukoliko je to potrebno, i sami korisnici obrađuju podatke koji su na drugačiji način već bili obrađeni. Mada korisnici podataka često koriste računar, postojanje računara nije pretpostavka da jedan subjekt bude ili ne korisnik. **Pojedinac u odnosu na korisnika, kad je u pitanju pravo na obaveštenost, ima dva osnovna prava. Prvo pravo pojedinca je da bude informisan**, od bilo kog korisnika podataka, koji ima podatke o njemu. **Drugo pravo je da bude snabdeven primerkom (kopijom) takve informacije.** Kopija može biti u alfabetskom ili grafičkom obliku, ali je bitno da je pojedincu razumljiva. Pri tome je poželjno da se ova informacija ili kopija dostavlja i sa objašnjenjima ukoliko se koriste njemu nepoznati termini ili kodovi (npr. mora se dostaviti i značenje iskorišćenih skraćenica, simbola i sl.)<sup>31</sup>. U svakom slučaju ako subjekt podataka od korisnika želi da sazna da li on i koje podatke ima on će uputiti

<sup>30</sup> Chalton S., Gaskill S., op. cit., str. 1-034, 1-035.

<sup>31</sup> Edwards E., Savage N., Walden I., op. cit., str. 105.

zahtev korisniku, koji je dužan da mu odgovori na zahtev i da mu dostavi informaciju ili kopiju takve informacije. Za razliku od pružaoca ICC usluga, koji sam obaveštava subjekta podataka o njihovom postojanju, korisnik podataka će to učiniti kao odgovor na upućenu molbu (zahtev). U nekim pravnim sistemima (npr. V. Britanije u zakonima (Zakon o zaštiti podataka) je predviđeno, a što bi bilo oportuno i za nas, da **molba**, koju pojedinac upućuje korisniku da bi do ove informacije došao, zadovolji sledeće **uslove**: **1) da bude poslata od subjekta na koji se podaci odnose; 2) da je u pismenom obliku; 3) da se takvim podatkom ne otkriva tajna vezana za drugu osobu koja se može njime identifikovati; i 4) da je praćena sa odgovarajućom naknadom**, koja nije veća od zakonom dozvoljenog maksimuma.

Iako su na prvi pogled ovi uslovi sasvim razumljivi, ipak su oni isuviše strogi prema pojedincima na čije se podatke odnose, naročito onaj poslednji - o plaćanju naknade. Naime, plaćanje naknade često može biti ograničavajuća okolnost za korišćavanje ovog prava. Takodje, postojanje obaveze plaćanja naknade predstavlja svojevrsnu zaštitu korisnika a na štetu subjekta podataka, naročito ako se ima u vidu da korisnik može, u određenim slučajevima, odbiti molbu. Zbog toga bi zakonom trebalo predvideti rokove u kojima korisnik mora odgovoriti na molbu i sankcije u slučaju da se ovi rokovi ne poštuju, a naročito ukoliko podnosilac molbe zbog toga pretrpi neku štetu (npr. Zakon V. Britanije predviđa rok od 40 dana). Ukoliko se to desi, može da podnese tužbu sudu koji procenjuje opravdanost takvog ponašanja korisnika.

Sasvim je drugačija situacija kad je u pitanju treće lice koje traži neke podatke o drugim ličnostima. Za nju moraju da postoje posebno strogi uslovi za dobijanje takvih podataka ili za dobijanje informacije o njihovom postojanju u određenoj bazi.

#### ***b) Pravo na odgovarajuće korišćenje podataka o ličnosti***

**Pravo na odgovarajuće korišćenje podataka je pravo pojedinaca koje se, uglavnom, odnosi na: obezbedjenje odgovarajućeg korišćenja podataka o ličnosti od strane autorizovanih korisnika i sprečavanje korišćenja od neautorizovanih subjekata.** U prvom slučaju, iako na prvi pogled to izgleda besmisleno, neophodno je obezbediti da autorizovani korisnici koriste podatke za predviđene i propisane svrhe, u formi i na način na koji je to predviđeno. Ponekad je to teško ostvarljivo jer autorizovani korisnici u toku korišćenja podataka sami proširuju (opravdano ili neopravdano) svrhu korišćenja i time prekoračuju svoja ovlašćenja ili ih menjaju, s tim da neka od promena predstavlja (u suštini) zloupotrebu. Mada nije jednostavno razgraničiti zloupotrebe od drugih oblika promene, to je ipak moguće. Kod zloupotreba postoji namera da se podaci koriste u druge, nedozvoljene i nelegitimne

svrhe, odn. to je svaki događaj vezan za podatke zbog koga je žrtva - pojedinac pretrpela, ili je mogla da pretrpi gubitak, a izvršilac je to, sa namerom, ostvario ili je mogao da ostvari. Kod obične promene je najčešće je u pitanju ustanovljavanje da li je propisana svrha, preuska ili preširoka od potrebne. Veoma često, podaci koji skupljaju u statističke svrhe koriste u sasvim druge. Primera za to ima mnogo i kod nas i u drugim zemljama. Jedan se desio u vezi sa izjašnjavanjem Srba i drugih naroda i narodnosti u nekadašnjoj Republici Bosni i Hercegovini. Naime, predviđeno je izjašnjavanje i stanovnika ove Republike koji žive na teritoriji drugih republika, kao i njihovih potomaka. Formirani su glasački spiskovi i glasačka mesta u raznim gradovima po republikama. Jedna od njih je bila i Republika Srbija. Posle završenog glasanja postavljeno je pitanje: otkuda glasački spiskovi sa gotovo 100% tačnim podacima o adresama i poreklu potencijalnih glasača? Objašnjenje koje je dato upravo je pokazalo kako je podatke prikupljene za jedne lako moguće koristiti u druge svrhe. Podaci za glasačke spiskove dobijeni su iz statističkog popisa stanovništva iako po odredbama saveznog Zakona o statističkim istraživanjima i Zakona o popisu stanovništva, kao i republičkih zakona, statistički podaci prikupljeni od fizičkih lica, a odnose se na njihove lične, porodične i imovinske prilike, za popis stanovništva smatraju se službenom tajnom i ne mogu se koristiti za druge svrhe sem za statističke. Mnogo se pitanja time otvorilo, ali je najalarmantnije - da li će se podaci iz popisa stanovništva koristiti u još opasnije svrhe, npr. za progon zbog određenog izjašnjavanja o nacionalnosti. Istovremeno ovo možemo shvatiti i kao problem korišćenja podataka u određenoj formi, jer su svi podaci iz popisa stanovništva predviđeni da se koriste kao zbirni, a ne pojedinačni, individualni. Što se načina tiče obično se pod neodgovarajućim načinom, podrazumevaju neregularne sprovedene procedure i postupci korišćenja podataka.

**Zato je neophodno da se vodi računa o dve moguće situacije.** *Jedna, kad se u toku korišćenja podataka ustanovi da je svrha isuviše preusko definisana. Druga je sasvim druge prirode i, u suštini, predstavlja zloupotrebu od strane legitimnih korisnika.* U prvom slučaju moguća su dva rešenja - ili da se na isti način kako je utvrđena i legalizovana prvobitna svrha, ona proširi ili da se zatraži dozvola od subjekta podataka. Prvo rešenje znači, da se donesu izmene i dopune pravnog propisa kojim bi se svrha prikupljanja i korišćenja podataka utvrđivala. To je najduže, ali često i najbolje rešenje jer obezbeđuje sigurnost pojedinaca na koje se podaci odnose. Drugi način je da se "prećutno" proširi svrha i o tome obaveste pojedinci na koje se podaci odnose. Ukoliko se oni usprotive moguće je primeniti prvo rešenje ili odustati. Znači, uz dozvolu subjekta podataka svrha prikupljanja i korišćenja podataka se menja. Dozvola se može dati generalno ili samo za jedno zahtevano proširenje. Ni ovo drugo rešenje nije necelishodno, ukoliko nema mnogo subjekata podataka. Ono je preskupo i može predugo da traje ako ovih subjekata ima mnogo i od svakog od njih treba tražiti dozvolu. Naročito ako se uzme u obzir mogućnost da subjekti podataka ne dozvole da se svrhe prošire.

Situacija je drugačija ukoliko autorizovani korisnik vrši promenu svrhe prikupljanja sa namerom da podatke zloupotrebi ili ako podatke prikupljene za jednu koristi u druge svrhe. Ne tako retko namera zloupotrebe postoji i pre nego što je svrha prikupljanja i postojanja nekih podataka o ličnosti utvrđena. Često se dešava, ako se unapred zna, da se podaci o ličnosti ne smeju koristiti za neke svrhe, a da bi se izbegle mogućnosti zabrane prikupljanja i korišćenja podataka prezentira se jedna ssvrha, a već se zna, da će se kasnije koristiti za sasvim drugu. Tako, npr. podaci o socijalnom poreklu koji su, inače, veoma "osetljivi" podaci ne smaju se prikupljati i koristiti neograničeno. Da bi se dobilo legitimno pravo za njihovo prikupljanje i korišćenje prezentira se da je svrhe baze podataka praćenje socijalnog statusa stanovništava radi preduzimanja mera u obezbeđenju njihove ravnopravnosti. Potom se takva svrha "modifikuje" u pravljenje socijalne diskriminacije npr. u zapošljavanju, obrazovanju, napredovanju. To je veoma česta pojava i kad su u pitanju drugi podaci. Ne treba zaboraviti ni matični broj, niti podatke u telefonskim imenicima koji mogu, u određenim sistemima, predstavljati upravo one bezazlene podatke, čija se upotreba veoma jednostavno može zloupotrebiti<sup>32</sup>.

Nešto je drugačije kad je u pitanju zloupotreba već postojećih podataka za koje je određena svrha odavno utvrđena i čija je promena je izvršena tajno, bez dozvole i obaveštavanja. Pri tom, treba praviti razliku između prikupljanja, obrade i dostavljanja **nekorektnih podataka** (oni podaci koji su netačni ili podaci koji dovode u zabludu bilo koju činjenicu ili predmet) od situacije kad je u pitanju **ilegalno prikupljane i memorisanje dozvoljenih podataka**. Tako se, za prvi slučaj vezuje primer poznat kao slučaj Tomson protiv Udruženja maloprodaje San Antonio u SAD. Ovo Udruženje koristilo je kompjuterizovano radi "automatsko evidentiranje uhapšenih" dobijanja podataka o potencijalnim korisnicima kartica. Ove podatke, dobijene direktnom terminalskom vezom, automatski su unosili u fajlove svoje baze **SARMA** (*San Antonio Retail Merchants Association*), tako da su korisnici koji su imali pristup bazi mogli doći do njih i na osnovu toga doneti sopstvenu odluku o izdavanju kreditne kartice određenom kupcu. Takav podatak bi se odmah našao u bazi sa kompletnim obrazloženjem nepodobnosti što je predstavljalo osnovu da se i drugi podnosioci zahteva za karticu, po istom osnovu, odbiju. Ovo je izazvalo brojne probleme jer su se u, suštini, obavljala ukrštanja baza čije su pojedinačne svrhe bile potpuno drugačije. Sud, kome su se pojedinci žalili, prihvatio je njihovu tužbu kao osnovanu sa obrazloženjem da se ukrštanjem takvih baza menja njihova svrha, a za to je potrebna posebna dozvola i odgovarajući pravni osnov. SARMA je kažnjena za pretrpljeno

<sup>32</sup> Wolinsky C., Sylvester J., Privacy in the Telecommunications Age, Communication, vol. 35, no. 2/92, str. 23 - 25; Rotenberg M., Communications Privacy: Implications For Network Design, Communication, vol. 36, no. 8/93, str. 61 - 69; Samuelson P., First Amendment Rights For Information Providers, Communication, vol. 34, no. 6/91, str. 19 - 24; Drakulić M., Informacione tehnologije i privatnost, Kotor, zbornik radova sa XXI SYM-OP-IS'94, str. 268 - 272.

poniženje i stres, novčanom kaznom od \$10.000 po pojedincu, u čijim su se fajlovima našli ovi podaci i sa još \$4.485 za prekršaj<sup>33</sup>. Slično je i sa prikrićivanjem postojanja nekih podataka u bazi, odn. kad se prikupljaju i koriste bez unapred određene svrhe. Njihovo postojanje nigde se ne evidentira i nije zasnovano na nekom regularnom pravnom osnovu, već na volji subjekata koji to vrše. Često su ovi podaci vezani za rad policije i sličnih institucija, mada to nije strano ni preduzećima koja se skrivaju iza formulacije "za potrebe poslovanja". U svim ovim slučajevima, postojanje zloupotreba je teško otkriti, pogotovo za pojedinca, koji može biti obmanut i činjenicom da se takvi podaci nalaze u posebnoj formi ili u posebnim, njemu i drugima nedostupnim delovima baze ili ih je teško kontrolisati jer se operacije modifikacije izvršavaju jezicima višeg nivoa.

Posebno nastaje problem kad podatke koriste neautorizovani korisnici. Naime, svaki korisnik, da bi postojalo regularno korišćenje ličnih, ali, ne samo njih, podataka, morao bi biti autorizovan i to za sve operacije i svaki deo određene baze ili određenog podatka. Drugim rečima, **svaki korisnik trebalo bi da ima ovlašćenje za korišćenje određene baze i podataka**. To ovlašćenje, može biti na osnovu zakona ili volje nekog drugog subjekta, generalno ili specijalno, ograničeno ili neograničeno. Tako, korisnik može da ima pristup celoj bazi i svim podacima, može da ima pristup samo jednom delu baze ili određenoj grupi podataka, i može imati pristup stalno ili samo u određenim vremenskim intervalima celoj ili delu baze. Ukoliko prekorači data ovlašćenja, ili ih uopšte nema, korisnik se pojavljuje u svojstvu neautorizovanog korisnika i pristupom bazi ili određenim podacima, čini prekršaj ili krivično delo. Ta ovlašćenja koja korisnik ima uskladjuju se sa ciljem postojanja određenih podataka i ukoliko se korisnik pojavljuje kao neautorizovan tada se, pored ostalog, menja i cilj podataka i ugrožava pravo na njihovo odgovarajuće korišćenje. Ako dodje do ovakve situacije subjekt podataka bi morao o tome biti obavešten. Obaveštenje bi, pored toga, trebalo da sadrži i podatke o posledicama koje mogu za njega nastati, kao i o daljim načinima zaštite prava ukoliko do neželjenih posledica dodje.

U suštini, pravo na odgovarajuće korišćenje podataka o ličnosti ima svaki pojedinac, kako bi se omogućilo da on, i pored njihovog postojanja, u javnim ili privatnim bazama, osećao sigurnim da se ti podaci neće koristiti protiv njega ili zloupotrebljavati. Upotpunjavanjem ovog prava, odgovarajućim principima zaštite podataka o ličnosti omogućiti se primena drugih prava i principa.

### *c) Pravo pristupa i uvida*

---

<sup>33</sup> Sieber U., The Handbook on Computer Crime, Chichester, John Wiley & Sons, 1986., str. 22.

Pravo na odgovarajuće korišćenje, kao i druga prava ne bi se realizovala ukoliko subjekt podataka ne može da prokontroliše:

- kakvi se podaci u nekoj bazi o njemu nalaze?
- ko ih koristi i po kom osnovu?
- za kakve svrhe?
- da li se neki podaci čuvaju duže nego što je to potrebno i predviđeno?
- da li se u bazi nalazi više podataka nego što je to nužno?
- da li su podaci tačni?
- da li su se, i kad, podaci o njemu izgubili?
- da li su, kada i kako podaci uništeni bez ovlašćenja korisnika i pružaoca informacionih usluga?
- da li su i kako podaci objavljeni i u kojoj formi, bez dozvole, od strane korisnika, davaoca usluga ili trećih lica?

Drugim rečima, **pojedinač bi morao da kontroliše ispravnost postojanja, obrade i korišćenja podataka o njemu i ispravnost ovlašćenja korisnika**. Da bi on to svoje pravo mogao da koristi on mora da ima i **pravo pristupa i uvida u bazu**<sup>34</sup>. Uvid pretpostavlja: uvid u podatke koji se u bazi nalaze i uvid u podatke koji iz baze izlaze. U poslednje vreme sve je veća zainteresovanost pojedinaca da kontroliše kakvi i kome izlazni podaci o njemu kreću iz baza. Dešavalo se da se privatnost ne ugrožava ulaznim podacima, već izlaznim.

Pravo pristupa i uvida mora se upotpuniti i **pravom da pojedinac zahteva: 1) da se podaci iz baze brišu; 2) da se podaci menjaju u skladu sa njegovim zahtevima i propisanom svrhom; 3) da se pojedinim korisnicima ograniči autorizacija; 4) da se menja svrha za koju se podaci koriste; 5) da se podaci o ličnosti zaštite posebnim merama i mehanizmima; i sl.**

Pravo pristupa i uvida, celishodnosti radi, trebalo bi vremenski, kad kod je to moguće, ograničiti, kao što bi trebalo i predvideti sankcije za korisnika ili davaoca informacionih usluga ukoliko ne omoguće subjektu podataka da kontroliše, i to njemu razumljive, podatke. Naime, veoma često subjekt podataka kontrolu svojih podataka vrši iz čiste radoznalosti, pa bi bilo veliko opterećenje da mu se neograničen broj puta i u neograničenim vremenskim intervalima obezbedi uvid. Pogotovo ako se ima u vidu da se podaci o ličnosti u bazi nalaze u mašinski čitljivom obliku, pa ih treba prilagoditi da ih svaki pojedinac, bez obzira na obrazovanje, može razumeti. U tom slučaju bilo bi

<sup>34</sup> Po Predlogu zakona o zaštiti podataka o ličnosti ovo je pravo iskombinovano sa drugim i u šest tačaka člana 12. definisano kao "pravo građanina da zahteva...".

umesno da se predvide rokovi kad pojedinac može svoje podatke, i njihovu upotrebu, kontrolisati, naravno, zavisno od svrhe zbog koje se podaci vode i njihove prirode. U mnogim zakonima zbog toga je predviđeno plaćanje naknade.

Pravo pristupa i uvida može biti, opravdano ili neopravdano, ograničeno ili neostvareno ako davalac informacionih usluga ili korisnik odbiju da omoguće uvid. S obzirom, da su retki opravdani razlozi za odbijanje, pojedinac može na drugi način da zahteva da se ovo njegovo pravo poštuje. Izuzetak su samo oni podaci za koje je, u odgovarajućim pravnim aktima, predviđeno da predstavljaju izuzetak i ograničavanje ovog prava. Mnogi nacionalni zakoni, sistemom enumeracije određuju koji su to podaci ili situacije kad se ovo pravo ograničava. Tako, npr. Francuski zakon predviđa mogućnost da svojim zdravstvenim podacima subjekt podataka ne može da ima direktan pristup, već mu oni mogu biti saopšteni samo preko lekara, koji je za to određen.

Ukoliko se, pak, omogući pristup i uvid podataka i pojedinac ustanovi da postoje određene nepravilnosti, on može da zahteva da bude obavešten o njihovom otklanjanju. U zakonski predviđenom roku korisnik i davalac usluga moraju otkloniti nepravilnosti ili, ukoliko se u posebnom postupku utvrdi, da ne postoje, i dužan su, u određenom roku, po pravilu rešenjem, subjekta o tome obavestiti. Kada je subjekt podataka nezadovoljan ovim rešenjem, može da podnese žalbu nadležnom organu, organizaciji ili sudu.

#### ***d) Pravo na ispravku podataka o ličnosti***

Na osnovu kontrole podataka o svojoj ličnosti pojedinac može da ustanovi, izmedju ostalog, da se u BP nalaze netačni i neažurni podaci. Oni se u bazi mogu naći na više načina, najčešće na osnovu iskaza trećih lica ili na osnovu dokumenata u kojima se nalaze netačni ili neažurni podaci. Ponekad i sam korisnik "fabrikuje" netačne podatke, a ovakve situacije nisu strane ni pružiocima ICC usluga. Najviše pažnje netačnim ili lažnim podacima se posvećuje ako se oni nadju u bazama zbog "upada" hakera ili drugih lica koja takve podatke namerno ubacuju. Bez obzira od koga su netačni podaci o pojedincu uneti u bazu oni mogu da izazvu dalekosežne negativne posledice, naročito onda ako, na osnovu takvih podataka, pojedinac treba da koristi svoje pravo, npr. pravo na penziju, socijalnu pomoć i sl. Kada se konstatuje postojanje netačnih podataka potrebno je da prodje izvesno vreme da bi se podatak u bazi ispravio. Dokazivanje, po pravilu, pada na teret samog pojedinca, što umnogome komplikuje situaciju, a ne onoliko kao kad se neki podatak namerno, od strane zaposlenih u računskom centru, unese u bazu. Veoma je slikovit slučaj jednog programera, koji je programirao "zamku za podatke", kao program koji je kupio podatke o ličnosti iz videotekst sistema jedne baze i ubacivao ga u baze drugih korisnika, dodajući ih u fajlove

drugih lica, kako bi s njima manipulisao. Na osnovu toga mnogi pojedinci bili su snabdeveni nizom netačnih i tuđih podataka, pa je nastao problem pri rešavanju zahteva za dodeljivanje kredita.

Da bi ublažili posledice prouzrokovane ovakvim podacima **mnogi zakoni o zaštiti podataka predviđali su pravo pojedinca da ih ispravi**. Međutim, po zakonima nekih zemalja *nije dozvoljeno da pojedinac ovo pravo automatski iskoristi* kod pružaoca ICC usluga i/ili korisnika, već da se ono realizuje preko suda ili nadležnog tela. Tako je, npr. Zakon o zaštiti podataka V. Britanije prihvatio rešenje da se netačni podaci o ličnosti mogu ispraviti samo ako sud prihvati navode tužbe i naloži korisniku ili pružaocu usluga da ih ispravi, blokira ili izbriše.

Mada je ovo rešenje, na prvi pogled, potpuno logično i celishodno ipak postoje određeni razlozi zbog kojih treba biti sumnjičav u odnosu na njegovu efikasnost. Naime, da bi svoje pravo na ispravku realizovao, pojedinac mora da podnese tužbu sudu i da podnese dokaze o svojim navodima. Sud ispituje činjenice i stranke u postupku i često može tražiti i veštačenje ili dodatno ispitivanje istinitosti navoda i činjenica, ukoliko ustanovi da postoji namera da se podaci prikažu u drugom svetlu. To znači produžen period postojanja netačnih podataka i velike izdatke za sprovođenje postupka dokazivanja, kao i za advokate koji će to realizovati. Naročito onda kad se tačni podaci mogu dobiti samo na osnovu iskaza svedoka, do kojih je, ponekad, teško doći. Sve to zajedno otežava položaj pojedinca koji je, i onako, ugrožen postojanjem netačnih podataka. Ipak je bolje rešenje *da se ceo postupak ispravke vrši, uz odgovarajuću dokumentaciju, odmah kod subjekta nadležnog za prikupljanje, obradu i memorisanje podataka*, a samo izuzetno i kod suda.

Kada su u pitanju neažurni podaci, neophodno je praviti razliku kad su oni posledica propuštanja ažuriranja od strane pružaoca usluga, od slučaja kada je to propust subjekta podataka. U prvom slučaju troškovi postupka, nakon utvrđivanja njihovog postojanja, trebalo bi da padnu na teret onoga ko je ažuriranje propustio. U drugom slučaju to će biti na teret pojedinca koji je "zaboravio" ili nije hteo da o promeni svojih podataka obavesti nadležni subjekat.

Poseban je slučaj kada je tačnost podataka dovedena u pitanje zato što lice na koje se on odnosi osporava tačnost, ali ne može to da obezbedi da se to i utvrdi, a postoji neophodnost njihovog postojanja. Tada će ovakvi podaci biti **blokirani** (kako je predviđeno u čl. 14. Zakona SR. Nemačke).

Slična je situacija i kad se traži brisanje određenih podataka jer se oni prikupljaju, obrađuju i koriste u suprotnosti sa pravima pojedinaca ili se čuva veći broj podataka nego što je potrebno i duže nego što je predviđeno. Po zakonima nekih zemalja i to je u nadležnosti suda koji, bez obzira na ovlašćenja korisnika i pružaoca usluga, može narediti njihovo brisanje. Posebni slučajevi su: kada podaci postanu dostupni neautorizovanim korisnicima; kada se otkrivaju javnosti ili kada dodje do zloupotrebe od strane autorizovanih korisnika, pa se iz tih razloga traži njihovo brisanje. Tada ima smisla predviđanje nadležnosti suda, dok u prvom slučaju čini se da je mnogo celishodnije ovo pravo realizovati kod pružaoca usluga. Međutim, neophodno je imati u vidu da se brisanjem podataka o pojedincima može naneti šteta korisnicima podataka i zato je oportuno da se oni konsultuju pre nego što do stvarnog brisanja podataka i dodje. Možda će u takvoj situaciji korisnik usluga želeti da, bez obzira na dodatne troškove, neko drugi obavlja ICC usluge, i umesto brisanja, bazu prenese u drugi biro, centar.

*e) Pravo na pravna sredstva zaštite*

Kad pojedinac otkrije pojavu raznih nepravilnosti u vezi sa podacima o njemu, ostaje mu mogućnost korišćenja još jednog prava - **prava na pravna sredstva zaštite**. Ovo svoje pravo pojedinac će koristiti ukoliko nije zadovoljan odlukom pružaoca ICC usluga ili korisnika. U zahtevu, prigovoru, žalbi pojedinac navodi zbog čega je nezadovoljan, navodi nove činjenice, nove dokaze i razloge zašto ih nije naveo ranije.

Na osnovu pravnog sredstva zaštite, nadležni organ može da donese odluku da se određeno pravo pojedinca poštuje i da mu se zbog nepoštovanja prava, naknadi šteta, moralna ili materijalna,.

Znači, kao deo prava na pravna sredstva zaštite pojavljuju se još i **pravo pojedinca na naknadu štete** (materijalnu i moralnu) koju je pretrpeo zbog postojanja netačnih podataka i zbog izgubljenih ili uništenih podataka, kao i zbog pristupa neautorizovanih subjekata<sup>35</sup>.

U prvom slučaju efekat koji proizlazi iz nepostojanja "dostojne pažnje" o podacima ličnosti, doneto je pravo pojedinca na naknadu štete od pružaoca ICC usluga nastale kao posledica nehata ili namere u odnosu na postojanje takvih podataka. Cilj postojanja naknade usledila je iz potrebe da se predvidi i sankcioniše odgovornost za osiguranje tačnosti podataka. Ova obaveza postoji i kad su u pitanju korisnici podataka. Otuda se sve češće traži verifikacija tačnosti podataka od strane subjekta podataka. Ukoliko se verifikacija nije blagovremeno obezbedila sud, ili drugi nadležni organ, može da presudi na štetu korisnika zbog nehata koji je pokazao unošenjem neproverenih podataka ili pružaoca usluga zbog unošenja neproverenih podataka u bazu. U stvari, subjekt podatka stiče pravo da tuži za štetu koja bi nastala zbog propuštanja provere podataka i verifikacije tačnosti, dodajući i pravo na naknadu za moralnu štetu koja radi takvih podataka nastaje.

**Pravo na naknadu štete usled gubljenja, neautorizovanog pristupa, objavljivanja ili uništenja podataka treba da obezbedi subjektu podataka sigurnost da će se za njegove podatke, od strane pružaoca usluga i korisnika, preduzeti odgovarajuće mere zaštite.** Ako do toga ipak dodje, subjekt podataka može zahtevati naknadu štete koja je nastala ili je mogla nastati usled nehata ili namere korisnika ili pružaoca usluga. U takvim situacijama subjekt podataka može da podnese

<sup>35</sup> Edwards E., Savage N., Walden I., op. cit., str. 105.

tužbu sudu<sup>36</sup> koji će, na osnovu pribavljnih dokaza, odrediti visinu naknade, ali i brisanje takvih podataka ili preduzimanje mera zaštite uz obavezu sa izvesti i korisnika i pružaoca usluga o preduzetim merama i njihovim efektima.

Medjutim, odgovarajuće pravno sredstvo zaštite (tužba) biva aktivirano i kad je u pitanju krivičnopravna i prekršajna odgovornost. Ukoliko se utvrdi postojanje zakonom predviđenih povreda (sabotaže, špijunaže, vandalizma, virusa, hakinga, prevare, i sl.) kazniće se počinioc kaznom zatvora i/ili novčanom kaznom, što naravno ne isključuje ni mogućnost naknade štete, ali u posebnom građanskopravnom postupku, tim više ako su štete nastale kompjuterskim kriminalom izuzetno velikih vrednosti (kreću se i preko \$500.000 po delu)<sup>37</sup>.

Kao posebni zaštitnik prava pojedinca pojavila se i institucija ombudsmana, koja bi trebalo da obezbedi<sup>38</sup> svakog pojedinca od nezakonitog, nepravilnog ili neefikasnog rada uprave koja svakodnevno postaje sve veći korisnik podataka o ličnosti, ali i pružalac informacionih usluga i podataka. Zbog toga se uvodi institucija **"ombudsmana za zaštitu podataka"** tako da mnogi nacionalni zakoni, preuzimajući ovu instituciju iz nordijskog prava, formiraju posebna tela (komisije) ili zaštitu poveravaju specijalizovanom inokosnom organu (registrar, poverenik za zaštitu podataka i sl.). Pojedinaac može da se obraća ovom telu svaki put, kad smatra da mu je privatnost ugrožena nezakonitim, nepravilnim ili neefikasnim tretmanom podataka o njegovoj ličnosti.

**Ova prava ne bi se mogla efikasno realizovati, ako ne postoje i odgovarajuće obaveze i odgovornosti drugih subjekata.** Kao drugi subjekti pojavljuju se: **a)** korisnici podataka i pružaoci informacionih usluga i **b)** kontrolori podataka.

<sup>36</sup> Ovo je pravo predviđeno i u Predlogu zakona, no, pravo na pravni lek građanin ima zbog povrede svojih prava utvrdjenih ovim zakonom, ali pred nadležnim saveznim organom. Pred sudom će moći da traži zaštitu ukoliko mu je naneta šteta zbog korišćenja podataka prikupljenih na način i za svrhe koje nisu u skladu sa propisanim (čl. 15.).

<sup>37</sup> Heardndn K., Computer - Linked Crime - What is Happening?, edicija: A Handbook of Computer Security, London, Kogan Page, 1990., str. 21.

<sup>38</sup> Lilić S., Pravna informatika, Beograd, Zavod za izdavanje udžbenika i nastavnih sredstava, 1991., str. 206, 209.

*a) Obaveze i odgovornost korisnika podataka i pružaoca informacionih usluga*

**Pružaoi ICC usluga i korisnici obavezni su (i ovlašćeni) da prikupljanje, obradu i korišćenje podataka o ličnosti obavljaju na zakonit i "pošten" način,** vodeći računa: da li su podaci koje prikupljaju, obrađuju i koriste u skladu sa dozvoljenim svrhama; o tačnosti, ažurnosti i istinitosti; o vremenu za koje postoji obaveza prikupljanja, čuvanja i korišćenja; o rokovima za ispravku, dopunu, blokiranju podataka; o rokovima za postupanje po zahtevima za ispravku; kao i rokovima za podnošenje zahteva, odn. prijave za registraciju BP; ispunjenju svih zahtevanih uslova za potpunost sadržaja prijave; o obaveštavanju subjekta podataka o postojanju određene baze; dopuštenosti obrade, odn. da li za određenu obradu postoji izričito zakonsko ovlašćenje ili ono proističe iz, zakonom utvrdjenih, nadležnosti ovih subjekata ili je za to dobijena neophodna dozvola subjekta podataka; i sl. Posebno, pružaoi ICC usluga moraju preduzeti odgovarajuće mere obezbedjenja i zaštite IS. Kod nas su, npr. Uredbom o obezbedjenju i zaštiti informacionih sistema državnih organa<sup>39</sup>, predviđene organizacione i tehničke mere koje se moraju preduzeti u "cilju sprečavanja slučajnih grešaka, nepravilnog i neodgovornog prikupljanja, čuvanja, obrade, iskazivanja, korišćenja, oštećenja, uništenja, kao i falsifikovanja i zloupotrebe podataka". Isti propis predviđa, da za uspešno funkcionisanje mera obezbedjenja i zaštite se mora, između ostalog, obezbediti: da pristup podacima i računarskoj opremi mogu imati samo ovlašćena lica, da se mora kontrolisati ko i kada ulazi u prostorije računskog centra, na koji će se način i na kojim medijumima čuvati tajni podaci i sl. Ukoliko se ove mere ne preduzmu, pa dodje do gubljenja, oštećenja ili uništenja podataka, neautorizovanog pristupa ili zloupotrebe podataka, pružaoi ICC usluga odgovaraće za nastalu štetu. Time se, u stvari, želi obezbediti, da se odgovarajuće mere obezbedjenja i zaštite stvarno i preduzimaju.

U većini zemalja, kao posebna obaveza davaoca ICC usluga i korisnika, prijavljivuje se registrovanje kod odgovarajućeg tela (registrator, Centralni statistički zavod, Federalni poverenik za zaštitu podataka, Federalna komisija za zaštitu podataka, i sl.), odn. podnošenje zahteva za izdavanje dozvole od određene komisije (Komisija za zaštitu podataka - Švedska, Nacionalna komisija za informatiku i slobode - Francuska) za vođenje ili korišćenje neke baze podataka o ličnosti. Prijavu, odnosno, zahtev za registraciju podnosi korisnik podataka, davalac ICC usluga, kao i korisnik podataka koji se istovremeno pojavljuje i kao davalac ovih usluga. Naravno, postoje razlike između zemalja na koje se korisnike i pružaoce usluga odnosi ova obaveza, jer u jednoj grupi zemalja u pitanju su samo podaci koji se nalaze u državnim službama i službenim evidencijama (SAD, Kanada), dok se u drugim odnosi i na neslužbene, privatne,

<sup>39</sup> Uredba o obezbedjenju i zaštiti informacionih sistema državnih organa, Službeni glasnik SRS, br. 41/90, čl. 2, st.1.

subjekte (mada i tu postoje razlike u većini zemalja jednim su zakonom i istim pravnim režimom obuhvaćeni i jedni i drugi subjekti, dok se u drugim - Danska, Norveška - ova problematika rešava u dve vrste zakona). Iako svaka prijava mora da sadrži podatke koje predviđa zakon te zemlje, ipak je sigurno da su to i podaci: o sedištu i nazivu korisnika podataka; opisa podataka o ličnosti i razloga prikupljanja, obradivanja ili korišćenja; o izvoru podataka; o licima kojima se podaci saopštavaju; i sl. Prijava za registraciju, odn. zahtev za dozvolu predstavlja jedan od prethodnih uslova koji treba da ispune korisnik i pružalac usluga, da bi mogao podatke o ličnosti da koristi, prikuplja ili/i obrađuje.

Ponekad se dešava da se prijava ili zahtev negativno reše; tada korisnik ili davalac usluge ne smeju da raspolazu tim podacima, niti da ih prikuplja ili obrađuje, a ako bi to i dalje činili bili bi krivično i prekršajno kažnjeni.

Iz ovih obaveza i ovlašćenja davalac ICC usluga i korisnika proističu i njihove **odgovornosti** i to za<sup>40</sup>.

- ažurnost i tačnost podataka;
- nepovredivost materijalne sadržine podataka prilikom obrade i iskazivanja;
- obezbeđivanje uslova za nesmetano korišćenje podataka i informacija u skladu sa osnovnom namenom za koju se prikupljaju;
- obezbeđenje i zaštitu podataka i informacija<sup>41</sup>;
- primenu jedinstvenih definicija, klasifikacija, nomenklatura i identifikacija, kao i standarda u vezi sa čuvanjem, prenosom, obradom i iskazivanjem podataka, računarskom opremom i njenom programskom podrškom.

Ovlašćenja treba dopuniti i **specifičnom odgovornošću** koja je predviđena za podatke o ličnosti:

- obezbediti da se prikupljanje, obrada i korišćenje podataka ograniči samo na one podatke koji su neophodni;
- obaveštavanje pojedinaca o podacima koji će se prikupljati, obrađivati i koristiti, ko će ih prikupljati i za koje svrhe;
- obaveštavanje pojedinaca o posledicama koje mogu da nastanu ukoliko odbiju da daju odobrenje da se podaci o njima koriste;

<sup>40</sup> Npr., po članu 14. Zakona o društvenom sistemu informisanja Srbije, Službeni glasnik SRS, br. 49/89.

<sup>41</sup> Zakon o informacionom sistemu Republike Srbije, Službeni glasnik RS, br. 12/96, čl. 12. predviđa zaštitu informacionog podsistema u svim fazama razvoja i funkcionisanja.

- kontrolisanje dostavljanja podataka o pojedincima tako da ih mogu koristiti samo autorizovani korisnici i za autorizovane namene;
- osiguranje kvaliteta podataka, odn. njihovu kompletnost, tačnosti i ažurnost;
- obezbediti kontrolu izvora i korisnika podataka; i
- brisati podataka koji više nisu potrebni.

Ukoliko dodje do povrede odredbi zakona i podzakonskih akata kojima se predviđa zaštita podataka o ličnosti ovi subjekti podležu krivičnopravnim, prekršajnim i građanskopravnim sankcijama, s tim što se kao rešenje pojavljuje i mogućnost da im se zabrani rad, odn. zabrani pružanje određenih ili svih informacionih usluga ili korišćenje i raspolaganje ovim podacima. Na primer, po Zakonu o zaštiti podataka V. Britanije "ukoliko registrar utvrdi da je registrovano lice odstupilo ili da odstupa od načela zaštite podataka, može mu izdati načelno upozorenje kojim mu se nalaže da u određenom roku, preduzme mere koje su označene radi postupanja u skladu sa odgovarajućim načelom"<sup>42</sup>. U slučaju da se radi o većoj povredi, ili subjekt odbije, ili se ogluši o upozorenje, registrar može doneti odluku o brisanju iz registra. Tada će se korisnik ili davalac ICC usluga morati pridržavati odluke nadležnog tela o brisanju iz registra, koja, u stvari, znači zabranu korišćenja, prikupljanja i obrade podataka o ličnosti. Ukoliko se subjekt ne bi pridržavao odluke, odgovoraće za povredu propisa o zaštiti podataka.

Poseban problem je: **obaveza i odgovornost ovih subjekata o odnosu na svoje zaposlene** koji su u vezi ili mogu da dodju u dodir sa podacima o ličnosti<sup>43</sup>, pogotovo, što je i najveći broj počinitelja raznih dela kompjuterskog kriminala baš iz kruga informatičara-profesionalaca<sup>44</sup>. Za takve podatke se, po pravilu, predviđa da predstavljaju službenu tajnu, tako da zaposleni o njima moraju voditi računa u smislu njenog posebnog tretmana (slično rešenje je npr. prihvatio Ustav Republike Srbije koji u čl. 20. predviđa "Zajemčuje se zaštita tajnosti podataka o ličnosti"). Pokatkad se neki od ovih podataka proglašavaju za poslovnu tajnu korisnika ili davalac informacionih usluga, te se, otuda, moraju, kao takvi i čuvati, a zaposleni na to obavezivati. Radi bolje i sigurnije zaštite, često se u pojedinačnom ugovoru o radu (ovo može da važi i za nas), koji se zaključuje sa svakim zaposlenim ponaosob, preciziraju dužnosti i odgovornosti vezane za podatke koji predstavljaju službenu, poslovnu tajnu ili su proglašeni za neku drugu tajnu. Otkrivanje ili omogućavanje neautorizovanog pristupa ili drugih nepravilnosti i zloupotreba predstavlja krivično

<sup>42</sup> Guideline 3 for Data Protection Act 1984., London, The Data Protection Registrar, 1992., str. 20 - 26.

<sup>43</sup> Edwards E., Savage N., Walden I., op. cit., str. 189.

<sup>44</sup> Hearnden K., op. cit., str. 38 - 40.

delo, kao što je i teža povreda radne discipline koja povlači odgovarajuće disciplinske mere.

Pojavio se osobito težak problem u odnosu na **bivše zaposlene i njihovu obavezu i odgovornost na podatke o ličnosti**, koji su im bili dostupni. U ovakvim slučajevima teško je naći odgovarajuće rešenja<sup>45</sup>. Između ostalog, moguće je predvideti posebnu **konkurentsku klauzulu** u pojedinačnom ugovoru o radu, kojom se određeno lice obavezuje da se neće izvestan period (posle prestanka zaposlenja) baviti takvim poslom ili zaposliti kod direktnog konkurenta ili na geografskom području koje može da ugrozi rad korisnika ili pružaoca određenih ICC usluga (npr. u SAD to je 2 godine). Za poštovanje ovih obaveza predviđene su dodatne nagrade, kako zaposleni ne bi trpeo štetu. Nepoštovanje ovakve klauzule može izazvati i plaćanje ogromnih odšteta od strane bivšeg zaposlenog i/ili nove firme u kojoj se zaposlio i odao podatke o ličnosti predviđene za službenu (poslovnu) tajna. Pored konkurentne klauzule, često se u ugovor o radu unosi i **klauzula o poslovnoj tajni**, kojom se reguliše individualna obaveza bivšeg zaposlenog da čuva podatke o ličnosti kao poslovnu tajnu (naravno, ako su ovi podaci proglašeni kao takvi), kao i obavezu da neće raditi na istim ili sličnim poslovima izvesno vreme.

Drugi način je primena prava, radi sprečavanja nelojalne konkurencije. U anti-trustovskim, anti-monopolskim, kao i zakonima o nelojalnoj konkurenciji predviđaju se, kao dela nelojalne utakmice preuzimanje tuđeg radnika ili odavanje poslovnih tajni. Za učinjena ova dela predviđena je često krivična, kao i administrativna sankcija. Postoje i druga rešenja koja su, manje ili više, efikasna, a čija primena zavisi od pravnog sistema i dovirljivosti oštećenog korisnika ili davaoca ICC usluga.

Sve u svemu, ne sme se zaboraviti da obezbedjenje od ovakvog oticanja ili zloupotreba podataka o ličnosti, predstavlja obavezu i povlači odgovornost samog subjekta o čijim se zaposlenim (sadašnjim i bivšim) radi, tako da se subjekt podataka ili kontrolor pojavljuje sa svojim zahtevima.

#### ***b) Obaveze i odgovornosti kontrolora podataka***

Gotovo svi zakoni o zaštiti podataka i neki međunarodni instrumenti (npr. Evropska Direktiva) predviđaju **poseban organ za nadzor nad regularnošću i legitimnošću podataka o ličnosti i njihovom zaštitom**. Razlike postoje u vrsti ovog organa - dok jedne zemlje predviđaju **inokosni organ** (*Komesar* za zaštitu podataka

<sup>45</sup> Edwards E., Savage N., Walden I., op. cit., str. 198.

u Kanadi; Savezni *Poverenik* za zaštitu podataka i zemaljski poverenici za zaštitu podataka u Nemačkoj; *Registrar* za zaštitu podataka u V. Britaniji, državi Džersi i ostrvu Man), dotle se u drugim zemljama obrazuje **kolegijalni organ** za zaštitu (*Nacionalna komisija* za informatiku i slobode u Francuskoj; *Računarski odbor* na Islandu; *Komisija* za zaštitu podataka i *Savet* za zaštitu podataka u Austriji; *Biro* za zaštitu privatnosti u Belgiji; *Komisija* za nadzor podataka u Švedskoj, *Komitet* za zaštitu podataka u Japanu; i sl.). Neke od zemalja predviđaju i postojanje **posebnog suda za zaštitu podataka** (V. Britanija). U svakom slučaju u pitanju su **organi koji bi trebalo da budu nezavisni od državnih, političkih, pojedinačnih uticaja, kao i da budu ekspertni organi sa izuzetno visokim novom stručnosti, pravne i informatičarske**. Njih, po pravilu, imenuju najviši organi zemlje (ukazom Predsednika vlade imenuje ga Kruna u V. Britaniji; predsednik na predlog kancelara u Nemačkoj; Savezno veće u Švajcarskoj; i sl.).

Naša se zemlja uvrstila u onu grupu koja ovo telo nije predvidela, kao što nije usvojila ni poseban zakonski tekst o zaštiti podataka o ličnosti. U Predlogu zakona iz septembra 1995. godine<sup>46</sup> predviđa se da ostvarivanje nadzora vrši Savezno ministarstvo nadležno za pravdu.

Sa manjim ili većim odstupanjima ovi organi imaju **višestruku ulogu: 1)** regulativnu; **2)** savetodavnu, **3)** kontrolnu, **4)** ponekad oni imaju i ovlašćenja vezana za formiranje i upis u registar baza podataka.

Kao osnovno pravo i ovlašćenje pojavljuje se pravo uvida u sva dokumenta vezana za obradu podataka, sve BP, sve podatke i pravo kontrole kako se primenjuje odredba o zaštiti podataka, prava i principa koji iz njih slede. Osim toga, oni mogu da zahtevaju, da se određene baze, ukoliko se utvrdi da se u njima krše prava i principi, brišu iz registra ili da im se zabrani dalje egzistiranje. U drugim slučajevima može da izda nalog za izmenu, dopunu ili blokiranje podataka što predstavlja obavezu subjekta (o čijoj se bazi radi) da po tom nalogu, u određenom roku, i postupi.

U toku rada kontrolor podataka ima **ovlašćenje da donosi određene pravne akte**, kao što su razna uputstva, preporuke i sl. kojima se dopunjuju, za konkretne situacije, propisi o zaštiti podataka. Tako je npr. Nacionalna komisija za informatiku i slobode Francuske donela preko 50 raznih akata kojima se osigurava bezbednost sistema. Osim toga, u većini zemalja predviđeno je posebno ovlašćenje ovog organa da donosi pojedinačne i opšte odluke u posebnim, zakonom predviđenim, slučajevima, kao i opšte naredbe u cilju osiguranja bezbednosti sistema (čl. 20 Zakona Francuske).

<sup>46</sup> Predlog zakona o zaštiti podataka o ličnosti, čl. 19 - 24.

Takodje, može **da predlaže** zakonodavnim i drugim organima donošenje novih propisa, kojima bi se osigurala bezbednost obrade, odnosno korišćenja podataka o ličnosti i pružile odgovarajuće garancije tajnosti i sigurnosti podataka<sup>47</sup>.

**Savetodavna ovlašćenja** ovih organa najčešće se odnose na objašnjenje i pružanje pomoći svim subjektima koji su, na bilo koji način, vezani za podatke o ličnosti (od zakonodavnih, upravnih i sudskih organa do pojedinca koji je subjekt podataka). Na primer, Nacionalna komisija za informatiku i slobode (po Zakonu Francuske) davaocima ICC usluga daje obaveštenja o načinima olakšavanja primene prava pristupa, savetuje ih koje mere bezbednosti treba preduzeti, kako i u kojim rokovima treba podatke ispraviti ili upotpuniti, kako subjekt podataka može svoja prava koristiti i, sl. Ova funkcija, kao i neke druge, nije na adekvatan način kod nas predviđena.

Najznačajnija funkcija i uloga kontrolora podataka je, upravo, **kontrola**: primene zakona o zaštiti podataka; primene principa i korišćenja prava koje imaju pojedinci i stepena ispunjavanja, načina ispunjenja obaveza. Ovaj organ u kontroli primene ima mnogobrojna ovlašćenja - od direktnog pristupa u bazi određenim podacima o ličnosti, do isključenja uređaja ukoliko proceni da je to potrebno (npr. po zakonu Švedske). Isto tako, ovi organi mogu vršiti kontrolu na više načina: u prethodnom postupku ili razmatranjem predstavki o nepravilnostima i teškoćama koje se pojavljuju u vezi zaštite podataka o ličnosti. Pri tom, je neophodno istaći da se ta ovlašćenja odnose na sve BP i na sve subjekte, bilo da su oni državni organi, lokalne zajednice, javne ustanove ili privatna lica i organizacije<sup>48</sup>.

Pored raznih obaveza koje u svom radu imaju organi kontrole, jedna od najznačajnijih i u zakonima najčešće definisanih, je i obaveza da ne primaju uputstva (naredbe, molbe) niti podležu uticajima vlasti, odnosno da su nezavisni i da saznanja, do

<sup>47</sup> Nažalost, ova funkcija nije eksplicitno predložena Predlogom zakona, mada bi ona implicitno mogla proistići iz Ustava SRJ i Zakona o organizaciji i delatnosti saveznih organa uprave i saveznih organizacija.

<sup>48</sup> Po Predlogu zakona izveštavanje je jedna od najdetaljnije razradjenih funkcija, ali samo po broju odredbi u odnosu na druge funkcije. Nadležni savezni organ može da pregleda: sadržaj registra i sadržaj samih zbirki podataka o ličnosti; dokumentaciju koja se odnosi na prikupljanje, obradu, čuvanje, prenošenje i korišćenje ovi podataka; opšte akte rukovaoca zbirke; prostorije i opremu gde su smeštene. On može zabraniti prikupljanje, obradu, korišćenje i prenošenje ovih podataka, naravno, ako utvrdi postojanje određenih situacija (neispunjenje predviđenih uslova), i može da naredi da se: otklone uočene nepravilnosti; brišu cele zbirke ukoliko nije formirana i organizaovana u skladu sa zakonom; izmeni ili zabrani korišćenje ili brisanje ovih podataka, a kojima se krše prava građana. I konačno, ovaj organ može podneti prijavu za učinjeni prekršaj.

kojih su došli uvidom u podatke o ličnosti pojedinaca, čuvaju kao službenu tajnu, čak i onda kad im prestane mandat<sup>49</sup>.

Posebna obaveza ovih organa je **sastavljanje godišnjeg izveštaja koji se dostavlja**, po pravilu, **parlamentu ili drugom sličnom telu**<sup>50</sup>, a u kojem se iznose podaci o stanju u ovoj oblasti i ukazuje na moguća rešenja. Istovremeno, prema odredbama Evropske Konvencije i Evropske Direktive **sva nacionalna tela za kontrolu zemalja članica EZ trebalo bi da međusobno tesno saradjuju** kako bi se pratilo sprovođenje zakona o zaštiti podataka, sudski procesi koji se u vezi sa tim vode i problemi koji se pojavljuju.

### 2.1.2 *Zaštita podataka o ličnosti*

Informaciona privatnost, u stvari, odnosi se na **podatke o ličnosti**<sup>51</sup> (za razliku od privatnost koja je vezana za ličnost i koja, između ostalog, može biti ugrožena podacima o ličnosti, ali ne samo njima). Koji se podaci smatraju podacima o ličnosti, uglavnom se definiše odgovarajućim propisima (nacionalnim i međunarodnim). To su, pre svega, podaci kojima se mogu ugroziti: život, telesni i fizički integritet, čast i ugled, život porodice, identitet i ime, kao i podaci dobijeni povredom prava na tajnost pisama i drugih sredstava komuniciranja i nepovredivosti stana. Zakoni i drugi pravni akti bliže definišu vrstu i sadržaj ovih podataka. Tako, po Zakonima o zaštiti podataka V. Britanije, Džersija i ostrva Mana, pod podacima o ličnosti podrazumevaju se podaci koji se odnose na žive osobe koje se mogu identifikovati pomoću tih podataka, bilo na osnovu pojedinačnih ili na osnovu veze sa drugim podacima koje poseduje korisnik<sup>52</sup>, Švedski zakon definiše podatke o ličnosti kao podatke koji se odnose na neko lice, Zakon Savezne Republike Nemačke o zaštiti podataka, pod podacima o ličnosti podrazumeva podatke o ličnim ili stvarnim odnosima jednog određenog ili odredivog fizičkog lica, Zakon o informatici, evidencijama i slobodama Francuske ove podatke određuje kao sve one podatke na osnovu kojih se u

<sup>49</sup> Evropska Direktiva, glava VI, čl. 28.

<sup>50</sup> Chalton S., Gaskill S., op. cit., str. 1-138.

<sup>51</sup> Termin "**podaci o ličnosti**" mnogo je pogodniji od termina "**lični podaci**", koji se, čak, nalazi i Predlogu zakona, jer se ovim drugim terminom može lako stvoriti zabuna. Naime, lični podaci više odgovaraju isticanju da neki podatak pripada nekome (ličnosti), ali kao predmet svojinskih ili neki drugi odnosa (u smislu lične imovine). Mada se, u prenesenom smislu, ovaj termin može koristiti, ali veoma oprezno, za označavanje podataka koji se odnose na neku ličnost (oni mogu, ali ne moraju, biti njena svojina).

<sup>52</sup> Chalton S., Gaskill S., op. cit., str. 1-065 i 1-066.

bilo kom obliku - neposredno ili posredno, može identifikovati neko fizičko lice na koje se ti podaci odnose, i sl.<sup>53</sup>

Drugim rečima, prihvatajući data određenja u skoro svim nacionalnim zakonima, **podaci o ličnosti su svi oni podaci koji se odnose na neko određeno i odredivo fizičko lice, koje na osnovu njih može biti identifikovano.** Mada postoje posebni razlozi da se pri definisanju ovih podataka obuhvate samo podaci o živim fizičkim licima, ipak se integritet, čast, ugled i sl. mogu povrediti i onda kad je pojedinac, na koga se takvi podaci odnose, umro ili proglašen umrlim, tim više što se takvim podacima mogu naneti velike štete i što se ne pruža objektivna mogućnost da on takve podatke, ukoliko su netačni, ispravi, traži njihovo brisanje ili koristi druga prava koja bi mu lično, inače, pripadala. Neke mogućnosti postoje, ukoliko postoje relevantni dokazi, ali to je veoma problematično i još uvek pravno neraščišćeno, naročito, ako se ima u vidu da se radi o ličnom pravu pojedinca.

Pri određivanju **vrsta podataka** koji se mogu smatrati podacima o ličnosti, po pravilu koje se može prihvatiti, oni se specifikuju kao:

1. **podaci o činjenicama** (ime, adresa, godine, primanja i plata, religija, etnička pripadnost, rasa, broj i godine dece i drugih lica pod starateljstvom, članstvo u sindikatu, političke aktivnosti, ispitnim ocenama, rezultatima IQ testa, seksualnom životu, zdravstvenom stanju, osudjivanosti i svi drugi koji mogu predstavljati potencijalne podatke o ličnosti);
2. **podaci o mišljenjima i sudovima samog pojedinaca** (npr. o željama za napredovanje, braku, i sl.) **i drugih subjekata o njemu** (o kreditnoj sposobnosti, sposobnosti za neke poslove, mogućnostima za profesionalno napredovanje, i sl. koji, takodje, predstavljaju potencijalne podatke o ličnosti), i
3. **podaci o namerama** (uključujući i namere korisnika u vezi sa subjektom na koga se podaci odnose, kao što je, npr., mišljanje "X je sposoban da izvrši naše zahteve").

Slično je i kod nas. U Predlogu zakona o zaštiti podataka o ličnosti podrazumevajuse: "**informacije koje su sadržane u zbirkama tih podataka, a koji se**

<sup>53</sup> Lilić S. i grupa autora, Zaštita podataka u kompjuterizovanim informacionim sistemima, uporedno-pravna analiza, Beograd, Institut za uporedno pravo, 1987., str. 67 i 81.

**odnose na privatnost i integritet ličnosti, lični i porodični život, i druga lična prava, koja su u vezi sa identifikovanim licem ili licem koje se može identifikovati**"<sup>54</sup>.

Svakako da je jedno od najnovijih odredjenja dato u članu 2, tč. (a), **Direktive Evropskog Parlamenta i Saveta o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i slobodnom kretanju takvih podataka**<sup>55</sup> i po kojoj su to "sve informacije u vezi sa identifikovanim fizičkim licem ili onim koje može biti identifikovano (subjekt podataka - *data subject*), direktno ili indirektno, na osnovu posebnog identifikacionog broja ili na osnovu drugih činjenica koje su vezane za njegov fizički, psihički, mentalni, ekonomski, kulturni ili socijalni identitet".

Mnogi međunarodni i nacionalni instrumenti zaštitu podataka o ličnosti i informacione privatnosti predvideli su kroz **postojanje odredjenih principa, kao pravno formalizovanih etičkih kodova, sugerišući odredjen način ponašanja korisnika i davanja informacionih usluga**. Ovim principima bi se stvorila zajednička polazna osnova na kojoj bi se bazirala zaštita<sup>56</sup>. Oni bi trebalo da obezbede veću propulzivnu moć razvoja odredjenog načina ponašanja i obeshrabre one čije ponašanje odstupa od dozvoljenog. Pri tome, mora se voditi računa da se ovi principi, u suštini, pojavljuju kao uputstva za rad odredjenih subjekata. Primenom ovih principa pokušalo bi se njihovo ugradjivanje i u individualni kod svakog pojedinca koji sa podacima o ličnosti dolazi u dodir. U početku, ovi etički kodovi se nisu nalazili u pravu, ali dužom primenom i proverom u praksi, postaju standardi ponašanja.

**Osam principa zaštite podataka o ličnosti, opšte prihvaćenih, potiču iz Evropske konvencije**, a u nju su ugradjeni direktno iz Younger-og izveštaja. Kako ističu mnogi autori<sup>57</sup>, sedam principa vezano je za ponašanje korisnika, dok je osmi, neposredno vezan za sigurnost podataka, i odnose se i na korisnika i pružaoca usluga. U suštini, davalac usluga primenjivaće i prvih sedam principa ukoliko se istovremeno pojavljuje u ulozi "družaoca" podataka. U praksi se često dešava da se neke od aplikacija istovremeno rade i kod korisnika i kod davanja usluga, naročito onda kad mu primarni posao nije obrada podataka. Veoma je teško međusobno diferencirati primenljivost svih

<sup>54</sup> Predlog zakona o zaštiti podataka o ličnosti, čl. 2., st. 1., tč. 2.

<sup>55</sup> Ova je Direktiva doneta 25 oktobra 1995. godine i objavljena kao Direktiva br. 95/46/EC, Official Journal of the European Communities, no. 285/95.

<sup>56</sup> Zanimljivo je da Predlog zakona nije posebno predvideo ove principe, čime je izostavljena mogućnost boljeg tretmana ovih podataka, kao i ponašanja subjekata u odnosu na njih i zaštitu.

<sup>57</sup> Edwards C., Savage N., Walden I., op. cit., str. 72; Chalton S., Gaskill S., op. cit., str. 1-037., i drugi

ovih principa u odnosu na subjekte, a razlika medju njima više je akademska nego stvarna<sup>58</sup>.

Ovih osam principa bili su polazište za novu Evropsku Direktivu koja se opredelila samo za pet principa, specifikujući ih kao principe vezane za kvalitet podataka<sup>59</sup>.

Medjutim, više je nego sigurno da postojanje principa zaštite podataka o ličnosti ima za cilj, pored standarizovanja određenih operacija i radnji korisnika i davaoca ICC usluga, pružanje određene sigurnosti subjektima podataka, kao i obezbeđenje poštovanja njegovih prava na informacionu privatnost. Otuda postoji tesna povezanost izmedju principa i prava da se čini da je u pitanju jedno te isto. To je samo privid, pošto principi u suštini treba da budu u funkciji prava pojedinaca i da uskladjuju njihove interese sa interesima društva i korisnika. Ti principi su<sup>60</sup>:

***a) Podaci o ličnosti moraju se obradivati i dostavljati na "pošten" i zakonit način***

Koncept poštenog i zakonitog dostavljanja i obradjivanja podataka o ličnosti obuhvata metode koje bi trebalo da primenjuje bilo koji subjekt koji dolazi u dodir sa ovim podacima, nasuprot pojedinih metoda koje se često koriste i koje predstavljaju određene prevare i obmane u odnosu na svrhu zbog koje se podaci čuvaju, koriste ili obelodanjuju. Ovi zahtevi odnose se i na podatke koje dostavljaju subjekti podataka i na treća lica koja daju podatke o subjektu podataka. Pod prevarama i obmanama podrazumeva se mnogo toga: od otkrivanja identiteta osobe na koju se informacija odnosi, na osnovu pojedinačnih činjenica karakterističnih samo za nju, do dobijanja podataka za evidenciju koja ne postoji, ili stvaranje utisaka o nužnosti predavanja podatke o činjenicama koje, inače, ne bi bile evidentirane.

Za razumevanje ovog principa neophodno je napraviti razliku izmedju poštenog i zakonitog postupanja, s jedne, i dostavljanja i obrade podataka o ličnosti, s druge strane.

**"Pošteno" dostavljanje** podrazumeva, da su podaci o ličnosti autorizovani od strane osoba na koje se odnose, i da su na odgovarajući način od njih

<sup>58</sup> To ističu Chalton S., Gaskill S., op. cit., str. 1-037.

<sup>59</sup> Evropska Direktiva, glava II, odeljak I, čl. 6.

<sup>60</sup> Evropska Direktiva, glava II, odeljak I, čl. 6.

*potvrđeni*. Autorizacija se mora odnositi na pravni osnov po kome je na takav način dostavljanje podataka dozvoljeno, odn. da je predviđen u nekom nacionalnom zakonu ili odgovarajućem ratifikovanom međunarodnom aktu. To znači, da se **nepošteno dostavljanje** najčešće odnosi na (npr. po Uputstvu za primenu Zakona o zaštiti podataka V. Britanije) na sledeće situacije:

1. kad se u ime tobožnje svrhe prikupljanja ili korišćenja podataka od strane korisnika određena postavljaju pitanja ili daju određena objašnjenja koja, u stvari, nisu u skladu sa predviđenom svrhom;
2. kad se od pojedinca očekuje razumevanje, bez ikakvog objašnjenja, svrhe zbog koje se informacija koristi ili obelodanjuje;
3. kad se kod pojedinca stvara utisak da će informacija sastavljena od podataka o njegovoj ličnosti biti tretirana kao tajna, poverljiva;
4. kad se informacija dobija presijom ili navodjenjem na predavanje;
5. kad se pojedinac navede da misli da je obavezan da podatke o sebi daje.

Drugim rečima, primenom ovog principa trebalo bi da se favorizuje pojedinac, koji bi bio tačno i istinito obavešten: zašto se određeni podaci o njemu zahtevaju, u koje svrhe će se koristiti i obelodanjivati i daje preporuka u kojoj će se formi ovi podaci nalaziti i štampati. Znači, obezbeđuje mu se korišćenje prava na obaveštenost i pravo na korišćenje podataka, na odgovarajući način. Takodje, on treba da skrene pažnju odgovarajućeg tela (Registratora u V. Britaniji, Nacionalne komisija za informatiku i slobode u Francuskoj, i sl.) koje je nadležno za registraciju ovih podataka, odn. BP, na proveru da li su "ulazi" u skladu sa predviđenim svrhama.

Ovaj princip ne odnosi se na podatke i informacije koje su istorijskog, statističkog ili istraživačkog karaktera, kao ni na podatke koji bi štetili prevenciji ili otkrivanju kriminala, hvatanju ili hapšenju krivaca, razrezivanju i naplaćivanju poreza ili drugih dažbina<sup>61</sup>. Na primer, Zakon o zaštiti podataka V. Britanije kao podatke o ličnosti izuzete od primene ovog zakona predviđa podatke značajne za: državnu bezbednost, krivične i poreske stvari, zdravstveno i socijalno osiguranje, finansijske usluge, sudski imunitet i pravo tajnosti zastupnika, platne spiskove i račune, porodične i druge stvari, ispitne ocene i sl. Čini se da kod nas izuzimanje primene principa poštenog i zakonitog obradjivanja i dostavljanja podataka o ličnosti ne bi bilo u potpunosti celishodno, naročito kad se radi o statističkim i istraživačkim podacima, kao i podacima vezanim za razrezivanje i naplaćivanje poreza i dažbina, jer je način prikupljanja i

<sup>61</sup> Chalton S., Gaskill S., op. cit., str. 1-039.

dostavljanja ovakvih podataka predviđen zakonom i drugim pravnim aktima, pa bi njihovo izuzeće iz primene ovog principa predstavljalo, neku vrstu, zloupotrebe<sup>62</sup>.

Kad je u pitanju obrada podataka (pod njom se obično podrazumeva dopunjavanje, izmena, brisanje, rearanžiranje podataka ili izvođenje informacija iz postojećih podataka)<sup>63</sup> **"pošteno" postupanje znači da su u pitanju one operacije obrade na osnovu kojih se dobijaju istiniti i ažurni podaci o ličnosti**, odn. informacije bez iskorišćavanja prednosti koju mogu da imaju korisnici u odnosu na subjekt podataka. Naime, mogućnosti koje pruža automatska obrada podataka (AOP) daju izuzetnu moć korisnicima da raznim kombinacijama, postojećih podataka, dobijaju raznorazne informacije koje, inače, nisu bile moguće kad je obrada bila tradicionalna, ručna. Koristeći ovu svoju moć oni mogu da zbune subjekt podataka tako da ne iskoristi ovaj princip kad otkrije da su podaci o njemu "nepošteno" obrađeni.

Nezakonito obrađivanje i dostavljanje veoma se često podudara sa nepoštenim obrađivanjem i dostavljanjem, mada to uvek ne mora da bude tako. U suštini, **nezakonito dostavljanje predstavlja svako ugrožavanje poverenja onoga na koga se podatak odnosi ili ga poseduje, ili prestup, kao i kradja i prevara da bi do dostavljanja nekog podatka o ličnosti ili informacije došlo.**

Nezakonita obrada je vezana za nezakonite radnje i operacije nad podacima o ličnosti<sup>64</sup>. Vrlo često se ona vezuje za kriterijume selekcije podatka, npr. na osnovu tajnog uvođenja podatka o rasnoj ili nacionalnoj pripadnosti vrši se odabir potencijalnih kandidata koji će se zaposliti, iako se u većini zemalja diskriminacija ne priznaje i zabranjuje. U takvoj situaciji moći će se primeniti princip zakonitog i "poštenog" obrađivanja podataka pozivajući se na odgovarajući zakon ili međunarodni akt.

***b) Raspolaganje podacima o ličnosti mora da bude u skladu sa unapred odredjenom i pravno definisanom svrhom***

Raspolaganje podacima o ličnosti biće moguće samo ukoliko je ono u skladu sa unapred odredjenim svrhama (jednom ili više) i to ne bilo kako odredjenim, već koje su tačno i eksplicitno odredjene u odgovarajućim nacionalnim, pravnim instrumentima.

<sup>62</sup> Predlog zakona je kao izuzetak, odn. ograničenje prava koja ima građanin, odredio u vezi sa kaznenim evidencijama i evidencijama u oblasti bezbednosti SRJ (čl. 13).

<sup>63</sup> Predlog zakona pod obradom podrazumeva "skup ručnih, poluautomatizovanih ili automatizovanih aktivnosti radi prikupljanja, memorisanja, pregrupisavanja, izmene, razmene, prenosa, pretraživanja, širenja, zabrane korišćenja i brisanja podataka" (čl. 3. tč. 5).

<sup>64</sup> Chalton S., Gaskill S., op. cit., str. 1-040.

**Raspologanje sa podacima obuhvata niz operacija kojima se primenjuje složeni koncept baziran na kontroli sadržaja i posedovanju podataka.** Naime, podaci o ličnosti moraju se sadržajem uskladiti sa, pravnim aktom, dozvoljenom svrhom, što znači da je pri raspolaganju neophodno kontrolisati da li je sadržaj podataka ili informacija koje podatke o ličnosti sadrže, u skladu sa predviđenim svrhama. Kad se utvrdi uskladenost sadržaja sa svrhom mora se, takodje, utvrditi, istovremeno ili posebno, i da li njihovi korisnici postupaju u skladu sa njom, odn. da li su njihova ovlašćenja i autorizacije uskladeni sa svrhom zbog koje određeni podaci o ličnosti i postoje. Neispunjenjem ovog principa pojaviće se **problemi** ukoliko:

- svaka svrha zbog koje postoje neki podaci o ličnosti nije bazirana na zakonu ili drugom pravnom aktu, odn. nije zakonita;
- svaka svrha nije opisana u korisničkom ovlašćenju (obrazloženju ili preambuli ovlašćenja).

Mada je, ponekad, veoma teško dokazati nepostojanje zakonitosti, uvek se mora proveriti, kod svakog podatka, da li je svrha zakonita (da li je u skladu sa bilo kojim zakonom ili nekim drugim pravnim aktom) i da li, kojim slučajem, ona ne nedostaje ili je promenjena. Na primer, svrha prikupljanja i obrade nekih podataka o ličnosti, predviđena zakonom, isključivo služi sprečavanju dela nelojalne utakmice. Međutim, BP upravo sadrži podatke koji to omogućuju i ovlašćenja korisnika da baš do tih podataka dodje i koristi ih. U takvim slučajevima ovakvi podaci nemaju vrednost (mada je često obrnuto) i trebalo bi ih brisati, a korisniku preformulisati ovlašćenje. Slično je i kada se radi o definisanoj dužini memorisanja i korišćenja negativnih podataka o pojedincu (krivične sankcije, disciplinske mere i sl.) koji se, posle izvesnog protoka, zakonom predviđenog perioda, ne smeju koristiti kao relevantni. Pri registrovanju baze, ako se utvrdi postojanje ovakvih podataka, nadležno telo za registraciju mora na to da upozori davaoca ICC usluga i posle izvesnog vremena da zahtevaa brisanje ili ograničavanje njihovog posedovanja, ukoliko ih on, sam nije izbrisao ili preformulisao.

Ukoliko se, pak, neki podaci o ličnosti nadju u BP, a svrha im nije unapred utvrdjena odgovarajućim pravnim aktom, da bi se izbegle situacije koja bi zahtevala njihovo brisanje, može se zatražiti od nadležnog tela ili zakonodavnog organa, da se svrha naknadno utvrdi. Odbijanje naknadnog utvrdjivanja svrhe ili nepodnošenje zahteva, upravo će dovesti do primene ovog principa.

Naročito aktuelna primena ovog principa biće za one zemlje u kojima se, na osnovu posebnog zakona, predviđa postojanje registra svih BP (javnih i privatnih) i obaveza nadležnog tela da prilikom njihove registracije proverava postojanje svrhe i

uskладjenost sadržaja sa njom<sup>65</sup>. U slučaju da nadležno telo utvrdi nepravilnost i neuskладjenost sadržaja sa svrhama može, po posebnoj proceduri, da traži primenu ovog principa, što izaziva raznorazne posledice za korisnika i davaoca usluga. Takođe, ukoliko se traži promena svrhe i ovlašćenja korisnika, pa zahtev ne bude usvojen, nadležno telo to mora da notira i kontrolie, odn. ako dodje do promene (proširivanja, sužavanja postojeće ili utvrđivanja nove) ona se po unapred predviđenoj proceduri unosi u registar i izveštaj koji se dostavlja nadležnom organu (u V. Britaniji je to Parlament i Državni sekretar, a po potrebi može se i aktivirati posebni Arbitražni sud za zaštitu podataka).

To, istovremeno, pretpostavlja da se prilikom registracije tačno i eksplicitno navode pravni izvori i sadržaj svrhe, kako bi se mogla da sprovede kontrola. Osim toga, u godišnjem izveštaju, koji priprema registrator BP<sup>66</sup>, navode se i podaci o promenama i utvrđenim nesuglasicama, kao i sankcijama i merama koje su preduzete da bi se stanje ispravilo, odn. za koju bazu i zbog čega je primenjen princip vrednovanja podataka u odnosu na tačno i pravovaljano utvrđene svrhe.

*c) Podaci o ličnosti smeju se koristiti ili obelodaniti samo kompatibilno predviđenoj svrsi*

Podaci o ličnosti trebalo bi da se koriste, ali i obelodanjuju, u skladu sa svrhom koja je predviđena i definisana odgovarajućim pravnim aktom. Ako se ne postigne kompatibilnost podataka sa predviđenom svrhom dolazi do kršenja ovog principa.

Medjutim, kako se veoma često postavlja problem inkompatibilnosti korišćenja i obelodanjivanja podataka o ličnosti u odnosu na utvrđene svrhe to se postavlja pitanje šta ona znači? **Inkompatibilnost predstavlja nasilno korišćenje ili otkrivanje podataka o ličnosti u odnosu na, u odgovarajućem pravnom aktu, opisane svrhe.**

Primenom ovog principa pokušavaju se premostiti opasnosti koje prete podacima o ličnosti. **Prva opasnost nastaje u odnosu na nedovoljno jasno razgraničenje**, zakonom propisane, interpretacije ovog elementa u odnosu na drugi

<sup>65</sup> Kod nas je predviđen katalog zbirke kao pregled zbirke "ličnih podataka" koju vodi rukovalac zbirkom ovih podataka (Predlog zakona, čl. 3., tč. 4, 6; čl. 4).

<sup>66</sup> Predlogom zakona nije predviđena obaveza Saveznog ministarstva nadležnog za pravdu da priprema ikakav, pa ni godišnji, izveštaj o stanju i problemima vezanim sa ove BP.

princip koji ograničava posedovanje i raspolaganje podacima o ličnosti za nepropisane (u nekim zemljama i neregistrovane) svrhe<sup>67</sup>. Naime, termin korišćenje predstavlja esencijalnu komponentu posedovanja, pa se pri kontroli korišćenja, u osnovi kontroliše primena trećeg principa, dok kontrola posedovanja pretpostavlja i mogućnost raspolaganja, pa se tako obuhvata drugi princip. Nedovoljno razgraničenje može da izazove zbrku, koji će se princip primeniti, što će imati značajne posledice ukoliko se utvrde nesuglasice ili nepravilnosti.

***Druga opasnost*** vezana je za **zakonsku interpretaciju razlike između nenamernog ili namernog obelodanjivanja** podataka o ličnosti za koje se primenjuje ovaj princip i nagoveštava (moguće opasnosti), koje su vezane za primenu osmog principa baziranog na sigurnosti podataka.

Vodeći računa o mogućnosti primene ovog principa, zemlje koje su ga ugradile u svoje zakonodavstvo predvidele su da se prilikom registracije BP uvek mora navesti i za koje se svrhe ona koristi i, mada nešto manje restriktivno, u kojim slučajevima se podaci o ličnosti mogu obelodaniti trećim licima, vodeći pri tome računa o izuzecima koje zakon predviđa. Tako, Zakon o zaštiti podataka V. Britanije naglašava u tački 4. Uputstva za registrovanje podataka, značaj osiguranja koje se u potpunosti predviđa prilikom registracije BP, za sva korišćenja podataka o ličnosti na koje korisnik ima pravo. Obelodanjivanje ovih podataka nije tako strogo restriktivno jer ukoliko se pojavi potreba za obelodanjivanjem nekih podataka o ličnosti, koji nisu za to bili predviđeni, to se može, bez velikih problema, naknadno uraditi, ukoliko se slaže sa predviđenim svrhama. Naime, ne štiti se korisnik ako on želi, da određene informacije sastavljene od podataka o ličnosti otkrije, ukoliko je otkrivanje opisano pri registraciji ili je u skladu sa zakonom predviđenim slučajevima. Primer kršenja ovog principa<sup>68</sup> je kada neka organizacija prikuplja podatke o svojim kupcima kako bi im tobože priznala popuste, zatim proda te informacije trećoj strani.

***d) Podaci o ličnosti moraju da budu adekvatni, relevantni i, u dovoljnom broju, u odnosu na svrhu kojoj treba da služe***

Mada na prvi pogled najjednostavniji i najjasniji, ovaj princip može često da izazove nedoumicu ili problem, pogotovo, što se njegova primena, po pravilu, vezuje za organizacije i njihovu sopstvenu informacionu politiku. Nedoumice naročito nastaju oko tumačenja nijansi na osnovu kojih je moguće praviti razliku između adekvatnih i neadekvatnih, relevantnih i irelevantnih, dovoljnih i neumerenih podataka. Osobito, što

<sup>67</sup> Chalton S., Gaskill S., op. cit., str. 1-041.

<sup>68</sup> Edwards C., Savage N., Walden I., op. cit., str. 73.

se u određenim okolnostima neki podaci adekvatni, relevantni i u dovoljnom broju, da bi u slučaju njihove promene ti isti podaci bili neadekvatni, irelevantni i neumereni. Zbog ovih specifičnosti mnogi zakoni su ostavili su **organizacijama, na osnovu sopstvenog pogleda na ovu pojavu, utvrde meru na osnovu koje će moći, primenjujući ovaj princip u kontekstu sopstvene obrade podataka, odrediti takvu politiku posjedovanja podataka da ona bude u skladu sa neophodnim minimumom za svaku pojedinu utvrdjenu svrhu.**

Kod kršenja ovog principa, najčešće se ističe da je poseban problem prepoznavanje i dokazivanje usled subjektivizma i teškoća razlučivanja, npr. neadekvatnih i neažurnih podataka, a što se, svakako, različito reflektuje u odnosu na BP. Neadekvatne podatke treba brisati, dok netačne i neažurne treba menjati i ažurirati. Kao primer, za kršenje ovog principa mogu se navesti podaci o detaljima vezanim za karakteristike ličnosti pojedinaca prijavljenih, ali neprimljenih, na rad.

Primena ovog principa može biti bitna za one BP, ili njene delove, koji se vode za posebne namene (policijske i sl.) ili se, autoritetom određenog subjekta, isključuje stvarna kontrola, ili je ona veoma otežana i prepuštena subjektivnoj proceni.

***e) Podaci o ličnosti moraju biti tačni i ažurni***

Kolikogod postojale nepreciznosti oko adekvatnosti, relevantnosti i broja potrebnih podataka, kad je u pitanju četvrti princip, toliko je u petom došla do izražaja preciznost nacionalnih zakona u definisanju sadržaja termina tačnost i ažurnost<sup>69</sup>. Jedan od razloga za definisanje ovih termina je predviđanje i postojanje prava pojedinca na ispravku, kad se utvrdi da su podaci o njemu netačni i/ili neažurni, a što povlači obaveznu odštetu, kao i druge posledice. Drugi je, svakako, vezan za specifičnost ovih podataka - njihovu veliku promenljivost. Otuda ovaj princip treba da provejava kroz svaku operaciju i procese vezane za podatke o ličnosti.

**Tačnost podataka**, u većini zakona, *odnosi se na činjenice, nikako ne na utiske i mišljenja*, mada bi i o njima trebalo voditi računa, naročito onda kad se na osnovu takvih podataka može sprečiti ili ograničiti korišćenje nekog prava pojedinca. Ne treba zanemariti činjenicu da se mišljenje nekog subjekta o pojedincu može namerno ili slučajno iskriviti, a da to, može da predstavlja osnov za uskraćenje nekog njegovog prava. Na primer, mišljenje socijalnog radnika o podobnosti razvedenih roditelja za starateljstvo, koje preformulisano u bazi može da predstavlja osnov za gubitak

<sup>69</sup> Ovaj princip predviđen je i Predlogom zakona, čl. 16., st. 1.

starateljstva podobnog roditelja u korist nepodobnog. **Podaci su netačni ukoliko su nekorektni ili dovode u zabludu bilo koji deo činjenice vezane za pojedinca.** To će se desiti<sup>70</sup> kad korisnik dobije podatke od kojih se formira informacija:

1. za koje subjekt podataka ili treća strana tvrde da su tačni, a to nije slučaj;
2. u koju treba da su uključeni određeni podaci, a to se ne učini; ili
3. ukoliko subjekt podataka. zna i ne obavesti korisnika da su podaci o njemu nekorektni ili da ga mogu dovesti u zabludu

Netačnost podataka vezana je za nameru da se prikažu neke činjenice onakvim kakve, u stvari, nisu ili to nastane kao posledica neke propuštene radnje (forme ili obaveštavanja) ili slučajno. U svim tim slučajevima primeniće se ovaj princip.

Kako se često, u mnogim zemljama, korišćenje netačnih podataka direktno vezuje za odštete koje će korisnik morati da plaća, ukoliko se dokaže da nije dovoljno vodio računa o osiguranju tačnosti, zato se od njega zahteva da preduzima odgovarajuće mere osiguranja. Međutim, oceniti: da li je korisnik blagovremeno preduzeo odgovarajuće mere osiguranja tačnosti, veoma je teško utrditi i dokazati tako da se za svaki konkretan slučaj to mora ispitati. Zato, nadležni organ (u V. Britaniji, Džersiju, ostrva Man - registrar) izdaje nalog za ispitivanje svih činjenica relevantnih za ocenu da li je korisnik preduzeo sve potrebne korake. Po zakonu V. Britanije, a što bi bilo oportuno i za nas, te činjenice koje se ispituju su:

- da li je korisnik shvatio značaj netačnosti podataka o ličnosti i kakve su mu bile namere, odn. ako je izazvao ili je želeo da izazove štetu ili neprijatnost za subjekta podataka, da li je toga bio svestan?
- da li je izvor informacija koji je korisnik koristio pouzdan?
- da li je preduzeo odgovarajuće korake za verifikaciju informacija proveravajući ih i kod subjekta podataka?
- da li je poštovao sve procedure i pokušao da izbegne unošenje netačnosti?
- da li je primenio sve procedure za otkrivanje i korigovanje netačnosti?

Utvrđivanjem postojanja neke od ovih činjenica (bio je svestan, nije proverio pouzdanost izvora, nije preduzeo korake za verifikaciju, nije poštovao procedure ili ih je izbegavao i sl.) dovodi do primene ovog principa, a korisnik povlači odgovarajuće konsekvence.

---

<sup>70</sup> Chalton S., Gaskill S., op. cit., str. 1-042.

**Ažuriranje podataka preduzima kada je to potrebno, a u skladu sa njihovom svrhom i prirodom.** Tako, ako je (npr. po zakonu V. Britanije) svrha postojanja čuvanje istorijskih podataka, ažuriranje će biti neprikladno, ali ako podaci odražavaju aktuelne okolnosti vezane za subjekt podataka, oni se moraju ažurirati. Iako se čini, da je ispunjenje ovakvih zahteva sasvim logično, to je samo privid jer i "istorijski" podaci mogu biti značajni za pojedinca i korišćenje nekih njegovih prava. Naravno, mora se voditi računa da li se vođenje i korišćenje takvih podataka ne kosi sa nekim drugim pravnim osnovom, jer će se, u tom slučaju, steći uslovi za primenu prvog principa. Zbog toga je potrebno procenjivati, za svaki pojedini slučaj, neophodnost ažuriranja podataka o ličnosti i u skladu s tim, to i raditi.

*f) Podaci o ličnosti ne smeju se držati duže nego što je potrebno*

**"Vek" držanja i korišćenja podataka o ličnosti odredjen je svrhom zbog koje se prikupljaju i memorišu.** Međutim, davaoci ICC usluga i korisnici podataka skloni su da zapamćene podatke dugo čuvaju "zlu ne trebalo" i koriste. To ima smisla samo ako je utvrđena svrha takva, da je neophodno njihovo dugotrajno postojanje, kao što je to slučaj sa istorijskim, statističkim ili istraživačkim podacima, čiji je smisao praćenje neke pojave, kroz duži vremenski period. Ipak, postoji veliki broj podataka čije dugotrajno čuvanje i korišćenje, ne samo što nije celishodno, već može da bude i protivzakonito. Na primer, takav je slučaj npr. sa uslovnim osudama, za koje je predviđeno da se iz kaznene evidencije brišu posle jedne godine od vremena proveravanja, ako u to vreme osuđeni ne učini novo krivično delo; ili, novčane kazne koje se brišu po isteku od tri godine od dana izvršene, zastarele ili oproštene kazne, ukoliko za to vreme osuđeni ne učini novo krivično delo. Isti je slučaj i sa odlukama disciplinske komisije pred kojom je okončan disciplinski postupak. Donošenjem određene odluke koja se, po aktima te organizacije, unosi u odgovarajuću kadrovsku evidenciju, ali se posle proteka određenog vremena mora iz nje brisati. Situacija je slična i kad su u pitanju podaci koji ispunjavaju više svrha, a svaka od njih ima posebno utvrđene rokove. Tada će se uzeti najduži predviđeni period i njegovim istekom moraće se podaci brisati. Nešto je složenija situacija kad su u pitanju kompleksni podaci čiji se jedan deo koristi isključivo za jednu određenu svrhu za kraći period, a drugi delovi za više svrha i duže periode. Tada korisnik mora identifikovati razlike i poštovati ih. Protokom ovih termina, ukoliko se podaci iz BP ne izbrišu, steći će se uslovi za primenu principa da se podaci o ličnosti ne smeju držati duže nego što je potrebno.

Da bi se izbegla primena ovog principa i posledice koje zbog toga nastaju **neophodno je da korisnici povremeno prave reviziju svrhe i dužine korišćenja podataka i da brišu sve ne potrebne podatke.** Mnogi zakoni preporučuju primenu standarda "života" pojedinih kategorija podataka kako bi se korisnici mogli rukovoditi

njima, kao što se preciziraju i procedure, koje se koriste za reviziju i brisanje podataka i informacija čiji je rok istekao. Prateći Uputstvo za registratore V. Britanije (deo četvrti, paragraf 6.), a koje ne bi bilo štetno ni za nas, mogu se navesti sledeći pravila:

1. podaci koji služe za jednokratnu upotrebu brisaće se u danu ili mesecu kad im ističe rok;
2. podaci za koje korisnici imaju neki opravdan razlog da postoje duže, a propisima nije striktno određen rok, brisaće se prestankom tih razloga;
3. istorijski, statistički ili istraživački podaci za koje se utvrdi (od strane nadležnog organa i tela) da ugrožavaju pojedinca na koga se odnose, neće se koristiti da mu se ne bi nanela šteta ili bol.

Ukoliko se ne poštuju ova pravila pojedinac, na koga se podaci odnose, može da zahteva odštetu od korisnika ili davaoca ICC usluga, kao što i korisnik podataka može zahtevati od davaoca ICC usluga odštetu zbog neopravdanog i nedozvoljenog brisanja ili gubljenja potrebnih podataka. Često subjekt podataka i nadležni organ kontrole mogu da zahtevaju od korisnika da im dokaže da je određene podatke uništio po proceduri u skladu sa zakonom<sup>71</sup>. Ako korisnik ne uradi nastaću posledice koje prate primenu ovog principa.

***g) Subjekt podataka mora biti upoznat o vodjenju podataka o njegovoj ličnosti i mogućnostima pristupa***

Da bi se mogli korektno primenjivati prethodni principi i koristiti prava koje ima subjekt podataka, kao osiguranje, uveden je i ovaj princip, koji, doduše, više podseća na prava nego na princip. Ali to nije slučajno, niti je rezultat neke greške ili zabune, već predstavlja pretpostavku osiguranja postojećeg prava na informacionu privatnost. Da bi se mogao primeniti ovaj princip, svakom pojedincu<sup>72</sup> se mora obezbediti da:

1. bude informisan, u razumnim intervalima (bez nepotrebnih odlaganja i troškova), od svakog korisnika o postojanju podataka o njegovoj ličnosti i, da svakom takvom podatku ima pravo pristupa;
2. se takvi podaci isprave, blokiraju ili izbrišu kad je to potrebno.

Termin "**razumni interval**" pretpostavlja da *korisnik podataka ima obavezu da pojedinca obavesti o postojanju podataka, kao i pravu pristupa njima, u intervalu koji je ocenjen kao razuman, zavisno od njihove prirode, svrhe za koje se*

<sup>71</sup> Chalton S., Gaskill S., op. cit., str. 1-044.

<sup>72</sup> Lloyd I., Informarion Technology Law, London, Batterworth, 1993., str. 241.

***koriste i frekvencije prepravke.*** Prepravka ili brisanje, predstavlja izvesnu meru sigurnosti za pojedinca koja se prepliće sa primenom ostalih principa. U stvari, prepravka ili brisanje podataka pojaviće se kao posledica izazvana situacijama, kada se podaci ne koriste u skladu sa zakonitim i unapred predviđenim svrhama, kada im je u pitanju vrednost, ili kada se čuvaju duže nego što je to potrebno i sl. i to onda, ukoliko se i, pored primene odgovarajućeg principa i naredjenja odgovarajućeg subjekta (regitrara, npr.), ne otklone nepravilnosti. Tada se pojavljuje i subjekt podataka, koji, nakon utvrđivanja nastavljanja takve prakse, može zahtevati primenu ovog principa.

Ovoj princip, naravno, obezbeđuje i svojevrsnu kontrolu samog subjekta podataka, jer se može vršiti paralelno ili posebno od primene ostalih principa i kontrole koju obavlja nadležni organ ili institucija prilikom registracije i/ili godišnje provere regularnosti prijavljenih i registrovanih BP. Doduše, ova kontrola je najsubjektivnija, ali to ne mora biti njena mana nego prednost. Ko je više od samog subjekta zainteresovan za korišćenje ovog prava, pa, otuda, ko će bolje vršiti kontrolu nad njima? Ovde prisutan subjektivizam predstavlja okosnicu primene drugih principa.

***h) Mere sigurnosti preduzimaju se protiv neautorizovanog pristupa, menjanja, otkrivanja i uništenja podataka o ličnosti***

Mnogi osetljivi podaci o pojedincima mogu se naći pod određenim okolnostima u BP i poštujući ovaj princip svi subjekti (korisnici i davaoci usluga) moraju voditi računa o posledicama koje mogu nastati<sup>73</sup> ako se ne preduzmu odgovarajuće mere za sprečavanje:

1. neautorizovanog pristupa takvim podacima;
2. neautorizovanog menjanja ili brisanja takvih podataka;
3. neautorizovanog otkrivanja, odn. obelodanjivanja; i
4. slučajnog gubljenja ili uništenja.

Mere koje treba da preduzmu odgovarajući subjekti najčešće se odnose na korišćenje određene opreme i odgovornost zaposlenih koji mogu doći u dodir sa ovakvim podacima. Ove mere sigurnosti podataka o ličnosti treba da se ugrade u sistem obezbeđenja kako bi se kontinuirano i ozbiljno zaštitili osetljivi podaci od raznih povreda koje mogu nastati slučajno ili namerno. S obzirom na vrstu podataka i karakteristika okruženja u kom se odvijaju informacioni procesi primeniće se različiti, unapred predviđeni i definisani, standardi. Tako je, npr. po Zakonu o sigurnost kompjutera SAD iz 1987. godine, Nacionalni biro za standarde odgovoran za razvoj

<sup>73</sup> Edwards C., Savage N., Walden I., op. cit., str. 74.

tehničkih, menadžment i administrativnih standarda za efikasnost obezbedjenja sigurnosti i privatnosti kako bi se olakšala kontrola gubljenja i neautorizovanog menjanja podataka ili njihovog obelodanjivanja, kao i sprečavanje kradja i zloupotreba vezanih za kompjuter<sup>74</sup>. Obaveza je svakog subjekta koji dolazi u dodir sa podacima o ličnosti da ove mere primeni, pogotovo što se mnoge od njih definišu odgovarajućim internim pravnim aktim. To je, npr. slučaj kod nas. Preduzeća, druge organizacije i uprava koji prikupljaju, evidentiraju, obrađuju, iskazuju, prenose, razmenjuju i koriste podatke i informacije, dužni su da, u skladu sa zakonom, svojim aktima, urede mere zaštite podataka i informacija, od zaštite računarskih nosilaca podataka, do programske podrške, prenosnih puteva, i sl.<sup>75</sup>.

Vrlo često se mere predviđene ovim principom kombinuju sa pozitivnom praksom korisnika. Ukoliko se desi gubljenje, brisanje ili neautorizovani pristup, menjanje ili obelodanjivanje i utvrdi da je subjekt, kod koga se to desilo, odgovoran usled nepreduzimanja odgovarajućih mera, pa zbog toga dodje do nanošenja štete ili bola subjektu podataka, tada subjekt podataka može zahtevati odštetu.

Znači, **princip** da se mere sigurnosti preduzimaju protiv neautorizovanog pristupa, menjanja, otkrivanja i uništenja podataka o ličnosti **primeniće se uvek kad određeni subjekti** (korisnici i davaoci ICC usluga) **ne preduzmu odgovarajuće mere** i usled toga dodje do neautorizovanog pristupa, menjanja ili oticanja podataka o ličnosti, kao i njihovog slučajnog gubljenja i uništenja.

I na kraju, treba konstatovati da u zaštiti privatnosti, informacione privatnosti i podataka o ličnosti, prava, obaveze i odgovornosti, kao i principi zaštite predstavljaju ne samo neodvojivu celinu, već i takav Gordijev čvor čije odmršivanje može stvoriti nove probleme umesto rešavanja postojećih.

## 2.2. *Zaštita organizacija i poverljivih podataka*

### 2.2.1. *Zaštita organizacija*

Postojanjem i dostavljanjem određenih podataka može se ugroziti organizacija, bilo kog oblika i karaktera bila. Sve se češće govori o "privatnosti

<sup>74</sup> Tapper C., Computer Law, London, Longman, 1989., str. 334.

<sup>75</sup> Uredba o obezbedjenju i zaštiti informacionih sistema državnih organa.

organizacija”, odnosno podataka o njima. Mada se ovakvim odredjenjima ukazuje na neophodnost posebnog tretmana i zaštite podataka organizacija, ona nisu prihvatljiva, jer se privatnost može vezati samo za pojedinca, ličnost, individuu. Međutim, sigurno je da se pravnim mehanizmima i merama moraju zaštititi i organizacije, kao subjekti o kojima podaci postoje i mogu da se nadju u opticaju, jer to mogu biti “tajni” podaci i svrhe. Takođe, postojanje odredjenih podataka o organizaciji koji nisu tačni, ažurni ili potpuni, kao i podataka koji mogu biti dostupni trećim licima postaju problem o kome bi se trebalo naći rešenje. Mnogi od tih podataka mogu biti od vitalne važnosti za organizaciju, ali i osnova njihovog uspeha, poslovnosti i konkurentnosti. Pristup takvim podacima u spoljnim BP od strane neautorizovanih korisnika može ugroziti opstanak organizacije i diskvalifikovati je u poslovnim odnosima. Velike BP o patentima, licencama, know-how, finansijskim uspesima, neuspesima, mogućnostima, prometu, koje se mogu, iz raznih razloga i potreba, voditi kod državnih organa ili nekih drugih organizacija (banaka, statistike, komora) predstavljaju, pored svih svojih pogodnosti, i potencijalnu opasnost za one o kojima se vode. Zbog toga je neophodno obezbediti sigurnost podataka i predvideti odgovarajuće pravne instrumente na osnovu kojih bi se "subjektivitet" organizacija zaštitio.

Da bi se to postiglo neophodno je predvideti i odredjena **ovlašćenja organizacija** koja se odnose na prikupljanje, obradu, memorisanje i korišćenje podataka o njima, kao i odredjene **obaveze i odgovornosti subjekata** kod kojih se podaci, u BP, nalaze i koji su nadležni i ovlašćeni da takve podatke dostavljaju odgovarajućim subjektima.

Jedno od **ovlašćenja organizacije** moglo bi biti ovlašćenje da traži informacije o postojanju podataka, svrhama, vremenima, načinima obrade i vrstama korisnika koji ih koriste. **Ovlašćena lica organizacije** treba da kontrolišu kvalitet i sadržaj podataka da bi se mogla, u slučaju zloupotrebe, neovlašćenog pristupa, brisanja ili menjanja, zahtevati zaštita i naknada štete koja je nastala, ili je mogla nastati, sa takvim rukovanjem. Iako vrlo slična suštini prava informacione privatnosti ova ovlašćenja organizacija to ipak nisu. Mnoga od njih nalaze se u normama vezanim za fer postupke prikupljanja, obrade i korišćenja odredjenih podataka, dok su druga izvedena analogijom. Tim više, što je vrlo teško razlučiti da li su podaci o pojedincima značajniji pojedincima nego podaci o organizaciji samoj organizaciji. Ovo je, verovatno, bio razlog zbog kojeg su mnogi autori (pa i neki zakoni, npr. Norveške, obuhvatili pored podataka o ličnosti i podatke privatnih korporacija) pod pravo privatnosti podveli i organizacije. Iako zabune može biti, ipak treba naglasiti da je suština ovih prava različita, a pogotovo i njihov obim i način ostvarivanja.

Drugim rečima, organizacija bi mogla imati **ovlašćenja**: **a)** da *zahteva da bude obaveštena* o postojanju BP u kojoj se nalaze njeni podaci; **b)** da *očekuje da se sa njenim podacima adekvatno postupa* i da se na odgovarajući način koriste; **c)** da *pristupi svojim podacima* koji se kod nekog drugog vode; **d)** da *ispravi netačne, neažurne podatke*; i **e)** da se *žali nadležnom organu ili telu* zbog nepravilnosti u postupanju sa njenim podacima ili šteta koje zbog toga pretrpi. Kao posebnu dodaje se i **f)** da *zahteva posebno osiguranje* poverljivosti svojih podataka.

Kao i kad su u pitanju podaci o ličnosti, postupanje sa podacima organizacije treba da bude u skladu sa odgovarajućim principima.

### 2.2.2. *Zaštita poverljivih podataka*

Da bi mogli uživati posebnu zaštitu, s obzirom na značaj koji imaju, neophodno je klasifikovati podatke organizacije i na osnovu toga odrediti im stepen poverljivosti. Takvi podaci se, po mišljenju mnogih autora<sup>76</sup>, mogu svrstati u **pet kategorija**:

1. pronalasci, industrijski procesi i ključni tehnički podaci;
2. tehnički podaci i materijali;
3. podaci iz oblasti marketinga, kupovine, nabavke, klijentele i planova organizacije;
4. podaci iz oblasti finansija, računovodstva, prava i obezbeđenja;
5. podaci vezani za vođenje poslovnih knjiga i evidencije.

Dakle, **značaj ovih podataka i informacija ogleda se i u neophodnosti da se na osnovu kategorizacije oni tretiraju kao tajna (poslovna, službena) i to na različitim nivoima poverljivosti**. Naravno, pre daljeg razmatranja ovih nivoa, trebalo bi odrediti šta se pod tajnom (poslovnom) podrazumeva? Opšte značenje je da je **tajna pravom zaštićeno saznanje (podatak) o činjenici (radnji, postupku, događaju, ispravi, dokumentu, programu i sl.) u vezi sa subjektom (poslovnim), koje sme da poseduje samo određeno ili određena lica**. Vrlo je bliska i definicija data u Zakonu o suzbijanju nelojalne utakmice Japana iz 1990. godine koji pod poslovnom tajnom podrazumeva proizvodne postupke, metode prodaje i/ili druge podatke (informacije), a koji se odnose

<sup>76</sup> Manley W., II., Shrode W., Critical Issues in Business Conduct, Legal, Ethical and Social Challenges for the 1990's, New York, Quorum Book, 1989., str. 181 - 189; Unković D., Strategija i tehnika zaštite poslovnih tajni, Beograd, Savremena administracija, 1989., str. 25 - 28.

na tehničku ili poslovnu politiku, koji se čuvaju kao tajne i koji su generalno nepoznati javnosti.

Nivoa poverljivosti ima više, ali se najčešće ističu<sup>77</sup>:

**(a) Prvi nivo poverljivosti** čine najosetljiviji i najznačajniji podaci. Naravno, to su oni, po pravilu, malobrojni koji su u kategoriji *ključnih poslovnih tajni*. To su, prevashodno, podaci i informacije iz prve i delimično druge kategorije. Takvi podaci i informacije ne bi trebalo legalno da se nadju u internom IS, a još manje van organizacije, jer uvek postoji opasnost da "procure". To su, na primer<sup>78</sup>, nepatentirane formule i proizvodi (nepatentirani upravo da ne bi bili otkriveni ili nakon protoka, zakonom određenog, vremena postali javno dobro), koji, ukoliko se i nadju u BP u/ili van organizacije, nisu dati voljom i sa njenim znanjem. Ne treba zaboraviti da ni čuvena formula "Coca-Cola" ne samo što nije nikad patentirana, već je samo u delovima poznata pojedincima koji ne mogu rekonstruisati celinu, pa je više nego sigurno da se ona ne nalazi u bazi. Zbog toga treba stalno imati u vidu da će ovi podaci, **ukoliko postanu dostupni drugim "korisnicima", sigurno izazvati katastrofu za organizaciju i direktno će joj ugroziti opstanak**. Takve podatke, s toga, nikako ne bi trebalo memorisati, pa čak ni u slučajevima "posebnih ciljeva i razloga" jer njihova zaštita, ma koliko bila efikasna, ne može biti i potpuna, a strogo sankcionisanje posledica, koje njihovim iznošenjem van organizacije nastaju, nije dovoljna pretnja i upozorenje. Ukoliko se ovakvi podaci i informacije, iz bilo kog razloga, uz posebnu dozvolu, i nadju u internoj bazi podataka neophodno je obezbediti posebnu zaštitu pre nego što nastanu negativne posledice. *Čini se da je najefikasnija zaštita - hitno brisanje takvih podataka.*

**(b) Drugi nivo poverljivosti** trebalo bi da uživaju podaci i informacije koji predstavljaju *značajne (poslovne) tajne*. To su, na primer, radni nacrti, detaljni projekti komercijalnih proizvoda, sveobuhvatni interni priručnici. Ovi podaci, takodje, ne bi trebalo da se nadju u IS unutar, a pogotovo ne van organizacije. A ako se i nadju van organizacije ona mora biti informisana o njihovom postojanju; ko ih je dostavio; zbog čega i koliko dugo treba da se u njemu nalaze; ko ih i, u kojoj meri, može koristiti. Svaki autorizovani korisnik, a autorizacija podleže posebnoj proceduri i proveru, mora voditi računa o načinu i svrsi njihovog korišćenja i odgovarati za sve one postupke koji nisu po strogo utvrđenim, legalizovanim, pravilima. **U suštini i ove podatke trebalo**

<sup>77</sup> Pfleeger C., Security in Computing, Engelwood Cliffs, Prentice - Hall International, inc., 1989., str. 12 - 28; Palmer I. C., Potter G. A., Computer Security Risk Management, London, Jessica Kingsley Publishers, 1989., str. 29; Drakulić M., Pravni aspekti zaštite podataka u organizaciji, I stručni skup: Zaštita podataka u računarskim sistemima, Beograd, 1995., str. 230 - 255.

<sup>78</sup> Unković D., op. cit., str. 28.

bi, po pravilu, **izbegavati u bazama, naročito javnim**, jer, iako ne katastrofalna, njihova zloupotreba može biti od velike štete za organizaciju. Za povećanje sigurnosti ove podatke bi trebalo smestiti u posebne baze i kompjutere i čuvati na poseban način, koristeći sve softverske, hardverske, pravne, organizacione i druge mere. Pri tome, ne treba zaboraviti da se ovakvi podaci nikako ne bi trebalo naći u transferu podataka niti u komunikacionim mrežama, ma koliko one bile sigurne i pouzdane. *Svaki kontakt sa njima treba posebno evidentirati i posebno proveravati.*

(c) **Treći novo poverljivosti** čine podaci koji se svrstavaju u "*običnu tajnu (poslovnu) i koji se mogu naći, uz određeni tretman, u bazama podataka unutar i van organizacije.* Takvih podataka i informacija ima više i različiti su po svom značaju za organizaciju i korisnike. To su podaci vezani za planske dokumente, planove marketinga, finansijske i računovodstvene zapise i sl. Iako značajni za organizaciju oni, ukoliko se i otkriju neautorizovanim korisnicima (drugim organizacijama), *predstavljaju štetu, ali ne nenadoknadivu.* O postojanju ovih podataka, njihovoj upotrebi, korisnicima, dužini čuvanja i korišćenja, načinu iskazivanja i kvalitetu, nadležni organi u organizaciji, ne samo što moraju biti upoznati, već moraju dati dozvolu za njihovo prikupljanje, memorisanje i korišćenje.

(d) U **četvrtom nivou poverljivosti** pojavljuju se posebno zanimljivi *podaci organizacije* vezani za *know-how* koji su za organizaciju utoliko značajniji ukoliko joj obezbeđuju komparativnu prednost u odnosu na druge organizacije iz iste oblasti rada, delatnosti ili sa istim proizvodnim programima. Iako, po nekim pravima, ne pripadaju kategoriji ključne tajne oni bi to trebali da budu, makar samo u kategoriji "obične" tajne. *Ovi podaci trebalo bi da imaju specijalni status u bazama podataka i bez znanja organizacije ne bi smeli da se legalno naći van nje.* Naravno, ovi podaci kod nas nemaju isti tretman kao u drugim, razvijenijim, zemljama, ali bi se o njima moralo posebno voditi računa, jer, i oni predstavljaju podatke čijim gubljenjem, brisanjem, zloupotrebom, neautorizovanim korišćenjem mogu biti nanete štete organizaciji i njenoj specifičnosti<sup>79</sup>.

(e) **Peti nivo** čine "*nesenzitivni podaci kojima pristup nije, niti treba biti, posebno restriktivan.* To su svi oni podaci koji se mogu koristiti i u "javnom domenu" Medjutim, oni mogu da se pojave kao problem za sigurnost ukoliko dodje do njihovog kombinovanja, ukrštanja, povezivanja, pa se na taj način transformišu u osetljive podatke. Tada ih treba klasifikovati u jedan od prethodnih nivoa.

<sup>79</sup> Cornwall H., Data Theft, Computer Fraud, Industrial Espionage and Information Crime, London, A Mandarin Paperback, 1993., str. 28.

Da bi se postigla kolika tolika sigurnost podataka koji pripadaju ovim kategorijama neophodno je u organizaciji predvideti odgovarajuće mere i mehanizame, a kad ovi podaci treba da se nadju, ili se nalaze, van organizacije tada je nužno predvideti određena "prava", odnosno ovlašćenja organizacije, kao i obaveze i odgovornosti subjekata u čijim su bazama oni smešteni.

Ovlašćenja organizacija u odnosu na poverljive podatke koji se na nju odnose zahtevaju da subjekti koji ih prikupljaju, obrađuju ili koriste imaju određene obaveze i odgovornosti. Te odgovornosti i obaveze odnose se, pre svega, na: svrhu njihovog prikupljanja, čuvanja i korišćenja; način na koji se dobijaju; dužinu čuvanja; kvalitet i poseban tretman koji će morati uživati u poslovnom prometu, jer štete koje neadekvatnim tretmanom nastaju mogu biti velike, ponekad i nenadoknadive, ne samo za organizaciju, već i za državu, nacionalnu i transnacionalnu privredu. Međutim, neophodno je istaći da su postupci i procedure prikupljanja podataka različiti kad se radi o podacima o pojedincima i podacima o organizacijama usled razlika u "predmetu" zaštite. Dok se kod podataka o pojedincima štiti ljudska ličnost, dotle se **kod podataka o organizacijama štiti interes**, a što ima sasvim drugačiju pravnu prirodu. U prvom slučaju neophodna je ličnopravna zaštita subjekta, dok je u drugom imovinskopravna zaštita prioritetna (ličnopravne zaštite nema, sem ako nisu u pitanju zaposleni organizacije i njihovi podaci). Usled toga su **obaveze subjekata**, kod kojih se ovakvi podaci mogu u BP naći, vrlo slične obavezama proisteklim iz postojanje određenih podataka o ličnosti, ali zbog svoje pravne prirode ne i identične, i odnose se na:

- a) **ograničavanje prikupljanja podataka** samo na one podatke koji su neophodni i za svrhe koje su unapred utvrdjene i jasno definisane, a organizacija obaveštena o tome;
- b) **kontrolisanje dostavljanja podataka** organizacije autorizovanim subjektima i za autorizovane svrhe u periodima koji su unapred utvrdjeni;
- c) **obezbedjenje posebne kontrole** izvora, korisnika podataka i njihovih ovlašćenja;
- d) **brisanje** onih podataka koji više nisu potrebni ili su utvrdjeni da predstavljaju ključne tajne;
- e) **odvajanje** od ostalih podataka i poseban pravni tretman podataka koji predstavljaju značajne tajne, kao i know-how;
- f) **osiguranje kvaliteta** podataka, odn. njihove kompletnosti, tačnosti i ažurnosti;
- g) **prijavljivanje organizaciji** zloupotreba, krađa uništenja, delimičnog ili potpunog brisanja podataka, neautorizovanih pristupa ili nekontrolisanih tokova bilo kojih poverljivih podataka u bazi i iz baze;
- h) **prijavljivanje određenim nadležnim državnim institucijama**, organima i organizacijama neophodnost dostavljanja podataka o

organizaciji stranim subjektima, razlozima, načinima i oblicima u kojima se podaci nalaze zbog dobijanja dozvola i nakon dobijanja dozvola obaveštavanje o tome organizacije o čijim se podacima radi.

Sva ova ovlašćenja, obaveze i odgovornosti<sup>80</sup> imaju za cilj da obezbede da organizacija bude zaštićena od raznovrsnih neopravdanih, neodgovarajućih ili neodgovornih zahvatanja u poverljive podatke, a naročito one koji predstavljaju ili bi mogli da predstavljaju, poslovnu ili neku drugu tajnu i zbog čijeg prikupljanja van organizacije bi ona mogla da pretrpi štete.

Poseban problem nastaje kod primene PC tehnologije koji uobičajeno nisu snabdeveni operativnim sistemom koji obezbedjuje dovoljan stepen zaštite. U takvim slučajevima moraju se predvideti posebni oblici zaštite i pravno regulisati odgovornosti i ovlašćenja za nju.

### 2.3. *Zaštita podataka u prekograničnom toku podataka*

Prekogranični tok podataka (*Transborder Data Flaw - TDF*) predstavlja pojavu koja je u prethodnoj dekadi zaokupljala pažnju usled rapidnog napretka telekomunikacionih sistema i sve veće međunarodne trgovine informacijama i ICC uslugama. Upravo za prekogranični prenos podataka vezano je i pitanje trgovine kompjuterizovanih informacija, kompjuterskih i komunikacionih usluga. KT je pokazao i dokazao da se sve više brišu nacionalne granice i obaraju nacionalne barijere u toj trgovini.

U suštini, **prekogranični tok podataka** predstavlja<sup>81</sup> *transfer podataka preko državnih granica bez obzira na kojoj se vrsti medijuma oni nalaze*. Prenos podataka može se realizovati elektronski, kablovski ili preko satelita, mada nije isključeno ni, znatno sporijim, fizičkim prenosom magnetnih traka, diskova, kartica ili nekog još jednostavnijeg medijuma. Bitno<sup>82</sup> je da su podaci koji se nalaze u prekograničnom prenosu u **mašinski čitljivoj formi**. Takvi podaci mogu normalno biti uskladišteni ili reprocessirani u drugoj zemlji od one koja predstavlja zemlju porekla.

<sup>80</sup> Edwards C., Savage N., Walden I., op. cit., str. 323.

<sup>81</sup> Edwards C., Savage N., Walden I., op. cit., str. 121.

<sup>82</sup> Edwards C., Savage N., Walden I., op. cit., str. 121.

Lični, poslovni, tehnički ili organizacioni podaci koji se najčešće nalaze u prekograničnom prenosu podataka, po pravilu, se i koriste u sledeća četiri konteksta:

- **intra-organizacionih;**
- **inter-organizacionih;**
- za zadovoljavanje **potreba vlada;**
- **medjunarodnih informacionih poslova** (npr., gonjenja kriminalaca ili razmene podataka izmedju udaljenih baza).

Podaci i informacije koje se sada često nalaze u prekograničnom transferu su npr. informacije o rezervacijama avionskih letova izmedju poslovnica smeštenih u različitim zemljama jedne kompanije ili izmedju različitih avio kompanija (Pan Evropski sistemi rezervacije avio karata *Galileo* i *Amadeus* svakodnevno izvrši veliki broj rezervacija avio karata na svim kontinentima); milionske kreditno-kartične transakcije (*Americain Express* dnevno koristi TDF za više miliona transakcija vezanih za kreditnu karticu); elektronski transfer novčanih sredstava izmedju banaka (*SWIFT* sistem Društva za medjunarodne interbankarske finansijske telekomunikacije dnevno izvrši transfer ogromnih svota izmedju 1200 banaka u 50 različitih zemalja); i sl.

Iako veoma značajan za medjunarodnu trgovinu informacijama i uslugama, TDF biva veoma često i posebno regulisan nacionalnim propisima kako bi se sprečilo nekontrolisano oticanje i "curenje" podataka naročito zbog:

1. **potrebe da se zaštite pojedinci**, odn. privatnost (npr. jedan Švedski ministar 1979. godine izjavio je "ne može se verovati zakonima o zaštiti podataka o ličnosti drugih zemalja, tako da se naši građani u njima osećaju i bivaju nezaštićeni");
2. neophodnosti da se **zadrži u nacionalnim granicama ekonomska dobit** koja se postiže tzv. nacionalnom i medjunarodnom informacionom ekonomijom i trgovinom i sve većim učešćem informacija i ICC usluga u porastu nacionalnog bogatstva;
3. **nacionalne sigurnosti;**
4. **ranjivosti računara**, koja može izazvati ne samo ekonomsku, već i političku ranjivost nekog sistema ukoliko "kritična masa" nacionalno/ekonomskih podataka predje nacionalne granice.

Pojedine zemlje bore se da zaštite određene podatke i informacije raznim pravnim i administrativnim merama uvodeći, čak, i posebne takse za TDF kako bi uravnotežile trgovinu i razmenu nekih od njih.

Za podatke o ličnosti i naše je pravo predvidelo mogućnost iznošenja, no samo ukoliko se **poštuje princip reciprociteta**, što znači da je i zemlja u koju se oni unose obezbedila zaštitu kojom su obuhvaćeni i strani državljani, i to ne manje nego što se predviđa našim zakonima<sup>83</sup>.

Isto tako, pod posebnom prismotrom prava i odgovarajućih institucija su transnacionalne korporacije<sup>84</sup> koje često imaju za predmet poslovanja upravo podatke, informacije i ICC usluge, a koje je veoma teško podvesti pod zakone samo jedne zemlje. Radi toga se primenjuju razna rešenja vezana za njih, izmedju ostalog, i ugovori u kojima se predviđa nadležnost određenog prava.

Što se međunarodnih pravnih mehanizama tiče oni su mahom orijentisani na regulaciju transfera podataka o ličnosti, međunarodne telekomunikacije, izgradnju i primenu principa vezanih za međunarodni transfer. S obzirom da su veoma često u pitanju podaci o ličnosti to se modifikovani principi zaštite ovih podataka primenjuju i kad su u pitanju prekogranični tokovi. Pri tome, sve akcije koje se povodom njih preduzimaju imaju za cilj da omoguće **slobodu cirkulacije u međunarodnim razmerama** kompjuterizovanih podataka i informacija i njihovu zaštitu<sup>85</sup>. Da bi se to postiglo neophodno je<sup>86</sup>, poči od sledećeg:

- ♦ **obezbediti dostupnost i smanjiti**, u što je moguće većoj meri, **stvaranje neopravdanih prepreka** za prenos podataka preko granica;
- ♦ **ostvariti transparentnost u propisima i politikama** koje se odnose na ICC usluge;
- ♦ **realizovati potrebu za zajedničkim pristupima** i uskladenim rešenjima;
- ♦ **maksimalno voditi računa o posledicama međunarodnog prelivanja inicijativa** i nacionalnih politika. Na ove opšte zahteve nadgrađuju se i posebni koji se odnose na sigurnost i bezbednost podataka, odgovornost, izbor najpovoljnijeg zakona, verodostojnost, takse i obaveze, kao i na prepoznavanje prava na podatke.

Kao **osnovni principi TDF** koje treba poštovati i obezbediti pojavljuju se:

- a) dostupnost tržišta** sa uredjenošću i dostupnošću informacija;

<sup>83</sup> Predlog zakona o zaštiti podataka o ličnosti, čl. 26.

<sup>84</sup> O TNCs više kod Drakulić M., Osnovi Poslovnog prava, Beograd, FON, 1995., str.95 - 108.

<sup>85</sup> Evropska Direktiva je predvidela šest osnovnih principa za transfer podataka o ličnosti u treće zemlje, kao i slobodno kretanje takvih podataka unutar Unije (čl. 25.)

<sup>86</sup> Deklaracija o prekograničnim tokovima podataka OECD.

- b) *transparentnost* nacionalnih zakona;
- c) *nacionalni tretman*, naročito kad je u pitanju zaštita podataka i telekomunikacija;
- d) *nediskriminacija*;
- e) *precizna regulativa* na međunarodnom planu kako bi se izbegle suprotnosti i različiti tretmani;
- f) *državni monopol* kad su u pitanju određene, naročito, telekomunikacione usluge;
- g) *smanjenje dominantnih i povlašćenih pozicija*;
- h) *smanjenje nepoštenih trgovačkih prakse*;
- i) *smanjenje izuzetaka* i predviđanje jemstava, naročito kad su u pitanju podaci za koje postoje višestranji interesi.
- j) *decentralizacija nadležnosti* kad su u pitanju područja regulisanja određenih pitanja i aktivnosti.

Svi ovi zahtevi i principi treba da doprinesu ne samo progresivnoj liberalizaciji trgovine uslugama u uslovima poštene konkurencije, već i većoj sigurnosti TDF koji se u njima pojavljuju. Istovremeno ovi principi treba da omoguće prevazilaženje suvereniteta, nacionalne bezbednosti, samostalnosti i sl., a posebno standarda koji se pojavljuju kao izuzetno pogodno sredstvo da zemlje-protivnici i zemlje-provalnici upadaju u IS i komunikacione mreže. Time se standardizacijom omogućuje veća ranjivost sistema i postizanje suprotnih efekata od očekovanih (ako su očekivani efekti smanjenje troškova, povećanje efikasnosti i skraćivanje vremena prenosa, onda je jasno kakvi se suprotni efekti mogu pojaviti kao nuz-produkt). Ovo postaje osobito značajno pitanje ako neka zemlja ne prihvati standardizaciju ili ne potpiše odgovarajući međunarodni akt kojim se standardi propisuju ili ih namerno zloupotrebi i krši. Ovakvoj zemlji su, tada, pojednostavljene mogućnosti prepada i zloupotrebe prekograničnog toka tuđih podataka. Drugi je problem vezan<sup>87</sup> za dominaciju informaciono razvijenih zemalja. Naime, kad je u pitanju standardizacija opreme i mreža, veliki proizvođači su skloni predlaganju standarda koje prihvataju njihove vlade u zaštiti sopstvenih interesa, pa nerazvijene ili slabije razvijene zemlje, kupujući takvu opremu i služeći se kreditima, kupuju i sopstvenu vazalsku ulogu. Ova, i mnoga druga, pitanja treba tek rešiti menjajući i neke, već klasične, principe međunarodnog prava i međunarodnih pravnih standarda.

Osim toga, sve ove principe, slobode i ciljeve TDF treba povezati i sa elektronskom razmenom podataka.

---

<sup>87</sup> Kavran D., Uloga prava u razvoju i funkcionisanju informacionih sistema, Beograd, Anali Pravnog fakulteta u Beogradu, br. 2 - 3/89, str. 206.

#### 2.4. Zaštita podataka u elektronskoj razmeni podataka

Pre dvadesetak godina u SAD je počela ekspanzivna primena i razvoj **elektronske razmene podataka** (*Electronic Data Interchange - EDI*)<sup>88</sup>. Iako u tesnoj vezi sa prekograničnim tokovima podataka, EDI se, umnogome, od njega razlikuje, jer, pre svega, obuhvata elektronski prenos<sup>89</sup>, od računara do računara (*computer-to-computer*) trgovačkih, administrativnih i transportnih podataka korišćenjem dogovorenih standarda u koje je strukturirana EDI poruka<sup>90</sup>. To je, u suštini: *razmena strukturiranih komercijalnih podataka između računara posebnih firmi radi poslovnih transakcija, izvršena bez manuelne intervencije, elektronskim putem posredstvom standardizovanih poruka koje zamenjuju tradicionalna papirna dokumenta*<sup>91</sup>.

Znači, kao **bitni elementi** specifične razmene podataka izvršene uz pomoć EDI su<sup>92</sup>:

1. **EDI je razmena podataka**, odn. to je dvosmerni prenos poruka, pri čemu, se pod **porukama** podrazumeva *niz segmenata, strukturiranih korišćenjem dogovorenih standarda u kompjuterski čitljivom formatu koji su podobni da budu automatski i nedvosmisleno obradjeni*<sup>93</sup>.
2. **EDI je razmena strukturiranih podataka**, što znači da poruke moraju biti u određenom formatu, i to takvom koji omogućuje mašinsku obradu.
3. **EDI je razmena podataka između kompjutera zasebnih firmi**. "Zasebne firme" su ne samo različite organizacije, nego i različiti delovi iste organizacije.
4. U razmeni koja se odvija u **EDI nema manualnih intervencija**, što ujedno znači da je u pitanju razmena između aplikacija, a ne ljudi.
5. Najčešće se **EDI sprovodi u oblasti poslovnih transakcija**, koje obuhvataju trgovinu i transport, ali i administraciju.

<sup>88</sup> Doduše, u američkom pravu i ekonomiji pojavio se termin **elektronski transfer podataka** (*Electronic Data Transfer - EDT*), ali je on imao isto značenje kao i EDI.

<sup>89</sup> Kao elektronski prenos EDI poruka između trgovinskih partnera, definisan je najkraće EDI u materijalu Ekonomske komisije za Evropu Ekonomskog i socijalnog saveta UN, Trade/WP.4/R. 1089. iz 22. jula 1994.

<sup>90</sup> Evropski model EDI sporazuma Komisije EEZ o pravnim aspektima EDI, 1994, član 2., tč. 2.1, Beograd, Yu EDI forum, br. 2/94.

<sup>91</sup> Walden I, EDI and the Law, London, Bienheim Online, 1989., str. 73.

<sup>92</sup> Stojčić Z., EDI i razlozi njene primene, Brezovica, Prva YU EDI konferencija, 1993., str. 1.

<sup>93</sup> Evropski model EDI sporazuma, čl. 2., tč. 2.3.

6. **EDI je razmena poruka** koje se pojavljuju umesto tradicionalnih papirnih dokumenata
7. **EDI se realizuje korišćenjem dogovorenih standarda**, a najčešće su to EDIFACT standardi, pravila UN za EDI, koji predstavljaju niz međunarodno dogovorenih standarda, imenika, uputstava, naročito vezanih za razmenu koja se odnosi na trgovinu robom i uslugama između nezavisnih računarskih IS<sup>94</sup> i, naravno
8. **EDI je razmena elektronskim putem**, a ne magnetnim ili drugim medijima, kao što je često slučaj sa TDF.

Kad su u pitanju trgovački podaci, među njima su prioritetni podaci o: konkurentima; potrošačima; samoj organizaciji i ekonomskoj situaciji; koji ulaze u tzv. **3C informacije** (*Customers, Competition, Company*).

Sijaset je ciljeva zbog kojih se EDI uvodi, kao i razloga njegove primene, različite posledice, pozitivne i negativne<sup>95</sup>. Tako, kao **osnovni ciljevi** najčešće se pojavljuju<sup>96</sup>:

- ♦ *umanjenje ukupnih troškova* za obradu i tranziciju papirnih dokumenata (npr. čekova);
- ♦ *umanjenje grešaka* koje, inače, prave ljudi pri obradi;
- ♦  *smanjuje se vreme* potrebno za unos podataka;
- ♦ *prevazilaze se jezičke barijere* i problemi rada u različitim vremenskim zonama, a što se postiže nedvosmislenim sadržajem poruka;
- ♦ *ubrzava se dostava* podataka;
- ♦ *menadžment je efikasniji* na svim nivoima;
- ♦ *efikasnije se upravlja*, povećava se promet novčanih sredstava, obezbeđuju se ažurni tokovi i unapređuje kontrola ukupnih kretanja gotovine;
- ♦ omogućuje se *veća fleksibilnost prenosa* podataka, čiji broj nije ograničen;
- ♦ *povećava se produktivnost*;

<sup>94</sup> Evropski model EDI sporazuma, čl. 2., tč. 2.4.

<sup>95</sup> Ispitivanje i analiziranje posledica korišćenja EDI jedan je od značajnih predmeta u okviru **TEDIS** (*Trade EDI System*) programa koji se od 1988. godine realizuje u okviru EU, o čemu više kod Hussson P., The TEDIS EDI & ISDN Initiative, Online's Conference, Hamburg, 1995 -02-6/10; kao i kod Milošević M., Elektronska razmena podataka u Evropskoj Uniji, III YU EDI konferencija, Beograd, 1995., str. 18 - 24.

<sup>96</sup> Stojčić Z., op. cit., str. 2.

- ♦ *realizuju se i drugi ciljevi* koji zavise od delatnosti organizacija koje ih koriste.

Kao najmarkantniji razlozi primene ističu se najčešće oni vezani za ekonomske efekte koji se primenom postižu, vodeći, pri tome, računa o rezultatima prethodno sprovedene **cost - benefit analize**. Ova analiza treba da pokaže koje su prednosti za organizaciju, potrošača (kupca, npr.), ali i državu. Tako se, primera radi, pojavljuju prednosti i potencijalni uticaji na troškove (što je konstatovano i u *Bank of Montreal*)<sup>97</sup>. Uvodenjem EDI eliminisani su mnogi troškovi, kao što su: stalni troškovi vezani za čekove, koverta, papir, kucanja i štampanja; obrade; nesigurnosti pošte; gubitak dokumenata i sl. Potencijalno sniženje troškova i poboljšanje usluga očekuju se kod kurirskih usluga; tekućih troškova promene termina plaćanja, a značajno unapredjenje biće kod prognoze novčanih tokova.

Da je EDI, ipak, vredan određenih troškova vidi se iz same činjenice da se on uvodi u mnoge organizacije, mnoge zemlje, a, takodje, da su prvi pilot - projekti već startovali u Rusiji, Češkoj, Bugarskoj, Mađarskoj, Litvaniji, Poljskoj, Sloveniji, Jugoslaviji, pored, naravno, razvijenih evropskih, azijskih, američkih država, kao i Australije i poneke afričke zemlje.

Medjutim, često se postavlja pitanje kakve bi bile **negativne posledice**, ukoliko ih uopšte i ima?

- ♦ **efekti odbojnog psihološkog stava**, otvorenih i prikrivenih otpora uvođenju;
- ♦ **problemi sigurnosti i zaštite**, naročito kad su u pitanju davaoci servisa od kojih se zahteva posebna sigurnost u verodostojnosti poruka, izboru probne poruke, kontroli pristupa, integritetu i poverljivosti sadržaja, poverljivosti prolaza poruke, integritetu sekvence poruke, bezbednosti osetljivosti poruke, kao i sve veće raznovrsnosti ataka koji prete;
- ♦ zakonska ili druga pavana, **ograničenja, nepotpunosti ili nedorečenosti**<sup>98</sup>;
- ♦ **teškoće u prilagođavanju** postojećeg aplikativnog softvera;
- ♦ relativno **veliki inicijalni troškovi** uvođenja;
- ♦ **nedovoljna razvijenost organizacije** i uslovljenost odluke o uvođenju od raznih činilaca (organizacionih, socijalnih, ekonomskih, etičkih,

<sup>97</sup> Prevod iz: Financial Electronic Data Interchange - Overview Bank of Montreal, Yu EDI forum, br. 4/95.

<sup>98</sup> Nedin Z., Pravne prepreke razvoju EDI, Brezovica, Prva Yu EDI konferencija, 1993., str.257 - 263.

kulturnih i sl.), koji se, ponekad, ne uzimaju u obzir, što prouzrokuje negativnu klimu;

- ♦ drugi razlozi kontra EDI.

Pored ovih, pojavljuju se i mnogi drugi negativni efekti, te je na organizaciji i menadžerima da procene da li im se uvođenje EDI isplati i da li su očekivani pozitivni efekti veći od negativnih.

Naročito velika nepoznanice su **odgovornost** učesnika u EDI prenosima i obezbeđenje sigurnosti i zaštite podataka, odn. poruka.

Dakle, tipične odgovornosti koje imaju strane u EDI transakcijama pojavljuju se na stranama: **pošiljaoca** poruke; **davaoca** komunikacionih usluga, odn. servisa; i **primaoca** poruke. Ove odgovornosti su istovremeno i odgovornosti organizacija koje se u ovim ulogama pojavljuju. Tako, **pošiljaoc poruke** ima **odgovornost** za: otpremanje poruke u odgovarajućem formatu i po odgovarajućem protokolu; bezbednost od iskrivljavanja poruka; osiguranje korektnosti adresovanosti poruka na primaoca; osiguranje posebne autorizovanosti poruka; osiguranje uskladenosti poruka sa vremenom transakcije; postizanje svih neophodnih prava kopiranja; zadržavanje priključivanja, uključivanja, podataka i očuvanje tajnosti i sigurnosti primljene poruke. **Davaoc komunikacionih usluga** mora imati **odgovornost** za: otpremanje poruke u određenoj formi i po određenim protokolima; bezbednost od iskrivljavanja poruka; sigurnost da je poruka otpremljena ka primaocu i osiguranje tajnosti i sigurnosti poruke. **Primaoc poruke**, takodje, ima određene **odgovornosti**, i to: za osiguranje da je poruka usmerena ka njemu; priznavanje i verifikovanje poruke i osiguranje tajnosti i sigurnosti poruke. Znači, *svi subjekti u EDI imaju odgovornost i obavezu osiguravanja tajnosti i sigurnosti poruke kao zajednički imenitelj*<sup>99</sup>.

Odgovornost za bezbednost poruka predstavlja obavezu svih strana u EDI da će primenjivati postupke obezbeđenja i mere kojima će osigurati zaštitu od rizika neovlašćenog pristupa, izmene, docnje ili gubitka<sup>100</sup>.

<sup>99</sup> Svi ovi, i mnogi drugi, pravni problemi razmatraju se i rešavaju u okviru Ekonomske Komisije za Evropu, Ekonomskog i socijalnog Saveta UN. Primera radi trebalo bi videti materijale i izveštaje, obaveštenja i sl. kao što su: Internal Organization and Operating Procedures for Completion of the Work Program on Legal Questions and Other Legal Issues, Trade/WP.4/R. 1071, juli 1994; Legal Aspects of Trade Data Interchange, Trade/WP.4/R. 1096., od 22 jula 1994; Business and Information Modeling, Trade/WP.4/R. 1090. 22 juli 1994., i sl.

<sup>100</sup> Evropski model EDI sporazuma, čl. 6., tč. 6.1.

Ovi postupci treba da osiguraju proveru porekla i integriteta poruke. Svaki od ovih postupaka treba da obezbedi utvrđivanje pošiljaoca i primaoca poruka i njihove verodostojnosti. To se odnosi, naročito, na verodostojnost potpisa i verodostojnost dokumenata<sup>101</sup>. Takođe, nužno je i utvrđivanje potpunosti i izopačenosti poruka, kao i grešaka koje se mogu, slučajno ili namerno, pojaviti. To se specifikira u posebnom tehničkom dodatku ugovora koji zaključuju subjekti u EDI prenosima. Posebna je obaveza primaoca poruke da odmah, ili u određenom roku, obavesti pošiljaoca o odbijanju ili otkrivanju greške. Logična posledica obaveštavanja je zaustavljanje svih akcija po poruci od strane primaoca dok procedura traje. Pošiljaoc može ponovo poslati istu poruku, ali samo uz posebnu naznaku da je ispravna<sup>102</sup>.

Posebno se notiraju obaveze u obezbeđenju poverljivosti i zaštiti podataka o ličnosti. Ove obaveze nastaju ako strane u prenosu smatraju i sporazumeju se da su u pitanju poverljivi podaci u poruci koju pošiljaoc šalje. Zato on očekuje da primalac, ali i serviser, neće ove poruke, odn. podatke otkrivati niti dostavljati neovlašćenim licima. Naravno, ovi se podaci neće koristiti ni za svrhe koje nisu definisane. Autorizacija, otuda, pretpostavlja poseban tretman i podvrgavanje određenom stepenu poverljivosti. Takvi se podaci mogu kriptografisati ukoliko je to dozvoljeno po pravima zemalja iz kojih su stranke. Ovo se neće primenjivati ukoliko su u pitanju podaci koji su već dostupni javnosti.

Znači, nema velikih razlika između EDI i klasičnih poruka, samo što su opasnosti koje im prete drugačije. Tako, opasnost za EDI poruku su mogući upadi u sistem, haking i ubacivanje virusa, kao i mnogi drugi kojima se mogu izmeniti ili ukrasti poruke. Zato, sama zaštita treba da obuhvati<sup>103</sup>, prevashodno, zaštitu u lokalnom računarskom sistemu koji izvršava poslovnu aplikaciju i zaštitu u komunikacionoj mreži.

Obezbeđenje **sigurnosti** poruka, ostvaruje se kroz<sup>104</sup>:

- a) navodjenje minimuma bezbednosti** koji treba da se garantuje, a čija osnova je sporazum ili ugovor;

<sup>101</sup> Savić Z., Potpis i potvrđivanje verodostojnosti dokumenata, Brezovica, Druga YUEDI konferencija, 1994., str.154 - 157.

<sup>102</sup> Evropski model EDI sporazuma, čl. 6., tč. 6.2, 6.3.

<sup>103</sup> Savić Z., Razvoj sistema zaštite informacija u EDI okruženju, III YU EDI Konferencija, Beograd, 1995., str. 70.

<sup>104</sup> Vilus J., Građanskopravna odgovornost učesnika u EDI prenosima, Brezovica, Druga YU EDI konferencija, 1994., str. 79.

- b) **ispunjenje zahteva "komercijalne razumnosti"** prilikom korišćenja EDI od svake strane;
- c) **obezbedjenje svake strane od neautorizovanog pristupa** ili garantovanje da je u pitanju autorizovana transmisija; i
- d) **primenu od svake strane odredjenog sistema bezbednosti i tehnika** koje bi predstavljale osnove za "komercijalno razumnu bezbednost".

Drugim rečima, u EDI poruke treba ugraditi bar jedan, a po mogućnosti i više standarda vezanih za sigurnost, koji se odnose na: integritet EDI poruka, na autorizaciju njene originalnosti, nepriznavanje (dokazivanje) porekla, nepriznavanje (dokazivanje) njenog prijema i poverljivosti<sup>105</sup>.

Kada su u pitanju podaci o ličnosti, a naročito oni koji ulaze u sferu privatnosti i informacione privatnosti, onda njihova sudbina prati sudbinu ovih podataka u bilo kom IS, naravno, ukoliko je propisima zemlje ili zemalja porekla subjekata uključenih u EDI, predviđena posebna zaštita. Ako su u pitanju zemlje EU u kojima ne postoje posebni nacionalni propisi (što je redji slučaj) strane u EDI se mogu dogovoriti da se kao minimum standarda primenjuju odredbe **Konvencije Saveta Evrope o zaštiti pojedinaca u odnosu na automatsku obradu podataka**<sup>106</sup> i novodoneta **Direktiva o zaštiti pojedinaca u odnosu na obradu podataka o ličnosti i slobodnog kretanja takvih podataka**.

A od čega treba obezbediti poruke i zaštititi podatke?

Najočigledniji **prikaz poznatih pretnji** dali su D. Grebović<sup>107</sup>; i I. C. Palmer, G. A. Potter<sup>108</sup> navodeći sledećih 26:

#### Osnovne pretnje

| pretnja | opis | tip rizika | vrsta ugrožene informacije | zone slabosti |
|---------|------|------------|----------------------------|---------------|
|---------|------|------------|----------------------------|---------------|

<sup>105</sup> Pomenuti materijal Ekonomske komisije za Evropu, str. 23 i 60.

<sup>106</sup> Evropski model EDI sporazuma, čl. 7., tč. 7.3; Konvencija Saveta Evrope iz 1981.

<sup>107</sup> Grebović D., Aspekti bezbednosti i EDI, Beograd, EDI i EDIFACT standardi, Brezovica, II YU EDI konferencija, 1994., str. 111.

<sup>108</sup> Palmer I. C., Potter G. A., op. cit., str. 14 - 27.

|  |   |   |                   |                                 |
|--|---|---|-------------------|---------------------------------|
| <b>Čeprkanje po podacima</b>                 | neovlašćeno menjanje pri unosu podataka od neovlašćenog lica  | integritet ili raspoloživost              | osnovna pomoćna   | organizacija                    |
| <b>Salama</b>                                | prikrivanje pojedinačnih podataka od kojih je svaki ispod nivoa kontrolnog procesa  | integritet                                | osnovna           | rukovodjenje + kontrolna logika |
| <b>Superzapping</b>                          | programi koji su prošli sve kontrole modifikovanja i otkrivanja bilo kog sadržaja računara, naročito radi izmene podataka | integritet + raspoloživost + poverljivost | osnovna pomoćna   | rukovodjenje + kontrolna logika |
| <b>Trojanski konj</b>                        | neovlašćeni softver koji radi prikriveno  | integritet + raspoloživost                | pomoćna osnovna + | kontrolna logika                |
| <b>Programske bombe (logičke, vremenske)</b> | deo programa koji se aktivira nekim događajem i koji uništava softver i podatke javno ili prikriveno                      | integritet + raspoloživost                | pomoćna + osnovna | kontrolna logika                |
| <b>Virusi</b>                                | neovlašćeni softver koji se sam razmnožava i koji uništava softver i podatke javno ili prikriveno                         | integritet + raspoloživost                | pomoćna + osnovna | kontrolna logika                |
| <b>Trap door</b>                             | neotkrivena slabost u ovlašćenom softveru i hardveru, koja omogućava prikrivanje aktivnosti                               | poverljivost + integritet + raspoloživost | pomoćna + osnovna | kontrolna logika                |
| <b>Prljava pozadina</b>                      | kad sistem prihvati kao stvarne skriveni terminal ili osoba   | integritet, poverljivost, raspoloživost   | osnovna pomoćna   | kontrolna logika                |
| <b>Generalno spremanje</b>                   | neovlašćene radne izmene podataka i programa u toku njihovog izvršavanja  | poverljivost + integritet + raspoloživost | pomoćna + osnovna | kontrolna logika                |
| <b>Asinhrona pretnje</b>                     | neovlašćene izmene u redosledu isporuke podataka ili u redosledu izvršavanja softvera                                     | integritet                                | pomoćna + osnovna | organizacija + kontrolna logika |
| <b>Špijunaža</b>                             | emanacija kojom se kupe ili posmatraju produkti elektromagnetnih polja i dekodiraju                                       | integritet + raspoloživost                | osnovna pomoćna   | organizacija + kontrolna logika |
| <b>Terorizam i iznudjivanje</b>              | destrukcije fizičke prirode napadom na podatke ili pokušaj iznudjivanja   | poverljivost + integritet                 | osnovna pomoćna   | organizacija                    |

|  |  |   |   |  |
|--|--|---|---|--|
| <b>Lažno predstavljanje</b>  |  |   |   |  |
| <ul style="list-style-type: none"> <li>• lica</li> <li>• aktivnih programa</li> <li>• pasivnih objekata</li> </ul> | ⇒ -neovlašćeno korišće. identiteta drugih osoba radi zloupotrebe tuđih prava<br>⇒ -neovlašćeno korišće. prava drugih<br>⇒ -dovodjenje u zabludu lažnim predstavljanjem objekata i korišć. kontrolnih atributa dr. objekata | poverljivost + integritet<br><br>raspoloživost poverljivost + integritet poverljivost | osnovna + pomoćna<br><br>osnovna + pomoćna<br><br>osnovna + pomoćna | organizacija + kontrolna logika<br><br>kontrolna logika<br><br>organizacija + kontrolna logika |
| <b>Kačenje</b>   | neovlašćeno proširivanje korišćenja prethodno ovlašćenog prenosa od strane drugih lica ili procesa   | integritet ili poverljivost ili raspoloživost   | osnovna + pomoćna + pomoćna   | organizacija + kontrolna logika  |
| <b>Lešinarenje</b>   | namerna pretraga za podacima i njihovo neovlašćeno korišćenje nakon završetka ranijih aktivnosti lica ili procesa  | poverljivost  | osnovna + pomoćna   | organizacija + fizička zaštita + kontrolna logika  |
| <b>Odlivanje podataka</b>  | neovlašćeno korišćenje podataka koji su nenamerno stavljeni na raspolaganje  | poverljivost  | osnovna + pomoćna   | organizacija + fizička zaštita   |
| <b>Simulacija modeliranje</b>  | neovlašćena korelacija medju raznim delovima informacije korišćenjem softverskih alata sa mesta gde se informacije/hardver (ne) može dobiti legalano   | poverljivost  | osnovna + pomoćna   | organizacija + podaci  |
| <b>Kradja nosilaca</b>   | neovlašćeno iznošenje nosilaca ili čitavih uređaja   | poverljivost + raspoloživost  | osnovna + pomoćna   | organizacija + fizička zaštita   |
| <b>Kopiranje nosilaca podataka</b>   | neovlašćeno kopiranje podataka sa njihovih nosilaca  | poverljivost  | osnovna + pomoćna   | organizacija + fizička zaštita   |
| <b>Fizičko uništavanje/onemogućavanje</b>  | fizičko uništavanje / onemogućavanje nosilaca, računara, telekom. vodova, zgrada   | raspoloživost   | osnovna + pomoćna   | organizacija + fizička zaštita   |
| <b>Fizičko uplitanje</b>   | neovlašćena promena na nosiocimara, računarima, telekom. vodovima ili zgradama   | integritet + poverljivost + raspoloživost   | osnovna + pomoćna   | organizacija + fizička zaštita   |

|   |   |   |                   |   |
|---|---|---|-------------------|---|
| <b>Prinuda radi</b><br>• saznavanja<br><br>• menjanja | ⇒ prisiljavanje neke osobe za odavanje informacija ili softvera neovlašćenim osobama              | poverljivost                              | osnovna + pomoćna | organizacija                              |
|   | ⇒ prisiljavanje neke osobe koja treba da izmeni podatke ili procese radi dobiti neovlašćenih lica | poverljivost + integritet + raspoloživost | osnovna + pomoćna |   |
| <b>Ucenjivanje</b>                                    | iznudjivanje određenih radnji ubacivanjem virusa u softver spolja                                 | poverljivost + integritet + raspoloživost | osnovna + pomoćna | podaci                                    |
| <b>Hacking</b>  | prodor neovlašćenih lica u sistem   | poverljivost + integritet                 | osnovna + pomoćna | podaci<br>organizacija<br>kontrolna lista |
| <b>Razbijanje šifara</b>                              | neovlašćeno dekriptovanje informacija ili softvera  | poverljivost + integritet + raspoloživost | osnovna + pomoćna | podaci                                    |
| <b>Ponovno emitovanje</b>                             | neovlašćeno ponavljanje podataka  | integritet                                | osnovna           | organizacija + kontrolna logika           |

Za rešavanje problema vezanih za ove pretnje i za uklanjanje, koliko je to moguće, posledica od strane Medjunarodne organizacije za standardizaciju (*International Standard Organization - ISO*) izradjeni su OSI/RM standardi kojima bi trebalo obezbediti povezivanje otvorenih sistema, ali tako da oni budu sigurni, a njihove poruke bezbedne i podaci zaštićeni. OSI mehanizmi treba da obezbede: prevenciju, detekciju i oporavak.

### 3. Instrumenti zaštite

Zaštita podataka i subjekata predstavlja vrlo aktuelan predmet pravnog regulisanja u mnogim zemljama. Problemi zaštite zaokupljali su pažnju pravnika i prava već duže vreme. Tako se "privatnost" pojavljuje u nekakvom obliku, doduše, drugačijem nego danas, još u starom i srednjem veku. Koreni se, izmedju ostalog, mogu vezati i za **Veliku povelju o slobodama** (*Magna charta libertatum*) donetu u Engleskoj 1215. godine. Potom se postepeno prava i slobode unose i u druge akte npr. **Peticiju o pravima** iz 1628. godine Engleske (*Bill of rights*). Medju prvim izvorima pojavljuje se i engleski **Habeas corpus Act**, iz 1679. godine, i koji je još uvek, uz neznatne izmene, na snazi. On predstavlja model na kome će se donositi zakoni drugih zemalja, a koji će predviđjati neprikosnovenost lične slobode, kao prava gradjanina.

Pored ovih, značajni su i drugi akti medju kojima posebno mesto zauzimaju **deklaracije** koje se pojavljuju kao nacionalni ili medjunarodni akti. Deklaracije u unutrašnjem pravu predstavljaju akte vlade ili parlamenta u vezi određenih pitanja. To su npr. Deklaracija o nezavisnosti SAD iz 1776. godine, Deklaracija o pravima čoveka i gradjanina iz 1789. godine Francuske, a čiji se osnovi postulati i danas unose u ustave ove zemlje, i ne samo nje.

U medjunarodnom pravu **deklaracije** se pojavljuju kao izvor prava kojima se, obično, postavljaju pravna načela ili šira pravila, ili potvrđuju zajednički politički stavovi ugovornica po određenom pitanju<sup>109</sup>. Takva je **Univerzalna deklaracija UN o pravima čoveka i gradjanina** doneta 1948. godine u kojoj je predviđeno da se kao osnovno ljudsko pravo pojavljuje pravo fizičkih osoba da izraze i prime informacije. Član 19. predviđa "pravo da se... traže, prime, prenesu informacije i ideje kroz bilo koji medij bez obzira na granice", dok se u članu 18. predviđa sloboda od proizvoljnog mešanja u privatni život, porodicu, dom ili prepisku.

Na osnovu ove Deklaracije doneta je 1968. godine **Teheranska proklamacija o odgovornosti država za ostvarivanje ljudskih prava**.

Osim deklaracija, u medjunarodnom pravu su vrlo značajni i paktovi. **Medjunarodni pakt o ljudskim pravima** odn. **Pakt o gradjanskim i političkim pravima** i **Pakt o ekonomskim, socijalnim i kulturnim pravima** (usvojeni 1966. godine na Generalnoj Skupštini UN), između ostalog, predviđaju da se države zbog kršenja ljudskih prava mogu obratiti Komitetu za ljudska prava (dakle, i radi kršenja prava na privatnost).

No, bez obzira na te prve pokušaje da se pravnim aktima zaštiti pravo čoveka na privatnost ono što se danas pojavljuje kao značajan **izvor prava** su medjunarodni i nacionalni pravni akti kojima se regulišu u potpunosti ili delimično, samostalno ili u sklopu sa regulisanjem drugih pitanja, problemi zaštite subjekata i podataka. Unutrašnji izvori prava su ustavi, zakoni, podzakonski akti (uredbe, naredbe), opšta pravila određenih grana prava, sudska praksa i pravna nauka. Medjunarodni su izvori rezolucije, deklaracije, konvencije, direktive, smernice, preporuke, sporazumi ili bilateralni medjunarodni ugovori. Pored ovih, pojavljuju se i izvesni dokumenti koji nemaju snagu izvora prava, ali predstavljaju instrumente koji mogu značajno uticati na njih. Najčešće, oni su rezultat određenih aktivnosti koje su preduzimale medjunarodne organizacije, udruženja, asocijacije, kao i nacionalne stručne komisije i tela, a koje su kao rezultat imale određene akte, odnosno dokumenta. Takvi instrumenti su izveštaji,

<sup>109</sup> Bartoš M., Medjunarodno javno pravo, ugovorno pravo, Beograd, Službeni list SFRJ, 1986., str. 85.

na primer, Generalnog sekretara UN, preporuke i zaključci profesionalnih udruženja, rezolucije određenih političkih organizacija, i sl. Zbog značaja koji imaju, oni predstavljaju i instrumente, nacionalne i međunarodne, za rešavanje, regulisanje ili ukazivanje na potrebe pravnog regulisanja određenih pitanja vezanih za zaštitu subjekata i podataka. Medju njima naročito je značajan **Izveštaj Jangerove komisije** (*The British Younger Commission Report*) donet 1972. godine u V. Britaniji. Izveštaju su prethodile mnogobrojne aktivnosti raznih komisija, tela i pojedinaca koje su imale za cilj da obezbede pravo na privatnost svakom pojedincu i da ukažu na moguće opasnosti koje mu prete (1967. godine Alex Lyon predlaže Zakon o pravu privatnosti, nekako u isto vreme Nacionalni savet za ljudske slobode počinje kampanju za zaštitu prava privatnosti i utiče na izradu nacrtu novih potencijalnih zakona, i sl.). Ipak, ta ista Komisija u istom Izveštaju predlaže da se usvoje 10 principa pri zaštiti podataka<sup>110</sup>, koji ne samo da su i danas aktuelni, već su predstavljali osnovu i za mnoge nacionalne zakone i međunarodne akte. To su:

- a) Informacije se moraju čuvati tako da se ne menja posebna svrha i ne smeju se koristiti, bez odgovarajuće dozvole, za druge namene. To, u stvari, znači, da se **informacije mogu koristiti samo u skladu sa unapred određenom svrhom** i da u slučaju njihovog korišćenja u druge svrhe mora postojati posebna dozvola, dobijena od onoga o kome se informacije čuvaju i koriste.
- b) **Pristup informacijama treba ograničiti samo na one koji imaju ovlašćenja da ih koriste za ono zašto su namenjene**, što pretpostavlja da ih mogu koristiti, u skladu sa odgovarajućim aktima, samo oni koji imaju posebno ovlašćenje i za one namene na koje se to ovlašćenje odnosi.
- c) Za zadovoljenje određene svrhe (potrebe) **prikupiće se minimalan broj podataka koji je dovoljan da se postavljeni zahtev realizuje**. To pretpostavlja da je nužno voditi računa o broju i kvalitetu podataka kako se ne bi prikupljalo i čuvalo više nego što je potrebno.
- d) **U kompjuterizovanim statističkim sistemima moraju se** na odgovarajući način, projektovanjem i programiranjem, **odvojiti identifikacioni od ostalih podataka**. Ovaj princip kasnije će poslužiti kao osnova za odvajanje ličnih od ostalih podataka. Podaci o ličnosti čuvaće se po posebnom sistemu i za njih će važiti posebni režimi.
- e) **Informacije moraju biti tako sredjene da se problem može izložiti kroz informacije koje se na njega odnose**.
- f) **Izabrani nivo sistema zaštite mora se prethodno prilagoditi potrebama, zahtevima i specifičnostima korisnika**, čime se obezbedjuje zaštita od zloupotreba ili gubitaka informacija.

<sup>110</sup> Edwards E., Savage N., Walden I., op. cit., str. 71.

**g) Sistem kontrole treba da obezbedi otkrivanje bilo koje povrede sigurnosti.**

U projektovanju IS moraju se *definirati vremenski periodi posle kojih se informacija neće koristiti*. Na osnovu ovog principa formiraće se, u kasnijim godinama, princip vremenskog ograničenja čuvanja i korišćenja određenih podataka koji se posle predviđenog roka ne samo da ne smeju da koriste, već je neophodno da se i brišu.

**Sadržaj podataka mora biti ažuran** i mora postojati mehanizam za korekciju neažurnih podataka. Ovaj princip pretpostavlja tačnost i ažurnost podataka, jer samo takvi podaci treba da se nadju u BP, odnosno u IS. Da bi se to moglo realizovati potrebno je postojanje i obaveze odgovarajućih subjekata da o svakoj promeni obaveste onog kod koga se podaci nalaze. Subjekti u čijim se IS podaci nalaze moraju, u određenim vremenskim intervalima i po prijemu korekcije podataka, neažurne podatke ažurirati. S druge strane, primena ovog principa zahteva da subjekti o kojima se podaci čuvaju moraju biti upoznati sa postojanjem tih podataka i, istovremeno, imati pravo da zahtevaju da podaci o njima moraju biti tačni i ažurni. Takođe, ovaj princip kasnije će pretpostaviti još jedan - princip odgovornosti.

Mora se obratiti pažnja na *sistem vrednovanja odluka, presuda*. Iz ovog principa kasnije će se formirati *pravo žalbe* u situacijama kad subjekt, kod koga se podaci u nekoj bazi nalaze, odbije da ih izbriše, prepravi, ažurira, koristi u dozvoljene svrhe i sl., pa pojedinac na koga se podaci odnose nema drugog rešenja do da se obrati nadležnom sudu kako bi svoje pravo zaštiti. Sud koji donosi odluku mora voditi računa o postojanju ovog prava i u skladu sa njim presuditi, a subjekat kod koga se podaci nalaze mora presudu realizovati.

Jangerov izveštaj predstavljao je i obavezu vlade da sačini odgovarajući predlog za rešavanje problema nastalih usled sve većeg korišćenja kompjutera. Krajem 1974. završava se **Bela knjiga** koja se objavljuje 1975. godine i po kojoj je "upravo došlo vreme da oni koji koriste kompjutere za podatke o ličnosti moraju postati odgovorni za njih kako svojim sistemima ne bi ugrozili privatnost"<sup>111</sup>. To je bilo zeleno svetlo za početak zakonodavne aktivnosti i formiranje nezavisne upravne agencije za zaštitu podataka. U februaru 1976. godine Ser Janger postaje rukovodilac novog Komiteta za zaštitu podataka, ali ubrzo umire i umesto njega biva imenovan direktor Hatfield politehnike, Ser Norman Lindop. Lindop-ov Komitet počinje rad na ispitivanju uticaja kompjutera na privatnost. Nakon dve godine istraživanja ovaj Komitet upozorava da "najveća opasnost za privatnost koja preti ne dolazi od privatnog, već od javnog

<sup>111</sup> Edwards E., Savage N., Walden I., op. cit., str. 71.

sektora". Lindop-ov izveštaj (*Lindop Report*) biva objavljen 1978. godine<sup>112</sup> i upozorava na sledeće: "jednostavan set pravila postupanja sa podacima o ličnosti mora se promeniti korišćenjem kompjutera. Zakonodavstvo mora naći ravnotežu između različitih zakonskih interesa. Šema regulative zato mora biti fleksibilna: onoliko koliko su različiti slučajevi, vremena i interesi"<sup>113</sup>. U skladu sa ovakvim pristupom Izveštaj predviđa da se novoosnovani organ uprave mora pridržavati pravila prakse koristeći se saradnjom i konsultujući korisnike kompjutera i druge zainteresovane strane. Za postizanje pravovaljanosti rada mora se obezbediti funkcionisanje krivičnih sankcija i preduzeti registracija svih procesora podataka. U skladu sa tim Britanska vlada formira Registratora zaštite podataka koji je odgovoran za kreiranje i uspostavljanje registra korisnika podataka. Korisnici podataka se moraju pripremiti za primenu odgovarajućih principa zaštite podataka. Ti principi biće kasnije ugrađeni u Zakon o zaštiti podataka.

Na kraju, neophodno je istaći sledeće:

**Prvo. Problem zaštite podataka i subjekata je problem sa kojim se sreću,** manje ili više, **sve zemlje i međunarodna zajednica, pa se, otuda, i preduzimaju određene aktivnosti kako bi se rešio.** Rezultat tih aktivnosti su određeni instrumenti kojima se na probleme ukazuje ili se oni rešavaju. Ako se samo na njih ukazuje akti ne predstavljaju izvore prava, ali predstavljaju putokaze kako se, i kojim, izvorima prava mogu problemi rešiti. S druge strane, akti koji imaju snagu izvora prava su instrumenti kojima jedna ili više država regulišu određene odnose, prava i obaveze određenih subjekata u vezi sa zaštitom podataka i subjekata. Kako ih donose ili ratifikuju državni organi oni predstavljaju obavezu za one na koje se odnose i ukoliko se ne poštuju moraju snositi posledice propisanih sankcija. Zbog toga je neophodno praviti razliku između instrumenata koji su: 1) izvori prava; i 2) onih koji to nisu. U prvoj grupi su unutrašnji i međunarodni izvori prava, dok su u drugoj svi oni akti i dokumenti koje donose nacionalni ili međunarodni organi, tela, organizacije, udruženja, asocijacije. **Iako nemaju istu snagu obe grupe instrumenata su značajne za rešavanje problema zaštite subjekata i podataka, pa se zbog toga neće posebno isticati njihova priroda.** Klasifikacija koja je prihvaćena vezana je više za hronologiju nastajanja i karakter nego za njihovu pravnu prirodu.

**Drugo. U regulisanju problema zaštite postoji razlika između zemalja. Jedna je grupa zemalja u kojima se problemima zaštite prilazi<sup>114</sup>, sa stanovišta "privatno-pravne" zaštite, i vezuje se za pravo privatnosti, odn. donošenje "zakona o**

<sup>112</sup> Campbell D., Connor S., op. cit., str. 26.

<sup>113</sup> Edwards E., Savage N., Walden I., op. cit., str. 72 - 74.

<sup>114</sup> Lilić S, grupa autora, op. cit., str. 9 - 12.

**privatnosti". Druga je grupa zemalja u kojima je polazište "javno-pravna" zaštita i primena načela zakonitosti**, te se zaštita reguliše u okviru "**zakona o zaštiti podataka**". Postoje zemlje u kojima se rešava na specifičan način problem zaštite subjekata i podataka. To su npr. Japan i SRJ. Dok u Japanu ne postoji poseban zakon kojim bi se štitilo pravo privatnosti i podaci, kod nas je ova problematika rešavana u više navrata i sada je još uvek "važeće" rešenje da se ustavima (saveznim i republičkim) proklamuju prava privatnosti i posebne zaštite podataka o ličnosti, a da se u posebnim zakonima, koji su u postupku donošenja, predvide konkretna rešenja. Istine radi postoje i zemlje koje nisu, iz raznih razloga, našle za shodno da pitanje zaštite ugrade u domaće zakonodavstvo na bilo koji način i u bilo kom obliku. S obzirom na ove različitosti **prikaz stanja biće, pored hronologije, dat i po zemljama**, bez obzira koje su stanovište prihvatile i da li pripadaju kontinentalnom ili *Common Law* pravnom sistemu, s tim što neće biti prikazani svi zakoni i iz svih zemalja, već samo **oni koji su značajniji sa stanovišta naše zemlje** (interesantna i specifična rešenja, uticaj koji su imali na druge zemlje, učestalosti saradnje, problemi koji nastaju usled prekograničnog toka podataka i sl). Po istom principu biće dat i prikaz međunarodnih instrumenata (hronološki i po organizacijama).

### 3.1. *Međunarodni instrumenti*

Problem zaštite podataka i subjekata dobija sve više međunarodne razmere. Neka pitanja regulišu se bilateralnim (dvostranim) pravnim aktima između dve zemlje, dok druga zahtevaju, pored konkretnih, i regulisanje (utvrđivanje, uspostavljanje, konstituisanje) određenih opštih pravnih pravila.

Akti koji su doneti predstavljaju<sup>115</sup> "suštinski najznačajniji doprinos u oblikovanju međunarodnih standarda upotrebljivih za nacionalna zakonodavstva."

**Hronološki gledano** problem zaštite pokretan je i regulisan na međunarodnom planu ovim redosledom:

**Tabela 2 - b: Hronologija međunarodnih aktivnosti**

| Godina | Aktivnost određenog međunarodnog tela (organizacije, asocijacije, komisije) |
|--------|---|
| 1948.  | Univerzalna deklaracija o pravima čoveka i građanina UN                     |
| 1950.  | Evropska konvencija o pravima čoveka  |

<sup>115</sup>□turm L., Pravni aspekti zaštite podataka u savremenim informacionim sistemima, Beograd, Anali Pravnog fakulteta u Beogradu, br. 6/86., str. 656.

|       |   |
|-------|---|
| 1966. | Medjunarodni pakt o ljudskim pravima UN   |
| 1967. | Medjunarodna komisija pravnika pokreće inicijativu na Medjunarodnom skupu pravnika  |
| 1968. | OECD započinje Studiju o uticaju kompjutera na institucije i politike vlada   |
| 1973. | Izveštaj Generalnog sekretara UN "Ljudska prava i naučni i tehnološki razvoj"<br>Rezolucija Evropskog saveta o zaštiti privatnog života fizičkih lica u odnosu na elektronske banke podataka u privatnom sektoru  |
| 1974. | Izveštaj Generalnog sekretara UN "Ljudska prava i naučni i tehnološki razvoj - Upotreba elektronike koja može da utiče na lična prava i ograničenja koja bi, zbog takve upotrebe, trebalo uvesti u demokratskom društvu"  |
| 1974. | Rezolucija Evropskog saveta o zaštiti privatnog života fizičkih lica u odnosu na elektronske banke podataka u javnom sektoru<br>Univerzalna poštanska konvencija  |
| 1978. | Komisija EZ priprema osnovne pravce politike vezane za napredak informacionog područja<br>OECD se priprema za izradu Smernica o zaštiti poverljivosti u međjugraničnim tokovima podataka o ličnosti   |
| 1979. | Medjunarodna trgovinska komora formira Radnu grupu za ispitivanje pitanja koja se odnose na međjugranične tokove podataka   |
| 1980. | Afrički regionalni skup razmatra probleme prikupljanja i korišćenja podataka u međunarodnim razmerama<br>Medjunarodna trgovinska komora saopštava rezultate Radne grupe za ispitivanje pitanja koja se odnose na međjugranične tokove podataka<br>Medjunarodna komisija za probleme komunikacija UNESCO-a ukazuje na probleme vezane za ekspanziju komunikacijskih sredstava i mogućnosti, donosi Preporuku u vezi sa obavezama multinacionalnih kompanija pri objavljivanju podataka u međunarodnom sistemu komunikacija<br>Osniva se Medjunarodni centar za istraživanje i planiranje informacionih i komunikacionih sistema u sklopu UNESCO<br>Evropski savet donosi Konvenciju za zaštitu pojedinaca u odnosu na automatsku obradu podataka o ličnosti koja stupa na snagu 1985. godine |
| 1981. | Evropski savet donosi Preporuku za usvajanje Konvencije za zaštitu pojedinaca u odnosu na automatsku obradu podataka o ličnosti<br>Medjunarodni biro za informatiku UNESCO organizuje Svetski kongres o politici međunarodnih tokova podataka<br>Udruženje poštanskih i telekomunikacionih službi Evrope predlaže promene u praksi prenosa podataka<br>OECD donosi Smernice o zaštiti privatnosti u međjugraničnom toku podataka o ličnosti<br>Konferencija OECD o osetljivosti telekomunikacionih i informacionih sistema i o implikacijama društvenih zavisnosti od kompjutera  |
| 1982. | Konferencija OECD o zaštiti podataka koji nisu ličnog karaktera<br>Obnovljena Medjunarodna konvencija o telekomunikacijama<br>Komisija za ljudska prava UN izrađuje smernice za zaštitu podataka<br>Centar za transnacionalne kompanije UN izrađuje studiju o važnosti kompjuterizovanih informacionih tokova za multinacionalno poslovanje   |
| 1985. | OECD donose Deklaraciju o prekograničnim tokovima podataka<br>UNICTRAL (Komisija UN za međjunarodno trgovinsko pravo) donosi Preporuku o dokaznoj snazi podataka dobijenih upotrebom kompjutera<br>Ekonomska komisija za Evropu Ekonomskog i socijalnog Saveta UN razmatra procedure i preporuke za olakšavanje prenosa podataka koji prate tok dobara i trgovinu   |

|       |  |
|-------|--|
| 1986. | OECD donosi Kodeks liberalizacije tekućih nevidljivih operacija<br>OECD donosi Kodeks za liberalizaciju kapitalnih kretanja koji se odnose na unutrašnje neposredno investiranje i srodne aspekte prava etabliranja<br>Komitet za trgovinu OECD i Radna grupa za prekogranične tokove podataka razmatraju Referat o ispitivanju relevantnosti pojmovnog okvira za trgovinu kompjuterskih usluga i usluga kompjuterizovanih informacija<br>Komitet za politiku u informacijama, kompjuterima i komunikacijama (ICCP Komitet) razmatra materijal vezan za trgovinu ICC uslugama i prekograničnim tokovima podataka                   |
| 1987. | UNICTRAL donosi Pravni vodič za međubankovne prenose podataka elektronskim putem<br>Radna grupa OECD razmatra izveštaj o postojećim propisima zemalja članica i usvaja zajednički izveštaj<br>UNCID donosi Jednoobrazna pravila ponašanja važna i za EDI   |
| 1988. | Veće OECD razmatra predloge za reviziju Smernica<br>OECD priprema Nacrt internih smernica za zaštitu privatnosti svojih kompjuterizovanih kadrovskih informacionih sistema   |
| 1989. | Grupa eksperata EEZ priprema Predlog akcija vezanih za pravno regulisanje informacionih tehnologija i prioriternih problema koje treba regulisati u okviru Evropske zajednice  |
| 1990. | Obnavlja se i intenzivira rad na unifikaciji i harmonizaciji prava u okviru Evropske zajednice i vrši postepena priprema u V. Britaniji na prelazak na kontinentalni sistem prava<br>Počinje intenzivan rad grupe eksperata na rešavanju problema kompjuterskog kriminala u okviru EEZ i OECD<br>Generalna skupština UN donosi Smernice koje se odnose na kompjuterizovane dosjee podataka<br>Savet za saradnju potrošača donosi Smernice za trgovinsko - potrošačku razmenu i EDI korisnički vodič<br>Organizacija za razmenu podataka u teletransmisiji donosi tzv. ODETTE Smernice<br>CMI donosi Pravila elektronskog konosmana |
| 1992. | Savet Evrope donosi Preporuku o zaštiti podataka upotrebljenih za plaćanje i druge odgovarajuće operacije<br>Savet Evrope donosi Preporuku o zaštiti informacionih sistema<br>Savet Evrope razmatra Informaciju o precedentnom pravu u vezi Evropske konvencije o. ljudskim pravima  |
| 1993. | Savet Evrope usvaja Preporuku o zaštiti podataka u oblasti telekomunikacija  |
| 1994. | UNCTRAL donosi Model zakona o elektronskoj trgovini<br>Sekretarijat UNCTAD donosi Preporuku i priručnik za efikasnost trgovine<br>Komisija EU o pravnim aspektima EDI donosi Evropski model EDI sporazuma  |
| 1995. | Evropski Parlament i Savet usvajaju Direktivu o zaštiti pojedinaca u odnosu na obradu podataka o ličnosti i slobodnom kretanju takvih podataka   |
| 1996. | Evropska unija odn. LAB (Pravna savetodavna Komisija) organizuju Konferenciju o pristupu javnim informacijama kao ključu ekonomskog razvoja i elektronske demokratije u Stokholmu<br>Evropska unija organizuje Radnu konferenciju o Evropskoj Direktivi u Hanoveru   |

### 3.1.1. Zaključci Medjunarodne komisije pravnika

Prve konkretne inicijative vezane za zaštitu podataka potekle su **1967.** godine na **Medjunarodnom skupu pravnika** održanom u Stokholmu, organizovanog od **Medjunarodne komisije pravnika** (Komisija UN). Tada je konstatovano da je pravo privatnosti jedno od osnovnih ljudskih prava i sve zemlje bi trebalo da preduzmu odgovarajuće akcije i mere kako bi ono bilo zaštićeno. Mere i akcije treba preduzeti na nacionalnom i medjunarodnom planu, što znači da se pravnom regulativom i drugim sredstvima bi trebalo da propišu odgovarajuća pravna sredstva i sankcije u slučajevima njihovog kršenja. Po zaključcima ove Komisije<sup>116</sup> **pravna zaštita pojedinaca odnosila bi se na: 1)** mešanje u lični, porodični i domaći život; **2)** mešanje u stvari telesnog i duhovnog integriteta odn., u stvari, moralne i intelektualne slobode; **3)** napad na čast i ugled; **4)** prikazivanje u lažnom svetlu; **5)** objavljivanje irelevantnih činjenica o ličnom životu koje ga mogu izložiti sramoti; **6)** špijuniranje, uhodjenje, posmatranje i ispitivanje; **7)** mešanje u stvari korespondencije; **8)** saopštavanje datih ili dobijenih informacija od pojedinaca u uslovima profesionalne tajnosti.

Svi ovi oblici ugrožavanja prava na privatnost mogu nastati, između ostalog, i javnim saopštavanjem podataka o licima ili upotrebom uređaja za elektronsko praćenje i nadzor.

### 3.1.2. Izveštaji Generalnog sekretara UN

Nesporna uloga koju u zaštiti privatnosti imaju Univerzalna deklaracija o pravima čoveka i gradjanina i Medjunarodni pakt o ljudskim pravima ne umanjuje se drugim instrumentima koji se, u okviru UN, donose i usvajaju. Takvi su, svakako, **izveštaji** Generalnog sekretara podneti Ekonomskom i Socijalnom savetu u dva navrata - **1973.** i **1974.** godine. Prvi izveštaj pod naslovom "**Ljudska prava i naučni i tehnološki razvoj**" (*Human rights and scientific and technological developments*) predstavlja inicijalni dokument na osnovu koga će biti podnet drugi, mnogo iscrpniji i konkretniji, izveštaj pod nazivom "**Ljudska prava i naučni i tehnološki razvoj - Upotreba elektronike koja može da utiče na lična prava i ograničenja a koju bi, zbog takve upotrebe, trebalo uvesti u demokratskom društvu**" (*Human rights and scientific and technological developments - Uses of electronics which may affect the rights of person and the limits which should be placed on such uses in a democratic society*). U ovom drugom izveštaju navode se **medjusobne polazne osnove** i principi na kojima bi trebalo da se bazira pravno regulisanje zaštite prava pojedinaca pred pretnjama koje mogu nastati korišćenjem računara u IS u kojima se nalaze podaci o pojedincima. Da bi se to izbeglo, pretnje ublažile i učinile u što je moguće većoj meri

<sup>116</sup> Lilić S., op. cit., str. 15.

bezopasnima, Izveštaj preporučuje da se u **državama donesu nacionalni zakoni** kojima bi se zaštitila prava pojedinaca. Ovi zakoni treba da se odnose na informacione sisteme u državnom, ali i u privatnom sektoru čime bi se obezbedila jedinstvenost zaštite pojedinaca od prikupljanja, obradivanja, čuvanja i korišćenja podataka o njima.

Pored preporuke donošenja zakona, isti Izveštaj ističe potrebu da se prihvate i **materijalni standardi** za pripremanje nacionalnih zakonodavstava. Ovi standardi odnose se na prikupljanje samo onih podataka o pojedincima koji su neophodni zavisno od ciljeva zbog kojih se IS uspostavljaju. Pored toga, pojedinac mora biti obavešten o prikupljanju podataka i treba da da svoj pristanak pre nego što se podaci nadju na određenom medijumu. Od ovih načela, odn. standarda, mogući su izuzeci i to samo, za tačno i unapred, utvrđene slučajeve. Takvi slučajevi bi bili oni koji se tiču nacionalne bezbednosti ili se odnose na primenu načela zakonitosti kod krivično-pravnih i sudskih postupaka ili kad postoji, na osnovu drugih zakona, izričito ovlašćenje da se neki podaci i informacije mogu prikupljati i bez pristanka pojedinca. Bez obzira što predstavljaju izuzetke, ovi podaci se, takodje, moraju, na odgovarajući način i primenom odgovarajućih mera, zaštititi.

### 3.1.3. *Konvencija o zaštiti pojedinaca s obzirom na automatizovanu obradu podataka o ličnosti*

Ministarsko veće Evropskog saveta 17 oktobra 1980. godine objavilo je **Konvenciju o zaštiti pojedinaca s obzirom na automatizovanu obradu podataka o ličnosti** (*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*), tzv. **Evropsku konvenciju**<sup>117</sup>. Donošenje ove Konvencije predstavljalo je rezultat dugotrajnog procesa pripreme koji je započeo još daleke 1960. godine. Ministarski komitet je prihvatio predlog sa jednim uzdržanim glasom (SR Nemačka), a Konvencija stupa na snagu 5 godina kasnije, jer ju je, tek tada, potpisalo pet zemalja, kako je i bio uslov<sup>118</sup>.

**Konvencija** se sastoji iz **tri osnovna dela**: u *prvom delu* dat je "katalog osnovnih prava" pri zaštiti podataka; u *drugom delu* se nalaze odredbe o međunarodnim

<sup>117</sup> Savezna Skupština SRJ je usvojila Zakon o potvrđivanju ove Konvencije, Službeni list SRJ br.1/92 (Međunarodni ugovori), ali je u članu 3 ovog Zakona odredila da se Konvencija neće primenjivati za automatizovane zbirke sa ličnim podacima koje se vode u skladu sa propisima o kaznenoj evidenciji i propisima o evidenciji u oblasti državne bezbednosti.

<sup>118</sup> O toku rada na Evropskoj konvenciji više kod Drakulić M., op. cit., str. 153 - 158.

tokovima podataka, a *treći deo* posvećen je mehanizmima za ostvarivanje bilateralnih konsultacija.

U opštim odredbama istaknuto je da je "svrha ove Konvencije da osigura, na teritoriji svake zemlje potpisnice, svakom pojedincu, bilo koje narodnosti i bilo kojeg mesta boravka, poštovanje njegovih prava i osnovnih sloboda, a posebno prava na privatnost, s obzirom na automatsku obradu podataka koji se odnose na njega".

U sledećim članovima regulišu se pitanja definisanja osnovnih pojmova, obima, obaveza potpisnica, kvaliteta podataka, posebnih kategorija podataka, osiguranja, dodatnih mera, sankcija, izuzetaka i ograničenja i proširenja zaštite. Interesantna je odredba kojom se definišu **podaci** koji pripadaju **posebnoj kategoriji** i koji se ne smeju obrađivati automatski ako domaći zakon ne obezbeđuje odgovarajuće mere zaštite. Takvi su podaci: koji *identifikuju poreklo, političke stavove, religiozna i druga ubedjenja* i koji se *odnose na zdravstveno stanje*. Svi ostali podaci koji se smeju automatski obrađivati moraju imati odgovarajući kvalitet. **Kvalitet podataka** podrazumeva da su: **a)** prikupljeni i obrađivani tačno i legitimno; **b)** memorisani za specifične i legitimne svrhe i ne smeju biti korišćeni na način inkompatibilan tim svrhama; **c)** adekvatni, relevantni, nepreopsežni u odnosu na svrhe radi kojih su i memorisani; **d)** tačni, i kad je to nužno, ažurni; **e)** održavani u onom obliku koji dozvoljava identifikaciju subjekata podataka u onoj meri u kojoj je to potrebno za svrhe radi kojih se podaci memorišu.

#### Pojedinac ima pravo da:

- *utvrdi postojanje automatizovane datoteke podataka o ličnosti*, njenih najvažnijih svrha, kao i identitet i mesto boravka odn. sedište kontrolora datoteka;
- u razumnim intervalima, bez prevelikog zakašnjavanja ili troškova, *dobije potvrdu* o tome jesu li podaci o ličnosti koji se na njega odnose memorisani u automatizovanoj datoteci podataka, kao i da mu se predoče u razumljivom obliku;
- *zahteva*, zavisno od slučaja, *ratifikaciju ili brisanje takvih podataka* ako se oni obrađuju suprotno odredbama domaćeg zakona, imajući u vidu osnovne principe koji se odnose na kvalitet podataka i dozvoljenost automatskog obrađivanja;
- ima mogućnost *preduzimanja odgovarajuće akcije* (pravnog leka) po zahtevu za potvrđivanjem ili, zavisno od slučaja, primanjem, ratifikacijom ili brisanjem ne bude doneto rešenje, ili zahtev bude odbijen.

**Izuzeci** i ograničenja su moguća samo ako su izazvana nužnom merom demokratskog društva zbog državne sigurnosti, javnog reda, monetarnih interesa države, suzbijanja kriminalnih delikata, zaštite subjekata podataka ili prava i sloboda drugih subjekata, korišćenje za statistiku ili naučne svrhe kad očigledno ne postoji rizik od ugrožavanja privatnosti.

Regulišući TDF odredbe ove Konvencije predviđaju **slobodnu cirkulaciju podataka o ličnosti**, sem u slučajevima kada se njom može ugroziti privatnost ili ako domaće zakonodavstvo predviđa određena ograničenja i zabrane.

U ostalim odredbama predviđeno je **uvodjenje institucije opunomoćnika** koji treba da prati zakonodavstvo drugih zemalja potpisnica, dostavlja informacije o svojim nacionalnim aktima i pruža pomoć pojedincima čije je pravo privatnosti ugroženo. Pored toga, zemlje potpisnice se obavezuju da će formirati Savetodavni komitet koji ima za cilj da daje predloge i mišljenja o promenama, unapredjenju i sprovođenju ove Konvencije.

I na kraju, mora se istaći da je donošenje ove Konvencije imalo ne samo pravni nego i politički značaj za zemlje članice Evropske zajednice, jer omogućuje i predviđa saradnju u zaštiti pojedinaca od podataka kojima se može ugroziti njihovo pravo na privatnost. I ne samo članica Evropske unije, već i zemlja kakva je naša. Tako je 1992. godine Savezna Skupština SRJ donela Zakon o potvrđivanju ove Konvencije. Istovremeno ona će biti osnova za mnoge buduće međunarodne akte kojima se regulišu pitanja zaštite.

#### *3.1.4. Smernice za zaštitu privatnosti i prekograničnih tokova podataka o ličnosti*

Zemlje OECD su još pre više od petnaest godina počele rad na zaštiti podataka i privatnosti i to naročito u slučajevima kad je u pitanju TDF. Godine 1979. stručna grupa OECD, Radna grupa za informacionu, kompjutersku i komunikacionu politiku (ICCP) i Podgrupa vladinih eksperata za prekogranične barijere podataka i zaštitu podataka predložile su, posle dužeg vremena intenzivnog rada, Smernice za postizanje zaštite privatnosti i prekograničnih tokova podataka o ličnosti. Predlog Smernica je još doradjivan i doterivan kako bi postigao bolje formulacije i obuhvatio bolja rešenja, pa je tek 1981. godine Ministarski savet OECD prihvatio **Smernice za zaštitu privatnosti i prekograničnih tokova podataka o ličnosti** (*Guidelines of the Protection of Privacy and Transborder Flows of Personal Data*). Od 24 zemalja članica

OECD, 18 je odmah glasalo za Smernice, dok je šest zemalja, koje su se uzdržale (Australija, Kanada, Irska, Island, Turska, V. Britanija), zadržalo mogućnost da ih kasnije prihvate.

**Osnovni cilj Smernica** je da se između nacionalnih zakona i politika zemalja članica *postigne i realizuje zajednički interes u zaštiti privatnosti i sloboda pojedinaca* kako bi se savladale teškoće u razlikama i olakšao TDF. U tu svrhu preporučeno je da zemlje članice ugrade, ili bar uzmu u obzir, pri izradi nacionalnih zakona principe koji se tiču zaštite privatnosti i sloboda. Dalje se preporučuje da zemlje članice treba da nastoje da uklone ili spreče stvaranje prepreka, u cilju zaštite privatnosti i sloboda pojedinaca, u TDF.

Smernice su podeljene u pet celina (poglavlja). U prvom, opštem delu, date su definicije "kontrolora podataka", "podataka o ličnosti" i "prekograničnog toka podataka". Ne pretendujući da definišu za sve slučajeve sadržinu ovih pojmova, Smernice su, ipak, dale veoma prihvatljive definicije i za druge prilike. Tako se pod **"kontrolorom podataka"** *podrazumeva subjekt (lice ili grupa eksperata) koji, po nacionalnom zakonu, ima pravo da odlučuje o sadržaju i upotrebi podataka o ličnosti bez obzira jesu li takvi podaci sakupljeni, čuvani, obradjivani ili diseminirani od strane samog tog subjekta ili njegovog zamenika. "Podaci o ličnosti" su svi oni koji se odnose na identifikovanu ličnost ili ličnost koju je moguće identifikovati (subjekt podataka). "Prekogranični tokovi podataka" odnose se na kretanje podataka o ličnosti preko granica.*

Pored definicija, ovaj deo sadrži i odredbe o obimu primene, izuzecima i kako tumačiti njihovu pravnu prirodu. Ono što je značajno je da **se Smernice i principi koji se njima utvrđuju primenjuju na sve podatke o ličnosti bez obzira da li se oni nalaze u privatnom ili javnom sektoru**. Svi podaci koji se odnose na pojedince i kojima se mogu ugroziti privatnost i lične slobode predstavljaju predmet zaštite koja se predviđa ovim Smernicama. Izuzetak mogu biti samo oni podaci o ličnostima kojima se ne ugrožavaju privatnost i slobode i oni podaci koji se odnose na suverenost, nacionalnu sigurnost i državnu politiku i koje bi trebalo što redje prikupljati i puštati u međunarodne tokove ili iznositi javnosti.

Drugi i treći deo odnose se na osam osnovnih principa primene u pojedinim zemljama i slobodnom međunarodnom toku. To su:

1. **princip ograničavanja prikupljanja podataka** polazi od neophodnosti postojanja ograničenja i isticanja da se podaci o ličnostima moraju dobiti

na legitimni i pošten način i, kad god je to moguće, sa znanjem i uz pristanak onoga na koga se odnose;

2. **princip kvaliteta podataka** kojim se teži istaći neophodnost da podaci o pojedincu moraju biti relevantni u odnosu na svrhu za koju će se koristiti i u meri koliko je to potrebno u odnosu na nju, potom moraju biti tačni, potpuni i ažurni;
3. **princip navodjenja svrhe** ukazuje na težnju ograničavanja mogućnosti prikupljanja podataka o pojedincima za nedefinisane, neodređene, nepoznate svrhe. Otuda je neophodno svrhe unapred odrediti, bar za vreme njihovog prikupljanja, kako bi kasnija upotreba bila ograničena na svrhu koja je predviđena ili koja nije u suprotnosti sa njom;
4. **princip ograničenja upotrebe** uspostavlja takav odnos prema podacima o ličnostima da se ovi podaci ne smeju otkriti, staviti na raspolaganje ili koristiti na drugi način u odnosu na prethodno utvrđene svrhe ili da svrhe budu drugačije od onih koje su predviđene. Izuzeci mogu biti samo ako postoji saglasnost subjekta na koji se podaci odnose ili ako za to postoji zakonsko ovlašćenje;
5. esencijalni princip, koji se u odnosu na privatnost i zaštitu podataka pojavljuje, je **princip osiguranje** čija je suština u obavezности zaštite podataka o ličnostima raznim merama protiv gubitka ili neovlašćenog pristupa, uništenja, korišćenja, modifikovanja ili otkrivanja;
6. **princip otvorenost**, koliko je to moguće, s obzirom na specifičnost, način prikupljanja i svrhe korišćenja podataka o ličnosti;
7. da bi se osigurao pojedinac u odnosu na podatke koji se o njemu prikupljaju i koriste on bi trebalo da uživa i određena prava. Prava koje ima definisana su **principiom sudelovanja pojedinca** koji se odnosi na njegovo **pravo** da:
  - **kontrolise podatke** ili na drugi način dobija potvrdu da li kontrolor podataka ima takve podatke o njemu
  - **sazna podatke** koji se na njega odnose i to u razumno vreme, uz naknadu, ako je potrebna; na razuman način i u obliku koji mu je razumljiv bez poteškoća
  - **sazna zbog čega mu podaci nisu dostupni** kako bi se mogao žaliti ukoliko su razlozi neopravdani
  - **ospori podatke** koji se na njega odnose, a ukoliko se žalba prihvati može tražiti da se podaci izbrišu, isprave, upotpune ili dopune
8. **princip odgovornosti** polazi od nužnosti postojanja i predviđanja obaveza i odgovornosti drugih subjekata kako bi se mogla ostvarivati prava pojedinaca.

Treći deo predviđa utvrđivanje **osnovnih postavki** vezanih za slobodni tok podataka preko granica i određena, celishodna i nužna, **ograničenja** koja se moraju poštovati zbog zaštite privatnosti. Iako je slobodan, neprekinut i siguran TDF neophodan i značajan za ekonomski, privredni i socijalni razvoj, ipak, moraju postojati i određena ograničenja. Ograničenja se primenjuju u odnosu na zemlje koje ne prihvataju ili ne primenjuju u dovoljnoj meri Smernice. Takodje, ona mogu postojati ako nacionalni zakoni zemlje, preko koje podaci teku, takve podatke smatraju podacima iz sfere privatnosti i ukoliko druga zemlja članica (porekla, određenja) za njih ne pruža ekvivalentnu zaštitu. No, i pored mogućnosti postojanja izvesnih, opravdanih, ograničenja, Smernice preporučuju da zemlje članice, što je moguće više, izbegavaju donošenje zakona ili vođenje politike koji bi, u ime zaštite privatnosti, stvorili prepreke u međunarodnim tokovima podataka.

U suštini, Smernice OECD predstavljaju jednu od akcija koje preduzimaju razvijene zemlje kako bi zaštitile prava i slobode svojih građana, ali što je još značajnije, ona treba da doprinese slobodnom protoku podataka između zemalja članica i zajedničkom unificiranju prava kako bi su osigurala harmonizacija u onim oblastima koje su od zajedničkog interesa. Pri tome se ne sme zaboraviti da članstvo u ovoj organizaciji imaju i Australija, Finska, Kanada, SAD što znači da Smernice, iako slabije pravne snage nego Evropska konvencija, pružaju mogućnost šire primene i veće saradnje između zemalja.

### 3.1.5. Deklaracija o prekograničnim tokovima podataka

Zemlje članice OECD nisu se zadovoljile samo donošenjem Smernica, već su nastavile dalji rad u okviru Komisije za ICCP. Ova Komisija je još 1982. godine "uočila potrebu za međunarodnim pravilima koja bi se odnosila na prekogranične tokove podataka". Prihvatanjem nužnosti međunarodne regulative vezane za "kretanje podataka koji se mogu očitavati putem mašina, preko nacionalnih granica, radi obrade, čuvanja i pronalaženja, uključujući podatke emitovane preko kompjuterskih komunikacionih sistema"<sup>119</sup> je uslovilo da u okviru Komisije, Radna grupa za prekogranične tokove podataka počne rad na izradi studije, na osnovu koje će, potom, sačiniti i predlog Deklaracije. Predlog Deklaracije zemlje članice razmatraju i usvajaju na ministarskom sastanku 1985. godine. **Deklaracije o prekograničnim tokovima podataka** (*Declaration of Transborder Data Flows*) predstavlja otvaranje mogućnosti za saradnju zemalja povodom značajnog pitanja koje se odnosi na sve veći opticaj sve raznovrsnijih podataka i informacija van granica jedne zemlje. Tim

<sup>119</sup> Kavran D., op. cit., str. 202.

više što je pitanje prekograničnih tokova informacija i podataka postalo vitalno pitanje saradnje ili sukoba između različitih rešenja domaćih zakonodavstava.

Deklaracija je vrlo kratka, sadrži svega četiri tačke osnovnih principa i tri tačke koje se odnose na dalje oblike rada vezane za određene kategorije (tipove) prekograničnih tokova podataka.

Kao osnovni **principi** međunarodne saradnje utvrđuju se :

- ***princip unapredjenja dostupnosti podataka i informacija***, srodnih usluga i izbegavanja stvaranja neopravdanih prepreka međunarodnoj razmeni podataka i informacija;
- ***princip transparentnosti u propisima i politikama*** koje se odnose na informacione usluge koje imaju uticaj na prekogranične tokove podataka;
- ***princip zajedničkog pristupa i uskladenog rešavanja*** problema vezanih za prekogranične tokove podataka;
- ***princip respekta mogućih implikacija za druge zemlje*** kada se bave pitanjima vezanim za prekogranične tokove.

Ono što se posebno ističe je neophodnost daljeg rada i saradnje na rešavanju pitanja prekograničnog toka podataka koji se odnose na međunarodnu trgovinu, kompjuterizovane usluge i usluge kompjuterizovanih informacija ponudjenih tržištu i intra-korporacijskih tokova podataka.

Razlozi koji se u preambuli Deklaracije navode vezani su za pojavu raznolikosti učesnika u TDF, značaj koji ovi tokovi imaju, uticaj koji imaju nacionalne politike i različite mere koje vlade propisuju za njihovo sprovođenje i svest da ovi tokovi donose znatne društvene i ekonomske koristi koje proizlaze iz dostupnosti različitih izvora informacija, efikasnih i uspešnih informacionih usluga. Konstatovanje postojanja ovih razloga navelo je predlagače Deklaracije **da istaknu neophodnost saradnje i izmirenja različitih ciljeva koji se u nacionalnim politikama postavljaju**. Tim više, što se ovi tokovi vezuju, najčešće, za komercijalne ili nekomercijalne organizacije, pojedince i vlade koje u razmeni učestvuju sa velikim brojem kompjuterizovanih podataka iz oblasti trgovačkih aktivnosti, naučne i tehnološke razmene, i sl. Ovi podaci i informacije sve više prelaze nacionalne granice različitih država, pa je, otuda, neophodno sagledati i regulisati, na jedinstven način, njihovu međunarodnu dimenziju.

Deklaracija je predstavljala inicijalni dokument za dalji rad na **regulisanju međunarodne trgovine ICC uslugama** koje su "značajan oslonac za pružanje niza

drugih usluga, kao što su usluge vezane za bankarstvo, osiguranje, turizam, prevoz i proizvodnju"<sup>120</sup>. Obim ovih usluga sve više raste i kako se ističe u navedenom dokumentu: **1)** sve je veća uloga softvera u kompjuterizovanim sistemima i telekomunikacijama; **2)** proširuju se trendovi vezani za automatizaciju rada u fabrikama i kancelarijama gde se terminali međusobno povezuju, a papirnate transakcije kompjuterizuju; **3)** sve se više pojavljuju industrije bazirane na transakcijama i uslugama vezanim za podatke i aktivnostima izrazito komunikacionog karaktera; **4)** tehnološka dostignuća sve više poboljšavaju komunikacione mogućnosti i smanjuju troškove međunarodnog prenosa podataka; **5)** sve su značajnija dostignuća u mogućnostima usluga vezanih za podatke i telekomunikacije, što značajno utiče na poboljšanje prekogranične trgovine mnogih transnacionalnih usluga, koje se sve više baziraju na mrežama.

### 3.1.6. *Smernice koje se odnose na kompjuterizovana dosijea podataka*

Ujedinjene Nacije su, nakon višegodišnjih praćenja i analiziranja stanja vezanog za zaštitu, 14 decembra 1990. godine na zasjedanju Generalne skupštine donele **Smernice koje se odnose na kompjuterizovana dosijea podataka** (*Guidelines concerning Computerized Data Files*)<sup>121</sup>.

Smernice predstavljaju jedan od osnova za harmonizaciju nacionalnih zakonodavstva u regulisanju zaštite podataka o ličnosti.

Posebno su značajni **principi**<sup>122</sup> koje svaka zemlja članica treba da ugradi u svoje propise. To su:

- **princip zakonitosti i nepristrasnosti** pretpostavlja da se podaci o ličnosti ne smeju prikupljati ili obrađivati na nezakonit ili pristrasan način, naročito ne na način i za ciljeve koji su protivurečni načelima Povelje OUN;

<sup>120</sup> Trgovina informacionim, kompjuterskim i komunikacionim uslugama - Ispitivanje relevantnosti pojmovnog okvira za trgovinu uslugama, dokument DST/ICCP/86.21

<sup>121</sup> Resolution no. 45/75 OUN

<sup>122</sup> Kavran D., Pravo i regulacija zaštite podataka u informacionim sistemima, I stručni skup: Zaštita podataka u računarskim sistemima, Beograd, Savez inženjera i tehničara Srbije, 1995., str. 224; Marković N., Zaštita ličnih podataka, I stručni skup: Zaštita podataka u računarskim sistemima, Beograd, Savez inženjera i tehničara Srbije, 1995., str. 261 - 263.

- **princip tačnosti** osigurava da se podaci o ličnosti u kompjureizovanim dosijeima mogu naći samo ako su tačni, relevantni i kompletni a da bi se to i ostvarivalo nužna je provera, i to redovna;
- **princip tačno utvrđene svrhe** vezuje se za obavezu da se pre nego što počne prikupljanje i obrada podataka utvrde namene za koje će se to raditi;
- **princip dostupnosti** je istovremeno i pretpostavka za primenu ostalih principa, i znači da svaki pojedinac, uz odgovarajuću dokumentaciju, ima pravo da dobije informaciju o podacima koji se o njemu vode i pravo uvida, bez posebnih troškova, ako zahteva;
- **princip nediskriminacije**, odn. neizdvajanja, znači da se ne smeju prikupljati, niti koristiti, podaci koji mogu izazvati nezakonite i proizvoljne diskriminacije po rasi, etničkom i socijalnom poreklu, boji, seksualnom životu, političkom uverenju, verskim i sličnim ubedjenjima, pripadnosti sindikatu ili drugim udruženjima;
- **princip posebnog odobrenja za izuzimanje** treba da obezbedi da se odstupanja od ovih principa mogu tolerisati samo ako su posebno i izričito predviđena zakonima ili propisima koji se javno donose. Ta izuzeća su, po pravilu, vezana za nacionalnu bezbednost, javni red i mir, zdravlje, javni moral, i sl;
- **princip sigurnosti** treba da omogući zaštitu baza podataka o ličnosti, naročito od prirodnih opasnosti, ali i upada, neovlašćenog pristupa, zloupotrebe podataka ili kompjuterskih virusa;
- **princip uređivanja prekograničnog toka** ovih podataka mora da omogući nesmetan TDF podataka o ličnosti;
- **princip nadzora** predviđa da se u svakoj zemlji imenuje organ koji će biti ovlašćen i nadležan za kontrolu i praćenje primene svih ovih principa. Kontrola ne bi imala smisla ukoliko nije nepristrasna i nezavisna, a to znači da i organ koji vrši ovu funkciju mora imati takav status, osobito u odnosu na organe uprave, lica i agencije koje su odgovorni za obradu podataka<sup>123</sup>. Za povrede ovih principa ili prava koje ima pojedinac, nacionalna zakonodavstva su obavezna da predvide kaznene mere.

Smernice UN predstavljaju značajan korak u pogledu obaveza država da zaštite privatnost i podatke o ličnosti jer su neke zemlje radje izabrale put koji ne vodi toj zaštiti i obezbedjenju ostvarivanja tih prava.

<sup>123</sup> Što nije prihvaćeno u Predlogu zakona, po kome je to u nadležnosti Saveznog ministarstva nadležnog za poslove pravde.

### 3.1.7. *Direktiva o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i slobodnom kretanju takvih podataka*

Donošenjem Evropske Konvencije i Preporuke za njeno usvajanje<sup>124</sup> nisu se završile aktivnosti vezane za zaštitu podataka i ličnosti, već se u zemljama članicama Evropske Zajednice donose odgovarajući pravni akti kojima se sa njom usaglašava nacionalno pravo. To, ipak, ne teče savršeno sinhronizovano zbog razlike u pristupu. Dok je jednoj grupi zemalja, Belgija, Portugal, Španija, bilo potrebno desetak godina za donošenje odgovarajućeg nacionalnog propisa, dotle su druge, V. Britanija, reagovala brzo prihvatajući Konvenciju kao grubi okvir za sopstvena rešenja. Treća grupa zemalja, Nemačka, detaljno razrađuje koncept zaštite stavljajući interes pojedinca ispred interesa korisnika. Naravno, pojavljuje se i četvrta grupa zemalja, Grčka i Italija, koje uopšte ne donose nikakve akte, te materiju zaštite ostavljaju “nepokrivenu”<sup>125</sup>. U takvoj situaciji odgovarajuća tela i komisije Evropskog saveta, pokušavajući da nadju rešenje, počinju pripremu za donošenje posebne Direktive kojom bi se umanjili problemi u harmonizaciji i olakšao transfer podataka unutar Zajednice, ali i uspostavila pravila transfera. Tako postepeno dolazi do prve verzije Direktive koja se 1990. godine objavljuje i dostavlja parlamentima zemalja članica na razmatranje. Ta verzija je pretrpela brojne kritike i zahteve za dopune i izmene, što je predstavljalo inicijalni korak u izradi nove verzije. Revidirana verzija biva objavljena 1992. godine i ne prolazi baš najbolje u javnim raspravama. Zato se pristupa izradi i treće, finalne, verzije, koja nakon dvogodišnje rasprave biva razmatrana na Evropskom Savetu u februaru 1995. godine, da bi oktobra bila usvojena od strane Evropskog Parlamenta i Saveta. Poštujući obaveze koje po Mاستrihtskom ugovoru imaju, ministri zemalja članica obaveštavaju svoje vlade i parlamente o njenom donošenju uz predloge nacionalnih akcija u sprovođenju. Plan akcija, pored konkretnih mera koje treba u propisanim rokovima da se preduzmu u odnosu na uskladjivanje nacionalnih propisa sa Direktivom, obuhvata i predviđanje finansijskih sredstava za implementaciju, koja, kako se očekuje, neće biti mala (npr. po proceni Ministra pravde Holandije to je 25 - 50 miliona guldena samo za tu zemlju).

Usvojena **Direktiva o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i slobodnom kretanju takvih podataka**<sup>126</sup>(*Directive on the protection of individuals with regard to the processing of personal data and free movement of such data*) ima 34 člana grupisanih u sedam glava.

<sup>124</sup> Recommendation to Member States OJ. 1981. L 246/31.

<sup>125</sup> Wiebe A., Harmonization of Data Protection Law in Europe, Report on the Working Conference of the EC Data Protection Directive, Hanover, 1996., dokument preuzet sa Interneta.

<sup>126</sup> Official Journal of the European Communities, no. L281. iz 1995.

U **prvoj, uvodnoj, glavi**, osim predmeta Direktive date su i definicije, kao i domašaj i primena na nacionalna prava. Najznačajnije u ovom delu su, svakako, definicije osnovnih pojmova počevši od podataka o ličnosti, preko obrade podataka, sistema dosijea, kontrolora, procesora (obradjivača) podataka, treće strane, pa do korisnika i pristanka subjekta podataka. U svim tim odredjenjima najznačajnije je da pod **podacima o ličnosti** (*personal data*) **podrazumeva svaka informacija koja se odnosi na identifikovanu ili osobu (data subject) koja može biti identifikovana, direktno ili indirektno, a posebno na osnovu indentifikacionog broja ili na osnovu nekog drugog faktora specifičnog za njen fizički, psihički, mentalni, ekonomsk ili socijalni identitet**<sup>127</sup>.

Drugo odredjenje koje je izuzetno bitno je **obrada podataka** (*data processing*) pod kojom se podrazumeva **jedna ili skup operacija koje se na podacima o ličnosti obavljaju, bile one automatske ili ne, a koje su: prikupljanje, unošenje, organizovanje, skladištenje, adaptiranje, pretraživanje, dogovaranje, korišćenje ili pokazivanje transmitovanjem, diseminacijom ili na bilo koji drugi način činjenjem raspoloživom, ili blokiranje, brisanje ili uništavanje**.

Osim ovih daju se i ostale definicije, manje ili više već ugrađene u nacionalne zakone o zaštiti podataka<sup>128</sup>, a u Direktivi se odredjuje i da se ona neće primenjivati na podatke o ličnosti koji su u domenu javne sigurnosti, odbrane, državne sigurnosti, aktivnosti država u oblasti krivičnog prava, kao ni na podatke čiju obradu obavlja fizičko lice za čisto privatne aktivnost<sup>129</sup>.

**Druga glava**, inače i najopširnija, obuhvata opšta pravila legitimnosti obrade podataka i u devet odeljaka razmatra principe kvaliteta podataka, posebne kategorije obrade, prava subjkata podataka, izuzeća i ograničenja, poverljivost i sigurnost obrade, kao i objavljivanje.

Direktiva ističe pet osnovnih principa legitimnosti obrade:

- **poštena i zakonita obrada;**

<sup>127</sup> Direktiva, čl. 2 (a).

<sup>128</sup> Zanimljivo je da su nakon donošenja Direktive najeminentniji stručnjaci i nacionalna tela svake zemlje članice sačinili komparativnu analizu razlika i sličnosti njenih odredbi sa odredbama nacionalnih zakona. Takođe, neke od zemalja pozvale su, do određenog roka, sva zainteresovana lica da se uključe u raspravu o Direktivi u kontekstu nacionalnih propisa (npr. preko Interneta u V. Britaniji su pozvani svi zainteresovani da do 16. jula 1996. učine predloge ili dostave vidjenje daljeg usaglašavanja Zakona o zaštiti podataka sa Direktivom. U tom pozivu dati su i detaljni prikazi oba akta).

<sup>129</sup> Direktiva, čl. 3. paragraf 2.

- *prikupljanje za određene, eksplicitne i opravdane, svrhe* i obradivanje inkompatibilno tim svrhama;
- *adekvatnost podataka, relevantnost i ograničenost u broju* u skladu sa svrhama za koje su prikupljeni i/ili budućim svrhama;
- *tačnost* i, ukoliko je potrebno, svakodnevna *ažurnost*;
- *oblik koji dozvoljava identifikaciju subjekta podataka samo u intervalu koji je nužan za ostvarivanje svrhe* (sadašnje ili buduće), a ako su u pitanju istorijske, statističke ili naučne svrhe tada ih je moguće čuvati i duže ali samo uz odgovarajuću zaštitu.

Kao prava pojedinaca pojavljuju se, naročito: **1) pravo na obaveštenost**; **2) pravo pristupa**; **3) pravo na prigovor**; i **4) pravo na javnost operacija obrade**.

Direktiva posebno određuje obavezu država članica da zabrane obradu podataka o ličnosti koji odaju rasno ili etničko poreklo, politička uverenja, religijska i psihofizička ubedjenja, članstvo u sindikatu, kao i podataka koji se odnose na seksualni život i zdravlje. Ovi se podaci, ipak, mogu, u strogo propisanim uslovima, obradivati, npr. samo ako subjekt da svoj izričiti pristanak ili ako je obrada neophodna radi zaštite njegovih vitalnih interesa<sup>130</sup>.

**Treća glava** obuhvata tri člana i vezana je za sudske lekove, odgovornost i sankcije. U njoj je posebno važan član koji se odnosi na obavezu država članica da usvoje odgovarajuće mere obezbeđenja potpune primene odredbi Direktive i da posebno predvide sankcije u slučajevima njene povrede.

Transfer podataka o ličnosti u treće zemlje je sadržaj **četvrte glave** i posebno je značajan jer ga Direktiva dozvoljava ali samo ako te zemlje, u odnosu na osiguranje i adekvatni stepen zaštite ovih podataka, sa njom usklade svoja nacionalna zakonodavstva. Zato će treće zemlje saradivati sa Komisijom EZ, a ako ona utvrdi neadekvatnost zaštite onda države članice mogu preduzeti neophodne mere da zaštite svaki transfer.

U **petoj glavi** određuje se sistem sprovođenja i predviđaju obaveze država članica da u nacionalno zakonodavstvo implementiraju odredbe ove Direktive.

---

<sup>130</sup> Direktiva, čl. 8.

**Šesti deo**, odn. šesta glava propisuje ovlašćenja supervizora predviđajući da to može biti jedan ili više javnih organa u svakoj državi članici koji su obavezni da na svojoj teritoriji posmatraju primenu odredbi koje se donose na osnovu Direktive. Supervizor je, po odredbama Direktive, potpuno nezavistan u radu. Članovi i zaposleni imaju obavezu čuvanja u toku rada i nakon završetaka, kao profesionalne tajne, svih poverljivih podataka do kojih su došli u toku rada. Ipak, najvažnija su ovlašćenja koja ima supervizor, a to su<sup>131</sup>:

- ovlašćenje za istragu;
- ovlašćenje za intervenciju;
- ovlašćenje za učešće u pravnim postupcima.

Posebno se u okviru ovog dela razradjuju ovlašćenja i obaveze **Radnog tela za zaštitu pojedinaca** u odnosu na obradu podataka o ličnosti, a koje je savetodavno, nezavisno, telo sasatvljeno od predstavnika supervizora koje predloži svaka država članica, predstavnika jednog ili više organa vlasti iz Zajednice kao institucije ili tela i predstavnika Komisije. Ovo telo donosi odluke prostom većinom, a može:

- **ispitivati** svako pitanje koje pokriva primenu nacionalnih mera usvojenih na osnovu Direktive, pri čemu može i propisati jednobraznost primene;
- **davati mišljenje** Komisiji o nivou zaštite u Zajednici i trećim zemljama;
- **savetovati** Komisiju ukoliko su predloženi amandmani na Direktivu;
- **davati mišljenje** o nivou zakona u Zajednici.

Ovo telo može davati i preporuke koje razmatraju Komisija i Komitet, a ponekad i Evropski Parlament i Savet. Obavezno je da sastavi i objavi godišnji izveštaj o situaciji vezanoj za zaštitu pojedinaca u Zajednici i trećim zemljama<sup>132</sup>.

Naravno, **poslednji deo** su završne odredbe, kojima se određuje u kom periodu će zemlje članice morati uskladiti nacionalna zakonodavstva sa Direktivom. Po članu 32 taj period je 3 godine od dana njenog usvajanja. Izuzetak je ručna obrada podataka za koju se određuje usklađivanje u roku od 12 godina od dana usvajanja Direktive.

I na kraju nužno je konstatovati da ova Direktiva<sup>133</sup>:

---

<sup>131</sup> Direktiva, čl. 28.

<sup>132</sup> Direktiva, čl. 30.

**Prvo. Menja koncept zaštite,** prevazilazeći “statični koncept” zaštite podataka koji se nalaze u dosijeima u korist “dinamičnog koncepta” obrade podataka o личности bilo gde se oni nalazili.

**Drugo. Prevazilazi uske okvire** kompjuterizovanih, automatskih obrada, obuhvatajući i manuelne obrade, kojima se, takodje, mogu ugroziti prava pojedinaca na privatnost i informacionu privatnost.

**Treće. Pretenduje da obuhvati i privatni i javni sektor,** brišući značaj njihovih razlika u odnosu na značaj koje ima pravo privatnosti i zaštita pojedinaca.

**Četvrto. Daje državama članicama izvesne slobode u regulaciji,** kao što je i mnogo fleksibilnija u odnosu na nacionalne propise, pogotovo kad je u pitanju transfer podataka o личности unutar EU i između nje i trećih zemalja.

**Peto.** Teži da se zaštita prava uskladi sa slobodama личности, da se obezbedi ekvivalentni nivo zaštite u svim zemljama članicama, da se još više osigura harmonizacija prava naročito u primeni novih tehnologija, da se omogući postojanje izuzeća, ali samo pod tačno propisanim uslovima i kriterijumima, i naravno, *da se prevaziđu okviri zajednice i određeni principi “protegnu” na treće zemlje prema kojima i u kojima teče transfer podataka o личности iz Zajednice*<sup>134</sup>.

**Šesto. Može imati poseban značaj za našu zemlju** zbog transfera podataka i neophodnosti uskladjivanja našeg zakonodavstva sa njom. Tim više, što mi još uvek nemamo odgovarajuće propise vezane za ovu zaštitu.

### 3.1.8. Evropski Model EDI Sporazuma

Komisija EU o pravnim aspektima EDI, zbog sve veće zainteresovanosti zemalja članica za rešavanje pitanja iz EDI, kao i sve veće nužnosti da se definišu potrebe i uslovi za međusobno poslovanje stranaka, donela je 1994. godine

<sup>133</sup> Brum, Implementation of European Data Protection Directive: The View from Denmark; Karspersen, EC Data Protection Directive, Impact on Dutch Data Protection Law; Clark, Data Protection in Republic Ireland; Comments on the EC Data Protection Directive: The View from Sweden; Lloyd I., Introduction to the Data Protection Special Feature; Reports on the Working Conference of the EC Data Protection Directive, Hanover, 1996., dokumenti preuzeti sa Interneta.

<sup>134</sup> Recitals the European Parliament and the Council of European Union.

**Preporuku Evropskog Modela EDI sporazuma** (*Commission Recommendation of European Model EDI Agreement*)<sup>135</sup>, ne bi li se na jedinstven način regulisale ugovorne obaveze koje proizilaze iz osnovnih transakcija u kojima je korišćen EDI.

Model sporazuma<sup>136</sup> ima samo 14 članova, kojima može biti pridodat, još, i aneks vezan za Tehnički dodatak.

Definicije značenja osnovnih termina date su članom 2. Posebno su definisani pojmovi EDI, EDI poruke, UN/EDIFACT i potvrde prijema.

Što se **bezbednosti poruka** tiče stranke se obavezuju da primenjuju postupke i mere bezbednosti kojima će se osigurati odgovarajuća zaštita poruka. Zaštita je od rizika neovlašćenog pristupa, izmene, uništenja ili gubitka. Bezbednost obuhvata, prevashodno: proveru porekla; proveru integriteta; neodbacivanje porekla, kao i proveru prijema i poverljivosti<sup>137</sup>.

**Poverljivost i zaštita podataka o ličnosti** pretpostavlja sporazumevanje strana oko korišćenja posebnih oblika zaštite za određene poruke (kriptografisanje), ako je to njihovim pravima dozvoljeno. Zaštita podataka o ličnosti obavljaće se u skladu sa zakonima zemalja strana u sporazumu, naravno, ukoliko takvih zakona nema, kao minimum poslužiće Konvencija Saveta Evrope o zaštiti pojedinaca u odnosu na automatsku obradu podataka o ličnosti.

Sam Sporazum pored bezbednosti poruka i zaštite podataka o ličnosti i poverljivosti, predlaže regulisanje, ugovorom, **dostupnost podataka kao dokaza** (ovaj je problem rešen tako što se ugovorne stranke obavezuju, u skladu sa zakonom, da će u slučaju spora sudu učiniti dostupnim podatke, a da će poruke predstavljati dokaz o činjenicama koje su navedene), **operativnih zahteva** (osnovni zahtevi vezani su za opremu za rad, sredstva komunikacija, standarde poruka i kodove), **tehničkih specifikacija i zahteva** (koje će biti obuhvaćene Tehničkim dodatkom, a tiču se zahteva za operacionalizaciju, obradu i potvrdu poruka, njihovo

<sup>135</sup> Official Journal of the European Communities, no. L338/98 iz 1994.

<sup>136</sup> Vilus J., Evropski model EDI sporazume, (prevod), Yu EDI Forum, br. 2/94, str. 5 - 8.

<sup>137</sup> Zanimljivo je da se problem sigurnosti EDI naročito mnogo razmatra u okviru Ekonomske komisije za Evropu, Ekonomskog i socijalnog Saveta UN. Tako je jula 1994. u dokumentu, EWOS, Technical Guide (ETG) on EDI, u nekoliko delova raspravljano o ovom i pravnim pitanjima, WP. TRADE 4/R. 1089., od 22. jula 1994.

zasnivanje i skladištenje, zaštitu, zastarelost i ispitivanje, postupaka ispitivanja, i sl.), i **odgovornosti** strana Sporazuma. Posebno se regulišu slučajevi oslobađanja od odgovornosti kad šteta nastane docnjom, izostavljanjem ili greškom, kao i za štetu ili gubitak kad su docnja ili propust nastali van kontrole te stranke, a za koju nije moglo "razumno" da se očekuje da će nastupiti. Ukoliko se, pak, jedna strana opredeli da angažuje posrednika za obavljanje usluga prenosa, upisivanja ili obrade, pa nastane šteta, tada će ona odgovarati za štetu koja je nastala kao direktna posledica radnje, greške ili propusta. To će se desiti i strani koja od druge strane zahteva učešće posrednika za transmisiju, pa nastane šteta.

U slučaju da dodje do **spora** između strana potpisnica one mogu izabrati jednu od dve ponudjene alternative: arbitražu ili primenu odredbe o klauzuli nadležnog suda. Takođe, strane će se dogovoriti koje će pravo biti merodavno u slučaju obrade i skladištenja zaštite ili poverljivosti podataka o ličnosti.

Naravno, nikako se ne smeju zanemariti rešenja predviđena za **tretman zapisivanja i skladištenja poruka**. Tako, predviđa se da kompletan i hronološki zapis svih poruka, koje se nalaze u razmeni između strana trgovačke transakcije, moraju biti sačuvani i to neprepravljene i obezbeđene, u zakonom, predviđenim periodima. Taj period ne sme biti kraći od 3 godine. Samo skladištenje vrši u odredjenom formatu zavisno koja je strana u pitanju: pošiljalac u formatu u kom je dostavljena, a primalac u formatu u kom je primljena. Elektronski i računarski zapisi moraju biti lako dostupni i mora se obezbediti da budu reprodukovani u ljudski čitljivoj formi. To znači da se neće tretirati opravdanja u smislu "više ne postoji takva oprema".

### 3.2. *Nacionalni instrumenti*

Nacionalni pravni sistemi na različite načine, pravnim mehanizmima i merama, koje im stoje na raspolaganju, pokušavaju da regulišu zaštitu podataka i subjekata. Dok jedne zemlje ignorišu postojanje ovog problema te njihovi pravni sistemi "ćute" o tome, dotle druge zemlje, sa jednim ili više pravnih akata, manje ili više detaljno, regulišu ovo pitanje. Treće zemlje imaju specifične sisteme, pa samim tim i specifične instrumente. Znači, postoje veoma velike različitosti između nacionalnih rešenja i instrumenata kojima se ovi problemi žele rešiti. No, i pored svih razlika mogu se uočiti i određene sličnosti. Svakako da je jedna od najvažnijih da su sve one zemlje koje iole drže do sopstvenog razvoja, ili žele da ga postignu, donele ili su u fazi donošenja odgovarajućih pravnih akta kojima se regulišu ova pitanja. Takođe, nije slučajno da upravo te zemlje koje su donele ili donose odgovarajuće pravne akte vezane

za zaštitu podataka i subjekata, pokušavaju, manje ili više uspešno, da medjusobno sarađuju i pružaju jedne drugima određene usluge na tom planu.

**Hronološki** posmatrano najznačajniji **nacionalni propisi** donošeni su po sledećem redosledu:

#### Hronologija nacionalnih aktivnosti

| Godina | Država            | Nacionalni propis  |
|--------|-------------------|--|
| 1969.  | V. Britanija      | Zakon o nadzoru podataka (donet i odmah stavljen van snage)                      |
| 1970.  | Hese (SR Nemačka) | Zakon o zaštiti podataka   |
| 1973.  | SAD               | Zakon o poštenim postupcima pri kreditiranju                                     |
| 1973.  | Švedska           | Zakon o zaštiti podataka   |
| 1974.  | SAD               | Akt o privatnosti  |
| 1974.  | Minesota          | Zakon o privatnosti  |
| 1976.  | Kanada            | Zakon o ljudskim pravima   |
| 1977.  | SAD               | Izveštaj Komisije vezan za o zaštiti privatnosti                                 |
| 1978.  | Francuska         | Zakon o informatici, evidencijama i slobodama                                    |
| 1978.  | Danska            | Zakon o javnim evidencijama  |
| 1978.  | Danska            | Zakon o privatnim evidencijama   |
| 1978.  | Austrija          | Zakon o zaštiti podataka   |
| 1978.  | SAD               | Zakon o pravima na finansijsku privatnost  |
| 1978.  | Norveška          | Zakon o zaštiti podataka   |
| 1979.  | SR Nemačka        | Zakon o zaštiti od zloupotrebe podataka o ličnosti pri obradi podataka           |
| 1979.  | Luksemburg        | Zakon o označavanju osoba  |
| 1979.  | Luksemburg        | Zakon o zaštiti podataka   |
| 1980.  | SAD               | Zakon o zaštiti privatnosti  |
| 1980.  | SAD               | Zakon o poštenim postupcima sa podacima  |
| 1981.  | Island            | Zakon br. 03. koji se odnosi na sistematsku evidenciju podataka o ličnosti       |
| 1981.  | Izrael            | Zakon o zaštiti privatnosti  |
| 1982.  | Kvebek            | Zakon br. 65. koji se odnosi na zaštitu podataka u javnom sektoru                |
| 1982.  | Kanada            | Zakon o privatnosti  |
| 1983.  | New York          | Zakon o zaštiti privatnosti  |
| 1984.  | Švajcarska        | Nacrt Zakona o zaštiti podataka  |
| 1984.  | V. Britanija      | Zakon o zaštiti podataka (više puta u toku primene revidiran)                    |
| 1984.  | SR Nemačka        | Revizija Zakona o zaštiti od zloupotrebe podataka o ličnosti pri obradi podataka |
| 1984.  | Japan             | Smernice za administrativnu reformu  |
| 1986.  | Ostrvo Man        | Zakon o zaštiti podataka   |
| 1987.  | Džersi            | Zakon o zaštiti podataka   |
| 1988.  | Australija        | Zakon o privatnosti  |
| 1988.  | Republika Irska   | Zakon o zaštiti podataka (stupio na snagu 1989.)                                 |
| 1989.  | Holandija         | Zakon o zaštiti podataka   |
| 1991.  | Portugalija       | Zakon o zaštiti podataka o ličnosti  |

|       |                     |   |
|-------|---------------------|---|
| 1992. | Belgija             | Zakon o zaštiti podataka o ličnosti   |
| 1992. | Španija             | Zakon o zaštiti podataka o ličnosti   |
| 1992. | Mađarska            | Zakon o zaštiti podataka o ličnosti   |
| 1992. | Češka               | Zakon o informacionom sistemu   |
| 1992. | Slovačka            | Zakon o zaštiti podataka o ličnosti   |
| 1992. | Rumunija            | Nova verzija zakona o zaštiti podataka  |
| 1994. | SR Jugoslavija      | Prva verzija Predloga zakona o zaštiti ličnosti   |
| 1995. | SR Jugoslavija      | Druga verzija Predloga zakona   |
| 1996. | Republika Srbija    | Zakon o informacionom sistemu Republike Srbije  |
| 1996. | SR Jugoslavija      | Predlog zakona o zaštiti podataka o ličnosti (ponovo razmatran na Saveznoj Skupštini i odložen do daljnjeg) |
| 1996. | Republika Crna Gora | Počela priprema Zakona o informacionom sistemu Republike Crne Gore  |
| 1996. | Zemlje EU           | Počele pripreme u svim zemljama EU za uskladjivanje nacionalnih zakona sa Direktivom                        |

Sem nacionalnih instrumenata vezanih za zaštitu privatnosti ili podataka o ličnosti sve je veći broj zemalja koji u njih, naročito akte o zaštiti podataka, unose i zaštitu podataka u TDF. Osim podataka o ličnosti i zaštiti pojedinaca, mnoge su zemlje predvideli i zaštitu poverljivih podataka, regulišući ih kroz zaštitu poslovne tajne. Ni zaštita podataka u EDI ne ostaje po strani. Sve veći broj zemalja uvodi EDI, mada, za sada, pravni instrumenti zaštite još uvek nedostaju.

Ako bi se imala u vidu **vrsta pravnih akata** kojima se štite različite vrste podataka po različitim zemljama moralo bi se istaći sledeće:

**A. Zemlje u kojima je regulisana zaštita podataka o ličnosti i privatnosti** donele su:

**a)** pravne akte većinom u formi **zakona**. Neke zemlje zaštitu subjekata i podataka o ličnosti posebno regulišu i u **ustavima** (Španija, Portugalija, Bugarska, Slovačka), dok druge ustavnim odredbama samo načelno dodiruju ova pitanja (SRJugoslavija, R Srbija). Zemlje koje su zakonima regulisale zaštitu podataka i subjekata učinile su to:

- ♦ **posebnim zakonima** (*lex specialis*) kojima je jedini i osnovni predmet regulisanja ova zaštita, bilo da se radi o zaštiti privatnosti, bilo o zaštiti subjekata, bilo i jedno i drugo;
- ♦ **posebnim odredbama u zakonima** kojima je predmet nešto drugo (npr. krivični zakoni, trgovački zakonici);

- ♦ **celim sistemom zakona** koji jedni druge dopunjuju (npr. SAD) tako da predstavljaju jedinstvenu celinu u regulisanju većine pitanja koji se u vezi sa zaštitom pojavljuju.

**b) posebnim pravnim aktima** - podzakonskim aktima koji mogu imati obavezu snagu (odluke, uredbe, naredbe) i kojima se regulišu određena (konkretna) pitanja vezana za problem zaštite;

**c) posebnim aktima** (npr. Pravilnikom o zaštiti i upotrebi podataka u kompjuterizovanim informacionim sistemima, 1986, Japan) koje nisu donela zakonodavna tela, već **organi uprave**.

**B.** Zemlje koje su donele posebne pravne akte o **zaštiti organizacija i poverljivih podataka** uradile su to:

- a)** zakonom najčešće o preduzećima, korporacijama, kompanijama (SRJ, V. Britanija);
- b)** zakonom o nelojalnoj konkurenciji (Japan);
- c)** zakonom o poslovnoj tajni (SAD).

**C.** Zemlje koje su regulisale pitanja **zaštite podataka u međjugraničnim tokovima podataka** uradile su to pravnim aktima:

- a)** o zaštiti podataka o ličnosti (većina novih zakona);
- b)** posebnim zakonima (što je retko).

**D.** Što se tiče regulacije pitanja **zaštite podataka u EDI** gotovo su sve zemlje, za sada, izbegle posebno zakonsko regulisanje i prepustile ugovorima izmedju pojedinačnih strana.

Dakle, pošto je najzastupljenija zaštita podataka o ličnosti i privatnosti, to se većinom pravnih akta regulišu pitanja zaštite ovih podataka i subjekata. Njihove bitne i **zajedničke karakteristike**<sup>138</sup>, su:

**Prvo.** Većina zakona koja se odnose na zaštitu podataka odnose se na **zaštitu podataka i u privatnom i u javnom sektoru** i to, po pravilu, na IS koji imaju

---

<sup>138</sup> Lilić S., op. cit., str. 109 - 130.

*automatsku obradu podataka* (izuzetak je Švajcarska koja proširuje zaštitu i na podatke koji se ručno obrađuju, kao i Predlog zakona o zaštiti podataka o ličnosti SRJ).

**Drugo.** Svi zakoni imaju za cilj da zaštite određene interese (društvene, javne, privatne) koji se može ugroziti prikupljanjem, obradom ili korišćenjem određenih podataka. Razlike postoje između zakona koje donose *evropske zemlje* i u kojima je, po pravilu, objekt zaštite *opšti interes*, od *zemalja Common Law sistema* u kojima je primarni objekt *privatni* (izuzeci postoje i u jednoj i u drugoj grupi, mada nisu tipični).

**Treće.** Većina zakona sadrži odredbe o dopuštenosti obrade podataka, načelima, postupcima i metodama prikupljanja i načinima korišćenja. Tako, postoje razlike kad je u pitanju dopuštenost obrade podataka - *zakoni jedne grupe* zemalja predviđaju *dozvole*, kao mogućnost da subjekti koji žele da prikupljaju i obrađuju podatke do njih i dodju (Švetska, Francuska). Po *drugoj grupi zakona* dovoljno je da se subjekti koji se bave obradom podataka registruju, odn. upišu u odgovarajuće evidencije i koje vode, zakonom predviđeni, organi (SRJ po Predlogu Zakona, Švajcarska, V. Britanija, Austrija). U takvim zakonima propisuje se forma i sadržaj zahteva za upis u registre.

Načela, postupak i način obrade i korišćenja, po pravilu, su u gotovo svim zakonima *usklađeni sa odgovarajućim međunarodnim aktima*, s tim što je neophodno da se ispuni bar jedan od tri predviđena uslova. Prvi je vezan za prikupljanje i obradu onih podataka za koje postoje izričita, zakonom određena, ovlašćenja nadležnog subjekata. Drugi je ako to proizlazi iz zakonom utvrdjenih nadležnosti subjekata, a treći ako postoji saglasnost subjekta na koji se podaci odnose. Postojanje i zahtev za ispunjenje ovih uslova u većini zakona predstavlja način da se spreče zloupotrebe u prikupljanju i obradi podataka, kao i u načinima njihovog korišćenja.

**Četvrto.** *Gotovo svi zakoni predviđaju koja prava imaju subjekti na koje se podaci odnose*, bilo da su pravna ili fizička lica. Posebno se *decidirano određuju ta prava kad su u pitanju fizička lica*.

**Peto.** Izuzimajući SAD, Kanadu, SR Jugoslaviju, *svi zakoni predviđaju konstituisanje posebnih organa koji vrše nadzor nad zaštitom podataka*. Sastav, nadležnost, status ovih organa može biti od zemlje do zemlje različiti, ali je bitno njihovo postojanje. U suštini su se do sada iskristalisala dva shvatanja. *Po jednom* efikasnost kontrole (nadzora) moguća je samo onda ako nadzorni organ ima praktično

neograničeni pristup podacima koji se koriste i na osnovu "štih proba" ispitujući njihov sadržaj, tačnost, način korišćenje, svrhu prikupljanja i korišćenja. **Drugo shvatanje** negira valjanost "štih proba" i smatra da je neophodno koristiti metode statističkih uzoraka i nasumični izbor sa neograničenim pristupom izabranim podacima. Bez obzira koje je shvatanje prihvaćeno neophodno je istaći da ovi organi imaju relativno **veliku samostalnost u radu i da se** (bilo da su kolegijalni ili individualni) **od lica koja ulaze u njihov sastav zahteva izuzetna stručnost** (pravna i informatičarska).

**Šesto. Većina zakona predviđa izuzetke za određene grupe podataka** koji zbog toga ne podležu odredbama ovih zakona. Izuzeci su sa, većim ili manjim, odstupanjima skoro identični sa izuzecima predviđenim u Evropskoj konvenciji ili Evropskoj direktivi.

**Sedmo. Svi zakoni predviđaju i određene sankcije za kršenje njihovih odredbi.** Sankcije su kazne zatvora i novčane, koje su, po pravilu, vrlo visoke (kod nas između 5.000 i 50.000 za pravna lica, i 300 i 3.000 za ovlašćene u njima), kao i zabrana obavljanja delatnosti u određenom trajanju (kod nas to može biti od 3 meseca do jedne godine). Pored toga, lica čija su prava prikupljanjem, obradom i korišćenjem podataka ugrožena ili su zbog toga pretrpeli nekakvu štetu (moralnu ili materijalnu) mogu, redovnim sudovima u građansko-pravnim sporovima, podneti zahtev (tužbu) za naknadu.

**Osmo.** Iako se direktno ne tiče osobenosti zakona ipak je neophodno istaći **da su se skoro sve zemlje vrlo studiozno i dugotrajno prethodno za to pripremile.** Priprema se sastojala od formiranja odgovarajućih stručnih tela (komisija, radnih grupa i sl.) koja su kvalifikovano prikupljala potrebne podatke i izradjivala obimne, stručne studije i izveštaje (često podnošene i usvajane od najviših instanci organa vlasti - uprave ili, čak, skupštine) u kojima su se definisali okviri za analiziranje sistema zaštite, uključujući i definisanje interesnih krugova i analizu interesnih grupa i njihovih potreba u odnosu na zaštitu određenih prava. I ne samo to, nego su pored nacionalnih studija izradjivane i međunarodne studije (uporedne analize) kako bi se našla najbolja rešenja i ona uskladila između više zemalja (npr. Britanski nacionalni računski centar i njegovi nemački i francuski pandani uradili su zajedničku studiju o tajnosti podataka za EEZ). Pored njih su, čak, i velike nacionalne kompanije za proizvodnju i distribuciju opreme i podataka formirale svoje radne grupe i tela i na osnovu internih studija nudili odgovarajuća rešenja zakonodavnim telima svoje zemlje. Mnogi od ovih predloga bili su usvojeni i razradjeni u nacionalnim zakonima (npr. *International Computers Limited* - *ICL*, britanska organizacija za proizvodnju kompjutera sastavila je radnu grupu od svojih korisnika i dala joj zadatak da istraži sredstva za zaštitu i osiguranje. Radna grupa je izradila određene preporuke koje su postale standardi i modifikovani se ugradili kao

principi u odgovarajuće zakonske odredbe). Danas je situacija još povoljnija jer su mnoge zemlje prihvatile obavezu godišnjeg izveštavanja o stanju vezanom za zaštitu, kao i međusobnog izveštavanja i obaveštavanja o tome.

**Devet. Posebna pažnja posvećuje se pristupu podacima koje se nalaze pri vladama ili javnim telima.** Razlike koje se među zemljama pojavljuju oko realizacije ovog prava posledica su razlike u pristupu, odn. da li se štiti javni ili individualni interes. Zemlje kao što su Danska, Holandija, Švedska, Grčka, Francuska, Norveška, SAD, Kanada uspostavljaju pravo opšteg pristupa vladinim informacijama jer prevashodno štite individualni interes pojedinaca<sup>139</sup>.

Pošto i ostali podaci i subjekti, takodje, zahtevaju zaštitu, a ona baš nije razvijena, to se ove karakteristike mogu odnositi, sa određenim modifikacijama, i na njih.

### 3.3. *Instrumenti našeg prava*

Nalazimo se u pravnom haosu. Naime, naš pravni sistem, doživeo je značajne promene u poslednjih nekoliko godina. Prevashodno su na to uticali Ustavi (Savezni i republički), Ustavni zakon za sprovođenje Ustava SRJ<sup>140</sup> i drugi pravni akti, kao i promene koje su se u odnosu na saveznu državu desile. Tako je njenim razgrađivanjem dovedeno u pitanje važenja mnogih saveznih zakona. O tim činjenicama mora se posebno voditi računa, kao i novonastaloj pravnoj situaciji. S obzirom na sve to neophodno je pitanje nacionalnih instrumenata zaštite podataka posmatrati kroz vreme u kojem egzistiraju i u kontekstu novonastalih stanja.

Dakle, kad su u pitanju pravni instrumenti kod nas mora se imati u vidu da je jedna savezna država postojala faktički do juna 1991. godine, odn. januara 1992. godine i da je nakon toga nastala druga. Delikatno je pitanje tretmana nacionalnih instrumenata, jer mada formalno Jugoslavija i dalje kontinuirano postoji kao međunarodni subjekt

<sup>139</sup> Brunhann U., Privacy and transparency: how can they be reconciled; Beer T. A. L., National secrecy interest versus public access; McDonagh M., Access to public sector information: the Australian experience; Perritt H. H., Reinventing Government Through Information Technology; Seipel P., Public access to public -held information and dissemination policy - the Swedish experience; Weissenberg P., Opening Speech, Conference: Access To Public Information: A Key To Commercial Growth And Electronic Democracy, Stockholm, 1996. svi su ovi materijali preuzeti sa Interneta.

<sup>140</sup> Ustav i Ustavni zakon doneti su na Saveznom veću Savezne skupštine SFRJ 27 aprila 1992, a objavljeni u Službenom listu SRJ, br. 1/92.

(što je jedno vreme bilo sporno), pod nacionalnim instrumentima treba podrazumevati, znači, savezne i instrumente republika Srbije i Crne Gore. Medjutim, zbog geneze razvoja pojedinih pravnih instituta, prikazivaće se i stanje do juna 1991. godine. Medju instrumentima posebno se prikazuju oni koji su doneti u Republici Srbiji, zbog teritorijalnog značaja. Valja istaći da je spominjanje Zakona o zaštiti podataka o ličnosti Republike Slovenije učinjeno zbog toga što je on u momentu donošenja bio prvi takav zakon nekadašnje Jugoslavije i zato što su neka od rešenja bila gotovo po vrednosti ekvivalentna Britanskim ili dokumentima EU, OECD, i sl. Naročito što su mnoga rešenja i nakon 5 godina aktuelna i danas.

### *3.3.1. Savezni pravni instrumenti*

Naš pravni sistem imao je specifične instrumente u regulisanju zaštite podataka i subjekata, kao što je imao i specifičan put u regulisanju ovih problema.

Najrazvijenije zemlje svoje prve zakone donele su početkom 70-ih. Nepunih pet godina posle njih počele su pripreme na izradi odgovarajućih odredbi i u Jugoslaviji. Pripreme su se, uglavnom, odnosile na izgradnju društvenog sistema informisanja (**DSI**) kome su prethodile odgovarajuće studije od strane formiranih komisija i stručnih tela u okviru Saveznog izvršnog veća i Savezne skupštine. Tako je **Medjuresorska radna grupa SIV-a** pripremila **Informaciju o problemima elektronskih računara** i predala je SIV-u **1976. godine**, koji aprila iste godine razmatra ponudjenu Informaciju i nalaže izradu nove **Kompleksne analize o računarima**. U ovoj Analizi trebalo je, na osnovu prikupljenih podataka, konsultacija i razmatranja utvrditi opravdanost donošenja zakona, drugih akata, kao i dugoročne strategije i politike u ovoj oblasti. U Informaciji, kao posebna tačka, data je "Ocena stanja i predloga za utvrđivanje mera, strategije i politike u ovoj oblasti" i konstatovano (tč. 2.) da su: "Ustavom SFRJ, Zakonom o udruženom radu i društvenim planovima Jugoslavije i socijalističkih republika i pokrajina stvoreni potrebni uslovi za društveno uređjivanje područja informatike. Medjutim, načela u ovim aktima i razne inicijative i odgovori izmedju različitih struktura, ne mogu da zadovolje određene zahteve koje postavlja praksa. Zbog toga je neophodno da se pristupi izradi zakona i drugih akata, kojima bi se regulisala osnovna pitanja organizovanja, uređjivanja, razvoja i **zaštite informacionih tokova i sistema** ...".

U istoj tački, dalje, se ističe potreba donošenja saveznog zakona kojim bi se regulisali ovi problemi. Takodje se, u okviru **tačke 19** razmatra problem obezbeđenja i zaštite podataka koji se obrađuju u okviru ovih sistema i konstatuje da ne treba zanemariti iskustva nekih zemalja koje su zakonskim i drugim aktima regulisala "...".

**naročito načine čuvanja podataka u okviru sistema, odgovornost za sprovođenje organizacionih i tehničkih mera obezbeđenja i zaštite, krivičnu odgovornost za zloupotrebu podataka protiv građana (zaštita ličnosti i dr.)."**

Na osnovu iznetih konstatacija određuju se pravci politike i dugoročne strategije koja je, između ostalog, trebalo da se zasniva i na "potrebi za što bržim i potpunijim prerastanjem otvorenih i zatvorenih skupova informacija u jedinstveni skup, koji bi se otvarao fleksibilno prema našim potrebama kod informisanja drugih, u meri koja je neophodna radi našeg učešća u međunarodnoj podeli rada i posebno radi naše saradnje sa zemljama u razvoju. Ovaj fleksibilno zatvoreni sistem informisanja i rad sa informacijama, treba da se posebno reguliše predloženim zakonom kojim ... **Pri tome mora da se obezbedi i zaštita ličnosti od neovlašćenog korišćenja podataka i informacija ...**".

I na kraju, u programu rada za sledeću godinu (1977.) predviđena je i priprema nacrtu zakona kojim bi se regulisala ta pitanja.

Skoro istovremeno Skupština SFRJ formira, u okviru Komisije za informisanje, **Radnu grupu za pripremu teza o sistemu informisanja**. Ova Radna grupa u saradnji sa saveznim organima uprave (posebno Saveznim komitetom za informisanje i Saveznim sekretarijatom za pravosuđe i organizaciju savezne uprave) priprema svoj materijal "Izgradnja jedinstvenog društvenog sistema informisanja sa predlozima mera" u kome je istaknuta potreba donošenja zakona o DSI kojim bi trebalo regulisati i zaštitu podataka.

Pored ovih akcija na saveznom nivou i pojedine republike i pokrajine počele su rad vezan za pravce i smernice razvoja u oblasti informatike. Tako je npr. u Sloveniji **Republički komitet za društveno planiranje** pripremio (1977.) materijal "**Pravci i smernice razvoja integralnog informacionog sistema u SR Sloveniji**" u kome se kao jedna od smernica označava i "**ugradjivanje kriterijuma nacionalne zaštite, samozaštite, zaštite podataka i zaštite podataka o ličnosti od neovlašćenog korišćenja, kao i ugradjivanja kriterijuma opštenarodne zaštite u svim oblastima informacione delatnosti**". Za realizaciju ovih smernica preporučeno je donošenje zakona kojim bi se obuhvatile i "odredbe za informacione sisteme, AOP delatnost u vezi sa nacionalnom sigurnošću i samozaštitom, **zaštitom podataka**, kao i odredbe u vezi sa kriterijumima odgovornosti." Pri tome su bili utvrđeni i uslovi pristupanja podacima, ko i pod kojim uslovima može da koristi osnovne, a ko izvedene podatke.

Ovi prvi koraci u isticanju potrebe za pravnom regulativom kojom bi se propisale mere i mehanizmi zaštite podataka nisu se kasnije odvijali onako kako bi bilo prirodno očekivati. Vremenom su se aktivnosti usmerile u dva pravca i dve grupe internih subjekata.

U **jednoj grupi** subjekata krenulo se sa izradom posebnih studija iz kojih će kasnije slediti opšte odredbe u republičkim i pokrajinskim zakonima o društvenom sistemu informisanja, a potom i pripreme za donošenje posebnih zakona o zaštiti. **Druga grupa** subjekata zadržala se na opštim i prvim koracima u donošenju posebnih zakona, koje će posle izvesnog perioda napustiti i zadovoljiti se samo načelnim odredbama u okviru zakona o društvenom sistemu informisanja.

Prvoj grupi jedino je pripadala SR Slovenija koja je, nakon Zakona o društvenom sistemu informisanja, nastavila sa radom na pripremi i donošenju posebnog zakona o zaštiti podataka o ličnosti i podataka u međugraničnim tokovima. Otuda, **1984. godine je pripremljen Predlog za donošenje Zakona o zaštiti podataka u društvenom sistemu informisanja SR Slovenije**<sup>141</sup>. U okviru ovog predloga razradjene su **Teze za nacrt zakona** ali je Skupština Slovenije, raspravljajući o predlogu, ocenila da on ne može biti prihvaćen zbog toga što neka pitanja treba da se prvo reše saveznim zakonom. Međutim, **početkom 1990. godine (7. marta 1990.) Skupština Slovenije je donela Zakon o zaštiti podataka o ličnosti (Zakon o varstvu osebnih podatkov)**. Ovo je ujedno bio i prvi zakon ove vrste na tlu bivše Jugoslavije i imao je ukupno 42 člana. Uzor su mu bile Smernice OECD i Konvencija Evropskog saveta. Kao što je i bilo za očekivanje poseban deo Zakona odnosio se i na **prekogranični tok podataka**<sup>142</sup>.

Nažalost, savezni **Zakon o osnovama društvenog sistema informisanja i o informacionom sistemu federacije**<sup>143</sup> nije baš mnogo pažnje posvetio problemu zaštite podataka i informacija, a još manje podataka o ličnosti ili onih koji se mogu naći u prekograničnim tokovima. Svega dva, vrlo opšta i načelna, člana ovog Zakona napominju neophodnost zaštite<sup>144</sup> podataka i informacija i donošenja saveznog zakona o standardima u vezi sa čuvanjem, prenosom i obradom podataka, dokumentacijom sistema za automatsku obradu podataka, računarskom, mašinskom, programskom

<sup>141</sup> Fižgar A., O zaštiti podataka u društvenom sistemu informisanja, Beograd, Anali Pravnog fakulteta u Beogradu, br. 3 - 4/85., str. 464.

<sup>142</sup> Detaljnije kod Drakulić M., op. cit., str. 167 - 177

<sup>143</sup> Zakon o osnovama društvenog sistema informisanja i o informacionom sistemu federacije, Službeni list SFRJ, br. 68/81.

<sup>144</sup> Zakon o DSI i IS, čl. 11. tč. 9; čl. 18, st. 3.

opremom i iskazivanjem podataka. Ono što je **utvrđeno kao osnovno načelo je dostupnost podataka i informacija svim subjektima društvenog sistema informisanja izuzev ako zakonom ili opštim aktom nije predviđeno da predstavljaju tajnu**, što je u skladu sa proklamovanom slobodom informacija u drugim zemljama.

Neposredno posle donošenja ovog Zakona doneti su republički i pokrajinski zakoni o DSI u kojima su, više ili manje, detaljno dotaknuta i ova pitanja. Ovim zakonima, u tom periodu<sup>145</sup>, obuhvaćene su uglavnom **tri grupe pitanja** na sledeći način: **a) prava subjekata nisu naročito dobro definisana** Jedino u Zakonu tadašnje SRBiH predviđeno je **pravo pojedinca da može da ima uvid u podatke koji se na njega odnose i da sazna kome se ti podaci dostavljaju na korišćenje**<sup>146</sup>; **b) problemu zaštite nije bila posvećena baš osobita pažnja**, sem u Sloveniji i, donekle, u SRBiH i SAP Vojvodini<sup>147</sup>. Kazne za prekršaje koji povodom rukovanja nastaju nisu predviđene, niti je predviđena posebna odgovornost informacionih službi za štete koje nastaju zbog nedovoljno ili neadekvatno preduzetih mera obezbeđenja<sup>148</sup>; **c) izostavljeno je decidirano određivanje vrsta podataka koje bi trebalo posebno zaštititi**.

Interesantna je sudbina ovih zakona o DSI. Naime, savezni i republički zakoni (Srbije i Crne Gore) nisu, donošenjem novih Ustava i Ustavnih zakona o sprovođenju Ustava, prestali da važe, niti su predviđeni rokovi za njihovo menjanje, niti su doneti novi. Tako su ovi zakoni u tretmanu *stand by*, s tim što je za Zakon Srbije predviđeno kompletno ukidanje donošenjem posebnog novog zakona i saveznog Zakonom o zaštiti podataka o ličnosti.

Danas je situacija veoma komplikovana. U pripremi je Zakon o zaštiti podataka o ličnostima čija se i treća verzija nalazi u formi Predloga<sup>149</sup>, koji je prošao vladinu proceduru, stigao do Skupštine i u toku razmatranja od strane Ministra za

<sup>145</sup> Finžgar A., op. cit., str. 465.

<sup>146</sup> Zakon o društvenom sistemu informisanja SRBiH, čl. 47.

<sup>147</sup> U Zakonu o DSI SAPV se predviđala obaveza radnika koji rade na prikupljanju, obradi i čuvanju podataka, koji su predmet posebne zaštite, da ove podatke čuva kao tajnu dok rade, ali i posle toga i onda kad im, iz bilo kog razloga, prestane radni odnos.

<sup>148</sup> Fižgar A., op. cit., str. 466.

<sup>149</sup> Prvi je Predlog bio urađen od strane Saveznog Zavoda za informatiku i dostavljen Saveznoj vladi 21. aprila 1994. Ovaj je predlog zaustavljen u skupštinskoj proceduri i zamenjen novim Predlogom od juna 1995. Treći je Predlog iz septembra 1995. godine. Sve verzije su gotovo identične, razlike su u broju članova, kao i u nekim preformulacijama i definicijama.

pravdu povučen do daljnjeg<sup>150</sup>. Treća verzija Predloga ima 9 delova svrstanih u 27 članova<sup>151</sup>. Najznačajnija su, naravno, **prava građana**, kao fizičkih lica na koje se podaci odnose, a kojima se obuhvata:

- **pravo saznavanja** (u kojim se zbirkama nalaze podaci koji se na njega odnose, koji se podaci o njemu obrađuju, ko ih obrađuje u koje svrhe i po kom osnovu, i ko ih koristi i po kom osnovu)<sup>152</sup>;
- **pravo da zahteva od rukovaoca zbirkom obveštenje** o postojanju zbirke i pismeni dokaz o ličnim podacima koji se o njemu vode; **uvid** u podatke; **ispravku** netačnih podataka; **brisanje** podataka; **zabranu** korišćenja netačnih, neažurnih i nepotpunih podataka; kao i **zabranu** korišćenja podataka ako se ne koriste u skladu sa zakonom ili ugovorom<sup>153</sup>;
- **pravo na pravni lek** u slučaju povrede prava građanina i štete usled korišćenja podataka prikupljenih na način ili za namene koje nisu u skladu sa odgovarajućim odredbama zakona<sup>154</sup>;
- **pravo nacionalnog tretmana stranaca**, odn. pravo da uživaju ista prava kao i domaći državljani, naravno po principu reciprociteta<sup>155</sup>;
- pravo obezbeđenja određenog kvaliteta podataka, odn. oni moraju biti tačni, ažurni, zasnovani na verodostojnim izvorima i potpuni (zavisno od namene prikupljanja)<sup>156</sup>.

Osim odredbi o pravima građanina posebno su značajne odredbe o pravima i obavezama rukovaoca zbirkom ličnih podataka, kao državnog organa ili organizacije, pravnog ili fizičkog lica koje je zakonom ili pismenom saglasnošću građanina ovlašćeno za prikupljanje, obrađivanje, čuvanje i prenos ovih podataka, kao i uspostavljanje, održavanje i korišćenje zbirke ovih podataka. Rukovaoc može, a u nekim slučajevima i mora, da<sup>157</sup>:

<sup>150</sup> Juli 1996. godina.

<sup>151</sup> Pored opštih odredbi koje sadrže definicije osnovnih izraza (građanina, ličnih podataka, zbirke podataka, kataloga zbirke, obrade, rukovaoca zbirkom, korisnika zbirke) i predmeta i cilja Zakona, u drugom delu su određena prava i obaveze rukovaoca zbirke ličnih podataka (pod rukovaocem se podrazumeva fizičko ili pravno lice, odn. odgovorno lice u državnom ili drugom organu ili organizaciji, koje je zakonom ili pismenom saglasnošću građanina ovlašćeno da prikuplja, obrađuje, čuva i prenosi lične podatke i da uspostavlja, održava ili koristi zbirku ličnih podataka).

<sup>152</sup> Predlog zakona, čl. 11.

<sup>153</sup> Predlog zakona, čl. 12.

<sup>154</sup> Predlog zakona, čl. 15.

<sup>155</sup> Predlog zakona, čl. 24.

<sup>156</sup> Predlog zakona, čl. 16 i 17.

<sup>157</sup> Predlog zakona, čl. 4 - 11.

- *uspostavi zbirku;*
- *uspostavi i vodi katalog podataka;*
- *obradjuje i čuva lične podatke;*
- *ustupa zbirku ili njen deo ovlašćenom korisniku;*
- *poverava poslove ili deo poslova uspostavljanja i vođenja zbirke* drugom fizičkom licu ili pravnom licu koje je registrovano za obavljanje poslova prikupljanja, obrade, čuvanja, i davanja ličnih podataka;
- *utvrdi mere obezbeđenja i zaštite podataka;* i
- *vodi registar zbirke.*

Naravno, odredbe o nadzoru su, takodje, predviđene samo što je ta funkcija poverena saveznom ministarstvu nadležnom za pravdu, čime je prihvaćeno veoma nepovoljno rešenje suprotno intencijama svih međunarodnih akata, kao i iskustavima i rešenjima većine nacionalnih zakona.

Što se prekograničnog transfera podataka o ličnosti tiče, Predlog zakona ga je regulisao samo jednim članom predviđajući primenu principa reciprociteta u odnosu na državu u koju se podaci unose.

Kaznene odredbe su nešto preciznije i izdašnije predviđajući da kršenje odredbi ovog Predloga, odn. Zakona predstavlja prekršaj za koji se kažnjava pravno ili/i fizičko lice. Nisu predviđena krivična dela za pojedine nedozvoljene radnje vezane za podatke o ličnosti.

Za ceo ovaj Predlog zakona o zaštiti podataka o ličnosti može se reći da je karakteristično:

**Prvo.** Da se *bazira na Evropskoj Konvenciji*, kao i nekim rešenjima datim u Smernicama UN i zakonima drugih zemalja. Međutim, izostala su rešenja iz Evropske Direktive, mada je ona doneta pre nego što je treća verzija puštena u proceduru, čime su učinjeni značajni propusti.

**Drugo.** Znatne neujednačenosti posledica su što se *u nekim delovima Predloga polazi od veoma radikalnih rešenja i instituta* (predviđanje ugovora o uspostavljanju), dok se *u drugim zadržavaju termini i instituti iz prethodnih faza razvoja IS*, mada bi trebalo poći od suprotnog: savremenih trendova (BP, kolaboracionih sistema), a u dodacima predvideti uklapanja predjašnjeg stanja (zbirke podataka, kataloga podataka).

**Treće.** *Predviđena prava pojedinaca u odnosu na podatke trebalo je drugačije sistematizovati*, tako da se obuhvati sva njihova kompleksnost.

**Četvrto.** *Nedostaju principi bez kojih se ne može zamisliti ni jedan moderan i kompletan zakon ove vrste.*

**Peto.** *Nije predviđeno donošenje posebnih uputstava za realizaciju ovog zakona*, kao obaveznih pratećih akata kojim bi se potpunije odredila pravila i faze postupaka za sprovođenje svih prava i obaveza iz zakona.

**Šesto.** *Kaznene odredbe su, čini se, isuviše pomirljive, a kazne nedovoljno visoke da bi upozoravale potencijalne prekršioce i kažnjavale počinioc.* Samo visoke novčane i duže zatvorske kazne mogu predstavljati ozbiljnu pretnju za prekršioce i počinioc.

**Sedmo.** *Ipak je trebalo više pažnje posvetiti prekograničnim tokovima podataka.*

**Osmo.** *Nedopustivo je da nadzor bude u nadležnosti saveznog organa, kao i to što nije u potpunosti detaljno regulisan*, od sastava i statusa tog organa do procedure, detaljnijih obaveza i odgovornosti i, naravno, nadležnosti.

Ipak, mora se odati priznanje na upornosti da se ovaj Zakon definitivno donese što nesumljivo predstavlja ne samo pozitivni trend u našem pravnom sistemu, već i znatno približavanje zemljama koje su ove probleme definisale i regulisale. Tim više, što je u nekoliko navrata inicijativa postojala, ali se neslavno završavala.

### 3.3.2. *Pravni instrumenti Republike Srbije*

Za Republiku Srbiju ranije, a i sada, osobena je priprema zakona o informacionom sistemu, a ne o zaštiti podataka, što je i razumljivo zbog sukoba nadležnosti. Naime, to je moglo i da bude pogodno da su se prihvatala rešenja koja bi stvarno na kompleksan i celovit način regulisala ovu problematiku. Međutim, ponudjena rešenja bila su samo blede kopije nekih nacionalnih instrumenata drugih zemalja. Tako, poslednja verzija **Nacrta Zakona o obezbedjenju i zaštiti informacionih sistema zasnovanih na računarima iz 1986. godine** sadržala je svega 26 članova grupisanih u nekoliko poglavlja i predstavljala je samo još jedan, ali ipak

nedovoljan, korak u napred u odnosu na prethodne verzije. Bila su predviđjana gotovo sva prava iz zakona razvijenih država i Evropske Smernice i Konvencije. Nažalost, ovaj nacrt neslavno je završio, jer Skupština SR Srbije nije tekst ni razmatrala. Prekinut je dalji rad na donošenju posebnog zakona o zaštiti podataka, informacionih sistema i subjekata da bi se u oktobru **1989. godine doneo Zakon o društvenom sistemu informisanja**<sup>158</sup>. Sudbina i ovog Zakona je ista kao i saveznog zakona - niti je ukinut, niti izmenjen, niti se primenjuje. U okviru ovog Zakona bile je predviđjeno nekoliko posebnih odredbi o zaštiti podataka i informacija u DSI. Međutim, ostala pitanja vezana za zaštitu podataka nisu regulisana niti predviđjena.

Pravnu prazninu, donekle, je popunila **Uredba o obezbedjenju i zaštiti informacionih sistema državnih organa**<sup>159</sup>. Iako su se ovom Uredbom uređivale tehničke i organizacione mere obezbedjenja i zaštite (objekata u kojima je smeštena računarska oprema; same računarske opreme i nosioca podataka; programske podrške i računarskih mreža) ona je, u nekoliko svojih članova, predviđjala i obezbedjenje i zaštitu podataka.

Tako se pri projektovanju IS u "preliminarnoj studiji" utvrđivala priroda podataka, vrsta i stepen tajnosti podataka koji će se obezbedjivati i čuvati, pored vrste i tajnosti IS. U ostalim članovima, koji se odnose na mere obezbedjenja i zaštite pri projektovanju IS, predviđjene su i mere obezbedjenja i zaštite procesa prikupljanja, kontrole, obrade, čuvanja i korišćenja podataka koje se moraju detaljno razraditi u idejnom, glavnom i izvodjačkom projektu.

Uredba je predviđjala i da se "prikupljeni podaci mogu koristiti samo u službene svrhe i ukoliko im je rok trajanja prošao, odn. službena vrednost istekla, moraju se brisati", što bi bilo u skladu sa principom da se podaci ne smeju držati duže nego što je potrebno i principom da raspolaganje podacima mora biti u skladu sa unapred odredjenom i pravno definisanom (ovde službenom) svrhom. U skladu sa ovim principima je i odredba po kojoj "pristup podacima mogu imati samo ovlašćena lica".

Ostale odredbe odnose se na konkretne mere obezbedjenja i zaštite podataka, naročito tajnih, i tako se na posredni način poštuje princip da se mere sigurnosti preduzimaju protiv neautorizovanog pristupa, menjanja, otkrivanja i uništenja podataka, odn. kako je Uredbom predviđjeno "kako bi se sprečile slučajne greške, nepravilno i

<sup>158</sup> Zakon o društvenom sistemu informisanja, Službeni glasnik SR Srbije, br. 49/89.

<sup>159</sup> Navedena Uredba o obezbedjenju i zaštiti informacionih sistema državnih organa, trebala bi biti zamnjenjena novim propisima do oktobra 1996. godine.

nedozvoljeno prikupljanje, čuvanje, obrada, iskazivanje, korišćenje, oštećenje, uništenje, kao i falsifikovanje i zloupotreba podataka".

U suštini, ova Uredba predstavlja realizaciju principa obaveznosti preduzimanja određenih mera za obezbedjenje i zaštite podataka i drugih principa, koji, doduše, šturo iz nje provejavaju. Međutim, ona, svakako, nije bila niti je dovoljna, jer ne predviđa prava subjekata podataka i ostale obaveze i odgovornosti pružaoca informacionih usluga i korisnika. Osim toga, ona se odnosi samo na IS državnih organa, znači ne na sve, pa, čak, ni na sve javne, IS. Trebalo bi naglasiti da to i nije bio njen cilj, ali kako se područje zaštite veoma slabo pokriva drugim pravnim instrumentima Republike Srbije to je bilo za očekivati da će Uredbi prethoditi potpuniji pravni instrument. Tim više što je članom 20. Ustava Republike Srbije predviđeno "da se prikupljanje, obrada i korišćenje podataka o ličnosti uređuju zakonom, kako bi se osigurala tajnost podataka o ličnosti."

Umesto posebnog zakona o zaštiti podataka pripremalo se (Ministarstvo pravde, Savet za informacione sisteme državnih organa i modernizaciju rada) donošenje Zakona o informacionom sistemu Republike Srbije<sup>160</sup>. Nakon izvesnog vremena Zakon je i donet<sup>161</sup>. Međutim, od 18 članova koliko ukupno ima ovaj Zakon, dva su člana direktno (čl. 5 i 12), a jedan indirekto (čl. 15) posvećeni zaštiti. Prvim se predviđa da se "organ i organizacija, povezuju preko računarsko-telekomunikacione mreže i u okviru informacionog sistema obezbeđuju evidentiranje podataka na mestu njihovog nastanka, tačnost, kvalitet, zaštitu podataka pri obradi i prenosu, dostupnost podataka pod jednakim uslovima ovlašćenim korisnicima, primenu jedinstvenih standarda i razmenu podataka i dokumenata". Drugi je član nešto opširniji određujući "...obavezu organa i organizacije da preduzme mere obezbedjenja i zaštite informacionog podsistema u svim fazama razvoja i funkcionisanja, u redovnim i vanrednim prilikama". Istim se članom predviđa i obaveza Vlade Republike Srbije da propiše sadržaj i način sprovođenja mera obezbedjenja i zaštite informacionog sistema, a posebnim (čl. 15) se određuje rok od 6 meseci od donošenja Zakona za donošenje tih propisa. To bi, dakle, trebalo da bude nova uredba o merama obezbedjenja i zaštiti informacionog sistema, kojom bi se stavila van snage postojeća i obezbedila inovacija ranijih rešenja.

### *3.3.3. Zaključna razmatranja o pravnim instrumentima našeg prava*

<sup>160</sup> Nacrt je bio završen jula 1995, ali je do donošenja bio nekoliko puta menjan.

<sup>161</sup> Službeni glasnik RS br. 12/96.

Na kraju može se konstatovati sledeće:

**Prvo.** *Naše pravo ima više instrumenata kojima može (a ne mora) da reguliše pitanja zaštite podataka i informacija, kao i subjekata.* Ti instrumenti su različite pravne snage i teritorijalnog važenja, kao što se odnose i na različite subjekte. Kao najčešći i najkarakterističniji pojavljuju se **sledeće vrste pravnih instrumenata:**

**1) Ustavi** (savezni i republički) kojima se propisuju najčešće osnovna prava subjekata (fizičkih i pravnih lica) i načelno spominje zaštita od zloupotreba ili neovlašćenog korišćenje podataka i informacija kojima se mogu ugroziti prava i slobode subjekata.

**Ustav SRJ** predviđa pravo čoveka na lični integritet i dostojanstvo koji ne smeju biti ničim ugroženi niti ograničeni osim jednakim slobodama i pravima drugih i, ustavom, utvrdjenih interesa. Pored toga, zajemčuje se nepovredivost fizičkog i psihičkog integriteta čoveka, njegove privatnosti i ličnih prava<sup>162</sup>, kao i poštovanje ljudske ličnosti i dostojanstva u krivičnom i svakom drugom postupku<sup>163</sup>. Zajemčuje se nepovredivost stana, tajnost pisama i drugih sredstava komuniciranja. Ono pravo, koje je od posebnog interesa za zaštitu podataka, definisano je posebnim članom<sup>164</sup>, po kome se **jamči zaštita podataka o ličnosti**. Zabranjuje se njihova upotreba van namene za koju su prikupljeni. Predviđa se da svako ima pravo da bude upoznat sa prikupljenim podacima koji se na njega odnose, ali i pravo na sudsku zaštitu, ukoliko dodje do zloupotrebe ovih podataka. I naravno, posebnim stavom se određuje neophodnost donošenja posebnog zakona kojim bi se uređivala pitanja prikupljanja, obrade, korišćenja i zaštite podataka o ličnosti. Dakle, ***zajemčuju se pravo na privatnost i informacionu privatnost*** (mada se navode samo neka prava ovog kompleksnog prava).

**Ustavi republika** sadrže slične odredbe o pravu na privatnost i posebno zaštiti podataka kojima se to pravo može ugroziti. Tako Ustav Republike Srbije<sup>165</sup> propisuje ***da su ljudsko dostojanstvo i pravo na privatni život nepovredivi, a zajemčuje se i zaštita tajnosti podataka o ličnosti, s tim da će se prikupljanje, obrada i korišćenje ovih podataka regulisati zakonom.***

**2) Zakoni**, savezni i republički, su kod nas, kao i svuda u svetu najučestaliji pravni instrumenti kojima se reguliše ova materija. No, između zakona postoje razlike. Pored razlike u teritoriji na koju se odnose (cela zemlja ili jedna republika), neophodno je praviti razliku i između zakona kojima se regulišu samo ova pitanja i zakona kojima

<sup>162</sup> Ustav SRJ, čl. 22.

<sup>163</sup> Ustav SRJ, čl. 25.

<sup>164</sup> Ustav SRJ, čl. 33.

<sup>165</sup> Ustav RS, Službeni glasnik RS, br. 1/90., čl. 18 i 20.

je predmet regulisanja nešto drugo, uz koje se regulišu i ova pitanja. **U prvoj grupi** su, po pravilu, savezni, zakoni o zaštiti podataka o ličnosti. Za razliku od ovih, kod nas, je nešto češća **druga grupa**, kojima se regulišu druga pitanja, manje ili više bliska podacima, informacijama i IS (npr. Zakon o popisu stanovništva, domaćinstava i poljoprivrednih gazdinstava, Zakon o evidencijama u oblasti rada).

**3) Podzakonski pravni akti** (savezni, republički), kao što su uredbe, naredbe, uputstva, pravilnici.

**4) Opšti akti** organizacija ili asocijacija u kojima se predviđaju podaci koji se mogu smatrati poslovnom, službenom ili nekom drugom tajnom, kao i oni u kojima se regulišu status, sastav, prava i obaveze subjekata koji prikupljaju, obrađuju ili koriste podatke. Od opštih akata treba spomenuti da se ova problematika načelno regulišu u statutima, a detaljnije u pravilnicima, poslovnima, protokolima.

**5) Kolektivni, granski i, redje, individualni, ugovori o radu** kojima se regulišu prava, obaveze i odgovornosti zaposlenih i bivših zaposlenih u odnosu na obezbeđenje i zaštitu poverljivosti i tajnosti podataka.

**6) Odluke organa upravljanja** kojima se konkretni podaci proglašavaju za tajnu ili se predviđa način prikupljanja, obrađivanja i korišćenja određenih podataka i informacija.

**7) Rezolucije, deklaracije** i slični akti kojima se načelno i na opšti način propisuju npr. oblici saradnje subjekata u oblasti informatike, što je bilo uobičajeno pre 1990. godine i možda će biti u budućnosti.

**8) Ratifikovani bilateralni i multilateralni međunarodni akti** kojima se regulišu pojedninačni ili opšti odnosi vezani za zaštitu podataka i informacija ili subjekata. To bi, npr. mogle biti već spomenute međunarodne deklaracije, rezolucije, konvencije, smernice, preporuke, direktive donete od međunarodnih organizacija, čiji smo član ili to želimo da budemo (i koje, nažalost, nismo još ratifikovali, sem Konvencije EU o zaštiti podataka o ličnosti s obzirom na automatsku obradu podataka, 1992.) ili dvostrani međunarodni ugovori između naše i neke druge zemlje o saradnji, povezivanju ili priključivanju naših IS u odgovarajuće međunarodne računarske mreže. Ove međunarodne ugovore primenjuju direktno nadležni organi, po pravilu, nakon ratifikovanja i objavljivanja u odgovarajućem službenom listu. Izuzetno, međunarodni ugovori primenjuju se i pre ratifikacije, ako je tako određeno aktom o ratifikaciji ili samim ugovorom. Ratifikaciju, po pravilu, obavlja Skupština SRJ<sup>166</sup>. Situacija je,

<sup>166</sup> Čin ratifikacije treba odvojiti od čina potpisivanja, jer važeći postaje samo onaj međunarodni akt koji je ratifikovan, znači usvojen od strane najvišeg zakonodavnog tela jedne zemlje.

naravno, bila sasvim specifična zbog odluka o sankcijama Saveta bezbednosti UN, kojima se stornira naše članstvo u svim međunarodnim organizacijama i zabranjuje sklapanje bilo kakvih dvostranih međunarodnih ugovora. Nešto je bolje stanje nastalo nakon privremenog storniranja sankcija, ali ne i kompletnog vraćanja na međunarodnu scenu.

Pored ovih vrsta, pravni instrumenti mogu se razvrstati i po nadležnim subjektima za prikupljanje, obradjivanje i korišćenje podataka, kao i po kriterijumu obaveznosti po kome to mogu biti **pravni akti koji su obavezni za sve subjekte na koje se odnose** (čiji krug može biti vrlo širok), i pravne akte koji se odnose **samo na one subjekte koji su ih doneli** (npr. opšti akti važe samo za organizaciju koja ih je donela). Međutim, kako prethodni kriterijumi obuhvataju i ove, to je navedena podela i nabrojanje primarna.

**Drugo.** Studioznija analiza postojećeg stanja u jugoslovenskom pravnom sistemu ukazuje da *naše pravo, iako ima mogućnosti, gotovo da nema odgovarajućih, konkretnih, pravnih instrumenata za zaštitu podataka i subjekata*. Izuzetak je, naravno, Predlog zakona o zaštiti podataka o ličnosti, ali koji je samo predlog, a ne i zakon.

**Treće.** *Postojeći zakoni (savezni i republički) i drugi važeći pravni akti ne pružaju odgovarajuću pravnu osnovu zaštitu podataka i subjekata.*

**Četvrto.** *Akcije koje se, u vezi sa ovom problematikom, preduzimaju ne mogu pružiti odgovarajuće garancije da će se rešenja razvijenih zemalja usvojiti i prilagoditi našim uslovima*, a pogotovo da ćemo moći da pratimo aktivnosti kodifikacije i unifikacije evropskog prava.

**Peto.** *Pripreme za donošenje posebnih zakona o zaštiti podataka i privatnosti, kao i drugih subjekata i podataka, isuviše se sporo odvijaju*. Razlozi nisu samo eksterni.

**Šesto.** *Ovakav pravni sistem stvorio je mogućnost parcijalnog, nepotpunog i neusklađenog regulisanja ovih pitanja i prepuštanja "volji" subjekata da ove probleme reše na sopstveni način*. To, svakako, ne treba sporiti, ali ne i glorifikovati, tim više što se podaci ne nalaze samo kod organizacija, već i kod organa uprave i drugih subjekata, i što je za uspešnost zaštite potrebno predvideti i sankcije, kao što je potrebno i definisati prava, obaveze i odgovornosti raznovrsnih subjekata u vezi sa tim. Otuda, donošenje odgovarajućih posebnih zakona biće osnovna pretpostavka za obezbeđenje

zaštite, a ako se to još dopuni i novelama sadašnjih zakona kojima se regulišu pitanja iz krivične, poslovne, upravne i drugih oblasti i područja - zaštita će možda biti kompleksnija i nadajmo se uspješnija. Tu svakako ne treba zanemariti ni dopunske instrumente - podzakonske akte, kao i akte organizacija, organa.

# GLAVA 3

## ZAŠTITA KOMPJUTERSKIH PROGRAMA I SOFTVERA

|   |            |
|---|------------|
| <b>1. Uvodne napomene o zaštiti kompjuterskih programa i softvera</b>             | <b>166</b> |
| <b>2. Objekti zaštite</b>   | <b>167</b> |
| 2.1. Softver  | 167        |
| 2.2. Kompjuterski program   | 169        |
| 2.3. Izgled korisničkog interfejsa na monitoru                                    | 173        |
| 2.4. Proizvod reverzibilnog programiranja   | 174        |
| 2.5. Kompjuterski generisano delo   | 174        |
| <b>3. Oblici zaštite</b>  | <b>175</b> |
| 3.1. Kompjuterski programi i patentnopravna zaštita                               | 177        |
| 3.1.1. Opšte napomene o patentnopravnoj zaštiti                                   | 177        |
| 3.1.1.1. Uslovi i postupak sticanja prava na patent                               | 178        |
| 3.1.1.2. Sadržina prava na patent   | 180        |
| 3.1.1.3. Trajanje   | 181        |
| 3.1.2. Kompjuterski programi i nacionalni propisi zaštite patenta                 | 182        |
| 3.1.3. Kompjuterski programi i međunarodna zaštita patenta                        | 186        |
| 3.1.3.1. Pariska konvencija za zaštitu industrijske svojine                       | 186        |
| 3.1.3.2. Konvencija o evropskom patentu   | 187        |
| 3.1.3.3. Ugovor o saradnji na području patenata                                   | 188        |
| 3.1.3.4. Ugovor o rešavanju sporova između država u oblasti intelektualne svojine | 189        |
| 3.1.3.5. Sporazum o trgovinskim aspektima prava intelektualne svojine             | 189        |
| 3.1.4. Kompjuterski programi i patentna zaštita po našem pravu                    | 191        |
| 3.1.4.1. Obim, sadržina i trajanje prava na patent                                | 191        |
| 3.1.4.2. Kompjuterski programi nastali u radnom odnosu                            | 193        |
| 3.1.4.3. Zaštita prava na patent  | 194        |
| 3.2. Kompjuterski programi i zaštita žigom  | 199        |
| 3.2.1. Opšte napomene o zaštiti žigom   | 199        |
| 3.2.1.1. Uslovi i postupak sticanja prava na žig                                  | 201        |
| 3.2.1.2. Sadržina prava   | 201        |
| 3.2.1.3. Trajanje   | 202        |
| 3.2.2. Kompjuterski programi i nacionalni propisi zaštite žiga                    | 203        |
| 3.2.3. Kompjuterski programi i međunarodna zaštita žigova                         | 207        |
| 3.2.3.1. Pariska konvencija za zaštitu industrijske svojine                       | 207        |
| 3.2.3.2. Madridski sporazum o međunarodnoj registraciji žigova                    | 208        |

|          |  |     |
|----------|--|-----|
| 3.2.3.3. | <i>Ugovor o registraciji žigova</i>  | 209 |
| 3.2.3.4. | <i>Sporazum o trgovinskim aspektima prava intelektualne svojine</i>                        | 210 |
| 3.2.3.5. | <i>Direktiva Evropske zajednice o usaglašavanju zakona država članica u pogledu žigova</i> | 212 |
| 3.2.4.   | <i>Kompjuterski programi i zaštita žiga po našem pravu</i>                                 | 214 |
| 3.3.     | <i>Kompjuterski programi i regulisanje zaštite od nelojalne konkurencije</i>               | 219 |
| 3.3.1.   | <i>Opšte napomene o zaštiti od nelojalne konkurencije</i>                                  | 219 |
| 3.3.2.   | <i>Kompjuterski programi i nacionalni propisi zaštite od nelojalne konkurencije</i>        | 221 |
| 3.3.3.   | <i>Kompjuterski programi i međunarodna zaštita od nelojalne konkurencije</i>               | 225 |
| 3.3.3.1. | <i>Pariska konvencija za zaštitu industrijske svojine</i>                                  | 225 |
| 3.3.3.2. | <i>Sporazum o trgovinskim aspektima prava intelektualne svojine</i>                        | 226 |
| 3.3.3.3. | <i>Rimski i Mastrihtski ugovor</i>   | 227 |
| 3.3.4.   | <i>Kompjuterski programi i zaštita od nelojalne konkurencije po našem pravu</i>            | 229 |
| 3.3.4.1. | <i>Oblici u kojima se javlja nelojalna konkurencija</i>                                    | 230 |
| 3.3.4.2. | <i>Uslovi i oblici zaštite</i>   | 232 |
| 3.4.     | <i>Kompjuterski programi i autorskoppravna zaštita</i>                                     | 238 |
| 3.4.1.   | <i>Opšte napomene o autorskopravnoj zaštiti</i>  | 238 |
| 3.4.1.1. | <i>Uslovi zaštite</i>  | 238 |
| 3.4.1.2. | <i>Vrste autorskih dela</i>  | 244 |
| 3.4.1.3. | <i>Sadržina prava</i>  | 245 |
| 3.4.1.4. | <i>Lica koja uživaju zaštitu</i>   | 251 |
| 3.4.1.5. | <i>Trajanje</i>  | 253 |
| 3.4.2.   | <i>Kompjuterski programi i nacionalni propisi autorskoppravne zaštite</i>                  | 253 |
| 3.4.3.   | <i>Kompjuterski programi i međunarodna zaštita autorskog prava</i>                         | 261 |
| 3.4.3.1. | <i>Bernska konvencija za zaštitu književnih i umetničkih dela</i>                          | 261 |
| 3.4.3.2. | <i>Univerzalna konvencija</i>  | 263 |
| 3.4.3.3. | <i>Model zakona za zaštitu kompjuterskog softvera</i>                                      | 265 |
| 3.4.3.4. | <i>Rezolucija o zaštiti kompjuterskog softvera i integrisanih kola</i>                     | 266 |
| 3.4.3.5. | <i>Direktiva o pravnoj zaštiti kompjuterskih programa</i>                                  | 267 |
| 3.4.3.6. | <i>Sporazum o trgovinskim aspektima prava intelektualne svojine</i>                        | 271 |
| 3.4.4.   | <i>Kompjuterski programi i autorskoppravna zaštita po našem pravu</i>                      | 273 |
| 3.4.4.1. | <i>Kompjuterski programi kao autorsko delo</i>   | 274 |
| 3.4.4.2. | <i>Uslovi zaštite</i>  | 276 |
| 3.4.4.3. | <i>Sadržina prava</i>  | 277 |
| 3.4.4.4. | <i>Kompjuterski programi nastali u radnom odnosu</i>                                       | 288 |
| 3.4.4.5. | <i>Kompjuterski programi nastali po ugovoru o delu</i>                                     | 290 |
| 3.4.4.6. | <i>Trajanje</i>  | 290 |
| 3.4.4.7. | <i>Prenošenje autorskih prava na kompjuterskim programima</i>                              | 292 |
| 3.4.4.8. | <i>Zaštita prava</i>   | 294 |

|          |  |     |
|----------|--|-----|
| 3.4.4.9. | <i>Postupak fakultativnog sticanja autorskih prava na kompjuterskim programima</i> | 300 |
| 3.5.     | <i>Kompjuterski programi i zaštita sui generis pravom</i>                          | 303 |
| 3.6.     | <i>Kompjuterski programi i zaštita poslovne tajne</i>                              | 305 |
| 3.6.1.   | <i>Opšte napomene o poslovnoj tajni</i>  | 305 |
| 3.6.1.1. | <i>Karakteristike</i>  | 305 |
| 3.6.1.2. | <i>Kompjuterski programi, know how i poslovna tajna</i>                            | 307 |
| 3.6.2.   | <i>Kompjuterski programi i nacionalni propisi zaštite poslovne tajne</i>           | 308 |
| 3.6.3.   | <i>Kompjuterski programi i međunarodna zaštita poslovne tajne</i>                  | 316 |
| 3.6.3.1. | <i>Sporazum o know how kao globalnom izuzeću iz Rimskog sporazuma</i>              | 316 |
| 3.6.3.2. | <i>Sporazum o trgovinskim aspektima prava na intelektualnu svojinu</i>             | 317 |
| 3.6.4.   | <i>Kompjuterski programi i zaštita poslovne tajne po našem pravu</i>               | 317 |
| 3.6.4.1. | <i>Kompjuterski programi i zaštita poslovne tajne zakonskim propisima</i>          | 317 |
| 3.6.4.2. | <i>Kompjuterski programi i zaštita poslovne tajne individualnim ugovorima</i>      | 319 |
| 3.6.4.3. | <i>Zaštita od nezakonitih i nedozvoljenih radnji</i>                               | 321 |

## 1. Uvodne napomene o zaštiti kompjuterskih programa i softvera

U vreme pojave prvih računara dinosaurusa, cena hardvera je bila gotovo dve trećine cene svake instalacije. Situacija se revolucionarno<sup>1</sup> promenila razvojem personalnih kompjutera (PC), koji se u poredjenju sa računarima - dinosaurusima mogu slikovito opisati kao mravi. Ovi se računari ne iznajmljuju već kupuju i zamenjuju, unose se u velike i male organizacije, ali i u domove pojedinaca, korisnici im nisu više samo profesionalci, već sve više "amateri" koji ih upotrebljavaju za najrazličitije aktivnosti i obavljanje najrazličitijih poslova, čija lepeza se sve više širi. To je, naravno, izazvalo različite posledice sa kojima se trebalo suočiti i neke od njih i sprečiti. Kakve to razmere poprima može se videti i kroz višestruko ponovljenu pretnju Kini trgovinskim ratom od strane SAD, zbog piratstva računarских programa i trgovine krivotvorenom robom (računa se da je američki gubitak samo u 1995. godini od piraterije bio 6 milijardi dolara, od toga za ukupno 1.8 milijardi što je bila kriva Kina, više od 1.2 milijarde odnosilo se na pirateriju softvera), a što je istovremeno predstavljalo ozbiljnu smetnju međunarodnim trgovinskim i poslovnim odnosima. Vrlo ubedljivo deluju i podaci da svega 25% softvera koji se pojavi na tržištu donosi bilo kakve koristi svojim vlasnicima i/ili autorima<sup>2</sup>. Procenjuje se da SAD svake godine gubi stotine miliona dolara zbog nekontrolisanog kolanja softvera unutar i van granica. Ako se tome dodaju i druge zemlje u kojima razvoj i proizvodnja softvera predstavlja industrijsku granu u ekspanziji, sigurno da je zabrinutost imala stvarnih osnova. Trebalo je nešto učiniti, ali šta?

Jedna od ključnih stvari bilo je određivanje pravne prirode i osobenosti vlasništva računarskih programa. Od toga je zavisilo rešavanje praktičnih problema njihovog raspolaganja, korišćenja, prepravke, reprodukcije, distribucije jer bez programa računar postaje nekorisna, mrtva stvar. Otuda, da se to ne bi desilo, bilo je neophodno naći odgovore na niz pravnih pitanja. Odgovori na sva ova pitanja izazvali su mnoštvo burnih debata i rasprava između pravnika i informatičara, kao i između pravnika međusobno. **Ono što je bilo nesporno je da je kompjuterski program rezultat stvaralačkih napora jednog ili više tvoraca, čak i onda kad ga u potpunosti ili delimično generiše mašina.** Zbog toga se, prevashodno, i zaštićuje Pravom intelektualne svojine.

<sup>1</sup> Edwards C., Savage N., Walden J., Information Technology & The Law, Basingstoke, MacMillan Publishers LTD, 1990., str. 47.

<sup>2</sup> Collins W. R., Miller W. K., Spielman J. B., Wherrey P., How Good Is Good Enough?, Communication of ACM, vol. 37, no. 1/94, str. 85.

## 2. Objekti zaštite

Jedan od najvećih problema je definisanje predmeta zaštite. Kad su u pitanju računari ovaj problem postaje krajnje seriozan jer oni nisu, kao druge mašine, samo proizvod ljudskog intelekta, već predstavljaju njegov dodatak, podržavajući i podražavajući njegove funkcije<sup>3</sup>, a, istovremeno, zahtevajući rad čitave plejade raznih stručnjaka. To čini pravni problem zaštite komplikovanijim, a front prava većim i sa sve brojnijim pitanjima na koje se traže odgovori.

Prilazeći postupno definisanju stvarnog predmeta zaštite prvi značajni odgovori očekuju se u odnosu na distinkciju softvera i kompjuterskih programa. Mada se u praksi, pa, čak, i u nekim zakonima, veoma često ova dva pojma izjednačavaju, naizmeničnim korišćenjem jednog i drugog termina, u teoriji je sve manje autora koji sebi dozvoljavaju takav pristup, jer postoje sličnosti one ne znače i identičnost<sup>4</sup>.

### 2.1. Softver

Pod **softverom** (*software*) *podrazumevaju se kompjuterski programi, datoteke i prateća* (njemu pripadajuća) *dokumentacija* (kao što su menjueli i priručnici) *koji služe korisnicima*<sup>5</sup> Čak je i u Modelu zakona za zaštitu kompjuterskog softvera Svetske organizacije za zaštitu intelektualne svojine (**WIPO - World Intellectual Property Organization**) **softver** definisan kao *celina koja obuhvata kompjuterski program i to onaj koji je materijalno fiksiran na trakama, diskovima i sličnim medijumima; prateće materijale, kao što su priručnici za korišćenje programa ili za njihovo opsluživanje; i opis programa sadržanog u menjuelima programske logike*. Ovo odredjenje vrlo je slično prethodnom sem što se dokumentacija detaljnije specifikira, program vezuje za medijume, i što se u prvoj definiciji pojavljuju datoteke (u koje se smeštaju programi). Razlika u odredjenju računarskih programa proističe iz objašnjenja da se računarski programi moraju materijalno fiksirati na nekom medijumu.

Dakle, **softver** je kompleksan pojam pod kojim se podrazumeva celina sastavljena od dva (sastavna) dela, i to:

<sup>3</sup> Tapper C., Computer Law, London, Longman, 1989., str. 1

<sup>4</sup> Drakulić M., Kompjutersko pravo, Beograd, MST Gajić, 1992., str. 189.

<sup>5</sup> Bainbridge D., Computers and the Law, London, Pittman Publishing, 1990., str. XIX; Scott M., Computer Law, New York, Wiley Law Publications, 1987., str. G-7; itd.

1. **kompjuterskih programa** (i podprograma);
2. **prateće** (softveru pripadajuće) **dokumentacije** (priručnici i uputstva) *za korišćenje programa, njihovo opsluživanje i/ili razumevanje*. U određenim slučajevima pod pratećom dokumentacijom se podrazumevaju i **opisi programa, kao potpuni proceduralni prikazi podataka u verbalnoj, šematskoj ili nekoj drugoj formi, koji su dovoljni da se na osnovu njih izradi niz instrukcija, koje predstavljaju odgovarajući računarski program**<sup>6</sup>. Međutim, u prometu se uglavnom nalaze objedinjeni računarski program (jedan ili više, sa i bez podprograma) sa pratećom dokumentacijom, što čini **softverski paket**, a gotovo nikada, ili izuzetno retko, i opis programa.

Osim definisanja softvera sve se veća pažnja posvećuje i razlici između njihove dve osnovne vrste: sistemskog i aplikativnog. Njihova je pravna sudbina, donekle, različita, jer sistemski softver često prati sudbinu hardvera, dok se aplikativni tretiraju kao posebna kategorija za koju su se prihvatala i osobena rešenja.

**Sistemski softver** (*system software*) obuhvata: **operativni** softver i **prevodioc**.

**Operativni softver** (*operating software*), poznatiji kao operativni sistem, predstavlja veliku i kompleksnu grupu programa sa pratećom dokumentacijom koja od računara, kao inertne kutije, pravi mašinu sposobnu da ispuni korisničke zahteve. Većina instrukcija koje pokreću računar preko operativnog sistema su korisniku nevidljive i rade bez njegovog znanja i instrukcija. Operativni sistem najčešće se pojavljuje kao jedna od dve grupe softvera: prva je grupa na vrlo niskom nivou i najčešće je deo ROM-a i nije podložna čestim promenama, već je upravo onakva kakvu je proizvođač stvorio. Obično se označava kao **BIOS** (*Basic Input Output System*). Drugu grupu, po pravilu, stvaraju softverske kuće, a redje proizvođači računara. On se instalira u memoriju i omogućuje rad računara<sup>7</sup>. To su, u stvari, operativni sistemi, koji se učitavaju u memoriju prilikom uključivanja računara (boot-ovanja) i stvaraju okruženje u kome aplikativni softver može raditi. Najpoznatiji su UNIX, MS-DOS (*Microsoft Disk Operating System*), i sl.

**Prevodioci** (*compilers*) su deo sistemskog softvera koji prevode instrukcije napisane u izvornom kodu u jezik razumljiv mašini - jezik binarnih

<sup>6</sup> WIPO, Model Provisions On The Protection of Computer Software, Industrial Property, 1977.

<sup>7</sup> Burnside J. W. K., The Fundamentals of Computer Technology, edicija: Essays on Computer Law, Melbourne, Longman Cheshire Pty Limited, 1990., str. 28.

brojeva. Oni služe za prevodjenje programa napisanog u nekom višem programskom jeziku u mašinski. U cilju dobijanja konačne izvršne verzije program koristi i "usluge" jednog od podprograma koji se naziva *linker*. Znači, sem proste transformacije iz jednog u drugi oblik, što predstavlja **prevodjenje** (*compiling*), uz pomoć linker-a se vrši i **povezivanje** (*linking*) svih delova programa.

**"Programi tumači"** (*interpreters*) **su vrsta programa koji tumače izvorni kod za vreme izvršenja programa**. Oni, u suštini, imaju na raspolaganju osnovnu verziju programa koju transformišu na hardveru razumljiv način. Zbog toga se izvršavanje programa usporava, ali ga čine fleksibilnijim pošto za promenu nekog dela izvorne verzije nije nužno posebno prevodjenje.

**Aplikativni** (*application software*) **je dizajniran za zadovoljenje posebnih, specifičnih, korisničkih zahteva**<sup>8</sup>. U takav softver spadaju word-procesori, spreadsheet programi, programi za računanje, i sl. Ovo su programi opšte namene jer koriste širokom krugu korisnika. No, pored njih pojavljuju se i aplikativni programi posebne namene za određene korisnike i određene namene. Razlike medju njima osobito su važne sa aspekta zaštite prava autora, nosilaca, korisnika i naručilaca.

U pravu se, za sada, ne štiti softver kao celina, već neki od ovih njegovih delova. **Osnovni je predmet zaštite, u suštini, kompjuterski program. Dokumentacija** se tretira kao uputstvo. Ako je dokumentacija korisnička ne štiti se autorskim pravom, dok ukoliko je proizvođačka može se tretirati kao, autorsko delo ukoliko zadovoljava zakonom propisane uslove<sup>9</sup>. Naravno, ovo će imati dalekosežne posledice u slučajevima kada se zahteva patentna zaštita računarskog programa. **Opis programa**, sam po sebi ne uživa poseban pravni tretman.

Jedino što se na softveru jedinstveno štiti to je **znak**, sastavljen od reči, slogova, slova, imena, brojeva, slika, crteža, figurativnih elementi, kombinacije boja i bilo koje kombinacije takvih znakova koji se na njega stavljaju kao **žig** pod kojim se taj softver pojavljuje na tržištu, a koji mu služi da se razlikuje od drugih sličnih ili, čak, istih.

## 2.2. Kompjuterski program

<sup>8</sup> Burnside J. W. K., op. cit., str. 28.

<sup>9</sup> Henderson G. F., Intellectual Property: Litigation, Legislation and Education : A Study of the Canadian Intellectual Property and Legation System, 1996., preuzeto sa Interneta.

Kao najvažniji predmet zaštite pojavljuje se **sam kompjuterski program** (*computer program*) kojim se kontroliše ili uslovljava rad računara. Programi mogu biti stalni sastavni deo kompjutera ili integrisanih kola ili se mogu naći na magnetnim diskovima, trakama, disketama ili optičkim diskovima i sl. i unositi u memoriju onda kada je to neophodno<sup>10</sup>. Pod njim se, s toga, podrazumeva "*niz instrukcija koje su, po njihovom fiksiranju na neki, za mašinu čitljivi, materijalni nosilac, sposobne da na mašinu za obradu podataka deluju tako, da ona izrazi, ili postigne određenu funkciju ili zadatak ili rezultat*"<sup>11</sup>.

Kompjuterski program obuhvata:

1. **niz instrukcija**, fiksiranih na odgovarajući nosilac (sam tip nosioca nije relevantan što se zaštite programa tiče, već što se razumevanja za mašinu tiče), kojima se postiže određena funkcija, zadatak ili rezultat rada računara. Znači, instrukcije "kazuju" kompjuteru koja funkcija treba da se izvede u toj etapi rada. *One sadrže seriju znakova skupljenih u grupe koje mogu predstavljati komande (naredbe) računaru.*
2. sam po sebi niz instrukcija vezan je za algoritam i programski koncept. *Algoritam je serija instrukcija ili proceduralnih koraka u rešavanju posebnih problema*, dakle, metod, način, rešavanja određenog problema, *a programski koncept je programska zamisao rešavanja određenog problema.*

Sve više se u poslednje vreme pravi razlika između računarskih programa u širem i u užem smislu<sup>12</sup>.

**Kompjuterski program u širem smislu obuhvata programski koncept, algoritme i niz instrukcija.**

**Kompjuterski program u užem smislu je niz instrukcija kojima se upravlja obradom podataka.**

<sup>10</sup> Bainbridge D., op. cit., str. XVIII.

<sup>11</sup> WIPO, Model Provisions On The Protection of Computer Software, Industrial Property, 1977; slično je kompjuterski program definisao i US Copyright Act, Amended, Chapter 1. Subject matter and scope of copyright, & sect; 101. Definition, koji navodi: A "computer program" is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.

<sup>12</sup> Besarović V., Prednosti autorsko-pravne zaštite računarskih programa, Beograd, Anali Pravnog fakulteta u Beogradu, br. 2 - 3/89, str. 164.

Pored razlike koja se pravi izmedju odredjenja računarskih programa u užem i širem smislu sa stanovišta pravne zaštite<sup>13</sup>, neophodno je i uočiti **faze kroz koje prolazi proces njegovog stvaranja**<sup>14</sup>: **prva faza** sastoji se u stvaranju programskog koncepta na osnovu koga, i postavljenih korisničkih zahteva (ili zahteva naručioca), će nastati budući program; u **drugoj fazi** obavlja se programska priprema i u kojoj se pored algoritama koriste i blok dijagrami, dijagrami toka podataka, varijeteti dijagrami i drugi instrumenti na osnovu kojih će se prikazati utvrdjeni programski koncepti; **treća faza** je faza samog stvaranja programa, a taj proces stvaralaštva za rezultat ima tvorevinu kojoj treba obezbediti pravnu zaštitu. Pojedini autori<sup>15</sup> smatraju da postoji i faza kompajliranja, koja za pravo postaje relevantna zbog pravnog tretmana prevedenog programa - **četvrta**, zatim linkovanja - **peta**, i na kraju i kreiranja radne verzije na ROM čipu - **šesta**<sup>16</sup>. Ova poslednja faza, iako se primenjuje u samo malom procentu napravljenih programa, ostala je sporna jer predstavlja izradu mehaničkih pravila ili deo mašine. Upravo će ova faza biti zanimljiva u odnosu na patentnu zaštitu.

Od računarskih programa trebalo bi razlikovati programske jezike i oblike u kojima se program nalazi.

**Programski jezici** (*computer languages*) **predstavljaju definisani set simbola kojima se upravlja pomoću definisanih pravila**<sup>17</sup>. Njihova suština je da omogućе programerima da rade na visokom nivou apstrakcije umesto na nivou na kom kompjuter startuje program. Program je uvek napisan na nekom programskom jeziku, te je jezik sastavni deo programa. Za pravo postaje značajno kad se program napisan na jednom jeziku prebacuje na drugi i kako to pravno tretirati.

Računarski programi mogu se pojaviti u različitim verzijama: izvornoj, objektnoj i izvršnoj, odn., računarski programi mogu se naći u tri oblika: izvornom, objektnom (prevedenom), izvršnom i pseudo kodu. Za pravnike naročito je bila važna razlika izmedju objektnog i izvornog koda, odn. izmedju izvorne i objektnе verzije.

<sup>13</sup> Besarović V., op. cit., str. 163; Lipner S., Kalman S., Computer Law, Cases and Materials, Columbus, Merrill Publishing Company, 1989., str. 3. Intellectual Property Issues in Software, Washington, National Academy Press, 1992., str. 9.

<sup>14</sup> Od procesa kreiranja programa treba razlikovati **proces razvoja softvera** (*software developing*) koji sadrži osam koraka: od specificiranja problema i definisanja konstanti; dizajniranja eksterijala; dizajniranja interijala; transformacije dizajna u kod; testiranje, retestiranje, testiranje ponovo; izrada dokumentacije za korisnika; "paketiciranje" i iznošenje na tržište; i podrška gotovom proizvodu. Preuzeto iz knjige Intellectual Property Issues in Software, Washington, National Academy Press, 1992. str. 46.

<sup>15</sup> Lipner S., Kalman S., op. cit., str. 3.

<sup>16</sup> Intellectual Property Issues in Software, Washington, National Academy Press, 1992., str. 46.

<sup>17</sup> Burnside J. W. K., op. cit., str. 29.

**Izvorni kod** (*source code*) ili **izvorna verzija programa** (*source code version*) je program u formi u kojoj ga piše programer.

**Objektni kod** (*object code* ili *machine code*) ili **objektna verzija programa** (*object code version*) je program izražen u binarnim znacima, a nastaje nakon prevodjenja izvornog, programerski napisanog, programa pomoću nekog od programa prevodilaca<sup>18</sup>.

**Izvršni kod**, odn. **verzija** (*task version* ili *execute version*) je verzija programa koja se stvarno izvršava. Sve ostalo su pripremne verzije. Doduše, za pravo ova verzija je irelevantna.

**Pseudo kod** (*pseudocode*) je vrsta koda u kome su programske instrukcije pisane korišćenjem simboličke prezentacije koda operacija i adresa, a što zahteva prevodjenje na mašinski kod, korišćenjem kompajlera, pre nego što se program pusti u rad.

Znači, razlike između izvornog i objektnog koda od izuzetne je važnosti<sup>19</sup>. Za programera izvorni kod je lako razumljiv i obezbeđuje razumevanje logike i strukture programa i omogućuje mu da napravi alternative i modifikacije. S druge strane, ukoliko bi programer imao samo pristup objektnom kodu on ne bi mogao da napravi bilo kakvu značajnu promenu na programu. Otuda velika zainteresovanost za pristup izvornom kodu naročito kad se žele ispraviti bagovi<sup>20</sup> ili kad se želi povećati vrednost programa (odn. softvera). Istovremeno, lak pristup izvornom kodu omogućuje znalcima da prave plagijate ili da se upuste u piratstvo<sup>21</sup>. Tada na scenu stupaju pravnici koji treba da se angažuju u pripremi odgovarajućih pravnih propisa kojima bi se regulisali ovi problemi i ukoliko oni nastanu i sankcionisali počinioci.

Da bi izvorni kod imao odgovarajući tretman neophodno je da se, prilikom sklapanja ugovora između proizvođača računarskih programa (softvera) i korisnika o izradi i/ili korišćenju programa, odredi da li korisnik uopšte, i pod kojim uslovima, može da mu pristupi. Uskladjivanje interesa tvorca programa i korisnika dovelo je do

---

<sup>18</sup> Posebno je pitanje pravnog tretmana objektnog koda, odn. da li se on može podvesti pod literarno delo, prevod ili njegova reprodukcija, adaptacija.

<sup>19</sup> Burnside J. W. K., op. cit., str. 29.

<sup>20</sup> Eng. *bug* (buba, mana, defekt, kvar) je bilo koja greška ili zlonamerna funkcija kompjuterskog programa ili sistema.

<sup>21</sup> Burnside J. W. K., op. cit., str. 30.

toga da su mnogi proizvođači, kao uslov za svoj opstanak, videli u tome da drže izvorni kod deponovan na sigurnom mestu, često u bankama ili kod sebe, a da se korisniku samo izuzetno dozvoljava pristup.

### 2.3. Izgled korisničkog interfejsa na monitoru

Poseban problem pojavio se oko zaštite **izgleda korisničkog interfejsa na monitoru** (*user interface*), kao i njegovih delova - **ikona** (*icon*), **koji sadrže unapred definisane skupove naredbi, procedura i komandi kojim se program prikazuje korisniku**<sup>22</sup> i **preko koga ga korisnik "vidi i oseća"** (*"look and feel"*). Korisnički interfejs je, u suštini, posrednik između računara i korisnika. Njegov izgled, ponekad, predstavlja originalno rešenje. Zaštitu takvog rešenja pokušali su da dobiju proizvođači softvera čiji je korisnički interfejs imao dobro koncipirane i, na osnovu prethodno sprovedenih studija korisničkih zahteva, navika i prakse, dizajnirane izgleda. Mnogi od tih izgleda postali su maltene standardi. Softverske firme koje su želele da iskoriste te "standardne" izgleda su ih, po pravilu, bez saglasnosti kopirale i tako sebi povećale klijentelu naviklu na takve interfejse, ali i smanjile troškove kreiranja i dizajniranja sopstvenih rešenja. To je izazvalo ogorčenje kod tvoraca najčešće kompiliranih interfejsa (poznat je *Lotus, Apple Computer INC.*). Mnogi od kompilatora u SAD (čak i *Microsoft, Hawlett-Pacard*, a o malim softverskim kućama da se i ne govori) bili su tuženi. Jedan od najčuvenijih sudskih sporova započet je 1987. a okončan 1990. godine, i izazvao je ne samo veliko interesovanje već i mnogobrojne polemike. Bio je to spor *Lotus Development Corporation v. Paperback Software*, u kome je druga firma bila tužena radi direktnog kopiranja interfejsa, u čiji su razvoj ne samo uložena znatna sredstva, već i mnoga očekivanja o budućim prednostima u odnosu na konkurente<sup>23</sup>. Drugi, ništa manje poznat, bio je i spor *ATARI INC v. North American Phillips Electronics Corp.*, u kome je tužitelj pokrenuo spor zbog narušavanja autorskih prava i nelojalne utakmice za njegovu audio-vizuelnu igru *PAC-MAN*, od strane optuženog igrom istog tipa nazvanom *K. C. Munchkin*<sup>24</sup>. Međutim, kako ne postoji jedinstveno mišljenje da li se korisnički interfejsi mogu zaštititi kao originalna dela autorskim pravom to su i odluke sudova bile šarenolike<sup>25</sup>. Jedan od najčešće isticanih

<sup>22</sup> Lipner S., Kalman S., op. cit., str. 584.

<sup>23</sup> Samuelson P., How to Interpret the Lotus Design (And How Not To), *Communications of ACM*, no. 11/90., str. 27 - 33.

<sup>24</sup> Lipner S., Kalman S., op. cit., str. 41 - 50.

<sup>25</sup> U Kanadi je to prevaziđeno priznavanjem mogućnosti autorskopravne zaštite ukoliko su ispunjeni uslovi, međutim, postavilo se pitanje "fiksiranja" na medijumu. O svemu više kod Hendersona, G. F., op. cit., str. 4.

argumenata protiv njihove autorskopravne zaštite<sup>26</sup> je sprečavanje monopolskog položaja vodećih softverskih kompanija kojim bi se, s jedne strane, ograničavalo stvaranje novih rešenja, a s druge, zaustavio opšti trend standardizacije i inkompatibilizacije softvera različitih proizvođača (na to se pozivao i čuveni sudija Keeton u Lotus-om sporu). Iako se čini da je isticanje ovih argumenata sasvim opravdano ipak je ostalo niz pitanja koje u vezi sa zaštitom korisničkog interfejsa treba rešiti. Jedno je, uz prtpostavku da se radi o stvaralačkom delu, svakako, da se u ovom slučaju ne poštuje autorstvo i ne zaštićuju tvorci takvih, udobnih i elegantnih, rešenja, što je protivno prirodi autorskog prava. S druge strane, ako bi se ova rešenja posmatrala u kontekstu računarskih programa, nema razloga da se programi štite, a originalno rešenje vezano za izgled ekrana ne. Zar i zaštita računarskih programa ne predstavlja obezbeđivanje monopolističkog položaja? Kako je ovo još uvek pravno nejedinstveno rešeno to o zaštiti "look and feel" kompjuterskih programa tek treba povesti računa<sup>27</sup>.

#### 2.4. *Proizvod reverzibilnog programiranja*

Poseban predmet zaštite je računarski program nastao kao **proizvod reverzibilnog programiranja** (*reverse programming*), koji se sve češće pojavljuje u fokusu prava, s jedne strane, kao nešto čime se "dodiruje" osnovna ideja tvorca programa, a dolaženje do nje znači i otkrivanje cele logike rešenja određenog programskog problema, a, s druge, i ovaj se postupak smatra određenim intelektualnim postupkom samo što je intelektualna tvorevina dobijena njime istovetna sa određenom drugom, do koje se i želelo doći. Uopšte, reverzibilno programiranje osvetljava jednu, do sada, tamnu stranu intelektualnog stvaralaštva - slobodu ideje i njenu kontraverzu, monopol ekspoloatacije.

Slični predmet su i kompilacije, koje mogu, ali ne moraju biti rezultat reverzibilnog inženjerstva, a čija se zaštita sve više stavlja u žižu. Tim više, što se kompilacija može odnositi na programe, softver i podatke (odn. baze podataka).

#### 2.5. *Kompjuterski generisano delo*

<sup>26</sup> Lipner S., Kalman S., op. cit., str. 92-104; Erdelez S., Prikaz i analiza autorskopravne zaštite računarskih programa u SFRJ, Zakonitost, br. 7 - 9/90, str. 880.

<sup>27</sup> Samuelson P., The Ups and Downs of Look and Feel, Communications of ACM, vol. 43, no. 4/93, str. 29 - 35; Dossick S., User - Interface Copyrights: Obstacles to Innovation, IEEE Technology and Security Magazine, Fall 1994, str. 23 - 27.

Naravno, poseban problem i kako tretirati **kompjuterski generisano delo** (*computer generated work*), odn. **kompjuterski asistirano** (*computer-assisted* ili *computer-aided work*), kao što je muzičko ili literarno delo nastalo bez ljudskog autora dela. Mnoga su prava propustila da ih uopšte i konstatuju, a ona koja to ipak jesu tretiraju ih kao delo čoveka i to onoga koji je preduzeo sve aranžmane neophodne za njihov nastanak.

Vodeći računa o ovim mogućim predmetima pravne zaštite<sup>28</sup>, mada je ideo svakog od njih nesumnjivo vrlo veliki, ipak je bitno istaći da se kao prioritetni predmet u gotovo svim pravnim sistemima pojavljuju kompjuterski programi, a, retko, softver. Pri tome se mora poći od činjenice da hibridnim tehnologijama odgovaraju i hibridni sistemi pravnih rešenja<sup>29</sup>.

### 3. Oblici zaštite

Informaciono razvijene zemlje vrlo brzo su nakon prvih velikih ekonomskih eksploatacija i distribucija računarskih programa shvatile da je neophodna njihova pravna zaštita. U početku su se rešenja nalazila u **ugovorima**, kojima se prenosilo vlasništvo (kupoprodajom) ili pravo korišćenja (davanjem programa u zakup), i sl.<sup>30</sup> Međutim, vrlo brzo se pokazalo da se ugovorima ne može pružiti dovoljna zaštita jer oni važe za ugovorne strane (*inter partes*), a ne i prema ostalima (*erga omnes*) što znači da se ne može pružiti "univerzalna" zaštita koja bi se odnosila na sva ona lica koja mogu da dodju u kontakt sa njima. Ovo postaje naročito ozbiljno onda kad se tržište počinje zasipati sve jeftinijim računarima koje je trebalo opskrbiti i odgovarajućim programima. Tada se sve više ukazuje na brzo narastajuću potrebu da se računarski programi zaštite nekim drugim pravnim instrumentima i na drugi način.

<sup>28</sup> Commission of the European Communities, Green Paper: Copyright and Related Rights in Information Society, Brussels, COM(95)182 final; Commission of the European Communities, White Paper: Growth Competitiveness, Employment - the Challenges and Ways Forward into Twenty - first Century, Corfu, ISBN 92-826-74, 1994; Dyson E., Intellectual Property in the Net, Release, 1.0. 12./94; Norderhaug T., Oberding J., Designing a web of intellectual property, Computer Networks and ISDN Systems, no. 27/95., str. 1037 - 1045.

<sup>29</sup> Lehman B., Baker J., Oblon M., Intellectual Property and National Information Infrastructure (The White Paper) dokument koji je pripremila Radna grupa po nalogu predsednika Klintonu radi atikulacije nacionalne informacione infrastrukture i prava, a koji je podnet Kongresu septembra 1995. Materijal od 250 strana rezultat je dvogodišnjeg rada eksperata u Radnoj grupi i javnih rasprava nakon završenja prve verzije nazvane Green Paper. Ovaj dokument preuzet je sa Interneta.

<sup>30</sup> Edwards C., Savage N., Walden J., op. cit., str. 48.

Jedno od ponudjenih i obručke prihvaćenih rešenja pružilo je **Pravo intelektualne svojine**. Šta je to Pravo intelektualne svojine? Najkraće rečeno to je posebna grana prava<sup>31</sup> koja obuhvata *pravne norme kojima se reguliše skup duhovnih tvorevina povodom kojih, njihovi tvorci - autori imaju zakonom određena ovlašćenja moralnog i imovinskog karaktera*. Ono je zajednički naziv za Pravo industrijske svojine i Autorsko pravo<sup>32</sup>.

**Pravo industrijske svojine predstavlja skup pravnih normi kojima se regulišu tri grupe pojava i odnosa u društvu**<sup>33</sup>.

Prva grupa pojava i odnosa vezana je za kreativni rad **pronalazački rad**, čiji se rezultati mogu pojaviti kao: **1) pronalasci, 2) tehničke inovacije i 3) know-how**.

Druga su grupa pojava i odnosa **znaci razlikovanja**, koje čine: **1) modeli i uzorci, 2) robni i žigovi usluga i 3) oznake zemlje porekla**.

Treća grupa pojava različita je po svojoj pravnoj prirodi i dugo se nije ni smatrala delom Prava industrijske svojine. To je **pravo regulisanja zaštite od nelojalne utakmice**.

Suština tvorevina industrijske svojine vezana je za njihovu eksploataciju u privrednoj delatnosti i procesu rada. Otuda postoji velika zainteresovanost svake države da podstiče nastanak i korišćenje ovih dela i razvoj ovog prava jer se time povećava stepen njene razvijenosti i bogatstva.

Drugačiji duh i svrhu ima **Autorsko pravo**. *Ono je skup pravnih normi kojima se regulišu odnosi i pojave u vezi sa stvaranjem i korišćenjem autorskog dela iz oblasti književnosti, nauke i umetnosti*<sup>34</sup>. Samo ovo pravo obuhvata **objektivno**<sup>35</sup> i **subjektivno pravo**<sup>36</sup>.

<sup>31</sup> Detaljnije o Pravu intelektualne svojine kod Drakulić M., Osnovi Poslovnog prava, Beograd, FON, 1995., str. 185 - 265.

<sup>32</sup> Besarović V., Pravo industrijske svojine i autorsko pravo, Beograd, NIO Poslovna politika, 1984., str. 20.

<sup>33</sup> Besarović V., Savremeni koncept prava industrijske svojine, edicija: Pravo industrijske svojine, Beograd, Savez inženjera i tehničara Jugoslavije, 1988., str. 33.

<sup>34</sup> Besarović V., op. cit., str. 187.

Kompjuterski programi postali su veoma atraktivni predmet zaštite Pravom intelektualne svojine, bilo da su industrijska svojina ili autorsko delo. Priznanje kompetentnosti ovih instituta računarskim programima teklo je u više navrata, više etapa i sa različitim uspehom.

Danas su se u mnogim zemljama uglavnom iskristalisala patentna i autorskopravna zaštita. S obzirom da se najviše sudskih sporova pokreće, ali i najveći broj objekata zaštićuje Pravom intelektualne svojine u SAD, to je uzet primer procentualnog učešća pojedinih oblika zaštite u odnosu na pojedine objekte<sup>37</sup>.

***Patentnopravna i autorskopravna podrška pojedinim objektima KT***

| Patentna i autorska podrška |                      |              |           |                |                |
|-----------------------------|----------------------|--------------|-----------|----------------|----------------|
| Objekt zaštite              | Autorsko pravo (u %) | Patent (u %) | Oba (u %) | Ni jedna (u %) | Broj slučajeva |
| Izvorni kod                 | 86                   | 2            | 3         | 9              | 318            |
| Objektni kod                | 65                   | 2            | 3         | 30             | 293            |
| Pseudo kod                  | 37                   | 1            | 1         | 61             | 278            |
| Modularni dizajn            | 18                   | 9            | 1         | 72             | 269            |
| Algoritmi                   | 9                    | 12           | 1         | 78             | 303            |
| Komande kor. interf.        | 6                    | 1            | 0         | 93             | 294            |
| Ikone                       | 43                   | 0            | 1         | 56             | 307            |
| Layout kor. interf.         | 19                   | 1            | 1         | 79             | 302            |
| Sekvence kor. interf.       | 9                    | 1            | 0         | 90             | 295            |
| Look and feel               | 5                    | 0            | 0         | 95             | 312            |
| Funkcionalnost kor. interf. | 5                    | 4            | 0         | 91             | 300            |
| Kompjuterski imidž          | 81                   | 1            | 0         | 18             | 316            |

### *3.1. Kompjuterski programi i patentnopravna zaštita*

#### *3.1.1. Opšte napomene o patentnopravnoj zaštiti*

<sup>35</sup> **Objektivno** autorsko pravo čine norme kojima se određuje pojam i vrste autorskog dela, sadržina subjektivnog autorskog prava, ovlašćenja drugih lica vezanih za autorsko delo, vremensko trajanje pravne zaštite, prenos autorskog prava za života autora i posle njegove smrti i posebni vidovi pravne zaštite koji stoje na raspolaganju u slučaju povrede nekog od njegovih prava.

<sup>36</sup> **Subjektivno** autorsko pravo predstavlja ono pravo koje se priznaje autorima kao tvorcima književnog, naučnog ili umetničkog dela na njegovoj duhovnoj tvorevini.

<sup>37</sup> Samuelson P., Denber M., Glushko N., Developments on the Intellectual Property Front, Communication of ACM, vol. 34, no. 6/92, str. 35.

Da bi se kompjuterski programi mogli zaštititi patentom oni moraju biti pronalazak<sup>38</sup>. **Pronalazak je novo rešenje inventivnog nivoa nekog tehničkog problema koje se može primeniti u nekoj od privrednih delatnosti**<sup>39</sup>. Predmet pronalaska može biti proizvod, postupak i primena proizvoda ili postupka. **Kad se pronalazak pravno zaštiti on postaje patent.**

### 3.1.1.1. Uslovi i postupak sticanja prava na patent

Pronalazak postaje patent samo ako ispunjava uslove koji su predviđeni odgovarajućim pravnim propisima neke zemlje. Većina zemalja predviđa slične uslove, često se rukovodeći odredbama međunarodnih akata. Tako je i kod nas<sup>40</sup>. Da bi neki pronalazak mogao da dobije patentnu zaštitu mora da ispuni **uslove patentibilnosti**:

- a) da je **novost**, što znači da nije obuhvaćen stanjem tehnike<sup>41</sup>, odn. da nije bio dostupan javnosti pre podnošenja prijave za priznavanje;
- b) da ima određeni **inventivni nivo**, što znači da ponudjeno rešenje određenog problema za stručnjaka ne proizlazi, na određen način, iz stanja tehnike. Za mali patent zahteva se niži inventivni nivo od patenta što pretpostavlja da je rezultat rada koji prevazilazi rutinsko korišćenje stanja tehnike od strane stručnjaka<sup>42</sup>;
- c) **primenljivost** pretpostavlja da je pronalazak primenljiv u industrijskoj ili drugoj delatnosti, što proširuje mogućnosti primene pronalaska ne samo u industriji već i u trgovini, poljoprivredi i drugim delatnostima<sup>43</sup>;
- d) mnoga prava danas, kao i naše pravo nekada, predviđaju da pronalazak mora imati i **tehničku izvodljivost**, kao mogućnost da prosečni stručnjak bez, inventivnog napora, ponovi, materijalizuje, pronalazak, na osnovu podataka koji su navedeni u patentnoj prijavi. U ovom uslovu upravo se sagledava i suština ovog prava industrijske svojine.

<sup>38</sup> Pronalazak treba razlikovati od **otkrića** novih stvari ili prirodnih sila (nove biljke, nove rase, i sl.) ili prirodnih zakona i naučnih metoda, koji su i ranije postojali ali nisu bili poznati. Otkrića se, zbog opšteg interesa (civilizacije, čovečanstva) ne izuzimaju od opšte upotrebe, za razliku od pronalazaka. Da bi se autorima otkrića priznala neka prava dodeljuju im se diplome, nagrade, povlastice i sl.

<sup>39</sup> Besarović V., op. cit., str. 13.

<sup>40</sup> Zakon o patentima, Službeni list SR Jugoslavije, br. 15/95, čl. 5.

<sup>41</sup> Pod stanjem tehnike podrazumevaju se sva tehnička rešenja dostupna javnosti (čl. 6. Zakona o patentima SRJ)

<sup>42</sup> Zakon o patentima SRJ, čl. 9. st. 2.

<sup>43</sup> Besarović V., op. cit., str. 48 i 49; Zakon o patentima, čl. 10.

Da bi pronalazak bio zaštićen patentom nužno je da prodje određenu proceduru priznavanja. Priznavanje prava na patent, vrši se **po postupku**, najčešće, upravnom, koji ima po gotovo svim zakonima i međunarodnim aktima nekoliko faza. Po pravilu su to tri **faze**<sup>44</sup>:

1. podnošenje prijave i zahteva za priznavanje prava čini **fazu pokretanja postupka** za zaštitu pronalaska;
2. **ispitivanje** formalne i materijalne sadržine prijave i donošenje rešenja o priznavanju ili odbijanju traženog prava; i
3. **registrovanje** priznatog prava, zajedno sa izdavanjem isprave o priznatom pravu, objavom, štampanjem i stavljanjem spisa na uvid javnosti.

Prijavu podnosi sam pronalazač, mada je mogu podneti i druga, zakonom predviđena, lica. Kad se nadležnom organu, kod nas je to Savezni zavod za zaštitu intelektualne svojine (Savezni zavod), podnese prijava on mora konstatovati tačno vreme (dan i čas) kad je prijava podneta kako bi se moglo utvrditi **pravo prvenstva**. Ovo pravo<sup>45</sup> ima dvostruki značaj - **priznaje prioriteta i ekskluziviteta** podnosiocu u dobijanju zaštite ukoliko mu ona bude potrebna u odnosu na sva druga lica koja kasnije podnesu prijavu za iste ili slične oblike pronalazaka. Vreme po kom se računa pravo prvenstva značajno je i zbog rokova koji od tog trenutka počinju da teku<sup>46</sup>.

Nadležni organ utvrđuje ispunjenje formalnih i materijalnih uslova za sticanje prava, pa ukoliko utvrdi da su ispunjeni, izdaje rešenje, upisuje priznato pravo u registar, izdaje ispravu, objavljuje i stavlja na uvid javnosti patentni spis.

<sup>44</sup> Zakon o patentima Ruske federacije, 1992; Zakon o o patentima Danske, 1992; Zakon o zaštiti pronalazaka patentom Rumunije, 1991; Zakon o patentima SRJ, čl. 13 - 56; i mnogi drugi novijeg i starijeg datuma doneti zakoni.

<sup>45</sup> Besarović V., op. cit., str. 93; Zakon o patentima SRJ, čl. 30.

<sup>46</sup> Pariska konvencija čl. 4.

### 3.1.1.2. Sadržina prava na patent

Pronalazak koji ispunjava uslove patentibilnosti i koji je snabdeven patentom osigurava da njegov tvorac uopšte, pa i kompjuterskog programa, kako je predviđeno mnogim pravima, pa i našim, ima određena: moralna i materijalna **prava**. Suština **moralnih prava je u tome da se pronalazač naznači u patentnoj prijavi i u svim ispravama** (spisima, registrima, publikacijama) koje su vezane za njegov pronalazak<sup>47</sup>. **Materijalna prava** su kompleksna i sastoje se<sup>48</sup> od:

- a) prava **korišćenja** svog pronalaska;
- b) **monopolskog prava zabrane** drugim licima da ga koriste;
- c) prava **raspolaganja**; i
- d) prava **na naknadu** ukoliko ga neko drugi koristi.

Pravo na pronalazak može se prenositi, a kad mu se prizna patent lice na koje se prava prenose postaje **nosilac prava na patent** i stiče isključivo pravo apsolutnog karaktera, mada vremenski i teritorijalno ograničenog. Mnogi pravni sistemi, naš takodje, kao ključnu sadržinu prava na patent, predviđaju upravo materijalno-pravna ovlašćenje nosioca patenta<sup>49</sup> (iskorišćavanja, sprečavanja korišćenja drugih<sup>50</sup>, raspolaganja i ostvarivanja naknade za korišćenje od strane drugih).

Poseban je tretman *službenog pronalaska*, kao pronalaska nastalog u procesu rada (kod nas u radnom odnosu). **Pravo na zaštitu ima poslodavac** ukoliko je pronalazak nastao dok je zaposleni izvršavao svoje redovne radne obaveze ili naložene zadatke (npr. vezane za naučno - tehničko istraživanje i razvoj, ili po ugovoru o istraživačkom radu) ukoliko nije nešto drugo posebno ugovoreno. U slučaju da je pronalazak zaštićen na ime poslodavca, njegov tvorac ima uobičajeno moralno pravo i pravo na naknadu (ukoliko postoje ekonomski efekti korišćenja).

**Pravo na zaštitu ima zaposleni** ukoliko je u pitanju *poluslužbeni pronalazak*, odn. pronalazak stvoren u vezi sa aktivnostima poslodavca ili korišćenjem materijalno-tehničkih sredstava, informacija i dugih uslova koje stvara poslodavac, a ne

<sup>47</sup> Uredba o ratifikaciji Pariska konvencija za zaštitu industrijske svojine, Službeni list SFRJ, Međunarodni ugovori i drugi sporazumi, br. 5/74, čl. 4 ter; Zakon o patentima SRJ, čl. 12.

<sup>48</sup> Besarović V., op. cit., str. 56.

<sup>49</sup> Zakon o patentima SRJ, čl. 56.

<sup>50</sup> Sporazum o trgovinskim aspektima prava intelektualne svojine GATT-a, čl. 28., tč. 1.

radi se o uobičajenom delu iz redovne obaveze ili naloženog zadatka. Poslodavac ima pravo ekonomskog iskorišćavanja uz obavezu isplate naknade zaposlenom.

Specifičan je slučaj kad pronalazak stvori zaposleni u određenom roku (kod nas od 1 godine) **po prestanku radnog odnosa**, dakle bivši zaposleni, a koji bi da je stvoren u toku radnog odnosa nastao u obavljanju redovnih obaveza ili posebno poverenih obaveza, ili je u vezi sa redovnom aktivnošću poslodavca, odn. njegovim sredstvima.

Za ove će pronalaskе važiti poseban režim i posebni rokovi. Mnoga prava, pa i naše, posebno propisuju **obavezu čuvanja tajnosti ovakvih pronalazaka** (zaposleni i poslodavac dužni su čuvati njihovu tajnost sve dok ne budu objavljeni ili na drugi način dostupni javnosti), s tim da poslodavac može tražiti od zaposlenog da, u određenim okolnostima, čuva tajnu pronalaska i kad radni odnos prestane<sup>51</sup>. Pored ovog uslova često se zahteva ispunjenje i drugih prethodnih uslova (kod nas npr. da njihovo korišćenje ne može otpočeti ukoliko nisu rešena pitanja naknade).

Kako je osnovni cilj svakog prava na pronalazak da se on koristi to tvorac ovog dela industrijske svojine korišćenje može da obavlja sam, ali i da ga prenese, odgovarajućim pravnim sredstvima, na drugo lice ili lica (fizička ili pravna). Najčešće on to čini **ugovorom**. Ugovorima pronalazač, ili nosilac patenta može prenositi svoje pravo u potpunosti - **cesijom** ili delimično ustupanjem samo prava privrednog iskorišćavanja zaštićenog prava zainteresovanom licu na određeno vreme ili za određenu teritoriju - **licenca**, pri čemu su ugovori o licenci osnovni način pravnog prometa patenta<sup>52</sup>.

### 3.1.1.3. Trajanje

Većina zemalja, i naša, predviđaju da je **dužina trajanja patenta 20 godina**, odn. 10 godina za mali patent, **od dana podnošenja prijave**<sup>53</sup>.

Pravo patenta, i malog patenta, **prestaje**: **a)** neplaćanjem predviđene takse; **b)** odricanjem nosioca prava svog prava; **c)** smrću, odn. prestankom nosioca prava; **d)**

<sup>51</sup> Zakon o patentima SRJ, čl. 95 - 109.

<sup>52</sup> Besarović V., op. cit., str. 108 - 127; Verona A., op. cit., str. 94 - 96; Drakulić M., op. cit., str. 225 - 248.

<sup>53</sup> Po pravu SAD taj rok je 17 godina.

poništajem priznatog prava; e) oglašavanjem ništavim rešenja o priznavanju prava; i f) osporavanjem svojstva nosioca.

Kad je u pitanju računarski program ili softver davno započeta debata o mogućnosti njegove zaštite patentnim pravom još uvek nije završena. Postojanje oscilacija u određenim periodima samo su dokaz da se o ovom obliku zaštite ozbiljno razmišlja i pokušava naći odgovarajući način da se revidiraju veoma prisutne dileme oko njegovog tehničkog karaktera i ispunjenja uslova apsolutne novosti. Za sada je preovladalo shvatanje da programi nisu pronalasci, pa i ne mogu uživati patentnu zaštitu<sup>54</sup>. Ipak, neophodno je ova shvatanja staviti pod lupu sumnje jer su sve prisutniji pomaci u odnosu na tretman određenih instituta, pojmova (proširuje se npr. i pojam algoritma) i/ili sadržaja, što će mnoga izuzeća pretvoriti u bespredmetna. Isto tako, uveliko se preispituju i karakteristike određenih duhovnih tvorevina (npr. tehničkog karaktera programa), što, takodje, može dovesti do određenih promena. Za očekivanje su novi pristupi zaštiti i njenim objektima.

### 3.1.2. *Kompjuterski programi i nacionalni propisi zaštite patenta*

Do sredine 70-ih u malom broju zemalja problem pravne zaštite kompjuterskih programa pokušao se rešiti patentnim pravom, iako je postojalo, gotovo dominantno, mišljenje da je to teško ostvarljivo. Većina evrokontinentalnih zemalja, već tada, nije prihvatila patentibilnost kompjuterskih programa i kao najelegantnije rešenje *explicite* ga isključivala odgovarajućim propisima. Anglosaksonske zemlje, naročito SAD, pokušavale su pronaći pukotine, prilično se mučeći u sudskim sporovima, ne bi li ih, ipak, nekako "provukle kroz iglene uši prava". Tako su, poznati sudski sporovi koji su u to vreme vođeni u SAD *Gattshalk via Benson* (1972.) i *Parker via Flok* (1978.), a nešto kasniji *Diamond via Diehr* (1981), ušli u istoriju zaštite, ne samo radi usvojenih rešenja, već i postupka utvrđivanja osnova patentibilnosti pojedinih tipova računarskih programa. Oni su, u stvari, ukazali na svu neadekvatnost, a *priori*, odbijanja patentne zaštite. Slična je situacija bila i u Australiji gde je Patentni biro još 1966. godine odbio *N. V. Phillips Gloeilampenfabriken's Application* 36 AOJP 2392 radi neispunjavanja uslova novosti, a potom sledi i veći broj drugih (*British Petroleum C. Ltd. Applications* iz 1968; *Texas Instruments Inc's Application* iz iste godine, i sl.). Zanimljivo je da je za svaku od ovih prvih patentnih prijava bivao pozivan isti službenik Mr Asman, koji je odluke obrazlagao ranijim odlukama House of Lords (npr. iz spora *British United Shoe*

<sup>54</sup> Arsić Z., Patentnopravna zaštita kompjuterskog programa, Zbornik radova, Novi Sad, Pravni fakultet u Novom Sadu, 1988., str. 147; Besarović V., op. cit., str. 165; Bainbridge D., op. cit., str. 44 - 47.

*Machinery Company Limited v. Standard Rotary Machine CO. Ltd.*, iz 1918. godine po kojoj je zahtev bio odbijen jer mašina samo obuhvata ideju *per se*), a koje je primenjivao i na kompjuterske programe<sup>55</sup>.

Period između sredine 70-ih i druge polovine 80-ih bio je period napuštanja ove solucije i primarnosti autorskopravne zaštite.

Ubrzani razvoj softverske industrije ponovo ukazuje na neophodnost promene stava patentne zaštite prema kompjuterskim programima. Takođe, u SAD ni u prethodnom periodu (npr. od kasnih 60-ih do kraja 1992, zabeleženo je 9.000 patentiranih softvera, a samo u 1992. je izdato 1.300 patenata, što znači između 20 i 30 ih je izdato svake nedelje, a samo po neki su deo hardvera)<sup>56</sup> nije se napustio ovaj oblik zaštite što se pokazalo opravdanim. **Pod uticajem potreba i već provereno uspešnih rešenja počelo je ponovno razmatranje mogućnosti da se kompjuterski programi štite i patentnim pravom.** Naročito, kako ističu mnogi autori, kad su u pitanju novi operativni sistemi u ROM-u koji su, uz novi uređaj, mogli da predstavljaju i novo tehničko rešenje. Tada bi se mogla primeniti patentna zaštita, naravno, pod uslovom da se uz patentnu prijavu za zaštitu uređaja zahteva i zaštita programa (softvera) koji ga podržava. Ovakvi slučajevi proširivani su i na računarski program kojim se utvrđuje nov postupak proizvodnje<sup>57</sup>, kao deo tehničkog rešenja, čak, i ukoliko sadrži algoritam. Bio je to još jedan pokušaj, no, ne, u potpunosti, i neuspeo. Sve se češće u teoriji, ali i sudskim sporovima počinje fleksibilnije gledati na ove probleme i tolerantnije prihvatati argumenti *pro*, a ne samo *contra*<sup>58</sup>.

Dugo se jedan od glavnih uzročnika negativnog stava prema patentnoj zaštiti programa i softvera nalazio u tumačenju da li oni mogu da zadovolje uslov koji se za svaki pronalazak traži - da predstavljaju novost tehničkog rešenja<sup>59</sup>. Isto tako<sup>60</sup>, poseban problem pojavio se u obimu elemenata obuhvaćenih programom kod softvera koji mogu da ispunе uslov novosti. Pojavilo se mišljenje **da program u užem smislu ne bi mogao**

<sup>55</sup> Vebber D., *Patents and Trade Marks for Hardware and Software*, edicija: *Essays on Computer Law*, Melbourne, Longman Professional, Pty, 1990., str. 102 - 108.

<sup>56</sup> Aharonian G., *Setting The Record Straight On Patents*, *Communication of ACM*, vol. 34., no.1/93., str.17.

<sup>57</sup> Brown J., *The current status of copyright protection for computer software and some patent parallels*, London, *A Frank Cass Professional Journal, Computer Law & Practice*, br. 5/90., str. 172.

<sup>58</sup> Aharonian G., op. cit., str.17 i 18.

<sup>59</sup> Dworkin G., *The Patentability of Computer Software*, edicija: *Computer Law*, London, Blackstone Press Limited, 1990., str. 110.

<sup>60</sup> Besarović V., *Prednosti autorskopravne zaštite računarskih programa*, Beograd, *Anali Pravnog fakulteta u Beogradu*, br. 2 - 3/89., str. 165.

**da bude predmet patentne zaštite pošto ne može da ispuni uslov apsolutne novosti.** Naime, niz instrukcija, ma koliko njihov poredak u programu može izgledati kao novost, odn. nov, ne predstavlja novost. S druge strane, u pravnoj doktrini i praksi matematičke formule, naučna otkrića i naučne teorije, kao ni planovi, principi, ni metode u vezi sa obavljanjem umnog rada ili privrednih aktivnosti ne smatraju se pronalaskom, pa se, s toga, ne mogu ni zaštititi patentnim pravom<sup>61</sup>. Po takvom shvatanju, znači, **algoritam (kao metod), kao sastavni deo programskog koncepta, ne bi mogao da uživa patentnu zaštitu, pa zbog toga to ne može ni samo delo čiji je on sastavni element, odn. računarski program u širem smislu.** Medjutim, sam programski koncept, ukoliko ne sadrži algoritam, ako zadovoljava uslov apsolutne novosti (i druge uslove), mogao bi da uživa patentnu zaštitu kad je u pitanju računarski program i sam softver čija je idejna osnova po intelektualnoj sadržini slična ideji o pronalasku<sup>62</sup>. Drugim rečima, samo jedan deo računarskog programa ili softvera, i to programski koncept koji nije algoritam, mogao bi da bude predmetom patentne zaštite. Kako je utvrđivanje postojanja novosti u programskom konceptu predstavljalo posebnu teškoću i prolazilo kroz komplikovanu proceduru to se često napuštala ideja o patentnoj zaštiti programa i softvera. Upravo u ovom smislu grupisale su se zemlje u primeni patentne zaštite računarskih programa.

U nekim zemljama (Holandija, Madjarska), **eksplicitno se izostavljaju svi kompjuterski programi iz zakonima predviđene patentne zaštite i to se dosledno primenjuje u sudskoj praksi.** Ova rešenja su mahom vezana za evrokontinentalno pravo, ali su sve glasnjiji protesti, naročito zemalja u razvoju<sup>63</sup>.

U drugoj grupi zemalja (SAD, jedino za sada) **zakonima se isključuje patentna zaštita samih kompjuterskih programa "kao takvih",** podrazumevajući pod njima programe, pre svega, u užem smislu. Kad su u pitanju programi u širem smislu sudovi, u sporovima koji povodom zaštite programa nastaju, preispituju ovo rešenje. Naime, **za računarske programe čiji programski koncept zadovoljava uslov novosti u sudskoj praksi se preispituje i, ponekad, presudjuje u smislu odobravanja njegove patentne zaštite.** Preispitivanje se, po *Freeman testu*<sup>64</sup> odvija u dva pravca:

<sup>61</sup> Videti npr. čl. 52. t. 2. Konvencije o evropskom patentu.

<sup>62</sup> Besarović V., op. cit., str. 165.

<sup>63</sup> Reichman J. H., Uticaj TRIPS Nacrta ugovora na konkurentnost zemalja u razvoju na integrisanom svetskom tržištu, Patentni glasnik, br. 1/94., str. 125 - 127.

<sup>64</sup> Freeman test je prvi put sproveden u SAD u slučaju In re Freeman 197 USPQ 464., i postao je pravilo za rad.

1. Ispituje se da li programski koncept obuhvata algoritam ili ne. Ukoliko ga obuhvata ispituje se da li se njime *utvrđuje nova struktura ili novi oblici, pa, ako je to tako onda može doći do patentne zaštite*. Ako to ne postoji izuzimaju se iz patentne zaštite jer nije prihvaćena inicijativa Patentnog zavoda SAD data u posebnom **Uputstvu za proceduru ispitivanja patenta** (*Manual of Patent Examining Procedure*) koji je u algoritmu video<sup>65</sup> određenu *step-by-step* proceduru i određeni proces ili skup pravila radi čega ga je moguće uključiti u patentnu zaštitu.
2. Ukoliko *ne obuhvataju "algoritam"* u matematičkom smislu dalje ispitivanje je znatno olakšano jer to znači da ne postoje uslovi zabrane, pa, ako se ispunjavaju drugi uslovi može se patentirati.

Slično SAD-u, u Japanu<sup>66</sup> je Patentni zavod doneo i koristi "**Standarde za ispitivanje kompjuterskih programa kao pronalazaka**" koji se u svakom pojedinačnom slučaju koriste ne bi li se utvrdila činjenica da program "predstavlja tehničku ideju za korišćenje prirodnih zakona".

Pod uticajem SAD počinje i u drugim zemljama (Japan, Kanada) revidiranje stavova i **fleksibilno se omogućuje patentna zaštita računarskih programa, ali onih koji proširuju memoriju kompjutera i imaju tehnički karakter**, najčešće operativnim sistemima i grafikama, koji ispunjavaju uslov tehničkog karaktera novosti<sup>67</sup>. Pri tome se mora istaći da broj takvih programa nije baš mali, ali s obzirom da se radi o programima i softverima koji nisu radjeni za svakodnevnu i kućnu upotrebu, ili retko za nju (većina takvih softverskih tehnika ima suviše niski stepen novosti), to ukazuje na još jednu narastajuću opasnost - koncentraciju takvih patenata u rukama malog broja organizacija. Tako 12% od svih patentom zaštićenih softvera u SAD su vlasništvo IBM (oko 1000, npr. u 1992., od 1300 registrovanih) i ni jedna im se druga firma ne može približiti, što je slično i sa Japanom gde Hitachi ostavlja za sobom kompanije kao što je Toshiba, Fujitsi, Fanuc, Sharp, Mitsubishi<sup>68</sup>. Ovoj grupi zemalja priključuje se i V. Britanija koja, u principu, izostavlja patentnu zaštitu računarskih programa u zakonu, eksplicitno navodeći da oni nisu patentibilni kao takvi (Zakon o patentu iz 1977. i Zakon o autorskom pravu, dizajnu i patentu iz 1988. godine), ali

<sup>65</sup> Lipner S., Kalman., op. cit., str. 143 - 151.

<sup>66</sup> Japan je inače revidirao svoj Zakon o patentima, a revizija je stupila na snagu 01. 01. 1994., po kojoj je kompjuterskim programima isključena zaštita.

<sup>67</sup> Aharonian G., op. cit., str. 17 i 18., navodi da je većina softvera koji je npr. 1992. godine prijavljena za patentnu zaštitu upravo vezana za mašinu ili je deo nekog procesa, a računa se da je bar 3% od ukupno prijavljenih pronalazaka i softverskih patenata, takvih koji zahtevaju kompletnu reviziju sistema jer se ne uklapaju u postojeća odredjenja.

<sup>68</sup> Aharonian G., op. cit., str. 17.

dozvoljava njihovu indirektnu patentnu zaštitu, kao dela patenta mašine. Istovremeno se u praksi i teoriji raspravljaju dva seriozna pitanja: **a)** da li tako zaštićen program znači da kompjuter ukoliko ga ne sadrži ne bi bio patentiran. Slučaj *Merrill Lynch, Piers Fenner&Smith Incorporated's Applocation* (1988.) je upravo tako presudjen<sup>69</sup>; i **b)** može li se prihvatiti celishodnost ovakve zaštite kada samo oni programi koji idu uz računar i predstavljaju njegov "sastavni deo" dobijaju mogućnost indirektno zaštite dok drugi, možda istog tipa, koji nisu imali "sreću" da se pojave kao prateći deo računara koji se želi patentirati, ostaju nezaštićeni. Naročito onda kad se takav program radi po porudžbini, pa naručilac posla odustane usled čega program ostane van zaštite ili je radjen od male firme koja nema u programu hardver i/ili procese, što, opet, dovodi do problema dominacije giganata, s jedne, kao i pritisaka, nepravdnosti, s druge strane.

I na kraju, ima zemalja, doduše sve manje, koje **ignorišu kompjuterske programe kao objekt zaštite uopšte, pa i patentnim pravom.**

### 3.1.3. *Kompjuterski programi i medjunarodna zaštita patenta*

#### 3.1.3.1. *Pariska konvencija za zaštitu industrijske svojine*

I naravno, za zaštitu kompjuterskih programa patentom značajna je i **Pariska konvencija za zaštitu industrijske svojine** (*Paris Convention for Protection of Industrial Property*) iz 1883, revidirane 1900, 1911, 1925, 1934, 1958. godine. Po njoj pod **patentom se podrazumevaju razne vrste industrijskih patenata primljenih od zakonodavstava zemalja Unije kao patentni uvoza, patentni za usavršavanje, dopunski patentni i sertifikati, i sl.** S obzirom da se njome ne predviđaju uslovi koje treba da zadovolji neko delo da bi bilo pronalazak koji se može patentno zaštititi, to se ova solucija odnosi i na kompjuterske programe, prevashodno one koji se nalaze zajedno sa drugim pronalaskom. S druge strane, po ovakvom odredjenju ne postoje neke suštinske smetnje da se, ako dodje do revizije shvatanja uslova patentibilnosti ili karakteristika programa, oni, ipak, nadju zaštićeni patentom kao takvi. I u jednom i u drugom slučaju pripadnici svake zemlje Unije<sup>70</sup> uživaće (kao što i sada uživaju) u ostalim zemljama prava po **principima jednakog tretmana i minimalnih prava.** Znači, ukoliko bi se u jednoj zemlji priznala patentna prava domaćem tvorcu kompjuterskih programa, tada bi se isto to, i pod istim uslovima,

<sup>69</sup> Bainbridge D., op. cit., str. 48.

<sup>70</sup> 1992. godine Pariska Unija je imala 105 zemalja članica.

moralo priznati i strancu. Pored istih prava pripadnici svake zemlje Unije će imati i istu zaštitu ukoliko dodje do povrede njihovih prava, naravno, ukoliko ispunjavaju uslove koje mora da ispunjava domaći titular patentnih prava kompjuterskih programa<sup>71</sup>.

Godine 1991. na diplomatskoj konferenciji u Hagu WIPO-a razmatran je **Nacrt Ugovora kojim se dopunjuje Pariska konvencija za zaštitu intelektualne svojine** (Ugovor o patentu), čiji članovi o uslovima patentibilnosti, pravima iz patenta i zaštiti prava mogu biti od znatne važnosti za kompjuterske programe koji su sastavni deo nekog drugog pronalaska.

### 3.1.3.2. *Konvencija o evropskom patentu*

Kao povod za formiranje tvrdokornog shvatanja o nepatentibilnosti kompjuterskih programa uopšte poslužilo je i rešenje koje je predvidela **Konvencija o evropskom patentu** (*European Patent Convention*) iz 1973. godine sa izmenama i dopunama iz 1978. godine i po kojima računarski programi nisu patentibilni jer ne ispunjavaju jedan od tri obavezna i kumulativna uslova koji obezbeđuju patentibilnost<sup>72</sup>. Vrlo brzo ovo rešenje su prihvatili zakoni mnogih evropskih zemalja (mada su se pod njenim uticajem ona našla i u vanevropskim, čak i SAD), kao i sudovi u rešavanju sporova vezanih za kršenje nekog od prava u odnosu na korišćenje ili registraciju programa i softvera<sup>73</sup>. Međutim, **ova Konvencija izuzela je iz patentne zaštite "kompjuterski program kao takav"**, što je dovelo do niza nesuglasica i nesporazuma. Jedna je<sup>74</sup>, svakako, vezana za one programe kojima se omogućuje rad računara na nov ili poboljšan način. Oni se ne mogu podvesti pod termin "kompjuterski program kao takav" i trebalo bi da se dozvoli, uz pretpostavku ispunjenja drugih uslova, njegova patentna zaštita. Ovakvom rešenju sklon je i **Vodič Evropskog patentnog zavoda** iz 1985., koji u C-IV, 2.3 kaže: "Kompjuterski program biće nepatentibilan kao takav ili ukoliko je na nekom medijumu. Situacija se nije promenila ni kad je kompjuterski program ugrađen u već poznati kompjuter"<sup>75</sup>. U istom Vodiču preporučuje se patentibilnost ne programa kao takvih, već nekog drugog pronalaska koji može biti u formi pogodnoj programiranom računaru. Pri tome se vodi računa da li je u pitanju tehnički ili netehnički efekat koji pronalazak ima. Znači, program kojim se

<sup>71</sup> Pariska Konvencija za zaštitu industrijske svojine, od 20. marta 1983., Medjunarodni ugovori i drugi sporazumi, Službeni list SFRJ, br. 20/74., čl/ 2.1.

<sup>72</sup> Edwards C., Savage N., Walden I., op. cit., str. 48.

<sup>73</sup> Tapper C., op., cit., str. 6; Edwards C., Savage N., Walden I., op. cit., str. 48 - 51.

<sup>74</sup> Arsić Z., op. cit., str. 149.

<sup>75</sup> Edwards C., Savage N., Walden I., op. cit., str. 48.

rešava na novi način neki tehnički proces ili problem može se naći u situaciji da bude ocenjen kao patentibilan. Ukoliko ispunjava uslove, zaštita će mu trajati 20 godina od datuma podnošenja prijave<sup>76</sup>. Kako je na osnovu ovakvih stavova priznato ili odbačeno više zahteva mnogih evropskih i neevropskih firmi, npr. IBM, to se oni uzimaju kao primeri koje ilustruju ovakva rešenja. Tako je IBM bio odbijen od Evropskog Patentnog zavoda i Žalbenog veća za zaštitu programa "*spell checker*" (zaveden kao T121/85, 1989.), "*document abstracting and retrieving*" (T22/85 iz 1988.) i "*linguistic expression processing*" (T52/85, 1989), sa obrazloženjem da su to programi koji se koriste u ne-tehničke svrhe. Četvrtom programu (T6/83 iz 1988.) priznata je patentibilnost jer je imao "tehničke efekte" pošto je bio vezan za koordinaciju i kontrolu mreže procesora podataka u njihovoj komunikaciji<sup>77</sup>.

### 3.1.3.3. Ugovor o saradnji na području patenata

Da bi se olakšalo sticanje patenata u raznim zemljama potpisan je u Vašingtonu 1970. godine **Ugovor o saradnji na području patenata** (*Patent Cooperation Treaty*), kojim se uprošćava **procedura za međunarodnu zaštitu**. Od 1978. godine, kad je otpočela njegova primena, WIPO-u je stiglo na desetine hiljada nacionalnih prijava, dok u zemljama ugovornicama broj međunarodnih prijava doseže stotine hiljada<sup>78</sup>. Sama jedinstvena međunarodna prijava patenta na kompjuterskom programu, po ovom Ugovoru, može se podneti jednom nacionalnom patentnom zavodu (zavod primaoc) na jednom od službenih jezika, a imaće isti pravni učinak u onoliko zemalja Unije (oko 50, među kojima su i one najrazvijenije) koliko je prijavilac označio (prosečno u 31). Postupak ispitivanja ispunjenja uslova (franc. *recherche - rešerša*) može sprovoditi nacionalni zavod ili međunarodna ustanova (Međunarodni patentni biro u Hagu, u početku je to bio Međunarodni institut za patente)<sup>79</sup>. Ukoliko to želi, zemlja potpisnica Ugovora može posebno ratifikovati deo koji se odnosi na prethodno međunarodno ispitivanje prijave. Ono je poverljive prirode i dostavlja se samo podnosiocu prijave i Međunarodnom birou. Međunarodni biro u predviđenom roku podnosi izveštaj o ispitivanju koji predstavlja osnov za konačno rešenje. Ovaj Ugovor, koji je Jugoslavija potpisala i ratifikovala, prate detaljna pravila za

<sup>76</sup> Konvencija o evropskom patentu, čl. 63., koji je revidiran na diplomatskoj konferenciji 1991. godine, mada se revizija odnosi na pronalazke čija komercijalna eksploatacija sledi tek nakon dugotrajnih i skupih istraživanja i višegodišnjeg postupka puštanja u promet (lekova, npr.).

<sup>77</sup> Edwards C., Savage N., Walden I., op. cit., str. 50.

<sup>78</sup> Poredjenja radi Međunarodnom birou je 1979. god. podneto 2.625 prijava, dok je 1993. to bilo 28.577. Ukupan broj međunarodnih prijava na osnovu PCT do 1992. god. je 132.910., čime je zamenjeno oko 500.000 nacionalnih prijava (1993. je to 900.000), Patentni glasnik, br. 1/94., str. 132.

<sup>79</sup> Ugovor o saradnji u oblasti patenata, čl. 16.

spровodjenje kojima se olakšava sprovođenje patentne zaštite i centralizuje međunarodno objavljivanje međunarodnih prijava<sup>80</sup>.

#### *3.1.3.4. Ugovor o rešavanju sporova između država u oblasti intelektualne svojine*

Osim ovih međunarodnih akata u toku je donošenje novih ili značajne revizije postojećih. Takav međunarodni akt je i Nacrt **Ugovora o rešavanju sporova između država u oblasti intelektualne svojine**, koji je u nekoliko navrata razmatran od strane Komiteta eksperata WIPO-a od 1989. godine kada je formiran. U svega 18 članova pokušava se premostiti jaz među zemljama nastao radi različitosti tumačenja i primene međunarodnih odredbi ugovora iz intelektualne svojine<sup>81</sup>. Ako se kao predmet takvih ugovora nadju i kompjuterski programi, svakako da bi ovaj Ugovor imao određenu važnosti u sprovođenju jedinstvene procedure njihovog rešavanja.

#### *3.1.3.5. Sporazum o trgovinskim aspektima prava intelektualne svojine*

**Sporazum o trgovinskim aspektima prava intelektualne svojine** GATT-a (*Agreement On Trade - Related Aspects Of Intellectual Property Rights*) je donet u okviru Urugvajске runde 1992., a stupio na snagu 01. 01. 1995.<sup>82</sup>, a primena mu je obavezna tek po isteku roka od godine dana od dana stupanja na snagu. Zemlje u razvoju, kao i zemlje u procesu transformacije, imaju pravo da ovaj rok pomere za 4 godine. Najmanje razvijene, pak, zemlje imaju prelazni rok od 10 godina za obaveznu primenu Sporazuma, nakon isteka godine dana, ali uz odluku Saveta za trgovinske aspekte prava intelektualne svojine. Za to vreme razvijene zemlje će obezbediti podsticaje preduzećima sa svoje teritorije da unaprede i podstiču transfer tehnologije sa ovim zemljama. Nakon isteka prelaznog perioda obavezno se preispituje

<sup>80</sup> Prvi set CD-ROM diskova na kojima se nalaze međunarodne prijave objavljen je 1989. god., a izdat je 1993. godine.

<sup>81</sup> Totić B., Nacrt Ugovora o rešavanju sporova između država u oblasti intelektualne svojine, Patentni glasnik, br. 1/92., str. 282 - 284.

<sup>82</sup> Ovaj je Sporazum deo Finalnog akta GATT-a, o čemu više Drakulić M., Osnovi poslovnog prava, Beograd, FON, 1995., str. 186 -189; Drakulić M., GATT i Međunarodni trgovinski aspekti prava na intelektualnu svojinu - konsekvence Urugvajске runde, Zbornik radova: Zlatibor, IV Međunarodni Simpozijum SYM - ORG '95., str. 289.

sprovođenje Sporazuma, a nakon tog perioda svake dve godine će se realizovati ponovno preispitivanje, čiji rezultati i/ili konkretni predlozi predstavljaju osnove za dopune jedino u smislu prilagođavanja višem stepenu zaštite. Dakle, nema revidiranja u snižavanju nivoa, obima dostupnosti, sprečavanja zloupotreba i drugih pravila predviđenih ovim Sporazumom.

Ovim Sporazumom predviđeno je da se **patenti mogu dodeliti za pronalaskе iz svih oblasti tehnike, pod uslovom da su novi, da sadrže inventivni nivo i da se mogu primeniti u industriji**. Kako se kompjuterskim programima, na osnovu drugih međunarodnih akata na kojima se Sporazum bazira, negira svojstvo pronalaska, iako se Sporazumom to izričito ne određuje, to se njegove odredbe mogu na njih primenjivati samo ukoliko se radi o nekom drugom pronalasku čiji je on deo, i u tom slučaju prate ih sva prava koja pripadaju za glavni pronalazak. Znači,<sup>83</sup> **kompjuterski programi** će biti, kao i glavni patenti, **dostupni**, a patentna prava se mogu koristiti bez diskriminacije u odnosu na mesto pronalaska, oblast tehnike i to da li se radi o uvezenim ili lokalno proizvedenim proizvodima. Oni, doduše, mogu biti **isključeni**, zajedno sa osnovnim patentom, iz **komercijalne eksploatacije** na teritoriji zemalja članica ukoliko je to nužno da bi se zaštitili javni red i moral, uključujući i zaštitu života i zdravlja ljudi, životne sredine.

Na osnovu osnovnog patenta i **titulari kompjuterskog programa** imaće određena prava da: **a) spreče** treća lica koja nemaju saglasnost titulara da proizvode, koriste, nude na prodaju, prodaju ili uvoze predmet patenta; **b) spreče** treća lica koja nemaju saglasnost da vrše delo korišćenja, nudjenja na prodaju, prodaju ili uvoze u svrhe proizvode koji su direktno dobijeni na osnovu patentiranog postupka; **c) prenose** ili **ustupaju** patent u nasleđe ili da zaključuju licencne ugovore.

Postoje strogo propisani i predviđeni slučajevi kada će se kompjuterski programi, zajedno sa osnovnim patentom, moći **koristiti bez dozvole titula** za drugu upotrebu. To će biti u slučaju prinudne licence, unakrsne licence "prvog" i "drugog" patenta, i sl.

Trajanje patenta na **kompjuterskim programima**, kao i "prvom" patentu, je **20 godina od datuma podnošenja prijave**.

**Zaštita se sprovodi u građanskim i upravnim postupcima**, pri čemu se može prekršiocu prava naložiti plaćanje naknade za štitu koju je pretrpeo zbog povrede,

<sup>83</sup> Sporazum o trgovinskim aspektima prava na intelektualnu svojinu, čl. 27 - 35.

isplatu sudskih troškova, a što je najvažnije može se naložiti da *robu koja je povreda prava povuče*, bez naknade, iz trgovinskih tokova, pa u određenim slučajevima i *uništi*. Pored ovih mogu se izreći i *privremene mere, posebne prekogranične i krivične mere*.

S obzirom da se radi o međunarodnoj trgovini kompjuterskim programima i na njihovu zaštitu<sup>84</sup> će se primenjivati, Sporazum predviđena, dva osnovna principa: **nacionalnog tretmana i tretmana najpovlašćenije nacije**. Prvi princip predstavlja osnovu da se stranim državljanima<sup>85</sup> tvorcima i nosiocima prava intelektualne svojine priznaje takav tretman u zaštiti koji nije ni na koji način nepovoljniji od tretmana domaćih državljana. Drugim rečima to znači da se u odnosu na zaštitu prava intelektualne svojine strane ugovornice obavezuju da će na jednak način tretirati domaće i strane državljane, naravno uz pretpostavku da je minimum upravo ovaj predviđen u Sporazumu, a da nacionalna zakonodavstva mogu predvideti i sveobuhvatniju zaštitu. Drugi princip znači da ukoliko neka od država (strana) ugovornica prizna prednosti, povlastice ili imunitete vezane za zaštitu intelektualne svojine državljaninu bilo koje druge države to će odmah i bezuslovno značiti da se ta ista prava i u istom obimu dodeljuju i državljanima svih drugih strana GATT-a<sup>86</sup>. Svakako da će u, Sporazumom, određenim slučajevima postojati mogućnost izuzeća od primene ovih principa, ali ona neće moći biti svojevlasno određivana od zemalja ugovornica, već tek na osnovu odluke novoformiranog **Saveta za trgovinske aspekte prava intelektualne svojine** (*Council for Trade - Related Aspects Of Intellectual Property Rights*)<sup>87</sup> u okviru Svetske trgovinske organizacije.

I na kraju, neophodno je istaći da mada je patentna zaštita kompjuterskih programa najsigurniji oblik zaštite, ona je i najrigorozniji što se međunarodnih i nacionalnih instrumenata tiče.

### 3.1.4. *Kompjuterski programi i patentna zaštita po našem pravu*

#### 3.1.4.1. *Obim, sadržina i trajanje prava na patent*

<sup>84</sup> Pod **zaštitom** se podrazumeva dostupnost, sticanje, obim prava, održavanje i zaštita prava intelektualne svojine, kao i korišćenje ovih prava, čl. 3 i 4 Sporazuma.

<sup>85</sup> Pod **stranim državljanom** podrazumevaju se fizička ili pravna lica koja ispunjavaju kriterijume za dobijanje zaštite po Pariskoj, konvenciji.

<sup>86</sup> Od 1995. godine GATT je zamenila **Svetska trgovinska organizacija** (*World Trade Organization*).

<sup>87</sup> Skraćenica *Council for Trade - Related Aspects Of Intellectual Property Rights* je **Council for TRIPS**

Naše zakonodavstvo, u više navrata i bez posebnih potresa, prihvatilo je rešenja data u Konvenciji o evropskom patentu. Kao i prethodni zakoni<sup>88</sup>, i važeći Zakon o patentima, eksplicitno je izuzeo "programe računara" uz "otkrića, naučne teorije, matematičke formule i ostala pravila, planove, metode i uputstva za duhovnu aktivnost" iz patentne zaštite. Međutim, prihvatajući ovo rešenje naš Zakon ipak nije bio dosledan jer nije prihvatio formulaciju "kao takav" čime se, uz nepostojanje odredjenja šta se pod programima računara tačno podrazumeva, pokazalo veliko nerazumevanje razlika koje postoje. Pogotovo što su Evropska organizacija za patente i njen Evropski zavod za patente, vremenom, donekle revidirali prvobitne odredbe Konvencije, dozvoljavajući patentibilnost operativnih sistema. S obzirom na te promene u shvatanjima čini se celishodnim da se pravna praznina nastala nedefinisanjem kompjuterskih programa i softvera može, bez posebnih problema, popuniti prihvatanjem rešenja ponudjenih u Vodiču i zakonodavstvima i sudskoj praksi drugih zemalja.

Medjutim, postojeće stanje pokazuje da **naše zakonodavstvo explicite isključuje patentnu zaštitu kompjuterskih programa, ne smatrajući ih pronalascima**. Nesporno je da **patentna zaštita kompjuterskih programa u užem smislu za sada nije moguća**, upravo što ne mogu zadovoljiti zahteve vezane za novost, inventivni nivo, a osobito što je veliko pitanje tumačenja njihovog tehničkog karaktera<sup>89</sup> jer je to upravo i jedno od osnovnih ograničenja i dilema. Ostaje i dalje sporno pitanje mogu li se zaštititi programi u širem smislu? Čini se<sup>90</sup> da, ipak, treba razmišljati o mogućnosti da se **patentna zaštita može odnositi na kompjuterske programe u širem smislu i to one čiji programski koncept sadrži algoritme shvaćene kao postupak, odn. u "nematematičkom smislu"**, naravno samo pod uslovom da se može utvrditi njihova patentibilnost. To znači da se kumulativno moraju ispuniti svi uslovi koji se od pronalaska zahtevaju da bi mogli da budu zaštićeni patentom. Posebno je veliki problem kako će se tretirati ispunjenje uslova apsolutne novosti tehničkog rešenja koju treba da ima program ili softver. Problem jeste veliki, ali nije nerešiv<sup>91</sup>.

<sup>88</sup> Zakon o zaštiti pronalazaka, tehničkih unapredjenja i znakova razlikovanja, Službeni list SFRJ, br. 34/81., 3/90., 20/90.

<sup>89</sup> Postoje tumačenja da su kompjuterski programi po svojoj prirodi "**uputstva ljudskom razumu**", no, to je još uvek pod velikom rezervom. O tome više kod Marković S., Zaštita računarskih programa patentom, autorskim pravom i pravom sui generis, Ljubljana, Jugoslovenski spoljnotrgovinski vodič, Pravni vodič, 1987., str. 73.

<sup>90</sup> Iz razlika koji su prihvaćeni i u drugim zemljama i pravnim sistemima, koji su ranije navedeni.

<sup>91</sup> Prihvatljivije je stanovište američke sudske prakse, kao i shvatanja koja zahtevaju da se serioznije, naročito u patentnim zavodima i sličnim telima, počine shvatati sva "umetnost softvera" i njihova kompleksnost, koja često prevazilazi prosečna znanja kojim se barata pri ocenjivanju patentibilnosti.

Naše pozitivno zakonodavstvo, za sada, **nije isključilo mogućnost indirektne patentne zaštite kompjuterskih programa**. To će biti slučaj kad se patentnom prijavom za zaštitu novih kompjutera, postupaka, primene proizvoda ili postupaka ili nekog drugog pronalaska koji može biti u formi pogodnoj programiranom računar i koji predstavlja rešenja na novi način nekog tehničkog procesa ili problema, obuhvati i računarski program i softver. Tada **računarski program prati drugi pronalazak, kao njegov deo**. Pošto prati drugi pronalazak, prati i njegovu pravnu sudbinu. To znači da će i tvorac kompjuterskih programa imati određena (ista) moralna i materijalna prava. Patent za takav kompjuterski program traje **20 godina** (odn. 10 godina za mali patent), od datuma podnošenja prijave. Podnosilac prijave, nosilac patenta i sticalac isključivog prava licence kompjuterskog programa i softvera imaju **pravo na odgovarajući pravni lek** protiv svakoga ko povredi njihovo pravo.

#### *3.1.4.2. Kompjuterski programi nastali u radnom odnosu*

Ukoliko su programi nastali u radnom odnosu poslodavac ima pravo na zaštitu ako je zaposleni stvorio program obavljajući svoje redovne radne obaveze ili posebno naložene zadatke, a u pitanju je naučno - tehničko istraživanje i razvoj, odn. izvršavanje obaveza iz ugovora o istraživačkom radu. Ako su osnovni pronalazak i prateći program nastali u vezi sa aktivnošću poslodavca ili korišćenjem njegovih materijalno - tehničkih sredstava, informacija i drugih uslova, tada je će oni biti zaštićeni na ime zaposlenog, a poslodavac ima pravo ekonomskog iskorišćavanja. I, kao i u drugim pravima, naše je pravo predvidelo poseban slučaj nastanka računarskog programa od strane bivšeg zaposlenog u roku od godine dana od prestanka radnog odnosa. Za takav program primenjivaće se pravila kao da je nastao za vreme trajanja radnog odnosa. Naravno, u svim ovim slučajevima zaposlenom pripada odgovarajuća naknada. Kolika će ona biti zavisi od opšteg akta, ugovora o radnopravnom odnosu ili posebnog ugovora između poslodavca i zaposlenog.

Pošto prati pravnu sudbinu osnovnog pronalaska, kompjuterski program će se registrovati po istoj i u istoj proceduri pred Saveznim zavodom, uz poštovanje istih rokova i istih zahteva.

Zanimljivo je da iako ova solucija patentne zaštite kompjuterskih programa nije baš najpogodnija, niti kod nas posebno učestala, ipak je sve češća tendencija njenog korišćenja. Razlog je jednostavan. Naime, u slučajevima kad je moguće koristiti ovaj oblik zaštite **on je veoma efikasan i pruža veću pravnu sigurnost nego što je to slučaj sa autorskim ili nekim drugim oblikom zaštite**. Naročito što je sve evidentnija i

težnja ka internacionalizaciji koja se ne može toliko adekvatno osigurati drugim oblicima sa "manje strogom prirodom". Zar nije pogodnije imati patent izdat u jednoj zemlji, a koji može imati ista pravna dejstva u drugim zemljama, naravno, ukoliko se ispune uslovi predviđeni određenim međunarodnim konvencijama, nego autorsko pravo, poslovnu tajnu, ili neki drugi institut? Internacionalizacija patenta se odnosi i na samo njegovo izdavanje, što znači da ono može biti traženo za jednu, više ili sve države članice neke organizacije ili unije. Pri tom se ne sme zaboraviti ni činjenica postojanja Evropske Unije u kojoj se postepeno dostiže harmonizacija prava, ali i slobodna cirkulacija ideja, roba i usluga, u čemu će sigurno veliki udeo imati i kompjuterski programi. Internacionalizacija patenata računarskih programa dobija nove dimenzije.

Naravno, ni naše pravo ne bi smelo da ostane po strani i svakako bi stalno trebalo preispitivati mogućnosti za direktnu patentnu zaštitu kompjuterskih programa.

#### 3.1.4.3. *Zaštita prava na patent*

Konkretna mere zaštite kompjuterskih programa proizlaze iz činjenice ugrožavanja prava na patent. Po jugoslovenskim propisima zaštita prava na patent kompjuterskih programa realizuje se po pozitivnom **Zakonu o patentima**. Ovaj *lex specialis* predviđa dva oblika zaštite: **gradjanskopravnu i kaznenopravnu**. Tome još treba dodati i **krivičnopravnu** zaštitu predviđenu **Krivičnim zakonom**.

**Gradjanskopravna** zaštita treba da osigura zaštitu nosilaca prava na patent od nedozvoljenog uznemiravanja trećih lica ili da omogući priznavanje svog "autorstva".

Zaštita nosioca prava postiže se tužbom<sup>92</sup>:

- zbog *povrede prava*;
- za *povredu prava iz prijave*;
- za *osporavanje prava na zaštitu*;
- za *zaštitom prava poslodavca*, odn. zaposlenog;
- za *utvrđivanje svojstva pronalazača*.

Tužbu protiv svakog lica koje povredi pravo podnosi podnosilac prijave, nosilac patenta i sticalac isključive licence.

---

<sup>92</sup> Zakon o patentima, čl. 77 - 89

**Povreda prava**, zbog koje se pokreće postupak, može biti neposredna ili posredna, zavisno od toga da li se, bez saglasnosti nosilaca prava, direktno ekonomski iskorišćava zaštićeni program ili se omogućava njegovo iskorišćavanje. Ukoliko se kompjuterski program kao patent **ekonomski iskorišćava**, bez dozvole nosioca patenta, postoji **neposredna povreda prava**. To se dešava ako se zaštićeni kompjuterski program koristi u proizvodnji, stavlja u promet kao proizvod izradjen prema zaštićenom programu ili se njima raspolaže. **Posredna povreda prava** postoji ako treće lice, bez saglasnosti nosioca prava, nudi, isporučuje ili stavlja u promet na drugi način delove uređaja (supstance, kompozicije ili materijala) koji se odnose na neki bitni element tudjeg zaštićenog programa, čime se **omogućava** drugom licu da neovlašćeno ekonomski iskorišćava zaštićeni kompjuterski program<sup>93</sup>. Nije povreda prava ukoliko lice koje nudi ili isporučuje delove uređaja (supstance, kompozicije, materijala) ne zna ili iz svih okolnosti nije moglo znati da su delovi pogodni i namenjeni za ekonomsko iskorišćavanje tudjeg zaštićenog programa ili su u pitanju takvi delovi koji predstavljaju proizvode uobičajene na tržištu, sem ako je lice kome su isporučeni time nije navedeno da neposredno povredi nosioca patenta.

Postupak se pokreće podnošenjem tužbe sudu. Njom se može zahtevati: **1)** utvrđivanje postojanja povrede prava; **2)** zabranjivanje radnji kojima se povređuje pravo; **3)** naknada štete; i **4)** objavljivanje presude (o trošku tuženog).

Ukoliko je šteta namerno prouzrokovana može se tražiti i naknada do trostrukog iznosa obične štete i izgubljene dobiti.

**Tužba za povredu** može se podneti u roku od 3 godine od dana saznavanja za povredu i počinioaca, ali ne posle isteka roka od 5 godina od dana učinjene povrede.

Tužbom za povredu se može zahtevati i izricanje **privremene mere zabrane radnji kojima se povređuje pravo**. Mera može trajati do pravosnažne presude. U posebnim okolnostima privremena mera može se tražiti i pre podnošenja tužbe, ako se tužba podnese u roku od 15 dana od podnošenja zahteva za određivanjem mere.

Ceo postupak po ovoj tužbi je hitan.

Kad je u pitanju tužba za povredu prava iz prijave sud prekida rešavanje do odluke Saveznog Zavoda o priznavanju ili odbacivanju (odbijanju) zahteva za priznavanje patenta na kompjuterskim programima.

---

<sup>93</sup> Zakon o patentima, čl. 56.

Ako se radi o **tužbi za osporavanje prava na zaštitu** tada pronalazač ili njegov pravni sledbenik, imaju pravo da zahtevaju utvrđivanje prava na zaštitu određenog kompjuterskog programa, umesto lica koje ga je prijavilo za zaštitu. Naime, ne retko se dešava da se kao podnosilac prijave umesto pronalazača pojavi neko drugo lice. Tada je sasvim normalno da dodje do utvrđivanja prava na zaštitu, a što čini sud na osnovu tužbe. Ova se tužba podnosi sve do okončanja postupka.

Medjutim, može se desiti da je rešenje o priznatom pravu na patent kompjuterskog programa već izdato, a da pronalazač (odn. njegov pravni sledbenik) tvrdi da ima pravo na patent umesto lica ili zajedno sa licem koje je nosilac zahteva. Tada se tužbom pokreće postupak za osporavanje prava na zaštitu i to u roku trajanja patenta.

Poseban je slučaj kada poslodavac, ili zaposleni, imaju pravo na zaštitu ili na ekonomsko iskorišćavanje kompjuterskog programa iz radnog odnosa, a da do toga ne dodje. Tada oni **tužbom za zaštitu prava poslodavca, odn. zaposlenog** mogu zahtevati od suda da utvrdi njihova prava i zaštitu. Ova tužba se pokreće u roku od 2 godine od dana objave prijave za priznanje patenta, ali ne nakon isteka 2 godine od dana prestanka radnog odnosa u čijem je trajanju program stvoren.

Ponekad se dešava da je u zahtevu za priznavanje prava ili u nekoj drugoj ispravi navedeno drugo lice kao tvorac (pronalažač) kompjuterskog programa. Tada pravi tvorac ima pravo na ispravku. On će to realizovati **tužbom za utvrđivanje svojstva pronalazača**. Na osnovu tužbe i podnetih dokaza sud utvrđuje to njegovo svojstvo i nalaže upis njegovog imena u odgovarajuće isprave i registre Saveznog Zavoda. Rok za ovu tužbu nije vremenski ograničen. Ukoliko tvorac umre pravo na tužbu imaju njegovi naslednici.

**Kaznenopravna zaštita** može se primenjivati u slučajevima nedozvoljenog ponašanja u vezi sa korišćenjem zaštićenih prava na patent kompjuterskih programa. U pitanju je **privredni prestup** ili **prekršaj** preduzeća ili pravnog lica<sup>94</sup>.

Preduzeće ili drugo pravno lice kazniće se za teže oblike ugrožavanja i povrede prava na patent kompjuterskih programa kao za **privredni prestup** u više slučajeva.

---

<sup>94</sup> Zakon o patentima, čl. 110 i 111.

Ukoliko se desi da u proizvodnji dodje *do neovlašćenog korišćenja zaštićenog programa ili neovlašćenog stavljanja u promet predmeta izradjenih prema zaštićenom programu ili neovlašćenog raspolaganja patentom*, tada je u pitanju delo privrednog prestupa.

Ako preduzeće ili drugo pravno lice objavi poverljivi kompjuterski program, kao pronalazak, ili zatraži zaštitu poverljivog kompjuterskog programa u inostranstvu bez odobrenja saveznog organa nadležnog za poslove odbrane i tada je načinilo privredni prestup.

Za ova dela preduzeća ili druga pravna lica kažnjavaju se **novčanom kaznom** (od 5.000 do 50.000 dinara), a, takodje, i odgovorno lice (500 do 5.000 dinara).

Nedozvoljeno ponašanje može biti i **prekršaj**. Zakon je predvideo nekoliko takvih situacija.

Ukoliko organizacija ili drugo pravno lice zatraži zaštitu kompjuterskog programa u inostranstvu pre isteka roka od 3 meseca od dana podnošenja prijave nadležnom saveznom organu, čini prekršaj za koji treba da bude kažnjano.

Takodje, ako preduzeće ili drugo pravno lice otkrije kompjuterski program pre nego što bude objavljena prijava za priznanje patenta ili on postane na drugi način dostupan javnosti, opet je u pitanju nedozvoljeno ponašanje i prekršaj.

Naravno, ukoliko se preduzeće ili drugo pravno lice neovlašćeno bavi zastupanjem stranih pravnih i fizičkih lica i tada je u pitanju prekršaj.

Za sva takva dela prekršaja predviđene **kazne su novčane** (od 1.000 do 50.000 dinara) za preduzeće ili drugo pravno lice. Pored njih novčano se kažnjavaju i odgovorna lica u preduzeću ili drugom pravnom (500 do 1.500 dinara), kao i pojedinac koji je nedozvoljenu radnju učinio (500 do 1.500 dinara)<sup>95</sup>.

I kao najrigorozniji oblik zaštite našim, a i gotovo svim zakonima drugih zemalja, predviđena je i **krivičnopravna zaštita**. Po Krivičnom zakonu SRJ za

---

<sup>95</sup> Zakon o patentima, čl. 110 i 111.

**krivično delo povrede pronalaska**<sup>96</sup>, će se primeniti krivičnopravna zaštita u dva slučaja:

1. *neovlašćene upotrebe tuđeg prijavljenog ili zaštićenog kompjuterskog programa*, kao pronalaska, i to nije bilo kakvo neovlašćeno korišćene krivično delo, već ono koje se vrši u privrednom prometu; i
2. *neovlašćenog objavljivanja suštine prijavljenog kompjuterskog programa*, kao pronalaska, pre nego što je objavljen na način utvrđen zakonom.

Za povredu pronalazačkog prava kao krivičnog dela predviđena je strožija kazna nego kad je u pitanju kaznenopravna zaštita po Zakonu o patentima. U slučaju neovlašćene upotrebe tuđeg prijavljenog ili zaštićenog kompjuterskog programa, kao pronalaska, **kazna za počinioca je zatvor** od 3 meseca do 5 godina, a za drugo delo (neovlašćeno objavljivanje prijavljenog kompjuterskog programa) do 1 godine. Da bi bio odgovoran za ovo, kao i druga krivična dela, počinitelj mora biti uračunljiv, odn. biti svestan povrede kompjuterskog programa koju čini i hteti njeno izvršenje ili svestan da, usled njegovog činjenja ili nečinjenja, može nastupiti zabranjena posledica, s tim što na njeno ispunjenje pristaje.

---

<sup>96</sup> Krivični zakon Savezne Republike Jugoslavije, Službeni list SFRJ, br. 44/76; 34/84; 57/89; 3/90; 38/90; i Službeni list SRJ br. 35/92; 37/93 i 24/94. čl. 250.

### 3.2. *Kompjuterski programi i zaštita žigom*

#### 3.2.1. *Opšte napomene o zaštiti žigom*

Kompjuterski programi i softver su roba i to svojevrsna. Pojavljuju se na tržištu i u prometu. Veoma često se dešava da se u prometu pojave dva ili više slična, pa, čak, i ista programa. Kako ih razlikovati? Po proizvođaču, po nazivu, po ambalaži, po sklopu i rasporedu boja, po znacima kojim se obeležavaju, ili po svemu ovome zajedno? Jedan od odgovora je - po znacima razlikovanja<sup>97</sup> koji služe za obeležavanje i razlikovanje robe koja se pojavljuje u privrednom prometu<sup>98</sup>. Znači razlikovanja su pravo i to **apsolutno** jer sadrže dve vrste **ovlašćenja**: pozitivno i negativno. Pozitivno ovlašćenje sastoji se u pravu nosioca da koristi predmet zaštite, dok je negativno vezano za pravo nosioca da zabrani drugim licima nedozvoljeno korišćenje prava<sup>99</sup>. Takodje, svi znaci razlikovanja, izuzimajući oznaku porekla proizvoda, pored zaštite predviđene za dela industrijske svojine mogu uživati i autorskopravnu zaštitu. Osim toga, oni se često zloupotrebljavaju, te su i predmet nelojalne utakmice, pa ih je nužno štititi tim pravom.

Zajednička odlika pravne zaštite svih znakova razlikovanja je u teritorijalnom, a, za neke od njih, i u vremenskom ograničenju važenja. Teritorijalno ograničenje znači da prava vezana za znake razlikovanja važe na teritoriji zemlje koja ih je priznala. Vremensko ograničenje, ukoliko je predviđeno pozitivnim propisima, znači da zaštitu uživa autor i nosilac nekog od zaštićenih prava u određenom periodu i nakon njegovog isticanja delo postaje opšte dobro (*public domain*).

Što se vrste znaka kojim se mogu zaštititi kompjuterski programi tiče oni su retko vezani za modele i uzorke, a, s obzirom na njihovu prirodu gotovo nikad i za oznaku zemlje porekla. Na prvi pogled to izgleda sasvim logično i normalno. Naime, oznaka porekla vezuje se za prirodna svojstva određenog geografskog područja. Tako

<sup>97</sup> Besarović V., op. cit., str. 14; Verona A., op. cit., str. 143.

<sup>98</sup> Većina autora ističe da svi znaci razlikovanja da bi živali pravnu zaštitu moraju ispuniti **tri slična uslova**: **a) distinktivnost**, znači da svi znaci koji služe za razlikovanje i obeležavanje robe moraju da se razlikuju od postojećih i da budu novi u privrednom prometu; **b) primenljivost u privrednom prometu** bez obzira o kom se proizvodu radi (industrijskom, zanatskom, uslužnoj delatnosti); i c) gotovo svi znaci razlikovanja (izuzev oznake porekla proizvoda) **moraju predstavljati rezultat stvaralačkog rada** svog autora, npr. Besarović V., op. cit., str. 69 - 70.

<sup>99</sup> Besarović V., Savremeni koncept prava industrijske svojine, edicija: Pravo industrijske svojine, Beograd, Savez inženjera i tehničara Jugoslavije, 1988., str. 35.

shvaćeno, ovo pravo nema mesta u zaštiti računarskih programa ili softvera. Međutim, oznaka porekla u novije vreme označava i veštinu ljudi sa nekog područja. U tom slučaju ovo bi se pravo moglo primeniti i na programe i softver u određenim slučajevima. Tako, zahvaljujući reputaciji, prevashodno, IBM-a, SAD je prihvaćen kao zemlja u kojoj izrada programa i softvera pretpostavlja određeni kvalitet tako da stavljanje oznake ima i garantnu funkciju. Istovremeno korišćenjem oznake zemlje porekla na prozvodima IBM ili drugih američkih kompanija ima značaja u odnosu na imitatorske i kompilatorske zemlje, čak i onda kad su određeni programi izradjivani u njima, a vodili se kao IBM-ovi. Međutim, situacija postaje mnogo složenija kad su u pitanju Tajland, Tajvan, Hong Kong, koji su svoju slavu "savršenog imitiranja" doveli dotle da njihova naznaka porekla počinje da označava i izuzetno dobar kvalitet (uz nisku cenu), što im daje prioritet u odnosu na mnoge informaciono razvijene zemlje, pa u poslednje vreme i sam SAD.

I pored revidiranja shvatanja o mogućnosti korišćenja oznake zemlje porekla i za računarske programe, ipak su oni u najčešće zaštićeni žigom. S obzirom da je **žig pravo kojim se štiti znak koji je u prometu namenjen za razlikovanje robe, odn. usluga iste ili slične vrste jednog fizičkog ili pravnog lica i da se on stavlja na robu ili njeno pakovanje, pa je vezan za telesne stvari (robni žig) ili služi za razlikovanje raznih usluga (žig usluga), to se njima mogu štiti i kompjuterski programi i softver**. I robni i žigovi usluga se mogu grafički predstavljati kao reči, slogani, slova ili kombinacija reči i slova, brojeva ili crteži i slike<sup>100</sup>. Takodje, oni mogu biti trodimenzionalni oblici, kao i video i audio oznake. Po pravilu, ne predviđaju se nikakva ograničenje u pogledu boje koja će se koristiti ili načina na koji će znaci biti ispisani. Svi elementi žiga uživaju pravnu zaštitu i to zajedno. Pravo na žig stiče se rešenjem nadležnog organa, najčešće posebnog zavoda za žigove, mada može biti i zajednički organ za patente, žigove, uzorke, modele, oznake zemlje porekla (kao kod nas Saveznog Zavoda za intelektualnu svojinu) i upisom žiga u odgovarajući registar. U nekim zemljama pravo na žig stiče se činjenicom njegove prve upotrebe (anglo-saksonsko pravo).

Znak je, dakle, veoma bitno obeležje proizvođača kompjuterskih programa i pružaoca softverskih usluga. Često se ističu sledeće **funkcije znaka zaštićenog žigom**, u opšte, a posebno kompjuterskih programa i softverskih usluga, u privrednom životu<sup>101</sup>: **1) identifikacija** proizvođača ili pružaoca usluga; **2) razlikovanje** jedne

<sup>100</sup> Zakon o žigovima, Službeni list SRJ, br. 15/95., čl. 4.

<sup>101</sup> Besarović V., op. cit., str. 79 - 81.

vrste programa i usluga od drugih istih ili sličnih; **3) garantovanje** određenog kvaliteta programa ili usluga;<sup>102</sup> i **4) propaganda**, jer je moćno sredstvo za reklamu.

### *3.2.1.1. Uslovi i postupak sticanja prava na žig*

Da bi znaci mogli da uživaju zaštitu kao robni ili žigovi usluga moraju ispunjavati **odredjene uslove**. Uslovi se najčešće nabrajaju korišćenjem generalne klauzule, a nekad se ona kombinuje sa negativnom enumeracijom kojom se isključuju sva ona svojstva koje ne bi smeo ili ne bi trebalo da ima znak koji se želi zaštititi.<sup>103</sup>

Suština prava na žig vezuje se za ovlašćenje nosioca žiga da upotrebljava zaštićeni žig u prometu za obeležavanje svoje robe ili usluga. Ovo je isključivo pravo nosioca prava na žig (po našem Zakonu nosilac prava na žig je pravno lice koje se bavi određenom delatnošću ili fizičko lice, pri čemu ono, pravno ili fizičko lice, može da bude naše ili strano). Ukoliko ima pravo na žig nosilac može žig stavljati na sam proizvod ili na pakovanje, u poslovne isprave i u reklamno-propagandne materijale.

**Postupak** za sticanje prava na žig je upravni postupak i sastoji se, po pravu većine zemalja, od **tri faze**<sup>104</sup>:

1. podnošenje prijave i zahteva za priznavanje prava čini **fazu pokretanja postupka** za zaštitu;
2. **ispitivanje** formalne i materijalne sadržine prijave i donošenje rešenja o priznavanju ili odbijanju traženog prava; i
3. **registrovanje** priznatog prava, zajedno sa izdavanjem isprave o priznatom pravu i objavom.

### *3.2.1.2. Sadržina prava*

**Prava koja nosilac žiga** ima mogu biti **moralna i imovinska**. Najčešća **imovinska** su:

<sup>102</sup> Denning P., What is Software Quality?, Communications of ACM, vol. 35., br. 1/92., str. 13 - 15.

<sup>103</sup> Zakon o žigovima SRJ, čl. 1 - 7.

<sup>104</sup> Zakon o žigovima SRJ, čl. 7 - 31; Francuski Zakon o žigovima i uslužnim žigovima, Patentni glasnik, br. 5/92., čl. 6 - 14; Japanski zakon o žigovima, Patentni glasnik, br. 2/94., čl. 5 - 18.

- a) *pravo na korišćenje*, odn. obeležavanja robe ili usluga;
- b) *pravo zabrane* drugima da neovlašćeno koriste isti ili sličan znak;
- c) *pravo upotrebe znaka zaštićenog žigom na pratećim materijalima* (pakovanju, katalozima, prospektima, oglasima, ponudama, uputstvima, fakturama, korespondenciji, drugim oblicima poslovne dokumentacije, i sl.).

S obzirom da se često radi o estetskom idejnom rešenju znaka to i njegov autor ima određena moralna i izvesna materijalna prava. **Moralno pravo je da mu se ime nadje u prijavi za priznavanje prava na žig i u svim ispravama koje se odnose na predmete na koje se žig stavlja.** Materijalna prava su isključivo svedena na pravo naknade, a ne na pravo raspolaganja i korišćenja.

Žig ili pravo iz prijave može se prenositi i to ugovorima (o licenci, franšizi, zalogu) za sve kompjuterske programe ili samo za neke programe ili softverske usluge.

### 3.2.1.3. Trajanje

Dužina trajanja žiga je **10 godina**, s tim što se može **produžavati neograničen broj puta**, a važi od datuma podnošenja prijave.

Kao i kod drugih prava industrijske svojine i pravo na žig je teritorijalno ograničeno.

Žig **prestaje** iz više razloga: **a) istekom roka** od 10 godina ako se nije produžilo važenje; **b) odricanjem** nosioca prava; **c) prestankom** pravnog odn. fizičkog lica koje je nosilac prava, a nema pravnih sledbenika; **d) oglašavanjem** rešenja o priznanju žiga ništavim; i **e) nekorišćenjem** - u određenom vremenskom periodu (kod nas, u trajanju 5 godina od dana upisa žiga, odn. dana poslednjeg korišćenja).

Posebno je nužno istaći da većina zemalja poznaje i priznaje mogućnost međunarodne registracije žiga, a zahtev za to podnosi nosilac žiga ili podnosilac prijave.

### 3.2.2. *Kompjuterski programi i nacionalni propisi zaštite žiga*

Znaci razlikovanja su postali veoma značajan oblik Prava industrijske svojine kad su u pitanju produkti KT. Naročito značajni postaju robni ("trgovački", "trade mark", <sup>TM</sup>) i žigovi usluga ("serves mark", <sup>SM</sup>) u odnosu na kompjuterske programe i softver. Naime, sam cilj postojanja i funkcija koju ova vrsta znakova razlikovanja ima pokazala se potpuno efikasna baš u slučaju stalnog proširenja tržišta i povećanja broja proizvođača programa i softvera. Mnogi od njih su male, gotovo beznačajne firme koje svoj prodor na tržište i privlačenje kupaca baziraju na oznakama sličnim renomiranih firmi. Time potvrđuju tvrdnju B. Niblett-a "da tržišni uspeh jednog računarskog programa umnogome je posledica dobro izabranog naziva. Naziv koji se lako pamti i koji je distinktivan mnogo više će potencijalnom kupcu predstavljati poziv za kupovinu nego svetleća reklama pored koje prodje, jer može identifikovati program i proizvođača i nagovestiti određeni kvalitet"<sup>105</sup>. Pogotovo ako se ima u vidu da su velike i/ili uspešne firme ulagale velika sredstva za ispitivanje i testiranje zahteva korisnika i njihovih navika, osim što su ulagala u razvoj programa ili softvera. Po podacima o strukturi potencijalnih kupaca i njihovom načinu rada sa računarima čitavi timovi psihologa, sociologa, dizajnera, stručnjaka za marketing i drugih dobijali su zadatak da paralelno sa kreiranjem programa kreiraju i njegov naziv i izgled na ekranu. Dobijeni zadatak dobro izvršen stvarao je nazive i druge oznake koje su ulazile u memoriju potrošača i svaki novi proizvod sa slični nazivom ili znakom drugog proizvođača dovodio je do zabuna.

Šta sve kao žig može biti registrovano može se videti iz sledećih primera. Poznat je slučaj spora između *Digital Equipment Corporation v. C. Itoh*, japanske firme za proizvodnju terminala<sup>106</sup>. Naime, *C. Itoh* je **imitirala** oblik i **naziv** *Digital*-ovog terminala VT200 na svom CIT-200+. Sud se odlučio da testira funkcionalnost, sličnost koja može da izazove zabluđu i mogućnosti svakog proizvođača da ulaže u razvoj i finansijske izdatke za reklamu. Interesantni podaci dobijeni su u testu sličnosti. Za sporni terminal, iako nisu skinute oznake, od 97 ispitanika 44 se izjasnilo da je u pitanju *Digital*-ov proizvod. S obzirom da *Digital* nije registrovao naziv i oblik svog terminala (a po američkom i engleskom pravu i prvo korišćenje može zaštititi, dodoše građanskopravnom zaštitom ili pravom suzbijanja nelojalne utakmice), a utvrđena je činjenica da su ga Japanci namerno imitirali u izgledu i brojevima kao delu naziva, to je sud preporučio *Digital*-u da ubuduće vodi računa da registruje naziv kao robni žig jer je to jeftinije i efikasnije nego vođenje sporova i dokazivanje namernosti u imitiranju, kao

<sup>105</sup> Edwards C., Savage N., Walden I., op. cit., str. 65.

<sup>106</sup> Tapper C., op. cit., str. 119 i 120.

i gubljenja dobiti koja zabunom nastaje, kao što je to bilo u slučaju kad su potrošači kupujući japanski proizvod misli da je *Digital*-ov.

Drugi interesantan spor vodile su *Computer Associates International Inc.* i *Computer Automation Inc.* zbog **istih početnih slova** prilikom obostranog pokušaja da registruju kao žig te inicijale. Kako su se u međuvremenu firme dogovorile koja će koristiti inicijale i taj dogovor želele da registruju, sud je smatrao da takav dogovor nije valjan, po američkim propisima, jer namerno može dovesti u zabludu korisnike usluga obe firme tako da nije dao dozvolu za podnošenje prijave za zaštitu<sup>107</sup>. Sličan je slučaj i sa dvema kompanijama od kojih se jedna zvala *General Electric Company*, a druga *The General Electric Company LTD.* Razlika u nazivu bila je samo u postojanju člana i dodatka LTD., koja se gubila u inicijalima tako da su obe imale iste inicijale (*GEC*). Sud, pred kojim je vođen spor zbog zaštite prava znaka razlikovanja, stao je na stanovište da kompanija koja je prva upotrebila znak ima i dalje pravo na njega. Nešto je drugačiji slučaj je sa firmama *Digicom* i *Digicon* koje mogu izazvati zabunu kod nepažljivog potrošača jer se razlikuju samo po jednom, i to zadnjem, najnedistinktnijem slovu. Međutim, kako su u pitanju firme u različitim poslovima (*Digicom* - digital communication, a *Digicon* - digital consulting) to se sud našao u teškoj situaciji da proceni kojoj od ove dve firme treba da uskrati pravo na znak. U ovom slučaju sud je konstatovao da je ipak delatnost slična i da bi trebalo obe firme da razmisle o svom nazivu<sup>108</sup>. Ukoliko se, pak, radi o drugoj delatnosti ovakvo neznatno razlikovanje ne dovodi do uskraćivanja prava na žig obema firmama.

Kao ilustracija neophodnosti zaštite žigom znaka kompjuterskog programa ili softverske usluge pojavljuje se i slučaj tužbe *Apple Computer INC.* podnete protiv *Formula International Inc.* ne samo što je kopiran njegov operativni sistem, već i što je dat **naziv** - "*Pineapple*" - koji asocira na Apple-ov program čime se mogu dovesti u zabludu potencijalni kupci. S obzirom na sve okolnosti, zanemarujući piratstvo koje se sudilo po drugom osnovu, sud je stao na stanovište da takav naziv ne sme biti registrovan, niti korišćen<sup>109</sup>. Veoma je sličan i slučaj kad se neznatnim proširivanjem znaka naziva jedne firme služi druga, čime se korisnici mogu dovesti u zabludu ili kad se pod imenom firme pokušava registrovati poslovna delatnost npr. "Trgovina za kompjuterski softver" i "Trgovina i servis za kompjuterski softver". Upravo zbog toga je u prošlosti, a konstatujući da je veoma teško izabrati pravi znak kad su u pitanju

<sup>107</sup> Tapper C., op. cit., str. 118.

<sup>108</sup> Od znaka robe ili usluga treba razlikovati ime pod kojim jedna poslovna organizacija posluje. Naime, kad je u pitanju znak štiti se grafički izgled, dok se kod firme štiti individualno obeležje pod kojim jedan poslovni subjekt posluje. Za zaštitu znaka primenjuju se odredbe Zakona o žigovima, a za zaštitu firme primenjuju se odgovarajuće odredbe Zakona o preduzećima.

<sup>109</sup> Tapper C., op. cit., str. 118.

računari, softver, usluge, i da se često dešava da firme izaberu generične termine, Federalni zavod za žigove SAD koristio kompjuterski rečnik kako bi kvalifikovano mogao obrazložiti odbijanje registracije takvog znaka ili izvršiti njihovo svrstavanje u grupu slabih znakova. Naime, u pravu SAD i V. Britanije<sup>110</sup> postoji razlika između registracije, pa, otuda, i uslova i obima i kvaliteta zaštite, **jakih znakova** (grupa A) i **slabih znakova** (grupa B). Istovremeno su se i savetovali podnosioci prijave za registraciju da izaberu distinktivne, neobične nazive (grupa A) umesto generičkih i opisnih (grupa B)<sup>111</sup>.

Mnogi sporovi su vodjeni zato što je u znaku stajala asocijacija na delatnosti i način obavljanja i to još neistinito (*United State Golf Association* dobila je da izradi algoritme za izračunavanje poena u golfu, mada se time uopšte nije bavila, ali je naziv asociirao da je u pitanju kompetentna firma. Sličan je slučaj i sa agencijom *COMPUTDATA* koja je svoje ime želela da koristi u pružanju usluga, ali ne računarskih, jer ionako nije imala kompjutere i sl.). Naime, većina zakona i međunarodnih akata predviđaju **da se žigom ne može zaštititi znak koji isključivo označava vrstu robe, odn. usluge, njihovu namenu, vreme i način proizvodnje, poreklo, kvalitet, cenu i sl.**

Svi ovi primeri, vezani za robne i žigove usluga, pokazuju višeznačnost njihove funkcije u prometu. U raznim zemljama se sa različitom detaljnošću pristupa ovom problemu, tim više što je većini informaciono razvijenih zemalja izuzetno mnogo stalo da bude reda na njihovom sopstvenom tržištu i da se maksimalno zaštite proizvođači tako konjunktne robe kakvi su kompjuterski programi i usluge. S druge strane, one teže i da zaštite domaće proizvođače od, često, nelojalne konkurencije drugih zemalja čija se proizvodnja bazira na imitiranju, kompiliranju ili piratstvu ideja.

Posmatrajući zakonska rešenja i sudske odluke u raznim zemljama u vezi sa zaštitom računarskih programa i softvera žigom može se **konstatovati sledeće**:

**Prvo. Računarski programi i softver mogu biti zaštićeni žigom gotovo po svim pravima.** Takav oblik zaštite smatra se i veoma poželjnim, što se može videti iz velikog broja sudskih sporova koji nastaju oko prava na žig i prava iz žiga.

**Drugo. Kao predmet zaštite žigom u vezi sa računarskim programima i softverom pojavljuju se njihov naziv i znak pod kojim se pojavljuju u prometu, kao i**

<sup>110</sup> Bainbridge D., op. cit., str. 55.

<sup>111</sup> Bernacchi R., Frenk P., Statland N., op. cit., str. 3.90.

**znak proizvođača ili pružaoca usluga.** Pored naziva ovim pravom se zaštićuje i oblik ambalaže, boje i njihov raspored, kao i niz drugih pratećih stvari (poznata je plava boja polja sa žutim velikim italic slovima *IBM*, koje se stavljaju na omotače, kutije *IBM* softvera).

**Treće.** Sa većom ili manjom oscilacijom zaštita programa ili softvera **žigom traje između 7 i 20 godina**, sa mogućnošću neograničenog produžavanja. Gotovo sva prava predviđaju i **mogućnost prestanka prava na žig usled njegovog nekorišćenja**. Taj period se kreće najmanje od tri (Italija, Francuska) najviše do šest (SAD) godina.

**Četvrto.** U svim zemljama kao uslov za sticanje prava na žig za kompjuterske programe ili softver pojavljuje se **distinktivnost**, što znači da znak programa ili softvera mora biti takav da ga odvaja od svih drugih. Pri tome pojedine zemlje (Italija, SAD, V. Britanija) prave razliku između jakih i slabih žigova. Tako bi *Windows*, *Lotus*, *Apple* bili jaki žigovi, dok bi slabi žigovi, sastavljeni iz opštih izraza, imena, bio Infoart, ili teško zapamtljive kombinacije brojeva i slova, *D3Mo*. Kao drugi uslov pojavljuje se zahtev **da se znak može grafički prikazati**. Međutim, neki zakoni (Francuski, iz 1991.) predviđaju da se znaci mogu sastojati i od **čujnih znakova** (muzički izrazi, fraze), **figurativnih znakova**, tzv. **trodimenzionalnih** (sintetizovane slike, hologrami, i sl. naš novi zakon) i **svetlećih** (Mađarski). Zanimljivo je da ni jedna zemlja koja je revidirala svoje žigovno pravo **nije unela** i **video znak** kao vrstu znaka kojim se može zaštititi neki proizvod ili usluge. Mada primenom analogije i video znak programa koji sadrži određeni oblik slova ili sklad boja na kolor monitoru ili u plastičnom delu imena (npr. jabuka) mogli bi biti zaštićeni. Posebno treba istaći da **svi zakoni predviđaju i znake koji se ne smeju koristiti** (Crvenog krsta, grbovi, suprotni moralu i sl.), te ni nazivi programa to ne bi smeli da sadrže.

**Peto.** Pojavljuju se **dve grupe zemalja u odnosu na osnov nastanka prava na žig**. **Jedna grupa** (SAD, V. Britanija, Italija) kao osnov ovog prava ima dve mogućnosti: **registracijom** i **pravom prve upotrebe**. **Druga grupa** (Nemačka, Francuska, zemlje Beneluksa, skandinavske zemlje i dr.) **sticanje prava na žig vezuje samo za registraciju**. **Bez obzira koja od zemalja je u pitanju kod registrovanog žiga pojavljuje se oznaka** ® (*registered*) **u krugu u desnom gornjem uglu znaka** (*Microsoft*®). Ukoliko se želi naznačiti o kojoj vrsti žiga je reč označava se odgovarajućim znakom (*Windows*™ ili *Software Consulting*™). Postojanje ovog znaka ili primenom prava prve upotreba na računarskom programu ili softveru označava da nosilac prava ima određena imovinsko-pravna ovlašćenja, najčešće prava isključive upotrebe tog znaka i zabrane drugim licima da ga upotrebljavaju.

**Šesto. Mahom sve zemlje predviđaju i dodatnu zaštitu znaka autorskim pravom.** To je moguće samo onda kad se radi o umetničkom delu, odn. takvom obliku znaka koji predstavlja kreativno delo svoga tvorca. Autor idejnog rešenja ima moralno pravo da bude naznačen u prijavi za priznavanje prava na žig i u svim ispravama koje se na predmet njegovog rada odnose.

**Sedmo. Pravo na zaštitu žiga i podnošenja prijave za zaštitu znaka programa ili softvera može dobiti i međunarodne razmere** ukoliko se od domaćeg nadležnog organa (zavoda, biroa) traži i međunarodna zaštita, odn. međunarodna registracija na osnovu Pariske konvencije, Madridskog aranžmana o međunarodnom registovanju žigova, ili nekog drugog regionalnog sporazuma.

### 3.2.3. *Kompjuterski programi i međunarodna zaštita žigova*

#### 3.2.3.1. *Pariska konvencija za zaštitu industrijske svojine*

Medju najvažnijim međunarodnim izvorima na kojima se bazira zaštita žigova, pojavljuje se, pre svega, **Pariska konvencija za zaštitu industrijske svojine**. Ona je predvidela međunarodnu registraciju žigova polazeći od primene sledećih načela: **a) nacionalnog tretmana, odn. jednakog tretmana;** **b) asimilacije** - čija primena znači da se pripadnici zemlje nečlanice Unije izjednačuju sa pripadnicima zemlje članice ako na teritoriji jedne zemlje članice imaju domicil, za fizička lica, odn. stvarno industrijsko preduzeće, za pravna. Po ovom načelu zaštitu prava na žig imaće i Tajlandjani ili Tajvanci (nečlanice) ukoliko žele da registruju žig svog programa ili softvera, npr. u SAD, pod istim uslovima kao i državljani, odn. preduzeća iz SAD ukoliko imaju domicil ili "stvarno i ozbiljno" trgovinsko ili industrijsko preduzeće; **c) minimalnih prava** - primena ovog načela znači da će strana firma ili pojedinac koji žele da registruju ili na drugi način zaštite svoj žig na teritoriji druge zemlje članice Unije imati, pored prava predviđenih nacionalnim zakonom, još i prava predviđena ovom Konvencijom. Kao **jedno od prava** predviđenih Konvencijom pojavljuje se i **pravo sajamskog prioriteta** po kome će se pravo prioriteta zasnivati danom izlaganja programa ili softvera sa tim znakom na sajmu (izložbi). Time se proizvođači programa i softvera mogu zaštititi i onda kad nisu stigli da žig registruju pre sajma, a želeli su da prezentiraju svoj program ili softver. Drugo od tih prava predviđenih Konvencijom je **pravo nezavisnosti** koje znači da pravna sudbina žiga za program ili softver koji je zaštićen, ili registrovan, u jednoj zemlji Unije je nezavisna od pravne sudbine istog žiga u drugim zemljama; **d) "telle quelle"** - svaki znak programa ili softvera koji je uredno prijavljen u zemlji porekla može se zaštititi "takav kakav je" i u ostalim zemljama Unije,

bez traženja posebnih uslova. Izuzetak su slučajevi: ako je žig u suprotnosti sa moralom ili javnim poretkom; ako je takve prirode da može naškoditi stečenim pravima trećih lica; ako nije distinktivan. Tada zemlja u kojoj se zaštita traži može odbiti registraciju.

I ne samo to, Pariska konvencija<sup>112</sup> predviđa da će **proizvodi koji bespravno nose jedan fabrički ili trgovački žig biti uzapćeni pri uvozu** u onim zemljama Unije u kojima ovaj žig ima pravo na zakonsku zaštitu. Zaplena se vrši u zemlji u kojoj je učinjeno delo bespravnog stavljanja žiga ili u zemlji u koju takav program ili softver bude uvezen. Ova se mera vrši na osnovu zahteva javnog tužioca, drugih nadležnih organa, jedne od zainteresovanih strana, fizičkog ili pravnog lica. Ne mora doći do zaplene programa ili softvera sa bespravnim žigom ako je proizvod u tranzitu. Oduzimanje može biti zamenjeno nekom drugom merom ukoliko je to predviđeno domaćim propisima, kao što je mera zabrane uvoza ili oduzimanja u unutrašnjosti zemlje.

### 3.2.3.2. *Madridski sporazum o međunarodnoj registraciji žigova*

**Madridski sporazum o međunarodnoj registraciji žigova**<sup>113</sup> (*International Registration Trademark Treaty*) donet je u Madridu 1891. godine i u više navrata revidiran. **Osnovni sadržaj vezan mu je za međunarodno prijavljivanje žigova i proceduru za njegovo sprovođenje.** Prijava (sa naznakom o međunarodnoj registraciji) se podnosi nacionalnom organu nadležnom za registraciju žigova na području zemlje porekla<sup>114</sup>, koji je prosledjuje Međunarodnom birou. Međunarodni biro odmah registruje žig unošenjem u međunarodni registar i objavljuje ga u mesečnoj publikaciji, a primerke dostavlja nacionalnim zavodima u kojima je zaštita zatražena. Značaj i dejstvo međunarodne prijave jednak je dejstvu zaštite žiga na osnovu nacionalnog prava. Ako je žig ranije registrovan u nekoj zemlji, pa potom registrovan i pri Međunarodnom birou, međunarodna registracija zamenjuje nacionalnu.

**Međunarodna zaštita žiga** na kompjuterskom programu ili za softverske usluge, po ovom aktu, **traje 20 godina**, a može se se produžavati i za narednih 20. Međunarodno registrovani žig zavisao je prvih pet godina od registracije u zemlji

<sup>112</sup> Pariska konvencija, čl. 9.

<sup>113</sup> Poznat i kao Madridski aranžman za žigove.

<sup>114</sup> 1992. godine Madridski aranžman je imao 31 zemlju članicu, prosečan broj prijava je te iste godine bio 13.567, a od stupanja na snagu ukupno 280.000.

porekla. Naime, sve promene u tom periodu reflektovaće se i na međunarodnu registraciju. Posle tog perioda međunarodna registracija je nezavisna.

Jugoslavija je potpisala Madridski sporazum, a ratifikovala njegovu stokholmsku verziju (iz 1967.)<sup>115</sup>.

Da bi anglo-saksonske zemlje, kao i tri zemlje EU, zbog dvojstva priznavanja žigova, mogle da prihvate ovaj Sporazum, 1989. godine potpisan je **Protokol za Madridski aranžman o međunarodnom registrovanju žigova** (*Protocol for International Trademark Treaty*, poznat kao Madridski protokol). Ovaj je protokol zaključen i da bi se uspostavila veza između madridskog sistema i žigovnog sistema EU.

### 3.2.3.3. Ugovor o registraciji žigova

**Ugovor o registraciji žigova** (*Trademark Registration Treaty*) je još jedan od međunarodnih akata kojim se želelo pojednostavljenje procedure međunarodne registracije žigova i ublažavanje teškoća nastalih Madridskim sporazumom. Ovaj je Ugovor potpisan u Beču 1973. godine, no, nije postigao očekivane efekte, te je 1991. god. "zamrznut"<sup>116</sup>.

<sup>115</sup> Madridski sporazum o međunarodnoj registraciji žigova, Službeni List SFRJ., br. 2/74.

<sup>116</sup> Za razliku od Madridskog sporazuma, **međunarodna bi se prijava, po ovom ugovoru, direktno podnosila Međunarodnom birou**, koji odlučuje, na osnovu poredhodno sprovedenog rešenja, o valjanosti zahteva i donosi odgovarajuću odluku. Ukoliko je odluka pozitivna Međunarodni biro upisuje žig u međunarodni registar i notifikuje registraciju svim državama u kojima je zaštita zatražena. Ovaj Ugovor, pored ostalog, predviđa gašenje žiga zbog nekorišćenja, propisujući za to rok od bar 3 godine. Kao ni mnoge druge, ni ovaj akt Jugoslavija nije ratifikovala, s tim, što ovaj nije ni potpisala.

#### 3.2.3.4. *Sporazum o trgovinskim aspektima prava intelektualne svojine*

Za zaštitu prava na žig kompjuterskih programa i softverskih usluga svakako da je od ključne važnosti **Sporazum o trgovinskim aspektima prava intelektualne svojine** GATT-a. Njime je, pored odredjenja da se pod **žigom podrazumeva bilo koji znak ili kombinacija znakova podobna za razlikovanje kompjuterskih programa ili softverskih usluga jedne firme od programa i usluga druge**, predviđeno da se znaci mogu sastojati od: reči, uključujući i lična imena, slova, brojeva, figurativnih elemenata i kombinacije boja, kao i bilo koje kombinacije tih znakova. Ovi se znaci mogu registrovati. Priroda programa ili usluga nikako ne može biti prepreka registraciji. Ako žigovi sami po sebi nisu podobni za razlikovanje programa ili usluga na koje se odnose, zemlje ugovornice mogu usloviti registraciju i distinktivnošću stečenu upotrebom.

Na osnovu odredbi ovog Sporazuma titular prava ima isključivo pravo da spreči sva treća lica da, bez njegove saglasnosti, koriste u toku trgovine identične ili slične znake za računarske programe ili ICC usluge koji su identični ili slični onima za koje je žig registrovan, a naročito ako postoji verovatnoća da će zbog toga doći do zabune<sup>117</sup>.

Po ovom Sporazumu **prvobitna registracija i svako obnavljanje registracije žiga na kompjuterskom programu ili za usluge traje najmanje 7 godina** i može biti obnovljena neograničen broj puta.

Ukoliko se za održavanje registracije zahteva upotreba, onda se registracija može poništiti posle kontinuirane **neupotrebe od najmanje 3 godine**, izuzev ako ne postoje smetnje za to (najčešće su to razlozi koji proizlaze nezavisno od volje titulara, npr. restrikcija uvoza).

Kako se kompjuterski programi nalaze u trgovinskim tokovima, to je za trgovinu od izuzetnog značaja pojava **krivotvorenih programa**, pod kojim se podrazumeva, pre svega, **program sa krivotvorenim žigom, odn. program na odredjenom medijumu zajedno sa ambalažom koja bez ovlašćenja nosi žig identičan registrovanom za takav program, a koji se, po svojim bitnim svojstvima, ne može razlikovati od registrovanog i koja vredja prava vlasnika** (na osnovu zakona zemlje

---

<sup>117</sup> Sporazum, čl. 16., tč. 1.

uvoza). Za takve programe Sporazum je predvideo: **a) građanske i upravne postupke** sa mogućnošću primene **sudskih zabrana** (tako, sudski organi imaju ovlašćenje da, odmah posle carinjenja, nalože strani da prestane sa povredom prava kako bi se sprečio ulazak u trgovinske tokove, na njihovoj teritoriji, uvezenih krivotvorenih programa) i **naknadi štete titularu prava** kojom se kompenzira povreda koju trpi od strane namernog ili prekršioca koji je imao osnova da zna da je u prekršajnoj aktivnosti učestvovao, **nadoknadjuju troškovi** nastali u sudskim postupcima, i/ili **nadoknadjuje izgubljeni profit**. Pojava odredbi o naknadi štete titularima prava, predstavlja realizaciju osnovne premise "da su prava intelektualne svojine privatna prava". Titular ima i pravo na informaciju o identitetu trećih lica uključenih u proizvodnju i distribuiranje krivotvorenih računarskih programa, kao i o njihovim distributivnim kanalima; **b) ovlašćenja sudskih organa** da nalože da se utvrdjeno krivotvoreni računarski programi, bez bilo kakve naknade, *povuku iz trgovinskih tokova*, ali vodeći računa da se ne načini šteta titularu prava, ili *da se unište*; **c)** mogućnosti da **sudski organi izriču privremene mere** radi sprečavanja povreda i čuvanja relevantnih dokaza (mere se naročito izriču radi sprečavanja povrede ovih prava i stavljanje u promet programa preko trgovinskih kanala koji su u njihovoj nadležnosti, ali i zbog čuvanja relevantnih dokaza o učinjenim povredama, i sl.); **d)** izricanje **zabrane puštanja u promet krivotvorenih programa**. Naime, sudske mere (privremene ili trajne) nisu i jedina pravna sredstva koja stoje na raspolaganju radi efikasne zaštite prava na žig, već se one dopunjuju i **posebnim pograničnim merama koje primenjuju carinski organi** u slučaju pojave uvoza ove robe. Pri tome, uvoznik i podnosilac zahteva treba da budu odmah obavešteni o ovoj zabrani; **e)** nadležni organi su ovlašćeni da **nalože uništavanje ili povlačenje krivotvorenih programa** u skladu sa propisanim principima (princip nenanošenja štete titularu prava, princip nekršenja postojećih ustavnih odredbi, i princip srazmere između ozbiljnosti povrede i pravnih sredstava i interesa trećih lica). Takođe, krivotvorenim programima nadležni organi neće dozvoliti reeksport, niti će ih podvrgnuti nekom drugačijem carinskom postupku, osim u izuzetnim okolnostima; **f)** mogućnost **pokretanja krivičnog postupka i kažnjavanja počinioca** koji su svesno (namerno) krivotvorili žig zbog njihovog komercijalnog korišćenja. Sporazum upozorava na **nužnost predviđanja strogih krivičnih sankcija** kako bi se delovalo na odvraćanje budućih počinioca. Zato se predlažu, pored novčanih, i kazne zatvora. Naravno, nacionalnim zakonodavstvima ostavljen je izbor kolike će one biti. Osim kazne zatvora i novčane kazne preporučuju se i mere oduzimanja, zaplene i uništenja "inkriminisane robe i svih materijala i alata koji su se koristili pri izvršenju krivičnih dela". Znači, ako se uništenje ne ostvari po nalogu carinskih i drugih nadležnih organa do njega može doći po osnovu izricanja odgovarajuće mere u krivičnom postupku<sup>118</sup>.

<sup>118</sup> Drakulić M., Pravna zaštita kompjuterskih programa, D. Milanovac, Zbornik radova: 10. YU Info-TEH'95., 1995., str. 263 - 270.

### 3.2.3.5. *Direktiva Evropske zajednice o usaglašavanju zakona država članica u pogledu žigova*

Od regionalnih međunarodnih akata značajna je **Direktiva Evropske zajednice o usaglašavanju zakona država članica u pogledu žigova** (*Council Directive harmonizing the member state laws related to trademarks*)<sup>119</sup>. Ovom Direktivom izvršena je harmonizacija nacionalnih prava žigova, kako bi se obezbedio njihov kontinuitet, ali i jedinstven sistem zaštite koji osigurava nesmetan tok robe i usluga i ravnopravnu utakmicu na zajedničkom tržištu. Njom je definisano **šta se pod žigom podrazumeva** i određuje da je **to bilo koji znak koji se može grafički predstaviti** (reči, uključujući i lična imena, crteže, slova, brojeve, oblik robe ili njeno pakovanje) **ako se na osnovu tog znaka program ili usluga može razlikovati od drugih**<sup>120</sup>. Posebno se nabrajaju oni **znaci koji se ne mogu registrovati** ili ukoliko se to i učini registracija će biti nevažeća. Pored žigova koji se ne mogu registrovati, Direktivom su predviđeni i **žigovi koji se ne smeju registrovati**. Među takvim su oni koji su suprotni dobrim poslovnim običajima, ili su u pitanju žigovi programa koji obuhvata znak visoke simboličke vrednosti (religiozne, npr.), ili sadrže ambleme, bedževe, štitove, ili su u suprotnosti sa javnim moralom. Dakle, takvi se znaci ne smeju naći na programima niti se smeju koristiti za softverske usluge. Posebni su slučajevi kada se žigovi ne mogu registrovati jer postoji konflikt sa ranijim pravom (pod ranijim pravom podrazumevaju se raniji žigovi)<sup>121</sup>.

Na osnovu registracije žiga kompjuterskog programa ili softverskih usluga, **titular prava ima isključiva prava iz žiga**. On može sprečiti sva treća lica da bez njegove saglasnosti koriste u prometu (trgovačkom): znak koji je istovetan sa žigom programa ili softverskih usluga koje su istovetne sa onim za koje je žig registrovan, ili je u pitanju takva sličnost koja može dovesti javnost u zabunu (npr. tako što se znak povezuje sa žigom). Osim ovih prava titular, zavisno od predviđenosti po zemljama, može imati i ovlašćenja da spreči sva treća lica koja nemaju njegov pristanak da koriste u trgovačkom prometu bilo koji znak koji je identičan ili sličan žigu, u vezi sa robom ili uslugama koje nisu slične onima za koje se žig registruje, ali je taj žig već stekao određeni ugled u zemljama članicama, pa korišćenje takvog žiga predstavlja sticanje

<sup>119</sup> Direktiva je doneta 1988., a u Službenom listu Evropske zajednice objavljena 1989. godine. Integralni tekst je objavljen u podlisku Patentnog glasnika SRJ, br. 6/93.

<sup>120</sup> Direktiva, čl. 2.

<sup>121</sup> **Raniji žigovi** su žigovi identični ranije registrovanom žigu ili identičani ili sličani ranijem, a kojima se može izazvati zabunu. To su i žigovi Zajednice, žigovi registrovani u drugim zemljama ili na osnovu drugih međunarodnih ugovora. Isto tako, to su i žigovi slični ranijem nacionalnom žigu, slični ili isti ranijim žigovima garancije ili sertifikatu žiga čija je važnost istekla i sl.

nepravedne koristi ili nanošenje štete distinktivnom karakteru i ugledu žiga<sup>122</sup>. Takodje, titular može zabraniti i: pričvršćivanje znaka na program ili njegovo pakovanje; nudjenje programa ili njegovo stavljanje na tržište ili skladištenje u iste svrhe pod tim znakom, ili nudjenje ili vršenje usluga pod tim znakom; uvoz ili izvoz programa pod tim znakom; korišćenje znaka na poslovnim papirima i u oglasima.

Titular prava ne može se protiviti daljem komercijalnom korišćenju kompjuterskih programa koji su "pokvareni ili promenjeni" nakon njihovog dospeća na tržište, niti zabraniti upotrebu žiga za programe koji su stavljeni na tržište Zajednice pod tim žigom od njegove strane ili uz njegov pristanak.

Ukoliko titular prava na žig određenog računarskog programa ne počne da stvarno koristi žig u državama članicama, za programe i usluge za koje je registrovan u roku od 5 godina od datuma okončanja postupka registracije, ili je sa takvom upotrebom prestao tokom neprekidnog perioda od 5 godina, njegov će žig biti podvrgnut sankcijama zbog nekorišćenja - **prestaće mu važenje**.

Sa ovim Smernicama zemlje članice su morale do 1991. godine usaglasiti svoje nacionalne zakone, propise ili upravna akta, ili doneti nove.

Kako je ranijom Direktivom (Directive 3842/86.) osnovan **Evropski zavod za žigove** (*European TradeMark Office*) sa sedištem u Alikanteu (Španija) u kome se registruju žigovi po jednostavnom postupku, to ova registracija znači da je žig zaštićen na teritoriji Zajednice, odn. svih zemalja članica. Naročito je značajno rešenje po kome će *za programe iz zemalja nečlanica ukoliko imaju isti žig kao i neki programi iz zemalja članica važiti zabrana uvoza, odn. pojavljivanja na tržištu Zajednice*. Ovakvo rešenje može imati, pored zaštitne, i protekcionističku i monopolističku funkciju.

---

<sup>122</sup> Direktiva, čl. 5. tč. 2.

### 3.2.4. *Kompjuterski programi i zaštita žiga po našem pravu*

Kompjuterski programi i softver, po ranijem<sup>123</sup> i važećem<sup>124</sup> zakonu, kao i bilo koja druga roba ili usluge, mogu se označiti znakom, a on zaštititi žigom. Zaštita bi značila sledeće:

**Prvo.** Kako naše pravo pripada grupi prava koji *zaštitu obezbeđuje registracijom, to se i za kompjuterske programe i softver primenjuje isti režim*. Znači, zaštita je moguća tek ako se ostvaruje u upravnom postupku, koji se vodi pred saveznim organom (Savezni zavod za zaštitu intelektualne svojine)<sup>125</sup>.

**Drugo.** *Zaštita se odnosi na znak koji u prometu služi za razlikovanje jednog od drugog kompjuterskog programa*, odn. jednih od drugih softverskih (ICC) usluga fizičkog ili pravnog lica. **Pravo kojim se štiti znak je žig.**

**Treće.** Da *bi se žigom mogao zaštititi znak nužno je da se ispune, zakonom, predviđeni uslovi*. To su: *destingtivnost i primenljivost* u prometu, kao i *oblici koje znak može imati*. **Znak se može sastojati od reči, slogana, slova, brojeva, slika, crteža, rasporeda boja, trodimenzionalnih oblika, kombinacije tih znakova, ali i od muzičkih fraza koje se mogu grafički prikazati**<sup>126</sup>. Znači, znak koji se štiti žigom grafički se predstavlja, što predstavlja uslov vezan za oblik. Medjutim, prilikom određivanja koje uslove treba da ispuni znak kompjuterskog programa, ili usluga, naše pravo je prihvatilo, pored generalne klauzule, i sistem negativne enumeracije. Naime, da bi se mogao zaštititi znak programa, odn. usluga, **on ne sme biti**<sup>127</sup>:

- ♦ protivan moralu i zakonu;
- ♦ po svom ukupnom izgledu nepodoban za razlikovanje programa, odn. usluga u prometu;
- ♦ takav da isključivo predstavlja oblik određen prirodom programa ili oblik neophodan za dobijanje određenog tehničkog rezultata;

<sup>123</sup> Zakon o zaštiti pronalazaka, tehničkih unapređenja i znakova razlikovanja.

<sup>124</sup> Zakon o žigovima.

<sup>125</sup> Zakon o žigovima, čl. 7.

<sup>126</sup> Zakon o žigovima, čl. 4.

<sup>127</sup> Zakon o žigovima, čl. 5.

- ♦ takav da isključivo označava vrstu programa, odn. usluga, njihovu namenu, vreme ili način proizvodnje, kvalitet, cenu, količinu, masu i geografsko poreklo;
- ♦ takav da je uobičajen za označavanje određene vrste programa ili usluga;
- ♦ takav da svojim izgledom ili sadržajem može da stvori zabunu u prometu u pogledu porekla, vrste, kvaliteta, ili drugih svojstava programa, odn. usluga;
- ♦ da sadrži zvanične znakove ili punceve za kontrolu ili garanciju kvaliteta ili ih podržava;
- ♦ da je istovetan zaštićenom znaku drugog lica za istu ili drugu vrstu programa, odn. usluga;
- ♦ da je sličan zaštićenom znaku drugog lica za istu ili sličnu vrstu programa, odn. usluga, ako ta sličnost može da stvori zabunu u prometu ili dovede u zabludu učesnike u prometu;
- ♦ koji je, bez obzira na program ili usluge, na teritoriji naše zemlje nesumljivo poznat kao znak visokog renomea kojim svoju robu ili usluge obeležava drugo lice, čuveni žig;
- ♦ koji izgledom ili sadržajem povredjuje autorska ili prava industrijske svojine;
- ♦ koji sadrži državni ili drugi javni grb, zastavu ili amblem, naziv ili skraćenicu naziva neke zemlje ili međunarodne organizacije, kao i njihovo podražavanje, osim po odobrenju nadležnog organa odnosno zemlje ili organizacije; i
- ♦ koji predstavlja ili podražava nacionalni ili religiozni simbol.

Ukoliko se radi o liku ili imenu nekog stvarnog lica za zaštitu je prethodno potrebna njegova ili dozvola njegovih pravnih sledbenika.

**Četvrto. Registrovani računarski program i softver uživaće zaštitu 10 godina, s tim što se njegovo trajanje može produžiti neograničeni broj puta.** Rok počinje teći danom podnošenja uredne prijave.

**Peto. Postupak zaštite odvija se kroz tri faze:**

- 1. pokretanje postupka** za priznavanje žiga započinje podnošenjem prijave (prijava sadrži zahtev za priznavanje žiga, znak koji se želi zaštititi

i spisak robe, odn. usluga na koje se odnosi) i upisom prijave u poseban registar prijave<sup>128</sup>;

2. **rešavanje po prijavi** obuhvata ispitivanje formalnih i materijalnih uslova za priznavanje, kao i donošenje odgovarajućeg rešenja;
3. **upis u registar žigova, izdavanje isprave o žigu i objavljivanje priznatog prava** je treća faza, koja može obuhvatiti međunarodnu registraciju. Ukoliko se želi međunarodno registrovanje zahtev se podnosi Saveznom zavodu, u skladu sa Madridskim sporazumom, koji ga prosledjuje odgovarajućem telu nadležnom za ovaj vid registracije.

**Šesto. Nosilac prava na žig kompjuterskog programa ili softverskih usluga, može biti domaće ili strano pravno ili fizičko lice.** Pri tome, strana fizička i pravna lica uživaju ista prava kao i domaća, što je u skladu sa međunarodnim ugovorom ili načelom uzajamnosti<sup>129</sup>. Nosilac prava podnosi prijavu za registraciju. Ime tvorca znaka se unosi u prijavu i druge isprave što je njegovo moralno pravo. Što se materijalnih prava autora tiče on ima pravo na naknadu (od ove naknade treba razlikovati i pravo na posebnu naknadu). **Nosilac prava ima pravo korišćenja i pravo zabrane drugim fizičkim i pravnim licima na korišćenje znaka** bez njegove dozvole za obeležavanje istih ili sličnih programa, odn. usluga. On, takodje, ima i pravo **upotrebe znaka zaštićenog žigom na sredstvima** za pakovanje, katalogima, prospektima, oglasima, drugim vrstama ponuda, uputstvima, fakturama, u korespondenciji ili drugoj poslovnoj dokumentaciji, kao i na uvezenim programima i uslugama<sup>130</sup>. Ovo poslednje ovlašćenje je od posebnog interesa za računarske programe i obeležavanje prateće dokumentacije istim znakom kao i samog programa, što nije baš bilo uobičajeno u našoj poslovnoj praksi. **Nosilac prava može svoje pravo pravnim poslom preneti na drugo pravno ili fizičko lice**, odn. ustupiti ga. Pravo se može preneti cesijom. Ako se želi ustupiti samo pravo privrednog iskorišćavanja zaštićene oznake i to u odredjenom vremenu ili na odredjenoj teritoriji i naše pravo dozvoljava zaključenje **ugovora o ustupanju**, odn. sporazum o ustupanju. Ukoliko se želi preneti žig odn. pravo iz prijave za sve programe ili samo za neki onda se to vrši posebnim ugovorom o prenosu prava (licencom, franšizom, zalogom i sl.), s tim da kolektivni žigovi ne mogu biti predmet ovih ugovora.

<sup>128</sup> Kao i zakoni drugih zemalja i naš Zakon o žigovima predviđa postojanje dve vrste registara: **registar prijave za priznavanje žigova** i **registar žigova**. Oba vodi Savezni zavod za zaštitu intelektualne svojine.

<sup>129</sup> Zakon o žigovima, čl. 6.

<sup>130</sup> Zakon o žigovima, čl. 31.

**Sedmo. Pravo na određeni znak i u našem pravu podrazumeva da se on koristi, odn. pravo može prestati nekorišćenjem ako nosilac prava žiga na računarskom programu ili softveru bez opravdanog razloga ne koristi žig za označavanje programa ili ICC usluga neprekidno u trajanju od 5 godina od dana upisa u registar žigova,** odn. od onda kad je žig poslednji put korišćen. Na zahtev zainteresovanog lica može prestati pravo. Ako je u pitanju kolektivni žig, on može prestati i ukoliko se upotrebljava suprotno opštem aktu o tom žigu.

**Osmo. Žig može prestati pre isteka perioda od 10 godina i u drugim slučajevima predviđenim zakonom,** kao što je odricanjem prava od strane nosioca, sudskom odlukom ili samim prestankom postojanja nosioca. Naravno, ono može prestati i zbog neplaćanja propisane takse. Poseban je, pak, slučaj kada se rešenje o priznanju ili međunarodnom registrovanju oglasi ništavim.

Zaštita prava na žig kompjuterskih programa i softvera pretpostavlja i sudsku zaštitu. Osnova za ovu zaštitu je **Zakon o žigovima**, koji je predvideo dva oblika zaštite: građanskopravnu i kaznenopravnu.

**Građanskopravna zaštita** traži se u slučajevima: **povrede žiga** ili **osporavanja prava**.

**Povreda žiga je svako neovlašćeno korišćenje zaštićenog znaka od strane bilo kog učesnika u prometu ili neovlašćeno raspolaganje zaštićenim znakom ili podražavanje zaštićenog znaka.** U slučaju ove povrede lice čije je pravo povredjeno (podnosilac prijave, nosilac žiga ili sticalac isključive licence) podnosi tužbu zbog povrede, u roku od 3 godine od dana kada je saznao za povredu i učinioca, a najkasnije 5 godina od učinjenog dela.

Tužbom se može zahtevati **naknada štete** koja je namerno prouzrokovana, i to do visine trostrukog iznosa stvarne štete i izgubljene dobiti, kao i privremena mera **zabrane vršenja radnji** kojima se povređuju prava iz žiga, ali i privremena mera **oduzimanja programa** ili njegovog isključenja iz prometa.

Postupak po ovoj tužbi je hitan.

Ako je jedno lice podnelo prijavu ili registrovalo na svoje ime znak kojim obeležava svoje kompjuterske programe ili softverske usluge, a drugo lice taj isti znak koristi za obeležavanje programa i usluga i on postane opšte poznat za obeležavanje

njegove robe, tada to lice može tražiti, tužbom, da ga sud ogласи za podnosioca prijave, odn. nosioca prava.

Tuženi može dokazati da je isti ili sličan znak koristio isto vremena koliko i tužilac, pa će tada sud odbiti tužbeni zahtev.

Ako, pak, sud prihvati tužbeni zahtev, tada na osnovu primljene presude, Savezni zavod upisuje tužioca u odgovarajući registar.

**Tužba za osporavanje žiga** ne može se podneti po proteku roka od 5 godina od dana upisa žiga u registar.

Povrede prava ne moraju uvek biti građanskopravne prirode. One mogu biti i privredni prestupi ili prekršaji, što sa sobom povlači **kaznenopravnu zaštitu**.

Kazneno-pravna zaštita za **privredni prestup** postojaće onda kada preduzeće ili drugo pravno lice povredi žig, odnosno pravo iz prijave. **Kazna će biti novčana** (od 5.000 do 50.000) i za preduzeće i za odgovorno lice (od 500 do 5.000 dinara).

Ukoliko se preduzeće ili drugo pravno lice **neovlašćeno bavi zastupanjem stranih pravnih ili fizičkih lica** u pitanju je **prekršaj**, za koji će se kazniti preduzeće **novčanom kaznom** (od 1.000 do 15.000), odgovorno lice (od 500 do 1.500), kao i počinioc koji se neovlašćeno bavio zastupanjem (od 500 do 1.500).

Pored ovih oblika zaštite predviđena je i **krivičnopravna zaštita**. Krivični zakon SRJ<sup>131</sup>, predviđa "Ko se u nameni da obmane kupca ili korisnika usluga posluži tuđjom firmom, **tuđjim žigom** ili zaštitnim znakom ili tuđjom oznakom robe ili unese pojedina obeležja oznake u svoju firmu, svoj žig ili zaštićeni znak ili u svoju posebnu oznaku robe, **kazniće se zatvorom do tri godine**." Znači, i kad je u pitanju znak računarskog programa i softvera, ili neki drugi deo koji se može zaštititi žigom, ukoliko se koristi od neovlašćenih lica i to u nameri da se obmanu kupci ili korisnici usluga,

---

<sup>131</sup> Krivični zakon SRJ, čl 165.

primenjivaće se ova odredba KZ. Pri tome nije bitno da li je stvarno do zablude i došlo, već krivično delo postoji nezavisno od moguće posledice<sup>132</sup>.

Pored ovih oblika zaštite predviđa se i mogućnost **zaštite od nelojalne konkurencije**, s time što se ove zaštite mogu paralelno sprovoditi.

### 3.3. *Kompjuterski programi i regulisanje zaštite od nelojalne konkurencije*

#### 3.3.1. *Opšte napomene o zaštiti od nelojalne konkurencije*

Pored nespornih oblika industrijske svojine, kao što su pronalasci, tehnička unapredjenja, know-how, znaci razlikovanja, pojavila se i jedna posebna kategorija - **nelojalna konkurencija**, odn. **sprečavanje nelojalne konkurencije**. U pravnoj doktrini i zakonskim propisima postoje razna shvatanja šta je nelojalna konkurencija, kom pravu ona pripada, kojim normama je regulisati. Postojanje različitosti posledica je, između ostalog, i izbora kriterijuma. Tako, jedna grupa shvatanja polazi od motiva zbog koga je delo nelojalne utakmice nastalo, druga se baziraju na vrsti upotrebljenih sredstava, dok su trećima polazišta cilj koji se postiže. No, bez obzira na postojanje ovakvih shvatanja čini se najprihvatljivije posmatrati nelojalnu konkurenciju kao ukupnost sredstava, ciljeva i motiva<sup>133</sup> na osnovu kojih je moguća distinkcija lojalnog od nelojalnog ponašanja, pri čemu nelojalno ponašanje za posledicu može imati stvarnu štetu i izgubljenu dobit, kao i neimovinsku, moralnu (ugled, i sl.), štetu načinjenu nekom poslovnom subjektu ili drugom učesniku u poslovnom prometu (npr. potrošačima). Naravno, veoma je teško striktno odvajanje nelojalnog od lojalnog ponašanja, isto kao što je teško striktno odvajanje nelojalne utakmice od drugih dela. Ponekad u pozadini nelojalne utakmice može biti i krivično delo, mada u suštini **nelojalna konkurencija predstavlja određene radnje nekog poslovnog subjekta koje su protivne dobrim poslovnim običajima i kojima se nanose ili mogu naneti štete drugom subjektu, potrošaču ili državi**<sup>134</sup>.

Kao **elementi dela nelojalne utakmice** pojavljuju se, dakle:

1. da je čine samo određeni subjekti - poslovnici;

<sup>132</sup> Manigodić M., Robni i uslužni žigovi, Beograd, Pronalazaštvo, 1989., str. 62.

<sup>133</sup> Besarović V., op. cit., str. 151.

<sup>134</sup> Drakulić M., Osnovi Poslovnog prava, Beograd, FON, 1995., str. 118 - 138.

2. radnja ili delo se mora odnositi na poslovnu delatnost;
3. radnja ili delo mora da je učinjeno u cilju nadmetanja, takmičenja;
4. ponašanje mora biti u suprotnosti sa dobrim poslovnim običajima;
5. da je prouzrokovana šteta;
6. ponašanje mora biti usmereno protiv zaštićenog lica.

Znači, u većini zemalja koje predviđaju postojanje nelojalne utakmice (posebnim zakonima ili propisima iz poslovnog, trgovačkog, građanskog ili prava industrijske svojine) prihvaćeno je da su počinioci nelojalne utakmice poslovni subjekti, da oni to čine u okviru svoje redovne poslovne delatnosti i to radi konkurencije (poslovne) sa drugim poslovnim subjektima, a suprotno dobrim poslovnim običajima i sa posledicom nanošenja ili mogućeg nanošenja štete.

S obzirom da je u pitanju povreda dobrih poslovnih običaja, a da se oni razlikuju međusobno zavisno od ciljeva, privredne i tržišne politike, kao i sredine u kojoj se pojavljuju, to se u zakonima različitih zemalja mogu pojaviti i različita dela koja će se kvalifikovati kao nelojalna utakmica. Pri tome, pod **dobrim poslovnim običajima** *podrazumevaju se pravila ponašanja kojih se pridržavaju* (dobrovoljno u nekim zemljama) *ili obavezno* (kod nas) *svi učesnici u poslovnom životu jer su zbog dugogodišnjeg ponavljanja i primenjivanja postali standardi i ušli u društvenu svest kao obavezna pravila ponašanja*<sup>135</sup>. Po pravilu, oni nisu pisana pravila. Ponekad to postaju kad su u formi uzansi. Uzanse su zbirka propisa prikupljenih, sistematizovanih i objavljenih dobrih poslovnih običaja od strane nekog ovlašćenog tela (npr. berze, komore, udruženja, pa, čak, i korporacije).

Kako je nelojalna konkurencija institut potekao iz nemačkog prava, to i danas njihova teorija i zakonodavstvo umnogome određuju pravce definisanja, a naročito određivanja ponašanja koja se tretiraju kao dela ove utakmice. Primenjujući *generalnu klauzulu* mnoga prava, pa i naše, pored opšteg pojma dela nelojalne utakmice, određuje i vrste tih dela.

Što se računarskih programa i ICC usluga tiče, oni po svojoj prirodi i značaju, predstavljaju izazov za konkurentske organizacije, te se problem njihove zaštite sve češće stavlja u prvi plan u suzbijanju nelojalne utakmice i kažnjavanju nelojalnog ponašanja. Tim više, što ono predstavlja zajedničkog povezičelja anti-monopolskog prava sa pravom intelektualne svojine i poslovnom tajnom. Čak, anti-monopolsko

---

<sup>135</sup> Besarović V., op. cit., str. 155.

pravo<sup>136</sup> u mnogim sistemima obuhvata nelojalnu utakmicu, a poslovna tajna, kao institut, pripada pravu nelojalne utakmice jer supstituiše takmičarske sposobnosti pojedinih poslovnih subjekata isto kao što predstavlja i ključni element još jednog instituta - know-how.

### 3.3.2. *Kompjuterski programi i nacionalni propisi zaštite od nelojalne konkurencije*

Kompjuterski programi i softver postali su veoma česti objekat oko koga se vode čitave borbe između različitih proizvođača i veoma često te borbe nose i elemente nelojalne utakmice. Ulog je isuviše velik da bi se pojedine organizacije dobrovoljno odricale učešća u konkurentskom nadmetanju ne bi li osvojili što veće i što bogatije tržište. Što je broj konkurenata rastao i što je raslo učešće softvera i računarskih programa u odnosu na hardver, to su se i mnoge organizacije okrenule njegovoj proizvodnji i prodaji. U povećanoj konkurenciji uvek se pojavi po neko čije ponašanje postaje suprotno dobrim poslovnim običajima i koji na osnovu nelojalne konkurencije postiže veliki profit na uštrb drugih. Koristeći se nelojalnom reklamom, zloupotrebom ili imitiranjem žigova, ocrnjivanjem, davanjem netačnih podataka o programima i softveru, prikriivanjem njihovih mana, neposrednim kopiranjem, ropski podržavajući tudj program i sl. pojedine softverske kuće došle su do velikih dobiti nanoseći štetu drugima.

Primera radi može se navesti sudski spor između *Graver Tank v. Mfg Co.* pošto se firma *Mfg Co.* u reklamiranju svog softvera poslužila **istim sredstvima** (slične reklamne poruke koje su se pojavljivale po stručnim časopisima, magazinima, TV) i sa gotovo **istim sadržajem** ("Ako niste imali prilike da upoznate ovakav softver učinite to odmah! Nazovite nas. Dobićete prototip, savet stručnjaka i ... Zadovoljstvo će biti vaše"). Ovakva poruka pojavljivala se danima u raznim TV programima, ali kako je pre toga slična sadržina već bila upućivana od *Graver Tank*-a potencijalnim kupcima u sećanju je ostajala poslednja. Ona se veoma često poistovećivala sa prvom. Doduše, znalcima specifičnih programa *Graver Tank* bile su poznate osobine i kvalitet njenih programa, ali su mislili da se radi o "firmi-ćerci". Počelo je naručivanje. Tek kad su se stalni kupci javili u *Graver Tank*-u su postali svesni da je u pitanju oblik **"servilnog pridržavanja reklame"**. *Graver Tank* je podneo tužbu sudu za nastalu štetu i povredu

<sup>136</sup> Antimonopolsko pravo teži da ublaži dominaciju određenih organizacija na tržištu. Pod ovo pravo podpadale su mnoge američke i druge korporacije, a među njima često su se nalazile i one iz oblasti kompjuterske tehnologije. To je 1995. god., npr. slučaj sa *Microsoft*-om čiju je mrežu (*Microsoft Network*) ispitivalo Ministarstvo pravosuđa SAD zbog namere korporacije da distribuira svoj softver *Microsoft '95.*, PC PRESS, no. 4/95., str. 13.

ugleda. Sudija koji je predmet dobio zahtevao je da se u postupku utvrđivanja činjenica i istinitosti navoda tužioca učini i psihološki test. Formirane su dve jednake grupe od po 30 ljudi. U prvoj grupi bili su oni koji se bave delatnošću za koju je pripremljen softver, ali koji se nisu sretali sa proizvodima ni jedne od ove dve firme, mada su čuli za firmu tužitelja. U drugoj grupi bili su potpuni laici, slučajno izabrani, za koje se kasnije utvrdilo da većina od njih čak ni nema računar. Obe su grupe testirane višestrukim ponavljanjem originalnim spotovima. Nakon završenog testiranja gotovo polovina ispitanika prve grupe (13) bila je ubedjena da se radi o softveru firme *Graver Tank*. Jedan deo (6) nije zapamtio ni naziv ni jedne od ovih firmi, ali je zapamtio naziv softvera i karakteristike druge firme. Treći su uočili razliku (11). Podaci dobijeni u drugoj grupi bili su još zanimljiviji jer se radilo o "prosečnim" kupcima. Manje od polovine ih je bilo zbunjeno i nisu znali da kažu ni o čemu se radi (12). Drugi su smatrali da se radi o istoj firmi (11), a treći su zapamtili samo reklamu druge firme (7). Na osnovu rezultata sud je konstatovao da je reklama bila zbunjujuća. Kako nije bio problem oko dokazivanja koja je firma tvorac reklame (iz finansijskih izveštaja oko angažovanja stručnjaka za marketing i psihologa, koje, inače, nije imala druga firma), vremena pojavljivanja reklame i sl. konstatovano je da je u pitanju delo nelojalne utakmice i *Mfg Co.* je kažnjen za štetu i izgubljenu korist nastalu pometnjom na tržištu, čiju je visinu utvrdio sud u sumi od 1.2 milona dolara i gotovo isto toliko za gubljenje renomea pošto je bio u pitanju softver koji po kvalitetu nije bio ni približno dobar kao softver firme tužitelja, što je izazvalo revolt kod nekih kupaca<sup>137</sup>.

Veoma je čest slučaj kad jedna firma **koristi ugled** druge ne bi li postigla bolje rezultate. Tako se na Jugu Engleske pojavila firma pod nazivom *Computer Equipment Sales* i koja se uspešno bavila maloprodajom kompjutera i programa. Njene usluge su bile vrhunskog kvaliteta, cene niske, a servis efikasan. Nakon nekoliko godina njen je renome postao besprekoran. No, uskoro se pojavila nova firma pod nazivom *Computer Equipment Sales and Service*. Da ne bi bila odbijena ova firma, svesna dela koje čini, nije svoj naziv registrovala kao žig. Međutim, delatnost je nesmetano obavljala. Uskoro su mnogi kupci pohrlili u nju. Došlo je do tužbe, zbog štete i izgubljene koristi koju je prva firma, tužitelj, trpela<sup>138</sup>.

Posebnoj kategoriji pripadao je slučaj firme koja je **dala netačne podatke o svom softveru**, navodeći da je u pitanju softver koji omogućuje praćenje stanja na zalihama i signalizaciji nabavke sirovina za farmaceutske delatnosti. Međutim, radilo se o običnom softveru koji je samo delimično bio prilagodjen specifičnoj delatnosti za koju je nudjen i reklamiran. Kako je više kupaca bilo nezadovoljno to su se oni udružili,

<sup>137</sup> Bernacchi R., Frank P., Statland N., op. cit., str. 3.22.

<sup>138</sup> Bainbridge D., op. cit., str. 57.

posle odbijanja proizvođača da učini promene na softveru, i podigli zajedničku tužbu. Sud je navode tužbe prihvatio<sup>139</sup>.

Kao tipično za računarske programe i nelojalnu utakmicu spominje se i slučaj jednog programera koji je po porudžbini izrađivao programe za obradu podataka za finansijsko poslovanje. Tako je u jednom trenutku, nakon izrade programa za jednog naručioca, isti program ustupio i drugoj organizaciji, i to bez znanja i dozvole naručioca. Potom se uspostavilo da je ta druga organizacija direktni konkurent naručioca. Naručioc je pokrenuo sudski postupak protiv druge organizacije za delo nelojalne utakmice. Sud je presudio u korist naručioca smatrajući da je u pitanju nemoralnost koja se kosi sa dobrim poslovnim običajima i to zbog toga što je: tužena organizacija do programa došla nemoralnom radnjom programera, koji je zloupotrebio svoj odnos sa naručiocem; tuženi učestvovao u utakmici sa programom koji je izradjen za konkurenta, od njega plaćen i proveren, te je i rizik grešaka bio drugoga; i ono što je najvažnije tuženi je ostvario prednost nad naručiocem jer je uštedeo vreme i troškove izrade programa<sup>140</sup>. U pitanju je **ropskog podražavanja** programa do koga se došlo na parazitski, podmukao i prevaran način.

Jedno od ne tako retkih oblika nelojalne utakmice su i premijski poslovi u kojima neki poslovni subjekt daje veću od dozvoljene premije ili daje poklone kupcu uz svoj softver odn. računarske programe. U početku bili su to "programi igrice", a danas se prave čitavi spiskovi mogućih programa poklona koji, zavisno od cene proizvoda i želja kupaca, će biti poklonjeni uz program ili softver. Ovakvim premijama ne samo što se privlače kupci nego i stiče neosnovana materijalna korist i ekonomska prednost u odnosu na druge subjekte.

Na osnovu ovih slučajeva može se videti da su oblici nelojalne konkurencije raznovrsni i zaključiti:

**Prvo.** Prava gotovo svih razvijenih zemalja poznaju nelojalnu konkurenciju. Razlike postoje samo kojim propisima ih regulišu. U jednoj grupi zemalja doneti su posebni zakoni, dok su u drugima ta pitanja rešena u propisima o industrijskoj svojini, privredni odnosima i sl. ***Kad su u pitanju računarski programi, softver i ICC usluge može se konstatovati da se i oni mogu pojaviti kao predmet nelojalnog nadmetanja. Po pravilu, oni su implicitno uvršćeni u oblike nelojalne utakmice***, a koji su to oblici zavisi od metoda koji je primenilo pravo te zemlje. Uglavnom postoje **dve grupe**

<sup>139</sup> Bainbridge D., op. cit., str. 57; Intellectual Property Issues in Software, Washington, National Academy Press, 1992. str. 24.

<sup>140</sup> Preuzeto od Marković S., op. cit., str. 57.

**zemalja: 1)** one koje primenjuju metod "*generalne klauzule*" kojom se na osnovu uslova i primera datih u odgovarajućem zakonu mogu pretpostaviti ponašanja koja predstavljaju nelojalnu konkurenciju. Sam predmet nije definisan, pa i računarski programi, softver i ICC usluge mogu da se nadju u ovim oblicima, s tim što se slučajevi koji nisu navedeni kao oblici nelojalne utakmice mogu naknadno uvrstiti. Tako bi se moglo postaviti pitanje da li se *shareware* programi mogu pojaviti kao oblik nelojalne konkurencije ili ne? Za sad ne postoji njihovo uvrščavanje u ove oblike, ali nije sigurno da to neće ubrzo biti, ukoliko su nazivi ovakvih programa "pozajme" od poznatih proizvođača i time izazove zabuna kod potencijalnih kupaca ili korisnika; i **2)** one zemlje koje primenjuju metod "*limitativnog nabiranja*" po kome su oblici nelojalne utakmice samo oni koji su izričito u zakonu predviđeni kao takvi. Ukoliko se računarski programi, softver i ICC usluge pojave u nekom od njih, biće predmet primene prava i sankcija za nelojalnu utakmicu. Kako programi, softver i ICC usluge mogu biti predmet sasvim specifičnih, a nepredviđenih dela, to se može desiti da ne budu zaštićeni ovim pravom.

**Drugo.** Većina zemalja kao **oblike u kojima se javlja nelojalna utakmica** najčešće predviđaju:

- a) nelojalnu reklamu;
- b) ocrnjivanje;
- c) davanje netačnih podataka o sebi ili robi i prikrivanje mana;
- d) neovlašćena upotreba obeležja druge organizacije;
- e) podmićivanje;
- f) premijski poslovi;
- g) ropsko podražavanje tuđe robe.

Bez obzira da li predviđaju sve ili samo neke od ovih oblika, gotovo sva prava su detaljno obradila **nelojalnu reklamu**, *pod kojom se podrazumeva reklamiranje, oglašavanje ili nudjenje robe ili usluga koje se obavlja navodjenjem podataka ili upotrebom izraza kojima se stvara ili može stvarati zabuna na tržištu*. Tako, pravo SAD predviđa sledeće oblike nelojalne reklame: netačno tvrdjenje o svom programu (vrhunski kvalitet, unikat); nelojalno reklamiranje prilikom prezentacije programa (korišćenje svedočenja poznatih ljudi); nelojalno reklamiranje u pogledu cena (označavanje sniženja koga nema); ocrnjivanje tuđeg proizvoda; nelojalno reklamiranje kod raznih oblika garancija; TV zloupotrebe i sl.

**Treće.** *Ukoliko se pojave kao predmet nelojalne utakmice kompjuterski programi, softver i ICC usluge se ne štite kao takve, već se sankcioniše radnja protivna dobrim poslovnim običajima kojom se nanosi, ili može naneti, šteta drugoj*

*organizaciji, a sve radi sticanja prednosti na tržištu.* Drugim rečima, zaštita se odnosi na organizaciju i/ili potrošače, ali i "društvene" interese.

**Četvrto. Zaštita po pravima većine zemalja sastoji se u imovinskopravnoj,** odn. građanskopravnoj zaštiti, koja se ostvaruje tužbom u parničnom postupku. Kad su u pitanju zemlje Common law sistema to je "*passing off*" institut, kojim se štiti "*goodwill*", dobra reputacija, renome, i poslovne veze firme koje su godinama građene, a koje se ugrožavaju jer se "proturaju" tuđji programi na tržište tako da stvaraju utisak, privid, da ih je proizvela renomirana firma. Moguća je i *krivičnopravna* i *upavnopravna zaštita*. U nekim zemljama primenjuje se i jedan specifičan oblik - *zaštita pred sudovima časti*.

**Peto. Ovaj oblik zaštite programa, softvera i ICC usluga može biti i supsidijaran,** odn. pojaviti se kao dodatni uz druge oblike zaštite (npr. patentom, žigom), s tim što se razlikuje predmet zaštite. Ukoliko se pojavljuje kao takav, ovaj oblik obezbeđuje potpuniju i kompleksniju zaštitu.

### 3.3.3. *Kompjuterski programi i međunarodna zaštita od nelojalne konkurencije*

#### 3.3.3.1. *Pariska konvencija za zaštitu industrijske svojine*

Osnovni međunarodni instrument kojim se reguliše zaštita od nelojalne utakmice je **Pariska konvencija za zaštitu industrijske svojine**<sup>141</sup>. Po ovoj Konvenciji međunarodna zaštita kompjuterskih programa, softvera i ICC usluga od nelojalne utakmice sastoji se od **tri elementa**:

1. zemlje članice Unije obavezne su da osiguraju pripadnicima Unije stvarnu zaštitu od nelojalne utakmice;
2. pošto Konvencija predviđa primenu metoda "generalne klauzule" to da bi se počinioci kaznili za delo nelojalne utakmice potrebno je da je ono protivno "poštenim običajima u industriji ili trgovini". Kao takva navode se tri dela (koja, inače, predstavljaju minimum):
  - a) *ponašanje jednog poslovnog subjekta kojim se može stvoriti zabuna*, a koja su realizovana ma kojim sredstvima, u vezi sa preduzećem,

<sup>141</sup> Pariska konvencija za zaštitu industrijske svojine, čl. 10 bis.

kompjuterskim programom, softverom ili ICC uslugom jednog od konkurenata,

- b) *lažni navodi* koji imaju za cilj da diskredituju proizvođača, program, softver ili ICC uslugu, i
  - c) *korišćenje oznaka ili navoda čija upotreba u trgovini može dovesti javnost u zabludu* o poreklu, načinu proizvodnje, osobinama ili pogodnostima za upotrebu određenog programa, softvera i ICC usluge. Kako je u pitanju "generalna klauzula" moguće je ova dela proširiti zavisno od nacionalnog prava zemlje članice;
3. kako Konvencija ne predviđa posebne sankcije to se mogu primeniti one koje su propisane nacionalnim zakonima zemalja članica.

Znači, postojanje ovog oblika zaštite od nelojalne utakmice od posebnog je interesa za računarske programe, softver i ICC usluge s obzirom na prirodu njihove trgovine i sve većeg izlaženja iz nacionalnih granica.

### 3.3.3.2. *Sporazum o trgovinskim aspektima prava intelektualne svojine*

**Sporazumom o trgovinskim aspektima prava intelektualne svojine** GATT-a predviđena je zaštita poverljivih podataka u cilju efikasne zaštite od nelojalne utakmice. Po odredbama člana 39. ***predviđeno je pravo fizičkih i pravnih lica da sprečavaju da se podaci koji su na osnovu zakona u njihovoj nadležnosti ne otkrivaju drugima, niti da ih drugi stiču ili koriste bez saglasnosti, a na način koji je suprotan dobrim poslovnim običajima.*** Izrazom "način suprotan dobrim poslovnim običajima" se obuhvata, bar, praksa proistekla iz povrede ugovora, narušavanja poslovnog poverenja i sl., a podrazumeva pribavljanje poverljivih podataka od strane trećih lica koja znaju, ili su u velikoj meri dužna da znaju, da je takva praksa nedozvoljena. **Poverljivi podaci** su:

1. podaci koji su poverljivi u smislu **da nisu**, posmatrani kao celina ili kao skup neophodnih komponenata, **opšte poznati** ili **lako dostupni** licima u krugovima koji se uobičajeno bave tom vrstom informacija;
2. **velike tržišne vrednosti** zbog svoje poverljive prirode; i
3. **predmet odgovarajućih mera** koje preduzimaju lica koja su na osnovu zakona obavezna da čuvaju poverljivost tih podataka.

Posebno se predviđaju slučajevi **ograničavanja konkurencije izdavanjem licenci**. Strane ugovornice mogu usvojiti odgovarajuće mere za sprečavanje ili kontrolu

prakse izdavanja licenci ili određivanja uslova licenciranja koje predstavljaju zloupotrebu prava intelektualne svojine sa negativnim posledicama na konkurenciju na tržištu na kom se pojavljuju. Ukoliko titular prava intelektualne svojine vrši radnje protivno zakonima i drugim propisima strana čiji to titulari rade i strane koje smatraju da titulari vrše zloupotrebe će pristupiti konsultacijama, a radi storniranja takvog stanja. Da bi se to realizovalo strane u konsultacijama se moraju međusobno informisati i to podacima koji su dostupni javnosti, kao i sa drugi informacijama, a u skladu sa nacionalnim zakonima i međusobno zaključenim ugovorima koji se odnose na čuvanje tajnih podataka<sup>142</sup>.

### 3.3.3.3. Rimski i Mاستrihtski ugovor

Pravo Evropske Unije je gotovo od samog nastanka zaokupljeno problemom nelojalne utakmice<sup>143</sup>. Već su **Pariskim sporazumom** iz 1951. godine odredbama 60 - 67 i 274 utvrđena su prva pravila koja su se odnosila na utakmicu u okviru Evropske Zajednice za uglj i čelik. Samo šest godina kasnije donosi se **Rimski ugovor** (*Treaty establishing the European Economic Community*) kojim se uspostavlja Evropska zajednica i kojim se u više odredbi regulišu i ova pitanja (2, 8, 3(f), 9, 30-34, 47, 85, 86, 92, 93, 94, 168, 189, 193-198, 222). Zatim sledi **Mاستrihtski ugovor** iz 1993. godine i niz posebnih akata (direkiva, preporuka, rezolucija) kojima se regulišu pojedina pitanja vezana za konkurenciju<sup>144</sup>. Po Rimskom i Mاستrihtskom ugovoru predviđena je sloboda kretanja roba i usluga, ali i "regulisanje zabrane anti - konkurentskih dogovora između poslovnih firmi pošto to može ozbiljno ugroziti Evropsko tržište". U vezi sa ispitivanjem povreda i ponašanja vezanih za nelojalnu konkurenciju ili monopolizam osnovana je posebna Komisija sa sedištem u Briselu. Ona treba i da donese odgovarajuća pravila ili uputstava radi ostvarivanja poštene konkurencije, kao i onemogućavanje svih onih radnji koje predstavljaju sprečavanje,

<sup>142</sup> Sporazum, čl. 40.

<sup>143</sup> Borchardt K. D., *The ABC of Community Law*, Luxembourg, Office for official publications of the European Communities, 1994., str. 42 i 43.

<sup>144</sup> Posebno značajni postaju dokumenti tipa "knjige" koji se donose kao analize ili putokaz za dalje pravce aktivnosti, među kojima je i **Bela knjiga o pripremama pridruženih zemalja Centralne i Istočne Evrope za integraciju u interno Zajedničko tržište Unije** (*White paper - Preparation of the Associated countries of Central and Eastern Europe for Integration into Internal Market of the Union* - 1995.), **Bela knjiga o rastu, konkurentnosti, zaposlenosti - izazovi i putevi ka 21 stoleću** (*White Paper - Growth, Competitiveness, Employment - The Challenges and Ways Forward into the Twenty-first Century* - 1994.). O tome više kod Drakulić M., Milovanović A., *Nelojalna konkurencija u pravu Evropske Unije*, Vrnjačka Banja, Zbornik radova: V međunarodni simpozijum SYM ORG '95; kao i: Mathijsen P. S. R. F., *A Guide to European Union Law*, London, Sweet & Maxwell, 1995; Savić N., Pitić G., *Vodič za beli papir Evropske unije*, Beograd, Poslovni krug, 1995.

narušavanje ili ograničavanje konkurencije, kao i zloupotrebe u korišćenju dominantnog položaja na zajedničkom tržištu, ili njegovom bitnom delu<sup>145</sup>. Pri tome, se kao zloupotrebe, na Zajedničkom tržištu pojavljuju i dela nelojalne utakmice, mada su ta dela mahom vezana za monopol, monopolističke sporazume i dominantan položaj na tržištu, a manje za klasična oblike nelojalne utakmice.

Naime, nelojalna konkurencija je često posledica zauzimanja dominantnog položaja, odnosno njegova zloupotreba. Zbog toga konkurentsko pravo EU predviđa koje korišćenje dominantnog položaja, jednog ili više preduzeća, predstavlja zloupotrebu, te je zabranjeno. Naravno sudovima (nacionalnim i unijinom) i nacionalnim pravima je ostavljeno da definišu šta se pod zloupotrebom, a šta pod dominantnim položajem smatra. Tako je u slučaju *Hoffman - La Roche* Sud pravde definisao zloupotrebu<sup>146</sup> kao “objektivni koncept stvaranja dominantnog položaja koji za posledicu ima slabljenje konkurencije, a nastao je primenom metoda takvih transakcija i ekonomskih operacija čiji su efekti u narušavanju normalnih uslova konkurencije u proizvodnji ili pružanju usluga”.

Odredbе Rimskog i Mastroitskog ugovora predviđaju četiri najčešća slučaja tih **zloupotreba**:

1. **nametanje cena** (kupovnih ili prodajnih) ili drugih uslova razmene, posredno ili neposredno;
2. **ograničavanja** proizvodnje, plasmana, tehničkog razvoja, a na štetu potrošača;
3. **nametanje** nejednakih uslova za ekvivalentne transakcije; i
4. **uslovljavanje** zaključenja ugovora dodatnim uslovima.

Naravno, pored ovih imenovanih oblika zloupotreba pojavljuju se i drugi kao što je npr. **odbijanje snabdevanja potrošača** ili potencijalnih potrošača od strane dominantnih organizacija, što izaziva brojne sudske sporove.

Ništa manje značajna nije ni zloupotreba **prava intelektualne svojine**, naročito vezana za kompjuterske programe i softver, i za koja se vezuje postojanje monopolskih prava njihovih nosilaca, a kojima se ograničava tržište i stvara jaz između njih i kupaca tehnologije. Ovaj se problem multiplicira razlikama koje između zemalja članica postoje, kao i razlikama sa drugim zemljama - nečlanicama. Zemlje članice

<sup>145</sup> Lopandić D., Janjević M., Ugovor o Evropskoj uniji, od Rima do Mastrohta, Beograd, Medjunarodna politika, Pravni fakultet, Fakultet političkih nauka, Institut ekonomskih nauka, Evropski pokret u Srbiji, 1995., str.72 - 77.

<sup>146</sup> Weatherill S., Cases and Materials on the EC Law, London, Blackstone Press Limited, 1992, str. 237.

moгу zabraniti uvoz, izvoz i tranzit robe ukoliko su te barijere opravdane i sluųe, izmedju ostalog, zaštiti “industrijske i trgovačke svojine”. Pretpostavka za uvođenje ovih barijera je da motiv nije diskriminacija ili prikriveni oblik ograničavanja tržišta medju zemljama. I ne samo to, permanentno se postavlja pitanje opravdanosti izuzimanja iz dejstva odredbi Ugovora (čl. 86) ekskluzivnih prava nosioca prava i garantovanje tog ekskluziviteta prema trećim licima. Monopolski karakter ovih prava je čest povod sudskih sporova (*Volvo AB v. Eric Veng; Tetra Pak Rausing S.A v Commission*), koji su trebali da razreše problem ovih prava, naročito kad su ona u suštini nosila i karakteristike zloupotreba dominantnog položaja<sup>147</sup>.

Za sprovođenje odredbi o konkurenciji (tačnije članova 85 i 86) Rimski, odn. Mاستrihtski ugovor je predvideo donošenje odgovarajućih specijalizovanih pravila i uputstva od strane Saveta (prvo takvo pravilo je Regulation 17), a na predlog Komisije i uz prethodnu saglasnost Evropskog parlamenta. Ova uputstva i pravila treba da se donesu 3 godine od stupanja Ugovora na snagu. Jedan od osnovnih razloga je uvođenje kazni za sklapanje sporazuma kojima se ograničava ili narušava konkurencija. Osim toga njihov cilj je i ubrzanje i pojednostavljenje administrativnih postupaka, kao i nadzor u primeni odredbi Ugovora. Kako je prisutan problem razgraničenja nadležnosti Komisije i Suda, to pravila i uputstva treba i to da razgraniče. Posebno je značajno razgraničenje izmedju nacionalnih propisa i odredbi Ugovora, odnosno akata Unije donetih na osnovu njih. Pri tome se stalno mora imati u vidu da stvarna primena i poštovanje pravila konkurencije zavisi od postojanja odgovarajućih sudskih i administrativnih organa u državama članicama. Sudski sistemi treba da garantuju takve sudske postupke koji se baziraju na dostupnosti i brzini u rešavanju sudskih sporova proisteklih iz kršenja odredbi o konkurenciji i ponašanju na zajedničkom tržištu.

U skladu sa zahtevom o harmonizaciji prava zemalja članica doneta je i **Direktiva 92/59** (*Directive 92/59*) kojom se zaštićuju potrošači, određuje minimum standarda sigurnosti proizvoda i predviđaju zaštitne mere kako bi se rizici upotrebe sveli na najmanju meru<sup>148</sup>. Medju proizvodima mogu se naći i kompjuterski programi, te je nužno da i oni prate postavljene standarde.

### 3.3.4. *Kompjuterski programi i zaštita od nelojalne konkurencije po našem pravu*

<sup>147</sup> Singleton S., *Introduction to Competition Law*, Pitman Publishing, London, 1992., str. 137.

<sup>148</sup> Cartwright P., *Product Safety and Consumer Protection*, *The Modern Law Business*, no. 58/95., str. 222 - 231.

### 3.3.4.1. Oblici u kojima se javlja nelojalna konkurencija

Po našem pravu **nelojalna utakmica** je svaka radnja poslovnog subjekta koja je protivna dobrim poslovnim običajima i kojom se nanosi, ili može naneti, šteta drugom poslovnom licu i potrošačima<sup>149</sup>. Takodje, naše pozitivno pravo pri određivanju pojma i elemenata nelojalne utakmice prihvata metod "generalne klauzule"<sup>150</sup>. Naime, predviđaju se samo neka, najkarakterističnija, ponašanja koja se mogu smatrati oblicima nelojalne utakmice i koja se navode kao primeri<sup>151</sup>, a za svako novi oblik ili delo koje se pojavi posebno se utvrđuje da li su njime povredjeni dobri poslovni običaji, ili ne.

Ako bi kompjuterski programi, softver ili ICC usluge bile predmet nelojalne konkurencije raznih poslovnih subjekata, najčešće bi to bilo kroz:

1. **nelojalnu reklamu** (superlativna reklama, kritikujuća, naslanjajuća, itd.);
2. **ocrnjivanje**;
3. **davanje netačnih podataka** o programu, softveru ili ICC uslugama;
4. **prikrivanje** mana programa, softvera, ICC usluga;
5. **povredu tuđih poslovnih odnosa**;
6. **zloupotrebu na rasprodajama**, naročito u vreme popularnih novogodišnjih i božićnih rasprodaja;
7. **neovlašćenu upotrebu obeležja druge organizacije**;
8. **ovlašćenu upotrebu spoljnih obeležja druge firme**;
9. **neovlašćeno korišćenje tuđih poslovnih usluga**;
10. **podmićivanje**, koje obuhvata i premijske poslove.

Tako, kao delo nelojalne utakmice moglo bi se proglasiti reklamiranje proizvoda jedne poznate strane softversko-hardverske organizacije koja je tvrdila da paket njenih programa sadrži i računarske programe kojima se podržava automatizacija kancelarijskog poslovanja, a što je u osnovi bila **prevarna reklama**. Između ostalog, to je bio razlog što je druga firma naručila kompletnu konfiguraciju računara i sve programe<sup>152</sup>. Prilikom instaliranja utvrđeno je da je aplikacija vezana za automatizaciju nezavršena i da je u fazi testiranja. Kako je prilikom kupovine bilo ponuda i drugih firmi, to je konstatovano postojanje dela nelojalne utakmice, tim više, što je naknadno

<sup>149</sup> Zakon o trgovini, Službeni list SRJ, br. 32/93., čl. 22.

<sup>150</sup> Besarović V., op. cit., str. 153.

<sup>151</sup> Zakon o trgovini ih navodi 10, a Zakon o spoljnotrgovinskom poslovanju 6.

<sup>152</sup> Slučaj je lično poznat autoru, desio se 1989. godine u Sloveniji, a radilo se o firmi iz Srbije koja je bila zastupnik američke firme za računare.

ustanovljeno, proveravanjem direktno kod proizvođača, da ta konfiguracija nije podržana softverom. Naime, još nezavršeni računarski program uopšte nije bio za taj, već za drugi tip mašine. Kako je u pitanju bila prevaziđena tehnologija, to se katalog koji je pratio reklamu i ponudu pojavio kao netačan i istovremeno su prikrivene mane tog tipa PC. Ovo je tipično **delo nelojalne reklame** čija je posledica stvaranje zabune među subjektima kako bi se određena (zastarela, nepouzdana, nesolidna, sa bagovima i sl.) konfiguracija i softver plasirali na tržište i ostvarila zarada.

Druga dva slučaja vezana su za istu firmu, ali za druge oblike nelojalne utakmice. Naime, ova firma, kao zastupnik poznate kompanije iz SAD, prilikom davanja ponuda za prodaju navodila je i usluge održavanja. To je stvarno i radila. Nakon raskida saradnje sa američkom firmom naša je firma preuzela korisnike, ali je ugovore o održavanju, zahvaljujući činjenici da su se korisnici navikli na nju i kvalitet ranijih usluga koji je bio izuzetan, sa istim korisnicima revidirala i, umesto godišnje, ugovarala mesečno servisiranje. To je bila prilika da svakog meseca enormno povećava cenu. Naša firma je bila tužena i Privredni sud u Beogradu je konstatovao **delo ovlašćene upotrebe spoljnih obeležja druge firme i prevarne reklame**.

Ista firma je bila i "kooperant" poznate inostrane firme, a ne samo njen zastupnik. Svi domaći kupci su to znali, kao što su i znali da su hardver i softver, koji je prodavala, dobrog kvaliteta. Nisu imali ništa protiv ni u slučajevima kad su kao rezervne delove ili dodatne računarske programe dobijali proizvode naše firme, koja je imala isključivu licencu za svoje proizvode na ime strane. U toku ekspanzije na tržištu Srbije naša firma je postepeno svoje, mnogo skuplje programe, prodavala kao proizvode strane firme. Kako su joj ovi poslovi veoma dobro išli naša firma počela ih je nuditi umesto stranih. Strana kompanija dugo nije znala za ovaj "uspešni poslovni potez" i kad je to saznala raskinula je sve ugovore sa našom firmom. Domaća firma je, pored toga, još i bila tužena za delo **prisvajanja poslovnih usluga**, jer je neovlašćeno prisvojila poslovne veze i kontakte, kao i renome, kvalitet, od strane firme.

### 3.3.4.2. *Uslovi i oblici zaštite*

Da bi se računarski programi, softver ili ICC usluge našli kao predmet dela nelojalne konkurencije neophodno je ispunjenje određenih **uslova**, odn. postojanje sledećih **elemenata**<sup>153</sup>:

1. **da je nelojalna utakmica izvršena samo od strane poslovnih subjekata** (naša ili strana preduzeća, društvena, privatna, mešovita);
2. **da je vezana za poslovnu delatnost bez obzira koja to vrsta delatnosti** (proizvodnja programa, promet programa i ICC usluga i sl.);
3. **da je izvršena u cilju nadmetanja poslovnih subjekata**, odn. radi privredne utakmice;
4. **da se krše dobri poslovni običaji**; i
5. **da je posledica šteta**, materijalna i/ili moralna, koja je naneta ili je mogla biti naneta drugom poslovnom subjektu i/ili potrošaču.

Ukoliko su učinjena dela nelojalne utakmice u vezi sa kompjuterskim programima, softverom i ICC uslugama **naše pravo**<sup>154</sup> **predviđa nekoliko oblika zaštite** koji se mogu pojedinačno ili kumulativno koristiti. Tako se, kao glavna, predviđa **kaznenopravna zaštita**. Osim toga predviđena je i **krivičnopravna zaštita**, kao i poseban vid - **zaštita od strane sudova časti**. Raniji su propisi predviđali i **gradjanskopravnu i upravnu pravnu zaštitu**, no važeći je Zakon to propustio ili sveo na neznatnu mogućnost u rešavanju.

Dakle, osnovni oblik zaštite je **kaznenopravna** koja se primenjuje za sva ona ponašanja koja nose elemente nelojalne utakmice i koja su **privredni prestupi** ili **prekršaji**. Za privredne prestupe kažnjavaju se **novčanom kaznom** preduzeća ili pravna lica, kao i odgovorno lice u okviru njega. Prekršaj povlači niže **novčane kazne** za pravno lice ili trgovca, kao i odgovorno lice.

**Krivičnopravna** je zaštita predviđena Krivičnim zakonom Savezne Republike Jugoslavije u posebnom odeljku koji se odnosi na krivična dela protiv privrede i jedinstva jugoslovenskog tržišta. Od nekoliko članova koji su se u ranijoj

<sup>153</sup> Vlašković V., op. cit., str. 97 i 98.

<sup>154</sup> Zakon o trgovini; Zakon o suzbijanju nelojalne utakmice i monopolističkih sporazuma, Službeni list SFRJ., br. 32/1974.

verziji odnosili na nelojalnu utakmicu<sup>155</sup> u Zakonu je ostao samo onaj vezan za **neovlašćenu upotrebu tuđe firme** pod kojim se podrazumeva ponašanje sa namerom da se obmanu kupci programa ili korisnici ICC usluga. Za to delo predviđena je **kazna zatvora do 3 godine**<sup>156</sup>. Isto se desilo i sa krivičnim delom koje je postojalo po Zakonu o trgovini iz 1990. godine - izgubilo se.

**Krivičnopravna zaštita** predviđena je i Krivičnim zakonom Republike Srbije<sup>157</sup>, i direktno se odnosi na dva dela: **narušavanje poslovnog ugleda i kreditne sposobnosti i obmanjivanje kupaca**.

**Narušavanje poslovnog ugleda i kreditne sposobnosti**<sup>158</sup> je relativno novo krivično delo, uvedeno 1994. godine sa ciljem da se kazne svi oni koji narušavaju poslovni ugled nekog poslovnog subjekta iznoseći o njemu neistinite podatke ili neistinito prikazuju njegovo poslovanje. To znači, **ko iznosi neistinite podatke o proizvođaču programa, softvera ili pružaocu ICC usluga biće kažnjen zatvorom do 1 godine**. Ako nastupe teške posledice učinilac se kažnjava **zatvorom od 3 meseca do 3 godine**. S obzirom da je u pitanju fizičko lice to ono može biti iz druge organizacije i delo činiti radi eliminacije subjekta iz poslovne utakmice jer mu je poslovni ugled ugrožen.

Drugo delo se tiče **obmanjivanja kupaca**<sup>159</sup>, a izvršava se:

- a) stavljanjem u promet kompjuterskih programa **sa oznakom u koju su uneti podaci koji ne** odgovaraju sadržini, vrsti, poreklu ili kvalitetu programa, odn. usluga;
- b) stavljanjem u promet programa **koji po kvalitetu ne odgovaraju** onome što se redovno pretpostavlja kod takvih programa ili usluga;
- c) stavljanjem u promet programa **bez oznake** o sadržini, vrsti, poreklu, ili kvalitetu, a oznaka je propisana.

<sup>155</sup> Zanimljivo je da je član koji se odnosio na nelojalnu utakmicu u poslovima spoljnotrgovinskog prometa članom 43. Zakona o izmenama KZ SRJ, Službeni list SRJ, br. 37/93., brisan.

<sup>156</sup> Krivični zakon SRJ, čl. 165.

<sup>157</sup> Krivični zakon republike Srbije, Službeni glasnik RC, br. 26/77; 43/77; 20/79; 24/84; 39/86; 51/87/6/89; 42/89; 21/90; 49/93; 67/93; 47/94. Zakonom o izmenama Krivičnog zakona Socijalističke Republike promenjen je naziv u Krivični zakon Republike Srbije, Službeni glasnik RC, br. 42/92.

<sup>158</sup> Krivični zakon RS, čl. 139b.

<sup>159</sup> Krivični zakon RS, čl. 146., st.1.

U svim ovim slučajevima predviđena je **kazna zatvora do 3 godine i novčana kazna**.

Krivični zakon Srbije ide i korak dalje - predviđa posebno krivično delo lažne reklame<sup>160</sup>. Pod njom podrazumeva **obmanjivanje kupaca lažnim objavljivanjem**:

- a) da je *snižena cena* računarskim programima ili obavljanju ICC usluga;
- b) da se *vrši rasprodaja* programa;
- c) da *predstoji povišenje cena*; ili
- d) na *drugi način*.

Za ova ponašanja kazna je **novčana ili zatvora do 1 godine**.

Vezu sa nelojalnom utakmicom računarskih programa ili obavljanja ICC usluga mogu imati i dela: **nedozvoljene trgovine; nedozvoljene proizvodnje; kršenja propisa o cenama; i povlašćivanja kupaca**, mada su ona više vezana za neke oblike špekulacije ili monopolskog ponašanja.

**Nedozvoljena trgovina** postojala bi u slučajevima kad neko nema dozvolu za trgovinu, npr. neregistrovano pravno ili neovlašćeno fizičko lice, a nabavi programe ili predmete koji sadrže programe, u većoj količini ili vrednosti radi prodaje. Isto tako nedozvoljena trgovina postojaće i ako se neko neovlašćeno i u većem obimu bavi trgovinom ili posredovanjem u trgovini. Može se desiti i da zastupa domaće proizvođače programa ili vršioce ICC usluga u njihovom prometu. U svim ovim slučajevima pojaviće se u nelojalnoj utakmici sa licima koja imaju dozvole i ovlašćenja. Za takvo ponašanje predviđena je **kazna zatvora do 3 godine i novčana kazna**.

Posebno se predviđa i slučaj kad se neko bavi **prodajom programa čiju je proizvodnju neovlašćeno organizovao**, što neodoljivo podseća na uobičajenu aktivnost kopiranja i prodaje programa bez odgovarajuće saglasnosti.

Lica koja vrše neovlašćenu prodaju, kupovinu ili razmenu programa čiji je predmet zabranjen ili ograničen, takodje, čine krivično delo. **Kazna može biti zatvor od 3 meseca do 5 godina**.

---

<sup>160</sup> Krivični zakon RS, čl. 146., st. 2.

Ako se još i **organizuje mreža prodavnica ili posrednika ili se postiže imovinska korist** čiji iznos prelazi zakonom limitirani, **kazniće se zatvorom od 1 do 8 godina**.

U svim ovim slučajevima **kompjuterski programi** (i sve kopije) **koji su predmet nedozvoljene trgovine se oduzimaju**.

Ukoliko se pojave kompjuterski programi takve prirode da se njihova proizvodnja ili prerada zabranjuje<sup>161</sup>, a to se i dalje obavlja u pitanju je krivično delo **nedozvoljene proizvodnje**, a **kazna je zatvor do 3 godine**. Naravno, **program i računar na kome se proizvodi se oduzimaju**.

Mada na prvi pogled izgleda više kao monopolsko nego delo nelojalne utakmice ipak elementi nelojalne utakmice postoje i u ponašanju kojim se **krše propisi o cenama**, prodajom programa ili vršenjem ICC usluga po cenama koje su znatno više od propisanih<sup>162</sup>. Za takve slučajeve predviđena je **kazna zatvora do 3 godine**, s tim što se **kaznjava ne samo za učinjeno delo, već i za pokušaj**.

Specifičan oblik nelojalne utakmice je **povlašćivanje određenih kupaca**<sup>163</sup>. U ovom delu postoje i elementi špekulacija. U svakom slučaju to se može dešavati sa računarskim programima u posebnim uslovima (npr. primene sankcija) kada zbog zabrane uvoza može doći do njihove nestašice ili nestašice novih verzija nužnih za dalji rad nekog tehnološkog procesa. Tada, kao i u slučaju kada se određenim kupcima prodaju programi u nesrazmerno velikoj količini ili se pojedini kupci obaveštavaju o sniženju, odn. povišenju cena, dolazi do krivičnog dela povlašćivanja kupaca i mogućnosti **kaznjavanja počinioca novčanom ili kaznom zatvora do 3 godine**. Ukoliko još dodje i do uznemiravanja građana, što je za računarske programe, ruku na srce, neuobičajeno, tada je u pitanju teži oblik dela i **kazna zatvora od 6 meseci do 5 godina**.

Važeći Zakon o trgovini nije *explicite* predvideo **gradjanskopravnu** ili imovinskopravnu zaštitu, već je to ostavio uobičajenim odredbama obligacionog prava. Ova zaštita ostvaruje se na osnovu tužbe u parničnom postupku. Tužba može biti za:

- **obustavu;**

<sup>161</sup> To bi npr. bili programi koji su se pojavili u Australiji i koji se koriste za autanaziju, ili programi koji vredaju javni moral, kao što je slučaj sa dečijom pornografijom koja je uzela maha u SAD, Kanadi, V. Britaniji, i koja dobija razmere epidemije jer se sve češće koristi Internet.

<sup>162</sup> Krivični zakon RS, čl. 151.

<sup>163</sup> Krivični zakon RS, čl. 152.

- *otklanjanje;*
- *naknadu štete*<sup>164</sup>.

Veoma često se tužba za obustavu i tužba za otklanjanje podnose zajedno jer se tužbeni zahtevi međusobno dopunjuju i baziraju na istim činjenicama.

Kad je u pitanju *tužba za naknadu* pretrpljene štete tužilac mora dokazati da je između štete koja je nastala, ili je mogla nastati, i određenog ponašanja koje čini nelojalnu utakmicu, postojala uzročna veza., naravno i da je tuženi odgovoran za štetu. Veliki je problem kako utvrditi odgovornost, odn. na osnovu kog će se kriterijuma ona odredjivati. Usaglašen je stav da se ona ocenjuje na osnovu određenog ponašanja koje se ne bi moglo očekivati od dobrog i pažljivog privrednika u određenim okolnostima. Šteta mora da je izazvana namerno, krajnjom ili običnom nepažnjom. Znači, ukoliko organizacija namerno stavi sličan ili isti znak na računarski program, kao što je znak neke druge firme, i zbog toga izazove zabunu i štetu poslovanju firme sa prvobitno zaštićenim znakom, tada će odgovarati za tu nastalu štetu. No, većina prava, pored stvarno prouzrokovane štete, prihvata i izgublenu dobit kao nešto što bi trebalo nadoknaditi. Posebno je značajna i šteta koju pretrpi organizacija zbog gubitka ugleda, imidža, goodwill-a, te može zahtevati naknadu ove neimovinske štete. Svakako da značaja ima unošenje povrede ugleda u krivično zakonodavstvo, ali nije zanemarljiva činjenica i plaćanja odštete. Tim više, što se u sudskim sporovima u drugim zemljama visina naknade za ovu štetu kreće u ogromnim sumama, tako da njihova visina predstavlja svojevrsnu pretnju eventualnim počiniocima. Međutim, kad su u pitanju baš programi, softver ili ICC usluge, učestalost dela nelojalne utakmice je sve veća, kao što raste i broj zahteva za naknadu štete zbog gubitka ugleda i visine naknade koje se za to presudjuju. Kod nas se ova praksa još nije ustalila, što je posledica, između ostalog, i nemarnosti sa kojom se mnoge male firme odnose prema toj instituciji.

**Pravo na podnošenje** ovih tužbi mogu imati: poslovni subjekti koji su **oštećeni**; **privredna komora** i drugi oblici udruživanja, **potrošači** i drugi zainteresovani organi ili organizacije<sup>165</sup>.

Osim izostanka građanskopravne iz našeg pozitivnog prava izostala je i **upravnopravna zaštita**, koja naročito značajna biva za sve one slučajeve u kojima i sa kojima su ugroženi i oštećeni potrošači. Nedostatak upravnopravnih mera u tekstu zakona kojim se reguliše nelojalna utakmica nije razumljiva pogotovo što je ova zaštita postala toliko važna da se u međunarodnim i nacionalnim okvirima ona posebno

<sup>164</sup> Besarović V., op. cit., str. 176 - 179.

<sup>165</sup> Zakon o trgovini, čl. 40.

reguliše. Mnoge su zemlje predvidele posebne komisije koje se staraju o zaštiti potrošača (*Federal Trade Commission* u SAD) i, naravno, o kvalitetu i komformnosti kompjuterskih programa i izvršenih ICC usluga<sup>166</sup>.

Paralelno sa razvojem uobičajenih oblika zaštite od nelojalne konkurencije razvijala se i jedna posebna zaštita koja se realizovala **pred sudovima časti**. To su specijalizovani sudovi koji se formiraju pri trgovinskim (privrednim) komorama, a odlučuju o kršenju dobrih poslovnih običaja. Za takve povrede, na osnovu sprovedenog postupka, sud časti može izreći jednu od sledećih mera:

- ♦ *opomena* bez objavljivanja u štampi;
- ♦ *opomena sa objavljivanjem* na skupštini komore;
- ♦ *javna opomena* sa objavljivanjem u štampi;
- ♦ *gubitak prava* na izbor u organe komore;
- ♦ *zabrana učešća* na sajmovima, izložbama, i sl.

Iako sasvim logično proizlazi iz same prirode ponašanja koje se karakteriše kao nelojalno ova zaštita nije još uvek, kod nas, zauzela dostojno mesto. Mali broj slučajeva ne ohrabruje da će njen značaj porasti, niti u će se bolje i više sankcionisati ponašanja koji je prouzrokuju. Za očekivati je da vreme ovog oblika zaštite tek dolazi, a osobito što se kompjuterskih programa i ICC usluga tiče.

Na osnovu svega prethodnog može se konstatovati sledeće:

**Prvo.** *Naše pravo priznaje mogućnost da se kao predmet nelojalne utakmice mogu pojaviti kompjuterski programi, softver i ICC usluge.* Prihvatanjem "generalne klauzule" propisani oblici ove konkurencije mogu se proširiti i sa specifičnim delima.

**Drugo.** Svakako treba imati u vidu *da se ne štite kompjuterski programi kao takvi, već poslovni subjekti od radnji i ponašanja drugih poslovnih subjekata, a kojima se krše dobri poslovni običaji i nanosi šteta.* Medjutim, za programe i softver treba imati u vidu još jednu osobenost. Dobri poslovni običaji koji su se formirali gotovo kao standardi podrazumevali su do nedavno skoro normalnim kopiranja i korišćenje programa bez dozvole nosioca prava, naročito stranih firmi. U takvim slučajevima veoma je problematično kako ove "običaje" tretirati. Isto tako pitanje je i tretmana ponašanja "dobrog i pažljivog privrednika", kad iza toga postoje znatne

---

<sup>166</sup> Drakulić M., op. cit., str. 174 - 180.

"uštede" zbog korišćenja kopiranih i neovlašćeno proizvedenih, neovlašćeno puštenih u promet i instaliranih programa.

**Treće.** U našem pravu, kao i u mnogim drugima, *potpunija efikasnost primene zaštite od nelojalne utakmice predstavlja dopunu zaštite računarskih programa, softvera i ICC usluga drugim pravima* (autorskim, žigovima i sl.).

**Četvrto.** Za očekivati je da "svetli dani" ovog oblika zaštite tek dolaze i *da će ona uspeti izboriti dostojno mesto u skladu sa značajem koji ima.*

### 3.4. *Kompjuterski programi i autorskopravna zaštita*

#### 3.4.1. *Opšte napomene o autorskopravnoj zaštiti*

Da bi kompjuterski program uživao autorskopravnu zaštitu on mora da predstavlja intelektualnu tvorevinu koja je nastala kao rezultat duhovnog stvaralaštva određene osobe - tvorca dela<sup>167</sup>. S obzirom da se radi o tvorevinama ljudskog duha to se postavilo pitanje da li ona mora biti u nekoj formi i u kojoj<sup>168</sup> da bi mogla uživati autorskopravnu zaštitu. Uglavnom su se u teoriji pojavila dva shvatanja. **Po prvom, monističkom**<sup>169</sup>, da bi neka tvorevina mogla da se podvede pod autorsko delo bitna je činjenica da je ideja izražena u nekoj formi. Sama ideja, kao sastavni deo unutrašnje ličnosti autora i njegovog intelekta ne uživa autorskopravnu zaštitu. Pri tome je neophodno naglasiti da vrsta, način i oblik izražavanja ne predstavljaju ključnu komponentu za zaštitu autorskog dela. **Drugo shvatanje, dualističko**<sup>170</sup>, polazi od toga da se izražajna forma dela i ideja ne mogu odvojiti, pa otuda autorskopravna zaštita obuhvata i jednu i drugu komponentu autorskog dela.

##### 3.4.1.1. *Uslovi zaštite*

<sup>167</sup> Izuzetak su ona dela koja su nastajala kroz vekove i čiji autor nije poznat (narodne pripovetke, pesme i sl).

<sup>168</sup> Osnovni je zahtev da je delo rezultat duhovnog stvaralaštva, a ne rutinskog rada, što kompjuterski program zadovoljava činjenicom da predstavlja ukupnost intelektualno razradjenog materijala za rešavanje određenog problema pomoću uređaja za obradu podataka, Parać Z., Kompjuterski program - autorsko djelo i u jugoslovenskom autorskopravnom režimu, Zbornik referata: Posvetovanja Pravni aspekti varstva in uporabe računalniških programov in podatkovnih baz, Nova Gorica, 1988., str.105.

<sup>169</sup> Monističko je shvatanje preovladjujuće i pojavljuje se u nemačkom i anglosaksonskom pravu.

<sup>170</sup> Dualističko shvatanje posebno je zastupljeno u francuskom pravu i pravima zemalja kojima ovo prava predstavlja uzor.

Da bi neka tvorevina ljudskog duha mogla da predstavlja autorsko delo, po pravilu, bi trebalo da zadovoljava **odredjene uslove**, a najčešći su:

- a) da delo bude u nekoj **izražajnoj formi**;
- b) da delo bude **originalno**;
- c) da delo bude **objavljeno**;
- d) da su **ispunjene formalnosti**, kao što su: **oznaka copyright, depozit, registracija i "klauzula o proizvodnji"**.

Prvi uslov **da delo bude u nekoj izražajnoj formi** ne znači da se i određuje koja je to forma.<sup>171</sup> Forma u kojoj je izražena sadržina jednog autorskog dela ne mora da bude i fizički materijalizovana forma (npr. usmena književna dela, muzička dela bez nota). Međutim, ono što je bitno i usvojeno u mnogim zakonima je da je program fiksiran na nekom sredstvu (medijumu), a da li je to sada poznato ili kasnije pronadjeno, je nerelevantno. Bitno je da se delo, odn. kompjuterski program može "opaziti, reprodukovati ili na drugi način saopštiti, bilo neposredno, bilo uz pomoć odgovarajućih mašina ili uredjaja".<sup>172</sup> Ovo pitanje je bilo ranije posebno bitno zbog razumljivosti programa u objektnom kodu. Danas se ono više ne postavlja. Pored toga, sadržina nekog dela štitiće se i ako ono nije u definitivnoj formi, ukoliko je nedovršeno, ali može u dovoljnoj meri da odrazi sadržinu. Posebno je značajno da materijalna podloga na kojoj je delo fiksirano u većini zemalja ne uživa autorskopravnu zaštitu bez obzira koliko je originalna<sup>173</sup>. Analogijom se može zaključiti da ni omot, performanse ili veličina diskete neće uživati zaštitu zajedno sa računarskim programom.

**Originalnost** je uslov i pretpostavka da neko delo iz oblasti književnosti, nauke ili umetnosti može predstavljati autorsko delo. Obično je originalnost vezana za ličnost autora - **autorska originalnost** i za rezultat njegovog stvaralaštva - **originalnost dela**.

**Originalnost autora znači da delo odražava njegov individualni karakter, da je rezultat njegove inspiracije i individualnog duhovnog sadržaja njegovog tvorca.** Kad su u pitanju kompjuterski programi ranije se postavljalo pitanje da li u njima postoji individualnog izraza njihovog autora, ili su individualna tvorevina zadati problemi i parametri njihovog rešavanja. Čak je postojala i dilema da li bi više

<sup>171</sup> Besarović V., op. cit., str. 213.

<sup>172</sup> čl. 102 (a) Zakona o autorskom pravu SAD.

<sup>173</sup> Npr. pored originalnosti književnog dela vrlo često i oblik knjige, oprema ili vrsta slova se pojavljuju kao originalna ideja, međutim, oni neće uživati autorskopravnu zaštitu.

programera stvorilo, u osnovnim crtama, jednake programe zavisno od konkretnih okolnosti u kojima se ovi programi stvaraju. Teorija i praksa su negativno odgovorili na ova pitanja, čime se ova dilema otklonila<sup>174</sup>. **Postojanje originalnosti autora znači da se kod drugih ljudi, koji imaju dodir sa delom, izaziva osećaj (utisak) do tada nevidjenog dela.** Takodje, originalnost dela pretpostavlja autorsku originalnost onda kad postoji izvornost i autentičnost inspiracije, odn. kad delo predstavlja novu duhovnu tvorevinu i kad je rezultat izvorne inspiracije. Tako, npr. jedan sistem inženjer napravi originalni računarski program. Pored njega radi drugi sistem inženjer koji, inspirisan rešenjima svog kolege, napravi drugi program. Bez obzira koliko je ličnih elemenata uneo drugi sistem inženjer njegovo delo neće uživati autorskopravnu zaštitu jer ne ispunjava autorsku originalnost, niti je rezultat izvorne inspiracije.

Oko odredjivanja pojma originalnosti dela bilo je mnogo rasprava i nesuglasica jer je originalnost veoma slična pojmu novosti. Iako vrlo slične, originalnost i novost se razlikuju po kriterijumu po kom se procenjuju. **Originalnost se procenjuje uvek po subjektivnom kriterijumu** jer je, po pravilu, umetnička kategorija (stilsko, npr.) koja se vezuje za estetski kriterijum (otuda i teškoće u uvrščavanju računarskih programa u autorska dela, medjutim, kako se stvaralaštvo odnosi i na naučna dela to bi isti kriterijumi originalnosti mogli da važe i kod njih). Poseban je problem konkretnog kriterijuma po kom će se to ocenjivati. Da bi se olakšalo utvrdjivanje u američkoj sudskoj praksi<sup>175</sup> je, npr. formulisan test za ocenu, po kome se utvrdjuje da li određeni program ima "*protectable form of any idea*" ili samo "*idea*". Ukoliko u ima "*protectable form of any idea*" pružiće mu se zaštita, a ukoliko je u pitanju samo ideja, ne. **Novost je kategorija koja se procenjuje po objektivnom kriterijumu** pošto novost pronalaska znači da on predstavlja tehničku novost, a ne subjektivni utisak. Od ove novosti treba razlikovati novinu rešenja<sup>176</sup> koja predstavlja onu razliku po kojoj se jedan program pojavljuje kao produkt kreativnosti u kojoj je individualan izraz autora i po kome se razlikuje od drugog i/ili "potencijalnog ostvarenja prosečnog programera". Kategorija "prosečnog programera" pojavljuje se kao kriterijum za odredjivanje da li ima odstupanja od "rutinskog i prosečnog u struci". Ovo je bitno za odredjivanje jedinice "znatnog odstupanja od granice prosečnog", a što može imati značaja za autorskopravnu zaštitu. Naime, "prosečni" ili neznatno iznad granice proseka programi ne bi trebalo da se pojave kao autorska dela, niti bi se "prosečnim programerima" trebalo priznati svojstvo autora<sup>177</sup>. Dakle, primenom ovog kriterijuma sadržaj jednog kompjuterskog

<sup>174</sup> Parać Z., op. cit., str. 107.

<sup>175</sup> Početak je bio spor *Apple Computer, Inc. v. Franklin Computer Corp.*, o čemu više kod: Parać Z., op. cit., str. 108; Lipner S., Kalman S., op. cit., str. 18 - 32.

<sup>176</sup> Parać Z., op. cit., str. 110.

<sup>177</sup> U teoriji i praksi se zdušno vodila diskusija za odredjivanje šta se pod "prosečnim" programom i programerom podrazumeva, o čemu više kod Parać Z., op. cit., str. 112.

programa moći će se razlikovati od drugog, a autorskopravnu zaštitu može uživati onaj koji je vidljivo iznad "prosečnog".

Rešenje nesuglasja i dileme oko utvrđivanja konkretne originalnosti nadjeno je u formuli koju je dao *Viši zemaljski sud u Frankfurtu* pre desetak godina (1984. godine) i po kojoj je **kompjuterski program originalan ako**<sup>178</sup>:

- tok programa i struktura naredbi ne proizlaze nužno iz programskog zadatka;
- autor može slobodno da bira između različitih formula i puteva rašavanja programskog zadatka, odn. ako može u znatnoj meri da sam postavlja varijable;
- se ne iscrpljuje samo u mehaničko-tehničkom izvođenju i rasvetljavanju opštepoznatih činjenica.

Suština **originalnosti kompjuterskog programa** kao autorskog dela, znači, leži u njenoj kompleksnosti jer je sačinjavaju **dva elementa: subjektivni**, individualnost izraza svakog programera i njegove lične duhovne sfere, a što varira od programa do programa; i **objektivni**, da je novina u smislu odnosa novog prema već postojećim programima<sup>179</sup> ili svih ostalih koji nastaju ili će nastati nezavisno od njega<sup>180</sup>.

Ono što je bitno da samo originalno delo, zajedno sa autorskom originalnošću, može da ispunjava uslov za autorskopravnu zaštitu. S obzirom da je život mnogo komplikovaniji i da se neke stvari, odnosi i oblici ne mogu tako lako odvojiti, to se prvo u praksi, pa potom i u propisima, pojavilo i izvedeno delo za koje autori žele da obezbede pravnu zaštitu. Ne ulazeći u mnogobrojne rasprave i shvatanja o prirodi ovakvih dela treba istaći da se kod izvedenih dela autor može vrlo blizu primači plagijatu, kopiji, podržavanju, a za koje važe posebne sankcije u okviru građanskopravne i krivičnopravne odgovornosti. Pogotovo što se to sve zajedno teško može odvojiti. Međutim, i naše pravo poznaje kategoriju izvedenih autorskih dela navodeći da su to prevodi, prilagođavanja, muzičke obarde i druge prerade autorskih dela.<sup>181</sup>

---

<sup>178</sup> Marković S., op. cit., str. 112.

<sup>179</sup> Parać Z., op. cit., str. 15.

<sup>180</sup> Marković S., op. cit., str. 106.

<sup>181</sup> Zakon o autorskom pravu, Službeni list SFRJ, br. 19/78; 24/86; 21/90; čl. 5.

U nekim, najčešće **anglosaksonskim**, pravnim sistemima, pored ovih, predviđali su se i drugi uslovi koje je trebalo da ispuni neko delo da bi moglo da uživa autorsku pravnu zaštitu. Tako se kao **posebni i neophodni uslovi** pojavljuje objavljivanje i ispunjenje određenih formalnosti.

**Objavljivanje dela je radnja kojom se neko delo prezentira javnosti, većem krugu lica koja međusobno nisu povezana nekim relacijama.** Od momenta objavljivanja, po ranijim zakonima SAD i V. Britanije, autorska dela su počinjala da uživaju zakonsku zaštitu, dok neobjavljena dela uživaju mnogo manju zaštitu. Tako je dužina pravne zaštite npr. za neobjavljena dela bila 28 godina i ako se zaštita ne bi obnovila delo bi postalo javno dobro. S obzirom da se ovakva diferencijacija između objavljenih i neobjavljenih dela pokazala neadekvatnom to se od 1978. godine u SAD<sup>182</sup> izjednačavaju objavljena i neobjavljena dela<sup>183</sup>.

Neka prava (naše, npr.) ne predviđa da ovaj uslov predstavlja konstitutivni element za sticanje autorskopravne zaštite, međutim, **ono se pojavljuje kao jedno od moralnih prava autora.** Takođe, objavljivane je i **bitni element u zaštiti za neka, zakonom predviđena, dela** (npr. fotografska i dela primenjene umetnosti, računarske programe nastale u radnom odnosu). Za njih pravna zaštita počinje teći<sup>184</sup> ili prestaje<sup>185</sup> od momenta objavljivanja. Pri tome se mora istaći da se pod "**objavljenim delima**"<sup>186</sup> *podrazumeva izdavanje dela sa pristankom autora, bez obzira na način izrade njihovih primeraka, ako je stavljanje na raspolaganje ovih primeraka bilo takvo da zadovoljava potrebe javnosti, vodeći pri tome računa o prirodi dela.* Kad su u pitanju kompjuterski programi za njih autorska imovinska prava, u slučaju da je nosilac tih prava pravno lice, prestaju 50 godina nakon **ostvarivanja programa.** Sam termin "ostvarivanje programa" nije preciziran tako da je to ostavljeno da se tumači analogijom ili sličnim terminima u odgovarajućim međunarodnim aktima. To znači da bi se imovinska prava nad računarskim programom mogla koristiti neophodno je da se **utvrdi početak njegovog ostvarivanja.**

<sup>182</sup> Copyright Act of 1976 (P.L. 94 - 553).

<sup>183</sup> McFarlane G., A Practical Introduction to Copyright, London, Waterlow Publishers, 1989., str. 105 - 115.

<sup>184</sup> Čl. 84. našeg Zakona o autorskom pravu kaže da autorsko imovinsko pravo na fotografsko delo, na delo proizvedeno po sličnom postupku i na delo primenjene umetnosti prestaje po isteku 25 godina po objavljivanju.

<sup>185</sup> Takođe, ako se kao nosilac autorskog imovinskog prava pojavljuje pravno lice njegovo autorsko pravo prestaje po isteku 50 godina po objavljivanju dela.

<sup>186</sup> Bernska konvencija za zaštitu umetničkih i književnih dela, 1886., čl. 3. tč. 3.

Ostavljajući po strani celishodnost i opravdanost ovakvih rešenja vezanih za objavljivanje, odn. ostvarivanje autorskih dela, kao uslov za njihovu pravnu zaštitu, ono što je bitno je da se u međunarodnom autorskom pravu objavljivanje pojavljuje kao jedan od uslova za sticanje ovog prava. Bernska i Univerzalna konvencija o autorskom pravu<sup>187</sup> predviđaju da "objavljena dela državljana svake države ugovornice i dela objavljena prvi put na teritoriji neke takve države uživaju u svakoj drugoj državi ugovornici zaštitu koju ova druga država pruža delima svojih državljana objavljenim prvi put na njenoj sopstvenoj teritoriji, kao i zaštitu specijalno priznatu ovom konvencijom".

**Ispunjenje formalnosti** je uslov koji su, nažalost, napustile mnoge zemlje koje su ga predviđale. Izuzetak su SAD, koji i posle donošenja novog Zakona o autorskom pravu, predviđa formalnosti kao što su: oznaka copyright, depozit, registracija i "klauzula o proizvodnji". Postojanje ovih formalnosti, kao uslova zaštite prava, priznaje i Univerzalna konvencija<sup>188</sup>, ostavljajući mogućnost da se oni unutrašnjim zakonodavstvima predvide.

**Oznaka copyright** postala je opšte poznata oznaka autorskog dela i autorskog prava. Sastavni deo oznake čini navodjenje naznake copyright, copr. ili ©; ime nosioca i godinu prvog izdanja dela, odn njegovog pojavljivanja<sup>189</sup>.

**Depozit** je uveden u autorsko pravo SAD-a da bi se dela, naročito iz književnosti, a, donekle, i nauke, sačuvala u Kongresnoj biblioteci<sup>190</sup>. U stvari autor je dužan da 2 primerka najboljeg izdanja svog dela deponuje u ovu biblioteku i to u roku od 3 meseca od izdavanja. Još 2 primerka autor je dužan da deponuje u Birou za autorsko pravo i to nakon registracije dela. Ukoliko to ne uradi on ne može uživati autorskopravnu zaštitu, niti će imati pravo da podnese tužbu za povredu svog prava. U

<sup>187</sup> Univerzalna konvencija o autorskom pravu, 1952. godina, izmenjena 1971., čl.II.

<sup>188</sup> Univerzalna konvencija, čl. III, tč. 1.

<sup>189</sup> Oznaka copyright je u autorskom pravu SAD značila i nešto više - delo koje se pojavi bez ove oznake pravnu zaštitu uživa 5 godina, ali pod uslovom da su ispunjene formalnosti vezane za depozit i registraciju. Po isteku tih 5 godina delo prelazi u javni domen.

<sup>190</sup> Institucija depozita prvi je put uvedena još 1710. godine Aninim zakonom o autorskom pravu V. Britanije, kojim je predviđeno deponovanje 10 primeraka na univerzitete i biblioteke. Od ovog se uslova kasnije odustalo.

V. Britaniji<sup>191</sup> depozit je predviđen, ne kao uslov za zaštitu autorskih prava, već kao obaveza izdavača<sup>192</sup>. Slično rešenje ima i naše pravo.

**Registracija** je obaveza koju ima autor i sastoji se u prijavljivanju dela nadležnom telu ili organu za autorska prava (u SAD to je Biro za autorska prava) i to u zakonskom roku (3 meseca, npr.) nakon objavljivanja. Ukoliko to ne učini autor neće moći da podnese tužbu za povredu autorskog prava. Registracija, kao i depozit, su uslovi koji su danas sve više napuštaju.

**Klauzula o proizvodnji** predstavljala je obavezu da se delo objavi na domaćoj teritoriji (u. SAD). Ukoliko se to ne učini delo ne uživa autorskopravnu zaštitu. Kako je postojanje ove klauzule predstavljalo ozbiljnu smetnju za priključenje SAD Pariskoj uniji to je ova klauzula bila donekle izmenjena, a Zakonom iz 1976. godine i ukinuta (od 1.VII 1982.).

Pored ovih, neki nacionalni zakoni predviđaju i druge formalnosti kao što su: overene isprave, plaćanje takse, i sl.

#### 3.4.1.2. *Vrste autorskih dela*

Uslovi koje treba da se ispune da bi neka tvorevina ljudskog duha mogla da uživa autorskopravnu zaštitu odnose se na neko od, u zakonu, navedenih dela. Naime, u većini savremenih zakona prihvaćeno je rešenje da se vrsta dela koja uživaju autorskopravnu zaštitu odredjuju "*generalnom klauzulom*" kojom se određuje opšti pojam, definicija autorskog dela i nabrajaju pojedine vrste. Pri tome, ukoliko se delo ne nalazi u okviru nabrojanih i ukoliko nije izričito navedeno da se ne smatra autorskim delom primenom ove klauzule može se smatrati da to jeste. Drugi, redje zastupljen, metod je "*enumeracije*" po kome se taksativno nabrajaju vrste dela, te ukoliko neko delo nije u njih explicite uvršćeno ne može uživati autorskopravnu zaštitu.

<sup>191</sup> McFarlane G., op. cit., str. 11.

<sup>192</sup> Zakon o bibliotekama u Britaniji iz 1972. godine predviđa da izdavač svaku knjigu štampanu u V. Britaniji u roku od mesec dana od štampanja mora da dostavi Britanskom muzeju. Ukoliko to ne učini moraće u toku godine dostaviti kopiju Oksfordskoj Bodleian biblioteci, Univerzitetskoj biblioteci u Kembridžu, Nacionalnoj biblioteci [kotske, Biblioteci Trinity koledža u Dublinu i Nacionalnoj biblioteci u Velsu.

Izražajna forma u kojoj se fizički materijalizuju dela u oblasti književnosti, nauke i umetnosti može biti: **govor, zvuk** ili **slika**, pa, otuda, se najčešće sledeća **dela** smatraju autorskim<sup>193</sup>:

1. **govorna** (pisana - knjige, brošure, kompjuterski programi, članci, usmena - predavanja, govori, i sl.);
2. **audio** (muzička);
3. **vizuelna** (likovna, plastična, filmska, dela arhitekture, fotografska, koreografska i sl.);
4. **audio-vizuelna** (pozorišna, operaska, filmska).

Naravno da se u vreme digitalne tehnologije i primene multimadija razlike medju ovim vrstama dela gube, što predstavlja novi problem za Pravo intelektualne svojine, a posebno za autorskopravnu zaštitu.

#### 3.4.1.3. *Sadržina prava*

Na svoje delo njihov autor ima određena **subjektivna autorska prava**, koja, u suštini, obuhvataju dve vrste ovlašćenja: **ličnopravna, odn. moralna prava autora i imovinskopravna, odn. imovinska (materijalna) prava autora**.

**Moralna prava autora su apsolutna prava koja deluju erga omnes, što znači da je samo autor taj koji može da se stara o svom delu i da zabrani trećim licima da ga koriste ili raspolažu njime.** Mada se čini da apsolutni karakter ovih prava autora biva ograničen kad su u pitanju treća lica (koautori, opšti interes), međjutim, to su strogo određene situacije (zakonom) sa ciljem da se regulišu određene situacije koje mogu nastati (npr. odustajanje od ugovora, uništenje dela od strane samog autora). Pored apsolutnosti, ova prava prati još i **neotudjivost** što znači da se ne mogu prenositi na druge jer imaju za cilj zaštitu ličnosti autora. U većini zemalja kontinentalnog evropskog

<sup>193</sup> U domaćoj i stranoj literaturi postoje razne podele vrsta dela, zavisno od usvojenog kriterijuma. Tako je, npr., S. Marković u Prednacrtu Zakona o autorskim i susednim pravima (1994. god.) pošao od: jezičkih, zvučnih, vizuelnih, zvučno-vizuelnih dela, dok V. Besarović razlikuje: govorna, muzička, kinematografska, dela likovne umetnosti, dela primenjene umetnosti, fotografska, kartografska i plastična dela, narodna književnost i umetnička dela.

prava ova prava traju i po isteku imovinskih prava što znači da su **ona nezastariva**<sup>194</sup>.

**Moralna prava** autora u većini zemalja obuhvataju:

1. pravo *objavljivanja dela*;
2. pravo na *priznanje autorstva*;
3. pravo na *poštovanje nepovredivosti dela i autora*; i
4. pravo *pokajanja*.

**Pravo objavljivanja dela** znači da autor odlučuje da li će se, i u kom obliku, njegovo delo objaviti, prikazati ili na drugi način učiniti dostupnim javnosti. Takodje, autor ima pravo i da promeni mišljenje o objavljivanju svog dela iako je već dao saglasnost, s tim da u određenim slučajevima ima obavezu da naknadi štetu koja nastaje zbog njegovog odustajanja.

**Pravo na priznanje autorstva** je pravo autora da na svoje delo stavi svoje ime (ime i prezime, samo ime ili prezime, pseudonim ili neki simbol ili znak pod kojim je poznat). Autor se može odlučiti da svoje delo ne obeleži svojim imenom i zahtevajući poštovanje anonimnosti. Kako se ovo pravo autora smatra i njegovim duhovnim očinstvom na delu, to se često ono naziva i **pravom paterniteta**.

**Pravo na priznanje autorstva** je složeno i sastoji se, po pravilu, od **tri prava**<sup>195</sup>:

1. **da obeleži** svoje delo i da zahteva od subjekata koji njegovo delo iskorišćavaju da ga obeležavaju njegovim imenom;
2. **da zabrani** zloupotrebu svog imena u bilo koje svrhe;
3. **da se suprotstavi** uzurpiranju i nedopuštenom prisvajanju svog dela.

Poštovanje nepovredivosti dela i autora je suština **prava na zaštitu integriteta**. Kako autor ima pravo da se suprotstavi bilo kom deformisanju ili menjanju

<sup>194</sup> U tom smislu i **Direktiva o harmonizaciji trajanja zaštite autorskih prava i srodnih prava** (Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain rights), Official Journal of European Communities, no. L 290/9., članom 9 propisuje da države članice regulišući moralna prava svojim zakonima mogu predvideti i druge termine od onih u ovoj Direktivi. Naime, po njoj prava autora književnih i umetničkih dela traju za života autora i 70 godina posle smrti računajući od dana kad je delo učinjeno dostupnim javnosti. Dakle, nema razlike u trajanju moralnih i materijalnih prava.

<sup>195</sup> Besarović V., op. cit., str. 255.

svog dela on, takodje, ima pravo i da se suprotstavi svakoj njegovoj upotrebi koja bi mogla da vredja njegovu čast i ugled. Drugim rečima to znači, da i onaj na koga su izvesna prava ugovorom ili na osnovu drugog pravnog osnova preneti, ne može, bez dozvole autora, da delo skraćuje, modifikuje, popravlja, proširuje, ili vrši bilo kakve izmene u delu. Čak i kad je originalno delo<sup>196</sup> preneto u svojinu drugog lica ono mora od autora tražiti saglasnost ako želi da ga menja. Do ograničenja ovog prava može doći pod strogo propisanim uslovima.

**Pravo pokajanja** je pravo autora da povuče delo iz prometa i da izvrši izmene u već objavljenom delu. Pri korišćenju prava na pokajanje autor mora, ukoliko je vlasništvo dela preneo na treća lica, da obešteti korisnika, odn. njegovog vlasnika. U većini zemalja zakoni ne postavljaju nikakve uslove pod kojima, ili zbog kojih, autor može da koristi ovo pravo. Izuzetak je naša zemlja po čijem Zakonu o autorskim pravima<sup>197</sup> autor može da se koristi pravom pokajanja i da delo povuče iz prometa ako korišćenje njegovog dela može naneti štetu njegovom naučnom ili umetničkom ugledu. Pri tome se mora voditi računa da je pravo pokajanja strogo vezano za autora tako da ni jedan drugi nosilac autorskog prava (sleđenik, po zakonu ili ugovoru) nema pravo da povuče delo iz prometa, niti da ga menja.

**Imovinska prava autora** su skup prava koje ima autor povodom svog autorskog dela. U većini zemalja **sadržina imovinskih prava** vezuje se za:

- a) **pravo iskorišćavanja dela;**
- b) **pravo da pusti delo u promet** u obliku i na način za koji smatra odgovarajućim;
- c) **pravo sledjenja;**
- d) **pravo pristupa** primercima dela;
- e) **pravo na naknadu** kada se njegovo delo daje u zakup; i
- f) **pravo na reviziju** ugovorene naknade.

Najsloženije imovinsko pravo je **pravo iskorišćavanja dela** koje čini kompleks prava autora vezanih za:

- **pravo objavljivanja;**
- **pravo preradjivanja;**

<sup>196</sup> Veoma je diskutabilno koja će se kopija smatrati originalnom, odn. da li je original ono što se nalazi u kompjuteru autora, ili kopija na magnetnom, ili na optičkom medijumu, jer su sve kopije identične originalu. Aktuelnost ove dileme proističe iz stanja tehnike i mogućnosti da se ne samo prave bezbrojne kopije, već i da one, zahvaljujući laserskim štampačima, budu potpuno identične, te je gotovo nemoguće utvrditi njihovu izvornost.

<sup>197</sup> Zakon o autorskom pravu, čl. 30.

- *pravo reprodukovanja;*
- *pravo umnožavanja;*
- *pravo obradivanja;*
- *pravo prikazivanja;*
- *pravo izvodjenja;*
- *pravo prenošenja;* i
- *pravo prevodjenja.*

Osnovni princip je da samo autor ima pravo raspolaganja svojim delom, a sva ostala lica delo mogu iskorišćavati samo uz njegovu dozvolu. **Davanje saglasnosti za iskorišćavanje dela je autorizacija.** Autorizacija je neotudjivo pravo autora da odluči u kom obliku će se njegovo delo iskorišćavati. Postoje različiti načini iskorišćavanja dela<sup>198</sup>, što zavisi od niza okolnosti kao što su: priroda i vrsta dela, opšti napredak nekog društva i njegove potrebe, razvoj tehnologije, razvoj medija i sl. Tako, kad su u pitanju računarski programi postoje različiti načini na koje autori mogu svoje programe iskorišćavati. U informaciono razvijenim zemljama oni se nalaze na optičkim diskovima, a kod nas još uvek su najčešće u pitanju magnetni mediji (diskovi, diskete, a ne retko i magnetne trake). Autoru kad nas, otuda, nije celishodan izbor optičkog diska kao medija ukoliko želi iskorišćavanje svog programa jer takvom tehnologijom raspolaže manji broj korisnika. Isto tako, do skora nismo imali masovno korišćenje programa, pa i smeštanje programa na medije koji to omogućuju nije bilo preporučljivo. Slična situacija očekuje i programe koji bi od autora mogli biti proglašeni za *public domain* (*public domain* - javno vlasništvo su programi koje autor proglasi javnim dobrom u cilju masovnog korišćenja, bez naknade i daljih prava autora da njima raspolažu), što je moguće u informaciono razvijenim zemljama. Kod nas takav izbor autora smatrao bi se bezumnim, pa sigurno da ovaj način nije za sada u opciji. Ono što je, takodje, bitno je da pravo iskorišćavanja dela pretpostavlja i **pravo autora da dobije naknadu** ukoliko njegovo delo, uz njegovu saglasnost, iskorišćava neko drugo lice. Izuzetak je ako se autor odrekne naknade predviđajući to u ugovoru. Kad su u pitanju računarski programi autor se naknade može odreći ukoliko program proglasi za javno vlasništvo ili ukoliko ih proglasi *shareware* programima (programi deonice, udeli). *Shareware* programi se distribuiraju besplatno. Medjutim, njihovo korišćenje nije besplatno nakon isteka određenog vremena (po pravilu, rok je 20 do 40 dana). Znači, autor se odriče naknade za korišćenje ovakvog programa za izvesan period. U tom periodu korisnik može program iskorišćavati do "besvesti", a da ne plati naknadu. Po pravilu, programi su sa ugrađenom zaštitom, kao i serijskim brojem, te ukoliko se kopije pojave na tržištu lako se može otkriti ko je te neautorizovane radnje dozvolio ili sam počinio. Postojanje ovih tipova programa kod nas još nije postala svakodnevna praksa, pa, čak, ako se i pojavljuju pojedinačni slučajevi oni brzo bivaju zloupotrebljeni,

<sup>198</sup> Besarović V., op. cit., str. 259.

čime se potvrđuje konstatacija da izbor različitih načina iskorišćavanja dela umnogome zavisi od stepena razvijenosti zemlje. Otuda se ostali izuzeci od prava autora na naknadu za iskorišćavanje dela taksativno navode u odredbama odgovarajućih propisa (npr. naš Zakon o autorskom pravu predviđa ograničenje prava iskorišćavanja autorskog dela kad je u pitanju opšti interes).

**Pravo da pusti delo u promet u obliku i na način za koji smatra odgovarajućim** je pravo autora koje znači njegovu slobodu da odredi vremensko trajanje korišćenja autorskog dela od strane drugih lica, kao i imovinske koristi koje iz ovog prometa proizlaze. Mada ovo pravo mnogim pravima (npr. našim) nije izričito predviđeno ono ipak proističe iz drugih moralnih i imovinskih prava. S obzirom na prirodu računarskih programa ovo pravo postaje veoma bitno jer autoru omogućuje da izabere ne samo koju verziju programa će pustiti u promet, nego i način na koji će to uraditi.<sup>199</sup> To će legalizovati njegov izbor da ne stavi u promet izvorni kod, kao i stavljanje autorskih bagova, koji inače ne remete rad programa, a kojima se lakše može dokazivati autorstvo. Takođe, ono će naročito značajno postati u primeni "*doktrine prve prodaje*" (*first sale doctrine*) ako se autor opredeli za *shrink-wrap* ("zamotanu") licencu koja će obavezivati svakog onog ko je otvaranjem omotača na medijumu i skidanjem markera označio nameru da koristi program i time sebe obavezao na poštovanje restrikcije u kopiranju, korišćenju ili prepravci<sup>200</sup>. Iako relativno nova, ova se licenca sve više nalazi u upotrebi, tim više, što nosi veoma velike pogodnosti za nosioca (izostajanje garancija i obaveza, npr.), ali i za korisnika (motivacija za povećanjem ovih licenci svakodnevno se dopunjuje novim pogodnostima tipa: unapredjene verzije se daju za znatno manju cenu; pomoć se brzo i efikasno pruža, čak i telefonom; daju se pokloni za one koji nazad pošalju svoje registracione kartice, i sl.)<sup>201</sup>.

**Pravo sledjenja**<sup>202</sup> je pravo koje do sada nije bivalo priznavano autorima kompjuterskih programa. Ono bi, u suštini, značilo pravo autora jednog originalnog izvornog koda<sup>203</sup> da može, za vreme trajanja autorskopravne zaštite, zahtevati da mu se ustupi jedan deo dobiti koju je ostvario prvi vlasnik ili korisnik daljom prodajom

<sup>199</sup> U teoriji i praksi postavilo se pitanje tumačenja i tretmana primeraka računarskih programa. Naime, bila je dilema da li se pod primerkom istog programa u izvornom kodu mogu smatrati i materijalni nosioci programa u objektnom kodu.

<sup>200</sup> Lipner S., Kalman S., op. cit., str. 427.

<sup>201</sup> Pearson E. H., White A., Recent Developments In Computer Law in the US, edicija: Essays of Computer Law, Melbourne, Longman Professional, 1990., str. 234 - 237.

<sup>202</sup> Čl. 14. ter Bernske konvencije, predviđa ovo pravo za autore originalnih dela likovne umetnosti i autore izvornih rukopisa književnih, naučnih i muzičkih dela.

<sup>203</sup> Primedba M. D.

(preprodajom) dela drugim licima<sup>204</sup>. To znači da se ovim pravom obezbeđuje autor da bude informisan da novi vlasnik raspolaže njegovim delom. Pored prava da bude obavešten o novom vlasniku, autor, pri postojanju prava sledjenja, ima i pravo da od prodavca dobije procenat od prodajne cene.

**Pravo pristupa primercima dela** je jedno od novijih prava koja priznaju nacionalni zakoni pojedinih zemalja (npr. Zakon o autorskom pravu Nemačke) i koje se sastoji u pravu autora da od držaoca njegovog dela (originala ili reprodukcije) može zahtevati da mu dozvoli pristup delu ako mu je potrebno za reprodukovanje ili obradu i to onda kada time ne ometa držaočeve zakonske interese<sup>205</sup>. Ovo pravo je od posebnog značaja za računarske programe jer omogućuje autoru da pristupi svom programu i tako istovremeno izvrši kontrolu nad korišćenjem i eventualnim prepravkama koje su bez njegovog znanja nastale. Međutim, ono je isto tako i veoma problematično ukoliko se njime krši ili ugrožava pravo na privatnost sopstvenika ili korisnika.

**Pravo autora na naknadu kada se njegovo delo daje u zakup** je, takodje, predviđeno prvi put u nemačkom Zakonu o autorskom pravu, i ima za cilj da spreči bogaćenje zakupoprirnca koji delo dobijeno u zakup daje ili ustupa nekom trećem licu i iz toga dobija neku korist komercijalne prirode. Ovo se pravo, u novije vreme, proširuje i na slučajeve kada su reprodukcije učinjene pristupačnim javnosti. Za oba oblika ovog prava autor ima pravo na naknadu "*tantijeme za iznajmljivanje*"<sup>206</sup>. S obzirom da su računarski programi upravo ona autorska dela koja se često daju u zakup, to priznavanjem postojanja ovog prava predstavlja i osnovu za korišćenje tantijema, kao i kontrolu kopija (reprodukcija) koje je zakupoprirnac dostavljao trećim licima. Upravo su od toga pošle i odredbe Direktive za pravnu zaštitu kompjuterskih programa EU-a i Sporazuma o trgovinskim aspektima prava intelektualne svojine GATT-a kojima je data mogućnost da autor i njegovi naslednici dozvole ili zabrane vlasniku programa da primerke programa daje u komercijalno iznajmljivanje javnosti (zakup), ukoliko se vlasnik time bavi kao poslovnom aktivnošću. Naravno, ovo se neće odnositi na one programe koji nisu osnovni predmet zakupa<sup>207</sup>.

**Pravo na reviziju ugovorene naknade** je pravo koje štiti autora u slučaju kada se ustanovi da je ustupanjem prava iskorišćavanja znatno oštećen (ovo pravo predviđa i naš Zakon o autorskom pravu). Kad se ustanovi da je prihod koji ima autor toliko nesrazmeran prihodu koji se ostvaruje korišćenjem dela autor može da zahteva da

<sup>204</sup> Besarović V., op. cit., str. 264.

<sup>205</sup> Besarović V., op. cit., str. 265.

<sup>206</sup> Besarović V., op. cit., str. 265.

<sup>207</sup> Slično rešenje je prihvaćeno i u čl. 29., Prednacrta.

se ugovor izmeni i kako bi bio povoljniji za njega<sup>208</sup>. I ovo pravo može imati velikog značaja za autore računarskih programa, naročito u situacijama kad je naknada koju dobijaju za iskorišćavanje bila izuzetno mala. To se često dešava studentima autorima programa, koji pod lošim okolnostima zaključuju ugovore sa softverskim firmama, bilo zbog želje da zarade bilo kakvu sumu ili zbog težnje da ih naknadno, posle završavanja studija, ove firme zaposle. Ne retko se dešava da studenti, ili mladi programeri, zbog prestiža budzašto ustupe svoje programe, pa naknadno ustanove da su se prevarili i bili oštećeni. Međutim, ni za druge kategorije autora kompjuterskih programa ovo pravo nije nerelevantno.

#### *3.4.1.4. Lica koja uživaju zaštitu*

Autorskopravnu zaštitu, po većini nacionalnih zakona, uživaju prevashodno ona **lica koja imaju status autora**. Osim njih ovu zaštitu mogu uživati i još neka lica, kao što su: **koautori i nosioci autorskog prava**. Dok su autor i koautori izvorni nosioci autorskih prava, dotle su nosioci autorskog prava lica na koje je autor preneo deo svojih ovlašćenja (prava).

**Autor je ono fizičko lice koje je odredjenu duhovnu tvorevinu, koja ispunjava zakonom predviđene uslove da bude autorsko delo, stvorilo.** Kako se pod autorskim delom smatraju tvorevine ljudskog duha iz oblasti književnosti, nauke, umetnosti i drugih oblasti stvaralaštva to će svako delo morati zadovoljiti ovaj uslov, kao i uslove vezane za originalnost i formu. Da li je delo u potpunosti završeno, ili ne, nije relevantno da bi njegov tvorac uživao ovu zaštitu, jer autorsko pravo autor stiće aktom stvaranja, a ne završavanja, dela. Čak nije ni bitno da li lice, odn. lica koja se mogu smatrati autorom, ima poslovnu sposobnost (kao što su maloletnici ili duševno bolesna lica). Takodje, nije bitno da li je neko lice koje se smatra autorom dalo izjavu volje da želi da to bude ili ne.

Ono što jeste bitno je, a što se u većini zakona<sup>209</sup> prihvata, da se **autorom smatra ono lice čije je ime i prezime ili pseudonim na delu naznačeno**<sup>210</sup>. To znači da autor može odlučiti da li će na svoje delo staviti puno ime i prezime, ili pseudonim (jedan ili više), ili neće, čak, staviti ništa. U slučajevima kada su u pitanju dela sa pseudonimom ili anonimna dela, autorska prava štiti ili ostvaruje izdavač koji se

<sup>208</sup> Besarović V., op. cit., str. 266.

<sup>209</sup> U skladu sa čl. 15. st.1. Bernske konvencije.

<sup>210</sup> Zakon o autorskom pravu, čl. 8., st.2.

pojavljuje kao pretpostavljeni autor dok se suprotno ne dokaže, ili dok se autor ili njegovi nasljednici ne pojave i počnu da se staraju o autorskim pravima<sup>211</sup>.

Pod autorom smatra se i fizičko lice koje je stvorilo zbirke autorskih dela (npr. skup programa i podprograma), kao i autori prevoda ili prilagodjenog, obradjenog ili na drugi način preradjenog, dela. Pri tome, važno je da se autorska prava autora izvornog dela ne smeju povrediti.

**Koautori su sva ona lica koja su učestvovala u intelektualnom stvaranju dela i čiji je doprinos kreativan.** Mnoga prava prihvataju ideju o nedeljivosti autorskog prava svih onih lica koja su saradnjom stvorila neko autorsko delo. Udeo svakog koautora utvrđuje se srazmerno stvarnom doprinosu ukoliko njihov odnos nije ugovorom drugačije određen.

**Nosioci autorskog prava**, u teoriji, nacionalnim i međunarodnim normama, **su, fizička i pravna, lica na koje se, putem ugovora, zakona i nasledjivanja, prenose određena autorska prava.** Po pravilu, prenose se imovinska prava.

Ukoliko je autorsko delo nastalo **u radnom odnosu**, kad je zaposleni izvršavao svoje radne obaveze, onda se **organizacija**, odn. poslodavac pojavljuje kao nosilac autorskih prava za određeno vreme (kod nas pet godina) i to bez traženja dozvole od autora. Autoru i dalje pripadaju moralna prava (navodjenje imena, npr.) i određena materijalna (pravo na naknadu, npr.).

Ako je autorsko delo stvoreno **po narudžbini**, onda je nosilac imovinskih autorskih prava **naručilac**, ukoliko se drugačije u ugovoru ne odredi. Moralna prava i dalje ostaju autoru.

Kad se radi o prenošenju autorskih prava po osnovu nasledjivanja onda **naslednicima**, kao nosiocima, pripadaju sva autorska prava u određenom vremenu trajanja nakon smrti autora. Od moralnih prava, ukoliko nije testamentom drugačije određeno, naslednicima pripada pravo da zahtevaju da se na delu označi autor, da se usprotive svakom deformisanju dela, njegovom skraćivanju ili menjanju. Pored toga, oni imaju pravo i da spreče svako korišćenje dela kojim bi se ugrozio ugled i čast autora.

---

<sup>211</sup> čl 15. st. 3. Bernske konvencije.

### 3.4.1.5. Trajanje

Dužina trajanje autorskih prava vezana je za njihovu vrstu i prirodu. **Moralna prava nemaju rok trajanja**, dok se za **imovinska najčešće predviđa odredjenje "za života autora"** ili od objavljivanja ili nastanka, **i određeni period nakon smrti**. Taj period je, zavisno od nacionalnog prava, od 15 (npr. bivšem SSSR) do 80 (Kolumbija) godina, mada je u najvećem broju zemalja to 50 godina (25 za određena dela) nakon smrti autora. Situacija je nešto promenjena donošenjem Direktive o hatmonizaciji trajanja autorskog prava i srodnih prava po kojoj je rok 70 godina. Nakon isteka tih rokova dela postaju **slobodna, odn. javno dobro**, te se mogu bez dozvole i naknade koristiti, pa, čak, i preradjivati, umnožavati. Neka prava predviđaju plaćanje posebnih naknada i za dela kojima je protekla pravna zaštita (domain public payment).

### 3.4.2. Kompjuterski programi i nacionalni propisi autorskopravne zaštite

U traženju rešenja za obezbedjenje pravne sigurnosti kompjuterskih programa jedno od mogućih i, za sada, najčešćih je autorskopravna zaštita. Računa se da je sudska praksa SAD bila pramajka ove zaštite i da se pojavljivanje autorskopravne zaštite računarskih programa vezuje za rane 60te. Doduše, povod je bio "problematični" zahtev za registraciju objektnog koda računarskog programa korporacije *North American Aviation Inc.*, 1961. godine. Problematičnost je prouzrokovana teškoćom njegovog tretmana kao pisanog dela. Biro za autorska prava SAD 1964. godine prihvata da registruje prvi računarski program, ali kao literarno delo. Bila je to godina koja se računa kao godina njihovog prvog podvodjenja pod autorska dela<sup>212</sup>. Mada je bilo za očekivati da će u SAD biti donet i prvi propis, to nije bilo tako. Na dalekim, malim, i gotovo beznačajnim **Filipinima 1972.** godine donosi se **Dekret o zaštiti intelektualne svojine** po kome se kompjuterskim programima izričito priznaje autorskopravna zaštita. U SAD u to vreme i dalje traju, često i vrlo burne, rasprave da li se programi uopšte mogu zaštititi autorskim pravom, da li se mogu registrovati i deponovati kod Biroa za autorska prava, kao i kako zaštititi neobjavljene programe. Naime, u SAD je sve do 1976. godine važio Zakon o autorskom pravu (*Copyright Act*)<sup>213</sup> iz 1909. godine

<sup>212</sup> Marković S., op. cit., str. 95 i 96; Bernacchi R., Frank P., Statland N., op. cit., str. 3.36.

<sup>213</sup> Etimološko značenje termina **copyright** vezano je za ovlašćenje za umnožavanje (*copy*) odn. reprodukovanje ili autorizaciju drugima da reprodukuju neko autorsko delo, da bi se danas ovaj termin odnosio na sva ekskluzivna autorskopravna ovlašćenja koja se priznaju autoru.

koji je nastavilo sa uobičajenim dualizmom autorskopavnog sistema - s jedne strane Common law je važio za autorska dela koja nisu bila objavljena, a paralelno je važio i Zakon za objavljena dela. S druge strane, iako je predviđao zakonsku zaštitu za objavljena dela, ovaj Zakon je bio vrlo tolerantan u odnosu na neobjavljena. Kako se zaštita rukopisima, kao neobjavljenim delima, pružala primenom Common Law to je bilo za očekivanje da će se programi teško moći svrstati pod rukopise. No, Zakon nije bio rigorozan, pojam rukopisa fleksibilno se shvatao, te je bilo moguće zaštititi i neobjavljene programe<sup>214</sup>. **Ono što je od krucijalne važnosti je da su se programi svrstali u autorska dela, i to kao knjige.** Ovo jeste bilo važno jer su se pojavile sumnje kako ih je moguće registrovati s obzirom da su bili "čitljivi" samo za mašine, a pri registraciji je trebalo ne samo utvrditi njihovu originalnost, već ih i deponovati u Birou i Kongresnoj biblioteci? Drugo sporno pitanje bilo je da li su programi pisani od autora s obzirom da su unošeni u mašinu i jedino razumljivi ukoliko bi se sa mašine čitali? Poseban problem se pojavio kod tumačenja oblika u kom je potrebno da bude program učinjen dostupnim javnosti da bi se taj oblik mogao smatrati javnim objavljivanjem, pošto je javno objavljivanje bilo jedan od uslova po kom se računao početak trajanja zaštite. Takođe, poseban problem je bio kako zadovoljiti zahtev o upozoravajućoj napomeni (oznaci) jer je njeno stavljanje praćeno drugim podacima (godina objavljivanja, upozorenja da se ne sme reprodukovati i sl.) predstavljalo jedan od uslova za uživanje autorskopravne zaštite, a što je bilo moguće na dva načina: **a)** u okviru samih mašinski čitljivih kodova, ali nedostupnih ostalima sem autoru i malobrojnim znalcima, ili **b)** pojavom na ekranu, što nije smatrano kao dovoljno opšte upozoravajuće<sup>215</sup>. Svi su se ovi problemi rešavali u hodu i mahom zahvaljujući dobroj volji sudskih i ostalih institucija.

Kolike su to bile muke može se videti iz slučaja *Data Cash Systems, INC. v. JS&AGroup, INC.* iz 1979. godine. Tužitelj je smatrao da postoji kršenje autorskih prava i nelojalna konkurencija od strane tužene korporacije i njenih zaposlenih. Dela su učinjena reprodukovanjem, uvozom, distribucijom, prodajom, propagandom. Naime, kompanija *Data Cash Systems INC.* je naručila od *D. B. Goodrich and Associates* dizajn i razvoj računarskog programa za kompjuterizovanu igru šaha, *CompuChess*, koju je tužitelj proizveo i prodao. Od septembra 1976. do aprila 1977. *D. B. Goodrich and Associates* dizajnirala je i razvijala osnovne instrukcije koje su bile naredbe računaru kako da igra šah i to na 6 nivoa složenosti i težine. Instrukcije su bile prevedene u programski jezik, source program je bio preveden na mašinski jezik, asemblerski program je potom korišćen za kreiranje objekta programa u ROM-u. ROM je instaliran u računaru. *CompuChess* je koristio tastaturu i uređaj za prikaz podataka za unose i izlaze

<sup>214</sup> Scott M., op. cit., str. 3-6.

<sup>215</sup> Scott M., op. cit., str. 3-8.

informacija. Igrač je unosio određeni potez pritiskanjem određene tipke na tastaturi i dobijao na ekranu prikazan broj i alfabetski znak za potez koji je odigrala mašina.

Pri kraju 1977. godine tužitelj je počeo prodaju programa. Na ROM-u, samom programu, pakovanju ili pripadajućoj dokumentaciji nije bilo oznake autorstva. Oznaka autorstva pojavljivala se na izvornom programu i svakoj kopiji. U novembru 1978. izvorni program je unet u Autorskopravni Registar, a krajem istog meseca izdata je potvrda o registraciji tužitelju. Na kraju 1978. godine tuženi je počeo prodaju *JS&A Chess* računara. ROM ove mašine bio je identičan sa ROM-om tužiteljevog *CompuChess*. Početkom 1979. godine *Data Cash Systems, INC.* je podneo tužbu za kršenje autorskih prava i nelojalnu utakmicu. I pored uočljive identičnosti ROM-ova sud je posumnjao da je bilo direktnog kopiranja tužiteljevog ROM-a. Čak je na osnovu neospornih činjenica dokazano je da je tuženi *JS&A* poštovao tužiteljeve zahteve u odnosu na autorska prava (pojava oznake autorstva na kopijama i izvornom programu). Takođe, sud je smatrao da bi postojalo kopiranje nekog kompjuterskog programa kopija se mora videti i pročitati. Mora biti u čoveku čitljivom obliku. Što se tiče problema sa ROM-om, primenjena je analogija sa slučajem međjusobnog odnosa između arhitektonskog plana i izgrađene zgrade. Zgrada je rezultat plana, a ne njegova kopija. Ukoliko je u ROM ugrađen program onda on nije kopija programa. Dakle, po mišljenju suda nije postojalo kopiranje tužiteljevog računarskog programa u ROM-u tuženog, tako da je zahtev odbijen<sup>216</sup>.

Dalja ponudjena rešenja suštinski su polazila od toga da se računarski programi mogu tretirati kao publikacije. Ukoliko su bili objavljeni sa, zakonom zahtevanom, oznakom (*copyright*, sva prava pridržana i sl.) bili su zaštićeni zakonskim autorskim pravom, i uživali svu zaštitu od momenta "objavljivanja". Ako nisu imali odgovarajuću oznaku autorstva tretirani su kao opšte dobro.

Pošto je bilo sve više zahteva da se Zakon iz 1909. menja, između ostalog i zbog promena koje su usledile kompjuterskom revolucijom, to je u oktobru 1976. godine predsednik Ford potpisao **Zakon o autorskom pravu** (*Copyright Act*) koji je značio generalnu reviziju autorskog prava. Kako su neke od promena zahtevale izvesne pripreme Zakon je stupio na snagu tek 1978. godine. Zanimljivo je da se tek ovim Zakonom među autorska dela uključuju i književna. Istovremeno je propušteno da se kao posebna kategorija autorskih dela uvedu i računarski programi. **Zato je uvršćivanjem književnih u autorska dela utoliko značajnije što su se i programi podvodili pod njih.** Ovakav pravni tretman programa, verovatno, je bio posledica stava koji je zauzela posebna Komisija Kongresa.

<sup>216</sup> Lipner S., Kalman S., op. cit., str. 5 - 7.

Naime, 1974. godine Kongres je osnovao **Nacionalnu komisiju za nova tehnološka korišćenja autorskih dela** (*National Commission on New Technological Use of Copyrighted Work*) čiji je zadatak bio da prikupi podatke i prouči korišćenje računara i pripremi preporuke na osnovu kojih će Kongres moći da se odluči o daljoj promeni u autorskom pravu, kako bi se na adekvatniji način priznali i zaštitili programi i uskladili opšti interesi sa interesima tvoraca. To se odnosilo, takodje, i na softver i baze podataka. Pored ovih trebalo je rešiti i druge probleme. Komisija je tek 1978. godine objavila svoj konačni Izveštaj.

Polazna osnova Izveštaja bila je da su kompjuterski programi originalna autorska dela i da kao takva treba da uživaju autorskopravnu zaštitu. Mada drugačije prirode nego što su to gramofonske ploče, filmovi ili videotrake, programi su ipak originalno koncipirani, distribuirani i napisani kao serija instrukcija i kad su materijalizovani niko ne može reći da su književna dela<sup>217</sup>. Međutim, to ne znači da se oni ne mogu i ne treba da zaštite autorskim pravom, ali kao posebna autorska dela.

Pod uticajem nalaza ove Komisije, a i sve većem uključenjem pravnika koji podržavaju ideju o autorskopravnoj zaštiti računarskih programa, predsednik Karter je decembra 1980. godine potpisao amandman poznat kao **Zakon o autorskopravnoj zaštiti kompjuterskog softvera** (*The Computer Software Copyright Act*) kojim se obezbedila posebna autorskopravna zaštita **kompjuterskim programima i to kao književnim delima**. Ovim su zakonom (odn. amandmanom) definisani i računarski program. Definisanje kompjuterskih programa nije istovremeno rešilo i dileme koje su se u vezi sa njima pojavile. Između ostalog, to je bio i problem objektnog koda, teške primenljivosti "doktrine prve prodaje" i sl., zbog čega su pokretani mnogi sudski sporovi. Jedan od prvih takvih sporova<sup>218</sup> koji će biti okvalifikovan kao vesnik novog talasa započet je, u stvari, nizom sporova između *Apple Computer INC. v. Franklin Computer Corporation* (1982. godine i 1983.) u kojima su se, u početku, iskristalisana sledeća rešenja: **a) autorsko pravo ne zaštićuje objektni kod** za razliku od izvornog koda, pošto delo koje se zaštićuje nije lako "uočljivo" i "čitljivo", što je upravo slučaj sa objektnim kodom; **b) autorskopravna zaštita ne može se primeniti za zaštitu softvera ugrađenog u ROM**, jer ROM je deo mašine više nego što je autorsko delo; **c) autorskopravnom zaštitom ne mogu se zaštititi programi operativnog sistema** za razliku od aplikativnih programa koji su eksterni, van mašine, i koje može videti i korisnik. Programi operativnog sistema su procesi, sistem ili metod operacija koje se mogu zaštititi patentom, a ne autorskim pravom. Naime, *Apple* je tužio firmu *Franklin Computers* za korišćenje, prodaju i kršenje *Apple*-ih registrovanih autorskopravno zaštićenih 14 kompjuterskih programa

<sup>217</sup> Scott M., op. cit., str. 3-13.

<sup>218</sup> Bernacchi R., Frank P., Statland N., op. cit., str. 3.38.

koji su pratili prodaju kompjutera *Apple II*. *Franklin Computers* je napravio kompjuter *ACE 100*. Pri tome, nije bilo ni nerelevantno da je *Apple*, Kalifornijska firma, te 1982. godine predstavljala vodeću firmu za PC, zapošljavala 3.000 ljudi, prodala oko 400.000 kompjutera i u toj fiskalnoj godini imala promet od \$350.000.000. Druga firma je iz Pensilvanije, osnovana 1981. godine, sa 75 zaposlenih i sa manje od 1.000 prodatih računara. Obe firme su u svoje računare ugradile "osnovnu ploču" na kojoj se nalazio veći broj čipova. Neki od čipovi su skaldištili informacije u RAM-u, a ostali u ROM-u. *Franklin* je "dizajnirao" kompjuter kompatibilan *Apple*-u. To je značilo da je većina softvera pisana za *Apple* bila istovremeno pogodna i za *ACE*. *Apple* je smatrao da je *Franklin* "ukrao" logiku i strukturu njihovog sistema. Tuženi se branio da nije kreirao mašinu kompatibilnu *Apple*-u, već kompatibilan softver. Sudu je prezentirano 14 *Apple*-ih programa koji su predstavljali deo *Apple*-og operativnog sistema (npr. *Autostart ROM*, *Applesoft*, *DOS*). Tužba se pozivala na sledeće: operativni sistem je izražajna forma, ne ideja ili proces, ukoliko je u ROM-u ili na floppy disku, objektni kod ili objektni program je oblik izražavanja forme i delo za koje se može utvrdjivati autorstvo (on je, u suštini, "jezik" mašine i nije napravljen da bi ga čitali ljudi, kao što i nije izvedeno delp izvornog koda), ROM je samo medijum za izražavanje forme, a ne mehanički uređaj. Sud je smatrao da je tuženi napravio gotovo savršeno kompatibilan softver i doneo odluku sa već spomenutim obrazloženjem<sup>219</sup>. Drugostepeni sud je smatrao: **a) da je kompjuterski program, bilo u objektnom bilo u izvornom kodu, literarno delo** i zato može biti zaštićen od nedozvoljenog kopiranja; **b) kompjuterski program u objektnom kodu, koji se nalazi na ROM-u je autorsko delo** te uživa autorskopravnu zaštitu; **c) kompjuterski programi operativnog sistema nisu sami po sebi isključeni iz autorskopravne zaštite**; i **d) ugroženost investicija nosilaca autorskih prava i konkurentska pozicija** koju je izazvalo konkurentsko kopiranje velikog broja ključnih programa nosioca autorskih prava **predstavlja nenadoknadivu štetu i povlači donošenje sudskog naloga**. Na osnovu ovih zaključaka drugosepeni sud je prethodnu prvostepenu odluku preinačio. U kasnijem sporu u odbrani *Franklin Computers* se pozvao na sudsku presudu donetu tri dana posle one prve, u kojoj su se primenile odredbe amandmana iz 1980. godine.

No, i pored svih mana (posebno mu je pripisivana nejasnost u definisanju kompjuterskog programa) ovaj amandman je imao veliki uticaj na druge zemlje da izmene svoje postojeće ili donesu nove zakone o autorskom pravu u koje su unele i zaštitu kompjuterskih programa (negde i softvera)<sup>220</sup>. Tako, hronološki posmatrano, npr. donose se:

#### *Hronologija nacionalnih aktivnosti*

<sup>219</sup> Lipner S., Kalman S., op. cit., str. 30.

<sup>220</sup> Fisher N., Intellectual Property Rights on the Internet (Political Topic for Succession), may 1996, preuzeto sa Interneta.

| Godina | Država          | Akt   |
|--------|-----------------|---|
| 1983.  | Madjarska       | Dekret o izmenama i dopunama Zakona o autorskom pravu   |
| 1984.  | Australija      | Amandman Zakon o autorskom pravu  |
| 1985.  | SR Nemačka      | Amandmani na Zakon o autorskom pravu  |
| 1985.  | Japan           | Revizija Zakona o autorskom pravu   |
| 1985.  | Tajvan          | Izmena Zakona o autorskom pravu   |
| 1985.  | Francuska       | Julski Zakon o autorskim pravima i pravima izvodjača, proizvođača fonograma i videograma i preduzeća za audio-vizuelnu komunikaciju |
| 1985.  | Bugarska        | Podzakonski akt o ustanovljavanju posebne zaštite softvera  |
| 1985.  | V. Britanija    | Amandman Zakona o autorskom pravu (kompjuterskog softvera)  |
| 1987.  | Malezija        | Zakon o autorskom pravu   |
| 1987.  | J. Koreja       | Zakon o zaštiti računarskih programa  |
| 1987.  | Brazil          | Zakon br. 7646/87   |
| 1988.  | V. Britanija    | Zakona o autorskom pravu, dizajnu i patentu   |
| 1988.  | Kanada          | Nacrt Zakona C60  |
| 1989.  | Danska          | Novela Zakona o autorskom pravu   |
| 1990.  | Češkoslovačka   | Amandman na Zakon o autorskom pravu (odvajanjem ostao je da važi za obe zemlje)   |
| 1990.  | SFR Jugoslavija | Zakon o dopunama i izmenama Zakona o autorskom pravu  |
| 1993.  | Bugarska        | Zakon o autorskim pravima   |
| 1994.  | Egipat          | Zakon br. 354/54 o autorskom pravu  |
| 1994.  | Rumunija        | Nacrt zakona o autorskom pravu  |
| 1994.  | SR Jugoslavija  | Prednacrt Zakona o autorskom pravu i susednim pravima   |
| 1995.  | SR Jugoslavija  | Prednacrt Zakona o autorskom pravu i srodnim pravima  |
| 1996.  | SR Jugoslavija  | Predlog Zakona o autorskom pravu i srodnim pravima  |

Ako se pored vremena kad je došlo do izmena ili donošenja novih zakona o autorskom pravu u mnogim zemljama<sup>221</sup>, posmatraju i rešenja koja su za računarske programe u njima usvojena, može su konstatovati da uglavnom postoje određene grupe zemalja sa **sledećim rešenjima**:

1. grupa zemalja koje računarske programe podvode pod **literarna dela**;
2. grupa zemalja koje računarske programe predviđaju kao **posebna autorska dela**;
3. grupa zemalja koje računarske programe podvode **kao prevode ili druga autorska dela**;
4. zemlje koje računarske programe svrstavaju u **naučno - tehničke prilaze**;

<sup>221</sup> Tako je 1994. godine u Luksemburgu održana konferencija u okviru EU COPERNICUS Program: Property Rights in Central and Eastern Europe, na kojoj su razmatrana pitanja vezana za ovu zaštitu u Rumuniji, Rusiji, Poljskoj, Češkoj, Slovačkoj, Sloveniji, Bugarskoj, Madjarskoj, materijal preuzet sa Interneta.

**5. zemlje u kojima se kompjuterskim programima priznaje autorskopravna zaštita, ali u sudskim sporovima, a ne u propisima<sup>222</sup>.**

Od ovih pet solucija može se reći da je **najzastupljenija ona koja računarske programe svrstava u književna dela.**

Ako bi se analizirala rešenja koja postoje u nacionalnim pravima zemalja koje su pravno zaštitile računarske programe kao autorska dela **može se zaključiti sledeće:**

**Prvo. Veliki broj zemalja,** prevashodno informaciono razvijenih, a sve više i nerazvijenih, **ubrzano preduzima niz akcija u rešavanju problema pravne zaštite uglavnom kompjuterskih programa, a u manjem obimu i softvera.** Većina se opredelila za noveliranje postojećih zakona o autorskom pravu priznavanjem programa "svojestvo" predmeta autorskopravne zaštite. Jedan broj zemalja, za sada vrlo mali, doneo je posebne zakone i izvršio reviziju autorskog prava u želji da uključi računarske programe u posebna autorska dela i da im obezbedi posebne, specifične, oblike i režime autorskopravne zaštite. Takodje, postoje i zemlje, čiji je broj, srećom, svakim danom sve manji, koje su potpuno ignorisale postojanje potrebe za zaštitom programa, kao i posebna grupacija zemalja koje su se oslonile na sudsku praksu u okviru koje su priznale autorskopravnu zaštitu, ali je još nisu i pravnim propisima regulisale. Ovakvo stanje posledica je uticaja raznih činioca, potreba i težnji. Nesumnjivo je najznačajnija potreba vezana za razvoj softverske industrije i zainteresovanost država za taj razvoj. Ništa manje značajana nije ni želja nekih država da sačuvaju ili postignu poseban status u međunarodnoj trgovini ovim proizvodima. Oba ova razloga, a i mnogi drugi, doveli su do prava kojim je trebalo obezbediti regulisanje i sankcionisanje ovih pretenzija - što se manifestovalo i u uključivanju problema zaštite programa u pravne instrumente.

**Drugo. Rešenje koje je najčešće prihvatano u regulisanju kompjuterskog programa, kao autorskog dela, je njegovo podvodenje pod književna dela i primena modificovanih pravila koja se predviđaju za njihovu autorskopravnu zaštitu.** Ovo je i najkomfortnije rešenje jer ne izaziva velike promene u postojećim pravnim sistemima. Mada opterećeno nizom nedostataka ovo se rešenje vrlo brzo proširilo. S jedne strane, ono je pozitivno pošto je obezbedjuje sličan pravni tretman računarskih programa u većem broju zemalja, što znatno utiče na olakšavanje harmonizacije prava na raznim regionalnim ili širim međunarodnim osnovama. S druge strane, ono se negativno odražava na same računarske programe, jer im ne priznaje sve osobnosti koje su za njih

<sup>222</sup> Edwards C., Savage N., Walden I., op. cit., str. 61 - 64; Krmić - Fikeys N., Problemi autorskopravne zaštite kompjuterskih programa, Zakonitost, br. 1/90. str. 97.

specifične i po kojima se, u suštini, razlikuju od književnih i drugih, za sada priznatih, autorskih dela.

**Treće.** *U većini zemalja štite se materijalizovani kompjuterski programi*, što je posledica monističkog shvatanja prirode autorskog dela, po kome je, da bi se tretirao kao rezultat ljudskog stvaralaštva i da bi mogao da predstavlja autorsko delo, potrebno da bude izražen u nekoj, bilo kakvoj formi. Sama ideja se ne štiti.

**Četvrto.** *U gotovo svim nacionalnim pravima u kojima je priznata autorskoppravna zaštita kompjuterskih programa (ili softvera) autorima se priznaju sva moralna prava, dok postoje razlike, od zemlje do zemlje, u vrstama priznatih imovinskih prava.* Tako se najčešće posebno<sup>223</sup> regulišu pitanja zaštite prava autora vezana za umnožavanje i kopiranje, preradu i prevodjenje programa. Ponudjena rešenja uglavnom priznaju autorizaciju, kao način zaštite ovih prava, ali i autora i nosioca.

---

<sup>223</sup> Besarović V., Prednosti autorsko-pravne zaštite računarskih programa, Beograd, Anali Pravnog fakulteta u Beogradu, br. 2-3/89. str. 167.

### 3.4.3. *Kompjuterski programi i međunarodna zaštita autorskog prava*

#### 3.4.3.1. *Bernska konvencija za zaštitu književnih i umetničkih dela*

**Bernska konvencija za zaštitu književnih i umetničkih dela** (*Bern Convention for the Protection of Literary and Artistic Works*), iz 1886. godine, više puta revidirana (poslednje revizije u Stokholmu 1967. i Parizu 1971.), predstavlja jedan od ključnih međunarodnih izvora autorskog prava. U njoj su, pored opštih načela, nacionalnog tretmana i minimalne zaštite, propisana i odredjenja književnih i umetničkih dela, kao i obrazovanje Bernske unije. Osim toga, **ovom Konvencijom ustanovljena je prvi put i relativno velika dužina trajanja zaštite autorskog prava na period koji traje za života autora i 50 godina posle njegove smrti**<sup>224</sup>. Na računarske programe i softver primenjuju se, pored ovih opštih odredbi, naročito odredbe članova 8, 9, 12 i 16.

Autori književnih i umetničkih dela, znači i kompjuterskih programa, uživaju, za sve vreme trajanja svojih prava na originalno delo, isključivo pravo na prevode ili da daju odobrenja za prevodjenje svojih dela. To drugim rečima znači **da se od autora računarskog programa mora tražiti odobrenje za prevodjenje iz jednog u drugi programski jezik** (čl. 8).

Član 9. je značajan jer po njemu "autori književnih i umetničkih dela zaštićenih ovom Konvencijom", dakle, i računarskih programa, **"uživaju isključivo pravo da daju odobrenje za reprodukovanje** ovih dela, bez obzira na koji način i u kom obliku". Kad su u pitanju kompjuterski programi reprodukovanje ima drugačije značenje i pod njime se podrazumeva kopiranje, pa, otuda, **za njihovo kopiranje je potrebno dobiti dozvolu autora**. Izuzetak su samo kopije neophodne za rad, za koje nacionalna prava predviđaju drugačiji tretman. Tačka 2. istog člana kojom se zakonodavstvima zemalja Unije ostavlja pravo da dopuste reprodukovanje (kopiranje, pomenutih kompjuterskih programa) u izvesnim posebnim slučajevima (normalan rad i sigurnost korisnika, back-up kopije, ili za privatno izučavanje i privatno profesionalno istraživanje, ako to ne donosi profit ili neku drugu materijalnu korist), pod uslovom da ovo reprodukovanje nije na štetu redovnog korišćenja i da ne nanosi neopravdanu štetu zakonitim interesima autora. Ovaj član, uz čl. 12., posebno **je značajan i za**

<sup>224</sup> Bernska konvencija, čl. 7. t. 1.

**reverzibilno programiranje, odn. reverzibilno kompiliranje.** Kako je reverzibilno kompiliranje, u stvari, prevodjenje aplikativnog programa u izvorni kod (koji se inače ne predaje, već, po pravilu, ostaje kod autora) ono predstavlja određenu adaptaciju i pretpostavlja kopiranje, odn. reprodukciju. U slučaju da se reverzibilnim kompiliranjem želi doći do izvornog koda ono predstavlja, upravo, slučaj "nanošenja štete redovnom korišćenju" računarskog programa i biće u sukobu sa "redovnim korišćenjem". Retko ko to radi zbog istraživanja i studiranja, mada ukoliko je tako neće podlegati ovim odredbama.

Isto tako ove odredbe značajne su i za **sprečavanje piratstva** (neovlašćenog kopiranja i korišćenja kompjuterskih programa i softvera), kao pojave koja je uzela maha i nanosi ogromne štete ne samo autorima, nego i nacionalnim privredama. Tako po podacima koje su objavili Amerikanci, SAD je samo od N.R. Kine, u kojoj nije bilo zakonske zaštite računarskih programa i softvera, a istovremeno kako nije ni članica Unije, piratstvom izgubio 300 miliona dolara samo u 1988. godini<sup>225</sup>. Prvo u 1994., pa potom u 1995. godini, zbog piratstva računarskih programa, SAD je gotovo objavila trgovinski rat Kini. Pretnja se završila izmenama odredbi Zakona o autorskim pravima i obećanjima Kineske vlade da su mere uništenja piratskih fabrika u celoj zemlji sprovedene, kao i uveravanjima da se dalje piratske i druge nelegalne aktivnosti neće tolerisati.

Ukoliko je računarski program reprodukovao, odn. kopiran na nedopušten način primeniće se član 16. ove Konvencije po kome će nedozvoljena, odn. **reprodukcija računarskog programa na nedopušten način, biti zaplenjena u zemljama Unije u kojima originalno delo uživa zakonsku zaštitu.**

Autor kompjuterskih programa (kao i drugih književnih i umetničkih dela) ima isključivo pravo da daje odobrenje za adaptaciju i druge prerade svojih dela (čl. 12.). Znači, *korisnici i treća lica ne mogu bez dozvole autora preradjivati ili doradjivati računarske programe*. Doduše, nacionalna zakonodavstva su u pogledu kompjuterskih programa bila fleksibilnija i predvidela izuzetke u slučajevima kad se radi o "neophodnim prepravkama za normalno korišćenje", s tim što su, neka bolje neka lošije, definisala šta se pod tim "normalnim korišćenjem" podrazumeva.

Sve evidentnija pitanja i problemi vezani za kompjuterske programe, kompjuterizovane baze podataka, emitovanje preko satelita, grafičku reprodukciju, digitalne zapise slike i zvuka i velike količine iznajmljenih zvučnih zapisa i videotraka,

<sup>225</sup> Computer Software & Intellectual Property, Background paper, Office of Technology Assessment, Congress of United States, 1990., str. 17.

doveli su do sve jasnijeg stava o neophodnosti nove revizije<sup>226</sup>. Da bi se brže rešili ovi problemi Međunarodni biro je pripremio Nacrt odredbi mogućeg ugovora po ovim i drugim pitanjima - **Protokol**. S obzirom na nesuglasice oko neophodnosti regulisanja ovih pitanja ovaj Protokol još nije usvojen, mada se satajao, u više navrata, Komitet eksperata.

Još je jadan momenat, vezan za Bernsku konvenciju, izuzetno važan. Godine 1988. Bernskoj Uniji, posle gotovo jednog veka apstinencije pristupa i SAD. Naime, nakon neuspelih više puta preduzimanih akcija o pristupanju Bernskoj Uniji, Ministarstvo inostranih poslova formira *ad hoc* Radnu grupu (*The Ad Hoc Working Group US Adherence to the Bern Convention*) koja, proučivši pitanja vezana za mogućnost pristupa, priprema Finalni izveštaj 1986. godine. Slede mnogobrojne debate da bi se 1988. godine doneo **Zakon o primeni Bernske konvencije** (*The Bern Convention Implementation Act*), koga je jednoglasno usvojio Senat i Predstavnički dom, a, potom, potpisao Predsednik. Akt je deponovan kod generalnog direktora WIPO-a, a stupio na snagu marta 1989. godine. Jedan od ključnih razloga prihvatanja Konvencije bili su i **trgovinski interesi** SAD u oblasti kompjuterske tehnologije i pritisak velikih američkih korporacija zbog komercijalnog iskorišćavanja ovih prava, naročito u inostranstvu, za što im je bila potrebna podrška Konvencije<sup>227</sup>.

### 3.4.3.2. Univerzalna konvencija

Ništa manje značajna za međunarodnu zaštitu autorskih prava nije ni **Univerzalna ili Ženevska konvencija**, tzv. **UCC konvencija** (*The Universal Copyright Convention*), doneta 1952. godine. Nastala je kao pokušaj UNESCO-a da se proširi krug zemalja i onima koje nisu prihvatile Bernsku konvenciju (SSSR, SAD, Kina, i dr.). Značaj ove Konvencije je načinu rešavanja problema različitosti pravnih sistema, kao i u osnivanju **Svetske unija o autorskom pravu**. Medjutim, iako pretenciozno zamišljena da zameni Bernsku konvenciju i okupi veći broj zemalja, UCC to ipak nije uspela, mada su se oko nje okupile zemlje koje nisu imale interesa da pristupe Bernskoj konvenciji. Pored njih mnoge zemlje, i Jugoslavija, pristupile su njoj, a ostale i pri Bernskoj. To je bilo moguće osobito zbog toga što obe konvencije ne čine paralelne i komplementarne sisteme. U odnosu na računarske programe i softver ova Konvencija je značajna jer:

<sup>226</sup> Bogša A., Kratka istorija prvih dvadeset pet godina Svetske organizacije za zaštitu intelektualne svojine, Patentni glasnik, br. 2/93., str. 359 i 360.

<sup>227</sup> Ginsburg J., Kernochan J., One Hundred and Two Years Later: The US Joins The Bern Convention, RIDA, no. 141/189., str. 71.

**Prvo.** Predviđa *upotrebu oznake C, odn. ©* praćenu imenom nosioca autorskog prava i naznačenjem godine prvog objavljivanja, pri čemu, znak, ime i godina moraju biti stavljeni na način i na mesto kome se jasno uočava da je autorsko pravo zadržano<sup>228</sup>. Znači, i za računarske programe primenjivaće se ova oznaka, a od nacionalnog zakonodavstva zavisi na koje mesto će oznaka biti stavljena, odn. šta će se pod formulacijom "mesto i način koji jasno pokazuje da je autorsko pravo zadržano" podrazumevati.

**Drugo.** Za razliku od Bernske, Univerzalna konvencija *propisuje kraće rokove zaštite* (zbog zemalja koje takva rešenja imaju u svojim propisima) predviđajući kao *minimalan period za života autora i 25 godina od njegove smrti, odn. 25 godina od momenta objavljivanja ili registracije dela*<sup>229</sup>. Pod "objavljivanjem" se podrazumeva reprodukovanje u materijalnom obliku i stavljanje na raspolaganje javnosti primeraka dela, čime se pruža mogućnost da oni budu čitljivi ili vizuelno uočljivi. Za dela primenjene umetnosti rokovi su skraćeni na 10 godina, što može biti značajno za dizajn znakova razlikovanja računarskih programa. S obzirom na svojstva koje programi imaju čini se celishodnije ovo rešenje jer je sama priroda ovih dela takva da ona "zastarevaju" i u mnogo kraćem roku. Isto tako, što se tiče termina "objavljivanja", po kome se računaju rokovi i osnove zaštite. Međutim, primenjujući ovu Konvenciju na računarske programe, **objektni kodovi i operativni sistemi, odn. programi, kao i programi u ROM-u neće se moći štititi jer nisu "čitljivi i vizuelno uočljivi"**.

**Treće. Imovinska prava koja ima autor odnose se naročito na: isključivo pravo reprodukovanja i isključivo pravo prevodjenja.** Oba ova prava su od interesa za računarske programe, odn. njihove autore. Da bi se kopirao računarski program mora se tražiti dozvola od autora, bilo da se kopira u originalnom obliku, bilo u izvedenom. Znači, i kad se dobiju objektni kodovi programa, pošto je to izvedeni oblik izvornog koda, neće se moći izvršiti kopiranje (pa ni reverzibilno kompiliranje) ukoliko se ne dobije dozvola autora, čime se mnogo jasnije određuje sadržaj prava na reprodukovanje. Ovo pravo može biti nacionalnim zakonom ograničeno određenim izuzecima, ali samo onima koji nisu u suprotnosti sa "duhom i odredbama ove Konvencije".

Pravo na prevod, odn. prevodjenje iz jednog u drugi programski jezik ne može se izvršiti ukoliko se ne dobije dozvola autora. Ovo pravo nacionalnim

<sup>228</sup> UCC konvencija, čl. III., tč.1.

<sup>229</sup> UCC konvencija, čl. IV., tč. 2, 3.

zakonodavstvom može biti ograničeno, ali uskladjeno sa odredbama Konvencije<sup>230</sup>. Ukoliko dodje do prevodjenja, na "prevodu" se mora navesti naziv programa i ime autora originalnog dela i to biti "štampano" na svim primercima prevoda, odn. pojavljivati se na ekranu, omotu medijuma i sl., zavisno koje je rešenje prihvaćeno.

Zanimljivo je da **ova Konvencija nije predvidela pravo davanja dozvole za adaptaciju.**

#### 3.4.3.3. *Model zakona za zaštitu kompjuterskog softvera*

Značajne aktivnosti preduzimaju se i na međunarodnom planu. Tako je WIPO 1977. godine doneo **Model zakona za zaštitu kompjuterskog softvera** (*Model Provisions on the Computer Software*)<sup>231</sup> koji polazi od svojevrsnosti računarskih programa i teškoća njihovog podvodjenja pod autorska dela i još teže pod pronalske, pokušavajući da se nadju specifična rešenja. Bio je to i pokušaj zaštite pravom *sui generis* koja, inače, nije bila prihvaćena ni u teoriji ni u zakonodavstvima. Model zakona trebalo je da predstavlja taj pravni okvir u koji je bi se smestile sve, ili bar većina, posebnosti softvera i računarskih programa. Istovremeno on je trebalo da posluži i kao putokaz nacionalnim zakonodavstvima za iznalaženje odgovarajućih rešenja u zaštiti. Kako ponudjena rešenja iz ovog Modela nisu postala opšteprihvaćena to su se u okviru WIPO-a nastavile aktivnosti. Rezultat je bio **Nacrt međunarodnog ugovora o zaštiti računarskog softvera** (*Draft Treaty for the Protection of Computer Software*) iz 1984. godine, koji je isto tako neslavno prošao kao i Model zakona. Pored isticanja nužnosti zaštite pravom *sui generis*, oba su akta pošala od softvera kao predmeta zaštite i time učinila korak napred u odnosu na sva dotadašnja, ali i kasnija rešenja.

<sup>230</sup> UCC konvencija, čl. V., tč. 2.

<sup>231</sup> WIPO, Model Provisions on the Computer Software, Industrial Property, 1977, str. 265.

#### 3.4.3.4. Rezolucija o zaštiti kompjuterskog softvera i integrisanih kola

Ni Medjunarodno udruženje za zaštitu prava industrijske svojine (*Association Internationale pour la Protection de la Propriete Industrielle*) nije ostalo dužno. Godine 1986. na kongresu u Londonu donosi se Rezolucija o pitanju 57., odn. **Rezolucija o zaštiti kompjuterskog softvera i integrisanih kola** (*Resolution of Protection of Computer Software and Integrated Circuits*)<sup>232</sup>. Po ovoj Rezoluciji, donetoj na osnovu izveštaja 20 nacionalnih grupa (svaka obuhvata određen broj zemalja) sa prezentacijom i objašnjenjem rešenja na osnovu kojih je softver zaštićen, **prihvaćeno je sledeće:**

1. **softver treba zaštititi**, na medjunarodnom i nacionalnom planu, **autorskim pravom**, kao autorsko delo, mada se ne isključuje ni zaštita ugovorima, pravom zaštite od nelojalne konkurencije i pravilima koja se odnose na zaštitu žigova;
2. **zaštitu autorskim pravom prihvatiti** i u drugim medjunarodnim sporazumima;
3. neophodno je **izgraditi pravila** koja će moći da se ugrade, brzo i jednostavno, u **autorskopravnu zaštitu** softvera;
4. ukoliko se to bude obezbedilo, ovakav medjunarodni **tretman softvera će omogućiti njegovu adekvatnu zaštitu**;
5. preporuke koje proizlaze iz ove Rezolucije **ne isključuju i iznalaženje drugih, specijalnih, rešenja** za obezbedjenje zaštite softvera u drugim medjunarodnim sporazumima;
6. na osnovu odluke AIPPI pripremiće se posebna studija koja treba da pokrene iznalaženje odgovora na sledeće: **koja su pravila za zaštitu softvera pogodna, koje elemente softvera je moguće posebno zaštititi istim sistemom, koja su ekskluzivna autorska prava, koji je obim tih prava, koji su uslovi za zaštitu**, odn. da li su to i depozit i oznaka registracije, i sl.;
7. razmotriti i proučiti da li je potrebno **menjati pravila autorskog ili drugih prava** da bi se obezbedila zaštita softvera na nacionalnom i medjunarodnom planu.

Sem same činjenice da je ova Rezolucija doneta još 1986. godine, njen je značaj i u tome što su pokrenuta suštinska pitanja koja će u narednim godinama biti

<sup>232</sup> AIPPI, Resolution of Protection on the Computer Software and Integrated Circuit, Report Expert Committee, 1986.

rešavana na međunarodnom i nacionalnim planovima. Osim toga, pošto je u pitanju dokument AIPPI-a u čijem radu učestvuju najjemenentniji eksperti (*Expert Committee*) koji su predložili Rezoluciju i čije odluke, akte i preporuke poštuju zakonodavci i sudska praksa u većini zemalja članica, to je njegova Rezolucija predstavljala jednu od okosnica rešenja zaštite na međunarodnom i nacionalnom planu.

#### 3.4.3.5. *Direktiva o pravnoj zaštiti kompjuterskih programa*

Veoma značajna aktivnost vezana je za **Evropsku Uniju**, u okviru koje je 1988. godine objavljena studija pod nazivom **Zelena knjiga o autorskom pravu i uticaju tehnologije** (*Green Paper on Copyright and Challenge of Technology: Copyright Issues Requiring Immediate Action*)<sup>233</sup>, a koju je izradila posebna Komisija. Na osnovu ove studije doneta je **Direktiva o pravnoj zaštiti kompjuterskih programa** (*Council Directive 91/250/EEC on the legal protection of computer programs*)<sup>234</sup>. Direktiva je postala sastavni deo programa za 1992. godinu (stupila je na snagu 1. januara 1992.). Doneta je u cilju ukazivanja rastućeg značaja koji KT ima za sve aspekte ekonomskih aktivnosti<sup>235</sup>. Svrha joj je, takodje, da ukaže na pomankanje zaštite u nekim zemljama članicama Unije od neautorizovanog korišćenja programa, kao i predviđanje, mahom, tradicionalnih oblika zaštite. Kako neki postojeći oblici zaštite ne pružaju autorima sigurnost, osobito ne od neautorizovanog kopiranja i korišćenja njihovih dela, a pošto računarski programi i softver predstavljaju značajne izvore prihoda i za države, to se pokazala nužnom harmonizacija prava svih država članica. Naime, ovo je oblast koja je do tada bila, uglavnom, predmet nacionalnog regulisanja i izmakla je kontroli Unije, što se pokazalo kao značajan promašaj jer je ometao slobodno kretanje robe i usluga i ograničavao joj nadležnost. Ako se tome doda i činjenica da slučajevi pojedinačnih nacionalnih prava i sudske prakse ne obezbeđuju uniformnost u rešavanju problema, što se posebno vidi kad se ti problemi pojave pred Evropskim sudom časti, to je onda sasvim razumljivo zašto se Komisija opredelila na donošenje ove Direktive. Sasvim je sigurno da ona treba da **omogući harmonizaciju i unifikaciju nacionalnih pravnih sistema**, kao što je to slučaj sa regulisanjem žigova ili patenata. **Direktiva obezbeđuje da osnovna pravila zaštite kompjuterskih programa važe na teritoriji cele Unije i upotpunjava postojeće režime zaštite, ukoliko je to potrebno, ili uvodi nove tamo gde ne postoje.** Osim toga, očekuje se da će ona biti naročito značajna u predstojećoj promeni Common Law-a. Ona je utoliko značajnija koliko su

<sup>233</sup> COM (88) 172.

<sup>234</sup> Council Directive of 14 May 1991. OJ. L.122/42. 1991.

<sup>235</sup> Prinsley M., S. Baxster, The proposed European Directive on the legal protection of computer programs, London, A Frank Cass Professional Journal, Computer Law & Practice, no. 6/90. str. 217.

sami “računarski programi fundamentalna komponenta informacione supermagistrale i vitalni deo razvoja proizvodne industrije programa”<sup>236</sup>. Istovremeno, ova Direktiva predstavlja jednu od ključnih strana petougla zaštite intelektualne svojine u EU koga sačinjava: zaštita baza podataka, zaštita prava zakupa i iznajmljivanja određenih prava vezanih za autorsko pravo u okviru prava intelektualne svojine, zaštita autorskih prava u satelitskoj emisiji i kablovskoj retransmisiji, zaštita integrisanih kola i harmonizacija dužine trajanja zaštite autorskih i srodnih prava<sup>237</sup>. Naravno, ona ima i posebno važnu ulogu u predviđanju minimuma prava, u svim zemljama članicama, koja treba da imaju autori kako bi zaštita bila potpunija.

**Direktiva polazi od sledećih pretpostavki:**

**Prvo.** Definisanje kompjuterskih programa je nepodesno s obzirom na brzinu tehnološkog razvoja. Ipak, *kompjuterski program obuhvata materijalizaciju, u svakom obliku, zapisa ili koda niza instrukcija na osnovu kojih računar izvršava pojedinačne naredbe ili funkcije*. To ne obuhvata ideje, principe, logiku, algoritme programskog jezika uključenog u program. U toj dishotomiji ideja/materijalizacija sama ideja se ne štiti. S druge strane, materijalizovana ideja u objektnom ili izvornom kodu je na određen način obuhvaćena.

**Drugo.** Prihvaćeno je stanovište mnogih nacionalnih prava da se *programi štite kao autorsko delo i to kao književno delo*. U toj autorskopravnoj zaštiti štiti se individualna materijalizacija autorskog dela (isključujući algoritme i njihovo kopiranje). Time se ne blokira tehnički progres, a sprečava nedozvoljena i neautorizovana reprodukcija.

**Treće.** *Prihvataju se i drugi aspekti i objekti zaštite kompjuterskih programa*, kao što je npr. softver, ukoliko to nije deo zaštite predviđene ovom Direktivom i ne kosi se sa njom. Naime, drugi objekti mogu se štititi ukoliko je to predviđeno nacionalnim pravom. Tako, ako se softver po nacionalnom pravu štiti kao posebno književno delo onda se ta mogućnost ne isključuje samom činjenicom da softver nije objekt koji je obuhvaćen Direktivom. Pored toga, *dozvoljena je mogućnost dodatne zaštite* institutom poslovne tajne, pravom zaštite od nelojalne utakmice, pa se, čak, ne isključuje ni kumulativna zaštita programa autorskim pravom i ostalim pravima predviđenim u nacionalnim sistemima.

<sup>236</sup> Commission of the European Communities, Green Paper of Copyright and Related Rights in Information Society. Brussels, 1995., str. 30.

<sup>237</sup> To su tzv: *Computer Program Directive, Database Directive, Rental Right Directive, Satellite and Cable Directive, Integrate Circuit Directive i Terms of Protection Directive*.

**Četvrto. *Da bi računarski program mogao da se štiti kao književno delo*** na osnovu ove Direktive ***neophodno je da bude originalan***. To znači da se originalnost predviđa kao minimalni uslov koji treba da zadovolji jedan računarski program da bi mogao da uživa zaštitu koju ima svako, i bilo koje, književno delo.

Ovim osnovnim pretpostavkama neophodno je dodati i rešenja koja nudi Direktiva u odnosu na autorstvo programa, povlastice u zaštiti, ograničenja i vreme trajanja zaštite.

Direktiva pod **autorom računarskog programa podrazumeva fizičko lice koje je program kreiralo**. Njemu pripadaju sva moralna i materijalna prava. Ukoliko u stvaranju programa učestvuje više fizičkih lica ekskluzivno autorsko pravo pripašće svima podjednako, sem ako nije ugovorom drugačije predviđeno. Nosilac autorskog prava za program izradjen po narudžbini je, po pravilu, naručilac ukoliko ugovorom nije drugačije određeno. Ako, pak, program nastane kao tvorevina zaposlenog u toku radnog vremena on će uživati moralna prava dok će nosilac materijalnih prava biti poslodavac, naravno, ako drugačije nije ugovorom predviđeno.

Posebnim članom Direktive<sup>238</sup> predviđeno je da **autor ima isključivo pravo da daje dozvolu (autorizuje)** za: reprodukovanje (***pravo reprodukcije***), menjanje (***pravo prerade***) i distribuciju (***pravo raspolaganja***) programa prodajom, lizingom, zakupom, iznajmljivanjem u bilo kom smislu i obliku, za delove ili celinu. Onoliko koliko je to neophodno, i za vreme za koje smatra da je potrebno, autor će ograničiti reprodukciju programa u delu ili celini pri prihvatanju, pregledanju, izvršavanju, prenošenju i čuvanju programa. Isto tako, bez dozvole autora ne smeju se programi menjati, ni u celini niti neki njihov deo. Autor posebno ima pravo kontrole distribucije programa. Ovo se pravo autora iscrpljuje nakon prvog puštanja programa na tržište i prenosi se na nosioca prava.

Izuzeci od ovih prava autorizacije postoje u slučajevima koji se taksativno u Direktivi navode. Tako, **bez autorizacije nosioca prava moći će se vršiti reprodukcija ili adaptacija prodatog ili na drugi način objavljenog programa onoliko koliko je to neophodno da bi se program mogao koristiti u svrhe za koje je nabavljen**, jedino ako nije u pitanju ugovor o licenci koji su sklopili autor i nosilac prava. Reprodukcijska i adaptacijska prava za druge svrhe mora da podleže autorizaciji. **Distribuiranje programa bez dozvole nosioca prava korišćenja biće moguće samo ukoliko je vezano za određene neekonomske svrhe** (npr. za nastavu), osim ako, opet,

<sup>238</sup> Direktiva o pravnoj zaštiti kompjuterskih programa, čl. 4.

nije u pitanju ugovor o licenci. **Dekompilacija** će, takodje, **biti dozvoljena ako se do informacija za drugi, s njim u neposrednoj vezi, program ne može drugačije doći.**

**Zaštita se<sup>239</sup> garantuje 50 godina od dana nastanka programa.**

Na kraju, neophodno je istaći da je Direktivom predviđeno da se zemlje članice Evropske Unije obavezuju da će rešenja njome predviđena ugraditi u svoje pravo - zakonske ili administrativne propise. O načinu i obliku uvođenja odredbi Direktive u nacionalno pravo države članice moraju obavestiti Komisiju.

Iako od izuzetne važnosti za dalji tretman računarskih programa i njihovu zaštitu, Direktiva je načinila i nekoliko propusta. Tako, nisu najcelovitije napravljene razlike između raznih modaliteta koji se u vezi sa programima i softverom pojavljuju i koji zahtevaju različitosti u pristupu i rešavanju. U želji da ne bude isuviše normativistička Direktiva je ostala isuviše opšta i uopštena. Svakako da je veoma elegantno rešenje izosavljanje definisanja samih računarskih programa i time stvorena mogućnost da se promenama koje nastaju ne moraju vršiti promene u ovom aktu i nacionalnim pravima, no, ipak, to otvara čitavu lepezu problema. Kako će nacionalni sudovi u sporovima oko zaštite tretirati programe i koja će odredjenja prihvatiti, što može značiti stvaranje neravnomernosti i nejednačenosti. I ne samo kod sudova.

S obzirom da se u većini zemalja članica računarskim programima i, pokadšto, softveru prilazi kao autorskom, i to književnom delu, to se na njih primenjuju i opšte odredbe Bernske i Univerzalne, odn. Ženevske konvencije<sup>240</sup>.

---

<sup>239</sup> Kako je definisano članom 8.

<sup>240</sup> Burkill G., Reverse compilation of computer programs and its permissibility under the Bern Convention, A Frank Cass Professional Journal, Computer Law & Practice, no. 4/90; Computer Software & Intellectual Property, Background paper, Office of Technology Assessment, Congress of United States, 1990., str. 24.

#### 3.4.3.6. *Sporazum o trgovinskim aspektima prava intelektualne svojine*

I, naravno, od posebnog značaja je i **Sporazum o trgovinskim aspektima prava intelektualne svojine**. Po njemu su **kompjuterski programi posebno izdvojeni u okviru autorskih i srodnih prava, i predviđeni da se štite, u izvornom ili objektnom kodu, kao književna dela**, a na osnovu Bernske konvencije<sup>241</sup>. To, s jedne strane, znači da se oni štite kao ostvarenje, a ne kao ideje te im na osnovu toga slede uobičajena autorska prava, i da se posebno predviđaju i specifična prava kao što je pravo iznajmljivanja. **Pravo iznajmljivanja** je pravo koje sve strane ugovornice garantuju autorima i njihovim naslednicima, a sastoji se u davanju dozvola ili zabranjivanju komercijalnog iznajmljivanja javnosti originala ili kopija kompjuterskih programa. Ovo se obaveza ne odnosi na ona iznajmljivanja kod kojih program nije osnovni predmet<sup>242</sup>.

Sporazum je predvideo i trajanje zaštite kompjuterskih programa određujući **tri solucije**: **a)** uobičajeno trajanje zaštite zavisno od životnog veka fizičkog lica; **b)** ako se podje od drugog osnova tada je minimalni rok **50 godina od kraja kalendarske godine u kojoj je dozvoljeno objavljivanje**; ili **c)** ako ne postoji takvo dozvoljeno objavljivanje, onda **50 godina od nastanka**, odn. 50 godina od kraja kalendarske godine u kojoj je nastalo.

Medjutim, za trgovinu je od izuzetnog značaja **pojava krivotvorenih kompjuterskih programa**, kao i **programa ili robe koja ih sadrži, a proizvedenih na osnovu nezakonitog prisvajanja**. Ovi programi i roba su, u suštini, bilo koji kopirani programi ili roba napravljeni bez saglasnosti titulara prava ili lica koje je on ovlastio u zemlji proizvodnje, koji su uradjeni direktno ili indirektno sa predmeta, a izrada kopije predstavlja povredu autorskog ili srodnog prava (na osnovu zakona zemlje uvoza).

Solucije koje se mogu preduzeti u slučajevima povrede prava intelektualne svojine ili pojave robe proizvedene na osnovu nezakonitog prisvajanja autorskopravno zaštićenih programa mogu biti različite:

- *nužnost obezbedjenja efikasnih postupaka zaštite* predviđanjem u nacionalnim okvirima i odgovarajućim nacionalnim zakonima (poštujući zahtev izbegavanja stvaranja barijera legitimnoj trgovini, zahtev

<sup>241</sup> Sporazum o trgovinskim aspektima prava intelektualne svojine, čl. 10.

<sup>242</sup> Sporazum o trgovinskim aspektima prava intelektualne svojine, čl. 11.

pravičnosti i jednakosti za sve, kao i zahtev dokazane zasnovanosti i mogućnosti preispitivanja);

- *predvidjenost* da sudski organi imaju ovlaštenje da, odmah posle carinjenja, **nalože strani da prestane sa povredom prava** kako bi se sprečio ulazak u trgovinske tokove na njihovoj teritoriji uvezenih programa kojim se vredja pravo intelektualne svojine i naložiti naknadu štete titularu prava. Titular ima i pravo na informaciju o identitetu trećih lica uključenih u proizvodnju i distribuiranje programa i usluga koji predstavljaju povredu prava, kao i o njihovim distributivnim kanalima;
- *predvidjenost* ovlašćenja sudskih organa da nalože da se **programi** za koju se utvrdilo da predstavlja povredu prava, bez bilo kakve naknade, **povuku** iz trgovinskih tokova ili unište, ali vodeći računa da se ne načini šteta titularu prava;
- *predvidjenost* mogućnosti da **sudski organi izriču privremene mere** radi sprečavanja povreda i čuvanja relevantnih dokaza;
- *predvidjenost* izricanja **zabrane puštanja u promet** programa proizvedenog na osnovu nezakonitog prisvajanja autorskih prava;
- *predvidjenost* ovlašćenja nadležnih organa da nalože **uništavanje ili povlačenje** programa dobijenih povredom autorskih prava u skladu sa propisanim principima;
- *predvidjenost* mogućnosti **pokretanja krivičnog postupka i kažnjavanja počinioca** koji su svesno izvršili piratstvo autorskih prava zbog njihovog komercijalnog korišćenja. Osim kazne zatvora i novčane kazne preporučuju se i mere oduzimanja, zaplene i uništenja "inkriminisane robe i svih materijala i alata koji su se koristili pri izvršenju krivičnih dela".

Dakle, akcija na specifičnoj *medjunarodnoj zaštiti teče paralelno u tri univerzalne i više regionalnih organizacija*. Paralelizam je sasvim očekivan, ali ne i celishodan. Ponekad će, mada redje, postojati i istovremena zaštita sa sva tri akta. Ipak se stalno mora imati u vidu da je zaštita koja je predviđena Sporazumom o trgovinskim aspektima prava intelektualne svojine proistekla iz akata WIPO-a.

#### 3.4.4. *Kompjuterski programi i autorskopravna zaštita po našem pravu*

Aprila 1990. godine Savezno veće Skupštine SFRJ usvojilo je Zakon o izmenama i dopunama Zakona o autorskom pravu<sup>243</sup>. **Tog datuma pridružili smo se zemljama koje su prihvatile autorskopravnu zaštitu računarskih programa.** Inicijativa za rešavanje problema zaštite je formalno potekla od Saveznog zavoda za informatiku, ali je stvarno predstavljala odgovor na već duže vremena postavljano pitanje - kako zaštititi računarske programe. Sigurno je da je na traženje rešenja ne mali uticaj imala i činjenica da se naša zemlja našla na crnoj listi SAD-a zbog nepoštovanja autorskih prava i njihove neadekvatne zaštite, odn. odsustva bilo kakve pravne zaštite računarskih programa. Neslavna tradicija se nastavljala te smo po dokumentima i studijama međunarodnih organizacija i asocijacija bili apostrofirani kao jedna od zemalja koja ništa nije preduzela na planu rešavanja ovog problema. Predsednik AIPPI-a je, prilikom jedne posete Jugoslaviji, posebno ukazao i upozorio (ne bez argumenata) na neophodnost brzog preduzimanja, odgovarajuće akcije u pravnom regulisanju računarskih programa, softvera i mikročipova ukoliko želimo da pratimo svetske tendencije razvoja KT, s jedne, i Prava intelektualne svojine, s druge strane. To je, svakako, bilo opravdano jer smo u to vreme (1985.) imali 3.002 računara, a već dve godine kasnije 14.793. Te računare je trebalo opskrbiti odgovarajućim programima, a njih je trebalo zaštititi, osobito uvozne. Naravno, ne bi trebalo zaboraviti da je pojava PC donela masovno nelegalno korišćenje kompjuterskih programa (nekoliko sati pre svetske promocije CD sa *Microsoft '95* se našao u Beogradu i to po ceni od 30 DEM, a ubrzo potom počela je distribucija domaćih piratskih kopija). Situacija je postajala složenija gotovo svakodnevnim povećavanjem broja privatnih firmi za pružanje računarskih usluga ili onih koje se u svom radu služe računarima<sup>244</sup>. Mnoge od njih se bave kreiranjem i izradom programa i softvera. I njih je bilo potrebno zaštititi, kao što je trebalo obezbediti i one firme koje se, kao delatnošću, bave distribucijom određenih programa, domaćih i stranih. Ništa manje značajno nije bila ni želja da se u ovoj oblasti pojave naši računarski programi i softver na drugim, pa i svetskom tržištu, a što je bilo otežano, između ostalog, i zbog nemogućnosti obezbedjenja čak ni minimuma prava koja bi im se garantovala. A kako bismo tek pružili stranim?

<sup>243</sup> Zakon o autorskom pravu, Službeni list SFRJ, br. 19/78; 24/86; 21/90.

<sup>244</sup> Po podacima dobijenim na osnovu istraživanja koje je sprovedeno u organizacijama Srbije u toku 1995. u 1996. godine u 15,7% anketiranih organizacija samostalno se razvijao aplikativni softver; u 30,4% razvijan je uz konsultaciju sa drugima, u 32,6% pretežno je izradjen po narudžbini, a u 21,3% je potpuno kupljen. Istraživanje pod nazivom "Menadžment u funkciji inovacija" obavljeno je u organizaciji Univerziteta u Beogradu, Centra za menadžment, a rezultati su publikovani 1995. i 1996. godine u dve knjige pod istim nazivom. Autor ove knjige učestvovao je kao član tima u sprovođenju ankete i obradi podataka vezanih za menadžere informatike i inovativnu aktivnost preduzeća.

U to vreme sve je jasnije da je intelektualna svojina postala značajna komponenta privrednog razvoja neke, pa i naše, zemlje i da ima udela u zauzimanju povoljnog položaja na svetskom tržištu. Ako, pak, ta svojina nije racionalno i efikasno pravno regulisana položaj će biti znatno oslabljen, a zemlja će biti, između ostalog, svrstana u nesigurne ili "piratske"<sup>245</sup>. Kako računarski programi i softver nisu kategorije koje se lako svrstavaju u neke postojeće i poznate pravne institute, a sigurno pripadaju nekom od oblika prava intelektualne svojine, to je bilo neophodno u pravnim propisima pronaći odgovarajuća rešenja i obezbediti pretpostavke za ostvarivanje uloge koju oni za razvoj zemlje imaju. Svakako da nalaženje rešenja nije jednostavno i brzo, ali isto tako ne sme biti ni predugo jer se nanete štete teško ispravljaju i nadoknađuju.

Svi ovi, a i mnogi drugi, razlozi doveli su do donošenja Zakona o izmenama i dopunama Zakona o autorskom pravu.

Medjutim, još se nisu ni sagledali prvi pozitivni efekti izmena i dopuna Zakona, kada se pristupilo pripremama za donošenje novog Zakona o autorskom i srodnim pravima<sup>246</sup>. Same pripreme i izrada nekoliko verzija tog Zakona trajale su više od dve godine. Rezultat je Predlog Zakona čije se donošenje očekuje u jesenjem zasedanju<sup>247</sup>.

#### *3.4.4.1. Kompjuterski programi kao autorsko delo*

Zakonom o izmenama i dopunama Zakona o autorskom pravu **kompjuterski programi eksplicitno se smatraju autorskim delima** čime su uvedeni u našu pravnu doktrinu i, što je još bitnije, u naš pravni sistem<sup>248</sup>. To znači da im se priznalo autorskopravno svojstvo i time obezbedio pravni osnov za zaštitu Autorskim pravom.

Nažalost, to je i ostao jedini izričito priznati pravni oblik zaštite, jer postojanje mogućnosti primene većine drugih oblika ne znači da se oni stvarno i

<sup>245</sup> Erdelez S., op. cit., str. 873.

<sup>246</sup> Rešenja koja se prikazuju su iz Predloga zakona o autorskom i srodnim pravima, Beograd, juli 1996., a ova je verzija sa neznatnim primedbama i sugestijama prihvaćena sredinom avgusta 1996. godine od Savezne vlade i upućena u dalju proceduru.

<sup>247</sup> S obzirom da u momentu predaje i štampanja rukopisa Zakon o autorskom i srodnim pravima nije bio donet, to se rešenja koja su u njemu prihvaćena ukratko prikazuju, uz komparativnu analizu sa trenutno važećim Zakonom.

<sup>248</sup> Zakona o autorskom pravu, čl. 2..

primenjuju, kao što je i njihov supsidijaran (osim patentne zaštite) karakter u toj zaštiti umnogome povećao značaj koji priznata autorskoppravna zaštita sada ima, pa samim tim i ovog Zakona koji ju je predvideo.

Naš zakonodavac se, dakle, opredelio za *izdvajanje računarskih programa kao posebne vrste autorskih dela priznavajući mu specifičnosti po kojima se razlikuje od drugih dela iz oblasti književnosti, nauke i umetnosti*. Time smo se uvrstili u onu grupu zemalja koja priznaje računarske programe kao posebna autorska dela. Ovakav pravni tretman je utoliko značajniji što na indirektan način, ipak, računarske programe odvaja od dela kakva su pisana dela, dela svih grana primenjenih umetnosti i slična. Drugim rečima, ovakav pravni tretman značio je korak dalje, na prvi pogled, u odnosu na većinu, pa čak, i informaciono najrazvijenijih, zemalja koje su računarske programe podvele pod literarna dela. Na sreću, taj pristup je i dalje zadržan<sup>249</sup>. Dodali su se modaliteti računarskog programa koji uživaju autorskoppravnu zaštitu, odn. **da se računarski programi u izvornom, objektnom i izvršnom kodu smatraju autorskim delom**. Takodje je isključena mogućnost da se štiti softver jer se iz autorskoppravne zaštite eksplicitno izostavljaju opšte ideje, načela, principi i uputstva, koji su sadržani u autorskom delu. To znači da se ne mogu štititi ni algoritmi u najapstraktnijem vidu, niti dokumentacija ako je u programu (van programa, dakle, bi mogla)<sup>250</sup>. Ipak bi se trebalo složiti sa mišljenjem da bi autorskoppravna zaštita računarskih programa trebala da obuhvati:

- originalni konkretni niz instrukcija;
- originalnu strukturu programa;
- originalni konkretizaciju algoritama<sup>251</sup>.

Ono što ostaje kao nedorečenost je **neodredjivanje šta se pod računarskim programom podrazumeva**, što dovodi u pitanje efikasnost njegove zaštite<sup>252</sup>. Naime, neopredeljujući se za solucije koje postoje u nekim zakonima, a delimično i Direktivi EU o pravnoj zaštiti kompjuterskih programa, naš Zakon (Predlog zakona) je stvorio mogućnost da se na njih primenjuju posebne procedure i da za njih važe posebna prava. To i nije loše kad bi se sve te posebnosti u potpunosti pravno i

<sup>249</sup> Naime, u jednoj od verzija Prednacrta Zakona bio je napušten ovaj pristup, te su računarski programi svrstani u jezička autorska dela sa opravdanjem da to odgovara "semantičkoj prirodi ove vrste dela, i uskladjivanju sa članom 10, stav 1. Sporazuma o trgovinskim aspektima prava intelektualne svojine, a i članom 1, stav 2 Direktive EZ" kako je to izneto u obrazloženju člana 4. Prednacrta Zakona o autorskom pravu i susednim pravima, Beograd, 1994., str. 22, kao i Prednacrta iz avgusta 1995. godine.

<sup>250</sup> U članu 7 st. 1 Predloga zakona stoji: "Autorskoppravnom zaštitom nisu obuhvaćene ideje, načela, principi i uputstva koji su sadržani u autorskom delu.

<sup>251</sup> Marković S., op. cit., str. 20; Parać Z., op. cit., str. 105.

<sup>252</sup> Isto je rešenje prihvaćeno i u Predlogu zakona.

regulisale. Kako to baš nije slučaj onda se može desiti da se preterano vremena izgubi u dokazivanju i razjašnjavanju nečega za što ne postoji, ni u teoriji Kompjuterskog prava, a ni praksi, jedinstveno mišljenje. Tim gore, što ni naše sudije i drugi pravnici nisu baš naročito "informatičarski" obrazovani i što im nijanse u razlikovanju između računarskih programa u užem i širem smislu ili softvera nije oblast sa kojom su "familijarni". Isto tako će problema biti i sa raznim subjektima koji su uključeni u razne poslove oko računarskih programa i koji će imati različita tumačenja prava ili obaveza koje im iz autorskopravne zaštite u vezi sa predmetom pravnih poslova proističu. Naravno da mogu nastati štete dok se ne dobije tumačenja. No, ovaj problem treba ostaviti praksi da ga rešava "u hodu".

Ono što je bitno istaći je da priznavanje svojstava autorskog dela računarskim programima znači da i sami programi, ako je autor, npr. anoniman ili je program učinio dostupnim javnosti pod pseudonimom, uživaju zaštitu. Priznavanje svojstva autorskog dela kompjuterskim programima je značajno i **zbog zaštite njegovog naslova (naziva)** koji, da bi mogao biti zaštićen, mora biti originalan i mora predstavljati proizvod intelektualnog stvaralaštva autora<sup>253</sup>. Za to su posebno zainteresovane softverske kuće, kao nosioci autorskih prava nad autorskim delima svojih zaposlenih, jer su i naziv programa uključeni u borbu za kupca. Kad je u pitanju naziv računarskog programa Zakon ne isključuje ograničavanje njegove zaštite u slučajevima postojanja drugog programa sa istim nazivom, naročito ako je namenjen za istu svrhu. Zaštitu će uživati program koji se prvi pojavio. Da bi se, ipak, obezbedila još sigurnija zaštita naziva programa, naročito zbog postojanja konkurentske borbe, ali i nelojalne utakmice<sup>254</sup>, trebalo bi ga dodatno zaštititi žigom. Medjutim, ukoliko ne postoji posebna zainteresovanost autora ili nosioca autorskih prava za dodatnom zaštitom naziva, a naziv ispunjava predviđene uslove za zaštitu kao sastavni deo programa, primenjivaće se odredbe Zakona o autorskom pravu.

#### 3.4.4.2. *Uslovi zaštite*

Da bi kompjuterskim programima mogli da se smatraju autorskim delom neophodno je da **ispune, zakonom predviđene, uslove**<sup>255</sup>. To su:

<sup>253</sup> Zakon o autorskom pravu, čl. 7; Predlog zakona, čl. 4., st. 2.

<sup>254</sup> Zanimljivo je da je u verziji Predloga zakona iz aprila 1996., bila predviđena i mogućnost posebne zaštite naziva propisima o suzbijanju nelojalne utakmice, dakle Zakonom o trgovini. No, u kasnijoj verziji ovo je izostavljeno.

<sup>255</sup> Oba ova uslova predviđena su u Zakonu i Predlogu zakona.

1. *da su ideje iz programa materijalizovane i izražene u nekoj formi*; koja će to forma biti nije bitno; i
2. *da su originalni* odn. da su u pitanju originalne duhovne tvorevine autora.

Kako naše pravo ne predviđa druge uslove, to znači da računarski program mora ispunjavati samo ova dva uslova da bi bio autorsko delo. Za razliku od Zakona, Predlog zakona određuje da vrednost, umetnička, naučna ili neka druga, nije bitna, kao što nisu bitne ni: namena, veličina, sadržina, način ispoljavanja. Takođe, dopuštenost javnog saopštavanja sadržine računarskog programa nije uslov koji bi trebalo da zadovolji da bi bio autorsko delo.

#### 3.4.4.3. Sadržina prava

Kad jedan računarski program ispuni uslove da bude autorsko delo tada i njegov autor uživa određena prava koja proističu iz činjenice da je baš on njegov tvorac. To znači da će on uživati moralna i imovinska autorska prava.

##### a) *Moralna prava autora*

Moralna prava autora kompjuterskih programa su njegova isključiva i neotudjiva prava. Po Zakonu i Predlogu zakona autor ima sledeća moralna prava<sup>256</sup>: pravo pateniteta, pravo naznačenja imena, pravo na suprotstavljanje nedostojnom korišćenju kompjuterskog programa, pravo na objavljivanje, pravo na zaštitu integriteta kompjuterskog programa i pravo pokajanja.

Svaki autor ima **pravo na priznavanje autorstva - pravo paterniteta**. Ono se po Zakonu sastojalo od tri prava: *prava da sam obeleži svoj program* i da zahteva da sva lica koja ga iskorišćavaju, takođe, ga obeleže njegovim imenom; *prava da zabrani zloupotrebu svog imena* i *prava da se suprotstavi uzurpiranju ili nedopuštenom prisvajanju njegovog programa*<sup>257</sup>.

<sup>256</sup> Razlike između rešenja Zakona i Predloga zakona na prvi pogled ne izgledaju značajnim, međutim, to je samo prividno. Raskoraci su znatni. To je slučaj naročito sa moralnim i imovinskim pravima, kod kojih razlike ne proističu samo iz nužnosti regulacije novih prava, već i iz potpuno različitog pristupa svim pravima.

<sup>257</sup> Besarović V., op. cit., str. 255 i 256; Zakon o autorskom pravu, čl. 28 i 29.

Predlog zakona je predviđja dva različita prava: *pravo paterniteta* i *pravo na naznačenje imena*, a izostavio pravo na suprotstavljanje uzurpaciji i nedopuštenom prisvajanju računarskog programa, ostavljajući jedno slično, ali ne i isto pravo - pravo na suprotstavljanje nedostojnom iskorišćavanju dela.<sup>258</sup>

**Pravo na naznačenje imena** najbolje se realizuje kroz *odluku autora da stavi svoje ime, prezime ili pseudonim ili znak na program*<sup>259</sup>, i to na svaki primerak<sup>260</sup>. Prava na naznačenje imena autor se može u odredjenim slučajevima odreći. Kad su u pitanju računarski programi, s obzirom na specifičnost ovog autorskog dela, postavilo se pitanje gde će se to ime naći da bi ovo pravo bilo uvaženo.

Postoje shvatanja<sup>261</sup> da se ime naznačava na listingu i/ili pratećoj dokumentaciji - publikaciji (što više odgovara pravima u kojima se računarski program podvodi pod literarna dela) i to odmah na prvoj strani ispod naziva ili na poledjini strane na kojoj je naziv programa. Poseban problem nastaje kod programa koji nisu čitljivi za čoveka<sup>262</sup>. Za takve slučajeve, u većini zemalja koje su prihvatile označavanje listinga kao prioritetnog mesta za označavanje autora, predviđaju se dodatna pravila. Tako je npr. **Biro za autorska prava SAD-a izdao Uputstvo za pravilno smeštanje takvih naznaka**<sup>263</sup>. Po ovom Uputstvu za dela koja su na mašinski čitljivim kopijama, smeštenim na neki od medijuma i sa kojih se delo ne može uobičajeno vizuelno uočiti, autor može, za ubeležavanje svog imena, da bira jednu od sledećih varijanti:

- *poruka koja se pojavljuje na korisničkom terminalu;*
- *oznaka koja se kontinuirano nalazi na ekranu;*
- *oznaka koja se nalazi na kopijama u mašinski-čitljivom obliku i to takvom da se pojavljuje na vizuelno-perceptibilnim izlazima sa, ili veoma blizu, naslova ili pri kraju;*
- *čitka napomena koja je prilepljena na omote, kutije ili na neke druge "zaštitnike" kopija i medijuma.*

Mada predstavlja manji problem, Uputstvom je predviđeno i označavanje imena autora kod programa koji su u mašinskom jeziku. Kako se mašinski kod normalno generiše u računaru prevodjenjem, ovakva naznaka uključena je u izvorni kod. Pri tome,

<sup>258</sup> Predlog zakona, čl. 14 i 15.

<sup>259</sup> Isti tekst, samo u posebnoj odredbi, predviđen je i u Predlogu zakona, čl. 15.

<sup>260</sup> Predlog zakona, čl. 57, st. 1.

<sup>261</sup> Reed C., op. cit., str. 103.

<sup>262</sup> Edwards C., Savage N., Walden I., op. cit., str. 59 i 60.

<sup>263</sup> Scott M., op. cit., str. 3-68 i 3-69.

ova oznaka mora biti u formi koja se može prevesti. Na ovaj način može se unositi oznaka i u jezik izvornog koda programa u alfa numeričkom obliku koji obuhvata sva tri elementa oznake (©, ime i prezime autora i godina prvog objavljivanja). Nakon mašinskog prevodjenja oznaka se pojavljuje u mašinskom jeziku u obliku koji se može videti kada se program štampa ili se prikazuje.

Druga grupa shvatanja polazi od toga da je dovoljno da se ime autora nadje na terminalu<sup>264</sup>.

**Čini se da je za nas najpogodnija varijanta da se ime autora nadje i na listingu, pratećoj dokumentaciji i na terminalu**, u nekoj, za tu priliku, najpogodnijoj varijanti, kao što je to rešeno Uputstvom Biroa za autorsko pravo SAD-a. Ovakvo rešenje veoma pogoduje našem shvatanju da su kompjuterski programi posebna autorska dela, pa, otuda, za njih treba i da važe dodatna pravila. Jedno od njih je i ovo. Opravdanja za njega ima više, a jedno je i da se neki programi najviše eksploatišu u direktnom interfejsu korisnik - računar. Takođe, ne treba zaboraviti ni varijantu da se naznaka autora unese i na medijum (npr. omot diskete, CD-a) na koji je smešten sam program, mada to i nije naročito sigurno jer se takve nalepnice ili drugi sistemi mogu lako brisati, odlepljivati i jednostavno "izgubiti", kao i u uputstvu (na način kako se obeležava autor kod knjiga i drugih pisanih dela) koji ga prati. Iako našim Zakonom, niti Predlogom zakona, nije izričito predviđeno, a s obzirom da postoji mogućnost distribucije programa van granica naše zemlje, bilo bi poželjno da se uz ime nadje i oznaka copyright, odn. njegova opštepriznata skraćenica ©, kao i godina kada je program nastao. Pogotovo što smo i mi potpisnici UCC konvencije kojom je to predviđeno. **Svakako da bi usvojena rešenja trebalo da budu jednoobrazna bez obzira kod koga se kompjuterski program registruje, te bi posebnim Uputstvom koje bi pripremio i doneo Savezni zavod za intelektualnu svojinu<sup>265</sup>, to sve trebalo propisati.** Šteta je što u Predlogu zakona nije predviđena ova obaveza donošenja ovog Uputstva.

Na prvi pogled čini se da je problem mesta na kom će se naći oznaka autora marginalan u odnosu na druge probleme. Pogotovo što autori računarskih programa često, iz neznanja ili nemarnosti, ne stavljaju na svoj program naznaku svog imena. Medjutim, ovo postaje vrlo bitno za korišćenje drugih autorskih prava, ali i za dokazivanje autorstva u slučaju kad postoji kradja celog ili dela programa i njihovo preoznačavanje. Da bi se osigurali od takvih slučajeva autori ugrađuju u originalni

<sup>264</sup> Edwards C., Savage N., Walden I., op. cit., str. 59.

<sup>265</sup> Najcelishodnije bi bilo da ovo Uputstvo, kao i ostale detalje vezane za postupak registrovanja, izradi Savezni Zavod za intelektualnu svojinu.

izvorni kod programa namerne greške koje je teško otkriti bez instrukcija samog autora. Druga mogućnost je da se u originalnu verziju programa ugrade nepotrebni algoritmi koji neće imati uticaja na njihovu kompatibilnost, ali zato obezbeđuju lakše dokazivanje autorstva i otežavanje premeštanja ili brisanja naznake autora<sup>266</sup>.

***Pravo autora kompjuterskog programa da zabrani ili se suprotstavi takvom iskorišćavanju svog programa kojim se vredja njegova čast ili ugled***<sup>267</sup>, odn. kojim se ugrožavaju ili mogu ugroziti njegovi opravdani lični i moralni interesi je suština **prava na suprotstavljanje nedostojnom korišćenju kompjuterskog programa**. Ovo je pravo posebno izdvojeno i u Predlogu zakona.

**Pravo objavljivanja kompjuterskog programa je isključivo ovlašćenje autora da odluči da li će i na koji način objaviti svoj program**. Da bi se program, znači, pojavio u javnosti nužno je da to učini autor. Ovo pravo sadrži i imovinsko-pravna ovlašćenja, no, njegova je osnovna suština da jedino autor može tu odluku doneti<sup>268</sup>. Ovo pravo Predlog zakona dopunjuje sa odredjenjem da do objavljivanja samo autor može javno davati obaveštenja o sadržini svog dela ili ga opisivati. I to je isključivo pravo autora.

**Pravo na zaštitu integriteta kompjuterskog programa obuhvata isključivo pravo autora da menja program, da dozvoli preradu, da dozvoli njegovo skraćivanje**<sup>269</sup>. To, takodje, znači i suprotstavljanje javnog saopštavanja programa u izmenjenoj ili nepotpunoj formi<sup>270</sup>.

I naravno, kao u postojećem, ali ne i u budućem zakonu, predvidja se **pravo na pokajanje na osnovu koga autor svoj kompjuterski program može povući iz prometa, ukoliko njihovo korišćenje može naneti štetu njegovom ugledu**. Ovo se pravo moglo realizovati ili otkupom svih primeraka programa (što je u odnosu na pirateriju izuzetno teško ili gotovo neizvodljivo) ili uskraćivanjem daljeg korišćenja (što je isto toliko neizvodljivo). Naravno, ako se program ponovo nadje u prometu raniji korisnik ili sopstvenik ima prvenstveno pravo da se njim koristi. Znači, ako se autor

<sup>266</sup> Edwards C., Savage N., Walden I., op. cit., str. 59.

<sup>267</sup> Zakon o autorskom pravu, čl. 28.

<sup>268</sup> Zakon o autorskom pravu, čl. 27; Predlog zakona, čl. 16.

<sup>269</sup> Zakon o autorskom pravu, čl. 28.

<sup>270</sup> Predlog zakona, čl. 17.

pokaje, pa program povuče iz prometa, i onda se predomisli, prethodni korisnik će biti prvi koji pravo korišćenja treba da dobije.<sup>271</sup>

**b) Imovinska prava autora**

Autoru pripadaju i određena materijalna prava na osnovu kojih on ostvaruje svoj materijalnopравни interes. Od svih imovinskih prava koja pripadaju, autoru svakako je najkompleksnije i možda i najznačajnije **pravo iskorišćavanja kompjuterskog programa**. Zakon je predvideo da ovo pravo obuhvata: pravo objavljivanja; pravo preradjivanja; pravo reprodukovanja; pravo umnožavanja; pravo obradjivanja; pravo prikazivanja; pravo "izvodjenja"; pravo prenošenja; i pravo prevodjenja dela. Predlog zakona je ovom pravu pristupio drugačije, sistematičnije i modernije, praveći razliku između **prava iskorišćavanja dela u telesnoj formi** i **prava iskorišćavanja dela u bestelesnoj formi**. Dok se prvi vid ovog prava zadržava na: pravu na snimanje i umožavanje, pravu na stavljanje primeraka dela u promet i pravu davanja primeraka u zakup, dotle drugi vid prava obuhvata: pravo izvodjenja, pravo predstavljanja, pravo prenošenja izvodjenja i predstavljanja, pravo javnog emitovanja, pravo javnog saopštavanja dela koje se emituje i pravo javnog saopštavanja dela sa nosača zvuka i slike<sup>272</sup>.

Polazeći od specifičnosti računarskih programa može se konstatovati da su za njih vezana pet ključnih **prava iskorišćavanja**<sup>273</sup>: pravo reprodukovanja (pravo snimanja i umožavanja); pravo na prerađu, pravo na prevod, pravo stavljanja programa u promet i pravo davanja u zakup.<sup>274</sup>

**Pravo reprodukovanja kompjuterskih programa, odn. pravo snimanja i umožavanja** je pravo od izuzetnog značaja za autora ili nosioca autorskog prava na računarskom programu. Kako se reprodukovanje računarskih programa realizuje "kopiranjem" programa, a ono ima poseban smisao za programe, to se kod njih dva odvojena prava (reprodukovanje i presnimavanje - umnožavanje), u suštini, stapaju u jedno. Isto tako, zbog raznih, a najviše sigurnosnih razloga, svaki program bi trebalo i umnožiti da bi se obezbedio od uništenja, te je kopiranje sastavni

<sup>271</sup> Zakon o autorskom pravu, čl. 30. U jednoj verziji Prednacrta zakona bilo je izričito predviđeno da autor kompjuterskog programa nema pravo pokajanja. Sadašnjim Predlogom zakona pravo pokajanja se uopšte ne predviđa.

<sup>272</sup> Predlog zakona, čl. 20 - 30.

<sup>273</sup> Čini se da je ipak umesto prava reprodukovanja pogodniji termin pravo snimanja i umožavanja, kako je to prihvaćeno Predlogom zakona.

<sup>274</sup> Fikeys-Krmić N., op. cit., str. 98.

deo njegovog uobičajenog korišćenja. Pošto Zakon u odnosu na ova dva prava nije bio dovoljno precizan, *to se pod reprodukovanjem može podrazumevati kopiranje*<sup>275</sup>. Kopiranje u neograničenom broju primeraka nije dozvoljeno, pa makar to bilo i zbog namene za koju je nabavljen i od strane korisnika koji ga je nabavio. Znači, za kopiranje programa neophodna je dozvola autora ili nosioca autorskog prava, ali se, usled nepreciznosti u Zakonu, mora pokušati protumačiti šta bi ono obuhvatalo, odn. koliko kopija je dozvoljeno i da li je u određenim situacijama uopšte potrebno da se traži dozvola autora ili nosioca autorskog prava. U skladu sa shvatanjima prihvaćenim od strane većine zemalja, moglo bi se tumačiti da se program može instalirati (znači, za te potrebe dozvoljena bi bila samo jedna kopija) na samo jednom računaru i napraviti samo onoliko kopija koliko je to nužno za arhivske svrhe i za zamenu izgubljene, uništene ili dotrajale kopije (izgleda da je i ovde ostalo da se tumači koliko kopija je "nužno")<sup>276</sup>. I to samo za potrebe korisnika, a bez dozvole autora ili nosioca autorskog prava<sup>277</sup>. Za sve druge slučajeve umnožavanja neophodna je saglasnost autora ili nosioca autorskih prava, a u takvim prilikama davanje saglasnosti vezano je za određenu naknadu koju tražilac dozvole treba da plati.

Zanimljivo je da u Predlogu zakona **pravo na snimanje i umnožavanje**<sup>278</sup> računarskih programa posebno podrazumeva "*i smeštanje celog ili dela programa u memoriju računara, odn. puštanje programa u rad na računaru*"<sup>279</sup>. Naravno da je i za to nužna dozvola autora ili nosioca autorskih prava<sup>280</sup>.

**Pravo preradjivanja je pravo koje pretpostavlja da korisnik, u slučaju da želi da preradi program, morati da zatraži dozvolu autora**<sup>281</sup>. Medjutim, naš

<sup>275</sup> Erdelez S., op. cit., str. 878; Fikeys-Krmić N., op. cit., str. 98.

<sup>276</sup> U skladu sa čl. 9. Zakona o autorskom pravu.

<sup>277</sup> U nekim zemljama, kao što je Nemačka, i za sigurnosne kopije se zahteva dozvola autora, što može izazvati zastoje u radu i povećati rizik od opasnosti gubljenja.

<sup>278</sup> Inače, u čl. 20. Predloga zakona snimanje je beleženje dela na telesni nosač koji može biti papir, magnetna traka, vinilni disk, kompakt disk, filmska traka, kasete i slično. Umnožavanje nije definisano, ali je naznačeno da se ono može vršiti "naročito štampanjem, crtanjem, gravurom . . . , kao i mehaničkim i magnetnim beleženjem". **Bitno je da umnožavanje dela postoji nezavisno od broja primeraka dela, tehnike kojom se umnožava i trajnosti primeraka.**

<sup>279</sup> U obrazloženju člana 21, stav 3 (sada član 20, stav 5) jedne verzije Prednacrt zakona predlagač se poziva na Direktivu EZ po kojoj se (čl. 4. tč. a.) pod **umnožavanjem** podrazumeva "**učitavanje računarskih programa u računar, kao i rad programa na računaru**" jer se u tehničkoj osnovi tih procesa nalazi prolazno i kratkotrajno beleženje programa u memoriju računara.

<sup>280</sup> Medjutim, ovo je pravo u koliziji sa ograničenjem kada "lice koje je na zakonit način pribavilo primerak računarskog programa da, radi sopstvenog uobičajenog namenskog korišćenja programa, bez dozvole autora i bez plaćanja autorske naknade: smešta program u memoriju računara i pušta program u rad."

<sup>281</sup> Zakon o autorskom pravu, čl. 5, 27.

Zakon predviđa da ako se prerada programa od strane korisnika vrši radi korišćenja u svrhe zbog kojih je i nabavljen, onda će se to moći realizovati i bez te dozvole. Primenom ove odredbe donekle se ograničava autorovo pravo, i omogućuje zloupotreba, jer nije precizirano šta se podrazumeva pod terminima "prilagodjavanje i korišćenje u svrhu zbog koje je pribavljen". U kojim delovima i u kom obimu se ta prilagodjavanja mogu realizovati nije precizirano, već je svedeno na "opšti interes" koji važi za književna i umetnička dela koja se izvode i predstavljaju u vidu nastave, i sl., što je sasvim druga priroda i druga svrha nego korišćenje računarskih programa. Ovakav stav je suprotan uobičajenom shvatanju da je za preradu programa neophodna dozvola autora, a samo izuzetno korisnik će to moći da učini i bez nje.

Ovo pravo, međutim, nije posebno regulisano u Predlogu zakona sem u okviru moralnog prava na zaštitu integriteta dela, kao i u slučaju kad se prerada, odn. izmena vrši bez dozvole autora i bez naknade a od strane lica koje je legalno program pribavilo. U tom slučaju lice će, samo ili preko drugog stručnog lica koje radi po njegovom nalogu, otkloniti greške u programu i izvršiti druge neophodne izmene. Ovo će biti moguće, naravno, ako nije ugovorom drugačije određeno. Ovakvo rešenje postaje utoliko opasnije ukoliko iz tih izmena nastane delo prerade, koje, takodje, predstavlja autorsko delo<sup>282</sup>. Posebnu opasnost nosi program dobijen reverzibilnim programiranjem, ukoliko je program prerade, jer mu se priznaje svojstvo autorskog dela.

**Prevod kompjuterskog programa je moguć ukoliko postoji dozvola, kao isključivo pravo, autora.** Prevod izvornog programa samatra se novim autorskim delom, naravno, ukoliko zadovoljava za to predviđene uslove<sup>283</sup>. Izuzetno se prevodjenje može izvršiti i bez dozvole. Međutim, što se prevodjenja programa tiče, pored ovih opštih pravila koja važe za svaki prevod, za njih se vezuju i određene osobenosti. Tako, npr. prebacivanje izvornog koda programa sa jednog na drugi programski jezik ne predstavlja samo njegov prevod, već i preradu. U stvari, veoma često je potrebna posebna intervencija u smislu iznalaženja novih rešenja pogodnih za taj programski jezik, a nekad su te intervencije neznatne jer ih vrše specijalni aplikativni programi za prevodjenje iz jednog u drugi određeni programski jezik (npr. iz *FORTRAN*-a u *COBOL*). Uobičajene su, pak, takve intervencije koje predstavljaju sasvim nova i drugačija rešenja od onih koja se nalaze u prvobitnom programskom jeziku. Otuda je neophodno da se dobije dozvola od autora ili nosioca originalne verzije. Isto tako, jedno je vreme preovladavalo shvatanje da je prebacivanje izvornog u objektni kod, u suštini,

<sup>282</sup> Predlog zakona je **delo prerade** definisao *kao delo u kome su prepoznatljivi karakteristični elementi preradjenog (izvornog) dela*.

<sup>283</sup> Zakon o autorskom pravu članovi: 5, 27, 42, 43, 44, 45, 46 i 47; Predlog zakona, čl. 5.

prevod<sup>284</sup>. Kasnije se počelo isticati da je, iako se prebacivanje vrši nakon sintaksne analize, ono nije prevod jer se radi o prebacivanju iz jednog u drugi oblik u srazmeri 1:1, odn. jednoj naredbi izvornog odgovara jedna naredba objektnog koda. Takođe, ovom "prevodu" se to svojstvo negiralo i zbog pomanjkanja čovekovih intelektualnih kreativnih napora i originalnosti. Ovo bi drugo shvatanje moglo biti prihvaćeno i kod nas<sup>285</sup>.

Predlog zakona, dosledno primenjujući pristup priznavanja "opštih prava"<sup>286</sup> nije specificirao pravo na prevodjenje. Jedino je priznao svojstvo autorskog dela delu prerade, prevoda ili prilagođavanja, naravno, ako ispunjava uslove i ne ograničava prava autora izvornog dela (programa)<sup>287</sup>.

**Pravo puštanja (odn. stavljanja) u promet primeraka kompjuterskog programa** je isključivo pravo autora koje nije bilo eksplicitno navedeno u Zakonu, za razliku od Predloga zakona koji ga navodi u okviru grupe prava na iskorišćavanje dela u telesnoj formi<sup>288</sup>. *Suština ovog prava autora je da drugome dozvoli ili zabrani da stavi primerke njegovog programa u promet.* Samo stavljanje u promet se određuje u Predlogu zakona kao: nudjenje primeraka dela (programa) radi stavljanja u promet, skladištenje primeraka dela (programa) radi stavljanja u promet i uvoz primeraka dela (programa). Ovo pravo se odnosi samo na vlasnike programa koji ih nisu nabavili legalno ili od ovlašćenih lica. Znači, vlasnik legalno pribavljenog računarskog programa može ga slobodno dalje stavljati u promet.

**Pravo davanja u zakup kompjuterskog programa** nije, kao posebno pravo, predviđeno u Zakonu, ali je zato predviđeno u Predlogu zakona. Mada na prvi pogled prevaziđeno omasovljavanjem korišćenja PC i standardnih programa, ovo pravo bi moglo imati značaja za posebne, aplikativne programe izradjene namenski. Naime, *autor imajući isključivo pravo zabrane ili davanja dozvole za davanje svog programa u zakup, treba da ima i upliva u dobit koja se ostvaruje zakupom.* Medjutim, to učešće

<sup>284</sup> Ovo je usvojio i *UK Copyright, Design and Patents Act*, po čijem ss. 21 (3) i (1): "prevod obuhvata i verziju programa u ili van programskog jezika ili koda u drugom kompjuterskom jeziku ili kodu, koje nisu privremenog karaktera i nastale u toku izvršavanja programa."

<sup>285</sup> Marković S., op. cit., str. 133.

<sup>286</sup> Po V. Besarević (op. cit., str. 261.) u okviru načina iskorišćavanja dela pojavile su se dve grupe zemalja. Po jednoj, različiti načini iskorišćavanja grupišu se u dve kategorije "opštih" prava: pravo iskorišćavanja u bestelesnoj formi i pravo iskorišćavanja u telesnoj formi. Ovoj grupi pripada Zakon o autorskim pravima Nemačke i sada Predlog zakona SRJ. Druga grupa zemalja, kojoj smo i mi pripadali, nabroja pojedine oblike iskorišćavanja dela, te se kao jedan od njih pojavljuje i prevodjenje.

<sup>287</sup> Predlog zakona, čl. 5, st. 3.

<sup>288</sup> Predlog zakona, čl. 21.

u dobiti imaju autori koji svoje pravo ustupe proizvođaču fonograma ili videograma, ali ne i autor koji svoj program ustupi softverskoj firmi, odn. proizvođaču softvera. Nepriznavanjem ove mogućnosti autoru računarskog programa, on se definitivno stavlja u podređen položaj u odnosu na autore dela kakva su fonogrami ili videogrami. Zašto bi autor zabeleženog zvuka, odn. određenog niza zvukova (kako je Predlog zakona definisao fonogram) ili zabeleženog niza slika, sa ili bez pratećeg zvuka, na nosaču slike, odnosno nosaču slike i zvuka (kako je videogram definisao Predlog zakona) imao više prava nego autor računarskog programa?. Posebnih opravdanja nema, ali je Predlog zakona, ipak, ovoj kategoriji autora uskratio pravo učešća u dobiti postignutoj davanjem primeraka programa u zakup.

Iako prava iskorišćavanja dela u bestelesnoj formi ne mogu, ili teško mogu da se primene i na računarske programe, ipak postoji jedno od tih prava predviđeno Predlogom zakona koje bi moglo da se "protegne" i na njih. To je **pravo javnog saopštavanja dela na nosaču zvuka ili slike**. Ovo pravo je sastoji se u mogućnosti autora da zabrani ili dozvoli da delo, zabeleženo na kompakt ili optičkom disku ili nekom drugom nosaču, javno saopšti uz pomoć tehničkih uređaja za reprodukovanje zvuka ili slike<sup>289</sup>.

Medju pravima koja izlaze iz grupe prava na iskorišćavanje predviđa se jedno koje, iako predviđeno za originale dela likovne umetnosti i izvorne rukopise književnih, naučnih i muzičkih dela, bi moglo da se odnosi i na računarske programe. To je **pravo sledjenja**. Naime, vrednost originalnog izvornog koda leži u njegovoj prirodi jer njegovo posedovanje znači širom otvorena vrata za sve dobronamerne ili zlonamerne, naročito nedozvoljene, aktivnosti. *Autor treba da bude obavešten da je sopstvenik ili korisnik njegov izvorni kod dalje preprodao*. Prodavac mora da omogući autoru deo od novoprodajne cene. Visinu procentualnog učešća određuje odgovarajući nadležni organ. Pravo sledjenja je neprenosivo za života autora, niti ga se on može odreći. Ono se može nasledjivati. Njegov je značaj u tome što se pruža mogućnost autoru da, ipak, dobije pravičniju naknadu za svoje delo. Često autor u teškoj situaciji proda ili ustupi izvorni kod, po nižoj ceni od realne vrednosti, sopstvenik ili korisnik ga dalje preprodaje, najčešće kao objektni kod, i time se neosnovano bogati. Prodajom izvornog koda autor je sam sebe onemogućio u daljem iskorišćavanju svog programa. S druge strane, vlasnik ili korisnik daljom preprodajom mogu postizati velike imovinske koristi. Taj nesklad bi se mogao prevazići aktiviranjem ovog prava.

---

<sup>289</sup> Predlog zakona, čl. 29.

Veoma slična rešenja su prihvaćena i u Predlogu zakona<sup>290</sup>, s tim, što autor ima pravo da bude obavešten u roku od 30 dana od dana prodaje od vlasnika primerka njegovog originalnog dela. To obaveštenje obuhvata ime i adresu novog valasnika. Zar se to ne približava sve alarmantnijoj potrebi kontrolisanja korišćenja programa i sprečavanja kriminala u vezi i sa njim? Rešenja koja su nalažena u *clipper* čipu samo mogu poslužiti kao povod da se ovo pravo dodeli i autorima računarskih programa. U tom slučaju oni bi, takodje, potraživali iznos 3% od prodajne cene, čime bi se ublažile i mnoge nepravde koje im se nanose. Naravno, ne treba zanemariti brojne teškoće koje bi u realizaciji ovog prava nastale, no, one nisu nesavladive.

Za sva ostala prava koriste se odredbe Zakona, odn. Predloga zakona, koje važe i za druga autorska dela, iako je trebalo poveriti računa da se neka od tih prava u zakonima drugih zemalja znatno preciznije određuju i dobijaju drugačiji kontekst, s obzirom na osobenosti.

### c) Ograničenja autorskog prava

Svaki autor ima pravo da svoja prava realizuje bez zastoja, u potpunosti i onako kako sam želi. To jeste njegovo pravo koje u nekim, strogo predviđenim, situacijama može biti ograničeno. **Ograničenje znači da se bez dozvole i bez naknade** (izuzetno uz naknadu) **delo može umnožiti, javno saopštiti ili stavi u promet**<sup>291</sup>. Kad su u pitanju računarski programi to su sledeća ograničenja<sup>292</sup>:

1. *umnožavanje i javno saopštavanje radi sprovođenja službenog postupka* pred sudskim ili drugim državnim organima (po Zakonu i Predlogu zakona);

<sup>290</sup> Predlog zakona, čl. 31 i 32.

<sup>291</sup> Ograničenja predviđaju i druga prava. Tako, npr. američki Zakon o autorskim pravu (sa amandmanima iz 1992. i 1993. godine) predvideo je kao **opšta ograničenja: fer korišćenje** između ostalog i za potrebe: nastave, istraživanja, kritike, komentarisanja, novinskog izveštavanja, školovanja (sect:107) i **reprodukovanje za potrebe biblioteka i arhiva** (sect:108). **Posebno vezana za računarske programe** su ograničenja: **transfera privatnih primeraka za potrebe zakupa ili zajma za neprofitne svrhe biblioteka ili obrazovnih institucija** (sect: 109); **pravljenja novih primeraka kompjuterskog programa ili njihova prerada** kad je takva kopija ili prerada kreirana kao osnovni korak u upotrebi mašine, ali nikako ne i za druge svrhe, ili za arhiviranje kad su sve arhivske kopije uništene i time se dovodi u pitanje posedovanje programa. Ovakve kopije mogu se iznajmljivati, pozajmljivati, prodavati samo kao deo neke pozajmice, zakupa ili prodaje ili bilo kog oblika prenosa. Prerade se ne mogu prenositi bez saglasnosti nosioca prava (sect: 117). Kompletni članovi US Copyright Act, as Amended, preuzeti su sa Interneta.

<sup>292</sup> Ograničenja su u Predlogu zakona regulisana članovima 35 - 52, i grupisana u: zajedničke odredbe; suspenzije isključivih prava i prava na naknadu i zakonsku licencu.

2. *umnožavanje i korišćenje za potrebe nastave* (ograničenje je proisteklo iz Zakona po kome je to dozvoljeno uz naknadu<sup>293</sup>, ali uz naznaku autora i porekla pozajmice, ali je po Predlogu zakona ostavljeno samo za dela sa nosača zvuka i slike);
3. *umnožavanje primeraka dela za potrebe ličnog obrazovanja i slične svrhe*, s tim što se ovi primerci ne smeju stavljati u promet niti koristiti za neke druge, pogotovo komercijalne, svrhe (ograničenje je predviđeno Zakonom, ali je eksplicitno, iz teško objašnjivih razloga, u Predlogu zakona isključeno za računarske programe, kao npr. i za novu građevinu koja se pravi po uzoru na postojeću koja je autorsko delo<sup>294</sup>);
4. *smeštanje programa u memoriju računara i puštanje programa u rad* od strane lica koje ga je legalno pribavilo i koje to čini zbog uobičajenog namenskog korišćenja<sup>295</sup> (ovo je novo ograničenje predviđeno Predlogom zakona);
5. *otklanjanje grešaka u programu, kao i vršenje neophodnih ispravki*, od strane lica koje ga je legalno pribavilo i koje to čini zbog uobičajenog namenskog korišćenja (mada slično jednom od ograničenja po Zakonu, ipak je novo);
6. *umnožavanja radi zamene izgubljene, uništene ili dotrajale kopije*, odn. *pravljenja rezervnog primerka* (po Zakonu je to bilo onoliko kopija koliko je nužno, bar te tri kopije, po Predlogu samo jedna);
7. *izvršavanja dekompilacije radi pribavljanja neophodnih podataka za postizanje interoperativnosti tog sa drugim, nezavisno stvorenim, programom ili određenim računarskom opremom, ako se do njega ne može doći na drugi način i ako se taj podatak ne saopštava drugima ili koristi za druge svrhe* (ovo nije bilo izričito dopušteno po Zakonu, ali je bilo posredno zabranjeno, dok je Predlog zakona ovim dopuštanjem legalizovao reverzibilni inženjering, odn. reverzibilno programiranje, doduše od strane lica koje je legalno pribavilo program i koje to čini zbog uobičajenog namenskog korišćenja, odn. drugog stručnog lica koje radi po njegovom nalogu);
8. *umnožavanje za arhivske svrhe* (ovo ograničenje nije predviđeno Predlogom zakona);
9. *preradjivanje radi korišćenje u svrhe za koje je nabavljen* (ovo ograničenje nije predviđeno Predlogom zakona);

<sup>293</sup> Zakon o autorskom pravu, čl. 48., tč. 1.

<sup>294</sup> Izostavljanje ove mogućnosti više liči ili na nerazumevanje karakteristika računarskih programa i isključenih sličnih dela (što je manje verovatno), ili na unošenje ovog izuzeća pod nekim pritiskom (što je više verovatno).

<sup>295</sup> Na žalost, u Predlogu zakona nije detaljno definisano šta se pod "sopstvenim uobičajenim namenskim korišćenjem" podrazumeva, tako da se nepreciznosti karakteristične za Zakon ponavljaju.

10. umnožavanje i prikazivanje radi demonstriranje rada uređaja, ali samo u prodavnicama, na sajmovima (novo ograničenje ustanovljeno Predlogom zakona. Svi snimci koji se zbog toga načine moraju se bez odlaganja brisati<sup>296</sup>.);
11. *umnožavanje i stavljanje u promet primeraka računarskog programa u slučajevima zakonske licence* (po Predlogu zakona).

Naravno, sva ova ograničenja odnose se na imovinska prava autora ili nosilaca autorskih prava, s tim što ih je po Predlogu zakona predviđen veći broj<sup>297</sup>. Ma koliko ograničenja bila neophodna ona predstavljaju i svojevrsnu opasnost zbog mogućih zloupotreba i izbegavanja obaveza prema autorima ili nosiocima autorskih prava. Tome posebno mogu doprineti nedorečenosti u određivanju pojedinih termina, čime se otvara širok front za malverzacije.

#### 3.4.4.4. *Kompjuterski programi nastali u radnom odnosu*

Ova, a i druga imovinska, prava se donekle modifikuju<sup>298</sup> uvođenjem **"primarnog" nosioca autorskog imovinskog prava**. Taj primarni nosilac (treba ga razlikovati od autora koji je "izvorni" nosioci) je pravno lice, odn. poslodavac kod koga je, ili za koga je, računarski program izradjen<sup>299</sup>. Ovo je znatno odstupanje od uobičajenog shvatanja da se pored autora pojavljuju i nosioci imovinskih prava, na koje autor dobrovoljno prenosi deo svojih ovlašćenja. Ako je kompjuterski program nastao u radnom odnosu nosilac svih imovinskih autorskih prava je pravno lice ili poslodavac kod koga je autor zaposlen. Već ionako nepovoljan položaj autora kompjuterskih programa još se pogoršava time što mu se materijalna prava, odn. prava iskorišćavanja, nakon protoka određenog vremena "ne vraćaju". Naime, za sva ostala autorska dela nastala u radnom odnosu izvorni nosilac svih imovinskih prava je autor, a preduzeće ili poslodavac ima pravo da u okviru svoje redovne delatnosti, a u periodu od 5 godina, iskorišćava to delo (u određenom roku i za određene svrhe), i to bez dozvole, ali uz naknadu autoru. Dogle, samom činjenicom da je kompjuterski program nastao u radnom odnosu i pri obavljanju redovnih obaveza u preduzeću, ili kod poslodavca, **ono/on**

<sup>296</sup> Predlog zakona, čl. 46.

<sup>297</sup> Postavlja se pitanje zbog čega je toliki broj ograničenja prihvaćen u našem Predlogu zakona i zašto to nisu ograničenja koja su opšteprihvaćena u nacionalnim i međunarodnim aktima? S druge strane, zabrinjavajuća je sve lošija pozicija autora, naročito takvih dela kakva su kompjuterski programi, i bolja, kompletnija, zaštita svih drugih subjekata.

<sup>298</sup> Zakon o izmenama i dopunama Zakona o autorskom pravu, čl. 4 i 7.

<sup>299</sup> Erdelez S., op. cit., str. 877.

**postaje nosilac imovinskih prava i to na neograničeni rok, bez obaveze plaćanja naknade, za bilo koju svrhu i sadržajno neograničeno.** Čak se isključuje i mogućnost da se o naknadi i ostalim autorskim pravima odlučuje na osnovu opšteg akta preduzeća, odn. ugovora sa poslodavcem. Tako je Zakon ozvaničio i poseban status autora računarskih programa, nažalost, ne baš povoljan, u odnosu na autore drugih dela.

Predlog zakona bio je još rigorozniji predviđajući da poslodavac, činjenicom da je računarski program nastao tokom trajanja radnog odnosa i pri izvršavanju autorovih radnih obaveza, dobija ovlašćenje ne samo na imovinskim pravima iskorišćavanja, već i pravo da objavi program. Naravno, prava iskorišćavanja može poslodavac realizovati u okviru svoje registrovane delatnosti. Kad su u pitanju računarski programi i dalje se prava iskorišćavanja prenose na poslodavca neograničeno i bez naknade<sup>300</sup>.

---

<sup>300</sup> Predlog zakona, čl. 92.

#### 3.4.4.5. *Kompjuterski programi nastali po ugovoru o delu*

Zakonodavac je bio gotovo dosledan jer je i **za kompjuterski program nastao po ugovoru o delu predvideo da je nosilac autorskog imovinskog prava naručilac, osim ako ugovorom nije drugačije određeno**. Nasuprot tome, kad je u pitanju bilo koje drugo autorsko delo koje je stvoreno po ugovoru o autorskom delu sva autorska prava pripadaju autoru, sem ako u ugovoru nije drugačije određeno. Razlika u odnosu na računarski program nastao u radnom odnosu, kad se bezpogovorno i bezpovratno imovinska autorska prava prenose na preduzeće, odn. poslodavca, je u tome što se autorska prava na programu nastalom po ugovoru o delu prenose na naručioca, ali je ostavljena mogućnost da se ugovorom i drugačije odredi. Znači, u ovom slučaju Zakon je bio nešto fleksibilniji.

Situacija je potpuno ista i sa Predlogom zakona, po kome ako je računarski program predmet ugovora o narudžbini, naručilac stiče sva prava iskorišćavanja, sem ako nije drugačije ugovoreno. Ovom članu dodaje se i član koji se odnosi na računarski program (bazu podataka, enciklopediju, i sl.) koji je nastao spajanjem "priloga" većeg broja autora. Takav program se tretira kao kolektivno autorsko delo. Autori delova isključivo ustupaju sva imovinska prava licu koje je organizator izrade kolektivnog dela<sup>301</sup>.

#### 3.4.4.6. *Trajanje*

Trajanje moralnih autorskih prava je **neograničeno**. Opšti rok trajanja autorskih imovinskih prava za računarske programe, kao i za druga autorska dela, je "za života autora" i 50 godina nakon smrti. Specifičnost koju je prihvatio Zakon odnosi se na računarske programe čiji je nosilac pravno lice. Za takve programe autorska imovinska prava traju 50 godina **posle ostvarivanja** računarskog programa<sup>302</sup>, za razliku od drugih autorskih dela kod kojih, ukoliko je nosilac imovinskih prava pravno lice, autorsko pravo prestaje po isteku 50 godina po objavljivanju dela.

Iako se očekivalo da će Zakon usvojiti kraći rok trajanja autorskih imovinskih prava to se nije desilo. Naime, veoma dugo i mnogo se ukazivalo na karakteristike programa koje skoro bespredmetnim čine ovako dugi rok trajanja imovinskih prava.

<sup>301</sup> Predlog zakona, čl. 89 i 91.

<sup>302</sup> Zakon o izmenama i dopunama Zakona, čl. 12.

Kako su računarski programi deo stvaralaštva koji podleže najbržem menjaju, te njihova originalnost, ali i korišćenje, izuzetno brzo zastarevaju ili prestaju. Svedoci smo da su se u vrlo kratkom intervalu promenile čitave generacije računara i pratećih programa. U tendenciji takvog razvoja, ali i rapidnog pojeftinjenja i jednih i drugih, teško je zamisliti da će se korisnici opredeliti za upotrebu zastarelih računara i programa. **Zato se čini da je dužina trajanja imovinskih prava preterana i da u suštini ne doprinosi, čak, ni ekonomskoj koristi svojim nosiocima**, pogotovo ako su to pravna lica. S druge strane, ako se gleda i interes društva ni tada ovaj rok nije baš adekvatan naročito za neke računarske programe koji su postali gotovo "klasika" u smislu kako se pod "klasikom" podrazumevaju neka dela od izuzetne vrednosti. Za takve programe, ali i one koji donose profit, sigurno postoji zainteresovanost društva (države) da oni što pre postanu opšte dobro.

Ostavljajući ovaj problem po strani, neophodno je razjasniti šta se pod terminom **"ostvarivanja kompjuterskih programa"** podrazumeva. U suštini, ovaj termin preuzet je iz zakonodavstva nekih zemalja i, donekle, iz Direktive EU, te bi bilo sasvim logično da se pod njim podrazumeva ono što se i u izvornim tekstovima podrazumeva. Međutim, Direktiva koristi drugi termin - **"od datuma kreiranja"**, odn. stvaranja (*creation*). Slično je i sa zakonima. Naš Zakon koristi termin **ostvarivanje** (*realize, accomplish*) što i u engleskom i u našem jeziku ima različita značenja. Čini se da je primereniji svojstvu autorskih dela termin **"datum nastanka"**, s tim, da se, ipak, mora definisati šta se pod tim podrazumeva.

Kao datum isticanja vremena kad je u pitanju period 50 godina nakon smrti autora, računa se od 1og januara one godine koja neposredno dolazi nakon godine u kojoj je autor umro, odn. kad je u pitanju koautorsko delo, od godine kad je poslednji autor umro. To isto važi i za programe nad kojima imovinska prava imaju pravna lica, odn. isticanje vremena biće 1og januara naredne godine od godine po kojoj se računa da je program ostvaren<sup>303</sup>.

**Predlog zakona nije specifikovao razlike izmedju trajanja imovinskih prava autora računarskog programa i ostalih autorskih dela**<sup>304</sup>. Dakle, moralna prava traju i po prestanku imovinskih prava<sup>305</sup>, a ona traju za života autora i 50 godina posle njegove smrti. Kad su u pitanju koautori, onda je to 50 godina nakon smrti autora koji je poslednji umro. Ako se autor, pak, ne zna, imovinska prava prestaju po isteku 50

<sup>303</sup> Ovakvo računanje u skladu je sa članovima 6 i 7 Bernske konvencije.

<sup>304</sup> Predlog zakona, čl. 95 - 102.

<sup>305</sup> Ovakvo definisanje trajanja je u najmanju ruku neobično, jer je mnogo neodređenije nego formulacija - neograničeno.

godina od dana objavljivanja. Nema odredbi o trajanju imovinskih prava ako je nosilac pravno lice. Datumi se računaju na isti način kao i u Zakonu.<sup>306</sup>

O pravu paterniteta, integriteta dela, suprotstavljanja svakom obliku nedostojnog iskorišćavanja dela stara se svako lice, kao i udruženja autora i institucije iz oblasti nauke i umetnosti. Ova udruženja i institucije se staraju i o imovinskim pravima posle isteka roka trajanja<sup>307</sup>.

Novina koja je uneta Predlogom zakona je da se za korišćenje autorskog dela, po isteku roka trajanja imovinskih autorskih prava, plaća naknada. Visina naknade ne sme biti veća od 1% od dobiti koja se ostvari korišćenjem. Naknada je prihod saveznog budžeta<sup>308</sup>.

#### *3.4.4.7. Prenošnje autorskih prava na kompjuterskim programima*

**Prenošnje autorskih prava na kompjuterskim programima**, kao i drugim autorskim delima, *može se vršiti, sa ili bez naknade, na druga pravna lica ili pojedince i to dogod autorska prava traju ili na odredjeno vreme*. Ovo se, naravno, ne odnosi na računarske programe nastale u radnom odnosu. Prenošnjem prava iskorišćavanja računarskog programa na jedno lice ne znači da ga ono može dalje prenositi na treća lica bez saglasnosti autora, odn. nosioca autorskog prava<sup>309</sup>. Ova zabrana je naročito značajna u raščišćavanju dalje sudbine računarskog programa od strane lica na koga je pravo iskorišćavanja preneto od strane autora, bez obzira da li je preneto u celini ili delimično, uz naknadu ili bez nje, na odredjeno vreme ili dok autorsko pravo traje. To može značiti i da se samo neko od prava korišćenja prenosi na drugoga, dok ostala može autor zadržati za sebe. Tako, ako se prenese pravo na prevodjenje sa jednog na drugi programski jezik, autor može to svoje pravo iskoristiti samo za jedan jezik. U slučaju da se želi prevodjenje na treći programski jezik mora se tražiti naknadna dozvola od autora i platiti mu odgovarajuća naknada.

---

<sup>306</sup> Predlog zakona, čl. 99.

<sup>307</sup> Predlog zakona, čl. 100.

<sup>308</sup> Predlog zakona, čl. 101.

<sup>309</sup> Zakon o autorskom pravu, čl. 52.

Autor računarskog programa može pravo korišćenja preneti na drugo lice i onda ako program nije završen ili tek treba da ga kreira (**budući programi**). Vrstu i uslove, kao i obim prava, autor računarskog programa određuje ugovorom, u kome se detaljno regulišu sva relevantna pitanja za obe strane. U ovakvim ugovorima može se eksplicitno predvideti i mogućnost da se prenesu prava i na treća lica.

Lice na koje se pravo iskorišćavanja prenosi nije ovlašćeno<sup>310</sup> da prilikom korišćenja unosi u autorsko delo bilo kakve **izmene**, ako to nije u ugovoru posebno određeno. To znači da se ni prenošenjem prava korišćenja na računarskim programima ne omogućuje da se program bilo kako izmeni, odn. to uradi bez dozvole autora. Ukoliko se to učini onda je u pitanju povreda prava autora, što povlači i određenu sankciju.

Drugim rečima, **predvidja se isključivo pravo autora** da na drugoga prenese pravo iskorišćavanja računarskog programa i korisniku dozvoli da program u određenom delu i obimu izmeni i preradi. Značaj ove odredbe je u tome što, s jedne strane, samo je autor ovlašćen da daje ove dozvole, a ne i nosilac autorskih prava, i s druge strane on određuje u kom delu i u kom obimu će njegov program biti izmenjen ili preradjen. Naravno, ni ovo ne važi za računarski program nastao u radnom odnosu, jer su ova ovlašćenja u rukama primarnog nosioaca.

Osim prenosa prava medju živima, pojavljuje se i jedan poseban oblik - prenos u slučaju smrti. To znači, ako autor umre autorska prava se prenose na njegove **naslednike**<sup>311</sup>. Naslednici imaju<sup>312</sup>: **a) pravo da vrše** (znači, nema prenosa) **ličnopravna ovlašćenja**, sem ovlašćenja na objavljivanje neobjavljenog, po volji autora, računarskog programa, i ovlašćenja na izmenu programa; **b) pravo na sva imovinskopravna ovlašćenja**.

Predlog zakona, sem istovetnih odredbi vezanih za prenos moralnih prava (koja se ne mogu preneti ugovorom), kad su u pitanju imovinska prava autora pravi razliku između ustupanja svih ili samo pojedinih prava, da li je ono isključivo ili neisključivo, kao i da li je predmetno, prostorno ili vremenski ograničeno. Ono što je bitno da lice koje je ustupanjem steklo imovinsko pravo od autora ili njegovih

<sup>310</sup> Zakon o autorskom pravu, čl. 53.

<sup>311</sup> Zakon o autorskom pravu, čl. 80.

<sup>312</sup> Ova određjenja prava naslednika preuzeta su iz Predloga zakona, čl. 52., jer je Zakon o autorskom pravu to ostavio odredbama zakona o nasleđivanju.

naslednika može to svoje pravo preneti na drugog samo ako ima dozvolu (autora ili naslednika)<sup>313</sup>.

#### 3.4.4.8. *Zaštita prava*

Autor računarskog programa **ima pravo na zaštitu ukoliko su mu moralna i imovinska prava povredjena**. Zaštita može biti **gradjanskopravna ili krivičnopravna**.

**Gradjanskopravnu zaštitu** imaju: autor, koautori, njihovi pravni sledbenici (naslednici, nosioci autorskih prava i posle njegove smrti organizacija autora kojoj je pripadao). **Zaštita se traži sudskim putem i to tužbom**<sup>314</sup>. Koja će to vrsta tužbe biti zavisi od prirode povrede. To može biti<sup>315</sup>:

1. tužba za *naknadu štete*;
2. tužba za *utvrđivanje*;
3. tužba za *osudu*;
4. tužba za *ustanovljavanje, preinačavanje ili preobražaj*; i
5. tužba na *činidbu*.

Šteta za koju može, autor ili ovlašćeno lice, da traži *naknadu* može biti: **obična šteta** (kojom se umanjuje njegova imovina), **izmakla dobit** (sprečavanje povećanja imovine) ili **povreda ličnih (moralnih) prava ili interesa** (da bude poznat kao autor) i koja je nematerijalnog karaktera. Da bi se zaštita mogla tražiti neophodno je: **1)** da je autor ili ovlašćeno lice **pretrpelo** štetu radnjom odgovornog lica, **2)** da su tom radnjom **povredjena** imovinska ili moralna prava, **3)** da je radnja **učinjena** na način protivan zakonu, **4)** da postoji **krivica**, **5)** da postoji **uzročna veza** između radnje i štete, i **6)** da, kao **posledica**, postoji povreda određenih prava autora. Šteta za povredu autorskih prava na računarskim programima može pravično da se naknadi o čemu odlučuje sud. Veoma često, kad su u pitanju autorska prava na računarskim programima, sud traži veštačenje (u drugim zemljama pošto su kod nas još uvek ovakvi sporovi retki), kako bi utvrdio visinu štete i naknade.

<sup>313</sup> Predlog zakona, čl. 52 - 61.

<sup>314</sup> Zakon o autorskom pravu, čl. 95.

<sup>315</sup> Milić D., Komentar Zakona o autorskom pravu, sa sudskom praksom, Beograd, Službeni list, 1987., str. 199 - 210.

Kad je u pitanju nematerijalna šteta, odn. povreda moralnih prava može se pored naknade narediti i: **1)** da se *presuda objavi* na trošak tuženog, **2)** da se tuženom *zabrani* dalja povreda autorskih prava, i **3)** da se predmeti kojima je nanešena šteta *unište ili preinače* (da se npr. program sa lažnim oznakama autorstva preinači tako što će se staviti pravi autor). Kao jedan vid zaštite naš Zakon predviđa i privremene mere oduzimanja spornog računarskog programa, njegovo isključenje iz prometa ili zabranu obavljanja započetih radnji kojima bi se mogla šteta, dok traje spor, naneti. Ovo poslednje je naročito važno kad je u pitanju kompjuterski program na kome nema označenog imena autora.

Prednacrt zakona je bio rigorozniji predviđujući da se tužbom može zahtevati:

1. *utvrđenje povrede prava (povreda prava* je iskorišćavanje zaštićenog računarskog programa upotrebom neovlašćeno umnoženih primeraka, kao i posedovanje i stavljanje u promet sredstava čija je isključiva namena olakšavanje uklanjanja ili onesposobljavanja tehničke zaštite računarskog programa ili druge vrste predmeta zaštite od neovlašćenog iskorišćavanja - dakle, tzv. "**nadmudrivanje zaštite od kopiranja**"<sup>316</sup>);
2. *prestanak povrede prava*;
3. *uništenje ili preinačenje predmeta* kojima je povreda izvršena (uključujući i primetke računarskog programa, njegovu ambalažu, disketu, i sl.)<sup>317</sup>;
4. *uništenje ili preinačenje alata i opreme* uz pomoć kojih su proizvedeni programi ili medijumi kojima je izvršena povreda prava, ako je to nužno za zaštitu (dakle, mogu biti uništeni i računari i druga oprema kojom se reprodukuju neautorizovani računarski programi);
5. *naknadu štete* (ako je u pitanju neimovinska šteta ona se dosudjuje u srazmeri sa intenzitetom duševne patnje kojui je autor pretrpeo zbog povrede svojih moralnih prava);
6. *objavljivanje presude o trošku tuženog*.

Pored uobičajenih sankcija vezanih za građanskopravnu zaštitu sud može izreći i *privremene mere oduzimanja ili isključenja* iz prometa programa kojima se vrši

<sup>316</sup> Prednacrt zakona, čl. 175.

<sup>317</sup> Tužilac može umesto zahteva za uništenje ili preinačenje kompjuterskog programa kojim je izvršena povreda prava zahtevati da mu povredilac preda te programe, Predlog zakona, čl. 173.

povreda prava ili meru **zabrane nastavljanja** započetih radnji kojima bi se mogla izvršiti povreda. Privremene mere mogu se izreći zbog obezbedjenja dokaza<sup>318</sup>.

Osim sudske zaštite u građanskopravnim sporovima, Predlog zakona je predvideo i **arbitražu za sporove između organizacije i korisnika koji je pravno lice**. Arbitraža bi trebalo da se sprovodi pred stalnim izbranim sudom za intelektualnu svojinu pri Privrednoj komori Jugoslavije<sup>319</sup>.

Za zaštitu kompjuterskih programa predviđena je i **krivičnopravna zaštita**<sup>320</sup>. Za neka dela predviđene su **kazne zatvora od 6 meseci do 3 godine**, što se odnosi na sledeće slučajeve:

- kad neko *pod svojim imenom ili imenom drugog objavi, prikaže, izvede ili prenese* *tudj kompjuterski program*, ili dozvoli da se to učini;
- kad se na *nedozvoljen način unesu delovi tudjeg računarskog programa* u svoj;
- kad se *deformišu, skrate ili na drugi način menjaju* *tudji kompjuterski programi*.

Za sledeća dela predviđene su **novčane kazne**, mada i ona predstavljaju **krivična dela**:

1. kad se *bez dozvole* autora ili nosioca autorskih prava na računarskom programu, a kad je ta dozvola potrebna, *objavi, preradi, obradi, reprodukuje, prikaže, prenese, prevede*, ili na neki drugi način iskoristi kompjuterski program;
2. kad se u *nameri pribavljanja materijalne koristi stavi u promet* računarski program za koji zna da je neovlašćeno reprodukovano ili umoženo, ili se javno (npr. na sajmovima, izložbama) izlaže.

I za jedna i za druga krivična dela gonjenje se preduzima po privatnoj tužbi. Ukoliko dela učini organizacija, kažnjava se za **prekršaj** i to **novčanom kaznom**<sup>321</sup>.

Sve je češća pojava **piratstva**. Ono se obično definiše kao **kopiranje, korišćenje i distribucija kompjuterskih programa povredom autorskih prava ili**

<sup>318</sup> Predlog zakona, čl. 177 - 182.

<sup>319</sup> Predlog zakona, čl. 182.

<sup>320</sup> Zakon o autorskom pravu, čl. 100 i 101.

<sup>321</sup> Po čl. 101., Zakona o autorskim pravima.

**poslovne tajne**<sup>322</sup>. Ova distribucija bez dozvole poprima ogromne razmere. Računa se da u svetu barem 60% svih programa (kod nas čak 98% operativnih sistema) biva neautorizovano kopirano i distribuirano. Piratstvo je od 1980. godine, radi razmera koje poprima, postalo masovna devijacija jer svako ko ima kompjuter teži da dodje, bez naknade, do svakog ili određenog, zaštićenog programa<sup>323</sup>. Područje piratstva kreće se od "sitnog" kopiranja kancelarijskih programa i instaliranja kod kuće, do procvata "gradova ili država pirata" u kojima se piratske kopije novih softvera mogu kupiti skoro pre ili neposredno nakon (svega par sati) izvornih, autentičnih. Ukoliko se programima osigura odgovarajuća zaštita uhvaćeni pirati će odgovarati za povredu. To može imati i preventivni značaj kao upozorenje namernicima da odustanu od takvog dela. Međutim, s druge strane, zaštita može istovremeno biti i izazov piratima. Ne retko se dešava da pravna zaštita predstavlja dodatni motiv za počinioce i povećava vrednost takvih programa na "crnom tržištu". To je u jednom trenutku dovelo i do pojave "amnestije" od strane velikih softverskih kuća u SAD koje su pozivale sve one koji su imali ilegalne kopije njihovog softvera da ih u razumnom roku plate, a za uzvrat bi odustajali od bilo kakve pravne akcije uz snabdevanje autentičnom verzijom<sup>324</sup>. Međutim, kako ni to nije postiglo nekave posebne efekte mnoge su softverske kuće krenule drugim putem: ili su počele ugradnju virusnih programa koji bi se aktivirali u slučaju neautorizovanog korišćenja softvera (sumnja se da je u *Microsoft* "snabdeo" virusima svoj *Windows '95*) i ili nekog programa, ili bi, kao što je slučaj sa *Microsoft*-om, počeli ugradnju posebnog identifikatora (slično clipper čipu, ali softverska varijanta) bez koga se korišćenje njihovog softvera ne može odvijati bez "šuma". Posebno su počele primene tih identifikatora pri uključivanju u Internet, što je, naravno, izazvalo prilične proteste u SAD i širom sveta<sup>325</sup>.

Ipak, usled postojanja mogućnosti za povećanje i učestalo preduzimanje piratskih napada na, pravom zaštićene, programe neophodno je bilo ove mogućnosti u zakonu predvideti i počinioce kažnjavati. To je bio i jedan od razloga zašto je krajem osamdesetih i početkom devedesetih godina došlo do noveliranja mnogih, pa i našeg krivičnog zakonodavstva. Uvedeno je, 1994. godine, novo krivično delo.

**Neovlašćeno korišćenje autorskog prava**, dakle i na računarskim programima, je posebno krivično delo predviđeno članom 183a Krivičnog zakona Srbije. Ono obuhvata **neovlašćeno objavlivanje, reprodukovanje, prenošenje,**

<sup>322</sup> World H. G., Shriver F. R., Computer Crime Techniques Prevention, Rolling Meadows, Bankers Publishing Company, 1989., str.29.

<sup>323</sup> U okviru EU formirana je *The European Computing Services Association* koja prati problem softverskog piratstva na teritoriji Unije i izveštava o gubicima nastalim zbog njega.

<sup>324</sup> Mawrey R., Salmon K., Computers and the Law, Oxford, BSP Professional Books, 1988., str. 184.

<sup>325</sup> Whitfield N., Net Answers, Personal Computer World, june 1996., str.220 - 225.

*prikazivanje ili na drugi način iskorišćavanje računarskih programa* (kao i videograma, fonograma ili drugih autorskih dela) zaštićenih zakonom. Počinioc će se kazniti *novčanom kaznom ili zatvorom do 1 godine*<sup>326</sup>. Da bi bio odgovoran za krivično delo, počinitelj mora biti uračunljiv, odn. biti svestan povrede kompjuterskog programa koju čini i hteti njeno izvršenje ili svestan da, usled njegovog činjenja ili nečinjenja, može nastupiti zabranjena posledica, s tim što na njeno ispunjenje pristaje. Ovim se članom zaštićuju računarski programi od piraterije, a svi oni, koji se ovim neovlašćenim aktivnostima bave, stavljaju sa one strane zakona i svrstavaju u pirate. Medjutim, predviđena kazna je izuzetno mala, tako da je ova odredba upravo suprotna članu 61. Sporazuma o trgovinskim aspektima prava na intelektualnu svojinu kojim se preporučuju što strože kazne, znači, visoke novčane kazne i duže kazne zatvora<sup>327</sup>. Osim toga, ovim članom Zakona nije predviđeno oduzimanje, zaplena, niti uništavanje piratskih kopija, kako je to inače predviđeno Sporazumom.

Ovaj član imaće smisla ukoliko se kazne pooštire i kad se budu dopunile odgovarajućim formulacijama vezanim za uništenje svih materijala i alata (kompjutera, disketa, hard diska, CD, uređaja za upisivanje, i sl.) koji su služili za izvršenje ovog dela.

Predlog zakona je bio ne samo detaljniji u određivanju vrsta krivičnih dela koja se odnose na razne povrede prava zaštićenih računarskih programa, već i nešto strožiji nego Zakon. Tako je kao **krivično delo** predviđeno:

- *objavljivanje pod svojim imenom ili imenom drugog, u celini ili delimično, tuđeg računarskog programa;*
- *izmena i prerada tuđeg računarskog programa bez dozvole autora;*
- *iskorišćavanje tuđeg računarskog programa na način kojim se ugrožava ili može ugroziti čast ili ugled autora;*
- *objavljivanje, u celini ili delimično, snimanje, umnožavanje, stavljanje u promet, davanje u zakup, ili na drugi način iskorišćavanje računarskog programa bez dozvole nosioca autorskih prava;*

<sup>326</sup> Članom 102 Zakona o izmenama i dopunama, Službeni glasnik RS, br. 47/94, dodat je ovaj član.

<sup>327</sup> Npr. američkim *The Federal Piracy and Counterfeiting Amendments Act* of 24 May 1982., predviđena je *kazna zatvora od 5 godina i/ili novčana kazna od 250.000 dolara* za "trgovanje lažnim (falsifikovanim) oznakama fonograma, kopijama filmova i drugih audiovizuelnih dela". Pošto je *Copyright (Computer Software) Amendment Act*-om iz 1985. godine, softversko piratstvo određeno kao kriminalna radnja ista kao i ona vezana za fonogram ili filmove, to se ovo određenje piratstva i kazni odnosi i na njih. U Kanadi može se dobiti *kazna i do 1 milion dolara* za ugrožavanje autorskih prava, dok je u Kini predviđena i *kazna zatvora od 5 godina*, pored novčane kazne.

- *stavljanje u promet ili davanje u zakup primeraka računarskog programa za koji se zna da je neovlašćeno snimljen ili umnožen u nameri pribavljanja materijalne koristi.*

Za ova krivična dela **kazne su isključivo zatvora** i kreću se od šest meseci do tri godine<sup>328</sup>.

Zanimljivo je da je predlagač izostavio odredjenja šta se sa samim programima dešava kad su oni predmet krivičnih radnji. Da li se uništavaju, predaju autoru ili nosiocu autorskih prava, da li se i na koji način obustavlja njihov promet, i šta se dešava ako se materijalna korist postigne, kao i mnogim drugim pitanjima? Činjenica je da su odredbe o sudskoj, građanskopravnoj, zaštiti daleko preciznije, što svakako predstavlja prilični nedostatak Predloga zakona.

Ukoliko je počinioc preduzeće ili drugo pravno lice onda su u pitanju privedni prestupi, odn. prekršaji. Kao **privedni prestupi** koji se kažnjavaju novčanom kaznom od 45.000 do 450.000 dinara predviđeni su:

1. *objavljivanje, u celini ili delimično, snimanje, umnožavanje, stavljanje u promet, davanje u zakup, ili na drugi način iskorišćavanje računarskog programa bez dozvole nosioca autorskih prava;*
2. *stavljanje u promet ili davanje u zakup primeraka računarskog programa za koji se zna da je neovlašćeno snimljen ili umnožen u nameri pribavljanja materijalne koristi;*
3. *obavljanje poslova kolektivnog ostvarivanja autorskog prava bez dozvole nadležnog saveznog organa;*
4. *neobaveštavanja organizacije o nazivu računarskog programa i obimu njegovog iskorišćavanja u roku od 15 dana od dana početka korišćenja, odn. 30 dana od dana korišćenja programa ako se to radi bez dozvole nosioca prava.*

**Novčana kazna** je predviđena za prekršaje i to u visini od 15.000 do 150.000 dinara. **Prekršaj** čini preduzeće ili drugo pravno lice ukoliko:

1. *bez navodjenja imena autora ili pod drugim imenom, u celini ili delimično, objavi tudj računarski program;*
2. *bez dozvole autora izmeni ili preradi tudj program;*

---

<sup>328</sup> Predlog zakona, čl. 183 i 184.

3. prilikom unošenja u evidenciju i deponovanja kod nadležnog saveznog organa računarskog programa *da neistinit ili prikrije pravi podatak o svom programu.*

Pored organizacije kažnjava se i odgovorno lice u preduzeću ili drugom pravnom licu.

I pored promena koje su se desile vezano za zaštitu autorskog prava, ipak je naše pravo ostalo indiferentno propuštajući da predvidi dela kakva su<sup>329</sup>:

1. *trgovina nedozvoljenim kopijama* koja obuhvata uvoz nedozvoljenih kopija i njihovo posedovanje ili poslovanje sa njima;
2. *obezbedjenje sredstava za pravljenje nedozvoljenih kopija* koje, pre svega, obuhvata takvo sredstvo koje je posebno dizajnirano ili prilagodjeno za pravljenje kopija nekog određenog programa koji poseduje neka određena osoba;
3. *olakšavanje povreda transmisijom* postoji kad se bez dozvole autora ili nosioca autorskih prava prenosi program telekomunikacionim sredstvima pri čemu se napravi kopija i to nedozvoljena;
4. *"nadmudrivanje" zaštite od kopiranja*<sup>330</sup> kojom se prave nedozvoljene kopije specijalnim uređajima ili sredstvima (npr. hardverskog uređaja za tzv. "ROM blowers") koje ima u svojinu, na čuvanju, posluži, zakupu i sl.<sup>331</sup>

I na kraju, autor kompjuterskog programa, kao i ostalih autorskih dela, uživa i **medjunarodnu zaštitu** po odredbama konvencija i rezolucija koje je naša zemlja potpisala i ratifikovala. To su pre svega Bernska i UCC konvencija i Rezolucija AIPPI o zaštiti računarskih programa i integrisanih kola.

#### 3.4.4.9. *Postupak fakultativnog sticanja autorskih prava na kompjuterskim programima*

<sup>329</sup> Reed C., op. cit., str. 88 - 91.

<sup>330</sup> Termin **zaštita od kopiranja** je u ar. 296 (4) *UK Copyright, Design and Patent Act*, iz 1988. godine definisana kao "*bilo kakvo sredstvo namenjeno sprečavanju ili ograničavanju kopiranja dela ili snižavanju kvaliteta napravljenih kopija.*"

<sup>331</sup> **Nadmudrivanje** je predviđeno u Predlogu zakona, ali kao osnova za građanskopravnu zaštitu.

Da bi se olakšalo dokazivanje autorskih prava na računarskom programu moguće ga je upisati u registar odgovarajućih autorskih (ova registracija nije uslov zaštite, već dobrovoljni izbor autora)<sup>332</sup>. Preko ovih organizacija vrši se kolektivno ostvarivanje imovinskih autorskih prava. Postupak je predviđen aktom organizacije i veoma je jednostavan. Obično ima **dve faze**:

1. podnošenje molbe za priznavanje prava čini **fazu pokretanja postupka**; i
2. **registrovanje** priznatog prava, zajedno sa izdavanjem isprave o priznatom pravu.

Prijavljivanje se vrši molbom za registraciju, uplatom određenog iznosa i predajom programa najčešće u dva primerka, od kojih se jedan smešta u arhivu, a drugi se, uz overu, vraća autoru.

Registrovanje je upisivanje osnovnih podataka o programu u registar. Čin registracije završava se izdavanjem potvrde. Za razliku od drugih zemalja, naročito onih u kojima se registracija vrši u biroima (zavodima) kao posebnim telima pri vladi ili upravi i koji izdaju odgovarajuća uputstva za sve tehničke i administrativne detalje važne za registraciju (u kom se vidu registruje, gde se stavljaju podaci i sl.), kod nas to još nije aktuelizovano. Otuda, s obzirom da postoji više autorskih agencija, primetne su i razlike među njima.

Predlog zakona predvideo je mogućnost kolektivnog ostvarivanja autorskog prava preko Organizacije za kolektivno ostvarivanje, koja je neprofitna organizacija i specijalizovana za ostvarivanje određenih vrsta prava. Ovu organizaciju osnivaju autori, nosioci autorskog prava, kao i njihova udruženja, koji su dužni da od nadležnog saveznog organa pribave dozvolu za pavljanje delatnosti. Rešenjem o izdavanju dozvole organizacija stiče pravo obavljanja delatnosti u trajanju od 5 godina. Isti savezni organ vrši i nadzor nad njenim radom.

Ono što je od izuzetnog značaja za dalji razvoj autorskog i srodnih prava su odredbe o evidenciji autorskih dela i predmeta srodnih prava. Naime, da bi se obezbedili dokazi nosioci autorskih prava na računarskim programima mogu deponovati primerke svog programa kod nadležnog saveznog organa. Primerci koji se deponuju moraju biti pisani dokumenti (rukopisi, štampani tekst, muzička partitura), zvučni, vizuelni ili audiovizuelni zapis ili u digitalnoj formi. Osim primeraka programa nosilac prava je dužan da da istiniti i potpuni podatak o svom programu.

---

<sup>332</sup> Zakon o autorskom pravu, čl. 91 - 95.

Savezni organ vodi evidenciju za svaku vrstu autorskih dela. Evidencija je javna knjiga, te se podaci koji se u njoj vode smatraju istinitim, dok se ne dokaže drugačije. Za unošenje u evidenciju i deponovanje plaća se taksa. Bliže određenje sadržaja i uslova evidentiranja i deponovanja određuje nadležni organ.

Mada su na prvi pogled ove odredbe izgledale kao značajan pomak u odnosu na dosadašnju praksu, to je, na žalost, samo na prvi pogled. Izostala su mnoga značajnija i detaljnija pravila i postupci, kao što je izostalo i određivanje prava uvida u evidenciju, korišćenja podataka i sl.

I na kraju moglo bi se konstatovati:

**Prvo.** *Sva rešenja koja su prihvaćena u našem zakonodavstvu više su vezana za materijalni interes naručioca i korisnika programa nego za autora.* Verovatno je to ceh koji prošlosti plaćamo pošto se još uvek nije prekinulo sa shvatanjima da je autor fizičko lice koji je "manje važan" od korisnika (koji je, po pravilu, pravno lice). S druge strane, prenošenje svih njegovih imovinskih prava na programu, ukoliko je on nastao u radnom odnosu ili po ugovoru o delu na pravno lice, obezbeđuje poslodavcu ulogu koja više ugrožava autora nego što ukupno stimuliše domaće stvaralaštvo u ovoj oblasti.

**Drugo.** *Veliki je pomak u odnosu na ranije naše, ali i zakone nekih drugih zemalja, što je kompjuterskim programima eksplicitno priznato svojstvo autorskog dela, i to posebnog.*

**Treće.** Na žalost neka rešenja koja su trebala da uslede posle određivanja ovakvog statusa kompjuterskih programa nisu se pojavila, tako da su *ostale mnoge nejasnoće, nedorečenosti i nepreciznosti*. Jedna od najvažnijih je i izostanak određenja samog kompjuterskog programa, definisanja posebnih značenja prava na prevod, adaptaciju i sl.

**Četvrto.** *Evidentne su neujednačenosti u regulisanju.* S jedne strane pojavljuju se detaljisanja (npr. u ograničenjima prava) i preregulacije, a s druge, javljaju se opštosti (npr. određenje trajanja moralnih prava).

**Peto.** *Izostala su neka, pogodna, rešenja koja se nude međunarodnim aktima, naročito Sporazumom o trgovinskim aspektima prava intelektualne svojine, ali i*

drugim (npr. dozvoljen je jedan vid reverzibilnog programiranja, koji je suprotan duhu Bernske konvencije).

**Šesto.** Iako nešto detaljnije kaznene odredbe Predloga zakona (u donosu na Zakon) su i, dalje, *nedovoljno obuhvatne za specifična krivična dela vezana za narušavanja prava zaštićenih programa, kao što su i kazne relativno blage* (i zatvorske i novčane).

**Sedmo.** Kao što je propuštena prilika da se Predlogom zakona depozit, označavanje i registracija uvrste u uslovi za zaštitu, tako je *propuštena prilika da Savezni zavod za intelektualnu svojinu*, kao kadrovski, organizaciono, stručno i tehnički (možda jedino ne finansijski) *najpogodnije telo za obavljanje poslova kolektivnog ostvarivanja autorskih i srodnih prava*, kao i koordinacije i saradnje sa sličnim telima i organima van naše zemlje.

**Osmo.** Sve ove karakteristike sadašnjeg našeg pravnog regulisanja zaštite računarskih programa ukazuju da je *potrebno ozbiljno razmišljanje u pravcu boljeg i efikasnijeg regulisanja ubuduće*. Možda čak i sui generis zaštitom.

### 3.5. *Kompjuterski programi i zaštita sui generis pravom*

Pravo *sui generis* je u početku zaštite kompjuterskih programa vidjeno kao najbolji pravni okvir u koga treba smestiti tako specifičnu sliku kakvi su programi. Opravdanje za podvođenje pod ovu zaštitu postojalo je u samoj prirodi ovih tvorevina<sup>333</sup>. Naime, kako programi i softver nisu u pravom smislu reči pogodni da budu predmetom patentne zaštite, a kako autorskopravna zaštita nije u potpunosti mogla zadovoljiti njihovu specifičnu prirodu, to je rešenje pokušano da se nadje u ovoj kategoriji. Iako nije bilo vidljivih razloga da se od specifičnosti i, njima, odgovarajućih rešenja odustane, tim više što je tome naginjao i WIPO sa svojim Modelom zakona o zaštiti kompjuterskog softvera, ipak je do toga došlo, čak mnogo lakše i brže nego što se moglo očekivati. I neke zemlje, uglavnom van evro-kontinentalnog i anglo-saksonskog sistema ili manje značajnih prava (Švedska, Češka, Slovačka) koje su naginjale ovoj zaštiti pokazale su se nedovoljno uticajnim da obezbede njegovu prevagu. Tako je od zaštite pravom *sui generis* odustao i Japan koji je bio, pored WIPO-a i Brazila, najbliži ovom rešenju. Jugoslavija se nije eksplicitno svrstala medju ovu grupu, iako rešenja koja su prihvaćena predstavljaju izuzeća od uobičajenih principa. No, od toga se, donekle,

<sup>333</sup> O tomw više kod Marković S., op. cit., str. 136 - 159.

odustalo u novim verzijama Predloga zakona o autorskom i srodnim pravima, kao što su se ovakvog rešenja odrekle i druge zemlje priklanjajući se većini sa autorskopravnom zaštitom. Razlog koji je istican vezan je za "načelne stavove" necelishodnosti i opasnosti od daljeg cepanja Prava intelektualne svojine pojavom novih kategorija koje ne mogu tako lako da se svrstaju u jednu od poznatih grupa. Možda ovaj razlog i ima smisla, međutim, čini se da se u odnosu na kompjuterske programe to sasvim olako prihvatilo. Pogotovo što mnogi predmeti vezani za kompjuterske programe i softver nisu obuhvaćeni patentnopravnom, niti autorskopravnom zaštitom iz savim jasnih razloga koji skoro bespogovorno stoje.

Obim i sadržaj zaštite, dužina trajanja, uslovi i sama njihova priroda ukazuju da oni nisu tipična autorska dela, a još manje literarna. Svakako da uveliko izgradjena i, u praksi mnogostruko, proverena autorskopravna rešenja su komfornija, no, kompjuterski programi i softver su isuviše značajni za sve sfere ljudskog života i stvaralaštva da bi se tako lagano prilika prepustila. Koliko bespredmetan postaje rok od 50 ili čak 70 godina trajanja zaštite nakon ostvarivanja ili nastanka programa, kad on postaje istorija maltene u jednoj godini? Kako opravdati postojanje i zaštitu primarnih nosilaca autorskih prava na programu nastalom u radnom odnosu na uštrb autora, kad je cilj samog Autorskog prava prioriteta zaštita prava autora, pa, tek, potom nosilaca? Kad su u pitanju programi situacija je dijametralno različita. Da li u potpunosti opravdano? Zar je arhitektonsko ili neko drugo delo osobenije i "autorskiije" od kompjuterskih programa?

Problemi obezbedjenja pristupačnosti, javnosti, objavljivanja, obeležavanja programa na vidljivom mestu i na vidljiv način autorskim imenom i znakom i rešenja kojima se to pitanje elegantno rešilo nije suštinski odgovor, jer se uslov vidljivosti, u suštini, nije ispunio. Kopiranje, broj dozvoljenih kopija, specifičnost postojanja izvornih i objektnih kodova, preradjivanje, šta smatrati originalom (back up verzije ili nešto drugo?) i mnoga druga, ukazuju da je logika zaštite donekle pomerena pojavom kompjuterskih programa.

Problemi postaju još komplikovanijim sa pojavom dela koja generišu sami kompjuteri. Kako njih tretirati? Veoma ih je teško podvesti pod tipična autorska dela, ne samo zbog autorske originalnosti, već i zbog mnogih drugih dilema vezanih za sadržinu i obim zaštite, autore i koautore.

Ilustrativnim nabrojanjem ovih problema ukazuje se samo na potrebu preispitivanja i revidiranja postojećih rešenja i veće fleksibilnosti u priznavanju takve svojstvenosti ovim delima koja je dovoljan razlog i za posebnu zaštitu.

### 3.6. *Kompjuterski programi i zaštita poslovne tajne*

#### 3.6.1. *Opšte napomene o poslovnoj tajni*

Institut poslovne tajne je most koji spaja pravo zaštite od nelojalne utakmice, know how kao deo pronalazačkog prava, patentno i autorsko pravo sa poslovnim i radnim pravom i lojalnošću zastupnika, posrednika, direktora, bankara. To je istovremeno i institut koji, u osnovi, ima neki podatak, informaciju, koji predstavlja krucijalnu dilemu svake organizacije - kako je zaštititi? Dragoceni podaci lako "iscure" iz organizacije i dopadaju u ruke konkurentima, a kada se to desi ugrožava se i njen opstanak.

##### 3.6.1.1. *Karakteristike*

Poslovnom tajnom, u stvari, štite se poslovne informacije i dokumenti neophodni za formiranje poslovnog znanja. To su oni podaci koji se koriste u poslovanju i koji se skrivaju i čuvaju od javnosti<sup>334</sup>. Poslovna tajna u mnogim pravima ima atribut svojine, može se prodati ili licencirati po izuzetnim cenama jer daje ključ za neku akciju, posao, položaj. Otuda se upravo ona pojavljuje i kao čest predmet raznoraznih ataka<sup>335</sup>. **Poslovna tajna su isprave i podaci koje kao takve organizacija odredi odgovarajućim aktom (statutom, odlukom organa upravljanja), a čije bi saopštavanje neovlašćenom licu bilo protivno poslovanju ili štetilo njenim interesima i poslovnom ugledu**<sup>336</sup>. Mnoga prava, definišući šta pod njom podrazumevaju, se slažu da je za podatak, informaciju, koji čini poslovnu tajnu karakteristično<sup>337</sup>:

1. da predstavlja **korisni podatak, informaciju, dokument** što znači da ima u osnovi **ekonomsku vrednosti**, stvarnu i potencijalnu, koja ne bi trebalo da bude poznata drugima jer ne samo što time oni dobijaju mogućnost za određenu korist, već što i onaj čija je tajna otkrivena gubi

<sup>334</sup> Slično ju je definisao i Zakon o suzbijanju nelojalne utakmice u Japanu iz 1990., po kome "**poslovna tajna** su proizvodni postupci, metode prodaje i/ili druge informacije koje se koriste u poslovanju, a odnose se na tehniku ili poslovnu politiku, koje se čuvaju i kontrolišu kao tajne i koje su generalno nepoznate javnosti."

<sup>335</sup> Lipner S., Kalman S., op. cit., str. 207.

<sup>336</sup> Drakulić M., Osnovi Poslovnog prava, Beograd, FON, 1995., str. 291.

<sup>337</sup> Bernacchi R., Frank P., Statland N., op. cit., str. 3-64.

jer njegovo "tajno" znanje postaje javno, a vrednost je imalo samo dok je tajno, drugima nedostupno;

2. da vrlo često predstavlja **kombinaciju** karakteristika ili komponenti koje su inače poznati javnosti, ali postupak i proces kombinacije predstavlja tajnu, što znači da je njena suština u novini, "inovaciji", načina na koji su komponente kombinovane, ali i samih komponenti ukoliko nisu opštepoznate;
3. da je **nepoznat javnosti**, što izgleda kao tautološka odrednica, no, nije, jer ukoliko postoji mogućnost da je generalno poznat i dostupan javnosti neće biti poslovna tajna. Posebno je pitanje "mere" nedostupnosti i kriterijuma na osnovu koga se merenje vrši<sup>338</sup>. Teret dokazivanja je uvek na vlasniku;
4. da se mora čuvati u **tajnosti**. Tajnost je ključna karakteristika. Naime, dok su udaljeni od drugih očiju dotle su i vredni. To se mora i želi osigurati, bili što će se u svom izvornom vidu učiniti nedostupnim i "nevidljivim" drugima, bilo što neće biti uvek očigledno kome pripadaju<sup>339</sup>. Najbolja ilustracija za tajnovitost i značaj koji ova karakteristika ima je njeno poredjenje sa Pandorinom kutijom<sup>340</sup>;
5. da je **proglašen** poslovnom tajnom. Dakle, poslovnom tajnom smatra se samo onaj podatak koji je aktom organizacije, zakonom ili odlukom nekog nadležnog organa za to proglašen;
6. da bi odavanje prouzrokovalo ili bi moglo prouzrokovati **štetne posledice za organizaciju**. Pri tome, štetne posledice mogu se ticati materijalnih i nematerijalnih vrednosti. Naročito su značajni ugled, imidž, goodwill organizacije, i dobit, koji se odavanjem mogu ugroziti, ili se ugrožavaju. Naravno da nije irelevantno ni gubljenje određene pozicije na tržištu;
7. da predstavlja **predmet mnogih aktivnosti** kojima se, s jedne strane želi zaštititi neka informacija, a, s druge, ona od drugih otkriti. Sticanje se može postići na zakonit, dozvoljen, ili nezakonit, nedozvoljen, način. Pribavljanje krađom, prevarom, industrijskom špijunažom, je mnogo češće nego legalno. Ovo je posebno važno zbog zaštite koju treba da

<sup>338</sup> Američki sudovi za utvrđivanje prirode neke informacije i njenu podobnost da bude poslovnom tajnom primenjuju različite testove. Jedan od najčešćih je vezan za utvrđivanje postojanja 6 faktora: (a) stepena do koga je informacija poznata van posla; (b) stepena do koga je poznata zaposlenima i drugima koji su u posao uključeni; (c) obim mera koje vlasnik preduzima da bi je zaštitio; (d) vrednost koju ima za vlasnika i konkurente; (e) količina truda ili novaca uloženog od vlasnika da bi se predmet razvio; i (f) lakoća ili težina sa kojom bi se informacija mogla nabaviti ili kopirati od strane drugih, Klitzke A., Trade Secrets: Important Quasi - Property Rights, The Business Lawyer, no. 4/86., str. 560.

<sup>339</sup> Tamaki Y., Zaštita poslovnih tajni u Japanu, Podlistak Patentnog glasnika, br. 1/93., str. 190.

<sup>340</sup> Unković D., Strategija i tehnika zaštite poslovnih tajni, Beograd, Savremena administracija, 1989., str. 13.

preduzima vlasnik, naročito kad su u pitanju sadašnji i bivši zaposleni, kao i oni koji imaju nameru da napuste organizaciju.

Kao najčešći predmeti o kojima se podaci, informacije ili dokumenta proglašavaju poslovnom tajnom pojavljuju se<sup>341</sup>: proizvodi, formule, tehnološki procesi, metod rada, mašine i njene izmene, dokumentacija o istraživanju i razvoju, prepiska, interna poslovna dokumentacija, obaveštenja o klijentima, finansijske i knjigovodstvene informacije, pravna pitanja, dokumentacija o planovima i strategiji, uzorak, kompilacija, i, naravno, **računarski programi, softver, kao i postupak programiranja i implementacije**.

### *3.6.1.2. Kompjuterski programi, know how i poslovna tajna*

Gotovo svaki računarski program i softver, ili većina, u celini ili u delovima, može biti i predmetom zaštite i institutom know how<sup>342</sup>, a najviše poslovnih tajni je vezano za know how.

*Naime, **know how** je skup praktičnih znanja i akumuliranih iskustava nematerijalnog karaktera za koje je značajno da se materijalizuje u nekim stvarima ili na neki način kako bi moglo biti preneto na treća lica.*

Da bi neko znanje i iskustvo predstavljalo know how potrebno je da ima sledeće elemente:

1. **tajnost**, odn. da znanje i iskustvo zainteresovana strana ne može lako steći i da joj nisu pristupačna;
2. **novost** koja je subjektivna, naime, da znanja i iskustva koja se prenose predstavljaju novost za sticaoca;
3. **prenosivost** bez koje se ne može postići njegova svrha;
4. **ekonomski interes** za onog ko ih poseduje jer ako su ona od čistog naučnog interesa onda ne ulaze u domen know how;

Elementi tajnosti i ekonomskog interesa obezbeđuju se proglašenjem know how za poslovnu tajnu.

---

<sup>341</sup> Unković D., op. cit., str. 18 - 20.

<sup>342</sup> Termin *know how* je potekao iz anglosaksonske literature i toliko se odomaćio u svim ostalim zemljama da se ne prevodi.

Know how može biti<sup>343</sup>:

1. **tehnički;**
2. **poslovni i trgovački** (organizacija preduzeća, administracija, knjigovodstvo, programiranje i sprovođenje finansijskog i komercijalnog poslovanja, marketing, reklame, i sl. ); i
3. **informacioni** (projektovanje, razvoj, implementacija IS i KT, procedure i postupci prikupljanja, obrade, distribuiranja i korišćenja podataka i informacija, kao i procedure i postupci stvaranja i razvoja softvera i kompjuterskih programa).

Zbog svojih specifičnih svojstava, know how je izostao iz većine starijih zakonodavstava, pa ni njegovi nosioci nemaju klasična prava<sup>344</sup>. Naime, i "autor" i nosilac know how nemaju pravni, već faktički monopol nad njim. Dok god je znanje i iskustvo u posedu njegovog imaoca i tajna za druge dotle know how postoji. Čim se ta osobenost izgubi, iz bilo kog razloga, gubi se i smisao ovog instituta.

Algoritmi, dijagrami, izvorni kodovi, šematski dijagrami, dokumentacija postaju sve značajniji za uspešnost poslovanja jedne firme, a često su produkt znanja i iskustva, te i know how. Ovaj institut postaje veoma interesantan kod projektovanja informacionih sistema i kreiranja nove metodologije. Za očekivati je da će vreme njegove primene u odnosu na KT i IS tek doći, naročito kad se radi o računarskim programima i softveru, pa će i zaštita poslovnom tajnom postati još aktuelnija.

### 3.6.2. *Kompjuterski programi i nacionalni propisi zaštite poslovne tajne*

Veliki je broj zemalja svojim nacionalnim propisima regulisao pitanja vezana za poslovnu tajnu, te se, otuda, i kompjuterski programi mogu naći pod njihovim udarom. Ako se posmatra stanje u pravnim sistemima informaciono razvijenih zemalja, može se konstatovati da gotovo sve one imaju poslovnu tajnu kao jedan od oblika zaštite kompjuterskih programa i softvera. Pri tome su se:

<sup>343</sup> Većina autora koja se bavi ovom problematikom opredeljuje se za tehnički i poslovni, odn. trgovački know how, međutim, to je nepotpuna klasifikacija i u nju se mora uvrstiti informacioni know how, kao posebna vrsta. Razloga ima mnogo, ali svakako bi trebalo istaći da su karakteristike ovog skupa znanja i iskustava toliko specifične da ne mogu da se podvedu ni pod jednu do sada priznatu.

<sup>344</sup> Pojavljuje se npr. u japanskom zakonu, ali vezano za ugovor o licenci know how, a povodom zaštite poslovne tajne.

1. neke od zemalja opredelile za donošenje **posebnih**, *lex specialis*, **zakona o poslovnoj tajni**, kao što je to slučaj sa SAD;<sup>345</sup>
2. druge, mnogobrojnije, su to regulisale u okviru **propisa o suzbijanju nelojalne utakmice** (Japan, raniji Zakon o suzbijanju nelojalne utakmice i monopolističkih sporazuma SFRJ, Zakon o nelojalnoj utakmici SR Nemačke, i dr.);
3. neke opredelile da je regulišu samo u **gradjanskim i krivičnim zakonima** (Kolumbija i druge latinoameričke zemlje), dakle, propisujući kazne;
4. u nekim zemljama preovladalo je mišljenje da je problem poslovne tajne ne samo problem antimonopolističkih zakona, krivičnih i gradjanskih, već i trgovačkih, kao i svih drugih koji imaju dodirnih tačaka sa njom (spoljnotrgovinsko poslovanje, npr.), znači, čitavog **spleta zakona** (SR Jugoslavija, npr.); i
5. naravno, u nekim zemljama poslovna tajna i njena zaštita nisu **se našli ni u jednom propisu**, ali su zato iskristalisana **pravila kroz sudsku praksu** (Kanada, npr.)<sup>346</sup>.

Mnogi poslovni podaci i informacije, predstavljaju poslovnu tajnu, ali, kada su u pitanju računarski programi i softver gotovo da nema ničega što ne može da bude poslovna tajna. Ipak, najčešći predmet poslovne tajne su:

1. **kompjuterski program** (izvorni kod) u celini ili njegovi delovi (ideja, niz instrukcija, struktura, algoritam);
2. **proces dizajniranja** programa od specifikacije problema do testiranje programa;
3. **bagovi i proces debugiranja**;
4. **novost** u programu zaštićenog patentom;
5. **korisnički interfejs i način rešavanja** zvučne i grafičke podloge (u video igri);
6. **softver**;
7. **"produkti"** reverzibilnog inženjerstva;
8. **kompilacije**;
9. **prevodi**;
10. **način zaštite** od neautorizovanog pristupa, korišćenja, modifikovanja, kopiranja (algoritam zaštite, password, i sl.);
11. **metodologija** projektovanja i dizajniranja rešenja IS;

<sup>345</sup> Uniform Trade Secret Act, 1979.

<sup>346</sup> Canadian computer litigation: where we are and where we are going? - trade secret protection for information technology, 1996., preuzeto sa Interneta.

12. **elementi ugovora** za izradu programa, naročito: "*bespoke*" softvera (*bespoke* je softver po meri, nestandardan, skup i obično se isporučuje na osnovu direktnog ugovora između softverske kuće i korisnika); uslovi pod kojima se zaključuju ostali kompjuterski ugovori (o licenci, franšizingu, konsaltingu, i sl.);
13. **dokumentacija** o planovima daljeg razvoja softverske firme i njenoj strategiji (ideje o novom softveru);
14. **svi drugi relevantni podaci i dokumenta**, kao što je prepiska sa korisnicima o bagovima, obaveštenje o klijentima, finansijski i slični podaci, kao i o postupku patentiranja, autorskopravnoj zaštiti ili postupcima pred sudom zbog nelojalne utakmice, i sl.

Poslovna tajna nažešće i najčešće je ugrožena od:

- a) **sadašnjih i bivših zaposlenih**;
- b) **hakera**, amatera i profesionalaca;
- c) **angažovanih i "iznajmljenih" stručnjaka**, privremeno i povremeno zaposlenih za obavljanje određenih poslova, aktivnosti ili konsultantskih usluga;
- d) **konkurenata**;
- e) **partnera**;
- f) istraživača, analitičara i sličnih **stručnjaka koji se bave ispitivanjem tržišta** u okviru specijalizovanih agencija ili istraživačkih (ponekad i naučnih) institucija;
- g) **zaposlenih u zavodima** (biroima) za registraciju patenata, znakova razlikovanja ili autorskih prava;
- h) **službenika poslovnih banaka i finansijskih institucija**;
- i) **drugih lica van organizacije** kao što su izvodjači instaliranja opreme, snabdevači, zajmodavci, agenti i zastupnici, knjigovodstveni i finansijski kontrolori, i sl;
- j) profesionalnih "**lovaca na poslovne tajne**" i druga lica.

Otkrivanje poslovnih tajni vrlo često predstavlja i kriminalnu radnju, pa čak i delo industrijske špijunaže. Međutim, bez obzira kako se kvalifikuje, napadnuti "objekt" je poslovna tajna, a **najčešći počinioци sadašnji i bivši zaposleni**.

Upravo na to ukazuju poznati sudski sporovi vezani za računarske programe i softvere kao predmeta otkrivene poslovne tajne. Tako, npr. jedan od poznatijih slučajeva<sup>347</sup> je spor *Q-CO. INDUSTRIES, INC. v. HOFFMAN, SOM, CPC* iz 1985.

<sup>347</sup> Lipner S., Kalman S., op. cit., str. 231 - 234.

godine. *Q-CO.* je firma iz Nju Jorka sa određenim poslovnim ugledom, Hoffman i Som su lični prijatelji. *Computer Promptly Corp. (CPC)* je kompanija osnovana početkom 1985. godine. *Q-CO.* je nameravala je da razvije svoj *VPS-500* softver. Softver, dizajniran za korišćenje PC kao "suflera" u TV emisijama i pozorištu, trebalo je da omogući prikazivanje uveličanih slova na monitoru kako bi spikeri i glumci direktno mogli da pročitaju svoje tekstove. Ova kompanija razvijala je softver za *Atari 800-XL*. Kompjuter je služio kao ekran "suflera". *Q-CO.* je svoj *VPS-500* softver registrovala kao autorsko delo u maju 1985. godine. Softver je bio rezultat Hoffman-ovog rada koji je od 1984. godine u *Q-CO.* bio stalno zaposleni radnik na razvoju baš tog softvera. Na njegov predlog ručno kontrolisani uređaji postali su deo kompjuterizovanog "suflera", a asistent za razvoj postao mu je Som. Hoffman je, dakle, bio stalno zaposleni, a Som konsultant. Hoffman je sam isplaćivao Som-a mada je kasnije dobijao povraćaj isplaćenog novca. Ni jedan od njih dvojice nije imao poseban ugovor o čuvanju poslovne tajne. Tokom 1984. godine Hoffman je kreirao kompjuterskog "suflera" koji će kasnije biti ugrađen u *VPS-500*. Prilikom kreiranja programa Som i Hoffman radili su na *Q-CO.* opremi i bili od njega snabdeveni svom potrebnom dokumentacijom i literaturom. Som je ubrzo postao glavni programer za *VPS-500*. Radili su veoma blizu jedan drugome, a ostali programeri i operateti nisu imali pristup ovom projektu, niti su znali bilo kakve detalje o njemu. Njih dvojica su direktno informisali potpredsednika kompanije o rezultatima. Dok je projekat trajao, naročito u poslednoj fazi, Hoffman je u razgovoru sa nekim službenicima i zaposlenima napominjao da bi bilo dobro da se po okončanju projekta za *Atari*, "sufler" prilagodi *IBM-PC*.

Od avgusta do decembra Hoffman je putovao sa Berg-om, svojim direktnim kontrolorom, na razna mesta, između ostalog i u Detroit u firmu *Marritz Communications* koja je saradivala sa Fordovim fabrikama. D. Device, službenik *Marritz Communications*, savetovao je Berg-a i Hoffman-a da prilagode svog "suflera" za *IBM-PC* jer su mnoge firme, pa i Ford, zainteresovane za takve programe.

U međuvremenu, tekao je rad na doterivanju softvera *VPS-500*. Krajem decembra (28. decembra) Hoffman i Som su demonstrirali zaposlenima poslednju verziju ovog softvera u Njujorškoj kancelariji *Q-CO*. Tri dana kasnije Hoffman je napustio *Q-CO*.

Tokom decembra Som je prikupljao literaturu i programe kako bi počeo razvoj softvera na *IBM-u*. Sredinom decembra pozvao je Smith-a, programera koji je razvio Banner program (poznati program za *IBM-PC*). Na sastancima i u telefonskim razgovorima Som i Smith su razmatrali mogućnosti razvoja "suflera" na *IBM-u*. Prilikom jedne posete N. Jorku Som (koji je živeo u Vašingtonu) se požalio Hoffman-u da nema novaca. Hoffman mu je dao \$1.000. Krajem decembra Som je poslao Smith-u

račun za nabavku monitora i drugih stvari potrebnih za rad na novom softveru (*CPC-1000*). Som je kasnije poslao Smith-u i uredjaj za ručno kontrolisanje "suflera" za *IBM-PC*. Smith mu je poslao generator slova ili izvršni program. Po dogovoru Smith je trebalo da kreira editor. Smith je prvi ček Somu poslao početkom januara, na sumu od \$777,85 što će biti sve za projekat *CPC-1000*. Na pitanja koja je Smith postavljao Somu oko programa koji mu nudi, Som je odgovarao da je to razvojni program pripremljen za obrazovne programe koje je on radio za jednog klijenta.

Sredinom januara Hoffman je osnovao firmu *CPC*, i dobio potvrdu o osnivanju. Som i Hoffman su bili predsjednici, sa akcijama 50:50. U februaru Hoffman je poslao prijavu za izložbu opreme i softvera u Las Vegasu. Nekoliko sledećih meseci Som je radio za *CPC* i autorska aplikacija za *CPC-1000* bila je gotova početkom aprila. Na izložbi bio je prikazan softver smešten na dva floppy diska, s tim što je drugi disk sadržao fragmente, a ne kompletan program. Prikazivanje softvera *CPC-1000* bio je šok za *Q-CO*. Mada je postojala određena razlika (pre svega, bili su za različite hardvere, pisani su u različitim jezicima - na Pascalu i IBM assembleru, odn. Basic Atari, imali su različite kontrolere, ni naredbe im nisu bile iste, iako su postojale sličnosti u 4 od 12 modula softvera, i sl.). *Q-CO* je tužila sudu Hoffman-a, Som-a i *CPC*. Sud je odbio zahtev *Q-CO* za povredu autorskih prava, međutim, dugo je raspravljao o povredi poslovne tajne. Pokrenuta su sledeća pitanja i pokušani da se daju odgovori:

1) Programi i softver se komercijalno distribuiraju u objektnom kodu, te se **objektni kod** može tretirati kao predmet učinjen dostupnim javnosti, pa otuda i **određene rezerve u odnosu na mogućnost njegove zaštite poslovnom tajnom**. U određenim situacijama on se, ipak, može pojaviti u tom svojstvu, naročito kad je u pitanju **reverzibilno inženjerstvo**. Kako o prirodi ove aktivnosti postoji neslaganje, od mišljenja da se samim činom dekompiliranja i disasembliranja došlo do izvornog koda, a kako on predstavlja poslovnu tajnu, to je i aktivnost koja je do nje dovela nedopuštena. Međutim, postoji shvatanje da izvorni kod dobijen reverzibilnim programiranjem, iako sličan, nije isti sa izvornim kodom koga je napisao originalni programer. Znači, ni poslovna tajna nije otkrivena do kraja, otuda, nema ni njenog kršenja. Prihvati li se ovakav stav može se desiti da "istraživač" izvornih kodova preko objektnih, sam zaštiti svoje "klon programe" poslovnom tajnom. Međutim, treba imati u vidu da se, npr. sudska, zaštita ovakve tajne ne može postići jer je radnja i rezultat protivan pravu i doktrini "fer korišćenja" (*fer use*). Ova doktrina pretpostavlja takvo korišćenje programa i softvera koje neće ugrožavati autorska i ostala prava, a reprodukovanje i prilagođavanje programa, što je suština reverzibilnog inženjerstva, od strane korisnika biće sa njom u suprotnosti. Otuda, ne samo da **ne bi trebalo reverzibilno inženjerstvo blagonaklono tretirati, već ga treba shvatiti kao jedan od ozbiljnih napada na programe i softver, pa čak, i onda kad nema ekonomsku korist u osnovi** (mada se kao i kod dizajna maske čipa dozvoljava reverzibilno

inženjerstvo u naučne i obrazovne svrhe, kad je u pitanju stvaranje novog rešenja, odn. nove i originalne maske).

**2)** Medjutim, **izvorni kod je taj koji, pored autorskopravne zaštite, može predstavljati i poslovnu tajnu**, naročito što se on, po pravilu, ne stavlja na uvid javnosti, odn. korisnicima. Ovo je, čak, moguće i u situacijama kad se program radi u jednom, a prodaje u drugom izvornom kodu. Na prvi pogled tu nema šta da se štiti poslovnom tajnom. No, ona ipak postoji jer ni jedan tvorac programa, niti softverska firma, ne propuštaju priliku **da u izvorni kod ubace "propusnicu" (password) kojima se sprečava neautorizovan pristup. Passwords u ovom slučaju predstavljaju poslovnu tajnu.** Otuda i izvorni kod softvera *VPS-500* predstavlja poslovnu tajnu koju moraju čuvati svi zaposleni koji sa njim dodju u vezu.

**3)** Mada ni Hoffman ni Som nisu imali posebne ugovore o čuvanju poslovne tajne (iako je to uobičajeno) ipak su morali da je sačuvaju, jer je ona imovina *Q-CO.*, pa su stvaranjem, a znajući da su uložena velika sredstva za razvoj, sopstvene kompanije ugrozili njenu svojinu (ovde su prisutni i elemenati nelojalne utakmice). S obzirom da nije postojalo kopiranje softvera, već samo ideje prilagodjavanja softvera određenoj mašini i da je sa tim bilo upoznato mnogo ljudi, to je sud stao na stanovište da u odnosu na to nema povrede poslovne tajne. U prilog im je išao i podatak da je paralelno sa ova dva softvera urađen i sličan softver u V. Britaniji. Kako **opštepoznate stvari i informacije ne mogu biti predmet poslovne tajne**, a podatak o potrebi izrade "suflera" na *IBM-PC* je bio poznat velikom broju ljudi iz različitih kompanija, to se ne može tretirati kao poslovna tajna. Dalje, ipak, razmatrajući ovaj problem sud je prihvatio **shvatanje da kombinacija ili kompilacija poznatih činjenica može biti toliko specifična da postaje ekonomski vredna i otuda podobna za poslovnu tajnu.** U ovom slučaju se radilo o iskazanoj zainteresovanosti potencijalnih kupaca za prilagodjavanje softvera baš *IBM-PC*. Primenjujući analogiju sa evidentnom poslovnom tajnom, kad je u pitanju spisak kupaca, sud je smatrao da je izkazana zainteresovanost potencijalnih korisnika postala Hoffman-u dostupna samo zato što je kao službenik *Q-CO.* dolazio do njih. Prema tome, i **podatak o potencijalnim korisnicima i njihovim zahtevima predstavlja poslovnu tajnu.**

**4)** Na osnovu veštačenja utvrđeno je postojanje identičnosti za četiri od 12 modula softvera. Kako je **struktura programa, organizacija i ideja nešto što predstavlja poslovnu tajnu, jer je know how**, to je u ovom delu ona povredjena. Mada se nije radilo o povredi autorskih prava postojali su elementi za povredu poslovne tajne.

5) Identičnost naziva i funkcija komandi u korisničkom interfejsu pokazala je da je u pitanju postojanje i "*look and feel*" spora. S obzirom da **korisnički interfejs** nije bio autorskopravno zaštićen (mada i ukoliko jeste on može biti predmet zaštite poslovnom tajnom), **to on pripada sferi poslovne tajne**, koja je očigledno bila otkrivena. Naročito ako se ima u vidu da baš ta četiri identična modula predstavljaju najvažnije fukcijske instrukcije.

Ovaj primer pokazao je samo na deo onoga što može biti predmet poslovne tajne kad su u pitanju kompjuterski programi i softver. Medjutim, to nije bilo sve.

6) Tako, **poslovnom tajnom** može se štititi i **operativni sistem i programi u ROM-u, ideja o novom softveru i hardveru, strategija razvoja i istraživanja vezana za novi softver i hardver, kao i podaci o istraživanju tržišta i marketingu**<sup>348</sup>, ali i uslovima pod kojima je zaključen ugovor o licenci.

7) Slično kao i sa reverzibilnim inženjerstvom, postavlja se i pitanje **da li je debugiranje programa otkrivanje poslovne tajne?** Iako je sam proces debugiranja veoma težak, ponekad je on više nego originalno kodiranje. Naročito što onaj ko je to uspeo ima "početnu prednost" u odnosu na ostale korisnike. I pored svih argumenata o kreativnosti, znatiželji, nemogućnosti da se, u određenim slučajevima, do autora ili nosioca prava, koji znaju "sistem", dodje (ukoliko je, npr. firma propala) **ipak sama činjenica da se probila, namerno preduzeta, zaštita otkrivanjem kako program radi** (to je mnogo zanimljivije i korisnije nego šta radi) **predstavlja kršenje poslovne tajne**. Naime, kad programer uoči koje funkcije program ima i na koji ih način realizuje, ne samo što ulazi u domen poslovne tajne, nego stvara sebi i drugima mogućnost da po istoj arhitekturi i proceduri uradi novi program koji će ekonomski eksploatisati. Znači, učinio je više nedozvoljenih radnji, od povreda autorskih ili nekih drugih prava, do otkrivanja poslovne tajne, od ataka na tuđu imovinu do stvaranja mogućnosti za postizanje neopravdane dobiti, do kršenje tuđeg know how, i sl. Zbog svega toga **neautorizovano debugiranje programa predstavlja otkrivanje tuđe poslovne tajne**.

8) Mada nije direktno vezana za računarske programe i softver **poslovnom tajnom može se zaštititi posebna metodologija projektovanja IS**.

Prihvatanje da se kompjuterski programi zaštite poslovnom tajnom proisteklo je iz određenih **pogodnosti** koje ovaj institut pruža:

<sup>348</sup> Bainbridge D., op. cit., str. 38.

**Prvo.** Kompjuterski programi su po svojoj prirodi izuzetno pogodan predmet zaštite, i isto tako veoma čest predmet napada, što je uslovalo *traženje pogodnijih oblika od klasičnih, ili pridodavanje klasičnim*.

**Drugo.** Kako se poslovnom tajnom štite i oni elementi računarskog programa kojima se ne pruža zaštita autorskim, patentnim ili drugim pravom, ili je ona izrazito otežana (to je slučaj sa algoritmima, idejama, i sl.), to je *ona veoma pogodan instrument zaštite*.

**Treće.** Autorsko, patentno i druga prava su sa određenim vremenom trajanja zaštite. *Poslovna tajna nema takvih ograničenja*, te je njena prednost upravo u nedefinisanim objektivnim vremenskim ograničenjima.

**Četvrto.** U slučaju nezakonitog sticanja i pribavljanja, kao i nesavesnog i zlonamernog korišćenja i otkrivanja poslovne tajne, po pravilu, se aktivira mehanizam krivičnopravne zaštite, pored građanskopravne. Time se *rigoroznijim sankcijama pokušava reagovati na sve izraženije pojave gubljenja podataka poslovne tajne*. Naročito je sve učestalija pojava zapošljavanja ključnih programera i projektanata konkurenata i sve razvijenija i raznovrsnija domaća i međunarodna industrijska špijunaža. Softverska industrija gotovo da je "idealno područje" njihove delatnosti radi skupih i riskantnih istraživanja i razvoja, ogromnih novčanih sredstava koja su u njoj obrću, brzih promena, velike konkurencije.

Međutim, u jednom periodu se uočavala tendencija napuštanja ovog pravnog instituta zbog nerešene dileme da li se<sup>349</sup> određeni softver i/ili program, proglašen za tajnu, može slobodno pojaviti na tržištu? Isticale su se još i druge **mane** ove zaštite. Najčešće: **1)** nepraktičnost (jer se odnosi na podatke koji se često kopiraju u velikim razmerama); **2)** "nepoštenost" (ona ne sprečava neke negativne pojave, npr. razvoj kompatibilnih programa); **3)** nerealnost (otkrivanjem tajne, održavanje dalje tajnosti je bespredmetno, a ne postoji ni mogućnost ugovornih obaveza kojima bi se utvrđivali institucionalni reciprociteti u vezi sa njom - nemoguće je ugovoriti pravo ili obavezu da ako jedan partner oda tajnu drugog, ovaj ima pravo da oda njegovu).

No, ipak su se mnoge dileme povoljno rešavale, tako da se poslovna tajna vratila na velika vrata u svet zaštite kompjuterskih programa i ostalih proizvoda KT.

---

<sup>349</sup> Tapper C., op. cit., str. 76 - 93.

### 3.6.3. *Kompjuterski programi i međunarodna zaštita poslovnih tajni*

Poslovna tajna nije čest i uobičajen objekt međunarodne zaštite. To, naravno, znači da se njome eksplicitno ne zaštićuju ni kompjuterski programi. S druge strane, oni su njome zaštićeni posredno, odredbama međunarodnih akata kojima se štiti od neloyalne utakmice, i kao know how. A kad je know how u pitanju tada se zaštita odnosi na određene pravne poslove kojima se znanje i iskustvo prenose. To su, pre svega, ugovori o licenici i o franžizingu.

U međunarodnim sporazumima o zaštiti od neloyalne utakmice malo je odredbi kojima se reguliše tretman poslovnih tajni. Tako, **Pariska konvencija za zaštitu industrijske svojine**, koja u članu 10bis reguliše zaštitu od neloyalne utakmice, ne predviđa povredu poslovnih tajni kao posebno delo.

#### 3.6.3.1. *Sporazum o know how kao globalnom izuzeću iz Rimskog sporazuma*

Kad su u pitanju kompjuterski programi i softver kao know how i poslovna tajna međunarodne transakcije sa njima nisu se posebno našle na udaru međunarodnog sporazumevanja. Prenos ugovorima o licenici ili franžizingu postali su više predmetom studija nego konkretnih odredbi.

Jedini izuzetak su odredbe **Sporazuma o know how kao globalnom izuzeću iz Rimskog sporazuma EU**. S obzirom na značaj koji imaju ugovori o transferu tehnologije za zemlje članice, koji, po pravilu, obuhvataju i transfer i ustupanje znanja i iskustva (računa se da 2/3 ovih ugovora obuhvata i know how), te i poslovnih tajni, to i ugovori o njihovom franžizingu treba da budu predmetom globalnog izuzeća. **Sporazum o know how** stupio je na snagu 1 aprila 1989. godine i obuhvata "čisti" know how. To su, prevashodno, nepatentibilne informacije, među kojima su i softveri. Osim ovoga, regulišu se i pitanja mešovitog know how, koji prati ustupanje patenta i zaštićenog znaka. Ustupanje se vrši isključivom licencom, koja važi za određeno geografsko područje i za određeni period - 10 godina. Dakle, **kompjuterski programi i softver mogu se naći u transferu i to im treba dozvoliti, kao što treba dozvoliti i posebne odredbe o poslovnoj tajni u takvim ugovorima.**

### 3.6.3.2. *Sporazum o trgovinskim aspektima prava na intelektualnu svojinu*

Nešto je bolja situacija sa **Sporazumom o trgovinskim aspektima prava na intelektualnu svojinu**, koji, čak, definiše šta se pod poverljivim podacima podrazumeva, podvodeći ih pod "*celinu ili skup neophodnih komponenti koje nisu poznate javnosti ili lako dostupne drugim licima u krugovima koji se uobičajeno bave tom vrstom informacija*". To su podaci koji imaju tržišnu vrednost zbog svoje poverljivosti i koji su predmet odgovarajućih mera koje preduzimaju lica obavezna da čuvaju poverljive podatke na osnovu zakona.

Znači, ako bi se kompjuterski programi želeli podvesti pod poslovnu tajnu trebalo bi da:

- a) **budu poverljivi**, što znači da ne mogu svi programi zadovoljiti taj uslov. Najčešće će to moći biti određeni kompjuterski programi i softver radjeni po narudžbini, ili takvi specijalni programi čija je priroda specifična i "poverljiva";
- b) kompjuterski programi i softver **velike tržišne vrednosti** (npr. izvorni kod i programska rešenja Windows '95), znači, pod ovu se zaštitu neće moći svrstati "programski sitniš"; i
- c) kompjuterski programi i softver koji su **posebnim merama zaštićeni** i to od strane subjekata predviđenih zakonom. Za sve ostale kompjuterske programe i softver Sporazum nije relevantni pravni osnov za međunarodnu zaštitu. Ono što je posebno bitno je da se poverljivi podaci vezani za programe i softver, kao poslovnu tajnu, **štite od neadekvatne komercijalne upotrebe**. To znači, da se kompjuterski program proglašeni za poslovnu tajnu neće moći komercijalno upotrebljavati ukoliko se ne steknu ti određeni uslovi.

### 3.6.4. *Kompjuterski programi i zaštita poslovne tajne po našem pravu*

#### 3.6.4.1. *Kompjuterski programi i zaštita poslovne tajne zakonskim propisima*

Jugoslovensko pravo pripada onoj kategoriji prava koja su problem zaštite poslovne tajne rešila kroz više zakona. Prevažodno u Zakonu o preduzećima, zatim u Zakonu o trgovini, Zakonu o spoljnotrgovinskom poslovanju, Krivičnom zakonu i Zakonu o obligacijama. Ono što je poseban kuriozitet je da je Zakon o trgovini ukinuo poseban Zakon o suzbijanju nelojalne utakmice i monopolističkih sporazuma, a time i posebno delo **odavanja poslovne tajne i vrbovanja tuđih radnika**, iako su to bila česta dela nelojalne utakmice. Međutim, ovih dela u praksi ima i dalje. Tako, npr. prilikom završavanja idejnog projekta za jednu našu organizaciju nekolicini projektanata su bili ponudjeni izuzetno povoljni uslovi zapošljavanja u njoj. Motiv je, između ostalog, bila izrada i realizacija izvodjačkog projekta. Kad nije u tome uspeła, organizacija im je ponudila da po povoljnijoj ceni, nego što bi dobili za timski rad, urade taj deo projekta. Pristali su. Izradom izvodjačkog projekta preneli su i know how tima. Za učinjeno delo trebalo je da budu tuženi, ali zbog nemarnosti i politike projektantske firme iz koje su potekli, nisu. I ne samo radi toga, već i zbog propuštanja da se ovakva znanja proglase poslovnom tajnom, kao i usled izostajanja ove vrste dela nelojalne utakmice.

Zakon o preduzećima je, definišući **poslovnu tajnu** kao "*isprave i podatke utvrđene odlukom uprave preduzeća, čije bi saopštavanje neovlašćenom licu bilo protivno poslovanju i štetilo bi njegovim interesima i poslovnom ugledu preduzeća*"<sup>350</sup>, dao osnov da se i kompjuterski programi mogu njom smatrati. Naravno, pod uslovom da su odgovarajućim aktom proglašeni za tajnu<sup>351</sup> i da nisu po zakonu javni ili podaci o kršenju zakona, dobrih poslovnih običaja i načela poslovnog morala.

Ono što je, takodje, bitno je da saopštavanje podataka ili isprava koji sadrže podatke o programu i softveru štetiti, ili bi štetilo interesima i poslovnom ugledu preduzeća. Znači, u slučajevima otkrivanja ovih podataka, pored materijalne, može se naneti šteta i ugledu organizacije.

Ukoliko su podaci vezani za kompjuterske programe ili softver proglašeni poslovnom tajnom dužni su da je čuvaju<sup>352</sup>:

1. **svi zaposleni** koji na bilo koji način saznaju za nju;
2. **osnivači, članovi, akcionari, članovi organa preduzeća;**
3. **bivši zaposleni** kojima je prestao radni odnos;

<sup>350</sup> Zakon o preduzećima, Službeni list SRJ, br. 29/96., čl. 90.

<sup>351</sup> Zakon o preduzećima u istom članu navodi da se o ispravama i podacima koji su proglašeni za poslovne tajne moraju obavestiti osnivači, članovi, akcionari, članovi organa preduzeća i zaposleni.

<sup>352</sup> Zakon o preduzećima, čl. 90 i 91.

4. **bivši osnivači, članovi, akcionari**, nakon prestanka mandata mandata organa preduzeća;
5. **lica izvan preduzeća** ako su znali ili su, s obzirom na prirodu tih isprava i podataka, morala znati da su poslovna tajna (dakle, zaposleni kod poslovnog partnera, prevashodno).

Novodoneti Zakon o preduzećima učinio je i korak napred u odnosu na prethodni predviđajući **klauzulu konkurencije**<sup>353</sup> koja obuhvata ograničenja za pojedine kategorije kadrova da ne mogu imati isto svojstvo, niti biti zaposleni, niti konkurisati u bilo kom drugom preduzeću, odn. pravnom licu iste ili slične delatnosti, a koja bi mogla biti konkurent. Razlog za uvođenje ove klauzule je, između ostalog, i zaštita poslovnih tajni. Naravno, oni se ne mogu pojavljivati ni kao preduzetnici koji obavljaju istu ili srodnu delatnost. To su sledeće kategorije:

1. **sadašnji članovi** ortačkog društva, komplementar komanditnog društva, član društva sa ograničenom odgovornošću i član uprave, nadzornog odbora i izvršnog odbora direktora društva s ograničenom odgovornošću, akcionarskog društava i društvenog i javnog preduzeća;
2. komanditori u komanditnom društvu ili akcionari u akcionarskom društvu bez javnog upisa akcija, **ako je to predviđeno osnivačkim aktom, odn. statutom**;
3. članovi ortačkog društva, komplementar komanditnog društva, član društva sa ograničenom odgovornošću i član uprave, nadzornog odbora i izvršnog odbora direktora društva s ograničenom odgovornošću, akcionarskog društava i društvenog i javnog preduzeća, **posle gubitka tog svojstva, ali ne duže od 2 godine**.

Ovaj, a i drugi zakoni (Zakon o osnovama radnog odnosa ili Zakon o radnim odnosima), ipak su propustili da detaljnije regulišu režim i tretman ovih podataka, kao i pitanja vezana za osiguranje od njihovog odavanja i otkrivanja. Prepustili su to odlukma uprave preduzeća.

#### 3.6.4.2. *Kompjuterski programi i zaštita poslovne tajne individualnim ugovorima*

U nedostatku preciznijih zakonskih odredjenja odgovarajuća, i to veoma efikasna, je regulacija **individualnim, pojedinačnim, ugovorima o radu**.

---

<sup>353</sup> Zakon o preduzećima, čl. 92.

Ovim se ugovorima mogu regulisati i pitanja vezana za konkurenciju (nelojalnu), i to naročito u odnosu na: **1) sferu profesionalnih** (npr. specifičnih projektantskih ili programerskih, kao i dizajnerskih i sl.) **aktivnosti radnika** (programera, sistem inženjera, projekatara BP, i sl.) koje podležu klauzuli konkurencije, a kojom se definiše krug poslova na kojima se ne može raditi kod drugog poslodavca; **2) sferu vremenskog ograničenja** kojim se predviđja optimalno najduža vremenska granica važenja ove zabrane (neka prava predlažu da taj rok ne treba da bude duži od 2 godine, naše je predvidelo isti rok za članove ortačkog društva, komplementara komanditnog društva, člana društva sa ograničenom odgovornošću i člana uprave, nadzornog odbora i izvršnog odbora, direktora društva s ograničenom odgovornošću, akcionarskog društva i društvenog i javnog preduzeća); **3) aspekte teritorijalnog važenja zabrana** kojima se određuju geografske zone dejstva emisije ove klauzule; **4) kompenzacije**, naknade, koje treba da dobije takav radnik za vreme trajanja ove klauzule, polazeći od vremena njenog važenja i za koje se može trpeti šteta - "*damnum emergens*" ili "*lucrum caesans*", a koje ne bi bilo da nije bilo ove klauzule; **5) sankcije** za kršenje konkurentske klauzule, koje su, pre svega, imovinske, a trpi ih radnik i poslodavac koji je radnika vrbovao, ako je znao i mogao znati za njeno postojanje. Doduše, Zakon o preduzećima je predvideo za propisane kategorije, ukoliko prekrše klauzulu konkurencije, i određene mere.

Iako ove klauzule, do sada, nisu, kod nas, baš osobito zastupljene u pojedinačnim ugovorima, pitanje je kako će to biti u budućnosti, tim više, što postoji shvatanje o nedopustivosti ovog uređivanja usled opšteg, imperativnog i materijalnog, načela radnog prava - "*in favor laborem*". Takođe, negira se i mogućnost predviđanja nepovoljnijih prava od onih utvrdjenih kolektivnim ugovorom i zakonima<sup>354</sup>. Ovakvo shvatanje moglo bi se primeniti za neke druge predmete, ali nema vidljivih opravdanja kad su u pitanju kompjuterski programi i softver. Pogotovo što je predviđanje konkurentske klauzule u pojedinačnim ugovorima o radu veoma efikasno rešenje, bar za utvrđivanje kruga radnika na koje se primenjuju zabrane, kao i za definisanje zabranjenih aktivnosti, vremena važenja klauzule i sl.<sup>355</sup>

Naravno, postoje i druge solucije, kao što je zaključivanje posebnih sporazuma između radnika i poslodavca tzv **sporazuma o posebnim odgovornostima**

<sup>354</sup> Zakon o osnovama radnog odnosa, Službeni list SRJ, br. 29/96., čl. 71 - 78; Zakon o izmenama i dopunama Zakona o radnim odnosima, Službeni glasnik RS, br. 24/96., čl. 100a.

<sup>355</sup> Jovanović P, Pitanje ugovora o radu i radnog odnosa povodom predloga Zakona, Privreda i pravo, br. 3-6/95, str. 619 - 629; Bogićević Č, Nedoželjena konkurencija u radnom pravu, Privreda i pravo, br. 3-6/95, str. 650 - 658.

**u odnosu na poverljivost**<sup>356</sup>. Modeli ovih sporazuma već duže vremena postoje u praksi pojedinih zemalja. Njihovo prihvatanje i preuzimanje predstavljalo bi znatan pomak u rešavanju pitanja od značaja za obezbeđivanje tajnosti određenih elemenata kompjuterskih programa i softvera, kao i konkretizovanje posebnih odgovornosti pojedinaca<sup>357</sup>. Ovi posebni sporazumi naročito su aktuelni kad su u pitanju novi programi nastali u radnom odnosu za koje autori žele da izvuku određenu (neuobičajenu) korist. Naime, jedan od onih problema koji se ovim sporazumom (ugovorom) može razrešiti je kako da se organizacija **obezbedi od nesavesnih i neodgovornih, a ponekad i zlonamernih, autora** koji se nemarno odnose prema programima (čime dovode u opasnost otkrivanja njihove tajne), ili ih bez ovlašćenja distribuiraju drugim licima (klijentima, partnerima) smatrajući da oni, kao autori, imaju na to pravo, ili ih otkriju javnosti, mada predstavljaju know how ili su bespokeni programi ili softver urađeni po meri, za poznatog kupca i proglašeni poslovnom tajnom.

#### 3.6.4.3. *Zaštita od nezakonitih i nedozvoljenih radnji*

S obzirom da su kompjuterski programi i softver, kao poslovna tajna, često izloženi raznim nezakonitim i nedozvoljenim atacima naročito špijunaži i kradji. Te radnje, kao i njihovo odavanje, izazivaju i konkretne mere zaštite i sankcije u slučaju kršenja.

Zaštita je najčešće **gradjanskopravna i krivičnopravna**.

U **gradjanskopravnoj** zaštiti **privatna tužba** se podnosi sudu, koji odlučuje o veličini naknade koju dobija oštećeni za materijalnu štetu, izgubljenju dobit ili moralnu štetu koju je odavanjem tajne pretrpeo.

**Krivičnopravna** zaštita primenjuje se za dela: **špijunaže** i posebnog dela **izdavanja i neovlašćenog pribavljanja poslovne tajne**. Sankcija je najčešće kazna zatvora.

<sup>356</sup> Manley W, II, Shrode W., Critical Issues in Business Conduct, Legal, Ethical and Social Challenges for the 1990s, New York, Quorum Book, 1989., str. 166.

<sup>357</sup> Ovaj se problem veoma mnogo razradjuje u literaturi vezanoj za zaposlene i konsultante u kompjuterskoj i informacionoj industriji. Tako, npr. Leonard P., Contracting with Staff and Consultants in Information Industry, edicija: Essays On Computer Law, op. cit., str. 132 - 155.

**Špijunaža je skup radnji nekog lica usmerene na poverljive ekonomske** (vojne, ili službene) **podatke ili pismena**. Radnje su vezane za saopštavanje, predaju, činjenje dostupnim ili pribavljaju ovih podataka ili pismena. Subjekti kojima se one saopštavaju, predaju i odaju su: strane države, strane organizacije ili lica kojima služe počinioci dela špijunaže.

Za ovo delo **kazna je zatvor** u trajanju najmanje **3 godine**. Ukoliko se radi o kvalifikovanom delu špijunaže (organizovanje obaveštajne službe), **zatvor traje najmanje 5 godina**. Za rad u stranoj obaveštajnoj službi kazna je **zatvor najmanje 3 godine**.

**Odavanje poslovne tajne** je krivično delo predviđeno Krivičnim zakonom republika<sup>358</sup>. Sastoji se **u neovlašćenom saopštavanju ili pribavljanju, predaji ili na neki drugi način činjenju dostupnim podataka** (o kompjuterskom programu ili softveru) **koji predstavljaju poslovnu tajnu**. Sve se aktivnosti preduzimaju radi predaje podataka nepozvanom licu.

Ko to čini kazniće se **zatvorom od 3 meseca do 5 godina**, a ako se delo učini iz nehata, kazniće se **zatvorom do 3 godine**.

Ukoliko se to učini iz **koristoljublja** ili su u pitanju **posebno poverljivi podaci** ili se to čini radi objavljivanja ili korišćenja podataka u **inostranstvu**, učinilac će se kazniti **zatvorom najmanje 1 godinu**.

Uz ove dve vrste sankcija, mogu se kazniti preduzeća za **privredni prestup i prekršaj**, a odgovorni **pojedinci posebnim merama za kršenje konkurentske klauzule**.

Za **privredni prestup**<sup>359</sup> kažnjava se preduzeće i odgovorno lice ukoliko **povredi konkurentsku klauzulu**. **Kazna je novčana** za preduzeće ili drugog subjekta poslovanja u visini od 45.000 do 450.000 dinara, a za odgovorno lice od 3.000 do 30.000 dinara.

<sup>358</sup> Zakona o izmenama i dopunama Krivičnog zakona Republike Srbije, Službeni Glasnik R.S., br. 47/94, čl. 141.

<sup>359</sup> Zakon o preduzećima, čl. 439.

**Prekršaj**<sup>360</sup> postoji ako se odlukom organa uprave ne utvrde isprave i podaci koji se smatraju poslovnom tajnom ili se ne utvrdi način njihovog čuvanja. Tada odgovara preduzeće i odgovorno lice, a **kazna je novčana** i kreće se u visini od 15.000 do 150.000, odn. 900 do 9.000 dinara.

Ukoliko dodje do **kršenja konkurentske klauzule** od strane članova ortačkog društva, komplementara komanditnog društva, člana društva sa ograničenom odgovornošću i člana uprave, nadzornog odbora i izvršnog odbora direktora društva s ograničenom odgovornošću, akcionarskog društava i društvenog i javnog preduzeća, tada su **mere** koje je moguće izreći sledeće<sup>361</sup>:

1. **prestanak radnog ili drugog ugovornog odnosa**;
2. **isključenje člana društva**;
3. **brisanje konkurentske delatnosti iz registra**;
4. **naknada štete**, odn. umesto nje preduzeće može tražiti: prepuštanje poslova učinjenih za svoj račun kao poslova učinjenih za račun preduzeća, prenošenje preduzeću koristi iz poslova zaključenih za tuđ račun kao poslova učinjenih za račun preduzeća, ustupanje preduzeću prava iz poslova zaključenih za tuđ račun kao poslova učinjenih za račun preduzeća.

I na kraju, kad bi se sumirale **odlike zaštite** kompjuterskih programa i softvera poslovnom tajnom kod nas, moglo bi se konstatovati sledeće:

**Prvo. Primena instituta poslovne tajne je moguća pri zaštiti kompjuterskih programa i softvera, a naročito u slučajevima "proizvodnje" za poznatog kupca.** To se obično radi za velike kupce koji mogu plaćati, pored cene gotovog proizvoda, i cenu njegovog razvoja. Pojavom kvalitetnih i moćnih PC, povezanih u mrežu, sve više se smanjuje tržište velikim mašinama i izradi sistemskih softvera po narudžbini. U poplavi raznih softverskih firmi sve se manje rade programi za određenog kupca jer se na sopstveni rizik proizvode raznovrsni programi za tržište. U takvoj situaciji **poslovna tajna ima smisla u fazi izrade i plasmana**, kako se novi program ne bi na tržištu pojavio kasno. Kad se softver pojavi na tržištu samo je pitanje vremena kad će postati predmetom reverzibilnog inženjerstva i debugiranja. Osobito se mora imati u vidu pojava hakera i pirata, koji "razbijaju" sve sigurnosne mehanizme, i što je program više zaštićen to je veći izazov. Rešenje, tada, nije u poslovnoj tajni, već u krivičnom zakonodavstvu.

---

<sup>360</sup> Zakon o preduzećima, čl. 440.

<sup>361</sup> Zakon o preduzećima, čl. 92.

**Drugo.** Naravno, ovaj oblik zaštite veoma se često predviđa u ugovorima sklopljenim prilikom nabavke "spoljnog" softvera i opreme, ali i odgovarajućim opštim aktima i ugovorima ukoliko se program izrađuje u organizaciji koja ga i koristi. Time *domet poslovne tajne biva ograničen i obuhvata uži krug lica* (pravnih i fizičkih) koji sa takvim programom ili softverom dolaze u vezu. To ujedno može predstavljati i njegovu prednost u odnosu na druge oblike zaštite.

**Treće.** Onda kad je moguća, i za programe i softver za koje je moguća, poslovna tajna predstavlja vrlo efikasan institut. Naročito za sve one objekte koji ne mogu da uživaju neki drugi vid zaštite.

**Četvrto.** Zaštita poslovnom tajnom ne isključuje druge vidove zaštite, već ih dopunjuje. Znači, *ona se može primenjivati paralelno sa drugim oblicima ne isključujući ih.*

**Peto.** Kad bi se bolje razradio i regulisao ovaj institut zaštite i više primenjivao u zaštiti kompjuterskih programa i softvera, *poslovna tajna bi bila vrlo čvrst zaštitni "omotač"*, tim više, što ona može pojedinačno da rešava određene probleme sa određenim kategorijama ljudi u određenim organizacijama i za određene kategorije podataka.

**Šesto.** Može se, ipak, reći da je *poslovna tajna efikasnija kad su u pitanju zaposleni, dok "dah" gubi od spoljnih počinioaca*, naročito joj izmiče jedna posebno važna kategorija, bivši zaposleni, koja je, po podacima, upravo kritična tačka svake softverske kuće.

Ovaj oblik zaštite treba kod nas tek razvijati uz svest o svim njegovim nedostacima i pogodnostima, kao i uloge koju može imati.

# GLAVA 4

## ZAŠTITA BAZA PODATAKA

|           |  |            |
|-----------|--|------------|
| <b>1.</b> | <b>Uvodne napomene o zaštiti baza podataka</b>                       | <b>328</b> |
| <b>2.</b> | <b>Objekt zaštite</b>  | <b>330</b> |
| 2.1.      | <i>Pojam baze podataka</i>   | 330        |
| 2.2.      | <i>Vrste baza podataka</i>   | 332        |
| <b>3.</b> | <b>Oblici zaštite</b>  | <b>333</b> |
| 3.1.      | <i>Baze podataka i nacionalni propisi</i>                            | 333        |
| 3.1.1.    | <i>Baze podataka i zaštita pravom sui generis</i>                    | 338        |
| 3.1.2.    | <i>Baze podataka i zaštita na osnovu srodnih prava</i>               | 339        |
| 3.1.3.    | <i>Baze podataka i autorskopravna zaštita</i>                        | 340        |
| 3.1.4.    | <i>Baze podataka i regulisanje zaštite od nelojalne konkurencije</i> | 342        |
| 3.2.      | <i>Baze podataka i međunarodna zaštita</i>                           | 343        |
| 3.2.1.    | <i>Bernska konvencija za zaštitu književnih i umetničkih dela</i>    | 344        |
| 3.2.2.    | <i>Sporazum o trgovinskim aspektima prava intelektualne svojine</i>  | 347        |
| 3.2.3.    | <i>Direktiva o pravnoj zaštiti baza podataka</i>                     | 348        |
| 3.3.      | <i>Zaštita baze podataka po našem pravu</i>                          | 354        |
| 3.3.1.    | <i>Baze podataka kao objekt zaštite</i>                              | 354        |
| 3.3.2.    | <i>Uslovi zaštite</i>  | 355        |
| 3.3.3.    | <i>Subjekti koji uživaju zaštitu</i>                                 | 355        |
| 3.3.4.    | <i>Sadržina autorskih prava</i>                                      | 356        |
| 3.3.5.    | <i>Sadržina srodnih prava</i>  | 356        |
| 3.3.6.    | <i>Ograničenja prava</i>   | 357        |
| 3.3.7.    | <i>Trajanje prava</i>  | 358        |
| 3.3.8.    | <i>Zaštita prava</i>   | 358        |

## 1. Uvodne napomene o zaštiti baza podataka

Svedoci smo žestoke ekspanzije i eksplozije raznih baza podataka. Sve je prisutniji razvoj mas-industrije baza podataka i sve uvažnije posebno tržište koje obuhvata čitav kompleks proizvoda i usluga vezanih za njih. Razvoj i eksponencijalni rast baza zahteva znatne investicije naročito u ljudske, tehničke ili finansijske izvore, često mnogo više nego u programiranje sistema<sup>1</sup>. Istovremeno one se mogu kopirati za neznatnu cenu. Ogromne investicije u moderna informaciona "stovarišta" i sisteme za pretraživanje zahtevaju i represije u odnosu na aktivnosti pirata i nelojalnih konkurenata. Neautorizovani pristupi i "kupljenje" sadržaja mogu imati velike ekonomske i tehničke konsekvence, tim više što su baze vitalna "alatka" u razvoju informacionog tržišta pošto se koriste u velikim varijetetima u odnosu na druge aktivnosti i industrije. Takodje, sve je prisutnija opasnost da se sadržaj baze otkrije ili elektronski rearanžira bez autorizacije, i da se uveća "proizvodnja" baza indentičnog sadržaja. Ranije, dok nisu postojali elektronski digitalizovani procesi i razni medijumi na kojima su bila fiksirana autorska dela, ona su bila međusobno izolovana različitim fiksirajućim i reproduktivnim tehnikama. Danas su te tehnike promenjene. Kompjuterizovano čuvanje i pretraživanje sistema, fizički limiti i sl. omogućuju da se stalno koriste različite vrste uspostavljenih zbirki. Digitalizacija je donela promene koje se vide i u "inteligentnoj primeni" koja se sve više koristi umesto "veštačke inteligencije" jer su nastali kompjuterski programi koji sami stvaraju baze. Zahvaljujući elektronskoj obradi podataka funkcija selekcije se transformiše i tranzituje od autora ka korisniku, čak i kad se kasnije sprovodi, na sadržajima baze, korišćenjem posebnog softvera. Metode elektronske obrade menjaju prirodu onoga što nastaje u zbirkama čiji sadržaji su uredjeni (sačuvani), ili kojima se pristupa elektronski. Razlike su sve vidljivije kad se radi o ovim i neelektronskim zbirkama ili antologijama. Posebno je pitanje prirode proizvoda nazvanog "kompilacija" i novih zbirki - baze. Tim više, što su baze pod udarom piratstva jer se lako mogu reprodukovati smanjivanjem troškova i postizanjem velike brzine korišćenjem modernih komunikacionih mreža. To je bio imperativ za preduzimanje posebnih mera da bi se obezbedila prava autorima i nosiocima prava, ali i izazov predstojećim neminovnim promenama Bernske konvencije, jer sadašnje odredbe nisu u stanju da sve to obuhvate.

Same su baze podataka, otuda, od sredine 70-ih, postale sve interesantniji objekt zaštite, pogotovo zbog:

---

<sup>1</sup> Tapper C., Computer Law, London, Longman, 1989., str. 50.

- **uvećavanja broja i ubrzavanja razvoja tržišta usluga vezanih za ASCII baze podataka**<sup>2</sup>, pri tom, izuzetno se uvećava korišćenje javnih baza i servisa, pogotovo naučnih, pravnih i finansijskih, osobito u SAD. Međutim, u mnogim zemljama baze još uvek nisu dovoljno prisutne, naročito ne one sa podacima o organizacijama, pravnim sistemima, aktima, odlukama, i sl., čime se sve više produbljuje jaz, naročito između SAD i ostalih. S druge strane, enormno raste udeo privatnih baza, naročito u zemljama kod kojih to ranije nije bilo izraženo (V. Britanija, Nemačka). Osim toga, od vitalne važnosti je pojava i **razvoj međunarodnog tržišta usluga** ovih baza;
- **povećavanja broja i značaja tržišta videotekst servisa**, inače, više karakterističnog za Evropu, nego za druge regione<sup>3</sup>. Tako se računa da je u Evropskoj Uniji 1989. godine bilo oko 25.000 videotekst servisa, a najveći broj njih je lociran u Francuskoj (u kojoj je u to vreme postojala i najveća instalirana baza sa oko 5 miliona videotekst terminala). Kako se videotekst komunikacioni medijumi mogu koristiti za različite svrhe od igara do elektronske pošte, jasno je koliki značaj ovo tržište ima. Zbog potrebe da se ovi servisi međusobno povežu ubrzano radi i na osiguranju standarda kako bi nacionalne mreže mogle da obezbede nesmetani međunarodni videotekst saobraćaj;
- **svakodnevnog i sve bržeg rasta tržišta CD ROM proizvoda i povećanje CD ROM baza podataka**<sup>4</sup>. CD ROM se sve više primenjuje u raznim domenima od medicinske dijagnostike do industrijske ili umetničke grafike i kompletnih enciklopedija. Dok je krajem 80-ih u ovoj oblasti dominirala SAD, dotle se u 90-im sve više eksponira Japan, a od evropskih zemalja Francuska, V. Britanija i Nemačka;
- **pojave novih medijuma za dostavljanje i prenos podataka** uključujući i satelitske i radio-relej kanale. Prenos se prilagođava velikom broju korisnika koji dobijaju raznovrsne podatke (npr. o cenama na raznim tržištima, rezultatima nadmetanja, i sl.) koristeći mogućnosti servisa audiotekstova, elektronskog izdavaštva, mreža tipa npr. DAINE u Evropskoj Uniji, ili servisa za elektronske informacije<sup>5</sup>. U razvoju ovih medijuma i servisa poseban je problem fragmentalizacija među zemljama, kao i postojanje jezičkih, pravnih ili tehnoloških razlika, što prouzrokuje podizanje barijera među njima.

<sup>2</sup> Samo 1989. godine u svetu vrednost on-line baza i real-time informacija bila je oko 8.5 biliona ECU, a u Evropi je taj iznos bio oko 2 biliona, po podacima Commission of the European Communities, Proposal for a Council Directive on legal the protection of databases, COM (92), 24 Final - SYN 393., str. 6 - 8.

<sup>3</sup> Commission of the European Communities, op. cit., str. 8 i 9.

<sup>4</sup> Commission of the European Communities, op. cit., str. 9 i 10.

<sup>5</sup> Commission of the European Communities, op. cit., str. 10 - 13.

Medjutim, pored svih ovih pojava sve je prisutnija i neravnoteža izmedju zemalja u razvijanju same industrije baza podataka, čija se komercijalizacija kritično približava bespravnoj prodaji proizvoda (npr. memorijskih čipova, digitalnih traka, CD ROM diskova sa bitnim bazama). Zbog toga njihova ekonomska budućnost zahteva obavezno postojanje odgovarajuće pravne zaštite ne samo elemenata koji mogu biti, manje ili više, relevantni za korisnika ili konkurenta, već i samih baza kao celine. No, mnogi pravni režimi uopšte ne sadrže zaštitni omotač za baze, niti je ona, od sredine 80-ih, od kada se i potencirala, konzistentna i harmonizovana. To je izazvalo mnogobrojne dileme i povećalo broj problema koje treba razrešiti. Tako se postavljalo pitanje šta se, u stvari, štiti: baza kao takva ili dela koja su u nju inkorporisana? Potom se postavljalo pitanje kako samu bazu tretirati - kao neko posebno delo intelektualne svojine ili kao zbirku, kolekciju, kompilaciju, antologiju ili tome slično delo? Poseban je problem nastao oko tumačenja uslova koje treba baze da zadovolje da bi mogle da uživaju zaštitu, naročito oko originalnosti i različitih standarda koje u njenom određivanju postoje u raznim zemljama. Ništa manje nije značajno ni pitanje tretmana stvaranja baze, a od dilema posebno je zanimljiva ona vezana za prirodu dela, kolektivnu ili individualnu. Isto je toliko bitno i razgraničenje izmedju ovlašćenja korišćenja baze ili njenog dela. Naravno, posebne su dileme bile vezane za formu u kojoj se baza nalazi i relevantnost te forme za odredjenje njenog tretmana, odn. ima li razlike ukoliko je baza elektronska ili u nekoj drugoj formi (npr. papirnoj)? Pitanje dužine trajanja zaštite izazivalo je razne solucije i dovodilo do mnogobrojnih rasprava, teorijskih i sudskih.

## 2. Objekt zaštite

### 2.1. *Pojam baze podataka*

Mnogi pravni problemi vezani za zaštitu proističu iz nejasnog definisanja njihovog predmeta. Taj se problem javio, donekle, i u vezi sa bazama podataka. One su **opšte definisane kao korisne, organizovane zbirke struktuiranih podataka koji se nalaze u različitim datotekama medjusobno povezanim programima koji omogućuju pristup korisnicima**<sup>6</sup>. U suštini to je bilo kakva zbirka uskladištenih podataka i/ili informacija, bez obzira kako su izražene, a koje su organizovane i uredjene saglasno nekom osnovnom principu kompiliranja u dela ili materijale, i koja

<sup>6</sup> Powers M., Chenel P., Crow G., Structured Systems Development, Analysis, Design, Implementation, Boston, Boyd&Fraser Publishing Company, 1990., str. 861; Weinberg G., Geller D., Computer Information Systems, An Introduction to Data Processing, Boston, Little, Brown and Company, 1985., str. 633.

omogućuje korisniku pronalaženje (trenutno ili najbrže moguće), i korišćenje pojedinačnih sadržaja<sup>7</sup>.

Što se, pak, pravnog odredjenja tiče, **baza podataka** (*data base*) se definiše kao:

1. **zbirka**, redje kao **kompilacija**, pri čemu se pod **zбирком** (*collection*) podrazumeva delo nastalo skupljanjem i skladištenjem već postojećih materijala ili podataka koji su odabrani, povezani ili uredjeni na takav način da za rezultat imaju originalno delo svog autora<sup>8</sup>, a pod **kompilacijom** (*compilation*) se podrazumeva delo prerade, u kome su vidljive karakteristične osobine tog, već postojećeg, dela;
2. da su podaci koji se u njoj nalaze **organizovani i uredjeni po odredjenim principima**;
3. da su podaci, materijali i/ili dela koji čine zbirku tako odabrani, povezani i uredjeni da **čine intelektualnu tvorevinu i novo delo**, pri tom se pod **delima** podrazumevaju literarna, umetnička, muzička ili neka druga autorska dela, a pod **materijalima** tekstovi, zvuci, slike, brojevi, činjenice, podaci, ili kombinacije svih njih; i
4. da su ti odabrani, sistematizovani i struktuirani podaci **materijalizovani na nekom nosiocu** (magnetnom, optičkom, električnom, ili nekom drugom).

Pravljenje zbirke predstavlja, po pravilu, intelektualnu aktivnost koja je rezultat uloženi napora, vremena, veština, znanja njenog/njenih tvoraca u organizovanju i prezentiranju podataka, kao i u otelotvorenju same baze. Pošto tvorac baze kreira modele podataka, tezaure, indekse ili sisteme ukrštanja, ovo su neophodni intelektualni koraci kojima se ne stvara mehanička zbirka i aranžman dela i/ili materijala, već je vrednost upravo u takvom "doziranju" sirovog materijala čijim procesiranjem nastaje novo derivativno delo, a ono najčešće biva prepoznatljivo kao autorsko. Budućnost elektronskog sakupljanja i manipulisanja podacima je u beskonačnosti procesa (*open-ended*) i stalnoj evoluciji uredjenja njihovog sadržaja. Bez obzira na sve veće mogućnosti automatskog stvaranja baze i održavanja uz pomoć inteligentnih ili ekspertnih sistema ugrađenih u softver, one, ipak, predstavljaju delo ljudskog napora. Čak i onda kada se pojavljuju kao kompjuterski generisana ili

<sup>7</sup> Rickestone S., Copyright and Data Bases, Edicija: Essays on Computer Law, Melbourne, Longman Chechire PTY Limited, 1990., str. 67.

<sup>8</sup> Copyright Act of 1976., US, & sect: 103.

kompjuterski asistirana dela i tada one predstavljaju, u krajnjem slučaju, tvorevinu određene osobe<sup>9</sup>.

## 2.2. Vrste baza podataka

U rešavanju sporova u zaštiti baza podataka i njihovih sadržaja sve relevantnija postaje i njihova klasifikacija na određene tipove, vrste, naročito sa aspekta zaštite podataka i dela koja sadrže. Pored podele na pravničke, medicinske, geografske, demografske, statističke, lingvističke i druge baze, one mogu biti i:

1. **Bibliografske baze** (*bibliographic data bases, bibliographic utility, networked bases*) su one koje sadrže zaglavlja, naslove ili druge identifikacione oznake, uređene po nekom sistemu ili principu. One ukazuju korisniku gde je locirano određeno delo ili informacija, kao što je monografija, sudski slučaj i sl. Ove baze privlače veliku pažnju te su mnogi stari i novi sudski slučajevi u V. Britaniji i Australiji pokrenuti upravo oko njihove zaštite, kao i statusa u njih smeštenih podataka<sup>10</sup>.
2. **Baze abstrakta ili rezimea** (*abstracts data bases, summaries data bases*) su one kojima se korisnicima daju neposredna znanja i ekstrakt o delu bez čitanja celog teksta. Pravljenje abstrakta je često povreda autorskih prava ukoliko je učinjena bez autorizacije i istovremeno su povod za rasprave da li se mogu autorskopravno zaštititi.
3. **Baze integralnog teksta** (*full-text data bases*) su one koje korisniku neposredno daju kompletan tekst nekog dela, npr. kompletne biblioteke ili potpuni tekstovi sudskih odluka. Pored svih prednosti ove su baze izazvale brojne rasprave zbog čestog izostavljanja dozvola za unošenje kompletnih dela, a posebno zbog daljih mogućnosti njihovog kopiranja i reprodukovanja.
4. **Ostale vrste baza** su adresari; imenici; spiskovi - potrošača, nabavljača, materijala, sastavnica, elemenata; katalozi roba i usluga; ili rokovnici. One su izazivale brojne sporove ne samo oko zaštite baze i/ili sadržaja, već i oko potrebe dobijanja dozvola pojedinaca da se njihova imena nadju u bazi, kao i na koji su način povezana sa imenima drugih.

<sup>9</sup> Reed C., Computer Law, London, Bleckstone Press, 1993., str. 83 i 84.

<sup>10</sup> Rickestone S., op. cit., str. 69 - 71.

Postojanje ovih vrsta baza svakako je bitno, no, nužno je istaći da se sadržaji u njima mogu naći u bilo kom obliku i na bilo kom medijumu, a za zaštitu je relevantno tek ukoliko se zadire u njihovu suštinu.

### 3. Oblici zaštite

#### 3.1. Baze podataka i nacionalni propisi

Pravna zaštita baza podataka uglavnom se vezuje za zemlje Evropske Unije<sup>11</sup>, SAD<sup>12</sup>, Japan i Australiju, a u novije vreme i za poneke zemlje Srednje i Istočne Evrope.

Prvi propisi u zemljama EU doneti su na samom početku 80-ih. Tako je to u **Australiji** bilo 1984. godine sa donošenjem amandmana na Zakon o autorskom pravu (*Copyright Amendment Act*), a u **SAD-u** je to bilo implicitno moguće još po Zakonu o autorskom pravu iz 1976 (*Copyright Act*) kojim su se definisale kompilacije u koje su se mogle svrstati i baze<sup>13</sup>. **Japan** je, međutim, 1986. godine Zakonom o autorskom pravu (*Copyright Law*) eksplicitno predvideo zaštitu "delo baza podataka". Po odredbama ovog Zakona pod bazama se podrazumevaju "one koje na osnovu nekog razloga prikupljanja ili sistematskog konstituisanja sadrže takve intelektualne tvorevine koje se mogu zaštititi kao posebna, nezavisna dela". Dalje se ovim aktom baze definišu i kao "agregat informacija, kao što su članovi propisa, brojevi ili dijagrami koji su sistematski konstituisani tako da takva informacija može biti pretražena računom"<sup>14</sup>.

<sup>11</sup> Tako je o stanju pravne zaštite baza podataka razmatrano i u: Report of Intellectual Property Rights Sub - Group on Intellectual Property Rights to the DTI Multimedia Industry Advisory Group, UK, 1995., str. 12. Dokument preuzet sa Interneta.

<sup>12</sup> Lehman B., Baker J., Oblon M., Intellectual Property and National Information Infrastructure (The White Paper), str. 64. Dokument preuzet sa Interneta.

<sup>13</sup> Po US Copyright Act, As Amended, Chapter 1. Subject matter and scope of copyright, & sect: 101. Definition: "**kompilacije** nastaju prikupljanjem i satavljanjem ranije postojećih materijala ili podataka koji su odabrani, uskladjeni ili aranžirani tako da od njih nastaje delo koje je i samo originalno autorsko delo. Termin kompilacija uključuje i kolektivno delo." Tekst preuzet sa Interneta.

<sup>14</sup> Article 12 bis, Article 2(1), Japan Copyright Law.

Pod uticajem prava Evropske Unije zemlje Istočne i Centralne Evrope, početkom 90-ih, počinju harmonizaciju svog prava radi usaglašavanja sa sporazumima o saradnji i pomoći<sup>15</sup>.

**Ruska federacija** unela je u svoj Ustav odredbe o regulaciji prava intelektualne svojine. Posebnim zakonom regulisana je pravna zaštita računarskih programa, čipova i baza podataka preuzimanjem rešenja iz odgovarajućih direktiva EU. Baze se zaštićuju kao zbirke, naravno ako su originalne po selekciji i aranžmanu podataka koji je sačinjavaju. Zaštita traje za života autora i 50 godina nakon smrti. Posebno su regulisana materijalna prava autora koji je bazu stvorio u radnom odnosu i koja na osnovu ugovora o zapošljavanju pripadaju poslodavcu. Nosioc ekonomskih prava može bazu i registrovati kod *Ruske agencije za zaštitu kompjuterskih programa, baza podataka i integrisanih kola*.

**Poljska** se potpisujući 1990. godine sporazum sa SAD-om i 1991. sa EU, obavezala da će u roku od 5 godina osigurati adekvatnu zaštitu prava intelektualne svojine. Međutim, novi set zakona koji je donela nije obuhvatio posebnu zaštitu baza podataka, već ih je, ukoliko zadovoljavaju uslov originalnosti, prepustio autorskopravnoj zaštiti. Istovremeno Zakon o nelojalnoj utakmici iz 1993. godine zabranio je diseminaciju netačnih informacija ili otkrivanje informacija iz baza. Međutim, posebnih, sui generis, prava zaštite baza u poljskom pravu nema.

**Madjarska**, nakon Dekreta iz 1983. godina kojim je predviđena zaštita računarskih programa, iako obavezna po sporazumu potpisanim sa EU, novim Zakonom o autorskim pravima nije predvidela posebnu zaštitu baza. Ukoliko zadovoljavaju uslov originalnosti moguće ih je zaštititi kao zbirke. Gotovo je isti slučaj i sa **Češkom Republikom**, čija promena Zakona o autorskom pravu nije regulisala posebnu zaštitu baza, ali je predviđena mogućnost zaštite pravom nelojalne utakmice u okviru Trgovačkog zakonika. Naime, nepošteno vadjenje informacija iz baze je okvalifikovano kao parazitsko ponašanje i na odgovarajući način sankcionisano.

**Rumunija** je Zakonom o autorskom pravu predvidela istovetnu zaštitu baza kao i bilo kog drugog autorskog dela.

<sup>15</sup> O stanju Prava intelektualne svojine u zemljama Istočne i Centralne Evrope (*Legal Aspects of Information Services and Intellectual Property in Central and Eastern Europe*) dati su prikazi na Konferenciji koju je organizovala Evropska komisija novembra 1994. godine u Luksemburgu, a čiji su materijali objavljeni od Komisije i *Centre de Recherches Informatique et Droit* februara 1995. godine. Materijali su preuzeti sa Interneta.

Zakonom o autorskom i susednim pravima **Bugarske** predviđena je zaštita baza podataka autorskim pravom. Osoba koja je izabrala i aranžirala materijale i/ili dela u bazi smatra se autorom i ima ista prava kao i bilo koji drugi autor. Ostala se prava regulišu posebnim ugovorima.

Prvim zakonodavnim pokušajima regulacije baza podataka prethodili su sudski sporovi u kojima su se veoma često iskristalisali stavovi koji će, potom, biti uneti u zakone. Jedan od najpoznatijih je bilo slučaj *Feist Publications v. Rural Telephone Service* iz 1991. godine<sup>16</sup>. U tom slučaju sud je smatrao da "bele strane" telefonskih imenika ne mogu biti zaštićene autorskim pravom jer ne sadrže elemente "originalnog utiska" koji se od autorskih dela zahteva. Sud je odbio žalbu koja se odnosila na "industrijsku zbirku" ili primenu teorije "u znoju lica svoga" (*sweat-of-the-brow*) vezanu za originalnost koju je niži sud koristio za odlučivanje o potvrđivanju autorskopравnih zahteva u telefonskim imenicima i jednostavnim činjenicama kompilacija. Stav Vrhovnog suda je bio da samo ako postoji neka kreativnost u prikupljanju ili aranžiranju činjenica njihova kompilacija će moći biti zaštićena autorskim pravom. Činjenice same po sebi, smatrao je sud, mogu se kopirati samo ako za to postoji volja ili to čini samo onaj ko je pripremio takvu kompilaciju.

Sud je u ovom slučaju više razmatrao stavove i diskutovao o razlozima za autorskopравnu zaštitu kompilacija uopšte<sup>17</sup>. Otuda je odluka proizvela naročito veliki uticaj u odnosu na sve one zahteve za autorskopравnom zaštitom koji su se ticali kompilacija. Pogotovo što oni koji vrše kompilacije elektronski smatraju da je njihova prava vrednost u podacima, a ne u načinu na koji oni mogu biti aranžirani. Rearanžiranje digitalnih informacija je jednostavno i jeftino.

Jedna je grupa servisa koji se bavi elektronskim informacijama nakon *Feist* slučaja smatrala da je takva odluka potkopavanje njihovog ekonomskog interesa u pripremanju kompilacija i njihove široke dostupnosti javnosti. Drugi su videli ovu odluku kao otvaranje novih horizonata i mogućnosti za pravljenje novih informacionih proizvoda potrebnih potrošačima. Između ostalog i zato što je Sud izneo nekoliko iznenadjujućih razloga za prevladavanje shvatanja Biroa za autorskopравnu zaštitu SAD, koji će ovu odluku pratiti konstatacijom o "bačenoj bombi" na američko autorsko pravo.

<sup>16</sup> Samuelson P., Copyright Law and Electronic Compilations of Data, Communications of the ACM, no. 2/92., str. 27 - 32.

<sup>17</sup> Prvi sudski slučajevi ticali su se prevashodno legitimiteta originalnosti uloženi napora u pravljenju zbirke uopšte, da bi se kasnije direktno ticali i baza. Tako je u V. Britaniji poznat spor *Financial Information Inc v. Moody's Investors Services Inc.*, iz 1986, kao i *West Publishing C. v. Mead Data Control Inc.*, iz iste godine u SAD.

O čemu se, u stvari, radilo?

*Rural Telephone Service* je korporacija ovlašćena za vršenje komunalnih usluga koje obuhvataju, pored ostalog, i telefonski servis za nekoliko gradova na severu Kanzasa. Ona je publikovala godišnji telefonski imenik. "Bele strane" su sastavni deo imenika i sadrže alfabetski spisak imena pretplatnika, grada u kome žive i brojeva telefona. *Rural* je distribuirala ove imenike bez ikakvih finansijskih opterećenja za svoje pretplatnike, a profit je postizala reklamama koje su se nalazile na "žutim stranama" imenika.

*Feist Publications* je firma koju je formirao profesor istorije na višoj školi, po imenu Feist, na severu Kanzasa. Ovaj preduzimljivi čovek je smatrao da je nužno obezbeđivanje jedinstvenih spiskova pretplatnika koji su, doduše, bili sastavni deo telefonskih imenika svih 11 telefonskih servisa iz tog dela Kanzasa. Otišao je kod svih 11 kompanija po dozvolu za korišćenje njihovih "belih strana" u svom imeniku. Sve, sem *Rural Telephone*, su mu dale zahtevanu dozvolu.

Suočivši se sa izborom izmedju nekompletnog imenika i neautorizovanog kopiranja *Rural*-ovih spiskova, *Feist* se odlučio na ovo drugo. Pored toga, znajući da telefonske kompanije, po pravilu uvek, stavljaju izmišljene spiskove u nameri da uhvate one koji kopiraju informacije iz njihovih imenika, *Feist* je iznajmio ljude da provere blizu 5.000 spiskova u *Rural* imeniku koje je hteo da stavi u svoj imenik. Medjutim, 4 lažna spiska su se, ipak, pojavila i kod njega. Više od 1.300 spiskova od *Feist*-ovog imenika, od skoro 47.000, je bilo identično sa *Rural*-ovim, a oko 3.600 je bilo skoro isto osim što je *Feist* dodao i adrese za prijavu na pretplatu.

*Rural Telephone* je tužio *Feist* za povredu autorskih prava i dobio spor u prvoj instanci. Sudija nižeg suda je smatrao da je tužiteljevo pravo povredjeno, jer je u pitanju povreda autorskog prava u odnosu na telefonski imenik koji je, po teoriji "u znoj lica svoga", originalan. U ovom slučaju je, takodje, prvostepeni sud video i povredu autorskih prava zbog neautorizovanog kopiranja imenika u svrhu postizanja ekonomske koristi u konkurentskoj borbi. Žalbeni sud je potvrdio isto obrazloženje, uz dopunu da je u pitanju i delo nelojalne utakmice, jer je *Rural Telephone* odbila da da dozvolu za "bele strane" zbog ubedjenja o motivisanosti *Feist Publication*-a za preuzimanje monopola žutih strana.

Spor je nastavljen i dalje, ali sa mnogo iznenadjenja, prvo iznenadjenje je u prihvatanju Vrhovnog suda da razmatra molbu *Feist*-a iako su postojali i drugi ranije podneti zahtevi. No, i stav na kome je sud bazirao svoju odluku bio je, takodje, veoma

diskutabilan baš zbog problematičnosti originalnosti spiskova. Vrhovni sud je, ipak, zaključio da treba odgovoriti sa "ne". Jedan od argumenata je u daljem favorizovanju teorije "u znoju lica svoga" jer se autorsko pravo stiče i zbog toga što je rezultat ljudskog rada, bilo da su "proizvodi uzvišene umetnosti ili inventivnosti, bilo da su samo svetovni, ovozemaljski naponi". Suština imovinskih prava, usled toga, proističe iz ulaganja u rad u kreaciju, a to je duboko ukorenjeno u anglo-američku jurisprudenciju. Pravo intelektualne svojine SAD-a, međutim, uvek ima i specifična pravila o vrstama intelektualnog vlasništva koja mogu biti kvalifikovana za zaštitu u određenim okolnostima. Neće sve u šta je uložen neki rad moći biti zaštićeno. Autorsko pravo traži da to bude još i originalno ili da postoji takav "utisak". Termin "originalnost" nikada nije definisan u zakonima SAD-a. Kongres je smatrao da sudovima treba dozvoliti da od slučaja do slučaja i na svoj način razvijaju shvatanja o tome. Otuda, tokom godina američki sudovi su definisali originalnost na različite načine. Tokom XIX veka u odlukama sudova delo ima originalnost samo ako "je ima za osobu koja traži da bude autor" i ako nije kopija nekog drugog dela. *Rural*-ove "bele strane" su zadovoljavale ove standarde. Zbog toga, standard "u znoju lica svoga" za originalnost ima svoju osnovu u odlukama sudova. No, po autorskom pravu SAD-a zaštita kompilacija informacija je, ipak, skoro na samom početku.

Ova odluka je bila značajna posebno za one firme koje su se počele baviti prodajom ili licenciranjem elektronskih informacija u posebnim, specijalizovanim oblastima. Tipično autorsko pravo nije bilo u stanju da obezbedi njihovu zaštitu, pa je ovaj slučaj upravo za neke od njih bio ta bačena bomba. Naročito za one koji se bave uslugama vezanim za elektronske informacije smeštene na CD ROM radi njihove široke distribucije javnosti. One mogu birati da li će se osloniti na dozvole za nove aranžmane na određeno vreme, ili će pristupiti kriptografiji pri kojoj će elektronski podaci biti dostupni javnosti, ali sa striktno kontrolisanim pristupima radi očuvanja izvora. Naravno, osnovni razlog leži u mnogo lakšem i jeftinijem kopiranju digitalnih nego štampanih informacija. Lakoća kopiranja učinila je razumljivom želju firmi za obezbedjenjem svojih vrednih digitalnih proizvoda od neovlašćenog pristupa. Slučaj *Feist Publication* pokazao je da je dozvoljeno kopiranje činjenica samo ukoliko ih neko aranžira na drugačiji način (sa postojećom tehnikom bilo kakva razlika može se lakše napraviti), ali da zabrana ličnom pristupu digitalnim informacijama mora postojati i biti, čak, i veća.

Zahvaljujući ovom slučaju neke su firme smatrale da postojeće rešenje u zaštiti nije dovoljno, te su zatražile patentnu zaštitu za postupak organizovanja podataka uključenih u baze. Ipak patentna zaštita baza podataka je još uvek kontraproduktivna ne samo u tehničkim, već i u pravničkim krugovima, bar isto koliko je u početku to bila autorskopravna zaštita kompilacija. Znači, ne treba se iznenaditi ukoliko se uskoro većina elektronskih baza podataka i informacija nadju u fokusu patentne zaštite.

Ipak, treba napomenuti da "bele strane" telefonskih imenika nisu kvalifikovane za autorskopravnu zaštitu ukoliko ne sadrže neki originalni način prikazivanja, sortiranja ili uređivanja sadržaja.

Što se pozitivnih propisa tiče, uglavnom, su se iskristalisale četiri solucije: zaštita *sui generis* pravom, zaštita srodnim pravom, zaštita autorskim pravom ili zaštita od nelojalne utakmice. U određivanju koji će se pravni režim izabrati kao najpogodniji za zaštitu baza podataka, nacionalna su se prava morala opredeliti za onaj režim koji najsigurnije obezbeđuje stabilnost i pouzdanost, zaštitu stečenih prava i investicija, kao i koherentnost sa zaštitom drugih sličnih dela i konzistentnost sa nacionalnom politikom. Takodje, morala se postići i izbalansiranost tretmana kreatora i korisnika baza.

### 3.1.1. Baze podataka i zaštita pravom *sui generis*

Jedno od rešenja bila je *sui generis* zaštita<sup>18</sup>. No, ubrzo se počela isticati njena nepodesnost, nekad sasvim opravdano, ali ne i u potpunosti. To se upravo desilo sa predlozima Komisije Evropske Zajednice<sup>19</sup> po čijem mišljenju se ova zaštita pokazala neodgovarajućom, jer ovaj pravni režim nije mogao biti, zbog nerazvijenosti i kratkotrajnosti, potpun i dovoljan u određenim delovima. Prilagođavanje specifičnim karakteristikama baza podataka nije moglo obezbediti pouzdanost niti stabilnost sve dok ne bi prošao izvesan period za koji bi svaka juresprudencija razvila stalne interpretacije teksta novog zakonodavstva u tako kompleksnom tehničkom polju.

Takodje, *sui generis* zaštita ne bi bila u stanju da obezbedi reciprocitet tretmana za baze van nacionalnih granica, sem u onim zemljama koje imaju ista rešenja ili ukoliko bi se, bilateralnim sporazumima, ona ugovarala. Naravno, postojala je mogućnost da se donošenjem odgovarajućeg novog multilateralnog međunarodnog sporazuma (npr. konvencije, smernica, preporuke) ovaj tip zaštite predvidi kao dominantan i preporuči za nacionalna zakonodavstva, uz sve očekivane i neočekivane rizike koji zbog odlaganja ili neprihvatanja nastaju.

Negativistički stavovi prema *sui generis* zaštiti ne mogu se *a priori* prihvatiti pošto je u pitanju zaštita jedne sasvim specifične intelektualne tvorevine koja se, iz

<sup>18</sup> **Pravo *sui generis*** je posebna, specifična zaštita kojoj je osnov u tome što se određena tvorevina, u ovom slučaju baza podataka, shvata kao toliko specifična da se ne može podvesti ni pod jednu poznatu tvorevinu niti delo jer iza njega stoje izrazito sukobljeni interesi proizvođača i korisnika.

<sup>19</sup> Commission of the European Communities, op. cit., str. 31 i 32.

mnogobrojnih razloga, ne može tako simplificirano podvesti pod, do sada, poznate institute. Tim više, što je sam početak pravne zaštite bio idealna prilika da se izbegnu "tesni kalupi" tradicionalnog prava. Opravdanje "opšte neprihvatljivosti ili neunificiranosti ovakvog rešenja" svakako nije seriozno jer značaj koji ova hiper industrija ima, i sve više će imati, ukazuje na suprotno. Malo bi zemalja propustilo da mnogo što šta menja ukoliko za to ima dovoljno opravdanih razloga. A značaj ove industrije i tržišta je, svakako, jedan od najopravdanijih<sup>20</sup>.

### 3.1.2. Baze podataka i zaštita na osnovu srodnih prava

Izbor srodnih prava<sup>21</sup>, kao adekvatnog pravnog režima zaštite baza podataka, je jedan od mogućih ali ne i najbolji, zbog poteškoća sličnih onima koje su karakterisale režim *sui generis*.

Jedan od najvećih problema je u postojanju tzv "dvoniznog" sistema za one baze koje bi mogle da uživaju zaštitu samo srodnim pravima i onih koje bi, osim te, imale i punu autorskopravnu zaštitu. No, ovaj se problem može lako izbeći takvim razvojem potpune i koherentne zaštite srodnim pravom kojim bi se anulirala potreba za autorskopravnom zaštitom koja bi vremenom sve manje bivala pozivana u pomoć<sup>22</sup>.

Drugi je problem vezivan je za pretpostavku da bi mnogo manje zemalja ratifikovalo posebnu konvenciju nego što je to slučaj sa Bernskom konvencijom, između ostalog i zbog poteškoća oko primene principa nacionalnog tretmana<sup>23</sup>. Ovo obrazloženje teško da bi se moglo prihvatiti jer je pojednostavljeno u onolikoj meri uolikoj je i razvoj autorskog prava nekada i sada potvrda obrnutog. Naravno, ovi protivargumenti stoje prevashodno ako se imaju u vidu posebna srodna prava, a ne

<sup>20</sup> U prilog tome može poslužiti primer SAD-a koji nije ratifikovao Bernsku konvenciju sve do momenta kad su procene ukazivale da dalje ostajanje van Bernske Unije nije više celishodno i biva sve više štetno. To je bio signal za ratifikaciju i noveliranje autorskog prava.

<sup>21</sup> Po Besarović V., op. cit., str. 190., korišćenje termina **srodna** odn. **susedna prava** stvar je prihvatanja jezika iz koga se prevodi. Tako **srodna prava** potiču iz nemačkog jezika (*Verwandte Schutzrechte*), u italijanskom to su **koneksna prava** (*Dritti connessi*), a u francuskom i engleskom to su **susedna prava** (*Droit voisins, Neighbouring rights*). U terminologiji prava EU u početku se koristio termin susedna, da bi danas preovladala upotreba srodnih prava. Jugoslovenski Predlog zakona o autorskom i srodnim pravima prihvatio je očigledno termin srodna, mada su u prvim verzijama figurirala susedna.

<sup>22</sup> Commission of the European Communities, op. cit., str. 32 i 33.

<sup>23</sup> Commission of the European Communities, op. cit., str. 32.

primena analogije sa fonogramima<sup>24</sup> (čime su u nekim zemljama pokušavali pravnici da odgovore na izazov koje su baze postavile), tim više što ta analogija ne može biti odgovarajuća. Tvorac baze preduzima intelektualne aktivnosti u prikupljanju i proveru materijala koje je pripremio za ugradnju u bazu, uređujući ih na takav način da korisnik može efikasno da realizuje svoje potrebe, unoseći određenu "ličnu notu", napor i originalnost, čega nema kod fonograma. Osim toga, kod baza i hardver mora biti interaktivan, što nije slučaj sa optičkim diskovima na koje se smešta muzika ili fonogram. Klasifikovanje i indeksiranje, je neminovnost kad su u pitanju baze, za razliku od fonograma.

Ali, uspostavljanje određenih principa zaštite srodnim pravima počevši od specifičnosti baza u odnosu na čestu kolektivnost u kreiranju, brzu zastarivost, dominaciju interesa pravnih u odnosu na fizička lica, izraženost potreba, interesa i zahteva korisnika izražena je u većoj meri nego kad su u pitanju druga dela, kao što i mnoštvo drugog ukazuje da bi zaštita po ovom režimu mogla biti ne samo celishodna i poželjna, nego bi i isto toliko bilo potrebno da se razvije koliko se moraju prilagođavati, menjati i inovirati pravila autorskog prava.

### 3.1.3. Baze podataka i autorskoppravna zaštita

Pokazalo se da je najkomfortnije rešenje ponudjeno sa autorskoppravnom zaštitom. Njome se prevashodno obezbeđivalo bezbolno podvodjenje pod odredbe Bernske konvencije i lagodan pristup zaštiti. Uključivanjem baza u dela zaštićena autorskim pravom postepeno se gubi razlika u pravnim sistemima i strukturama u različitim zemljama, a inovacija zakonodavstva lakše se sprovodi. Iako se ovakvo rešenje u prvom trenutku činilo najbezbolnijim ipak su se tražili mnogobrojni odgovori na pitanja tipa da li ih predvideti kao posebna ili ih podvesti pod neko, već poznato, delo? Najčešće se pribegavalo njihovom podvodjenju pod omotač zaštite zbirki ili kompilacija, čime se gubila razlika između papirnih i elektronskih oblika, koja je u momentu pojave elektronskih baza predstavljala isto onoliko veliki kamen spoticanja koliko su to bili kompjuterski programi. Argumenti su se nalazili u komparaciji sa pisanim literarnim delima i pokušajima da se poistoveti "fiksiranje" podataka i/ili materijala u mašinski čitljivoj formi na odgovarajućim nosiocima sa bilo kojim "zapisivanjem" na papirni medijum. Zabune su nastajale kad je trebalo protegnuti termin "izdavanje", odn. "objavljivanje" u konvencionalnom smislu i na automatizovane baze. Poteškoće se produbljuju činjenicom da se ove baze mogu kontinuirano menjati iz

<sup>24</sup> **Fonogram je zabeležen zvuk, odnosno određeni niz zvukova na nosaču zvuka** (Predlog zakona, čl. 119.).

sekunda u sekund, pripajanjem ili brisanjem istih sadržaja, tako da je veliki problem šta se, u stvari, autorskim pravom štiti, i koji je to momenat u kom je baza "uhvaćena" za zaštitu? Takođe, rasprave se i dalje razbuktavaju oko određivanja da li neka kompilacija podataka (ili materijala) kakva je baza, poseduje dovoljno originalnosti pošto podaci u računar u često nisu posebno, kreativno, uređeni već se to postiže softverom i posebnim, ne retko kreativnim, originalnim korisničkim zahtevima za određenim podacima čijim zadovoljenjem se dobija novo delo. Poseban se problem postavio oko tumačenja značenja postupka "skidanja" (*downloading*) podataka (materijala) i smeštanja u računar. Naime, da li se "skidanje" može tretirati samo kao prosto skladištenje podataka (ili materijala) u mašinski čitljivoj formi ili se radi o novom delu? Komplikacije se produžavaju ukoliko "skinuti" podaci nisu fiksno uređeni na određeni način, nov, originalan, tako da postoji značajna sličnost između novog i ranije zaštićenog dela. I svakako, teško se tumači značenje termina "kopiranje" i reprodukovanje, kad svako uključanje baze može da se tretira kao svojevrsno reprodukovanje<sup>25</sup>.

Medjutim, tretmanom baze kao zbirke ili kompilacije obezbeđuju se ista ekskluzivna autorska prava u odnosu na korisnike, kao i kad su u pitanju bilo koje zbirke ili antologije. Ona se naročito odnose na kopiranje (pod kojim se podrazumeva reprodukovanje)<sup>26</sup>, objavljivanje, menjanje i adaptiranje kao i "izvodjenje".

Ova su prava uobičajena za sva autorska dela, po prirodi nisu apsolutna i čest su predmet brojnih ograničenja od kojih je za baze najznačajnije ono koje se odnosi na fer korišćenje i poslovanje. **Poštena upotreba** obuhvata odgovore na četiri najčešće postavljena pitanja<sup>27</sup>:

1. **svrhe i karaktera korišćenja**, odn. da li je upotreba u komercijalne ili neprofitne svrhe, kao što je obrazovanje ili privatne svrhe;
2. **prirode dela** koje je zaštićeno autorskim pravom;
3. **veliçine i znaçaja preuzetog dela** u odnosu na autorskopravno zaštićeno delo kao celine; i

<sup>25</sup> Većina ovih pitanja se postavlja pred praksu i teoriju američkog i engleskog prava koja su među prvima prihvatila autorskopravnu zaštitu baza podataka kao validnu soluciju, o čemu više kod Tapper C., op. cit., str. 50 - 61.

<sup>26</sup> Kad je u pitanju britanski *Copyright, Design and Patents Act 1988*, sect: 16(1)(a) i 17, "**kopiranje**" znači reprodukovanje dela u bilo kojoj materijalnoj formi, a to uključuje i smeštanje dela na bilo koji medijum u elektronskom smislu. Kopiranje uključuje i pravljenje privremenih ili slučajnih kopija za neku drugu upotrebu. U američkom Copyright Act & sect: 106(1) i 101., definisan je pojam reprodukovanje, a u vezi sa njim i kopije koje na osnovu reprodukovanja nastaju.

<sup>27</sup> US Copyright Act, & sect: 107.

#### 4. efekte korišćenja u onosu na potencijalno tržište ili na vrednost autorskopravno zaštićenog dela.

Ukoliko su odgovori na ova pitanja i faktore takvi da sud može utvrditi nepoštenu upotrebu u pitanju su povrede autorskih prava i prekršci će morati odgovarati za to.

Autorskopravnom zaštitom baza podataka zaokružuje se koherentni paket pravne zaštite kompjuterskih programa jer baze u suštini sadrže i programe kojima se memorišu i manipulišu materijali i dela, a koje je teško medjusobno odvojiti<sup>28</sup>. Čak je sve učestalije mišljenje da je autorskopravna zaštita baza, mada ne i najadekvatnija, ipak takva solucija koja rešava mnoge, iako ne sve, probleme vezane za njihovu zaštitu. Pitanje je, doduše, šta će biti sa novim problemima koji svakodnevno izviru iz razvoja informacionih tehnologija i telekomunikacija. Da li će se autorsko pravo moći izboriti sa njima?

#### 3.1.4. Baze podataka i regulisanje zaštite od nelojalne konkurencije

Pošto autorskopravna zaštita nije jedino rešenje za sve probleme koji nastaju u zaštiti baza u nekim zemljama su se počela tražiti i druge mogućnosti u posebnim pravnim režimima i institutima. Jedno od njih je zaštita od nelojalne utakmice i parazitskog ponašanja. Ona postaju naročito aktuelna u slučajevima neovlašćenog kopiranja ili "vadjenja" sadržaja iz baza kojim se žele postići, i postižu se, komparativne prednosti na tržištu bez velikih finansijskih, organizacionih, ljudskih, tehničkih i drugih napora i angažovanja. Koliko je parazitsko ponašanje bivalo više isplativo to je rasla i potreba da se ono sankcioniše i parališe u što je moguće većoj meri. Sve se više formiraju stavovi da u tim i takvim slučajevima ima mesta primeni pravila prava zaštite od nelojalne utakmice. I ne samo to, već sve nužnije biva formiranje novih pravila i dobrih poslovnih običaja za nova ponašanja kakva su "vadjenja" i kopiranje sadržaja iz baza.

Mada je primena zabrana iz prava nepoštene utakmice sve aktuelnija kad su u pitanju baze, njihovo korišćenje je još uvek nepodesno. Pre svega, pravo nelojalne utakmice, sem u pojedinim izuzecima, nije još potpuno i dovoljno razvijeno u svim zemljama, pa postojanje različitih tehnika u raznim pravnim strukturama zahteva

<sup>28</sup> Commission of the European Communities, op. cit., str. 34.

izuzetne napore u harmonizovanju. Tim više, što zaštita baza zahteva poseban režim koji će se manifestovati u prevazilaženju razlika između prava i jurespudencije. To za sada gotovo da i nije moguće.

Posebno pitanje je vezano za suštinu prava nelojalne utakmice i regulisanje ponašanja među konkurentima. Proizvodjači i korisnici baza nisu konkurentni u pravom smislu reči što zahteva određene promene na koje mnoga prava još nisu spremna. No, značaj koji mas-industrija baza ima neminovno mora dovesti do određenih prilagođavanja i inoviranja prava.

Tako će se morati regulisati i pitanje prohibicije "vadjanja" dela (podataka, materijala) iz baza koje može imati anti - konkurentske implikacije. Zato je potrebno obavezati imaoce prava da učini informacije dostupnim konkurentima u svim okolnostima, a korisnicima treba da bude omogućeno da koriste sadržaj za sopstvene privatne, neprofitne, svrhe. Međutim, nikako ne treba tolerisati kopiranje sadržaja baze u komercijalne svrhe bez dozvole. To treba, svakako, predvideti kao posebno delo nelojalne utakmice.

Čini se da će ovaj oblik zaštite baza biti veoma zastupljen u nacionalnim pravima tim više što ne isključuje primenu drugih oblika zaštite, te zato može biti njihova veoma efikasna dopuna.

### 3.2. *Baze podataka i međunarodna zaštita*

Značaj koji hiper industrija baza podataka ima u nacionalnim okvirima u kratkom vremenu ih prevazilazi i zahteva međunarodnu zaštitu. Rasprava o međunarodnoj zaštiti je započela u okviru WIPO-a i mogućnosti podvodenja pod odredbe Bernske konvencije. Formiran je poseban *Komitet eksperata* koji je na prvom sastanku razmatrao mogućnost unošenja ovog predmeta u Ženevski Protokol Bernske konvencije o zaštiti književnih i umetničkih dela iz 1991., s tim što je Međunarodnom Birou povereno da nakon rasprave pripremi odgovarajući tekst.

Druga karika u lancu međunarodne zaštite svakako je **Sporazum o trgovinskim aspektima prava intelektualne svojine**.

Nešto pre WIPO-a problem internacionalne zaštite baza podataka postavlja se u fokus Evropske zajednice u okviru koje se 1988. godine donosi **Zelenu knjigu o**

**autorskopravnoj zaštiti i izazovima tehnologije**<sup>29</sup> koju je izradila posebna *Komisija*. Ona je tada anotirala da su pokrenuta brojna pitanja oko harmonizacije mera na polju autorskog prava, a polazeći od slobodnog kretanja roba, usluga, ljudi i kapitala, kao i prepreka koje se pojavljuju u slobodnoj konkurenciji na unutrašnjem tržištu. U glavi 6 izvučena je i podvučena nužnost harmonizacije pravne zaštite baza u okviru Zajednice. Prateći podatke, analize stanja i slušajući sve kritičnija upozorenja od aprila 1990. godine Komisija je prihvatila da se za potrebe usaglašavanja zakonskih, podzakonskih i upravnih akata zemalja članica donese poseban multilateralni akt kojim bi se osigurala zaštita baza. Bila je to **Direktiva o pravnoj zaštiti baza podataka**. Kao osnova poslužili su joj članovi 57(2)<sup>30</sup>, 66 i 100a Rimskog ugovora o osnivanju Evropske zajednice<sup>31</sup>.

### 3.2.1. *Bernska konvencija za zaštitu književnih i umetničkih dela*

Znači, Komitet eksperata razmatrajući dalje mogućnost podvodjenja baza podataka pod odredbe **Bernske konvencije za zaštitu književnih i umetničkih dela** raspravlja o tekstu *Medjunarodnog biroa* prezentiranom u dokumentu BCP/CE/1/2, nazvanim Memorandum, u kome se konstatuje da: "Danas raste broj argumenata da baze podataka - bilo štampane, ili u kompjuterskoj memoriji ili u nekoj drugoj formi - zaslužuju zaštitu takve vrste koja se može podvesti pod član 2(5) (kao zbirke) Bernske konvencije. Ako one čine intelektualnu kreaciju po logici koordinirane selekcije ili uređivanja njihovog sadržaja izvestan broj nacionalnih autorskih prava garantuje im zaštitu ne samo kao zbirci sastavljenoj od dela, već i kao bilo kojoj zbirci informacija, podataka i tome slično, ukoliko je takva zbirka originalna

<sup>29</sup> Green Paper on Copyright and the Challenge of Technology, COM (88) 172.

<sup>30</sup> član 57 (2) predviđa: "U istom cilju, a pre isteka prelaznog perioda, Savet donosi uputstva za usaglašavanje zakonskih, podzakonskih, upravnih odredbi država članica u vezi sa otpočinjanjem i obavljanjem samostalnih delatnosti, Savet odlučuje jednoglasno, na predlog Komisije i nakon konsultovanja Evropskog Parlamenta, o uputstvima čije izvršenje najmanje u jednoj državi podrazumeva izmenu postojećih zakonodavnih načela o režimu zanimanja kada je reč o obrazovanju i uslovima zapošljavanja fizičkih lica. U ostalim slučajevima, Savet odlučuje u skladu sa postupkom navedenim u čl. 189B.". Ugovor o Evropskoj uniji, od Rima do Mاستrihta, Beograd, Medjunarodna politika, Pravni fakultet, Fakultet političkih nauka, Institut ekonomskih nauka, Evropski pokret u Srbiji, 1995., str.61, 64, 78, 79, 101.

<sup>31</sup> Commission of the European Communities, op. cit., str. 38 i 39.

na osnovu selekcije, koordinacije i uređenja. Svaka ekstenzivna interpretacija Bernske konvencije u pokrivanju takve zbirke izgleda opravdanom."<sup>32</sup>

Tekst Memoranduma, otuda, predviđa da se zbirka podataka ili drugih nezaštićenih materijala može smatrati literarnim ili umetničkim delom i može biti zaštićena na isti način kao i zbirka dela na koju se primenjuje član 2(5) Bernske konvencije. U daljem objašnjenju se predlaže da baze treba uvek navoditi u tekstu Protokola upravo kao ilustraciju ovog tipa zaštićenog dela. Pri tome se mora imati u vidu da zaštita zbirke podataka ili nezaštićenih materijala neće, sama po sebi, učiniti taj podatak ili nezaštićeni materijal kvalifikovanim za autorskopravnu zaštitu.

Burne debate na sastancima Komiteta eksperata u novembru 1991. godine zaokružene su predlogom **Izveštaja** u kome su se indicirali sledeći zaključci: "pitanje zaštite baza podataka će biti rešeno u kontekstu predviđenog Protokola, a ono, takodje, zasluhuje i zahteva da se u budućim radnim dokumentima nadje i studija o mogućnosti zaštite onih baza koje sadrže velike količine podataka ili informacija i koje se sreću sa kriterijumom originalnosti, kao što je to slučaj sa katalogom robe koji treba da se narudžbenicom proda."<sup>33</sup>

Iz svih ovih rasprava i zaključaka proisteklo je da se:

1. Primenjuje član 2(5) Bernske konvencije po kome su zbirke književnih ili umetničkih dela, kao što su enciklopedije i antologije, koje prema izboru i rasporedu sadržine predstavljaju intelektualne tvorevine, **zaštićene kao takve, bez štete za prava autora na svako od tih dela koja čine sastavni deo ovih zbirki**. Zaštita koja važi u korist autora i nosilaca prava uživa se u svim zemljama Bernske Unije. Zbirka koju predstavlja baza je sposobna za zaštitu zbog prikupljanja ili uređenja njenih sadržaja koji postaju utoliko raznovrsniji ukoliko raste broj multimedijalnih interaktivnih baza u kojima se zajedno mogu naći zvuk, tekst, slika, podatak ili broj zajedno.
2. Prava koja se uživaju odnose se na imovinska i moralna prava. Od moralnih je najznačajnije **pravo priznanja** da je autor tvorac baze i **pravo da se protivi svakom iskrivljavanju, skraćivanju ili drugoj izmeni baze** ili svakoj drugoj povredi koja bi bila štetna za njegovu čast i

<sup>32</sup> Commission of the European Communities, op. cit., str. 37.

<sup>33</sup> Commission of the European Communities, op. cit., str. 37.

ugled. Trajanje ovih prava je najmanje do isteka imovinskih prava i samo izuzetno i ne ostaju na snazi posle smrti autora<sup>34</sup>.

3. **Trajanje zaštite** (imovinskih prava) je **za života autora i 50 godina nakon smrti**, sem ako nije nacionalnim zakonima drugačije predviđeno, što može biti značajno prevashodno za dela koja se u bazu unose<sup>35</sup>.
4. **Rokovi zaštite** odnose se ne samo na autora nego i na **saradnike koji su zajednički delo stvarali**<sup>36</sup>.
5. Za baze podataka od posebnog značaja bi bilo i **pravo reprodukovanja**, odn. isključivo pravo autora da daje odobrenja za reprodukovanje. Ono ostaje dvostruko značajno, s jedne strane zbog dela od kojih je baza sačinjena, a s druge, zbog same baze. Pri tom svako zakonodavstvo može dopustiti reprodukovanje u određenim slučajevima ali samo ako ono ne ide na štetu redovnog korišćenja ili zakonitih interesa autora. Reprokovanje je i svako zvučno ili vizuelno snimanje, što naročito postaje značajno u uslovima razvoja multimedija. Ukoliko dodje do reprodukovanja na nedozvoljeni način može se izvršiti zaplena baze, odn. njenog sadržaja<sup>37</sup>.
6. **Primenjivaće se i odredbe vezane za citate i korišćenje baza za nastavu**, ako je to u skladu sa dobrim običajima i u meri opravdanoj ciljem koji se želi postići<sup>38</sup>.
7. **Bez dozvole autora ne smeju se vršiti adaptacije, aranžmani i druge prerade baze i dela u njoj**, što je od krucijalne važnosti, a nije ni manje značajno pravo prevodjenja koje se vrši lično od strane autora ili davanjem dozvole ako to čine druga lica<sup>39</sup>.

Dakle, primenjujući na baze odredbe Bernske konvencije o zbirkama, redje o kompilacijama, otvorila su se vrata za njihovu međunarodnu, ali i za minimum nacionalne zaštite.

---

<sup>34</sup> Član 6. bis(2) Konvencije.

<sup>35</sup> Član 7. Konvencije.

<sup>36</sup> Član 7. bis Konvencije.

<sup>37</sup> Član 9. Konvencije.

<sup>38</sup> Član 10. Konvencije.

<sup>39</sup> Član 12. Konvencije.

### 3.2.2. *Sporazum o trgovinskim aspektima prava intelektualne svojine*

Pitanje zaštite baza podataka je, takodje, postavljano u okviru Urugvajskih pregovora GATT-a vezanih za donošenje Finalnog akta čiji se poseban Sporazum odnosi na međunarodnu trgovinu prava intelektualne svojine.

Nakon diskusije koja se vodila zaključeno je da se zaštita baza može podvesti pod zaštitu kompilacija, odn. kao "kompilacije podataka ili drugih materijala, bilo u mašinski čitljivoj ili drugoj formi, za koje postoji razlog za selekciju ili uređivanje njihovog sadržaja, i da predstavljaju (konstituišu) intelektualnu tvorevinu koja će se zaštititi kao takva. Takva zaštita, koja ne postoji za sam podatak ili materijal neće prejudicirati bilo kakvu autorskopravnu zaštitu samu po sebi."<sup>40</sup>

Taj je stav unet kao posebna tačka u član 10 **Sporazuma o trgovinskim aspektima prava intelektualne svojine**. Medjutim, Sporazum je propustio da definiše posebna, specifična, prava koja autori baza treba da uživaju. Ono što je određeno je:

1. da se **baze smatraju kompilacijama podataka ili materijala**, bez obzira na formu u kojoj se nalaze (mašinski čitljiva ili neka druga);
2. da se kao intelektualna tvorevina **štiti izbor ili uređenje sadržaja**, a ne sami podaci ili materijal, koji već kao takvi uživaju autorsku ili sličnu zaštitu;
3. da su u pitanju **ostvarenja**, a ne ideje, metode ili matematički koncepti kao takvi;
4. da se **kao uslov** tretmana baze kao intelektualne tvorevine pojavljuje **originalnost**;
5. da je **trajanje zaštite onoliko koliko je predviđeno Bernskom konvencijom ili dugim međunarodnim aktom**, a ako se izračunava na drugoj osnovi, a ne po životnom veku fizičkog lica, **da to trajanje ne sme biti manje od 50 godina od kraja kalendarske godine u kojoj je bilo dozvoljeno objavljivanje**. Ukoliko takvo dozvoljeno objavljivanje ne postoji taj rok je 50 godina od nastanka baze, odn. od kraja kalendarske godine u kojoj je nastala;

---

<sup>40</sup> Član 10 Sporazuma.

6. u slučaju da dodje do **povrede prava primenjivaće se postupci i pravila koja važe i za druge vrste dela intelektualne svojine**, od građanskih, upravnih, krivičnih do carinskih postupaka i mera.

Ono što je bitno je da se ovim Sporazumom potencira eliminacija iz međunarodne trgovine svih onih robe kojom se vredjaju prava intelektualne svojine uopšte, pa s toga, i bazama. Za sprovođenje ovog cilja zemlje potpisnice međusobno saradjuju, između ostalog i ustanovljavanjem u svojim nacionalnim upravama posebnih jedinica za kontakte i razmenu informacija o trgovini sa krivotvorenim proizvodima. Pri tom, nikako ne treba zanemariti ni činjenicu da će o tim i takvim podacima i materijalima svakako biti uspostavljene i posebne baze podataka, koje takodje, treba zaštititi.

### 3.2.3. *Direktiva o pravnoj zaštiti baza podataka*

U zemljama članicama Evropske Unije postojale su sve vidljivije razlike u pravnim režimima zaštite baza čime se vršila obstrukcija slobodne razmene njihovog sadržaja. To je izazvalo ozbiljne probleme. Postojeći propisi nisu mogli na odgovarajući način da favorizuju slobodnu cirkulaciju vezanu za baze, s obzirom da su zemlje koje su imale raščišćena pitanja njihove zaštite bile kurentnije i u povoljnijem položaju nego zemlje u kojima je zaštita bila neodgovarajuća. Ovo se reflektovalo i na rast industrije baza u Uniji, kao i na razvoj unutrašnjeg tržišta. Zahtev za postojanjem harmonizovanih uslova razvoja baza, s toga, pretpostavlja poboljšanje položaja Unije na međunarodnom tržištu. No, takvih uslova do početka 90-ih nije bilo na što ukazuje Zelena knjiga i "Panorama Industrije Evropske Zajednice u 1990."

Otuda se pristupilo pripremi i donošenju **Direktive Saveta o pravnoj zaštiti baza podataka** (*Council Directive on the legal protection of databases*)<sup>41</sup> koja u svega 17 članova reguliše osnovne principe i prava zaštite baza. Donošenju Direktive predhodile su opsežne pripreme koje su kao rezultat imale više različitih verzija teksta. Poseban problem bio je ne samo u definisanju baze, već i u odredjivanju *sui generis* prava koja se na nju odnose. Prva verzija razmatrana je od Ekonomskog i socijalnog Komiteta novembra 1992., a od Evropskog Parlamenta juna 1993. godine<sup>42</sup>. Ta je verzija imala svega 14 članova i polazila je od definisanja **baze podataka kao zbirke** tako uredjenih i zapamćenih dela ili materijala kojima je moguće elektronski

<sup>41</sup> Council Directive on the legal protection of databases, Official Journal of the European Communities of 27/3/96 no L 77, str. 20.

<sup>42</sup> Commission of the European Communities, Brussels, 13. may 1992, COM (92) 24 Final - SYN 393.

pristupiti i za čiji rad su nužni elektronski materijali (kao što je njen tezaurus, indeks ili sistem za dobijanje ili prikazivanje informacije), a koji se ne koriste ni jednim kompjuterskim programom u pravljenju ili radu. Naravno da se i neelektronske baze podataka, ukoliko zadovoljavaju odgovarajuće uslove, mogu tretirati kao zbirke i zaštititi autorskim pravom. Da bi uživala autorskopravnu zaštitu baza podataka mora biti **originalna**<sup>43</sup>. U čemu se originalnost sastoji zavisi od usvojenog pravnog režima, ali je za zaštitu, u svakom slučaju, bitno da bilo koji drugi autor nije u stanju da demonstrira originalnost tog izbora<sup>44</sup>. Sledeći pojam koji je definisan je **pravo na zaštitu od nepoštenog vadjanja** (*right to prevent unfair extraction*) koje ima tvorac baze da bi bio zaštićen od aktivnosti vadjanja i preiskorišćavanja materijala iz baze za komercijalne svrhe. Pored ovih, definisani su i pojmovi **nebitnog dela**<sup>45</sup> i **nesuštinskog, nebitnog menjanja**<sup>46</sup>. Tvorcima baze mora se osigurati zaštita od neautorizovanog vadjanja ili ponovnog korišćenja za komercijalne svrhe same baze ili njenih sadržaja, u celini ili u bitnim delovima<sup>47</sup>. Autor ima, u odnosu na selekciju ili uređenje sadržaja baze i elektronskog materijala (tezaurusa, indeksa ili sistema za dobijanje ili prikazivanje informacija korišćen u kreiranju ili radu na bazi), određena isključiva prava da čini ili autorizuje. Od ovih isključivih prava u odnosu na poštovanje sadržaja baze moguća su izuzeća, ali samo u strogo predviđenim slučajevima<sup>48</sup>. Dužina trajanja autorskopravne zaštite baze je ista kao i za literarno delo. Nebitne promene u selekciji ili uređivanju sadržaja baze neće produžiti originalni period njene autorskopravne zaštite. **Pravo na zaštitu od nepoštenog vadjanja** će teći od datuma nastanka (kreiranja) baze i isteći će na kraju perioda od **10 godina** od datuma kada je baza prvi put zakonito (pravovaljano) stavljena na raspolaganje javnosti.

Druga verzija (1993. godine) je sačinjena zbog mnogobrojnih primedbi i sugestija. Po podacima iznetim u novoj **Zelenoj knjizi o autorskom i srodnim**

<sup>43</sup> Po nekim shvatanjima ni selekcija, ni uređivanje ne predstavljaju posebno značajne kriterijume po kojima se određuje autor u svom individualnom izboru. Po tom kriterijumu drugi autor ne može replicirati isti sadržaj ako bi želeo da stvori istu celinu. Međutim, po drugim shvatanjima bitno je da drugi autor ne može lako da izbegne takav kriterijum kakav je npr. alfanumerički.

<sup>44</sup> Znači, neće biti zaštite ako je zaposleni koristio dobro poznate metode kao što je listanje spiskova alfanumerički aranžiranih, jer u tom slučaju bi autorskopravna zaštita obuhvatala svakog autora i sve kompilacije dela koje su alfanumeričke ili razumljive.

<sup>45</sup> **Nebitni deo** označava delove baze čija reprodukcija, kao i kvantitativna i kvalitativna procena u odnosu na baze iz kojih su kopirane, ne šteti ekskluzivnim pravima tvorca baze da je eksploatiše.

<sup>46</sup> **Nesuštinsko, nebitno menjanje** je dodavanje, brisanje ili popravljavanje odabranih ili uređenih sadržaja baze podataka koji su nužni da bi se nastavila funkcija na način na koji ih je njihov tvorac namenio.

<sup>47</sup> **Neautorizovani postupci** predstavljaju kršenje prava u elementima skupljanja i uređivanja baza, ali ne i istovremeni prekršaj prava u njenim sadržajima, mada oni mogu biti sami za sebe predmetom prava intelektualne svojine ili sličnih prava.

<sup>48</sup> Izuzeće je npr. za aktivnosti ili dela koja se vrše i primenjuju u cilju predavanja i ukoliko je njihovo korišćenje u skladu sa praksom "poštene upotrebe".

**pravima u informacionom društvu** došlo je do određenih poteškoća, ali se nastavio intenzivan rad na harmonizaciji unutrašnjih prava zemalja članica<sup>49</sup>.

Konačna verzija koja je usvojena od Evropskog Parlamenta marta 1996. godine obuhvata 17 članova grupisanih u četiri dela: delokrug, autorsko pravo, pravo *sui generis* i zajedničke odredbe. U recitalu datom u 60 tačaka date su osnove i razlozi donošenja ove Direktive i obrazloženja prihvaćenih rešenja. Osnovno je da se žele ublažiti razlike u pravnoj zaštiti baza i osigurati da se investicije i naponi vrednuju kroz režim autorskih i *sui generis* prava. Takođe, nisu zanemarene ni specifičnosti distribucije novim tehnologijama, naročito CD i CDROM-om. Naravno, sve to u kontekstu i skladu sa odgovarajućim akatima EU ranije donetim<sup>50</sup>.

U **prvom delu** dato je određenje **baze podataka** (*database*) koja se definiše kao ***zbirka nezavisnih dela, podataka ili drugih materijala sistematski ili metodično uređenih i pojedinačno pristupačnih elektronskim putem ili na drugi način***. Pravna zaštita se odnosi na sve baze (bez obzira u kakvom su obliku). Naravno, zaštitom baze se ne obuhvata i zaštita kompjuterskog programa koji se koristi za pravljenje ili njen rad ako je baza elektronska, jer je njima pružena zaštita posebnom Direktivom.

**Drugi deo** sa četiri člana se odnosi na autorsko pravo i u njemu se određuju: predmet zaštite, autorstvo, prava i izuzeća. **Predmet zaštite** su baze koje na osnovu izbora ili uređenja njihovog sadržaja predstavljaju originalnu intelektualnu tvorevinu autora. Ovakve baze uživaju autorskopravnu zaštitu. Ova zaštita se ne odnosi na njihov sadržaj.

<sup>49</sup> I po ovoj verziji BP (Amended proposal for a Council Directive on the legal protection of databases, COM (93) 464 Final - SYN 393, Brussels, October 1993), baza se tretira kao zbirka, te se štiti autorskim pravom kao literarno ili umetničko delo. Autor baze može biti fizičko lice, grupa fizičkih lica i/ili pravno lice. Inkorporacija u BP bibliografskog materijala ili izvoda apstrakta, navoda ili zaključaka koji ne substituišu sama originalna dela, neće zahtevati autorizaciju od nosilaca prava tih dela. Autor ima, u odnosu na selekciju ili uređenje sadržaja baze i elektronskog materijala, određena isključiva prava, ali su moguća i izuzeća. Kao prava *sui generis* predviđena su: **1)** pravo na zaštitu od neautorizovanog izvlačenja delimično ili u celini materijala, podataka ili dela iz BP u komercijalne svrhe, i **2)** pravo na zaštitu od neovlašćenog rekorišćenja sadržaja BP u komercijalne svrhe. Dužina trajanja autorskopravne zaštite BP je ista kao i za literarno delo. Pravo na zaštitu od neovlašćenog vadjenja traje 15 godina i počinje od datuma kada je BP prvi put zakonito postala dostupnom javnosti i od svake suštinske promene.

<sup>50</sup> Council Directive 92/250/EEC on legal protection of computer programs; Council Directive 92/100/EEC on rental and lending right and on certain rights related to copyright in field of intellectual property; Council Directive 93/98/EEC harmonizing the term of protection of copyright and certain related rights; European Convention for the Protection of Human Rights and Fundamental Freedoms; Council Directive 95/46/EC on protection of individuals with regard to processing of personal data and the free movement of such data.

Kao **autor** može se pojaviti *jedno ili grupa fizičkih lica koja su bazu stvorila, kao i pravna lica* ukoliko su pravom države članice priznati kao nosioci prava. Ukoliko je pravom zemlje članice priznat kolektivni rad imovinska prava pripadaju osobama koje su nosioci autorskih prava. Ekskluzivna prava na bazi koja je zajednički kreirana od grupe fizičkih lica su zajednička.

Autor baze ima sledeća **ekskluzivna prava da izvrši ili autorizuje**:

- a) *povremeno ili stalno reprodukovanje* u bilo kom smislu i u bilo kojoj formi u celini ili delu;
- b) *prevodjenje, adaptaciju, uređivanje ili bilo koju drugu promenu*;
- c) *svaki oblik distribucije baze ili njenih kopija*. Prvom prodajom kopija baze od strane nosilaca prava ili sa njegovom dozvolom iscrpljuje se pravo kontrole preprodaje te kopije u Zajednici;
- d) *svaku komunikaciju, izlaganje ili izvodjenje baze u javnosti*; i
- e) *svako reprodukovanje, distribuiranje, komuniciranje, prikazivanje ili izvodjenje rezultata prevodjenja, adaptacije, uređivanja ili bilo koje druge promene*.

Kao **izuzeci** predviđeni su u sledećim slučajevima:

1. ukoliko su aktivnosti reprodukovanja, prevodjenja, adaptacije, uređivanja, promene, distribucije, komunikacije, izlaganja, izvodjenja **nužne za pristup sadržaju baze i njegovo normalno korišćenje** tada ovlašćeni korisnik baze ili njene kopije neće za to tražiti dozvolu autora, a ako je ovlašćen za korišćenje samo dela baze onda će mu biti to dozvoljeno samo za taj deo;
2. ukoliko je pravom države članice predviđeno da se bez dozvole autora može vršiti reprodukovanje, prevodjenje, adaptiranje, uređivanje, promena, distribuiranje, komuniciranje, izlaganje, izvodjenje sadržaja za:
  - ♦ *privatne svrhe kad su u pitanju neelektronske baze*;
  - ♦ *posebne nekomercijalne svrhe ilustriranja u nastavi ili naučnim istraživanjima*;
  - ♦ *javnu sigurnost, administrativne i sudske postupke*; ili
  - ♦ *druge svrhe koje su predviđene tim pravom*.

Ovi izuzeci biće dozvoljeni samo ako nisu u suprotnosti sa normalnom eksploatacijom baza i legitimnim interesima nosioca prava.

Ceo treći deo i pet članova posvećeni su *sui generis* pravu kao pravu **proizvodjača baza** (*right for the maker of database*) čije se investicije mogu kvalifikovati i/ili kvantifikovati u postizanju, verifikaciji ili prezentaciji sadržaja koji se želi **zaštititi od vadjanja i/ili ponovnog korišćenja kompletnog ili bitnog dela**. Pri tome termin “**vadjenje**” (*extracting*) znači *stalni ili privremeni transfer celog ili bitnog dela sadržaja baze na drugi medijum u bilo kom smislu i bilo kom obliku*, a “**ponovno korišćenje**” (*re-utilization*) je *bilo koji oblik činjenja dostupnim javnosti dela ili celog sadržaja baze distribuiranjem kopija, zakupom, prenosom on-line ili na drugi način*. Nije dozvoljeno ni ponovljeno i sistematsko vadjenje ili ponovno korišćenje nebitnih delova sadržaja baze ako su te radnje u suprotnosti sa normalnom eksploatacijom baze ili preterano prejudiciraju opravdane interese proizvodjača baze.

**I ovlašćeni korisnik ima određena prava i obaveze** koje moraju biti u skladu sa pravima proizvodjača baze. Tako će on moći da vadi i ponovno koristi nebitne delove baze za bilo koje svrhe ukoliko je proizvodjač bazu učinio dostupnom javnosti. Ovlašćeni korisnik koji je učinio dostupnom javnosti bazu neće smeti učiniti ni jednu radnju suprotnu njenoj normalnoj eksploataciji ili opravdanim interesima proizvodjača. Takođe, ovlašćeni korisnik koji je učinio dostupnom javnosti bazu ne sme prouzrokovati štete nosiocima autorskih ili srodnih prava u odnosu na dela ili materijale sadržane u bazi.

**Izuzeci** od ovih *sui generis* prava, koje treba da predvide države članice, odnose se na mogućnost ovlašćenog korisnika da bez autorizacije proizvodjača vadi i ponovo koristi suštinske delove baze u slučajevima:

- ♦ *kad to vrši u privatne svrhe, a u pitanju su sadržaji neelektronske baze;*
- ♦ *kad to vrši radi ilustrovanja u nastavi i naučnim istraživanjima sve dok se to radi u neprofitne svrhe; i*
- ♦ *ako je to potrebno zbog javne bezbednosti ili za sprovođenje administrativnih i sudskih postupaka.*

**Pravo na zaštitu od neovlašćenog vadjanja i ponovnog korišćenja traje 15 godina od datuma završetka izrade baze.** Ovaj period teče od prvog januara sledeće godine. U slučaju da se baza objavi pre ovog roka, period zaštite počinje od prvog januara sledeće godine od datuma kad je baza prvi put učinjena dostupnom javnosti. Svaka suštinska promena sadržaja baze, uključujući i svako suštinsko menjanje akumuliranjem sukcesivnog dodavanja, brisanja ili prepravljavanja koja su rezultat novih suštinskih investicija, produžava vreme zaštite.

Poslednji, **četvrti deo** i šest članova čine zajedničke odredbe. U njima je predviđeno pravo na pravne lekove, kao i obaveza zemalja članica da do prvog januara 1998. godine donesu zakonske, podzakonske ili administrativne odredbe nužne za usklađivanje nacionalnog prava sa Direktivom. Tri godine nakon isteka tog roka, i svake tri godine potom, Komisija će podneti izveštaj Evropskom Parlamentu i Savetu o njenoj primeni i ako bude potrebno i predloge za njenu dopunu ili izmenu. Posebno značajno je i to što izveštaj treba da obuhvati i informacije o primeni *sui generis* prava, kao i njihovom kršenju.

Donošenjem ove Direktive učinjen je značajan korak u obezbeđivanju zaštite takvog specifičnog predmeta kakve su baze podataka. Ono što je karakteristično za ovaj međunarodni akt je:

**Prvo, ovo je prvi posebni akt kojim se reguliše pravna zaštita baza podataka na celovit način.**

**Drugo, priznata je specifičnost baza kao predmeta zaštite i predviđena zaštita autora, ali i proizvođača i ovlašćenih korisnika baza.** Iako sa različitim interesima ovi subjekti čine jednu celinu tako da njihova prava i ovlašćenja nisu protivurečna i isključiva, već međusobno dopunjujuća.

**Treće, s obzirom da se radi o različitim zemljama, različitom stepenu razvoja i različitim pravnim sistemima zemalja članica, to je Direktiva ostavila mogućnost da one predvide posebnosti svojim pravima, ali u okvirima datim u njoj. To znači da sve zemlje članice, kao minimum, moraju imati predviđena prava iz Direktive.**

**Četvrto, donošenje ovog akta ima i širi značaj od teritorije Evropske Unije.** To istovremeno znači da će i zemlje poput naše, takodje, težiti da svoja nacionalna zakonodavstva usklade sa njom. Kod nas je učinjen prvi korak. Koji će sledeći biti tek treba da se vidi?

**I peto, mada su nadjena rešenja za mnoga pitanja ipak su ostale i neke nerešene dileme.** Posebno su velike dileme oko određivanja specifičnosti moralnih i imovinskih prava naročito u satelitskom i kablovskom prenosu, kao i u mrežama tipa Internet. Svakako da time spisak dilema i otvorenih pitanja nije iscrpljen. Njihovo rešavanje tek predstoji.

### 3.3. *Zaštita baze podataka po našem pravu*

Kada su 1990. godine vršene izmene i dopune Zakona o autorskom pravu zaštita baza podataka je bila ne samo preuranjena, već i bez odgovarajućeg modela i uzora pošto je i u drugim zemljama još bilo daleko od rešenja. Kako su u međuvremenu nastale promene to je postepeno počela da se kristališe nužnost ove zaštite. Početkom 1994. godine počinju pripreme za donošenje novog Zakona o autorskom i srodnim pravima, što je iskorišćeno i za ustanovljavanje novih prava kakva su prava reproduktivnih umetnika, proizvođača nosilaca zvuka, proizvođača nosilaca slike, proizvođača emisija. Kao posebna, radjaju se i prava proizvođača baza podataka. Ova se nova prava svrstavaju medju srodna, čime se Jugoslavija uvrstila u zemlje koje su regulaciju ovih prava uklopile uz autorskopravnu zaštitu ne samo zbog srodnosti i sličnosti, nego i radi celishodnosti povezivanja i međusobnog uklapanja. Naime, i pored svih teorijskih razlika koje izmedju ovih prava postoje, evidentna je pojava da se gotovo svi oblici iskorišćavanja predmeta zaštite ovih prava, istovremeno pojavljuju i u oblicima iskorišćavanja autorskih dela<sup>51</sup>.

#### 3.3.1. *Baze podataka kao objekt zaštite*

U našem pravu **baze podataka** se tretiraju kao **zbirke elektronski uredjenih i zapamćenih podataka, dela ili drugih materijala kojima se elektronski pristupa i materijala neophodnih za njeno funkcionisanje** (kao što su rečnik, indeks ili sistem za dobijanje ili prikazivanje informacija).

Pri tom, se baze podataka pojavljuju kao autorska dela jer im se priznaje svojstvo zbirke. Dakle, kao i za ostala autorska dela i za njih je nebitna njihova umetnička, naučna ili neka druga vrednost, kao ni namena, veličina, sadržina i način ispoljavanja. Nije bitna ni dopuštenost javnog saopštavanja njihove sadržine. To znači, da bi uživale zaštitu kao zbirke, odn., kao autorska dela nije važno da li se radi o velikim ili malim bazama, da li služe za opštu namenu ili neku specifičnu, da li su im sadržina podaci, dela ili drugi materijal, ili sve to zajedno, i da li ti su podaci dopušteni za javno saopštavanje (pošto nije usvojen Zakon o zaštiti podataka o ličnosti, to je moguće, na žalost, da sadrže i ove podatke).

<sup>51</sup> Marković S., Obrazloženje Nacrta Zakona o autorskom pravu i susednim pravima, Savezno ministarstvo za razvoj, nauku i životnu sredinu, septembar, 1995., str. 40.

I onda kad **nije završena i do kraja dizajnirana** baza se smatra autorskim delom.

Naravno, **naziv baze** može se zaštititi autorskim pravom ako ispunjava uslove da bude autorsko delo, čime se ne sprečava mogućnost zaštite na osnovu propisa o suzbijanju nelojalne konkurencije.

Takodje, baze se pojavljuju i kao posebna dela zaštićena srodnim pravima.

### 3.3.2. *Uslovi zaštite*

Da bi mogle da uživaju zaštitu baze podataka moraju ispunjavati određene uslove - moraju biti **originalne i izražene u određenoj formi**. Originalnost baze kao duhovne tvorevine autora odnosi se na izbor i raspored sastavnih delova (podataka, dela, materijala), a ne na njen sadržaj, jer on i sam podleže zaštiti koja ni na koji način ne sme biti ugrožena zaštitom baze (kao zbirke). Koja će to forma biti za zaštitu nije relevantno. To može biti mašinski čitljiva, ali i neka druga forma<sup>52</sup>.

Kad su u pitanju srodna prava tada je to, po pravilu, zbirka elektronski uređenih i zapamćenih sadržaja, što znači da je forma vezana za njihovo elektronsko uređivanje i pamćenje.

### 3.3.3. *Subjekti koji uživaju zaštitu*

Pošto je baza podataka autorsko delo to se kao subjekt autorskog prava može pojaviti jedno ili više fizičkih lica koja su je stvorila, i koja se smatraju izvornim nosiocem tog prava. Pored njih, zaštitu uživaju i druga lica na koja su preneti autorska prava i koja mogu biti: naslednici, lica na koja su ugovorima ili na drugi način preneti autorska prava i poslodavci ukoliko je baza nastala u radnom odnosu.

Osim njih kao subjekt se pojavljuje i **proizvodjač baze**. To **pravno ili fizičko lice**. Ako je proizvodjač pravno lice tada je potrebno da je ono bazu sačinilo u svojstvu privrednog subjekta. Iz takvog određenja sledi da je nastanak baze vezan, mahom, za pravna lica i to kao privrednih subjekata.

---

<sup>52</sup> Predlog zakona, čl. 6., tč. 3.

### 3.3.4. *Sadržina autorskih prava*

Ukoliko baza podataka ispuni uslov da kao zbirka predstavlja autorsko delo tada njen tvorac ili tvoreci uživaju ista prava kao i autori bilo kog drugog autorskog dela. To su, prevashodno, sva **moralna prava** od prava paterniteta, prava naznačenja imena, prava objavljivanja, prava na zaštitu integriteta baze, pa do suprotstavljanja njenom nedostojnom iskorišćavanju.

Naravno, to su i **imovinska prava**, i to pet osnovnih prava vezanih za **pravo iskorišćavanja** (u telesnoj formi) baze ili njene prerade:

- a) *pravo reprodukovanja* (pravo snimanja i umožavanja);
- b) *pravo na preradu*;
- c) *pravo na prevod*;
- d) *pravo stavljanja baze u promet*; i
- e) *pravo davanja u zakup*.

Ovim pravima trebalo bi dodati i jedno novo - *pravo javnog saopštavanja sa nosača zvuka ili slike*. Ovo pravo postaje posebno aktuelno kod mulimedijalnih baza za koje bi autor trebalo da ima isključivo pravo da ih saopštava uz pomoć tehničkih uređaja za reprodukovanje zvuka i/ili slike<sup>53</sup>.

Ništa manje značajno nije ni *pravo pristupa primerku baze* koje autor može koristiti u slučaju da želi da umnoži bazu. Ovo pravo se odnosi na vlasnike primeraka baze i biće realizovano samo ukoliko se time bitno ne ugrožavaju njihovi opravdani interesi, odnosno lica koje drži primerak baze<sup>54</sup>.

### 3.3.5. *Sadržina srodnih prava*

Kao što autor baze podataka ima određena prava vezana za bazu kao autorsko delo, tako i proizvođač baze ima određena prava. Ta prava proizvođača su isključivo imovinska. To su ekskluzivna prava na<sup>55</sup>:

---

<sup>53</sup> Predlog zakona, čl. 29.

<sup>54</sup> Predlog zakona, čl. 30.

<sup>55</sup> Predlog zakona, čl. 134.

- a) **umnožavanje** (povremeno ili stalno) *baze u celini ili delovima* (bez obzira na namenu ili formu)
- b) **promenu** baze, odn. prevodjenje, adaptiranje, uređivanje ili neku drugu promenu;
- c) **umnožavanje rezultata promena** baze;
- d) **distribuiranje u javnost** same baze ili njene kopije, *kao i davanje u zakup*; i
- e) svako **povezivanje, komuniciranje, prikazivanje ili javno izlaganje** baze.

Proizvodjač baze podataka ima i **pravo suprotstavljanja**:

- ♦ *neovlašćenom izdvajanju celine ili dela osnovnog sadržaja baze*; i
- ♦ *neovlašćenom korišćenju izdvojene celine ili dela sadržaja baze*<sup>56</sup>.

### 3.3.6. Ograničenja prava

Izuzeci od isključivih prava autora i proizvodjača baza su upravo ona ograničenja koja se primenjuju na autorska prava. Pri tome bez dozvole i bez plaćanja proizvodjaču će se tolerisati:

1. *umnožavanje i stavljanje u promet* primeraka objavljene baze kao i bilo kog oblika javnog saopštavanja ako je to nužno zbog sprovođenja službenog postupka pred sudskim ili drugim državnim organima;
2. *umnožavanje ili stavljanje u promet* primeraka baze ako je ona već objavljena, ako se pojavila kao sastavni deo tekućeg događaja o kome se javnost obaveštava, i ako se to vrši u onom obimu koji odgovara svrsi i načinu izveštavanja o tekućem događaju;
3. *izvodjenje, predstavljanje, prenošenje izvodjenja ili predstavljanja, kao i javno saopštavanje* baze sa nosioca zvuka i slike, za potrebe nastave, ako je već objavljena, ako iskorišćavanje nema profitni karakter;
4. *umnožavanje i stavljanje u promet* primeraka *manjih delova* objavljenih dela za svrhe nastave ili ispita, i to samo u obimu u kojem je to dovoljno za jedan razred ili grupu učenika, studenata ili ispitanika;
5. *umnožavanje primeraka* objavljene baze za privatne svrhe, odn. lično obrazovanje ili uživanje. Ovi se primerci ne smeju stavljati u promet;
6. *smeštanje u memoriju računara* i puštanje u rad, otklanjanje grešaka, pravljenja rezervnih primeraka, dekompiliranje radi pribavljanja

<sup>56</sup> Predlog zakona, čl. 134.

neophodnih podataka, a sve to u cilju sopstvenog, uobičajenog i namenskog korišćenja baze (odn. računarskog programa);

7. *stavljanje u promet i umnožavanje primeraka manjih delova* baze ako je ona već objavljena, ako su ti delovi potrebni radi ilustracije, potvrde ili reference, ako se navede autor citiranog dela baze;
8. *umnožavanje izloženih baza* za potrebe izrade kataloga;
9. *umnožavanje baze* na telesnom nosiocu, javno saopštavanje za demonstriranje rada uređaja za snimanje, reprodukovanje i prenos zvuka i slike.

Osim ovih ograničenja primeniće se i **zakonske licence** za potrebe nastave, žičanog reemitovanja, i drugih, zakonom predviđenih, slučajeva.

### 3.3.7. Trajanje prava

Moralna prava autora baze i po prestanku imovinskih prava. **Imovinska prava traju za života autora i 50 godina nakon njegove smrti.** Rok počinje teći od prvog januara godine koja neposredno sledi za godinom smrti autora, odnosno poslednjeg autora ukoliko je u pitanju koautorsko delo.

**Trajanje imovinskih prava proizvođača baza je 15 godina od nastanka baze,** a računa se od 1. januara one godine koja neposredno sledi za godinom u kojoj je baza nastala. Ovim rokom priznate su specifičnosti baza. Ako su u pitanju bitne promene u selekciji i uređivanju baze rok se produžava još 15 godina. Pod **bitnim promenama** u selekciji ili uređenju *baze podrazumevaju se dodavanja, brisanja ili popravljavanja cele ili dela sadržine baze koji za rezultat imaju novu verziju baze podataka*<sup>57</sup>.

### 3.3.8. Zaštita prava

Zaštita autorskih i srodnih prava autora i proizvođača baza podataka može biti sudska i arbitražna. Sudska zaštita obuhvata građanskopravnu, krivičnopravnu i upravnu zaštitu, dok se arbitražna zaštita realizuje pred stalnim izabranim sudom za intelektualnu svojinu. Bilo koji od oblika sudske ili arbitražne zaštite pokrenuće se u slučajevima kada su prava povredjena ili ugrožena.

---

<sup>57</sup> Predlog zakona, čl. 139.

**Tužbom** se zahteva<sup>58</sup>: utvrđivanje povrede prava, njen prestanak, uništenje ili preinačenje predmeta kojima je izvršena povreda, uništenje ili preinačenje alata i opreme kojima su izvršene povrede, naknada štete, objavljivanje presude. Ukoliko utvrdi povredu ili mogućnost povrede, na zahtev nosioca prava ili po službenoj dužnosti, sud može izreći *privremenu meru oduzimanja ili isključenja iz prometa predmeta kojima se vrše povrede ili zabraniti nastavljanje započetih radnji*. Sud može i narediti, radi obezbeđenja dokaza, a bez predhodnog obaveštavanja, pregled baze i zaplenu dokumenata.

Sud može izreći i *kazne zatvora* (od 6 meseci do tri godine zavisno od dela) *ili novčane kazne* u slučajevima kad su povrede prava takve prirode da predstavljaju *krivična dela*<sup>59</sup>. To će se desiti u slučajevima:

1. *kad neko lice pod svojim imenom ili imenom drugoga objavi, izvede, predstavi, prenese, ili iskoristi tuđu bazu* (snimi, umnoži, prenese ili emituje);
2. *kad na nedozvoljen način unese delove tuđeg autorskog dela u svoju bazu*;
3. *kad bez dozvole izmeni ili preradi tuđu bazu*;
4. *kad bez dozvole objavi, izvede, predstavi, snimi, umnoži, stavi u promet, emituje, da u zakup bazu ili je na drugi način iskoristi*;
5. *kad radi pribavljanja materijalne koristi stavi u promet bazu za koju zna da je neovlašćeno umožena*; i
6. *kad prilikom registrovanja i deponovanja u javni registar saveznog organa da neistiniti ili prikrije pravi podatak o svojoj bazi*.

Ovim odredbama nužno se moraju dodati i odredbe iz krivičnih zakona (saveznog i republičkih).

Osim za krivično delo moguće je kazniti pravno lice za **privredni prestup**<sup>60</sup> ukoliko:

1. *bez dozvole titulara srodnog prava objavi, izvede, predstavi, snimi, umnoži, stavi u promet, emituje, da u zakup ili na drugi način iskoristi bazu*;
2. *u nameri pribavljanja materijalne koristi stavi u promet primerke tuđe baze za koju zna da je neovlašćeno snimljena ili umnožena*; i

<sup>58</sup> Predlog zakona, čl. 173.

<sup>59</sup> Predlog zakona, čl. 183 - 186.

<sup>60</sup> Predlog zakona, čl. 186.

3. *u roku od 15 dana od početka korišćenja baze, odn. 30 dana od dana početka korišćenja, a u pitanju je korišćenje bez dozvole, ne obavesti organizaciju o nazivu baze i obimu iskorišćavanja.*

U određenim slučajevima pravno i odgovorno fizičko lice mogu biti kažnjeni i za **prekršaj**<sup>61</sup>.

Dakle, za očekivati je da predviđanjem i preduzimanjem odgovarajućih pravnih mera zaštite baza podataka počinje novo razdoblje zaštite u informacionom društvu<sup>62</sup>.

---

<sup>61</sup> Predlog zakona, čl. 187.

<sup>62</sup> Drakulić M., Pravna zaštita baza podataka, Zbornik radova: XI naučno-stručni skup Info-Teh '96., Donji Milanovac, 1996., str.311 - 317.

# GLAVA 5

## ZAŠTITA TOPOGRAFIJE INTEGRISANIH KOLA

|           |   |            |
|-----------|---|------------|
| <b>1.</b> | <b>Uvodne napomene</b>  | <b>362</b> |
| <b>2.</b> | <b>Objekt zaštite</b>   | <b>362</b> |
| <b>3.</b> | <b>Oblici zaštite</b>   | <b>364</b> |
| 3.1.      | <i>Topografija integrisanih kola i nacionalni propisi</i>                     | 364        |
| 3.2.      | <i>Topografija integrisanih kola i međunarodna zaštita</i>                    | 367        |
| 3.2.1.    | <i>Direktiva o pravnoj zaštiti topografije poluprovodničkih proizvoda</i>     | 367        |
| 3.2.2.    | <i>Sporazum o zaštiti intelektualne svojine u vezi sa integrisanim kolima</i> | 368        |
| 3.2.3.    | <i>Sporazum o trgovinskim aspektima prava intelektualne svojine</i>           | 373        |
| 3.3.      | <i>Zaštita topografije integrisanih kola po našem pravu</i>                   | 378        |

## 1. Uvodne napomene

Razvoj hardvera ne može se zamisliti bez “silikonskog čipa”, ili jednostavno čipa. Ovaj minijaturni deo kompjutera postao je jedna od ključnih tačaka kompjuterske industrije i determinanta pozicije jedne zemlje u informacionom razvoju. Što je njihov značaj bio veći to je i zainteresovanost pojedinaca, organizacija i država rasla, naročito onih koje ih nisu bile u stanju proizvoditi. Počinje sve češće krivotvorenje, profesionalno organizovano piratstvo i pojavljivanje na svetskom tržištu čipova poznatog, ali ne originalnog porekla. Gubici, s jedne strane, postaju sve veći, kao i ulaganja u njihov razvoj, s druge. To svakako izaziva burne reakcije onih koji usled nelegalne i nepošteno proizvodnje integrisanih kola bivaju ugroženi. Sve je jači zahtev za njihovom zaštitom, a sve češće i ubrzanije aktivnosti u pronalaženju odgovarajućih rešenja. Naravno, jedno od najefikasnijih je i zaštita Pravom intelektualne svojine. U početku se intenzivno razmišljalo o patentnopravnoj zaštiti, no, ubrzo, sama priroda objekta zaštite isključuje ovaj i daje prioritet drugim oblicima.

I dok su teorijske rasprave uzimale sve više maha dotle je najzainteresovanija zemlja - SAD, donela, nakon višegodišnjih priprema, prvi pravni akt kojim se propisuje zaštita. Ubrzo slede Japan i Švedska, da bi potom i međunarodna pravna scena postala sve češće polje sukoba različitih interesa, ali i težnji za harmonizacijom međusobnih odnosa.

Za svega desetak godina, koliko je prošlo od prvih zakonskih odredbi, do danas, učinjeni su značajni koraci u rešavanju problema vezanih za osiguranje i odgovarajući pravni tretman integrisanih kola.

## 2. Objekt zaštite

U literaturi i pravnim aktima pojavljuju se termini: čip, poluprovodnik, integrisano kolo. Neki od njih se koriste kao sinonimi, a neki i u pogrešnom kontekstu. Otuda je izuzetno važno definisati objekt zaštite određujući upravo ove pojmove. Pri tom treba praviti razliku između onog što je objekt zaštite i onog čemu ili kome taj objekt pripada. Naime, određeni objekti zaštite pripadaju poluprovodničkim proizvodima ili čipovima, te je nužno definisati njih, da bi se zatim moglo odrediti šta se u vezi njih štiti.

Tako bi se pod **poluprovodničkim proizvodima** (*semiconductor product*) ili **integriranim kolima** (*integrated circuit*) mogli definisati<sup>1</sup> *svi proizvodi* (finalnog ili intermedijalnog oblika) *sastavljeni od dva ili više elementa* (obično tri) *od poluprovodničkih materijala tako raspoređenih da čine trodimenzionalni model koji obavlja, ponaosob ili zajedno sa drugim funkcijama, funkciju elektronike*<sup>2</sup>. Vrlo slično se definiše i **poluprovodnički čip** (*semiconductor chip*)<sup>3</sup> *pod kojim se smatra čip*<sup>4</sup> *sačinjen od elemenata napravljenih od poluprovodničkog materijala kao što je silikon, germanijum, galijum, sa izolatorima koji su različito kombinovani kako bi činili komponente elektronskog kola*. Naravno, nužno je istaći da noviji nacionalni zakoni izbegavaju određivanje vrste materijala, između ostalog, i zbog njihove stalne promenljivosti i razvoja.

Dakle, **poluprovodnički proizvod** (integrirano kolo) je obično sačinjen od:

1. *aktivnih elemenata* (npr. tranzistora);
2. *pasivnih elemenata* (npr. kondenzatora); i
3. *veza između njih u elektronskom kolu*.

Objekt zaštite nije samo poluprovodnički proizvod kao takav već neki od njegovih elemenata, odnosno neki od njegovih oblika: grafička shema integriranog kola ili njegovog dela; računarski zapis topografije; maske i sam čip<sup>5</sup>. Pri tom zavisno od toga gde se pojavljuje koristi se ili termin **raspored kola** (*circuit design* - Japan)<sup>6</sup>, **raspored slojeva** (*layout design* - Švedska)<sup>7</sup>, **maska** (*mask work* - SAD)<sup>8</sup> ili **topografija** (*topography* - EZ, WIPO, SR Jugoslavija)<sup>9</sup>.

<sup>1</sup> Bainbridge D., *Computers and the Law*, London, Pitman Publishing, 1990., str. 66.

<sup>2</sup> Dreier T., *Development of the Protection of Semiconductor Integrated Circuits*, IIC, Vol. 19., no. 4/88, str. 455.

<sup>3</sup> Reed C., *Computer Law*, London, Bleckstone Press Limited, 1993, str. 130.

<sup>4</sup> Sam termin **čip** (reč *chip* - en. - parče, deo, odlomak) označava uređaj napravljen prevashodno od silikona, koji se koristi za čuvanje, izvršenje ili rad memorije kompjutera ili kompjuterskog programa. To je, u stvari, mali deo od poluprovodničkog materijala, najčešće silikona, koji, sa slojevima sačinjenim od propusnih i izolacionih materijala čine mikro-elektronsko kolo uključujući brojne poluprovodničke delove (tranzistore, diode i sl.).

<sup>5</sup> Reed C., op. cit., str. 129 - 135.

<sup>6</sup> Act Concerning the Circuit Layout of a Semiconductor Integrated Circuit.

<sup>7</sup> Act for the Protection of the Layout Design of the Circuitry in Semiconductor Products.

<sup>8</sup> Semiconductor Chip Protection Act.

<sup>9</sup> Council Directive on the Legal Protection of Topographies of Semiconductor Products, WIPO, Treaty on the Protection of Intellectual Property in Respect of Integrated Circuits; Prednacrt zakona o pravnoj

Pri tom, **raspored slojeva** znači shemu štampanih veza poluprovodničkih integrisanih kola, dok **topografija** je, u suštini, trodimenzionalni raspored slojeva. Drugim rečima radi se o sinonimima.

### 3. Oblici zaštite

#### 3.1. Topografija integrisanih kola i nacionalni propisi

Nacionalna zakonodavstva su se pre desetak godina srela sa problemom zaštite topografije. Međutim, prvi oblici zaštite<sup>10</sup> vezuju se za kasne 50-te i zaštitu patentom (npr. u V. Britaniji Noyce of the *Fairchild Semiconductor Corporation* je prvi registrovao patent svog integrisanog kola 1959., da bi ga u komercijalnu upotrebu pustio dve godine kasnije<sup>11</sup>). Ipak, prvi pravni akt donet je u SAD-u 1984. godine pod nazivom **Zakon o zaštiti poluprovodničkog čipa** (*Semiconductor Chip Protection Act* - ili kratko nazvan - *Chip Act*)<sup>12</sup>. Ovaj je akt potpisao Predsednik Regan, a donet je nakon šestogodišnje pravničke rasprave u koju su veoma intenzivno bili uključeni i zainteresovani proizvođači<sup>13</sup>. Naročito je burno tekla rasprava oko dozvoljenosti reverzibilnog inženjeringa, kao i drugih svrha koje je trebalo zaštitom postići. Iako je pristup bio baziran na *sui generis* pravu mnoga usvojena rešenja potekla su iz principa autorskopravne zaštite, čemu se pribegavalo zbog straha američkih proizvođača od pojave stranih čipova i pokušaja njihove zaštite. Taj strah je doveo do usvajanja **principa reciprociteta** (druge zemlje takve akte nisu imale, a ni prava). Usvojen je još jedan princip koji baš i nije uobičajen za zaštitu Pravom intelektualne svojine, **princip retroaktivnosti**, koji se odnosio na obuhvat maski integrisanih kola koje su se u prvoj komercijalnoj eksploataciji našle od 1. jula 1983. godine. Koliko je to bilo značajno i jedva dočekano rešenje vidi se i iz podatka da je u 1985. godini ukupan broj maski za koje je zatražena zaštita po *SCPA* bio 1.880, a registrovano je 1.263. Zaštita se sastoji u sledećem<sup>14</sup>:

---

zaštiti topografija integrisanih kola, Savezno ministarstvo za razvoj, nauku i životnu sredinu, Savezni zavod za intelektualnu svojinu, avgusta 1996., čl. 2.

<sup>10</sup> Bainbridge D., op. cit., str. 65 - 69.

<sup>11</sup> Edwards C., Savage N., *Information Technology & The Law*, London, MacMillan Publishing, 1990., str. 70.

<sup>12</sup> Ovaj "Zakon", u suštini, predstavlja poseban deo američkog Copyright Act.

<sup>13</sup> Bernachi R., Frank P., Statland N., Bernacchi On Computer Law, A Guide to the Legal and Management Aspects of Computer Technology, Boston, Little, Brown & Company, 1986., str. 3 - 73.

<sup>14</sup> US Copyright Act, As Amended, Chapter 9. Protection of semiconductor chip products, &sect: 901 - 914. Dokument preuzet sa Interneta.

- ♦ odnosi se na *trodimenzionalni prikaz ili oblik* smešten na ili ugradjen u poluprovodnički proizvod<sup>15</sup>;
- ♦ *maska koja se štiti je ugradjena u proizvod poluprovodničkog čipa koji predstavlja krajnji proizvod ili je medjuoblik proizvoda*;
- ♦ *ne odnosi se na ideju, postupak, proces, sistem, metod, operaciju, princip, otkriće ili koncepciju*;
- ♦ maska mora biti *originalna* i *ne sme se sastojati od dizajna koji je već u prodaji, opštepoznat ili poznat industriji poluprovodnika* ili da nije u pitanju varijanta tog dizajna kombinovana na originalan način;
- ♦ registracija se može izvršiti u roku od 2 godine nakon datuma kad se maska prvi put ekonomski počela koristiti (*primena doktrine prve upotrebe*);
- ♦ *traje 10 godina* od dana registracije kod Biroa za autorska prava ili prve upotrebe, zavisno od toga šta je bilo prvo;
- ♦ *ekskluzivna prava* se odnose na: *reprodukovanje maske* (u optičkom, elektronskom ili drugom obliku) i *uvoz ili distribuciju čipa* u koji je ugradjena maska;
- ♦ *maska se mora označiti* rečima "mask force" ili samo "mask", odn. simbolom \*M\* ili M u krugu i imenom vlasnika ili skraćenicom po kojoj je poznat<sup>16</sup>;
- ♦ *reverzibilno inženjerstvo je dozvoljeno* ali u nastavne svrhe, za analizu ili razvoj koncepta, odn. za "**kreativno kopiranje**"<sup>17</sup>. To znači da ako se na osnovu testa o različitosti utvrdi "**suštinska identičnost**" između čipa koji je dobijen reverzibilnim inženjerstvom i osnovnog čipa u pitanju je povreda prava, a ako je u pitanju samo "*suštinska sličnost*" nema povrede.

Vlasnik je lice koje je kreiralo masku ili na koga su legalno preneti prava, a ukoliko je maska nastala u toku rada, vlasnik je poslodavac<sup>18</sup>.

<sup>15</sup> Po &sect; 901:US Copyright Act.

<sup>16</sup> Kako će se obeležavanje sprovesti zavisi od Uputstva koje je pripremio Biro za autorska prava.

<sup>17</sup> Simons J. F., Semiconductor Chip Protection and Sui Generis Legislation, edicija: Essays on Computer Law, Melbourne, Longman Chechire Pty Limited, 1990., str. 61.

<sup>18</sup> Poznat je slučaj *Brooktree v. Advanced Micro Devices (AMD)* iz 1988. godine u kome je tužena AMD, između ostalog, reverzibilnim inženjeringom, a na osnovu kopije tužiteljevog desetotranzistorskog statičkog RAM-a, dostavljenog od jednog zaposlenog u firmi koja je konkurent Brooktree-u i za koju se sumnjalo da je kopirala čip Bt451, proizvela dve identične maske čija prodaja je prouzrokovala velike štete tužitelju. Sud je pozivajući se na *Chip Act* odbio zahtev sa obrazloženjem da je reverzibilno inženjerstvo u određenim slučajevima dozvoljeno, a i da su ulaganja obe firme gotovo ekvivalentna. Više o ovom slučaju u Computer Industry Litigation Reporter, 1988.

Ubrzo nakon SAD-a, tačnije 31. maja 1985. godine Japan donosi svoj **Zakon koji se odnosi na shemu veza poluprovodničkog integrisanog kola** (*Act Concerning the Circuit Layout of a Semiconductor Integrated Circuit*). Za razliku od američkog Zakona japanski Zakon je predvideo da zaštita teče i zavisi samo od registracije (bila je moguća od 1. 1. 1986.), a i da nije vezana za reciprocitet, jer se isto garantuje i domaćim i stranim licima. Reverzibilno inženjerstvo je zabranjeno.

Nakon Japana i mnoge druge zemlje počinju ubrzano da donose odgovarajuće akte vezane za zaštitu topografije.

Većina zemalja koja se odlučila na regulisanje zaštite topografije predvidela je ovu zaštitu:

1. u okviru zaštite modela i uzoraka;
2. kao *sui generis* zaštitu; i/ili
3. kao suzbijanje nelojalne konkurencije.

Hronološki pregled nacionalnog regulisanja zaštite topografije:

| Godina         | Država           | Naziv   |
|----------------|------------------|---|
| 1984.          | SAD              | Zakon o zaštiti poluprovodničkih čipova   |
| 1985.          | Japan            | Zakon koji se odnosi na shemu veza poluprovodničkog integrisanog kola   |
| 1986.          | Švedska          | Zakon o zaštiti rasporeda slojeva u električnom kolu poluprovodničkih proizvoda   |
| 1987.          | V. Britanija     | Pravilnik o zaštiti topografije poluprovodničkih proizvoda  |
| 1987.          | SR Nemačka       | Zakon o zaštiti topografije mikroelektronskih poluprovodničkih proizvoda  |
| 1987.          | Francuska        | Zakon o zaštiti topografije poluprovodničkih proizvoda  |
| 1987.          | Holandija        | Zakon o zaštiti originalnih topografija poluprovodničkih proizvoda  |
| 1988.          | Španija          | Zakon o pravnoj zaštiti topografije poluprovodničkih proizvoda  |
| 1989.          | Portugalija      | Zakon o pravnoj zaštiti topografije poluprovodničkih proizvoda  |
| 1991.          | Finska           | Zakon o ekskluzivnom pravu na shemu veza integrisanog kola  |
| 1991.<br>1992. | Češkoslovačka    | Zakon o zaštiti topografije pluprovodnika stupa na snagu  |
| 1991.          | Madjarska        | Zakon o zaštiti topografije poluprovodnika  |
| 1992.<br>1993. | Poljska          | Zakon o topografiji poluprovodnika stupa na snagu   |
| 1993.          | Južna Koreja     | Zakon o zaštiti topografije poluprovodnika  |
| 1993.          | Švajcarska       | Zakon o topografiji   |
| 1992.          | Ruska federacija | Paket propisa za ustanovljavanje prava, podnošenje prijava i ispitivanje prijava za registrovanje računarskih programa i topografije poluprovodnika |
| 1993.          | Švajcarska       | Zakon o topografiji   |
| 1993.          | Južna Koreja     | Zakon o zaštiti topografije poluprovodnika  |

|       |                |  |
|-------|----------------|--|
| 1993. | Kanada         | Zakon o topografiji integrisanih kola                            |
| 1993. | Južna Afrika   | Zakon o industrijskim uzorcima i modelima                        |
| 1996. | SR Jugoslavija | Prednacrt zakona o pravnoj zaštiti topografije integrisanih kola |

Evidentno je da je najveći broj zemalja ipak prihvatio činjenicu da je topografija nešto specifično i da se njena posebnost ne može podvesti pod već poznate institute Prava intelektualne svojine<sup>19</sup>, mada su osim ovog oblika prihvaćeni i drugi modaliteti<sup>20</sup>. Jasno je da je ovakvo rešenje i bilo za očekivanje ne samo radi specifikuma koju ova tvorevina nosi, već i za dalji razvoj pojedinih instituta Kompjuterskog prava.

### 3.2. Topografija integrisanih kola i međunarodna zaštita

#### 3.2.1. Direktiva o pravnoj zaštiti topografije poluprovodničkih proizvoda

Sredinom 80-ih na međunarodnom planu počinju značajne akcije u nalaženju rešenja za međunarodnu zaštitu topografije, kao i usaglašavanje nacionalnih zakonodavstava ne bi li se ona harmonizovala. Jedna od najatraktivnijih međunarodnih scena pregovaranja i dogovaranja je Evropska zajednica. Težnja je bila da se pokušaju ponuditi odgovarajuća rešenja zemljama članicama koje nisu zaštitu zakonodavno regulisale. Donošenju Direktive prethodile su opsežne analize i studije *Komiteta eksperata*. Tekst je 16 decembra 1986. godine predložen Savetu EZ-a<sup>21</sup>. U **Direktivu o pravnoj zaštiti topografije poluprovodničkih proizvoda** (*Council Directive on the legal protection of topographies of semiconductor products*)<sup>22</sup> su uneta mnoga rešenja koja su se već nalazila u Zakonu SAD-a, mada su postojale i određene razlike. Tako, umesto maske, Direktiva (čl. 1.) određuju da je objekt zaštite **topografija**, podrazumevajući pod njom *trodimenzionalni oblik slojeva od kojih je*

<sup>19</sup> Razliku između poluprovodničkog čipa i standardnih autorskih dela većina autora vidi u činjenici: **a)** da je čip nevidljiv golim okom; **b)** čak i onda kad je vidljiv, čip nije dizajniran da zadovolji poglede, kao što je to slučaj sa rasporedom slojeva - shemom veza - jer je diktiran funkcijom, a ne formom; **c)** industrijska praksa vezana za dizajn novog čipa bazirana je na dizajnu već postojećeg; **d)** dužina trajanja zaštite ne treba da bude za "života autora i 50 godina nakon smrti", jer je to necelishodno; i **e)** da za razliku od drugih standardnih autorskih dela, čipove retko proizvodi autor pojedinac. Simsos J. F., op. cit., str. 51.

<sup>20</sup> Dreier T., Development of the Protection of Semiconductor Integrated Circuits, IIC, vol. 19., no. 4/88., str. 5.

<sup>21</sup> Reed C., op. cit., str. 245.

<sup>22</sup> Council Directive on the Legal Protection of Topographies of Semiconductor Products (87/54/EEC).

*poluprovodnički proizvod načinjen*. Topografija će moći uživati zaštitu **ako je originalna**, odn. ako je rezultat autorovih intelektualnih napora **i ako nije opštepoznata** (*commonplace*) u kompjuterskoj industriji.

**Ekskluzivna prava** koja se Direktivom garantuju su:

- a) *pravo na reprodukciju*;
- b) *pravo na komercijalnu eksploataciju*; i
- c) *pravo na određenu svrhu korišćenja*.

Ova prava naročito bivaju značajna za **reverzibilni inženjering** za koga se predviđa dozvoljenost samo u određenim slučajevima nekomercijalne upotrebe i zahteva *bona fide* kupaca.

Sama **zaštita traje 10 godina**, a rok teče od dana pokretanja zaštite. Ukoliko komercijalna upotreba nije realizovana, mada je topografija registrovana, istek roka je 15 godina od prve fiksacije ili kodovanja na poluprovodnički proizvod. Tada prestaju sva ekskluzivna prava. Znači, zaštita topografije teorijski može trajati najviše 25 godina nakon prve fiksacije ili kodovanja.

Naravno, sva prava pripadaju tvorcu, s tim što je zemljama članicama ostavljeno da odrede vlasništvo poslodavca ako je topografija nastala na poslu, sem ukoliko ugovorom o radu nije drugačije određeno.

Nosilac ovih ekskluzivnih prava može biti lice nacionalnosti koje bilo zemlje članice ili ono lice koje ima prebivalište na teritoriji neke od njih, a ako je u pitanju pravno lice ukoliko ima sedište u nekoj od zemalja članica.

### 3.2.2. *Sporazum o zaštiti intelektualne svojine u vezi sa integrisanim kolima*

Svetska organizacija za zaštitu intelektualne svojine donela je 1989. godine **Sporazum o zaštiti intelektualne svojine u vezi sa integrisanim kolima** (*Treaty on the Protection of Intellectual Property in Respect of Integrated Circuits*)<sup>23</sup>, tzv. **Vašingtonski Sporazum**, sa ciljem uspostavljanja i harmonizacije

<sup>23</sup> Treaty on the Protection of Intellectual Property in Respect of Integrated Circuits, WIPO/IPIC/DC/3.

medjunarodnog sistema pravne zaštite intelektualne svojine njihove topografije. Sporazumu je prethodila **Rezolucija o zaštiti kompjuterskih programa i topografije** iz 1986. godine, opširna trogodišnja priprema *Komiteta eksperata*, Direktiva Saveta EZ-a, ali i pravni akti 7 zemalja kojima se, od sredine 80-ih, regulisala ova problematika<sup>24</sup>. Ovim Sporazumom stvorena je Unija zemalja koje priznaju specifičnu, *sui generis* zaštitu na principu nacionalnog tretmana pripadnicima zemalja potpisnica, kao i asimilovanim licima svih drugih zemlja. Na Diplomatskoj konferenciji održanoj u Ženevi zakazana je nova konferencija u Vašingtonu na kojoj je zaključen Vašingtonski Sporazum. Jugoslavija je prisustvovala obema konferencijama i potpisala Sporazum<sup>25</sup>. Usvojeni Vašingtonski Sporazum u 36 članova rešio je nekoliko ključnih pitanja pravne zaštite topografije integrisanih kola, kao što su: predmet i uslovi; pravni oblik, sadržaj i obim zaštite; načela; ograničenja prava uopšte i u interesu međunarodnog saobraćaja; početak zaštite, iscrpljivanje prava i njegovo trajanje; ali i pitanja prinudne licence, savesnog pribavljanja mikročipova i institucionalna, odn. organizaciona i procesna rešenja.

**Predmet zaštite je trodimenzionalni raspored aktivnih i pasivnih elemenata, kao i njihovih međusobnih veza u elektronskom kolu.** No, svakako predmet zaštite nije bilo kakav raspored, već integrisan u jednom komadu. Drugim rečima, to je trodimenzionalni raspored elemenata u mikročipu. Pri tom zaštita obuhvata bilo koji oblik konkretizacije topografije, bez obzira da li se radi o grafičkoj shemi integrisanog kola ili njegovog dela; računarskom zapisu topografije; maski i/ili samom čipu<sup>26</sup>.

Da bi neki trodimenzionalni raspored elemenata i veza integrisanog kola mogao da uživa pravnu zaštitu nužno je da se ispune određeni **uslovi**. Osnovni uslov je **originalnost topografije**. Iako se originalnost veoma slobodno interpretira, pod njom se podrazumeva: **da je topografija rezultat stvaralačkog napora tvorca i da nije već opštepoznata** (*commonplace*). Inače, sama originalnost je uslov svojstven autorskom pravu i podrazumeva subjektivni osećaj stvaraoca, a to se kod topografije modifikuje u formulaciji "da nije opštepoznata", uobičajena. Opštepoznatost ne znači da su u pitanju svi ili prosečni potrošači (što se pojavljuje kod drugih dela), već se pod tim terminom podrazumevaju stručnjaci. Pod stručnjacima se, pak, podrazumevaju drugi autori (tvorci) i proizvođači topografija ili mikročipova. Ukoliko jeste poznata tada nema originalnosti, niti zaštite. To će se odnositi i na topografiju koja je kombinacija

<sup>24</sup> SAD, Japan, Švedska, V. Britanija, SR Nemačka, Francuska, Holandija.

<sup>25</sup> Savezni Sekretarijat za razvoj, Savezni zavod za patente, Platforma za učešće jugoslovenske delegacije na Diplomatskoj konferenciji radi zaključivanja Konvencije o zaštiti intelektualne svojine u vezi sa integrisanim kolima, Beograd, 1989.

<sup>26</sup> Reed C., op. cit., str. 129 - 135.

opštepoznatih elemenata i veza. Ukoliko kombinacija prodje dvostruki test originalnosti moći će da uživa zaštitu.

**Oblik pravne zaštite** ostavljen je izboru zemlji potpisnici. Ovo se može ispuniti alternativnim ili kombinovanim donošenjem propisa o posebnom, *sui generis* pravu, kao i zaštitom patentima, autorskim pravom, korisnim modelima ili nelojalnom konkurencijom. Pri tom, svakako treba voditi računa o činjenici da su u momentu donošenja ovog Sporazuma **sve zemlje koje su imale regulisanu zaštitu topografije integrisanih kola izabrale**, umesto već poznatih klasičnih instituta zaštite pravima intelektualne svojine, *sui generis* zaštitu. Ovakvo rešenje izabrano je i u Sporazumu upravo zbog specifikuma predmeta koji se teško uklapa u poznate okvire.

U Sporazumu je izabrana i posebna solucija za određivanje **sadržine i obima** isključivog subjektivnog prava na topografiju. Umesto uobičajene opšte definicije data je **lista radnji koje se smatraju nedozvoljenim** ukoliko se vrše bez ovlašćenja titulara prava ili njegovog sukcesora. Ove radnje, kao minimum koje treba svaka zemlja potpisnica da predvidi, su:

- a) **reprodukovanje** zaštićene topografije u celini ili njenih bitnih delova, bez obzira na tehniku i način reprodukovanja (npr. irelevantno je da li je to samo grafička reprodukcija, telesna reprodukcija kroz masku za proizvodnju slojeva mikročipa ili se radi o digitalnoj reprodukciji na magnetnom medijumu);
- b) **inkorporisanje** zaštićene topografije, u celini ili njenih bitnih delova, u mikročip;
- c) **uvoz, prodaja ili druge vrste puštanja u promet**, u komercijalne svrhe, zaštićene topografije ili mikročipa u kojem je inkorporisana, bez obzira da li je pušten u promet sam za sebe ili ugrađen u neki drugi proizvod<sup>27</sup>.

Osim liste nedozvoljenih radnji Vašingtonski Sporazum je predvideo i listu **ograničenja**. Naime, iako se vrše bez saglasnosti titulara ili sukcesora **ne smatraju se nedopuštenim radnje** kao što su:

- 1. reprodukovanje zaštićene topografije ili njeno ugrađivanje u čip ako je to **uradjeno u nekomercijalne svrhe ili isključivo radi istraživanja, analize i za potrebe nastave**;
- 2. reprodukovanje i ugrađivanje u mikročip originalne topografije koju je jedno lice stvorilo na bazi istraživanja i analize zaštićene topografije (*reverse engineering*). Takvo lice **može da uvozi, prodaje ili stavlja na**

<sup>27</sup> WIPO, Treaty on the Protection of Intellectual Property in Respect of Integrated Circuits, 1989.

**drugi način u promet reprodukcije svoje topografije ili mikročipove u koje je ona inkorporisana.**

Posebno **ograničenje prava** postoji u **interesu međunarodnog saobraćaja**. U stvari, neće se smatrati povredom prava ukoliko mikročip, u koji je inkorporisana zaštićena topografija, **slučajno ili privremeno dospe** na teritoriju zemlje potpisnice kao deo vozila, plovila ili letilice.

**Osnovno načelo** u primeni ovog Sporazuma i obezbeđivanja zaštite ovakvih "topografskih prava" je **načelo nacionalnog tretmana**, a sastoji se u obavezi svake zemlje potpisnice da pruži jednak tretman svim fizičkim licima koji su državljani neke od potpisnica ili imaju prebivalište na njenoj teritoriji, kao i domaćim državljanima. Načelo nacionalnog tretmana, proteže se i na pravna lica koja imaju "ozbiljno i stvarno industrijsko preduzeće" na teritoriji neke od zemalja potpisnica.

**Posebno načelo** vezano je za **iscrpljivanje prava**, kao prava pribavioca za vršenje bilo koje radnje koja predstavlja njegovo isključivo ovlašćenje bez ovlašćenja titulara, i koje nastaje onda kada titular prava, ili od njega ovlašćeno lice, stavi u promet materijalni predmet u koji je ugrađena zaštićena topografija. Dakle, jednom stavljen u promet materijalni predmet sa topografijom dovodi do iscrpljivanja subjektivnog prava.

Što se **početka zaštite** tiče, taj momenat se vezuje ili za: **nastanak; početak komercijalne eksploatacije; podnošenje uredne prijave za registraciju; ili samu registraciju** topografije kod nadležnog organa. Koji će od ovih momenata važiti kao nastanak subjektivnog prava **zavisiće od svake zemlje potpisnice** i njenog opredeljenja.

Od momenta nastanka topografije i početka zaštite zavisi i **dužina trajanja** topografskog prava. Ako je početak prava vezan za **momenat nastanka** tada pravo mora trajati **najmanje 15 godina** od nastanka. Za ostale slučajeve nastanka prava trajanje je **najmanje 10 godina** od momenta koji se računa kao relevantan. Zanimljive su alternative koje se u Sporazumu daju za opredeljivanje zemljama potpisnicima. Naime, rok trajanja zaštite može biti i 5 + 5, odnosno zaštita traje najmanje 5 godina sa mogućnošću produženja za narednih 5 godina (ili 30 meseci) ukoliko posle isteka prvobitnog roka zaštićena topografija i dalje ima komercijalnu vrednost.

Vašingtonskim Sporazumom je predviđena i posebna mogućnost, slično kao kod patenata, da zemlje potpisnice predvide **prinudnu licencu** (ili drugu meru)

radi obezbedjenja nekog javnog interesa (zdravlja ljudi, odbrane zemlje) i/ili najčešće u slučaju kad titular prava krši antimonopolske propise i zloupotrebljava svoj dominantan položaj na tržištu. Suština ove licence je u tom da se vršenje bilo koje radnje koja je, inače, **isključivo pravo** (ovlašćenje) **titulara prava prinudno prenosi na titulara licence**. Nju daje ovlašćeni organ uz obavezu plaćanja naknade titulara licence za korišćenje. Poželjno je da se visina naknade sporazumno dogovori, ali ukoliko to nije moguće, određuje je organ koji je izdaje. Ova ograničavanja prava titulara prava podložna su sudskoj reviziji i moraju prestati onda kad prestanu i razlozi zbog kojih je prinudna licenca izdata.

Posebno značajna **novina** uvedena u ovaj Sporazum odnosi se na **savesnog pribavioca** mikročipa u koji je inkorporisana zaštićena topografija, a mikročip je proizveden kršenjem "topografskog" prava. Znači, neće se smatrati povredom prava kad jedno lice uvozi, prodaje ili na drugi način stavlja u komercijalni promet takve mikročipove. Što se posledica ovakvih radnji tiče Sporazum ih nije posebno definisao. To se ostavlja zemljama potpisnicama da same regulišu svojim propisima, mada se smatra da je propuštena prilika da se obezbede titulari prava u dobijanju pravičnog obeštećenja za svaki nezakonito proizvedeni čip koji je u *bona fide* stavljen u komercijalni promet.

I na kraju, Vašingtonskim Sporazumom se predviđaju i **ingerencije Unije** u slučajevima potrebe revidiranja samog Sporazuma (Skupština može donositi takve odluke 4/5, a u određenim situacijama, i 2/3 većinom glasova). Pored drugih proceduralnih i organizacionih pitanja od posebnog su značaja: mere za nepoštovanje Sporazuma i pitanja vezana za članstvo (postanak ili prestanak).

U slučaju kada se jedna potpisnica ne pridržava odredbi Sporazuma, po mišljenju neke druge potpisnice, može doći do izricanja odgovarajuće mere, koju može, nakon bezuspešnog održavanja međusobnih konsultacija ili nepoštovanja panela sa izveštajima i preporukama Skupštine za rešavanje spora, izreći Skupština. **Mera** se sastoji u ovlašćenju strani u sporu u čiju je korist preporuka donesena **da ograniči primenu Sporazuma** u odnosu na subjekte koji su pripadnici druge strane u sporu ili su u njoj domicilirani.

**Članstvo Unije** može imati svaka država koja je članica Svetske organizacije za zaštitu intelektualne svojine ili je članica UN. Pored država, članica može biti i **medjunarodna organizacija**, a koja ima sopstvene propise o zaštiti intelektualne svojine u vezi sa topografijom i koje se primenjuju na teritoriji zemalja članica. Članstvo može i prestati, može se otkazati, a otkazni rok je godinu dana od notifikacije otkaza.

### 3.2.3. *Sporazum o trgovinskim aspektima prava intelektualne svojine*

**Sporazum o trgovinskim aspektima prava na intelektualnu svojinu** obuhvata zaštitu topografije, a naročito u slučajevima pojave krivotvorenih integrisanih kola na granicama. Od ukupno 75 članova Sporazuma četiri člana posvećena su zaštiti topografije integrisanih kola, ravnopravno sa autorskim i susednim pravima, žigovima, geografskim oznakama, industrijskim modelima i uzorcima, patentima, zaštitom poverljivih podataka i suzbijanjem nelojalne utakmice u ugovorima o licenci. Zemlje članice Svetske trgovinske organizacije (od 1. 1. 1995.) donoseći ovaj Sporazum, saglasne su, kad je u pitanju topografija integrisanih kola, da obezbedjenje zaštite počiva na zaštiti predviđenoj u Vašingtonskom Sporazumu. Naime, zemlje potpisnice Sporazuma obrazuju Uniju i priznaju posebnu zaštitu topografije integrisanih kola licima pripadnicima zemalja potpisnica, kao i asimilovanim licima svih drugih zemalja. Osim toga, iz Vašingtonskog Sporazuma se preuzima i odredjenje pojma topografije podrazumevajući pod njom iste sadržaje i uslove.

Sam Sporazum predviđa dva **osnovna načela** u sprovođenju njegovih odredbi. Pored uobičajenog **načela nacionalnog tretmana**, uvodi se i **načelo najpovlašćenije nacije**. Svakako da će u, Sporazumom, određenim slučajevima postojati i mogućnosti za izuzeća od primene ovih principa, ali ona neće moći biti svojevolsjno određivana od zemalja ugovornica, već tek na osnovu odluke novoformiranog *Saveta za trgovinske aspekte prava intelektualne svojine*.

Naročito je značajna primena odredbe Vašingtonskog Sporazuma koja se odnosi na **obim i sadržinu** isključivog subjektivnog prava koje se tiče nezakonitih radnji uvoza, prodaje i drugih oblika puštanja u promet u komercijalne svrhe, zaštićene topografije i mikročipova u kojima je ona inkorporisana, ukoliko se one vrše bez ovlašćenja titulara ili njegovog sukcesora. Pri tom, ako je u pitanju mikročip nije bitno da li je on pušten u promet sam za sebe ili kao deo nekog drugog produkta<sup>28</sup>. **“Nezakonitim smatraju sve radnje koje se vrše bez dozvole titulara prava, a kojima se obavlja uvoz, prodaja ili drugo distribuiranje u komercijalne svrhe zaštićene topografije ili proizvoda u koji je ugrađeno integrisano kolo, ako ono sadrži nezakonito reprodukovanu shemu”**<sup>29</sup>.

<sup>28</sup> WIPO, Treaty on the Protection of Intellectual Property in Respect of Integrated Circuits, 1989.

<sup>29</sup> GATT, Agreement of Trade-Related Aspects of Intellectual Property Rights of GATT, 1994.

Kao i Vašingtonski i Urugvajski Sporazum priznaje jednu posebnu situaciju **izuzeća** od prethodnog pravila. To je slučaj **sasvesnog pribavioca**, odn. lica koje vrši ili naloži vršenje uvoza, prodaje ili drugog oblika distribucije u komercijalne svrhe nezakonito reprodukovane sheme ili proizvoda u koji je ona inkorporisana, a ono nije znalo ili nije imalo osnova da zna da je integrisano kolo nezakonito reprodukovano ili da proizvod sadrži nezakonito reprodukovanu topografiju. Da bi se ovakva situacija prevazišla zemlje potpisnice Urugvajskog Sporazuma mogu propisati određeno vreme u toku koga lice koje je dobilo obaveštenje da je shema nezakonito reprodukovana može izvršiti bilo koje delo vezano za zalihe koje ima ili koje su naručene pre toga, ali **titularu prava mora uplatiti sumu ekvivalentnu iznosu odgovarajuće naknade** koju bi i inače platilo da je u pitanju slobodno ugovorena licenca za tu shemu.

**Posebna situacija** nastaje u "ostalim slučajevima" korišćenja bez dozvole titulara prava. Svi ovi slučajevi koriste se kad je u pitanju **prinudna licenca**. Ovu licencu, po pravilu, izdaje Vlada ili treće lice koje ona ovlasti. Doduše, odredbe o prinudnoj licenci odnose se na patent, ali primenom analogije mogu se odnositi i na topografiju. Pri tom, ukoliko zakon zemlje ugovornice dozvoljava "**drugu upotrebu**" (*druga upotreba je ona koja se razlikuje od uobičajene, ali koja ne dolazi sa njom u sukob i kojom se ne nanosi šteta legitimnim interesima titulara prava, a ni legitimnim interesima trećih strana*) predmeta zaštite (patenta ili topografije) bez dozvole titulara prava, uključujući i korišćenje od strane Vlade ili trećih lica koje je ona ovlastila, ona će biti moguća ako je u skladu sa pravilima propisanim Sporazumom. **Pravila**, koja se po sistemu *mutatis mutandis* primenjuju na topografiju, su:

1. *izdavanje dozvole za ovakvo korišćenje mora biti bazirano na razmatranju svakog pojedinačnog slučaja;*
2. *dozvola se izdaje samo u slučaju ako su prethodno izvršene određene radnje* (odn. ako je pretpostavljeni korisnik pokušao da dobije dozvolu titulara prava po prihvatljivim komercijalnim uslovima i rokovima i ako se sav taj napor nije, u razumnom vremenskom roku pozitivno realizovao) *u određenim okolnostima* (npr. neće se primeniti ukoliko postoji vanredno stanje u zemlji ili neke druge izuzetne okolnosti, slučajevi ili u javne nekomercijalne svrhe, što izaziva ukidanje uslova uz obavezu obaveštavanja titulara prava);
3. *ukoliko se i dobije dozvola, obim i trajanje korišćenja mora biti samo u svrhe za koje je ona dobijena;*
4. *ovakvo korišćenja je neisključivo;*
5. *ono je i neprenosivo osim kada su u pitanju delovi preduzeća ili aktivnosti u kome se korišćenje obavlja;*
6. *svrha ovakvog korišćenja je snabdevanje domaćeg tržišta zemlje ugovornice koja ga je dozvolila;*

7. *izdata dozvola može biti i ukinuta* ukoliko su okolnosti zbog kojih je dozvola data prestale da postoje i ako je manje verovatno da će se ponovo javiti, a što preispituje nadležni organ;
8. *titularu prava se mora isplatiti adekvatna nadoknada* uzimajući u obzir i ekonomsku vrednost dozvole;
9. *ovakve odluke podležu sudskoj reviziji* i drugim revizijama od strane više instance;
10. *naknade, isto tako, podležu revizijama* (sudskoj i viših instanci); i
11. *zemlje se ne moraju pridržavati uslova kada je korišćenje dozvoljeno da bi se ispravila praksa koja je utvrđena kao nelojalna*, i tada nadležni organi mogu da odbiju ukidanje dozvole<sup>30</sup>. Naravno, ova pravila treba shvatiti kao konkretizaciju odredbi Vašingtonskog Sporazuma koje se tiču prinudne licence.

Kad je u pitanju praksa **izdavanja licenci** uopšte, pa i one koja se odnosi na topografiju integrisanih kola, primenjivaće se odredbe kojima se reguliše **nelojalna konkurencija u cilju njenog suzbijanja**. Pogotovo što su se zemlje potpisnice ovog Sporazuma saglasile da ograničavanje konkurencije predstavlja takvu pojavu koja ima negativni uticaj na trgovinu, kao i transfer i širenje tehnologije. Ukoliko pojedine zemlje žele da preciziraju u svojim nacionalnim zakonodavstvima način i uslove licenciranja koji mogu da, u određenim slučajevima, predstavljaju zloupotrebu prava intelektualne svojine sa negativnim posledicama za konkurenciju na relevantnom tržištu, one to mogu i učiniti. One mogu usvojiti i odgovarajuće mere za sprečavanje i kontrolu takve prakse. Te mere mogu biti u povraćaju prava, u uslovima kojima se sprečavaju osporavanja važnosti ili prinudno izdavanje licenci i sl. U cilju rešavanja ovih problema obavlja se konsultacije između zainteresovanih zemalja<sup>31</sup>.

Ukoliko je u pitanju **trajanje zaštite** Urugvajski Sporazum se unekoliko razlikuje od Vašingtonskog i predviđa sledeće mogućnosti:

1. ako se u određenoj zemlji kao uslov zahteva registracija, zaštita ne može prestati pre isteka od *10 godina računajući od datuma podnošenja zahteva za registraciju ili od prve komercijalne upotrebe*;
2. ako se ne zahteva registracija kao uslov, zaštita će trajati najmanje *10 godina od datuma prve komercijalne upotrebe*; i
3. neka zemlja može predvideti i prestanak zaštite nakon *15 godina od kreiranja topografije*, bez obzira na prethodne rokove.

<sup>30</sup> GATT, Agreement of Trade-Related Aspects of Intellectual Property Rights of GATT, 1994.

<sup>31</sup> GATT, Agreement of Trade-Related Aspects of Intellectual Property Rights of GATT, 1994.

Osim svega ovoga, za topografiju važe i sva ona **pravila i postupci** koji se odnose na zaštitu drugih prava intelektualne svojine i međunarodnu trgovinu.

Naravno, ono što je od izuzetnog značaja za međunarodne trgovinske tokove je pojava **krivotvorene robe**, kao i robe proizvedene na osnovu **nezakonitog prisvajanja topografije**<sup>32</sup>.

U slučajevima povrede prava intelektualne svojine, ili pojave krivotvorene robe i robe proizvedene na osnovu nezakonitog prisvajanja topografije integrisanih kola mogu se izabrati sledeće **solucije**<sup>33</sup>:

- ♦ **obezbedjenja efikasnih postupaka zaštite** topografije integrisanih kola predviđanjem u nacionalnim okvirima i odgovarajućim nacionalnim zakonima, uz poštovanje tri osnovna zahteva: izbegavanja stvaranja barijera legitimnoj trgovini, pravičnosti i jednakosti za sve, kao i dokazne zasnovanosti i mogućnosti preispitivanja;
- ♦ **predviđanje građanskih i upravnih postupaka sa mogućnošću primene sudskih zabrana** što realizuju sudski organi nalažući strani, na osnovu ovlašćenja, odmah posle carinjenja, da prestane sa povredom topografskih prava. Time se **sprečava dotok uvezene robe** kojom se vredja pravo intelektualne svojine na svoju teritoriju. Osim prekida dotoka i vredjanja prava, **nadoknadjuje se stvarna šteta** koju trpi titular prava od namernog prekršioca ili onoga ko je imao osnova da zna da je u prekršajnoj aktivnosti učestvovao. Osim naknade pretrpljene štete **nadoknadjuje se i izgubljena dobit**. Takođe, se **nadoknadjuju i troškovi** nastali u sudskim postupcima. Ove odredbe o naknadi štete titularima prava, odnosno autorima, predstavljaju realizaciju osnovne premise o privatnom karakteru ovih prava. Posebno značajno postaje **pravo titulara na informaciju o identitetu** trećih lica uključenih u proizvodnju i distribuiranje robe i usluga koje predstavljaju povredu prava, kao i o njihovim distributivnim kanalima, što može biti putokaz za dalje praćenje prekršioca, kao i njihovo sprečavanje;
- ♦ predviđanje ovlašćenja sudskih organa da nalože **da se roba koja predstavlja povredu "topografskih" prava, bez bilo kakve naknade, povuče iz trgovinskih tokova**, ali vodeći računa da se ne načini šteta titularu prava, ili, ukoliko je u suprotnosti sa odgovarajućim ustavnim odredbama, **da se uništi**. To se odnosi i na sastavne delove od kojih su pretežno proizvedena integrisana kola i topografija kojom se krše prava;

<sup>32</sup> GATT, Agreement of Trade-Related Aspects of Intellectual Property Rights of GATT, 1994.

<sup>33</sup> GATT, Agreement of Trade-Related Aspects of Intellectual Property Rights of GATT, 1994.

- ♦ predviđanje mogućnosti da sudski organi izriču **hitne i efikasne privremene mere radi sprečavanja povreda i čuvanja relevantnih dokaza**, pri čemu se ove mere naročito izriču radi sprečavanja povrede topografskih prava i stavljanje u promet robe preko trgovinskih kanala koji su u njihovoj nadležnosti, ali i zbog čuvanja relevantnih dokaza o učinjenim povredama, i sl. Radi primene pravila *in audita altera partes* (neka se čuje i druga strana) bez odlaganja se obaveštavaju zainteresovane strane, a kako bi se obezbedilo prikupljanje i pružanje relevantnih podataka i dokaza za donošenje relevantne odluke (o izmeni mere, njenom povlačenju ili potvrdi). Ukoliko se utvrdi neosnovanost zahteva ili nepostojanje povrede prava ili pretnje, na osnovu zahteva optuženog, može se odrediti nadoknada za sve štete koje su izrečenom merom izazvane. Naravno, ne treba zaboraviti da su rokovi za izricanje mera, po prirodi stvari, relativno kratki i ne mogu biti duži od 20 radnih, odn. 31 kalendarskih, dana;
- ♦ izricanje **zabrane puštanja u promet krivotvorene ili robe proizvedene na osnovu nezakonitog prisvajanja topografskih prava**. Sudske mere (privremene ili trajne) nisu jedina pravna sredstva koja stoje na raspolaganju radi efikasne zaštite prava intelektualne svojine, već se one dopunjuju i posebnim **pograničnim merama** koje primenjuju carinski organi u slučaju pojave uvoza ove robe. Pismeni zahtev, sa odgovarajućim dokazima i dovoljno detaljnim opisom robe, podnosi titular prava nadležnim ili sudskim organima da bi carinski organi zabranili puštanje u promet takve robe. Pri tom, uvoznik i podnosilac zahteva treba da budu odmah obavešteni o ovoj zabrani. Ukoliko se desi da je došlo do nezakonitog zadržavanja robe podnosilac zahteva će primaocu robe i vlasniku isplatiti odgovarajuću **naknadu za nanetu štetu**. Naravno da titular prava ima **pravo da bude obavešten** o osnovnim akterima (imenu i adresi pošiljaoca robe, uvoznika i primaoca, kao i količini date robe) i **pravo da pregleda bilo koji zadržani proizvod**, sve u cilju adekvatnog potkrepljivanja svojih zahteva;
- ♦ predviđanje da bez obzira na ostala prava tužbe koja stoje na raspolaganju titularu prava u skladu sa pravom optuženog da traži donošenje odluke od strane sudskog organa, **nadležni organi su ovlašćeni da nalože uništavanje ili povlačenje krivotvorene robe u skladu sa propisanim principima** (princip nenanošenja štete titularu prava, princip nekršenja postojećih ustavnih odredbi, i princip srazmere između ozbiljnosti povrede i pravnih sredstava i interesa trećih lica). Kad je u pitanju krivotvorena roba nadležni organi neće dozvoliti njihov reeksport, niti će je podvrgnuti nekom drugačijem carinskom postupku, osim u izuzetnim okolnostima. Izuzetno se od ovih mera može odustati ako se radi o malim količinama robe nekomercijalne prirode sadržane u ličnom

prtljagu putnika ili poslate manjim pošiljkama<sup>34</sup>. Ovaj izuzetak tzv. *de minimis* uvoza može se primeniti i na proizvode sa nedozvoljeno kopiranim ili integrisanim topografijama, naročito ugrađenim u neke druge proizvode (satove, npr.);

- ♦ mogućnosti pokretanja **krivičnog postupka i kažnjavanja počinioca koji su svesno (namerno) krivotvorili žig ili izvršili piratstvo topografskih prava zbog njihovog komercijalnog korišćenja**. Sporazum upozorava na nužnost predviđanja strogih krivičnih sankcija kako bi se delovalo na odvraćanje budućih počinioca. Zato se predlažu, pored **novčanih, i kazne zatvora**. Naravno, nacionalnim zakonodavstvima ostavljen je izbor kolike će one stvarno i biti. Osim kazne zatvora i novčane kazne preporučuju se i **mere oduzimanja, zaplene i uništenja** "inkriminisane robe i svih materijala i alata koji su se koristili pri izvršenju krivičnih dela". Znači, ako se uništenje ne ostvari po nalogu carinskih, sudskih i drugih nadležnih organa u građanskim i upravnim postupcima, do njega može doći po osnovu izricanja odgovarajuće mere u krivičnom postupku.

Takodje, nužno je napomenuti da se sticanje i održavanje prava na topografiju mogu realizovati i na osnovu *inter partes* postupaka. Vrste i način pridržavanja postupaka i formalnosti, definisan je kao minimum u Sporazumu, što znači da će svaka zemlja moći predvideti i druga, proširujući već predviđena.

### 3.3. *Zaštita topografije integrisanih kola po našem pravu*

Donošenjem Vašingtonskog i Urugvajskog sporazuma stvorile su se pretpostavke izbora odgovarajućeg rešenja zaštite topografije i kod nas. Međutim, započeta promena zakona vezanih za zaštitu intelektualne svojine nije obuhvatila i ovaj predmet. Očekivalo se da će se odgovarajuća rešenja zaštite topografije integrisanih kola naći u njima, ali se očekivanja nisu ispunila. Naime, 28 februara od strane Veća republika i 21 marta 1995. godine od strane Veća građana Savezne skupštine, usvojen je paket zakona iz oblasti zaštite prava industrijske svojine, ali, medju njima nije bilo posebnog zakona kojim bi se regulisala ova materija. Jedno od ranije ponudjenih rešenja (u prednacrtima i nacrtima) bilo je i eventualno unošenje odgovarajućih odredbi u **Zakon o modelima i uzorcima** kojim se reguliše način ostvarivanja i zaštite

<sup>34</sup> GATT, Agreement of Trade-Related Aspects of Intellectual Property Rights of GATT, 1994.

prava na spoljne oblike proizvoda, slike i crteže, koji mogu da se prenesu na proizvod, pa i sheme integrisanih kola. No, i od toga se odustalo<sup>35</sup>.

Tako se Jugoslavija odjednom našla u sve malobrojnijim zemljama koje zaštitu topografije ignorišu. Na prvi pogled ne postoje baš neki izuzetno jaki interesi za prihvatanje nekih (ili svih) rešenja iz nacionalnih zakona drugih zemalja i međunarodnih akata i njihova ugradnja u naše nacionalno zakonodavstvo. Pogotovo što naša zemlja: **1) se ne nalazi među zemljama u kojima se kontinuirano i masovno kreiraju i realizuju** topografije integrisanih kola ili produkti koji ih sadrže, mada se su se u nevelikom broju naših organizacija izradjivala integrisana kola (npr. u niškoj Elektronskoj industriji, kao i u institutu "Mihajlo Pupin"), doduše po licencama<sup>36</sup>; **2) ne investira** u istraživanje i razvoj topografija<sup>37</sup>; **3) se pojavljuje** kao jedna od najvećih piratskih zemalja, jer nam **piratstvo**, kao izuzetno "unosna" aktivnost, **više odgovara** nego legalno snabdevanje licencama ili na drugi način stečenim topografskim pravima, koja iziskuju prilična sredstva za nadoknade i vreme za prenos; **4) preferira** uvozu, prodaji ili drugim oblicima puštanja u promet zaštićene topografije ili mikročipa stečenih na drugi način, za koje nisu potrebne **posebne formalnosti**; **5) izbegava sprovođenje svih sudskih, upravnih, carinskih i drugih postupaka** u slučaju pojave robe koja sadrži krivotvorenu ili nezakonito reprodukovanu topografiju, koja zahteva ne samo odgovarajuću pripremu, već i realizaciju (kadrovsku, materijalnu, organizacionu i sl.) i praćenje stanja, što sigurno može biti veoma skupo; **6) ima slobodu da preduzima bilo kakve aktivnosti kojima bi se štitilo nacionalno tržište**, kao i svoji državljani koji se pojavljuju kao tvorci i titulari topografskog prava izbegavajući princip nacionalnog tretmana i sve one obaveze koje iz oba međunaroda akta proizlaze.

Ipak, ni Jugoslavija, kao ni mnoge "manje razvijene" zemlje kojima sva ponudjena rešenja naročito ne konveniraju, ne sme zanemariti činjenice koje mogu imati značajne posledice na njihove trgovinske i druge odnose sa drugim, više, razvijenim zemljama. Tako se može reći da bi prihvatanjem i realizacijom ova dva Sporazuma Jugoslavija imala znatan pomak u odnosu na:

- ♦ **međunarodno regulisanje problema zaštite intelektualne svojine i usaglašavanje sa drugim zemljama** takvih rešenja koja bi mogla da znače podsticaje razvoja ove oblasti, mada se ne pojavljujemo kao

<sup>35</sup> Drakulić M., Pravo intelektualne svojine i zaštita topografija integrisanih kola, Beograd, Info, br. 6/95., str. 25 - 35.

<sup>36</sup> Po podatku iznetom u Obrazloženju prednacrta EI je do 1992. godine proizvodio integrisana kola po licenci RCA iz SAD.

<sup>37</sup> Po podacima iznetim u tužbi *Brooktree v. AMD*, tužitelj je samo između 1981. i 1986. godine investirao oko 3.8 miliona dolara u razvoj integrisanih čipova tipa "integrated circuit", a za razvoj integrisanih kola uopšte oko 30 miliona dolara.

proizvodjač, već više kao okruženje u kojem je moguće njihovo dizajniranje (projektovanje), a za čijom zaštitom, takodje, postoji potreba, kao i za njenom kastomizacijom, odnosno zaštitom projektovanja prilagodjenih topografija ili produkata dobijenih reverzibilnim inženjeringom;

- ♦ **obezbeđivanje harmonizacije našeg prava** sa međunarodnim standardima i principima vezanim za zaštitu intelektualne svojine i trgovinu robom koja je sadrži;
- ♦ **osiguravanje unifikacije mera i postupaka** kojima se obezbeđuje efikasno i ekspeditivno sprečavanje nezakonitih, nedozvoljenih i protivpravnih radnji vezanih za međunarodne tokove krivitvorene robe i robe proizvedene na osnovu nezakonito prisvojenih topografskih prava, čime se štite ne samo domaći proizvođači i tvorci, nego se na osnovu primene načela nacionalnog tretmana i najpovlašćenije nacije, obezbeđuje i zaštita stranih, što može dovesti do smanjenja međuvladinih sporova i sukoba koji zbog toga mogu nastati;
- ♦ **promene u politici i strategiji** odnosa prema delima intelektualne svojine i njihovom pravnom nacionalnom tretmanu; i
- ♦ **postizanje izvesne pravne sigurnosti** svih savesnih subjekata koji se pojavljuju u procesu nastajanja, proizvodnje, prometa i korišćenja topografije, mikročipova ili drugih proizvoda u koje su oni inkorporisani.

Ovi i mnogi drugi razlozi činili su se dovoljnim opravdanjima za zainteresovanost za prihvatanje nekih (ili svih) rešenja iz nacionalnih zakona drugih zemalja i međunarodnih akata i njihovu ugradnju u naše nacionalno zakonodavstvo.

Otuda Savezni **Zavod za intelektualnu svojinu**, u protekle dve godine, preduzima niz aktivnosti u pripremi za usaglašavanje naših propisa sa međunarodnim aktima, a i zakonima drugih zemalja<sup>38</sup>. Ova aktivnost, iako se odvijala u uslovima informativne blokade naše zemlje i prekida članstva i saradnje sa međunarodnim i nacionalnim institucijama, ipak je rezultirala **Prednacrtom Zakona o zaštiti topografija integrisanih kola**<sup>39</sup>. S obzirom da regularna procedura donošenja tek započinje i da su prihvaćena rešenja u Prednacrtu još radna, to je celishodno sačekati njigovo pojavljivanje u javnoj raspravi. Ono što je za sada moguće konstatovatovati je:

<sup>38</sup> U Obrazloženju prednacrta (str. 18 i 19) navedeni su nacionalni zakoni sledećih zemalja: SAD-a, Japana, Holandije, Španije, V. Britanije, Portugalije, Finska, Češke i Slovačke, Kanade.

<sup>39</sup> Prednacrt ima 26 članova kojima se pored predmeta zaštite regulišu i: uslovi; pravo na zaštitu; postupak; obim i sadržina zaštite; prenos prava; ograničenje; distribucija ili uvoz; prinudna licenca; trajanje zaštite, kao i poništaj registracije; oduzimanje zaštite; registar; pravna zaštita i kaznene odredbe.

1. Da su predložena rešenja **bazirana** na Vašingtonskom i Urugvajskom Sporazumu, kao i pojedinim rešenjima nacionalnih zakona.
2. Da je prihvaćeno rešenje **da se topografija integriranih kola**<sup>40</sup> **smatra intelektualnom tvorevinom**, koja za zaštitu pretpostavlja ispunjenje određenih uslova (originalnosti, intelektualni napor i da nije bila uobičajena u izradi topografija ni proizvodnji integriranih kola u vreme nastanka). Ukoliko topografiju čini kombinacija elemenata i medjuveza, i ona mora ispunjavati uslove. Zaštitu ne uživaju tehnologije za proizvodnju topografije ili integriranog kola, kao ni i ideje, postupak, proces, sistem, metod rada, koncept, princip, otkriće<sup>41</sup>.
3. Da ta intelektualna tvorevina svom stvaraocu<sup>42</sup> i titularu obezbeđuje **određena prava**, koja se mogu ostvariti ispunjenjem određenih uslova<sup>43</sup>. Ta prava su:
  - ◆ **pravo na reprodukovanje zaštićene topografije;**
  - ◆ **pravo na proizvodnju** integriranog kola koje sadrži zaštićenu topografiju;
  - ◆ **pravo uvoza, prodaje i distribucije u komercijalne svrhe.**
4. **Da je postupak za ostvarivanja prava upravni** i započinje podnošenjem pismenog zahteva za registraciju nadležnom saveznom organu. Ovaj organ vodi dve vrste javnih isprava: registar zahteva za upis topografije i registar topografije<sup>44</sup>. Zanimljivo je da je prihvaćeno rešenje da se u registar unosi i prenos prava na topografiju i prava na korišćenje.
5. Jedno od najkontraverznijih rešenja koje je prihvaćeno je, ne bez razloga, **dozvoljenost reverzibilnog inženjerstva** (reprodukovanje). Ono je dozvoljeno:
  - ◆ **za ličnu upotrebu;**
  - ◆ **za nastavu koja se odnosi na topografiju;**

<sup>40</sup> Po čl. 2. Prednacrta "**topografija je trodimenzionalni raspored elemenata, na bilo koji način prikazan, od kojih je najmanje jedan element aktivan, i neke ili sve medjuveze integriranog kola ili takvog trodimenzionalnog rasporeda pripremljenog za proizvodnju određenog integriranog kola**", dok se pod "**integriranim kolom** podrazumeva **proizvod u njegovom završenom obliku ili medjufabrikatu, u kome su elementi, od kojih je najmanje jedan aktivan, i neke ili sve medjuveze integralno formirane u i/ili na komadu materijala u kome se ostvaruje elektronska funkcija**".

<sup>41</sup> Gotovo indentično je rešenje u američkom Zakonu.

<sup>42</sup> Pod **stvaraocem** podrazumeva se jedno ili više fizičkih lica državljana SRJ ili lica sa stalnim boravkom ili sedištem u SRJ. Mada nije eksplicitno navedeno, u Prednacrta je predviđena mogućnost da stvaralac može biti i pravno lice.

<sup>43</sup> Ako se pravo na zaštitu ostvaruje registracijom ono se mora tražiti u roku od 2 godine od datuma komercijalne upotrebe te topografije bilo gde u svetu, a ako je u pitanju nekomercijalno upotrebljena topografija pravo počinje datumom stvaranja te topografije i završava se istekom roka od 15 godina.

<sup>44</sup> Ovom procedurom zaštita topografija se potpuno opravdano približava patentnoj zaštiti, mada su rešenja slična američkom režimu autorskog prava.

♦ *za razne analize i istraživanja.*

Ukoliko se na osnovu analize i istraživanja stvori topografija koja i sama zadovoljava uslove za zaštitu, ona se može ugraditi u integrisano kolo, a njen svaralac može imati sva predviđena prava.

6. Naše pravo prihvatilo je i mogućnost **postojanja iscrpljivanja prava** u posebnim slučajevima uvoza i distribucije. To povlači pravo na naknadu nosioca prava i to od momenta kada je distributer saznao za ilegalnu proizvodnju kola ili je posumnjao da ona postoji.
7. **Zaštita topografije je 10 godina** i teče od:
  - ♦ *datuma podnošenja urednog zahteva za registraciju;* ili
  - ♦ *datuma kada je prvi put komercijalno upotrebljena bilo gde u svetu.*
8. Radi nacionalnog interesa u slučaju da nosilac prava na topografiju ne želi da ih ustupi trećem licu, može se pribeći **prinudnoj licenci**. Ova se licenca sam može izdati pod dva uslova: da se koristi na teritoriji države i da nosilac prava dobije “razumnu” naknadu. Osim nacionalnog interesa prinudna licenca se izdaje i pri zloupotrebi monopolskog položaja nosilaca prava.
9. Naravno, sva ova prava se mogu povrediti i tada se aktivira **mehanizam pravne zaštite i kaznenih odredbi**.

Na kraju nužno je istaći da iako se ne može sa sigurnošću tvrditi da bi samo prihvatanje ovih rešenja moglo značiti značajan podsticaj razvoja ove oblasti, ipak **regulacija može uticati na poboljšanje stanja**.

# GLAVA 6

## ZAŠTITA OD KOMPJUTERSKOG KRIMINALITETA

|  |     |
|--|-----|
| 1. Uvodne napomene o zaštiti od kompjuterskog kriminaliteta        | 386 |
| 1.1. Šta ugrožava informacione sisteme?                            | 392 |
| 1.2. Ko i kako ugrožava informacione sisteme?                      | 394 |
| 1.3. Postoji li kompjutersko podzemlje?                            | 402 |
| 2. Objekt zaštite, kompjuterski kriminalitet - šta je to u stvari? | 404 |
| 3. Tipična dela kompjuterskog kriminaliteta                        | 413 |
| 3.1. Pravljenje i ubacivanje kompjuterskih virusa                  | 419 |
| 3.1.1. Virusi - kako je počelo?                                    | 419 |
| 3.1.2. Pojam kompjuterskog virusa                                  | 422 |
| 3.1.3. Tipovi i vrste kompjuterskih virusa                         | 424 |
| 3.2. Haking  | 428 |
| 3.2.1. Haking - kako je počelo?                                    | 429 |
| 3.2.2. Pojam hakinga   | 431 |
| 3.2.3. Tipovi hakinga  | 434 |
| 3.2.3.1. Amaterski haking  | 434 |
| 3.2.3.2. Profesionalni haking                                      | 436 |
| 3.2.4. Ko, zašto i gde hakuje?                                     | 438 |
| 3.2.5. Kako hakeri ulaze u sisteme?                                | 442 |
| 3.2.6. Otkrivanje, istraga i prevencija - da li su mogući?         | 444 |
| 4. Zaštita od virusa i hakinga                                     | 447 |
| 4.1. Pravna zaštita od kompjuterskog kriminaliteta                 | 447 |
| 4.1.1. Kompjuterski kriminalitet i nacionalni propisi zaštite      | 448 |
| 4.1.2. Kompjuterski kriminalitet i medjunarodna zaštita            | 454 |
| 4.1.3. Kompjuterski kriminalitet po našem pravu                    | 459 |
| 4.2. Etika i zaštita od kompjuterskog kriminaliteta                | 460 |

## 1. Uvodne napomene o zaštiti od kompjuterskog kriminaliteta

Pojava prvih kompjutera ranih 40-ih i njihova primena donela je i prve **zloupotrebe**<sup>1</sup>. Medjutim, prva evidentirana zloupotreba potiče iz 1958. godine, a među prvim sudskim postupcima je slučaj koji se desio 1966. godine u Minesoti i bio vezan za zloupotrebu jednog bankarskog sistema. Svega tri godine kasnije u Bruklinu je stradao, u saobraćajnoj nesreći, i prvi osuđjeni "elektronski" kriminalac (Alfonse Confessore)<sup>2</sup>. Istorija kompjuterskih zloupotreba zabeležila je primat SAD-a u svim dosad počinjenim delima kompjuterskog kriminala, s tim što je SAD i prva zemlja koja je počela sa formalnim proučavanjima i istraživanjima vezanim za ova dela i njihovu sociološku, psihološku, kriminalnu pozadinu. Ali svakako ne treba zaboraviti ni V. Britaniju u kojoj je štampana i jedna od prvih knjiga sa nazivom *Computer Crime* (**Gerald McHanight**), koja je već uveliko požutela od te davne 1973 godine. Prva pravnička studija vezana za zloupotrebe kompjutera ipak se pojavila u SAD još 1971. godine, da bi svega nekoliko godina kasnije bila upotpunjena i primerima iz sudske prakse i slučajevima iz domena istražnih organa (FBI i sličnih institucija). Zanimljivo je da su 1976. godine prvi agenti FBI bili upućeni na četvoronedeljne kurseve vezane za istragu dela kompjuterskog kriminaliteta<sup>3</sup>. Otuda C. Edwards, N. Savage, I. Walden<sup>4</sup>, kao karakteristiku vezanu za pojavu kompjuterskog kriminaliteta upravo ističu najviše zabeleženih slučajeva ovih dela u SAD. To je i sasvim razumljivo s obzirom na rasprostranjenost i zastupljenost kompjutera u toj zemlji.

Danas, gotovo sve informaciono razvijene i zemlje koje to pretenduju da budu formiraju posebne komisije ili komitete eksperata koji prate i istražuju kompjuterski kriminalitet na nacionalnom planu (npr. *Dutch Committee on computer crime*, **FBI National Computer Crime Squad**)<sup>5</sup>. I u okviru međunarodnih organizacija formiraju se tela eksperata sa istim ciljem. Tako u OECD funkcioniše poseban **Komit**

<sup>1</sup> Lipner S., Kalman S., *Computer Law, Cases and Materials*, Columbus, Merrill Publishing Company, 1989., str. 515.

<sup>2</sup> McKnight G., *Computer Crime*, London, Michael Joseph, 1973., str. 13., navodi da je američki sud konstatovao krivicu Confessore-a za 20 slučajeva krađe, utaje i drugih radnji izazvavši *Diners Club*-u gubitke u visini od \$ 621.000.

<sup>3</sup> Lipner S., Kalman S., op. cit., str. 515.

<sup>4</sup> Edwards C., Savage N., Walden I., *Information Technology & The Law*, Basingstoke, MacMillan Publishers LTD., str. 145.

<sup>5</sup> Mohrenschlager M., *Hacking: To Criminalize Or Not? - Suggestions For The Legislature*, *Computers & Security*, Vol. 14., no. 2/95., str. 105; FBI - National computer crime squad, dokument preuzet sa Interneta.

**ekspertata** (*Expert Committee*), a Evropski savet ima svoj poseban **Komitet eksperata za proceduralne pravne probleme vezane za informacione tehnologije** (*Expert Committee of the Council of Europe on Procedural Law Problems Connected with Information Technology, Select Committee of Experts on Computer-Related Crime of the Council of European*). Njihovi godišnji ili čak, polugodišnji izveštaji treba da rasvetle zakonomernosti "razvoja" ovog specifičnog kriminala i da internacionalizuju aktivnosti u njegovom praćenju i sprečavanju.

Dakle, pojava i primena kompjuterske tehnologije donela je niz raznih društvenih implikacija koje su u kontekstu imale i kompjuterski kriminalitet. U početku, nastao je jedan gotovo nesavladivi i teško otklonjivi strah od mogućnosti da će kompjuterska tehnologija ostaviti mnoge ljude bez posla, što je izazvalo nezadovoljstvo, pokušaje da se primena spreči (npr. u Zapadnoj Nemačkoj je u 1984. godini bilo više slučajeva organizovanih kradja originalnih računarskih programa i zamena takvim koji nisu mogli da realizuju ni osnovne rutinske operacije), **sabotaže**, gde je i koliko je to bilo moguće, kao i ignorisanje rezultata koji su nastajali njihovim korišćenjem (tako je 1980. godine u Tulonu bio osnovan poseban **Komitet za likvidaciju i subverziju kompjutera - CLODO** - koji je imao za cilj organizovanje spektakularnih napada na proizvođače kompjutera, dok su u Zapadnoj Nemačkoj u septembru 1983. godine organizovani bombaški napadi na kompjuterski centar *MAN*-a, što je prouzrokovalo gubitak od 2 miliona DM. Ne retko su računari "optuživani" za greške koje je pravio čovek i zloupotrebe iza kojih je opet stajao čovek. Kasnije sabotaze počinju sve više da se odvijaju pomoću kompjutera, tako da se kao njihov objekat pojavljuju sve komponente kompjutera, kao i podataka i računarskih programa i drugih vrednih informacija<sup>6</sup>.

Sredinom 80-ih **kompjuterski kriminalitet je uzeo velikog maha** s tendencijom rasta geometrijskom progresijom.

No, ni naša zemlja nije početkom 80-ih ostala imuna na pojavu prvih oblika krivičnih dela pri čijem izvršenju je korišćen računar. Od 1980. do 1985. godine zabeležena je pojava učestalog korišćenja računara u poslovnim bankama, a od strane njihovih radnika, za izvršenje pljačke i zloupotrebe službenog položaja. Ta pojava je posebno evidentirana na teritoriji grada Beograda i praćena od strane Gradskog sekretarijata za unutrašnje poslove<sup>7</sup>. Prvo takvo delo uradio je D. K. koji je, kao direktor Elektronskog centra za automatsku obradu podataka zajedno sa šefom obrade i pripreme

<sup>6</sup> Sieber U., *The International Handbook Of Computer Crime*, Chichester, John Wiley&Sons, 1991., str. 15 - 18.

<sup>7</sup> Krušić M., Iskustva GSUP-a Beograd u otkrivanju novih pojava oblika krivičnih dela iz oblasti privrednog kriminaliteta u poslovnim bankama, *Bezbednost*, br. 2/86., str. 169 - 176.

podataka, izvršio 1983. godine **delo pljačke sa zloupotrebom službenog položaja, kao i falsifikovanja službenih isprava**. D. K. je otvorio dinarsku štednu knjižicu na donosioca u jednoj banci. Korišćenjem sporazuma ove banke i jednog preduzeća o isplati ličnih dohodaka preko štednih knjižica on je davao posebne naloge o ispravci knjiženja koje je prikazivao kao navodno napravljenu grešku u prenosu podataka na "kasetu", pa je izbacivao po 20 imena radnika i iznos njihovih LD. Njihove je iznose prebacivao na broj svoje štedne partije. Ovom je transakcijom dovodio te radnike u minusni saldo. To je bilo veoma teško za utvrđivanje jer radnici nikada nisu podizali kompletni LD, te se ovaj minus nije nigde iskazivao, već se pojavljivao kao neslaganje stanja knjižica i knjigovodstva u banci. U suštini ove su radnje mogle biti otkrivene jer su se neslaganja pokazivala tek početkom iduće godine kada je trebalo upisivati kamate. Otkrivanje je posebno otežavalo i činjenica da su "kasete" za obradu podataka i prenošenje u memoriju, nakon tih radnji bivale brisane, odn. podaci su se brisanjem uništavali. Nalozi za ispravku, potpisani od strane direktora i ovlašćenog šefa odeljenja, odmah su uništavani, tako da je utvrđivanje pravog stanja bilo teško. Pored toga, da bi se otežalo otkrivanje izvršioci su davali i lažne naloge o navodnoj isplati povećih suma novca i tako svodili stanje na ispravno. Time su stvarali utisak da banka uopšte nije oštećena za taj iznos. Cilj im je bio isplata kamate, a ne same sume. Veštīm prikrivanjem, otkrivanje dela je bilo otežano, a D. K. je, čak, uspeo i da pobegne iz Jugoslavije. Novac je, naravno, podigao. Iz Pariza je vraćen zahvaljujući saradnji nadležnih organa.

Drugi je slučaj vezan za Z. M. blagajnika jedne od ekspozitura iste banke kao i u prethodnom slučaju. On je izvršio **krivično delo zloupotrebe službenog položaja i falsifikovanja službenih isprava**. Naime, u toj ekspozituri terminali su se koristili za ubacivanje novog stanja u memoriju računara smeštenog u ERC-u, kao i za provere stanja po partijama štediša koji su tražili isplatu. Te su poslove radili posebno obučeni radnici, a među njima je bio i Z. M. Ipak, nisu svi obučeni radnici radili ove poslove, već samo likvidatori. Oni su dobijali specijalne ključeve za startovanje. Svaki od ovih ključeva imao je svoju šifru, tako da se pri startovanju znalo ko je na kojem terminalu radio. No, kako su u toj ekspozituri vladali dobri međuljudski odnosi i poverenje, to je prvi ovlašćeni radnik stavljao svoj ključ na početku radnog vremena, a promene je obavljao bilo koji zaposleni. Upravo je to iskoristio Z. M. i sa svoje dinarske štedne knjižice koja glasi na donosioca zahtevao je isplatu veće sume novca. Pošto na knjižici to nije imao, pa je umesto negativnog salda, kako je to i bilo predviđeno programom, u knjižici zabeležena samo tražena suma, a u rubrici "stanje" iskazano stvarno stanje koje je bilo pre ove transakcije. Nakon ove transakcije Z. M. je odmah izvršio i novu promenu na terminalu, stornirajući tražene isplate. Tako je kroz dnevnik terminala prikazano da je isplata stornirana. Promena je, dakle, bila svedena na nulu. Pošto je mašina storniranje isplate prihvatila kao uplatu, to je na knjižici sada postojalo povećanje stanja imovine. Tako se stvorilo lažno stanje i Z. M. je mogao otići u bilo koju ekspozituru i podići tu sumu. Medjutim, on to nije uradio, već je sam sebi izvršio

isplatu. Kao i prethodno i ovo je delo moglo biti teško otkriveno jer se "slobodnim" korišćenjem ključa utvrđivanje izvršioca u znatnoj meri onemogućavalo. U početku je tako i bilo - samo je konstatovana isplata izvršena iz partije štednje na donosioca koji je bio nepoznat. Delo je uočeno tek kasnijom naknadnom kontrolom dnevnika terminala.

Za treće delo 1984. godine optužena je M. V. viši stručni saradnik u odeljenju za odnose sa drugim bankama iste banke kao i u prethodnim slučajevima. Ona je počinila **delo zloupotrebe službenog položaja i falsifikovanja isprave**. Dela je izvršila zahvaljujući kupovinama koje je obavljala jedna beogradska organizacija od jedne titogradske organizacije. Obezbeđenje plaćanja robe vršeno je izdavanjem menice avalirane od strane banke u kojoj je M. V. radila. Posle proteka zakonskog roka beogradska organizacija nije izvršila isplatu robe pa je SDK naplatu izvršio od avaliste. Sredstva su doznačena banci iz Titograda, jer je menični poverilac njen komitent. Prilikom doznake sredstava na virmanu je bila veoma nečitko popunjena rubrika "svrha doznake" tako da su sredstva jedno vreme ležala na privremenom računu titogradske banke. Kad je raščišćavano stanje neraščišćenih računa radnik titogradske banke se obratio banci u Beogradu. Posle razgovora sa više radnika saznao je da je iznos pogrešno upućen njegovoj banci i da treba da se vrati beogradskoj. Ne sačekavši teleks o potvrđi razgovora radnik je izvršio prebacivanje. Teleks potvrdu nije nikada ni dobio. Razgovor je u ime svoje banke obavljala M. V. te je radniku titogradske banke dala umesto broja banke broj štedne knjižice koja glasi na donosioca. Delo se zbog toga pojavilo kao delo nepoznatog počinioca. Ipak je bilo otkriveno, a kasnija istraga pokazala je da je na toj knjižici često bilo raznih transakcija u periodu između 1972. i 1979. godine. Uplate i isplate u 90% slučajeva vršio je radnik sa istom šifrom. Sumnjalo se da taj radnik zna vlasnika knjižice. Osim toga i rukopisi transakcija uplate, isplate, i knjiženja su bili isti što je ukazivalo na mogućnost da su vlasnik i likvidator isto lice. Na osnovu provere šifre utvrđeno je da je M. V. bila likvidator u tom periodu. Međutim, vlasnik knjižice nije bila ona. Traganje koje je nastavljeno dovodi do njenog muža, koji je vlasnik knjižice. Ona je znala broj, pa je otvorila duplu štednu knjižicu, tako da muž nije znao šta se sa njegovom knjižicom dešava. M. V. je potrošila sav njegov novac, a odluku da ga "vrati" donela je kad se javio službenik titogradske banke. To je učinila zahvaljujući pogrešnom usmeravanju uplate.

Četvrti slučaj vezan je za transakcije šalterskih službenika, koji su čekovnim blanketima do kojih su dolazili u svojoj ekspozituri, podizali veće sume novca u drugim ekspoziturama, a zatim deo novca odmah, na blagajni u ekspozituri u kojoj im se vodio tekući račun, uplaćivale. Deo novca je trošen. Uplatama i ovakvim isplatama stvarana je slika urednih štediša. Problem u otkrivanju bio je vezan za uobičajena pravila da banke prave promet u valuti po datumu kada druge banke (ili delovi gde su čekovi realizovani) skinu novac sa računa, a ne po datumu izdavanja čekova. Poseban je problem, kako je

dalje konstatovano, što krivična dela koja vrše zaposleni same banke žele da prikriju, takodje, i radi zakonskih odredbi zabrane uvida u dokumentaciju štednje.

Posebni slučajevi otkriveni tih ranih 80-ih bili su vezani za **prisvajanje devizne štednje** i odnosili su se na zloupotrebe elektronske obrade podataka: prisvajanjem deviznih sredstava sa tudje devizne štednje i kamatnog računa banaka, nedozvoljene kupovine deviza iz depozita po kreditima i zloupotreba kod obračunavanja i isplate devizne kamate. Pošto je tajnost štednog uloga zagantovana to je otežano otkrivanje ovih dela, kao i otkrivanje i dokazivanje krivice izvršilaca. To je bio slučaj i sa J. B. koji je, kao šef devizne štednje, internim nalogima prebacivao sredstva sa jedne partije štednje na drugu, tako što je vršio storniranje ovih promena i novih prebacivanja na svoju deviznu štednju, a štetu svodio na teret banke u kojoj je radio. Izvršenje ovih radnji omogućeno je načinom obavljanja memorisanja štednji iz koje su izostajali podaci o adresi štediše, njegovom nazivu, odn. imenu i prezimenu.

Dj. Č. je tokom 1980. - 1983. godine za "otkup" za račun banke deviznih depozita i dinarskih sredstava upućivala svoja sredstva na partiju kreditnog štediše i tako mu otplaćivala kredit, da bi zatim "internim nalogom" stavljala na isti nalog svoje ime i prezime, partiju depozita i deviznu partiju, i tako devizna sredstva usmeravala sebi. Umesto za račun banke Dj. Č. je za svoj račun vršila otkup, a kako se kasnije pokazalo i za račun svojih koleginica.

Osim ovih dela druga se, na žalost, kod nas još ne evidentiraju, čak se i pojedinačni slučajevi strogo drže u tajnosti. Ipak ponešto "procuri" i za trenutak nas upozori na opasnost. Tako, na primer, dva poznata i obnarodovana slučaja koja su se desila u Beogradu, imala su pored krivične i političku konotaciju. Upravo zbog toga je bilo za očekivati da će se otvoriti niz socioloških, pravnih i etičkih dilema i kod nas. Medjutim, to se ipak nije desilo. Mada je u trenutku u kom se pojavila organizovana "Beogradska grupa hakera" predstavljala pozitivnu pojavu, ona je istovremeno i ukazla da se takvo organizovanje može okrenuti protiv pozitivnih i opšteprihvaćenih moralnih i pravnih normi, ne onih koje su rezultat trenutnih političkih stanja i odnosa, već civilizacisko prihvaćenih, i upozorila da je i kod nas pojava kompjuterske mafije<sup>8</sup> moguća. Naročito ako se ima u vidu:

- 1. da je naše društvo još nespremno da se sa ovom pojavom suoči;**
- 2. da treba očekivati rasprostiranje ovih pojava na razne domene od vojnih, političkih, ekonomskih, pa do obrazovnih (npr. upadi u dobro**

---

<sup>8</sup> Drakulić M., A Step By Step Toward The Solution - Social, Legal And Ethical Dilemmas Of IT In Yugoslavia, Cavtat, Zbornik radova sa: XIV međunarodni simpozijum Kompjuter na sveučilištu, 1991, str. 4.4.2.

čuvane podatke o rezultatima prijemnih ispita za srednje škole i fakultete, naročito ove druge, jer se za izvestan broj fakulteta radi jedinstvena obrada i jedinstvene rang liste, sa mogućnošću prepravke rang lista) ili privatnih<sup>9</sup>;

3. **da napadi postaju sve egzotičniji**<sup>10</sup> i protežu se od pojedinačnih PC i IS do mreža, telekomunikacionih veza, bežičnih servisa, elektronske pošt i drugih objekata<sup>11</sup>;
4. više je nego sigurno da se može očekivati **da će se u plejadi amaterskih kriminalaca naći i neki "manji entuzijasta"** koga će "vrbovati" i naši profesionalni kriminalci, a koji se, takodje, osavremenjavaju;
5. **da sve složenosti političke situacije ne isključuju pojavu kompjuterskih kriminalaca, kao posebne grupe terorista** koji mogu imati ubojito oružje - podatke i razne finansijske transakcije, čijom zloupotrebom mogu biti izazvane i razne političke implikacije.

Pri celoj toj mogućoj viziji budućih događanja ne bi trebalo izgubiti nikako iz vida da se i ove grupe tehničke inteligencije mogu posmatrati kao deo embriona **info tehnokratije**<sup>12</sup>. Pojavljuje se, dakle, jedan poseban, specifičan i različit od bilo kog drugog, društveni sloj tehnokratije čiji su osnovni deo **informatičari**, profesionalci, čije znanje i umeće može biti okrenuto protiv svih ostalih<sup>13</sup>.

<sup>9</sup> Samuelson P., Computers Viruses and Worms: Wrong, Crime, or Both, Edicija: Computers Under Attack, Intruders, Worms, and Viruses, New York, ACM Press, 1990, str. 479-- 486.

<sup>10</sup> Anderson R., Why Cryptosystems Fail, Communications of the ACM, Vol. 37., No. 11/94., str. 32 - 42.

<sup>11</sup> Frankel Y., Herzberg A., Karger P., Krawczyk H., Kunzinger C., Yung M., Security Issues in a CDPD Wireless Network, IEEE Personal Communication, august/1995., str. 16 - 28.

<sup>12</sup> Word G. H., Shriver R. F., Computer Crime Techniques Prevention, Illinois, Bankers Publishing Co., 1987., str. 14.

<sup>13</sup> Stojković G., Drakulić M., Da li haking i virusi prete i našim informacionim sistemima, Zbornik radova sa: II međunarodnog simpozijuma Menadžment i organizacija, Kopaonik, 1991., str. 313.

### 1.1. Šta ugrožava informacione sisteme?

Pretnje koje se nad informacionim sistemima nadvijaju svakim danom su sve raznovrsnije i sve brojnije<sup>14</sup>. No, bez obzira na njihovu izuzetnu dinamiku može se reći da postoje **dva tipa opasnosti** koje ih ugrožavaju: to je **čovjek i njegovo ponašanje**, i to su opasnosti koje nastaju kao **vis maior**.

Prvi tip opasnosti vezan je za **čovjekovu nameru ili nepažnju**. Znači, u pitanju je ljudska težnja da se načini zlo, ili gruba nepažnja zbog koje nastaju negativne posledice za koje je čovek znao, ali je olako držao da će do njih neće doći<sup>15</sup>. Ove opasnosti mogu se pojaviti kao razni oblici krivičnih dela, privrednih prestupa, prekršaja ili grešaka.

Drugi tip opasnosti vezan je za one **situacije koje nastaju nezavisno od volje čoveka**, dejstvom okolnosti koje se teško mogu sprečiti, mada se u nekim slučajevima mogu predvideti.

Posledice koje nastaju dejstvom **prvog tipa opasnosti**<sup>16</sup> uglavnom se mogu svesti na **pet vrsta tipičnih pretnji** za sigurnost sistema<sup>17</sup>:

1. **razni oblici "upada"** - koji se manifestuju kroz prestanak rada sistema, što prouzrokuje gubitke, beskorisnost ili neupotrebljivost određene komponente ili celog sistema na duže ili kraće vreme ili u težim slučajevima, za uvek. Vrlo često upadi u sistem nastaju radi otkrivanja poslovnih ili ličnih tajni, uništenja ili otežavanja rada programa, uništenja

<sup>14</sup> Po United Nations Manual on the prevention and control of computer-related crime, International review of criminal policy, šest su osnovnih uzroka ranjivosti informacionog sistema od kriminala: **1)** ograničenost informacija i procesa; **2)** sistemska pristupačnost; **3)** kompleksnost; **4)** elektronska ranjivost; **5)** ranjivost elektronskih medija za obradu podataka; i **6)** ljudski faktor. Materijal preuzet sa Interneta.

<sup>15</sup> Petrović S., Ćirić V., Zaštita podataka u automatizovanim informacionim sistemima, Beograd, Naučna knjiga, 1986., str. 10-13.

<sup>16</sup> Pfleeger C., Security in Computing, New York, Prentice-Hall Inc., 1989., str. 4.

<sup>17</sup> Slične se opasnosti pojavljuju kod računarskih mreža i komunikacija na koje se napadi mogu podeliti u dve grupe: **aktivne i pasivne napade**. **Aktivni napadi** (*active attack*) **su promene sadržaja informacija ili njihovog toka i rezultiraju:** modifikacijama, fabrikovanjem i prekidanjem tokova. **Pasivni napadi** (*passive attack*) **su prisluškivanja i nadgledavanja tokova informacija, ali bez izmena.** O tomu više kod: Velašević D., Jovanović Z., Gajin S., Milojević I., Sigurnost i zaštita u računarskim mrežama, Zbornik radova sa I stručnog skupa: Zaštita podataka u računarskim sistemima, Beograd, 1995., str.28.

medijuma i opreme kako bi se otežao rad ili sprečilo pronalaženje odgovarajućih file-ova. Tako se kao upadi u sistem mogu pojaviti kradje, haking, poslovna špijunaža i sl;

2. **"presretanja"** - koja znače da je neki neautorizovani subjekat došao do podataka, softvera ili hardvera ili, čak, i do celog sistema sa ciljem da onemogući rad, prouzrokuje neku štetu i pribavi materijalnu korist. Kao tipični slučajevi pojavljuju se oni vezani za mreže i komunikacione veze u koje se uključuju vešti "presretači" ne bi li došli do podataka na osnovu kojih mogu usmeriti svoje poslovne aktivnosti i donositi odgovarajuće poslovne odluke. Ništa manje značajno nije ni nezakonito kopiranje programa ili čipova koji, takodje, pripadaju ovom obliku i koji poprimaju sve veće razmere, pokadkad i međunarodne;
3. **razni oblici neovlašćenog menjanja**, modifikovanja, neke od komponenti sistema ili celog sistema - po pravilu, to su neautorizovani subjekti koji žele da promene neku od komponenti bilo da su to učinili upadom u sistem ili presretanjem i tako došli do onog dela koji su hteli da promene. Ponekad su u pitanju namere da se nanese šteta sistemu ali i da se pokaže da ni jedan sistem nije potpuno siguran. Dugo su najčešći objekt ovih napada bili softver i podaci. Tako se kao oblici modifikovanja softvera pojavljuju logičke bombe, trojanski konj, trapdoor, i slični programi koji se ubacuju u postojeće. Međutim, ne bi trebalo zaboraviti i na ostale oblike napada koji se preduzimaju radi postizanja materijalne koristi time što se modifikovani softver na tržištu plasira kao sopstveni što, pored pojedinaca, čine i softverske firme, a to predstavlja svojevrsni oblik savremenog piratstva. U novije vreme sve se više ugrožavaju i mikročipovi, čije modifikovanje i ugrađivanje omogućuju poplavu klonova na kojima su svoj prodor u svet bazirale mnoge zemlje Dalekog istoka i koje su naterale "izvorne" zemlje da gotovo svakodnevno smanjuju cene, donose zaštitne zakonodavne i administrativne mere i povećavaju ulaganja u dalji razvoj. Ne retko ovi napadi se odvijaju i pod blagonaklonim pogledom države jer joj omogućuju pozitivne efekte u spoljnotrgovinskoj razmeni i povoljniji položaj na međunarodnom tržištu. Vrlo često neovlašćeno menjanje podataka, programa ili hardvera mogu načiniti i autorizovani subjekti prekoračenjem svojih ovlašćenja ili pristupom u, za njih, zabranjene zone;
4. **razni oblici "fabrikovanja" lažnih objekata sistema** - je osobito česta pojava u mrežama ili u bazama podataka u kojima se formiraju novi zapisi na osnovu lažnih podataka ili samo dodaju takvi podaci već postojećim kako bi se stvorila lažna slika o nekoj pojavi (npr. uspešnom poslovanju). Fabrikovanje lažnih objekata naročito velike razmere ima u finansijskim i bankarskim organizacijama u kojima se raznim sistemima (npr. "salami" tehnikom napada, kao udicom, skupljaju "delići" sa raznih tekućih računa

i prebacuju na jedan izmišljeni) vrše krađe, često i velikih razmera. Ovo, po pravilu, obavljaju zaposleni što znači da fabrikovanje mogu izvršiti i autorizovani subjekti, mada nisu retki ni neautorizovani; i

- 5. razni oblici nekontrolisanog oticanja i gubljenja podataka, programa ili mikročipova** - postaju sve učestaliji i najčešće se pojavljuju kao odraz nemarnosti, grešaka i propusta, iako nije isključeno ni da se to čini organizovano i namerno. To je moguće u onim IS u kojima odgovornost za sigurnost ne predstavlja jasno definisan skup prava, ovlašćenja i obaveza svih subjekata, od vrhunskih menadžera do svakog zaposlenog ponaosob.

Značajne, mada manje nepredvidljive, su *opasnosti koje prete od nastupanja više sile*. Mora se reći da su ove opasnosti i najčešće uključene u osiguranje sigurnosti jer se, u osnovi, baziraju na primeni fizičko-tehničkih mera tako bliskih informatičarima<sup>18</sup>. Verujući u dovoljnost ovih mera informatičari su skloni da sa njima započnu i završe osiguranje IS, smatrajući da su sasvim dovoljno učinili za njega. Ne može se negirati njihov značaj jer je izuzetno bitno kako su osigurane prostorije, oprema, fizički smeštaj i obezbedjenje softvera, pravljenje back-up verzija, kao i predviđanje i primena raznih sistema identifikacije autorizovanih korisnika (otisci prstiju, glasa, itd) i sprečavanje neautorizovanim subjektima prilaz ERC-u i podacima. Sigurno da oni jesu značajni, ali ne i dovoljni.

## 1.2. Ko i kako ugrožava informacione sisteme?

Dugo se verovalo da su informacioni sistemi sigurni od napada jer su se obezbeđivali tehničkim i fizičkim merama zaštite<sup>19</sup>. Kako je broj informacionih sistema rastao i kako se, zahvaljujući razvoju kompjuterske tehnologije, mreža povezanih sistema širila, to su se i povećavale opasnosti koje su im pretile<sup>20</sup>. Veliki računarski centri i softverske firme postale su prava Meka za razne zloupotrebe<sup>21</sup>. Sve veći broj podataka, sve bolji softver i sve savršeniji hardver povećavali su njihov značaj i podizali njihovu vrednost čime se postigla i veća zainteresovanost za upade, presretanje, piratstvo, neovlašćeno modifikovanje ili fabrikovanje lažnih komponenti od strane velikog broja različitih subjekata. Nepredvidljivost ove pojave najviše dokazuje

<sup>18</sup> Isti je slučaj i sa Zakonom o informacionom sistemu Republike Srbije, Službeni glasnik RS br. 12/96.

<sup>19</sup> Edwards C., Savage N., Walden I., op. cit., str. 1 - 4.

<sup>20</sup> Fidoten R., The Ethics of Information Resources, Dallas, Dallas Publ., 1990., str. 284.

<sup>21</sup> Drakulić M., Modus vivendi pravne sigurnosti informacionih sistema, Zbornik radova sa: II međunarodnog simpozijuma, Menadžement i organizacija, Kopaonik 1992., str. 278-286.

zatečenost država i njihovih upravnih, zakonodavnih, istražnih, pravosudnih i drugih organa, kao i nepromenljivost pravnih sistema da se sa tim suoče. Bio je to vrh ledenog brega, jer su mnoge od ovih opasnosti predstavljale i krivična dela koja su ubrzo prerasla klasična i postala "**kriminal belih kragani**". Osim toga, pojavili su se i "talentovani klinici" kojima je upad u informacione sisteme, naročito one poznate po specijalnoj zaštiti, predstavljao odraz prestiža i sinonim izuzetne moći. Što su štete bile veće i što su koristi rasle (primeru radi 1987. god. u zapadnonemačkoj automobilske kompaniji *Volkswagen* slučajno je otkrivena kompjuterska krađa počinjena 1984. god. koja je oštetila firmu u vrednosti od 260 miliona dolara i za koju se smatralo da je do tada najveća otkrivena kompjuterska krađa) to se rapidno i povećavao broj počinitelja. Šta više mnogi stručnjaci u ovoj oblasti<sup>22</sup> upozoravaju na dve izuzetno alarmirajuće pojave: **kompjutersku mafiju**, odnosno organizovani kriminal i **kompjuterski terorizam**. Organizovani kompjuterski kriminal biva mrežama povezan i internacionalizovan, s jedne strane, a s druge pojavljuje se u svim zemljama, čak i takvim kakva je ex je Sovjetski Savez<sup>23</sup>. Tome svakako treba dodati i sledeće činjenice<sup>24</sup>:

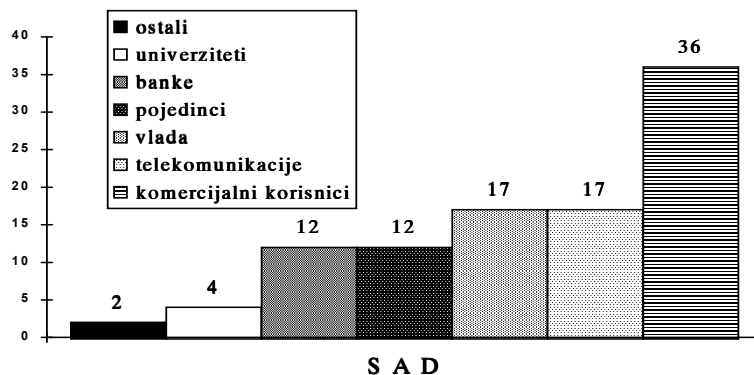
**Prvo. Izuzetno je teško, zbog prirode ovih dela, otkrivanje** (po proceni FBI-a manje od 1% od ukupnog broja dela kompjuterskog kriminaliteta biva otkriveno) **i to**, po pravilu, **slučajno**. To naročito, postaje veliki problem zbog teško pribavljivih dokaza o počinjenom delu, jer se ono vrše bez "krvi" i tragova<sup>25</sup>.

<sup>22</sup> Forester T., Morrison P., *Computer Ethics, Cautionary Tales and Ethical Dilemmas in Computing*, London, Basil Blackwell, 1994., str. 28 - 34.

<sup>23</sup> Hill S., Smith M., *Risk Management & Corporate Security, A Viable Leadership And Business Solution Designed To Enhance Corporations In The Emerging Marketplace*, Computers & Security, Vol. 14., no. 2/95., str. 200.

<sup>24</sup> Sieber U., op. cit., str. 3.

<sup>25</sup> Po UN Manual-u "**nevidljivost**" ovog kriminala leži u sledećem: **1)** sofisticirana tehnologija otežava otkrivanje, a nepoznate žrtve su obično informisane tek nakon učinjene radnje o njenom činjenju; **2)** istražitelji obično nemaju odgovarajuću obuku i iskustvo u kompleksnom okruženju obrade podataka; i **3)** mnoge žrtve nemaju tzv. "plan slučajnosti" na osnovu koga mogu izvršiti prepoznavanje incidenta.



Žrtve kompjuterskog kriminaliteta

**Drugo. Vrlo mali broj žrtava** (organizacija) *obnaroduje počinjena dela*<sup>26</sup> u strahu da, zbog nesigurnosti, partneri i komitenti ne otkazu poslove (što je karakteristično za banke i finansijske institucije čiji su sistemi i najviše ugroženi) ili zbog podataka koji baš i nisu legalno pribavljeni ili čije postojanje u bilo kojoj bazi nije dozvoljeno. Podaci o najčešćim žrtvama upravo ukazuju na to.

Tako je Craig Neidorf koji je pritvoren posle obimne istrage zbog upada u sistem *Bell South-a*, sa optužnicom koja bi mu "obezbedila" 65 godina zatvora i ogromne novčane kazne, bio oslobođen od optužbe zbog toga što su podaci po kojima je "vršljao" bili tajni, te je lakše bilo osloboditi počinioca nego otkriti postojanje ovih podataka. I sama činjenica da je istraga bila pokrenuta je začudjujuća, jer je češći slučaj "zataškavanja" upravo takvih podataka, kao i nedovoljne sigurnosti vladinih, bolničkih, vojnih i sličnih sistema<sup>27</sup>.

**Treće. Višestruka depersonalizacija kriminala** jer, s jedne strane, u većini slučajeva žrtve nisu ljudske, a s druge, i počiniocje je gotovo nemoguće otkriti.

<sup>26</sup> UN Manual posvećuje posebnu pažnju saradnji žrtve sa odgovarajućim telima i organima u obaveštavanju o počinjenom delu ili pokušaju da se ono učini. Ta saradnja prevazilazi i nacionalne granice.

<sup>27</sup> Denning D., *The United States v. Craig Neidorf*, *Communication of the ACM*, vol. 34., no. 3/91., str. 25 - 45.

**Četvrto. Specifična motivacija** koja se pojavljuje kao pozadina ovog kriminala, a što se naročito vidi iz najčešćih motiva<sup>28</sup> - kriminal kao igra, lakoća činjenja uz rešavanje ličnih i finansijskih problema, "magični izazov" da se učini i nemoguće, pojava modernih pirata ili kao neka vrsta novog "bojnog polja" za "savladavanje" menadžera od strane zaposlenih koji su u zavisnom položaju i ne mogu drugačije dokazati svoje sposobnosti. Tome svakako treba dodati i posebne karakteristike osumnjičenih kao što su: visok nivo znanja i zauzimanje pozicija od poverenja<sup>29</sup>.

**Peto. Relativno lako ostvarljive mogućnosti da se ispune brze dobiti i/ili jednostavnije dodje do raritetnih podataka.** To je ostvarljivo pošto se elektronskim transferom prenose enormne količine novca (npr. procenjeno je da *EFT* sistemom oko 200 biliona dolara dnevno promeni vlasnika samo u Njujorškim bankama što je otprilike istovetno i na međunarodnom tržištu razmene u Londonu na kome se transfer obavlja korišćenjem *EFT* sistema preko satelita) i što se, izmedju ostalog, mogu preko kompjuterske industrijske špijunaže otkriti i najtananije poslovne tajne i ne samo one, već se elegantno mogu saznati razni lični podaci pogodni za kasnije malverzacije, ucene, terorističke aktivnosti i sl. Posebno zanimljiv objekt na koji se usmeravaju napadi su računarski programi i telekomunikacione veze. Po podacima **SPA** (*Software Publishers Association*) i **BSA** (*Business Software Alliance*) u 1990. godini iznos štete zbog piratstva u Zapadnoj Evropi iznosio je oko 4.46 milijardi dolara, a u 1989. 3.38, dok je u 1988. bio samo 2.81 milijardi dolara. Sa SAD-om situacija je još alarmantnija<sup>30</sup>. Takođe, u 1994. godini 62% korišćenog poslovnog aplikativnog softvera u Azijsko - Pacifičkom regionu je piratsko (procenjuje se da je to ukupni godišnji gubitak od 8.1 biliona dolara), što je nešto manje nego prethodne godine kada je čak 75% korišćenog softvera bilo piratsko (gubitak od 9.9 biliona dolara)<sup>31</sup>, i sl. Ako se posmatraju i druge zloupotrebe i napadi na kompjuterske sisteme oni su sve veći i sa sve većim štetama. Tako je po podacima Američke advokatske komore u 1987. godini od 300 apostrofiranih američkih korporacija i vladinih agencija 72 su bile žrtve dela kompjuterskog kriminala, a u periodu od 12 meseci one su izgubile izmedju 145 i 730 miliona dolara. U 1991. godini istraživanja koja su obuhvatila korporacije i vladine agencije u Kanadi, Zapadnoj Evropi i SAD-u, a koje su imale 3.000 VAX-ova, 72% je izjavilo da su bili napadnuti u proteklih 12 meseci, 43% je imalo indicija da su u pitanju

<sup>28</sup> Backer J. B., *Introduction to Computer Crime*, North-Holland, Elsevir, 1984., str. 72 - 78.

<sup>29</sup> Lipner S., Kalman S., op. cit., str. 545 - 549.

<sup>30</sup> *Computer Software & Intellectual Property*, background paper, OTA, Congress of The United States Office of Technology Assessment, 1990., str. 17.

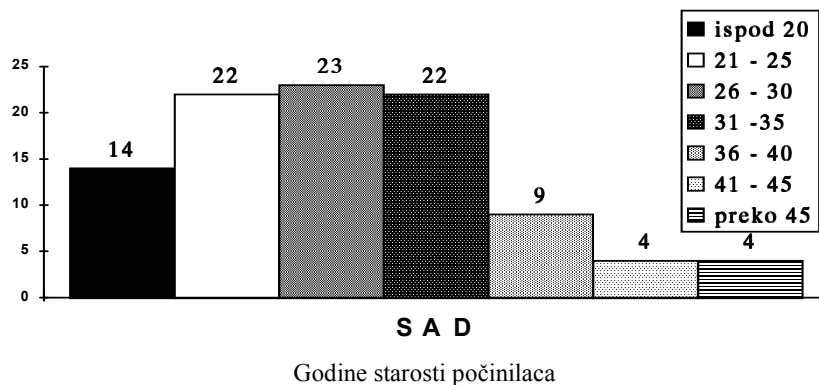
<sup>31</sup> Goodman S. E., Press L., *International Perspectives: Computing in Vietnam: An Asian Tiger in the Rough*, Communication of the ACM, vol. 38., no. 1/95., str. 11 -- 7.

kriminalne radnje, a 8% je izjavilo da je imalo sigurnosni incident tipa kompjuterskih krivičnih dela<sup>32</sup>.

**Šesto. Baza iz koje se regrutuju počinioci je izuzetno široka** jer uvođenjem informatike i u osnovne škole, kao i korišćenje "igrice" omogućuje prevazilaženje straha od mašina, te i sigurno baratanje njima.

**Sedmo. Stalno se pomera donja starosna granica počinilaca** na šta ukazuju podaci da je najveći deo populacije do 35 godina starosti, a među njima zabrinjavajuće raste učešće mlađih od 20 godina. Jedan od mnogih zabeleženih slučajeva kradje novca od strane desetogodišnjih dečaka u Australiji dovoljno je indikativan da zabrine<sup>33</sup>. Isto tako po podacima iz SAD starosna se granica brzo pomera na dole.

**Osmo. Sve je učestalije korišćenje novih i specifičnih metoda i tehnika izvršavanja** - haking, freking, kraking, virusi, crvi, logičke bombe, "trojanski konj", "seckana salama", "tajna vrata" i sl. su samo deo onog novog sa čime se do sada nisu služili počinioci dela. Otkrivanje i dokazivanje primene ovih metoda i tehnika izuzetno je teško, jer mnoge od njih upravo i služe kao maska za obavljanje nedozvoljenih, nelegalnih, neautorizovanih radnji.



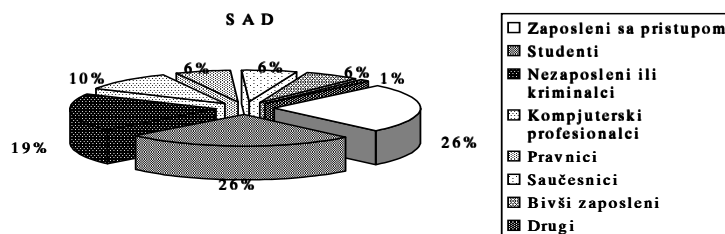
<sup>32</sup> Po UN Manual-u.

<sup>33</sup> Coldwell R. A. , Computer Crime: A Social Perspective, Edicija: Essays on Computer Law, Melbourne, Longman Chechire Pty. Lim., 1990., str. 219.

**Devet. Ove aktivnosti dobijaju nove dimenzije** - velika pokretljivost, kratko vreme, veliki prostor - omogućuju da planeta Zemlja za kriminalce postane globalno selo.

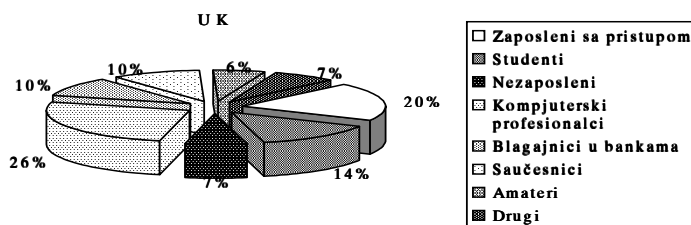
**Deseto. Odsustvo profesionalne etike** i nepostavljanje ovog kriminala kao etičke dileme informatičara ili korisnika, s obzirom da se zbog relativne novine društva nisu opredelila prema njima kao moralnim pogreškama<sup>34</sup>.

Ako se iz dostupnih podataka raznih napada na informacione sisteme i mreže, pored njihovih vrsta, težina i posledica, analiziraju i počinioci može se konstatovati da ih je **najveći broj iz kategorije zaposlenih u organizacijama** u kojima i dolazi do napada (po Hearden-u čak 80%, pri tom, npr. britanske banke gube oko 1% sopstvenog osoblja zbog disciplinskih prekršaja, među njima mnogi su vezani za zloupotrebe *ATM* - *Automatic Teller Machine*)<sup>35</sup>. Međutim, dalja analiza ukazuje da se kao kritične pojavljuju sledeće grupacije potencijalnih i stvarnih "napadača":



<sup>34</sup> Ovom se problemu i pitanju posvećuje posebna pažnja u UN Manual-u i predlaže da se kao obavezni sadržaj ove norme nadju u obrazovanju i obuci informatičara. Isto je i sa Rezplucijom UN usvojenom na 13 plenarnoj sednici VIII kongresa UN sa temom: "Prevent of Crime and the Treatment of Offenders".

<sup>35</sup> Po podacima u UN Manual-u, 90% dela ekonomskog kompjuterskog kriminala u zamljama Zapadne Evrope i Severne Amerike su počinjena interno, odn. od strane zaposlenih, a za ostala 72% su interna, a 23% eksterna.



Drugim rečima to su<sup>36</sup>: **informatičari - profesionalci, korisnici, i/ili treća lica** (fizička i pravna) koja se pojavljuju kao spoljni, ili unutar firme nelegalizovani subjekti koji u pristupu sistemima vide izvor bogatstva, moći ili posebnog statusa.

Najčešće osumnjičeni za ugrožavanje sigurnosti IS su, sa razlogom, oni koji obavljaju poslove vezane za njih - **profesionalni informatičari** (pod kojima se podrazumevaju svi čija je profesija informatika bez obzira na stepen stručne spreme - od analitičara, projekatara ili administratora baza podataka do operatera). Njima su dostupne sve komponente sistema tako da je sasvim razumljivo da se oni pojavljuju kao posebno kritična grupa. Pri tom ne bi trebalo zaboraviti ni na **bivše zaposlene** koji su sa sobom poneli i niz tajni. Kako su oni, iz bilo kojih razloga, napustili organizaciju vrlo ih je teško naterati da čute, naročito kad su u pitanju komercijalne tajne, razvojni softver ili topografija integralnih kola, a koji imaju izuzetnu cenu na tržištu zbog svoje originalnosti i specifičnosti. Posebno, ako je u pitanju naložalna konkurencija koja je raznim sredstvima privukla takve stručnjake (većim platama, učenom, posebnim beneficijama, povoljnijim uslovima rada i sl.). Tome treba dodati i činjenicu da kod nas tvorac računarskog programa koji je nastao u radnom odnosu nema nikakva imovinsko-materijalna autorska prava na svom autorskom delu, niti će takva prava imati nakon proteka izvesnog vremena, za razliku od drugih autorskih dela nastalih u radnom odnosu. U takvim situacijama, kad organizacija može postići izuzetno veliki profit, gotovo da je razumljiva težnja autora da barem "nešto" izvuče iz svog autorskog dela što će biti moguće i kroz njegovo nelegalno plasiranje (kao bivšeg zaposlenog). Problem se multiplicira<sup>37</sup> samom činjenicom da još uvek nije dovoljno izgrađena svest o značaju ove profesije, niti je izgrađen bazični kodeks etičkih normi koji bi obavezivao

<sup>36</sup> Wold G. H., Shriver R. F., op. cit., str. 6; Cornwall H., Data Theft, Computer fraud, industrial espionage and information crime, London, A Mandarin Paperback, 1987., str. 66.

<sup>37</sup> Cornwall H., op. cit., str. 262 - 278.

informatičare na isti ili sličan način kao što obavezuju lekare, advokate i druge koji imaju direktni kontakt sa tajnama<sup>38</sup>.

Druga velika kategorija koja teži da se domogne nekog dela sistema su **korisnici**. Po prirodi stvari, oni bi trebalo da budu najmanje zastupljeni u ugrožavanju sigurnosti sistema jer se pojavljuju kao autorizovani subjekti kojima je slobodan pristup - prevashodno podacima. Međutim, vrlo često korisnici nemaju pristup svim podacima ili da bi mogli da pristupe nekim to moraju platiti. Ponekad se upravo oni pojavljuju kao kradljivci podataka, računarskog vremena, ili vrše neautorizovano kopiranje softvera, mada i kradja mikročipova, takodje, može da se pojavi kao oblik njihovog napada na informacioni sistem. Svi ovi napadi posledica su, u većini slučajeva, visoke cene informacija, softvera, komunikacionih mreža ili mikročipova; konkurentnosti koja se dobijenim informacijama, softverom ili mikročipovima postiže u odnosu na druge korisnike (dovoljno je, npr. posedovati jednu informaciju pre drugih pa postići ogromne dobiti) i svrhe za koju se koriste određeni objekti napada (npr. ukoliko se dodje do podataka o planiranim budućim aktivnostima ili strategijama drugih korisnika to će imati izuzetnu vrednost i sl.). Oni nisu imuni ni od ubacivanja virusa, logičkih bombi, špijuniranja<sup>39</sup>.

Posebna kategorija su **treća lica** koja nemaju direktne veze sa informacionim sistemom ali, iz raznih razloga, to postaju. To su, na primer, zaposleni u organizaciji, instituciji ili organu uprave koji ne koriste sistem i ne pojavljuju se u niukakvoj aktivnoj vezi sa njima, ali se u jednom trenutku pojavljuju kao zainteresovani da dodju do određenih podataka. Faktički, oni su neautorizovani korisnici koji vrše napade unutar organizacije. Posebna grupa su treća lica van organizacije (u kojoj se IS nalazi) koja se pojavljuju kao hakeri, moderni pirati, ili u sličnim ulogama, a sa namerom da prodru u IS iz čiste radoznalosti ili iz neke koristi. Čine to jedanput ili više puta. Ono što je zanimljivo je **pojava studenata i to sa vrlo visokim stepenom učešća**. Razloga ima više, ali su dva najznačajnija: radoznalost i određeni nivo znanja. Međutim, kako su oni nevešti u takvim "rabortama" i hvalisavi, to se veoma lako otkrivaju.

<sup>38</sup> O tome više kod Drakulić M., Drakulić R., U susret profesionalnoj etici informatičara - bliska budućnost ili iluzija, Zbornik radova sa: XXIX SIM OP IS'94, str. 264 - 268.

<sup>39</sup> Wold G. H., Shriver R. F., op. cit., str. 32 - 36.

### 1.3. *Postoji li kompjutersko podzemlje?*

**Kompjutersko podzemlje** (*cyberspace underground*) predstavlja tamnu stranu računarstva. Ono se počelo radjati i razvijati zajedno sa kompjuterizacijom velikih organizacija i centralizacijom informacionih i kompjuterskih sistema. Organizacije postaju sve zavisnije od "poštenja" programera. Medju njima se, osim benevolentnih, nalaze i oni koji to nisu ili koji ne mogu odoleti izazovu "zlata vrednih informacija". Pojava mikroračunara i PC dovodi do dramatične eskalacije opasnih radnji i programa, često **nazivanih "tuće prljavih"** (*dirty dozen*), od kojih strah biva sve veći. Lista se sa nekoliko početnih "loših" programa proširuje na stotine, da bi danas to bila impozantna cifra<sup>40</sup>. U početku sporadične, pojedinačne radnje amatera, često maloletnih pojedinaca zabave radi, postaju vremenom organizovano podzemlje kojim vršljaju telepirati, hakeri, tvorcir virusa, lopovi, špijuni, saboteri i mnogi drugi. Podzemlje dobija svoje obrise. Pojedinci se medjusobno povezuju u grupe sve češće nalik bandama, ili, čak, mafiji. Pokadkad se njihove aktivnosti medjusobno isprepliću. Oni saradjuju ili se sukobljavaju. Diferenciraju se slojevi "običnih" kompjuterskih kriminalaca od "elite". Pri tom ne treba zanemariti ni činjenicu da što je nivo počinilaca niži to su grupacije podlije i kriminal koji vrše suroviji.

Na najnižem nivou su obični kompjuterski kriminalci, oni koji se bave kompjuterskom sabotazom, podmićivanjem, ucenama, pljačkama, terorizmom, pa, čak, i ubistvima korišćenjem računara. Zajednička odlika im je nasilje i vandalizam.

Drugi nivo kompjuterskog podzemlja, po gruboj klasifikaciji, sastoji se od tri vrste aktivnosti u kojima značajnu ulogu igraju moderni "Robin Hudovi" - hakeri, frekeri i tvorcir virusa. Njihova uloga je znatno drugačija od onih na drugim nivoima ili od ostalih grupacija kompjuterskih kriminalaca.

**Haker** (*haker*) je osoba koja ima znanje, sposobnosti i želje da u potpunosti neovlašćeno koristi tuđe kompjuterski sistem. Haking je zajednički naziv za aktivnosti hakera u cilju nasilnog pristupa, odnosno pokušaja pristupa informacionim sistemima da bi se nešto o njima naučilo ili da bi se otkrio neki važan podatak ili izazvao pad (*crack*) sistema, te se i hakeri ove vrste nazivaju **krakerima** (*crackers*). **Ako uništava programe ili datoteke u pitanju je obični kraker, a ako mu je cilj uništenje hardvera tada je to krašer** (*crasher*). On se po hakerima, navodno, izvodi u cilju istraživanja i proučavanja rada sistema. Usmeren je na "alate i smicalice" koji se

<sup>40</sup> Kane P., V.I.R.U.S. Protection, Vital Information Resources Under Siege, Includes dr Panda Utilities, New York, Bantam Books, 1989., str. 419 -463.

koriste za otkrivanje valjanih korisničkih šifara i lozinki za određene sisteme koji hakerima, inače, ne bi bili na raspolaganju. Naime, ukoliko sistem ne bi koristili bez dozvole, hakeri ne bi, uopšteno govoreći, imali pristup uobičajenim izvorima koji su na raspolaganju legitimnim korisnicima. Zbog toga nametljivci moraju eksperimentisati sa komandnim strukturama i istraživati sistemske datotake u nameri da razumeju i efikasno koriste sistem. Ovo je prva grupa aktivnosti koja daje stereotipnu sliku hakera kao tinejdžera nadvijenog nad tastaturom koji beskrajno traga za objašnjenjima i/ili slabim tačkama u sistemu bezbednosti. Međutim, etiketa "uništavači podataka ili oštećivači sistema" koja se lepi za hakere je generalno rezervisana za drugi, odnosno treći tip hakinga.

Druga vrsta aktivnosti vezana je za telefonsko "grebanje". Najčešće se ono, posle avanture John Draper-a, zvanog *Captain Crunch*, jednostavno naziva freking. **Freking je način nadmudrivanja mehanizma za naplaćivanje usluga telefonskih kompanija, jer omogućuje pozivanje bilo koga, bilo gde u svetu, bez plaćanja.** U mnogim slučajevima ono sprečava ili bar otežava mogućnost određivanja mesta poziva, time što se hvatanje izbegava premošćavanjem. Jedna od najpoznatijih akcija **frekera** (*phreakers*) vezana je za *Pacific Bell* u ranim 70-im kada je grupa tinejdžera ukrala ili oštetila kompaniju za stotine hiljada dolara izvedeći jednostavnu igru sa zaposlenima u telefonskoj centrali. Zivkali su zaposlene, lažno se predstavljajući, te ih ubedjivali da im otkriju lozinke koje su "zaboravili". U većini slučajeva igra je uspevala tako da su ulazili u KS ove kompanije i izvršavali modifikacije naredjenja za rad, izazivali prekid u uslugama i mnoge druge malicioznosti. Međutim, pravi napad na *Bell System* nastaje uvođenjem telefonskih kreditnih kartica. Ove kartice su otvorile vrata širokoj skali frekinga. Danas, ni posebno znanje ni oprema nisu neophodni za ove aktivnosti.

Poznata je i grupa frekera (deo čuvene grupe *Chaos Computer Club* iz Hamburga) koja je upotrebljavala međunarodne linije (koristeći imena i lozinke Hamburškog instituta za zaštitu) da bi više puta pristupila *NASA* kompjuterima u 1987., kao i brojnim vojnim mrežama. Nakon otkrivanja upada *NASA* je tri meseca radila na promenama lozinki i čišćenju ubačenog "*trap door*" programa. I druga grupa nemačkih frekera je dve godine, nadgledala Ministarstvo odbrane SAD, pre nego što je bila uhvaćena. Primera za ovu vrstu aktivnosti ima sijaset.

Za većinu iz kompjuterskog podzemlja freking je jednostavan "alat" koji dozvoljava pozive na velike udaljenosti bez plaćanja enormno velikih računa. Broj frekera, nasuprot broju hakera, je veoma mali. Ali, oni koji sebe tretiraju frekerima pravdaju se da to rade zbog učenja i istraživanja telefonskih sistema. Inače se o njima malo zna, kao što se i sposobnost za frekingom potcenjuje.

Na ovom nivou su i **tvorci virusa** (*virus makers*). Oni su ponekad i hakeri, te je veoma teško napraviti baš jasnu razliku između njih.

I na posljednjem, najvišem, nivou su **pirati** (*pirats*). Piratstvo se može realizovati uobičajenim kopiranjem i distribucijom softvera, računarskih programa, kao i čipova, ili se pojavljuje kao tele-piratstvo od strane **tele-pirata** (*tele-pirates*). **Tele-piratstvo** (*tele-piracy*) **je ilegalna distribucija kopija softvera i komercijalnih programa koja se postiže korišćenjem telefonskih modema**. Korišćenje telefona se ne plaća, tako da su tele-piratske aktivnosti trodimenzionalnog karaktera: haking, freking i neovlašćeno umnožavanje. Ono je istovremeno i masovna devijacija. Ulazeći silom i izbegavajući legalne puteve tele-pirati prihvataju frekersko/hakerska pravila i koriste iste sposobnosti, tako da ih frekeri, pa čak i hakeri, optužuju da su oni ti koji su odgovorni za većinu krađa izvršenih pomoću telefonskih kreditnih kartica. Zbog toga, kao i radi "nevešte" podzemne aktivnosti, piratstvo i pirati ne izazivaju toliko divljenje ili prestiž kao haking i hakeri.

Bez obzira koji je tip piratstva u pitanju, pirati su "elita" kompjuterskih kriminalaca jer su im radnje znatno elegantnije i manje nasilne. Retko se dešava da se oni bave uništavanjem ili sabotazama. Veoma često neke njihove aktivnosti više liče na nedoumice nego na namerno učinjena zlodela.

Dakle, kompjuterskim podzemljem "vršljaju" sve ove grupe, nekad ih je veoma teško razlikovati, a često se i međusobno mešaju, kao što se mešaju i njihove razne dimenzije. Ipak njihovo stavljanje pod istu etiketu je neadekvatno, jer se ignorišu međusobni funkcionalni odnosi i razlike.

## 2.      **Objekt zaštite, kompjuterski kriminalitet - šta je to u stvari?**

Kompjuterski kriminalitet je postao deo naše svakodnevnice, iako često nismo ni svesni da se sa njim srećemo ili ga, čak, i sami činimo. Pojava i silno povećavanje broja krivičnih dela učinjenih pomoću ili u vezi sa računarima postali su naglo narastajuća opasnost od koje se treba, a sve više i mora, braniti. Međutim, to je fenomen od koga su se pravnici "dugo čuvali" da ga primete i priznaju, tako da teorijske

rasprave i razni pokušaji da se definiše i klasifikuje još uvek traju<sup>41</sup>. Danas su se iskristalisala **dva pristupa** u određivanju ovog kriminaliteta<sup>42</sup>: po jednom postoji *njegovo jasno (eksplicitno) definisanje*, dok po drugom ono se *određuje posredno* navodjenjem ponašanja koja čine ovaj tip delikvencije. Ne ulazeći u teorijske rasprave o njihovoj validnosti, čini se najprihvatljivije određenje Ekspertne grupe OECD<sup>43</sup> po kome "**kompjuterski kriminalitet** (*computer crime*) **predstavlja svako ilegalno, neetičko ili neautorizovano ponašanje koje uključuje automatsku obradu podataka i/ili njihov prenos**". Ovom određenju treba dodati i to da je **kompjuterski kriminalitet**, u stvari, "*vršenje krivičnih dela kod kojih se računar i kompjuterska tehnologija pojavljuju kao orudje za činjenje određenih dela ili kao objekt zaštite*"<sup>44</sup>. To je zajednički termin koji se koristi za identifikovanje ilegalnih zloupotreba kompjutera i označava direktno korišćenje kompjutera u izvršenju kriminala. Pri tom se pod **zloupotrebom kompjutera** (*computer abuse*) podrazumeva "*svaki događaj u vezi sa upotrebom kompjuterske tehnologije u kom žrtva trpi ili bi mogla da trpi gubitak, a učinilac deluje u nameri da sebi pribavi ili bi mogao da pribavi korist*"<sup>45</sup>. Veoma se često koristi i termin **kriminalitet vezan za kompjutere** (*computer - related crime*)<sup>46</sup> koji u najširem smislu označava "*sve ilegalne akte za čije uspešno gonjenje je neophodno poznavanje kompjuterske tehnologije*"<sup>47</sup>.

Drugim rečima, kompjuterski kriminal predstavlja sasvim specifično ponašanje na koje se ne mogu, u većini slučajeva, primenjivati postojeći instituti krivičnog prava, jer:

**Prvo.** U pitanju je *takvo ponašanje koje je protivpravno, neetičko ili neautorizovano, a usmereno je na automatsku obradu podataka i/ili njihov prenos. S*

<sup>41</sup> Upravo je to konstatovano i u Manual-u UN, u kome se navodi problem definisanja i izostanak jedne opšte i međunarodno prihvatljive definicije. Takođe, navodi se da postoji onoliko definicija koliko i autora i napisanih studija, ali ono što je sigurno i oko čega se svi slažu je da - fenomen postoji.

<sup>42</sup> Ignjatović Dj., Poimovno određenje kompjuterskog kriminaliteta, Anali Pravnog fakulteta u Beogradu, br.1-3/91., str. 137.

<sup>43</sup> Sieber U., op. cit., str. 2.

<sup>44</sup> Edwards C., Savage N., Walden I., op. cit., str. 142.

<sup>45</sup> Parker D., Computer Abuse, Perpetrators and Vulnerabilities of Computer System, Menlo Park California, Stanford Research Institute, 1995., str. 8.

<sup>46</sup> UN Manual navodi da se u nedostatku opšte idefinicije i raščišćenih određenja termini kompjuterski kriminalitet i kriminalitet vezan za kompjutere koriste naizmenično. Isti dokument određuje da **kompjuterski kriminalitet** obuhvata *kriminalne aktivnosti koje su tradicionalne po prirodi, kao što su prevare, krivotvorenja ili zla i za koje počinilac po svim pravima dobija krivične sankcije*. Kompjuter stvara mnoštvo potencijalnih zloupotreba i zlonamernog korišćenja koje mogu, ili su, kriminal, takodje.

<sup>47</sup> Lipner S., Kalman S., op. cit., str. 513.

jedne strane, to znači da je u pitanju delo čoveka, a ne mašine, a s druge, da je predmet "napada" osoben. Otuda se javljaju posebne teškoće, naročito u definisanju da li je u pitanju takva radnja koja predstavlja krivično delo. Da bi to ponašanje predstavljalo krivično delo<sup>48</sup> neophodno je da se ispune sledeći uslovi:

- ♦ **da je delo čoveka** izraženo kao određeno ponašanje kojim se prouzrokuju određene posledice. Ponašanja koja se karakterišu kao krivična dela posledica su obavljanja određene **radnje izvršenja**. Radnja izvršenja se gotovo uvek sastoji iz većeg ili manjeg broja posebnih operacija ili pokreta povezanih u jednu celinu<sup>49</sup>. **Radnja** se može sastojati u **činjenju** (aktivno delovanje) ili **nečinjenju** (propuštanje aktivnog delovanja). Počinilac može delo učiniti sam ili zajedno sa nekim licem ili licima. Pri tom, radnja može biti, pored radnje izvršenja, radnja **podstrekivanja** ili radnja **pomaganja**. Ne ulazeći u detaljnija objašnjenja neophodno je istaći da svaka od ovih radnji, u slučaju kad ih vrši od bar dva lica u odnosu na isto krivično delo, predstavlja **sudeloovanje** ili **saizvršilaštvo**<sup>50</sup>. Za podstrekivanje i pomaganje naš Krivični zakon (KZ) predviđa da će se počinioc kazniti kao i da je sam delo učinio (mada se može i blaže kazniti za pomaganje u određenim slučajevima). Kad je u pitanju kompjuterski kriminalitet on bi mogao biti podveden pod ovaj uslov, jer se stvarno radi o delu čoveka, doduše sa malo specifičnim orudjem, objektom, subjektom - računarom, koji sve više postaje idealno orudje i ubojito oružje u rukama znalaca;
- ♦ **da je predviđeno i opisano u svojim bitnim obeležjima u zakonu kao krivično** (znači, primena postulata *Nullum crimen, nulla poene sine lege*). Ovo je jedan od glavnih kamena spoticanja vezanih za kompjuterski kriminalitet. Naime, krivični zakoni koji su ostavili prazan prostor za ovu vrstu kriminala ne dozvoljavaju analogiju. Ona, i da je dozvoljena, ne bi bila dovoljno obuhvatna za takva dela kao što su haking i virusi, koji su toliko posebni i svojevrsni da se ne uklapaju ni u jedno dosad poznato delo. U suštini, mnoga dela kompjuterskog kriminaliteta ne mogu da se podvedu pod druga, zakonima priznata i poznata, krivična dela;
- ♦ **da je društveno opasno**, što je određeno opštim načelima društvenog uređenja u određenoj državi i može biti različitog intenziteta. Tako, naš KZ<sup>51</sup> predviđa da nisu krivična dela ona koja predstavljaju neznatnu

<sup>48</sup> **Krivično delo je društveno opasno delo koje je zakonom određeno kao krivično delo i čija su obeležja određena zakonom** (čl.8. t. 1. Krivičnog zakona SFRJ, Službeni list SFRJ, br. 44/76.

<sup>49</sup> Živanović T., Krivično pravo, Beograd, Gundulić, 1935., str.176 - 179.

<sup>50</sup> **Podstrekivanje** ili radnja podstrekivanja predstavlja *navodjenje drugog lica na izvršenje krivičnog dela*. **Pomaganje** je, u stvari, *doprinošenje izvršenju krivičnog dela od strane drugog lica*.

<sup>51</sup> KZ, čl. 8. t. 2.

opasnost, jer imaju mali značaj i neznatne ili nikakve štetne posledice. Ovaj uslov, kad su u pitanju dela kompjuterskog kriminaliteta, ispunjava se često mnogo više nego i za jedno drugo delo. Smrt ili onesposobljavanje bolesnika usled upada i zaustavljanja sistema ili prepravljanja podataka o dijagnozi i terapiji je, svakako, društveno opasno delo. Isto tako, zloupotreba računara može predstavljati i masovnu opasnost.

Znači, da bi se neko ponašanje vezano za primenu računara ili prenos podataka moglo okarakterisati kao krivično delo neophodno je da se kumulativno ispune svi ovi uslovi. Kako to nije slučaj po našem pozitivnom krivičnom zakonodavstvu, dela koja su vezana za kompjuterski kriminalitet ne tretiraju se još uvek kao krivična.

Iako nije sastavni element pojma krivičnog dela, ipak, za njegovo razumevanje bitno je i vreme njegovog izvršenja<sup>52</sup>. Ono je od posebnog značaja kad su u pitanju dela kompjuterskog kriminaliteta za koje je veoma teško utvrditi, zbog specifičnosti, vreme nastanka dela. Posledica je, uglavnom, ta na osnovu koje se delo i otkriva, jer je gotovo nemoguće delo otkriti u samom nastajanju.

**Drugo. Za postojanje kompjuterskog kriminaliteta neophodno je postojanje računara, odnosno znanja vezanih za KT.** Pri tom, ne treba zanemariti činjenicu da kompjuteri u ovom svojevrsnom kriminalu mogu imati četvorostruku ulogu<sup>53</sup>:

- ♦ **objekta** - kada su kriminalne aktivnosti usmerene na uništenje samih kompjutera, podataka ili programa, kao i drugih uređaja koji im omogućuju rad;
- ♦ **“subjekta”** - kada se kompjuter pojavljuje kao odredište ili okruženje kriminala, izvor ili povod za korišćenje jedinstvenih formi i vrsta napada na imovinu;
- ♦ **instrumenta** - neki tipovi ili metode kriminala su kompleksni, te zahtevaju korišćenje kompjutera kao orudja ili instrumenta. Kompjuter se može koristiti "aktivno" ili "pasivno";
- ♦ **simbola** - kada se kompjuter koristi za zastrašivanje ili obmanjivanje.

<sup>52</sup> Smatra da je krivično delo učinjeno u vreme kad je počinilac radio ili bio dužan da radi bez obzira kada je nastala posledica.

<sup>53</sup> Lipner S., Kalman S., op. cit., str. 514.

Znači, za razliku od mnogih drugih krivičnih dela za koje nije bitno čime su počinjena (nož, puška, otrov - ubistvo je je počinjeno, a posledica je smrt jednog ili više lica) za postojanje kompjuterskog kriminaliteta neophodno je postojanje računara. Ova osobenost čini se da umnogome olakšava problem, jer omogućava da se jasno sagledaju orudje i objekt napada. Ono što je otežano je utvrđivanje postojanja krivične odgovornosti<sup>54</sup>. Da bi neko bio krivično odgovoran potrebna je njegova **uračunljivost** (da je počinilac u momentu činjenja mogao da shvati značaj svog dela i da je bio sposoban da upravlja svojim postupcima, odnosno da kod njega ne postoji neuračunljivost ili bitno smanjena uračunljivost)<sup>55</sup> i **vinost - krivica** je subjektivni element koji označava da je počinilac krivično delo učinio sa umišljajem ili iz nehata<sup>56</sup>. Predviđanje nehata kao oblika vinosti u krivičnim zakonima osobito je važno kad su u pitanju počinioци dela kompjuterskog kriminaliteta.

Kako se krivična odgovornost uvek procenjuje **individualno**, s obzirom na učinjeno delo, to se pored vinosti i uračunljivosti procenjuje i da li je delo učinjeno u **nužnoj odbrani** ili iz **krajnje nužde**. Ako se utvrdi da je u pitanju nužna odbrana ili krajnja nužda, onda se delo neće kvalifikovati kao krivično. Što se dela kompjuterskog kriminaliteta tiče gotovo za većinu od njih počinioци nisu bili u krajnjoj nuždi, niti je u pitanju nužna odbrana, čak i onda kad se radi o krađama, špijunaži, prevarama, sabotazi, učinjenim pod pritiskom, pretnjom ili ucenom.

Pored nužne odbrane i krajnje nužde mnogi krivični zakoni poznaju i institute **stvarne i pravne zablude**. Za razliku od situacije kad je u pitanju nužna odbrana ili stvarna nužda i kad se delo učinjeno pod tim okolnostima ne smatra krivičnim delom, dotle kad su u pitanju stvarna ili pravna zabluda onda dela koja nastanu u tim

<sup>54</sup> **Krivična odgovornost predstavlja subjektivno svojstvo koje se vezuje za počinioца nekog dela koje ima obeležja krivičnog.** Obično se u teoriji i zakonodavstvima pravi razlika između krivične odgovornosti u širem i užem smislu. Pod **krivičnom odgovornošću u širem smislu** podrazumevaju se tri stvari: **1)** da je lice krivično delo učinilo; **2)** da je imalo određena psihička svojstva; i **3)** da postoji određeni psihički odnos prema učinjenom delu. **Uže shvatanje krivične odgovornosti** vezano je za psihička stanja učinioca i njegov odnos prema delu.

<sup>55</sup> **Neuračunljivost** po našem KZ (čl.12. t.1.) postoji onda kad **počinilac u vreme izvršenja krivičnog dela nije mogao da shvati značaj svog dela ili nije bio u stanju da upravlja svojim postupcima zbog trajne ili privremene duševne bolesti, privremene duševne poremećenosti ili zaostalog duševnog razvoja.**

<sup>56</sup> **Umišljaj** pretpostavlja da je **učinilac nekog dela bio svestan svog dela i da je hteo njegovo izvršenje**, odnosno da je svestan da će zbog njegovog činjenja ili nečinjenja nastati zabranjena posledica i želeo je njeno nastajanje. **Nehat** postoji onda kad **je počinilac nekog dela svestan da zbog njegovog činjenja ili nečinjenja mogu nastati zabranjene posledice ali je olako drži da će moći da ih spreči ili da one ipak neće nastupiti.** Takođe, nehat postoji i onda ako počinilac nije bio svestan mogućnosti nastajanja zabranjene posledice mada je prema okolnostima i prema njegovim ličnim svojstvima bio dužan i mogao biti svestan te mogućnosti (čl. 14. KZ).

okolnostima jesu krivična dela, ali se počinioci oslobadjaju krivične odgovornosti (stvarna zabluda) ili predstavljaju fakultativni osnov za ublažavanje kazne (pravna zabluda)<sup>57</sup>. Postojanje stvarne i/ili pravne zablude veoma su česte baš kod dela kompjuterskog kriminaliteta koje počinu npr. studenti u izradi seminarskih radova ili radi prestiža koji žele da "upadom" dobiju. Međutim, ne treba zaboraviti one situacije kad su pod plaštom stvarne ili pravne zablude počinjena dela kompjuterske prevare i krađe.

Pitanje **krivičnih sankcija**<sup>58</sup> u odnosu na počinioce kompjuterskog kriminaliteta postaje jedno od ključnih pitanja u preventivi i sprečavanju ovakvih dela. Strogost sankcija može predstavljati pretnju, ali i izazov. Mada neka zakonodavstva pribegavaju malim kaznama, ponajčešće novčanim, mnoga su orijentisana ka strožim, ne bi li zaplašila impozantnu grupu počilaca<sup>59</sup>.

Mnoga zakonodavstva prihvataju **odredjena načela o krivičnoj sankciji**, koja bi trebalo primeniti i kad su u pitanju počinioci kompjuterskog kriminaliteta. To su, između ostalog, sledeća: **1) načelo legaliteta** u propisivanju, izricanju i izvršavanju krivičnih sankcija; **2) načelo pluraliteta** odn. predviđanje više grupa i vrsta krivičnih sankcija čime se stvaraju mogućnosti da se, s obzirom na ličnost počinioca, može primeniti ona sankcija koja najviše odgovara generalnoj i specijalnoj prevenciji kriminaliteta, i **3) načelo da je osnov i granica za određivanje krivičnih dela i propisivanje krivičnih sankcija zaštita čoveka i drugih osnovnih vrednosti društva i primenjivanje krivičnopravne prinude**.

Primena načela pluraliteta znači, pre svega, da je u krivičnom zakonodavstvu predviđeno postojanje više grupa i vrsti kazni. Tako, naš KZ predviđa sledeće grupe

<sup>57</sup> **Stvarna zabluda** postoji onda kad počilac krivičnog dela u vreme njegovog izvršenja nije bio svestan nekog njegovog, zakonom određenog, obeležja ili kad je pogrešno smatrao da postoje okolnosti prema kojima bi, da su one stvarno postojale, to delo bilo dozvoljeno (čl. 16. KZ). **Pravna zabluda** postoji onda kad počilac krivičnog dela iz opravdanih razloga nije znao da je to delo zabranjeno (čl. 17. KZ).

<sup>58</sup> **Krivična sankcija** predstavlja zakonom određenu meru koju, u zakonom propisanom postupku, izriče sud učiniocu krivičnog dela, zbog ili povodom učinjenog dela, a u cilju zaštite osnovnih vrednosti određenog društva.

<sup>59</sup> Za krivičnu sankciju neophodno je da se ispune sledeći uslovi: **a) primenjuje se samo prema učiniocu krivičnog dela; b) izriče se samo pod zakonom propisanim uslovima; c) izriče je sud kad, po zakonom propisanom, postupku utvrdi da postoje uslovi za njeno izricanje; d) svrha je suzbijanje društveno opasnih dela** kojima se ugrožavaju ili povređuju osnovne vrednosti jednog društva. Ovo je opšta svrha krivičnih sankcija koju dopunjuju, još i sprečavanje učinioca da krivično delo čini i njegovo prevaspitavanje, vaspitni uticaj na druge da ne bi činili krivična dela, jačanje morala društva i uticaj razvijanja društvene odgovornosti i discipline građana.

krivičnih sankcija: kazne, uslovnu osudu, sudsku opomenu, mere bezbednosti i vaspitne mere. **Kazne** mogu biti: smrtna, zatvor, novčana kazna i konfiskacija imovine. **Mere bezbednosti** su npr. zabrana vršenja poziva, delatnosti ili dužnosti; zabrana javnog istupanja; oduzimanje predmeta i proterivanje stranca iz zemlje. Od svih mera bezbednosti svakako su za **kažnjavanje počinioca kompjuterskog kriminaliteta najinteresantnija mera zabrane vršenja poziva, delatnosti ili dužnosti. Vaspitne mere** koje se izriču maloletnicima su: disciplinske mere; mere pojačanog nadzora i zavodske mere. One postaju najprimerenije kad su u pitanju deca kriminalci, odn. "pametni klinici". Medjutim, danas, kad se rapidno povećava udeo ove kategorije počinilaca mnogi zakoni izmenili su stav prema vaspitnim merama predviđajući pored njih i mere zatvora (maloletničkog). Tako je u federalnoj državi Kaliforniji pomerena donja granica za kažnjavanje na 10 godina i predviđena kazna zatvora za rasturače droge i hakere, odnosno "ubacivače" naročito štetnih i opasnih virusa.

Najčešće sankcije koje se izriču za dela kompjuterskog kriminaliteta uglavnom se kreću od novčanih i kazni zatvora do zabrane obavljanja delatnosti (npr. za krađu izvršenu pomoću računara koja je dostizala vrednost oko \$ 13.956 glavni kontrolor je, zajedno sa sinom, kažnjen sa po \$ 2.107 novčane kazne i 12 meseci zatvora; jedan zubar koji je od 1978. do 1982. godine "zaradio" sumu od \$ 316.981 ubacujući u listinge ime svog bivšeg zaposlenog kao pacijenta i naplaćujući od zdravstvenog osiguranja za poslove koje nije obavio kažnjen je pored novčane kazne i sa 18 meseci zatvora, a po izlasku iz zatvora od Zubarskog društva i zabranom vršenja delatnosti, i sl.).

Sve krivične sankcije se nakon pravosnažnosti presude unose u **kaznenu evidenciju**, s tim sto se u zakonu propisuje kome se ovi podaci i pod kojim uslovima mogu davati i kad nastaje brisanje i kojih osuda<sup>60</sup>. Za uspešno praćenje i sagledavanje uzroka, posledica i najuobičajenijih dela i počinilaca kompjuterskog kriminaliteta zato prevashodno bi trebalo obezbediti njihovo sistematsko i kontinuirano evidentiranje<sup>61</sup>. U većini informaciono razvijenih zemalja posebna tela i organi prate ove podatke (Istražna komisija u V. Britaniji; Nacionalni centar za podatke o kompjuterskom kriminalitetu, SAD; Komisija eksperata za praćenje ekonomskog kriminala u Nemačkoj, i sl.), ali i u okviru određenih međunarodnih organizacija (OECD, specijalizovanoj agenciji UN, EU) posebni podaci se vode o ovim delima. Pored toga, pojedinci-počinioci treba da znaju da će ih i koliko ovakvi podaci pratiti kroz profesiju i život.

<sup>60</sup> Npr. čl. 93 i 94. KZ

<sup>61</sup> To su predvidele i: Recommendation No. R (89) 9 on computer relating crime i Recommendation No. R (95) 13 of Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology.

Treće, posebno značajno za kompjuterski kriminalitet je i pitanje njegovog otkrivanja i vođenje krivičnog postupka u slučaju da se zna za njegovo postojanje<sup>62</sup>. Kad su u pitanju ova dela izuzetno veliki je problem otkrivanja i sprovođenje krivičnog postupka. S jedne strane, pošto su to dela koja se izuzetno teško otkrivaju, to je u vođenju krivičnog postupka potrebno specifično znanje kompjuterske tehnologije. Tako je za uključivanje u *Nacionalni eskadron za kompjuterski kriminal FBI-a (NCCS)* predviđeno da članovi moraju imati: **1)** određeni stepen obrazovanja iz kompjuterskih nauka; **2)** određena iskustva i obuku u industriji ili akademskim institucijama; **3)** odgovarajuća osnovna znanja iz ekonomije; **4)** znanja o podacima i telekomunikacionim mrežama; **5)** iskustva sa UNIX ili drugim operativnim sistemima<sup>63</sup>. Za ilustraciju tih znanja može poslužiti *slučaj Vogel*. Naime, grupa hakera 3 godine je uznemiravala *Vogel*-a. U nasumice započetoj igri na kraju je učestvovalo preko 100 ljudi, koji su svakodnevno i to više puta na dan uznemiravali *Vogel*-a i celu njegovu porodicu. Slučaj je stigao pred FBI, koji je zajedno sa Ministarstvom pravde i državnim tužilaštvom, više od 5 meseci vodio istragu ne bili se otkrili počinioci. Od strane FBI bi li su uključeni specijalisti za otkrivanje ovakve vrste kriminala, članovi *NCCS*-a. To ujedno govori o spretnosti počilaca i sve većoj potrebi za posebnim znanjima istražitelja. Računa se da više hiljada agenata FBI, CIA i drugih specijalizovanih agencija u SAD, posebno školovano za otkrivanje i gonjenje počilaca ovih dela. S druge strane, ne treba zaboraviti na činjenicu postojanja organizovanog kriminala koji vrše profesionalci, te otuda ne samo da je otežano otkrivanje i istraživanje, već opasnosti prete i subjektima u istrazi. Takodje, za razliku od drugih oblika kriminaliteta, specifičnost i masovnost orudja predstavlja veliki problem za otkrivanje počinioca. Sigurno je daleko lakše tražiti određeni tip pištolja (i zbog obaveze registracije i prijavljivanja pri kupovini) nego u moru kompatibilnih kompjutera naći onaj koji je poslužio kao sredstvo, ponekad i veoma udaljeno<sup>64</sup>. Pri tom, u pitanju su, po pravilu, izuzetno inetligentni i vešti počinioci koji se dobro čuvaju da se lako ne otkriju i da im se teško mogu naći pravno relevantni *corpus delicti*.

<sup>62</sup> **Krivični postupak je skup pravno normiranih radnji određenih državnih organa i drugih subjekata koje se vrše u slučaju verovatnoće da je učinjeno krivično delo da bi se ustanovilo da je krivično delo učinjeno, ko ga je učinio i da li, e u smislu propisa krivičnog prava, ima li osnova da se na učinioca primene krivične snakcije, pa, ako ima, da se one i primene.** Pored zakonom propisanih radnji, krivični postupak obuhvata i skup pravnih odnosa koji nastaju, razvijaju se i prestaju povodom delatnosti državnih organa i drugih subjekata u krivičnom postupku. S obzirom da se radi o specifičnoj materiji to pravo koje normira ove radnje i odnose predstavlja posebno pravo - **krivično procesno pravo**, a zakon kojim se to reguliše su posebni (npr. kod nas je to Zakon o krivičnom postupku - ZKP).

<sup>63</sup> O ovom eskadronu više u dokumentu FBI - National computer crime squad, preuzetom sa Interneta 1996.

<sup>64</sup> To je upravo i bilo obrazloženje za uvođenje *clipper chip*-a, ili posebnog softverskog dodatka Microsoft-a za Internet.

Otežano otkrivanje i praćenje najčešće su posledica sledećih okolnosti<sup>65</sup>:

- ♦ **velika sposobnost prerađivanja;**
- ♦ **skrivenost tragova;**
- ♦ **nevidljivost dokaza;**
- ♦ **teškoće u dešifrovanju dokaza;**
- ♦ **lako brisanje dokaza;**
- ♦ **veliki broj podataka;**
- ♦ **neiskustvo progonioca i tužioca;** i
- ♦ **pravna nesigurnost i nedostaci.**

Kako je najviše počinilaca unutar organizacija veoma često se prvi delovi istrage vode u njima. Najveći broj slučajeva otkriven je **internom kontrolom** (po podacima Istražne komisije V. Britanije u 1987. godini, od ukupnog broja u 48 slučajeva interna kontrola je bila "kriva" za otkrivanje počinioaca, a u 13 je to bio rezultat **interne istrage**)<sup>66</sup>. Zato je neophodno preduzimanje odgovarajućih mera sigurnosti u kojima interna kontrola (ona bi trebalao da bude sastavni deo procesa rada, dok je interna istraga vezana za određeni slučaj i obavlja se ad hoc, po potrebi) treba da obuhvata: kontrolu ljudi, strogu i striktnu raspodelu ovlašćenja, kontrolu ulaza, procesa, izlaza, fizičkog pristupa, softvera i komunikacija. To svakako ne bi trebalo da bude ugradjivanjem kliper čipa<sup>67</sup>, ili stalnim špijuniranjem i snimanjem zaposlenih<sup>68</sup>, već dobrim softverskim sistemom za evidentiranje, stalnim nadgledanjem sistemskih ulazaka i praćenjem svih signala<sup>69</sup>. Za uspešnost otkrivanja i sprečavanja od vitalnog je značaja da se kompletna postupak, strogo u tajnosti, unapred planira i organizuje<sup>70</sup>.

Osim interne, značajna je i **eksterna istraga** i otkrivanje dela i počinilaca. No, da bi se obezbedile osnovne pretpostavke za istragu, nužno je rešiti, na odgovarajući način, i posebne probleme koji se odnose na kompetenciju istražitelja,

<sup>65</sup> Sieber U., op. cit., str. 139 - 142.

<sup>66</sup> Edwards C., Savage N., Walden I., op. cit., str. 168.

<sup>67</sup> **Clipper chip je identifikacioni čip koji bi omogućio lakše priključivanje na mreže, ali bi on istovremeno služio i za špijunažu "preturanjem" po sistemu pojedinca, dešifrovanjem poruka poslanih telefonom, faksom ili modemom.** Njega je predložila američka vlada što je izazvalo burne reakcije, jer predstavlja jednu od najvećih pretnji ličnim slobodama i pravima. O tome više Garner R., Clipper's hidden agenda, Open Computing, vol. 11., no. 8/94., str. 51 - 55.

<sup>68</sup> Drakulić R., Drakulić M., Mogućnost IT prismotre - uzrok tehno-stresa, Zbornik radova sa naučnog skupa: "Tehnologija, kultura i razvoj", Beograd, 1994., str. 168 - 176.

<sup>69</sup> Grover D., The protection of computer software - its technology and applications, Cambridge, Cambridge University Press, 1989., str. 166.

<sup>70</sup> Doswell R., A Guide to Computer Crime Investigation, Edicija: A Handbook of Computer Security, London, Kogan Page, 1990., str. 128.

kompleksnost istrage i kompleksnost prava<sup>71</sup>. Posebno je važno da se istraga dobro pripremi, da se sprovede od starne kompetentnih i posebno obučених istražitelja. Kompleksnost istrage ogleda se u brojnosti veza i terminala, a naročito alarmantan postaje problem širenja mreža u koje se, pored organizacija i vladinih institucija, povezuju i pojedinci, te je veoma teško kontrolisati sve korisnike i zainteresovane. Što se, pak, pravne kompleksnosti tiče, ona enormno raste samim specifičnostima i mnoštvom varijanti načina izvršenja ovih kriminoidnih radnji.

**Četvrto, kompjuterski kriminalitet ne zna za granice, prelazi lagano iz jedne države u drugu, sa jednog kontinenta na drugi.** S obzirom na specifičnost radnje i ponašanja koje prouzrokuju ova dela, počinioci i orudja kojima se vrši, više nego i jedan drugi oblik kriminaliteta, kompjuterski nije fizički vezan za jedno mesto, niti za jednu žrtvu. Dovoljno je uleteti u neku internacionalnu mrežu pa da se mogu činiti, nevidljivo i gotovo neuhvatljivo, krađe, prevare, sabotaze i sl. To je npr. bio slučaj sa *Markus H.*, zapadnim Nemcem koji se vešto uvukao u kompjutersku mrežu **LBL** (*Lowrence Bekerly Laboratory*) i tako premostio prostornu razdaljinu između Nemačke i SAD. Ovaj haker, veoma pažljiv, pokušavao je i uspeo da udje u vojne baze podataka. Nakon dužeg vremena bio je otkriven, a tek naknadno se utvrdilo da je u pitanju agent KGB. Sam postupak otkrivanja bio je mukotrpan i dugotrajan i zahtevao je veliko strpljenje i znanje. Naročito pošto je sumnja, u početku, pala na studente iz kampusa Univerziteta u Kaliforniji, pa se istraga kretala u tom pravcu. Tek primenom posebne taktike, koju je sproveo *C. Stoll*, utvrđeno je da se "napad" vodi sa neke veće udaljenosti nego što su granice SAD. Takodje, mesto nastajanja posledice je od ključnog značaja za dela tele - piratstva. Ako je u pitanju delo u pokušaju ili priprema krivičnog dela tada se, pored uobičajenih, kao mesto izvršenja smatra i mesto gde je, po umišljaju potencijalnog počinioca, posledica trebalo da nastane ili je mogla nastati<sup>72</sup>.

Internationalnost predstavlja osobenost i tendenciju ovih dela. Zbog ove karakteristike, međunarodno povezivanje istražnih i drugih tela i organa predstavlja, ne samo potrebu, nego i imperativ<sup>73</sup>. Jedno od mogućih rešenja za prevenciju i kažnjavanje uhvaćenih počinitelja je harmonizacija i unifikacija kaznenog i procesnog prava, tako da pretnja u jednoj znači istu takvu pretnju u drugoj zemlji. Ovo je osobito važno i zbog obezbeđenja internacionalnih mreža podataka.

### 3. Tipična dela kompjuterskog kriminaliteta

<sup>71</sup> Pallmer I. C., Potter G. A., *Computer Security Risk Management*, London, Jessica Kinglley Publishers, 1989., str. 182.

<sup>72</sup> KZ čl. 32. t. 2.

<sup>73</sup> Na to obavezuje i UN Manual, kao i Recommendation No. R (95) 13. Evropske Unije.

Kao što još uvek ne postoji jedinstvenost u tome šta je kompjuterski kriminal, isto tako ne postoji saglasje ni koja dela i ponašanja treba tretirati kao dela u kojima postoji protivpravno, neetičko i neautorizovano ponašanje usmereno ka automatizovanim podacima ili njihovom prenosu. Među autorima koji se sve više bave ovom pojavom uglavnom su se iskristalisale **dve grupe** shvatanja: jedni polaze od opšteg pojma kompjuterskog kriminaliteta i *sva dela koja imaju svojstva osobena ovoj pojavi, pojmu, uključuju u njega*, dok drugi primenjuju metod *enumeracije i nabrajaju dela* koja se pod kompjuterskim kriminalitetom podrazumevaju.

**Prvoj grupi** pripadaju shvatanja npr. C. Edwards, N. Savage, I. Walden<sup>74</sup> koji smatraju da se dela kompjuterskog kriminala mogu podeliti na:

- dela u kojima **kompjuteri imaju "aktivnu" ulogu**, odnosno kriminal vezan za kompjutere;
- dela u kojima se **kompjuteri pojavljuju kao periferni objekt kriminala**.

Slično, mada ipak nešto drugačije, shvatanje ima npr. V. Vodinelić<sup>75</sup> koji dela kompjuterskog kriminaliteta razvrstava po tome da li je u pitanju **kompjuterski kriminalitet u užem ili širem smislu**. Pod kompjuterskim kriminalitetom u užem smislu ovaj autor podrazumeva računarske prevare, špijunaže, sabotaze, dok pod ovim delima u širem smislu podrazumeva i sva ostala dela.

**Drugoј grupi** pripadaju shvatanja npr. U. Sieber-a<sup>76</sup> koji prihvata odredjenje i podelu *Komiteta eksperata OECD* i smatra da se dela kompjuterskog kriminaliteta mogu svrstati u odnosu na posledice (ako je napadnut ekonomski interes, privatnost i sl.) u tri velike grupe:

- ♦ **dela kompjuterskog kriminaliteta vezana za ekonomski kriminal**, kao što su prevara, krađa, kompjuterska špijunaža i sabotaza, neautorizovan pristup sistemima i haking, piratstvo softvera, i sl;
- ♦ **dela kompjuterskog kriminaliteta vezana za kršenje prava privatnosti**, kao što su korišćenje netačnih podataka, ilegalno prikupljanje i čuvanje ličnih podataka, ilegalno otkrivanje i zloupotreba podataka, kršenje formalnosti prava privatnosti, i sl;

<sup>74</sup> Edwards C., Savage N., Walden I., op. cit. str. 142.

<sup>75</sup> Vodinelić V., Metodika otkrivanja, dokazivanja i razjašnjavanja računarskog kriminaliteta, Priručnik, 1990/4., str. 323 - 328.

<sup>76</sup> Sieber U., op. cit., str. 3 - 27.

- ♦ **ugrožavanje ostalih pravno zaštićenih interesa**, kao što je ugrožavanje nacionalne sigurnosti, kontrola prekograničnog toka podataka, integritet procedura vezanih za kompjutere i mreže podataka, i druga dela.

Ovoj grupi pripada i K. Tridemann, koji apstrahujući slučajeve kad se kompjuteri koriste za vršenje običnih krivičnih dela imovinskog karaktera<sup>77</sup>, smatra, manje pregledno i čini se sa obuhvatanjem manjeg obima specifičnih karakteristika ove pojave, da postoje četiri grupe dela kompjuterskog kriminaliteta i to:

- ♦ **manipulacija sa ulazima i izlazima**, kojoj pripadaju dela vezana za unošenje, obradu i davanje lažnih podataka;
- ♦ **industrijska** (kompjuterska) **špijunaža**;
- ♦ slučajevi **kompjuterske sabotaže**; i
- ♦ **kradja kompjuterskog vremena**.

Kao posebnu vrstu ovaj autor naknadno uključuje i dela "**kompjuterske prevare**" u kojima se posebno pojavljuje **zloupotreba šaltera za podizanje gotovog novca**.

Slična polazišta imaju i svi oni autori, pa čak i odgovarajuće **zakonodavne komisije** (npr. Velsa, Engleske, Škotske), koji još detaljnije navode pojedinačne oblike, odnosno krivična dela koja se mogu smatrati kompjuterskim kriminalitetom. Tako su to:

- ♦ **kompjuterska prevara**;
- ♦ **nedozvoljeno korišćenje računarskih podataka**, kao što je haking, kompjutersko prisluškivanje, nedozvoljena upotreba kompjutera za ličnu korist;
- ♦ **nedozvoljena primena ili destrukcija memorisanih podataka**;
- ♦ **odbijanje pristupa ovlašćenom korisniku**; i
- ♦ **nedozvoljeno uklanjanje takvih podataka**.

Isti metod je prihvatio i poseban *Komitet eksperata EU* koji je formulisao svoje shvatanje tipova dela kompjuterskog kriminaliteta u **Preporuci o kriminalitetu vezanom za kompjutere** (*Recommendation No. R.(89)9 on computer-related crime*), a koja je i prihvaćena od Komiteta ministara Saveta Evrope, i po kojoj se državama članicama preporučuje promena postojećeg ili stvaranje novog nacionalnog zakonodavstva vezanog za ovaj kriminalitet. Takođe, predviđa se donošenje posebnih smernica kojima bi se to bliže regulisalo. Naknadno donete Smernice predvidele su

---

<sup>77</sup> Ignjatović Dj., op. cit., str. 139.

listu minimuma koja se mora ugraditi u nacionalna zakonodavstva. Pored liste minimuma ove Smernice su predvidele i opcionu listu koje države članice mogu, ali ne moraju prihvatiti<sup>78</sup>.

**Lista minimuma** obuhvata sledeća dela kriminaliteta vezanog za kompjuter:

1. kompjutersku prevaru;
2. kompjutersko krivotvorenje;
3. kompjutersko oštećenje;
4. kompjutersku sabotažu;
5. neautorizovani pristup;
6. neautorizovano unošenje;
7. neautorizovano reprodukovanje zaštićenog kompjuterskog programa;
8. neautorizovano reprodukovanje zaštićene topografije.

**Opciona lista** obuhvata:

1. promenu kompjuterskih podataka ili kompjuterskih programa;
2. kompjutersku špijunažu;
3. neautorizovano korišćenje kompjutera; i
4. neautorizovano korišćenje zaštićenih kompjuterskih programa i topografije.

**Priručnik za zaštitu i kontrolu kriminaliteta vezanog za kompjuter** (*UN Manual on the prevention and control of computer-related crime*) je bio nešto jednostavniji i predviđa sledeće **osnovne tipove** kompjuterskog kriminaliteta<sup>79</sup>:

1. kompjuterske manipulacije;
2. kompjuterska krivotvorenja;
3. oštećenja na ili sa kompjuterskim podacima ili programima; i
4. pristup kompjuterskom sistemu ili servisima.

Od ovih shvatanja čini se ipak najprihvatljivije ono koje dela kompjuterskog kriminaliteta razvrstava na osnovu "uloge" koju u izvršavanju dela ima kompjuter, odnosno da li se radi o delima u kojima je kompjuter periferni objekt ili orudje ili se

---

<sup>78</sup> Više o tome u UN Manual.

<sup>79</sup> Za svako od ovih dela UN Manual je dao osnovne karakteristike.

kompjuter pojavljuje u "aktivnoj" ulozi. Takvo shvatanje omogućuje, pored uključivanja klasičnih dela kriminala, i ona koja se pojavljuju samo u vezi sa kompjuterima, kao što je haking, piratstvo softvera, stvaranje i ubacivanje virusa, ali ne samo njih, nego i drugih produkata vezanih za informacionu tehnologiju koja u sebi nose sve oblike zloupotreba. Polazeći od odredjenja zloupotreba računara, **dela kompjuterskog kriminaliteta u širem smislu**<sup>80</sup> bi obuhvatala:

1. dela vezana za **ekonomske vrednosti**:
  - 1.1. krivična **dela protiv intelektualne svojine**: neautorizovano modifikovanje, uništavanje, otkrivanje ili uzimanje podataka, programa, ili dokumenata koji su vezani (eksterno ili interno) za kompjuterski sistem, komunikacije i druge objekte intelektualne svojine (piratstvo i kradja programa, dizajna čipova);
  - 1.2. krivična **dela protiv kompjuterske opreme ili podrške**: neautorizovano modifikovanje, korišćenje, ili uništenje kompjuterskog sistema, komunikacionih veza ili druge kompjuterske opreme ili podrške (kompjuterske sabotaze, oštećenja softvera, hardvera);
  - 1.3. krivična **dela protiv korisnika računara**: neautorizovan pristup kompjuteru, kompjuterskom sistemu, komunikacionom sistemu i mrežama, ili uskraćivanje pristupa autorizovanim korisnicima kompjuterskih usluga;
  - 1.4. krivična **dela protiv pružaoca kompjuterskih usluga i vlasnika podataka**: kradja servisa, kradja informacija, kradja novca i sl., kao i kompjuterska špijunaža, kompjuterske prevare, uznemiravanja, iznudjivanja;
2. **povrede privatnosti** pomoću kompjutera:
  - 2.1. **proizvodnjom i korišćenjem netačnih podataka**;
  - 2.2. **nedopuštenim otkrivanjem ili gubljenjem podataka**;
  - 2.3. **nedopuštenim skupljanjem ili čuvanjem podataka**; i
  - 2.4. **povrede formalnosti i prava na informacionu privatnost i pravo privatnosti**.
3. **drugi oblici zloupotreba**:
  - 3.1. **krivična dela protiv države i političkih interesa**;
  - 3.2. **kompjuterski terorizam**.

<sup>80</sup> Parker D., Fighting Computer Crime, New York, Charles Scribner's Sons, 1981, str. 6; Florida Computer Crimes Act u knjizi: Lipner S., Kalman S., op. cit., str. 540 - 542; Sieber U., op. cit., str. 3 - 27.

Kao tipična dela u odnosu na **kompjuterski kriminalitet u užem smislu** (kriminalitet vezan za kompjutere), izvršena, dakle, pomoću i protiv računara pojavljuju se:

1. **pravljenje i ubacivanje kompjuterskih virusa;**
2. **haking;**
3. **piratstvo** (softvera, mikročipova, baza podataka)<sup>81</sup>;
4. **kompjuterska sabotaza;**
5. **kompjuterska špijunaža;**
6. **kompjuterske prevare;** i
7. **kradja kompjuterskih usluga.**

No, kako su od ovih dela najkarakterističnija dva: pravljenje i ubacivanje virusa i haking to će ona i biti prikazana. Pri tom, treba napomenuti da se veoma često ova dva dela međusobno isprepliću i da ih je ponekad gotovo nemoguće odvojiti.

---

<sup>81</sup> Ovo je krivično delo već bliže objašnjeno u odgovarajućim glavama.

### 3.1. *Pravljenje i ubacivanje kompjuterskih virusa*

"Ponoćni pohod na kompjutere - Napad na 23 miliona mikrokompjutera u svetu. - Mladi "hakeri" - savremeni tehnobanditi stvaraju viruse i ubacuju ih u međusobno povezane kompjuterske sisteme, što može da parališe svetsku privredu."

Takav se naslov pojavio u petak 13-og oktobra 1989. godine u "Politici" i imao za cilj da upozori vlasnike računara o pretnji koja je upućena svima i upozorava na "pohod" virusa nazvanog "*data-crime*".

**"Virus je podli mali programski stvor koji čuči u nekom kutku vašeg računara i koristi svaku priliku da napravi neku štetu u sistemu. Da bi se ta štetočina utamanila potrebno je mnogo znanja i živaca"** tako je viruse definisao M. Samociuk<sup>82</sup> pokušavajući da na slikovit način opiše ovaj novi fenomen i upozori da on i nije tako bezazlen, kao što na prvi pogled izgleda. Upravo to potvrđuje i činjenica da je u SAD<sup>83</sup> osnovano posebno udruženje za borbu protiv virusa (*Computer Virus Industry Association*).

#### 3.1.1. *Virusi - kako je počelo?*

Daleka 1949. godina - John von Neumann je sve više zaokupljen idejom o stvaranju samoreprodukujućeg kompjuterskog programa. U članku "Teorija i organizacija komplikovanih automata" koji je te iste godine objavio, izneo je svoju teoriju o kompjuterskim programima koji mogu da se multiplikuju. Kao i većina novih ideja i ova biva ismejana<sup>84</sup>. Međutim, ma koliko neverovatna, ova ideja, ipak, nije bila i nemoguća. To će desetak godina kasnije pokazati 3 mlada programera u *AT&T's Bell* laboratorijama. **Douglas McIlroy**, **Victor Vysotsky** i **Robert Morris** stvaraju igricu nazvanu *Core War*. Ova igra između dva programerska koda trebalo je da skрати i uveseli njihovo radno vreme. Cela igra je zamišljena kao set reproduktivnih programa nazvanih "organizmi". Na početku svaki igrač oslobadja svoj "organizam" u memoriji (memorija je bila core i otud naziv igre). Jedan "organizam" pokušava da uništi protivnički. Igrač sa najvećim organizmom na kraju igre biva proglašen pobednikom.

<sup>82</sup> Samociuk M., *Hacking*, Edicija: The Protection of Computer Software - its technology and applications, Cambridge, Cambridge University Press, The British Computer Society, 1989., str. 152.

<sup>83</sup> Roberts R., *Compute!'s Computer Viruses*, Greensboro, Compute! Books, 1988., str. 2.

<sup>84</sup> Kane P., op. cit., str. 23.

Posle svega, igrači bi obrisali svoje igrarije i odlazili kućama. Iako je bilo za očekivati da će ovaj način korišćenja radnog vremena biti okarakterisan, u najmanju ruku, kao zloupotreba resursa i da će igrači biti kažnjeni, to ipak nije bilo tako. Ne samo da je igranje bilo tolerisano, već ono postepeno biva uključeno u proces učenja. Ubrzo ova igra biva prenet na druga mesta i stiže do *M.I.T. (Massachusetts Institute of Technology)* i u *Xerox Palo Alto Research Center* istraživačkog centra. Kad se igra igrala na posebnim kompjuterima od strane dva igrača opasnosti su bile minimalne. Medjutim, program bi mogao početi da radi nekontrolisano, te je bilo potrebno jednostavno isključiti računar. Ubrzo se radja želja za povezivanjem kompjutera i uključivanjem više igrača. Tada dolazi do umnožavanja igre izmedju nekoliko povezanih mašina i ona poprima ružne odlike. Bez obzira na sve, igra postaje tajna zabava sve većeg broja lica. Tako, tokom 1983. godine do ove dobro čuvane tajne igre dolazi **Ken Thompson**. Thompson je, inače, tvorac *Unix*-a. Kad mu je uručivana jedna od najvećih nagrada u kompjuterskoj industriji, njegov pozdravni govor sadržao je recept za viruse u opisu tačnog koncepta *Core War*-a. U maju 1984. godine časopis *Scientific American* objavljuje članak u kome je opisana ova igra i poziva čitaoce da za svega 2 dolara kupe set instrukcija ove igre, preporučujući da je igraju kod kuće ili na poslu<sup>85</sup>.

Sam termin računarski virus prvi put je upotrebio **David Gerrold** 1972. godine u naučno-fantastičnom romanu "Kad je Hari bio neko"<sup>86</sup>. On je tvorac ideje o programu *Virus*, koji nasumice okreće telefonske brojeve, otkriva jedan računar, uvlači se u sistem i tamo pravi zbrku<sup>87</sup>.

Prvi pravi računarski virusi pojavili su se 1983. godine, mada je prva panika nastala na univerzitetu u Dortmundu 1980. godine otkrivanjem softvera nepoznatog autora. Softver je imao sposobnost "razmnožavanja". Istraživanje je ukazalo da je to bila programska forma koja je nosila upravo najbitnije karakteristike bioloških virusa<sup>88</sup>. Čovek za koga se zna da je medju prvima eksperimentisao sa kompjuterskim virusima

<sup>85</sup> Gotovo u isto vreme kad su se Morris, McIlroy i Vysotsky igrali u *Bell*-ovim laboratorijama na *M.I.T.* se osniva Tehnički klub za modele železnica. Ovaj najpopularniji klub postdiplomaca *M.I.T.*-a bio je jezgro hakera. Njegovi članovi igraju drugu igru - *Space War*. Ona, na samom početku 60-ih, ima grafiku i predstavlja preteču današnjih video igrica. Ovaj će klub biti spona izmedju naučne fantastike i stvarnosti. Naučna fantastika bila je kolevka mnogih ideja i rešenja.

<sup>86</sup> Drugi autori smatraju da je poreklo u romanu **John Brunner**-a *Shockwave Rider*, 1975. godine u kome je predviđao nastajanje kodova virusa i crva. Dve godine kasnije Thomas Rayn, objavljuje *The Adolescence of P-1* u kome daje zastrašujući primer inteligentnog virusa koji prouzrokuje informacionu bolest. O ovome više kod Kane P., op. cit., str. 25.

<sup>87</sup> Spafford E. H., Heaphy K. A., Ferbach D. J., *A Computer Virus Primer*, Edicija: *Computers Under Attack, Intruders, Worms, and Viruses*, New York, ACM Press, 1990., str. 318.

<sup>88</sup> Herweg R., *Bases of Computer Viruses*, Koln, Datakontext - Verlag, 1991., str. 9.

(instaliran na *Unix-u*) bio je **Fred Cohen**<sup>89</sup> sa *Southern California* univerziteta, 1983. godine<sup>90</sup>. Legendaran je postao jedan od prvih programa koji se pojavio prvo na fakultetskom računar u Kaliforniji, a proizvodio je u određeno vreme na ekranima male kvadratiće koji su brisali tekst od gore na dole, red za redom, ostavljajući poruku "*COOKIE, COOKIE, GIVE ME THE COOKIE*"<sup>91</sup>. Ako se reč *COOKIE* ne bi brzo ukucala, sadržaj teksta je bio nepovratno izgubljen. Ukoliko bi reakcija bila brza i reč otkucana, tekst se vraćao.

Januara 1986. godine u svet je krenuo i prvi virus koji je prešao nekoliko granica i uplašio veliku populaciju *IBM PC* korisnika. On se brzo širio od zemlje do zemlje kroz Evropu i prešao u Severnu Ameriku. Krenuo je iz *Brain computer* stor u Lahore, Pakistan, i za manje od 12 meseci "dotakao" je oko 1/2 miliona kompjutera i izazvao pustošenja, doduše manja, na stotinama univerziteta, u korporacijama i vladinim agencijama. Ovaj virus nazvan je *Pakistani Brain*. Bio je to prvi virus koji je izazvao veliku pažnju javnosti.

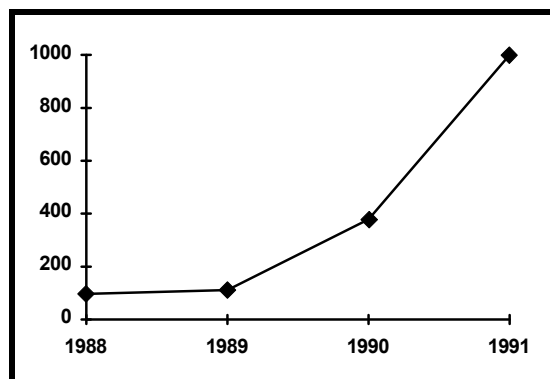
**Većina prvih računarskih virusa, dakle, nastala je na fakultetima.** Pisali su ih profesori i/ili studenti i u početku su imali samo akademski značaj. Sredinom 80-ih viruse sve više pišu hakeri, nalazeći u njihovom stvaranju intelektualni izazov, po mnogo čemu, uzbuđljive oblasti programiranja. U budućnosti će viruse, po svemu sudeći, pisati kriminalci koristeći ih za ostvarenje sopstvenih ciljeva. U doba kada moderna civilizacija sve više zavisi od računara i kada se sve više oslanja na njihovi ispravno funkcionisanje, širenje računarskih virusa treba osuditi i istovremeno preduzimati akcije radi njihovog svodjenja na najmanju moguću meru. Pogotovo što smo svedoci njihovog sve bržeg umnožavanja i sve većih šteta (računa se da su štete, npr., od virusa u V. Britaniji u 1977. godini iznosile nekoliko miliona funti za godinu dana) kojima su oni uzrok. Danas je visina ovih šteta ogromna. I ne samo da je to ogromno, nego i broj tipova virusa gotovo da svakodnevno raste. Primera radi tendencija rasta u periodu od 1988 - 1991. godine kretala se od 97 (1988.), pa 112 (1989.), 379 verzija (1990.), oko 1000 (1991.), što se može videti iz sledećeg grafika:

#### Razvoj vrsta virusa

<sup>89</sup> Inače, Fred Cohen sa ovim programima eksperimentisao je kao postdiplomac u okviru seminara iz sigurnosti. Ideja o pisanju kompjuterskog virusa ga je toliko zarazila da je za nedelju dana demonstrirao prost primer virusa. Njegov savetnik prof Len Adelman savetovao ga je da ovu tvorevinu nazove kompjuterskim virusom. Cohen je to usvojio, i nekoliko godina kasnije čak doktorirao. Njegov članak "Kompjuterski virusi - teorija i eksperimenti", objavljen 1987. godine u časopisu *Computer & Security* izazvao je strah kod mnogih, jer je prvi prikazao njihove karakteristike.

<sup>90</sup> Spafford E. H., Heaphy K. A., Ferbach D. J., op. cit., str. 318.

<sup>91</sup> Poznate su i varijante poruke "POLLY WANTS' A CRACKER" ili "COOKIE MONSTER IS HERE". Poruka odgovor je u sva tri slučaja ista.



Tako se danas može govoriti o nekoliko stotina raznovrsnih virusa (oko 500 osnovnih), od kojih mnogi imaju i razne varijante (preko 1000 varijanti).

Koliko će ih tek biti večeras?

### 3.1.2. Pojam kompjuterskog virusa

Virus je, u stvari, program koji ima mnogo sličnosti sa pravim virusom. Naime, najčešći način rada virusa je vezan za disketu na kojoj je "smešten". Kad virus bude sa diskete pročitao, on se elegantno i tajnovito premešta u memoriju i onda pažljivo "motri" na sve uređaje za smeštanje podataka koji su na njega priključeni i, npr., svaki put kad se stavi nova disketa proverava da li se njegova kopija nalazi i na njoj. Ako se ne nalazi, virus se premesti i tako u pravom smislu te reči, zarazi sve dostupne diskete. No, to nije sve: danas je na gotovo svakom PC-u ugrađen i hard disk, pa su virusi koji se smeste na hard disk posebno opasni, jer odjednom mogu uništiti veoma veliku količinu podataka. Tako, npr. kad se u oktobru 1988. godine **Robert Morris** junior, inače diplomac na *Cornell* univerzitetu, poigrao sa *APERNET* mrežom, nedelju dana je 6.000 kompjutera bilo onesposobljeno usled ogromnog zagušenja velikim brojem programa koji su izgledali kao komandni interpreti (*shell utilities*). Mnogi od ovih računara morali su biti zaustavljeni kako bi se očistili. Šteta je procenjena na preko 1 milion dolara<sup>92</sup>. Ni to nije sve: ukoliko je računar povezan u

<sup>92</sup> Eisenberg T., Gries D., Hartmanis J., Holcimb D., M. Stuart Lynn, T. Santaro, The Cornell Commission: On Morris and Worm, Edicija: Computers Under Attack, Intruders, Worms, and Viruses, New York, ACM Press, 1990., str. 253 - 260.

mrežu - virus se širi dalje i može zaraziti na desetine (stotina, hiljada ili čak miliona) računara<sup>93</sup>.

Virusi mogu napraviti štetu ne samo na podacima, već mogu i ozbiljno oštetiti kompjutere. Oni se, otuda, mogu pojaviti i kao orudje za kompjutersku sabotažu, jer mogu biti kreirani radi uništenja. Poznati su slučajevi da je usled konstrukcijske greške na računaru *Commodore 128*, postojao način da se pomoću tri instrukcije doslovno spali računar, ili da se na računaru *IBM PC* opremljenom sa hard diskom, na kome se nalazi smeštan veliki broj podataka i ne retko kompletni projekti i sl., napravi *HEAD CRASH*, spuštanjem na površinu diska magnetne glave za upis i čitanje za vreme dok se disk okreće. Jasno je da iz toga proizilazi šteta od najmanje \$ 600, a da i se ne pominju uništeni podaci i programi, pa ukupna šteta može iznositi i do nekoliko stotina hiljada dolara.

Šta se pod kompjuterskim virusom, u suštini, podrazumeva?

Pod terminom kompjuterski virus najčešće se podrazumeva šira grupa programa koja obuhvata svaki program koji izvršava neke namerne, nedokumentovane akcije bez znanja i na štetu svog korisnika<sup>94</sup>.

Veoma slično virusne programe definisao je i Cohen<sup>95</sup> podrazumevajući pod njima *svaki onaj program koji je u stanju da "zarazi" druge programe modifikujući ih, uključujući i mogućnost pravljenja sopstvene kopije.*

Drugim rečima, **kompjuterski virusi** (*computer viruses*) **su poseban tip računarskih programa koji mogu sami sebe reprodukovati i/ili klonirati, koji se šire, i to tajno, sa ciljem da inficiraju druge programe kako bi oni izvršavali ciljeve koje je unapred postavio tvorac virusa, a da pri tome inficirani programi ne izgledaju tako.** Iz ovih odredjenja jasno je da je u pitanju:

1. program koji je u stanju da **sam sebe reprodukuje ili klonira**<sup>96</sup>;
2. program koji **sebe kopira** u druge programe;
3. program koji se **širi tajno**, iako su mu posledice vidljive - javne;

<sup>93</sup> Stojković G., Drakulić M., op. cit., str. 4.

<sup>94</sup> Word G. H., Shriver R. F., op. cit. str. 27.

<sup>95</sup> Cohen F., op. cit., str. 22 - 35.

<sup>96</sup> Upravo su tako i definisani **kompjuterski virusi - kao programi koji imaju sposobnost da sebe reprodukuju ili kloniraju** - Haynes C., *The Computer Virus Protection Handbook*, San Francisco, Sybex, 1990., str. 28.

4. program čiji je **cilj izmena drugih programa** kako je to zamislio njegov tvorac;
5. da **inficirani programi**, na prvi pogled, **ne izgledaju drugačije** od normalnog;
6. program koji obuhvata neke **namerne nedokumentovane akcije** bez znanja svog korisnika;
7. program koji **najčešće pravi štete** izvršavajući upravo tu funkciju; i
8. **komputer radi sa ovim programom kao i sa bilo kojim drugim** - izvodi ih.

Dakle, virusni programi su opasnost koja se širi, sve su lakši za pravljenje i sve teži za bezbolno otklanjanje.

### 3.1.3. Tipovi i vrste kompjuterskih virusa

Virusa ima raznih, zavisno od načina kako "zaražavaju" programe i računare. Najčešće se<sup>97</sup> navode sledeći **tipovi virusolikih programa** kojima je **zajedničko to da izvršavaju nedokumentovane radnje** pri čemu najčešće uništavaju sve podatke koji su im dostupni iz računara na kojima se izvršavaju:

1. **bakterije** (*bacterium*) je program koji se pri izvršavanju širi ka drugim korisnicima i sistemima slanjem sopstvenih kopija, a hrani se jedući procesor i memorijske kapacitete svog domaćina.
2. **bombe - logičke** (logic bombs) i **vremenske** (*time bombs*) su programi koji se aktiviraju pri ispunjavanju ranije definisanih uslova. Oni su naročito opasni, jer sve do određenog događaja ostaju pritajeni u memoriji računara. Korisnik softvera u kome je implementirana ova vrsta programa, praveći sopstvene sigurnosne kopije, nesvesno zaražava druge diskete;
3. **crvi** (*worms*) su u početku bili pisani od strane sistem-programera radi povećanja stepena iskorišćenja računarskog sistema (npr. putovali su od jedne do druge stanice i isključivali "nezaposlenu"). Vremenom su ovi programi počeli da se zloupotrebljavaju radi kradje procesorskog vremena i potpunog blokiranja sistema. Sada su to programi koji se izvršavaju nezavisno od korisnika, širenjem kopirajući sami sebe na računarima. Veoma često su to programi "putnici" koji putuju od mašine do mašine i

<sup>97</sup> Word G. H., Shriver R. F., op. cit. str. 24 - 26; White S. R., Chese D. M., Kuo C. J., Copin with Computer Viruses and Related Problems, Research Report online version on CHES@IBM.COM, 1989., str. 24 i 25; Palmer I. C., Potter G. A., op. cit., str.5 - 20.

moгу, čak, pojedine delove imati na različitim mašinama. Ovi su programi orjentisani na putovanje u mrežama. Najčešće ne menjaju programe - domaćine. Kao termin pojavili su se u naučno - fantastičnoj literaturi kod **John Brunner**-a u priči *The Stockwave Rider* (1975.)<sup>98</sup>. U vezi sa računarima njihova pojava datira od početka 80-ih kada je prvi program crv implementiran u mrežu *Alto* na radnoj stanici u *Xerox Palo Alto Research Center*. Celih šest godina je trebalo da prodje da bi se ostvarila "crna slutnja" - šta će se desiti ako se ovakav program otrgne od kontrole i počne da se multiplicira u mreži? To se i desilo sa R. Morrisom, kome su se, navodno, programi - crvi, sa kojima je eksperimentisao, otrgli;

4. **trapdoor** ili **back door** je deo programskog koda čijim korišćenjem onaj ko radi na računaru može doći do operativnog sistema (**OS**). Tamo korisnik može (zavisno od gradje OS) formirati novi program ili koristiti programske naredbe ili ih prepraviti u svoju korist. Mnoge savremene OS-i rade grupe stručnjaka, tako da je mogućnost provale u OS smanjena, ali oni moraju ostaviti sebi alternativu da u OS vrše određene izmene i dopune, uz zahteve posednika OS. Za to im služi program trapdoor;
5. **trojanski konji** (*Trojan horses*) je program koji se trudi da preko privilegovanog korisnika uspostavi kontrolu nad operativnim sistemom. Prva ozbiljna rasprava o ovoj vrsti virusa bila je 60-ih godina u SAD-u. Naime, Trojanski konj je program koji sadrži skriveni, kamuflirani kod za izvođenje neke neželjene, zločudne, radnje. To je bio, npr., program sa porukom "Znam da ćeš mi dati ono što ja kažem da hoću, ali ono što kažem da hoću nije ono što hoću". Ovom porukom se od korisnika uporno i dosadno zahtevaju određene naredbe i ukoliko se one otkucaju on se povuče "zadovoljan", a ukoliko korisnik ne ispuni zahtev pojavljuju se sve češće poruke da će program biti izbrisan, pa se u jednom trenutku to i desi. Posebna vrsta su **satirični programi** (*spoofing programs*) koji izgledaju kao postupak logan. Kad napiše ovaj program autor ostavlja uključen računar, i namerno bez kontrole, tako da se neutralni korisnik uključuje u rad na uobičajen način - navodjenjem lozinke. Ne dobija ulaz već mu se pojavljuje poruka da nije u redu. Misleći da je u pitanju pogrešno otkucana lozinka korisnik ponovo unosi svoju lozinku, mada je već prvi put korisnik je uspostavio kontakt sa lažnom procedurom čija je osnovna namena - dolaženje do originalne lozinke<sup>99</sup>;
6. **virusi** (*viruses*) su programi koji imaju dve komponente: jednu, kojom kontrolišu širenje, i drugu, koja je manipulativna. Ukoliko je

<sup>98</sup> Stoch J. F., Hupp J. A., *The Worm Programs - Early Experience with a Distributed Computation*, edicija *Computers Under Attack, Intruders, Worms, and Viruses*, New York, ACM Press, 1990., str. 264 i 265.

<sup>99</sup> Vodinić V., op. cit., str. 332.

manipulativna komponenta izostavljena tada su, po pravilu, u pitanju "dobročudni" virusi; i

7. **zec** (*rabbit*) je program dizajniran da isprazni resurse sistema (CPU vremena, prostor diska, i sl.) premeštajući se po njima bez ikakvog ograničenja. Razlikuje se od bakterija po tome što je posebno dizajniran za iscrpljivanje resursa, a od virusa što u sebi sadrži kompletan program i ne treba da "inficira" druge programe. Prvi ovakav program nastao je 1974. godine u jednoj radnji u kojoj su bila povezana 3 kompjutera *IBM 360*. Napravilo ga je nekoliko pametnih mladih programera i kad je bio ubačen u ove računare imao je "očaravajuću" sposobnost da se umnoži i dva puta "baci" u *ASP* ulazni niz instrukcija koje se redosledom izvršavaju. Program je tako funkcionisao da, što je sistem više radio, bilo ga je teže isključiti. Naravno da su programeri bili otpušteni, ali je ovaj tip programa ušao u grupu virusolikih<sup>100</sup>.

Detaljnija podela<sup>101</sup> je ona po kojoj se **virusi mogu klasifikovati**:

1. prema načinu prenošenja: **boot** i **file** viruse;
2. po kategoriji programa koje napada: **sistemski**, **pojedinačni** i **ostali**;
3. po načinu razmnožavanja: **direktni** i **indirektni**;
4. prema delovanju: **maligni** i **benigni**;
5. po načinu instalacije: **rezidentni** i **nerezidentni**;
6. po načinu aktiviranja: **vremenski**, **slučajni**, **kvantitativni** i **ostali**;
7. po načinu aktiviranja: **prepisujući**, **neprepisujući**, **mutanti** i **skladišni**;
8. po mestu skladištenja: **virusi boot sektora**, **virusi glavne memorije**, **virusi korisničkih softvera**, i **posebno skriveni virusi**.

Što se pojedinačnih virusnih programa tiče njih je izuzetno mnogo. Pri tom, su najčešći: *Lehigh*, *Brain*, *Jerusalem*, *Švajcarski amiga*, *Božićna čestitka*, *Macmag*, *Score*, *IDen Zuk*, *AIDS*, *Datacrime*, *Evolucioni*, *Simulacioni*, *Bugarski* i drugi virusi. Godine 1994. pojavili su se i *Jumper*, *Junkie*, *SMEG* i *J&M* u Evropi, a *Bunny* sa tri verzije u Južnoj Africi<sup>102</sup>. 1995. godina bila je godina virusa *Windword.concept*, *Rainbow*, "*prank macro*" (širio se SAD-om, Kanadom, V. Britanijom, Francuskom, Nemačkom i Finskom, inficirajući data file-ove, a radeći na Mac, PCs Word for Windows 6, Word for Windows NT, Word for Windows 95, Word for OS.2. S&S)<sup>103</sup>, *Gringrich*, *Clipper*, *Clington*, *Lecture*, *SPA*, kao i nekih misterioznih kao npr. virus

<sup>100</sup> Kane P., op. it. str. 26. i 27.

<sup>101</sup> Kazić E., Virus, Računari, br.59/90.

<sup>102</sup> F - PROT Professional, Update Bulletin, Data Fellows, Finland, 1994.

<sup>103</sup> Abstracts of Recent Articles and Literature, Computer & Security. 14 (1995), str. 412.

koji je napao kompjuterske sisteme banaka, finansijskih institucija, investicionih posrednika i računovodstvenih firmi Kanade na dan isplata (*budget day*), uništio FATs (*file allocation tables*), jer je našao put do master diska. Većina od njih predviđena je za PC, koji su sve više osetljivi na napade. Rizik od zaraze je sve veći, a **najčešći izvori** (po jednom statističkom istraživanju magazina CHIP) su: **javni softver** (33%), **razmena programa** (13%), **igre** (11%), **nepoznati razlozi** (33%) i **ostalo** (10%).

Počinioci su posebna vrsta ljudi koji, kreirajući i distribuirajući ove maliciozne programe, a to čine: zlonamerni namerni "igrači" ili ne-zlonamerni slučajni "igrači". Svaki od njih ima sopstvenu motivaciju i sopstveni izbor metoda i načina na koji će svoju umotvorinu distribuirati i uputiti u pobedonosno putešestvije<sup>104</sup>. Najčešće je to "on" pošto nema nikakvog dokaza da su i žene uključene u krug tvoraca virusa ili njihovih distributera. Tvorci virusa regrutuju se iz svih krugova, od akademskih do kriminalnih. Oni imaju svoju posebnu subkulturu koja, kao osnovni moto, nosi parazitsko destruktivno ponašanje i težnju za stvaranjem panike usled zaraze koja se širi. Međutim, nikako ne treba zanemariti ni činjenicu da su mnoge viruse stvorili sami proizvođači softvera ne bi li svoje proizvode zaštitili od piratstva. U prilog tome je i sumnja da je *Microsoft* virusima zaštitio svoj *Windows '95*. Ono što nije pod sumnjom - u pitanju su izuzetno vešti i dobri informatičari.

No, bez obzira na vrstu i motivaciju tvoraca, da bi virusni program radio, neophodno je da stigne da se useli na izvršni kod i da se izvrši pre programa - domaćina. On to može uraditi tako što će napraviti **školjku** oko originalnog programa (*shell viruses*) i držati ga zatvorenog dok god ne uradi željenu operaciju. Takodje, može se desiti da se virus program "**zalepi**" za kraj originalnog koda i da se potom prebaci na početak menjajući podatke o startu i izvršavajući svoje operacije pre programa - domaćina (**add-on viruses**). Isto tako se može pojaviti kao program koji **zamenjuje** originalne delove i ceo originalni kod programa - domaćina (*intrusive viruses*).

Zavisno od komponenti koje sadrže, virusi imaju **tri faze** u svom radu: **1) aktivacija** - da bi se širili moraju biti aktivirani; **2) replikaciju** - šireći se inficiraju i programe - domaćine; i **3) manipulaciju** - na određeni način manipulišu sa sistemom. Kad će početi funkcionisanje virusa zavisi od načina na koji je smišljen njegov start. To može biti određen datum (npr. petak 13.), postojanje određenih file-ova, pojavljivanje određenog sadržaja na ekranu, kombinacijom ovih i drugih raznih načina.

<sup>104</sup> Gordon S., Technologically Enabled Crime: Shifting Paradigms for the Year 2000, Computer & Security, 14 (1995) 392 i 393.

Ono što je sigurno karakteristično za viruse je skoro svakodnevno povećavanje njihovog broja i sve teže se od njih se zaštititi. Pri tom, zaštita treba da se sastoji iz tri dela: **prevencije, lečenja i kažnjavanja**. Prevencija i lečenje ulaze u domenu tehničkih i organizacionih mera, dok je kažnjavanje tvoraca, ma koliko virus bio dobroćudan, bezazlen, u domenu prava.

### 3.2. *Haking*

Juna 1989. godine korporacija *Apple Computer Inc.* u Kaliforniji sreće se sa velikim problemom. Neko je ilegalno kopirao deo *Color Quick Draw* softvera koji kontroliše interni čip *Macintosh*-og displeja. Aktivnost koja nije naročito neuobičajena, ali je neobično bilo da je izvorni kod tog dela softvera umnožen i na disketama razaslat širom Amerike svim *Apple*-im poslovnim partnerima. Inače, ovaj izvorni kod bio je dobro čuvana poslovna tajna dostupna samo zaposlenima od poverenja.

Pozvan je FBI jer je sumnja pala na mnogobrojne programere koji su učestvovali u razvoju ovoga, ali i ostalih *Apple*-ovih softvera, a koji su iz bilo kog razloga napustili firmu. Opsežna istraga je dovela FBI do grupe "*Nu Prometheus*". U stvari, bila je to osoba ili više njih čiji su "nestašluci" prelazili vrlo tanku nit između kriminalaca i "spasilaca". Pitanje je bilo ko su oni i zašto su to činili? To se nikad nije saznalo jer FBI nije objavio rezultate istrage, mada su među informatičarima kružile glasine da su krivci bili otkriveni.

Petnaestog januara 1990. godine na Dan Martina Lutera Kinga, 60.000 ljudi gubi kompletne telefonske veze padom *AT&T* telefonskog sistema. Pad je počeo u maloj stanici na Menhetnu i širio se čitavim SAD-om. Polovina ukupne *AT&T* mreže biva zahvaćena. Prekid traje beskrajskih 9 sati. Svi softverski stručnjaci ove firme ubrzano rade na otkrivanju uzroka ne bi li otklonili posledice. Iako sličan bilo kom drugom padu, čak i fizičkom oštećenju sistema, to ipak nije bilo "to". Bio je to upad hakera i krah koji je izazvan ozbiljno je ugrozio *Bell Octopus*, čiji je *AT&T* deo.

Januara 1995. godine časopis *Communication of the ACM* pod naslovom "hakerska pljačka", objavljuje da su hakeri uleteli u *British computer system* i ukrali brojeve privatnih telefona Kraljice i Premijera sa kojih su oni komunicirali sa višim oficirima. Upadom u ovaj sistem i veze hakeri su saznali o tajnim komunikacionim stanicama SAD-a. Pristup je bio preko baze podataka *British Telecom*-a. Poruku o napadu je primio novinar *Independent*-a preko Interneta. Zanimljivo je da je dva meseca pre toga (tačnije, 24. novembra) član Britanskog Parlamenta Robert Ainsworth u

Parlamentu postavio pitanje - šta je preduzeto povodom hakinga kojim su bile ugrožene poverljive informacije u *British Telecom*-u<sup>105</sup>? Dakle, radilo se o istom delu upada, a i o ozbiljnosti ovakve pretnje u odnosu na poverljive podatke.

### 3.2.1. *Haking - kako je počelo?*

Hakeri se pojavljuju ranih 60-ih<sup>106</sup> kada se ovaj termin prevashodno koristi u pozitivnom smislu za "grupu mladih pionira, kompjuterskih zaljubljenika" na M.I.T.<sup>107</sup>. Dakle, bili su to kompjuterski entuzijasti koji su formirali klubove, međusobno razmenjivali vesti i stvarali posebne časopise, grupno prisustvovali i pratili gotovo sve sajmove računara i slične manifestacije i prezentacije, i, čak, imali svoju sopstvenu konvenciju o osnovnim pravilima ponašanja<sup>108</sup>.

Početkom 70-ih hackeri i dalje bivaju okupirani razumevanjem i savladavanjem kompjuterskih sistema, te ne čudi što su upravo oni bili i prvi koji su shvatili mogućnosti PC-a<sup>109</sup>. Istovremeno, tih godina radjaju se i prvi hackeri u modernom smislu iz hipi anarhističkog pokreta poznatog kao **Yippies** (*Youth International Party*). Bili su to **Abie Hoffman** i **Jerry Rubin** koji, vodeći sopstvenu bitku i rat, sistematskom krađom telefonskih usluga protestuju protiv Vijetnamskog rata<sup>110</sup>, a 1971. godine ova dvojica frekera pokreću *YIPL/TAP* magazine.

Medjutim, početak 80-ih doneo je i veliki publicitet hakerima hapšenjem "hakerske bande" poznate kao **Banda 414** (*414 Gang*) sastavljene od "pametnih klinaca", starih između 15 i 22 godine, koji su upadali u kompjuterske sisteme. Naime, 12 tinejdžera je upalo u više od 60 korporacijskih i vladinih kompjuterskih instalacija uključujući i *Los Alamos National Laboratories*, *Security Pacific Bank*, *Pepsi-Cola*, *Canadian cement company* i vršljalo kroz *Telenet national communication network* i 8 puta ilegalno ulazilo u kompjuterski sistem, svetski poznatog, *Sloan-Kettering* centara za rak, iz Nju Jorka, u kome je bilo smešteno 6.000 terapijskih zapisa tadašnjih i bivših

<sup>105</sup> CD - ROM: Parliament CD - ROM, Database: Parliament - 1994/95 Session.

<sup>106</sup> U suštini smatra se da su frekeri bili mladi telegrafisti koje je zbog "nestašluka" otpustila *Bell Company* 1878. godine, o čemu više kod: Sterling B., *The Hackers Crashdown: Law and Disorder on the Electronic Frontier*, electronic book, 1994.

<sup>107</sup> Roberts R., Kane P., *Compute!'s Computer Security*, Greensboro, Compute! Books, 1989., str. 16 - 18.

<sup>108</sup> Roberts R., Kane P., op. cit., str. 16 - 18.

<sup>109</sup> Kane P., op. cit., str. 75 - 83.

<sup>110</sup> Više o tome kod Sterling B., op. cit.

pacijenata, ukupno ga koristeći oko 10 sati. Doduše, većina ovih sistema nije imala adekvatno obezbeđenje, a za upade su najčešće korišćeni telefoni i PC koji su bili programirani za automatsko biranje brojeva (otuda se članovi ove grupe pre mogu smatrati za frekere, nego za hakere). Štampa je, saznajući za to, počela sistematsko korišćenje ovog termina u negativnoj konotaciji, što će imati dalekosežne posledice<sup>111</sup>. Pojam hakera evoluirao u negativnom smislu i upotrebljava se za označavanje "bezkrupuloznih mladih ljudi" koji koriste kompjuterske mogućnosti za upade u sisteme, krađu informacija, kompjuterskih i telekomunikacionih resursa i remećenje rada bez dozvole njihovih vlasnika i/ili korisnika<sup>112</sup>. Drugim rečima, oni se smatraju "elektronskim kriminalcima", pa, čak, i "elektronskim vandalima".

Tih 80-ih, tačnije 1984. godine, održava se prva hakerska konferencija, koja je počela kao *Kalifornijski susret digitalnih pionira i entuzijasta*. Hakeri koji učestvuju na toj konferenciji nisu imali ničeg zajedničkog sa današnjim digitalnim podzemljem. Drugi susret se odigrao 1990. godine u San Francisku na kome S. Brand, J. Lanie, C. Blanchard, I. N. Goldhaber formiraju **EFF** (*The Electronic Frontier Foundation*) čiji predsednik postaje A. Kapor (inače, predsednik Lotusa). EFF-u se priključuje **Well** (*The Whole earth 'etronic link*) bilten, nastao 1985. godine, koji kasnije postaje stožer uprave digitalnog podzemlja. Pored ovog biltena postoje i drugi hakerski časopisi npr. **2600** (osnovan 1984.), **Phrack** (1985 - 1989.) ili **Whole Earth Software Catalog**. Zanimljivo je da su te godine - godine nastajanja mnogih čuvenih hakerskih grupa. Tako, 1984. godine nastaje **Legija strašnog suda** (**Legion of Doom**). Potom slede i druge, manje ili više opasne, grupe<sup>113</sup>.

Za hakere u 80-im karakteristično je<sup>114</sup>:

- provale, krađe, neovlašćeni pristupi bivaju sve **raznovrsniji i složeniji**;
- **formiranje hakerskih grupa**;
- pojava sve različitijih mišljenja o hakerskim delima i aktivnostima (sve je manje divljenja, sve je više zabrinutosti i straha);
- **evidentan je problem oko odredjivanja pojma i sadržaja** hakerskih aktivnosti;
- **narastaju problemi** sa detekcijom, istragom, hapšenjem, dokaznim materijalima;

<sup>111</sup> Lobel J., *Foiling the System Breakers*, Computer Security and Access Control, New York, McGraw - Hill Book Company, 1986., str. 1.

<sup>112</sup> Denning D., *The United States v. Craig Neidorf*, Communications of ACM, vol. 34., No. 3/91., str. 24 - 32.

<sup>113</sup> Sterling B., op. cit.

<sup>114</sup> Zlatković T., *Haking kao kompjuterski kriminal*, diplomski rad, Beograd, FON, 1996., str. 14 i 15.

- **donošenje prvih zakona** kojima se reguliše ova pojava;
- **veoma brz razvoj novih tipova i dela hakinga**; i
- **sve ubrzaniji razvoj sistema sigurnosti i zaštite**, kao odgovor.

Upadi, vremenom, bivaju sve senzacionalniji i sve više utvrđuju stav o negativnosti hakinga i opasnom ponašanju hakera. Tako, *Captain Midnight*, *Wily Hacker*, *Markus H.'s*<sup>115</sup>, *HRH Hacker*<sup>116</sup>, i mnogi drugi, postaju u svetu kompjutera toliko poznati da su pomutili slavu mnogih softverskih tvoraca<sup>117</sup>.

U 90-im karakteristično je:

- upadi hakera u sisteme postaju sve **više dela organizovanog kriminala, ekonomskog i političkog terorizma**;
- **hakerska subkultura biva ugrožena ekonomskim i političkim pritiscima**, jer se države počinju ozbiljno boriti protiv njih;
- **haking definitivno dobija svoju kriminalnu dimenziju**;
- **sve je učestalije donošenje novih propisa** koji se odnose na aktivnosti hakera;
- **internacionalizuje se i harmonizuje saradnja** na praćenju, otkrivanju, krivičnom gonjenju i kažnjavanju hakera.

Dakle, pozitivni predznak se sasvim povlači. Hakeri se transformišu u one koji računar upotrebljavaju za ilegalne, neovlašćene ili "probijajuće" aktivnosti i ponašanja. No, bez obzira što su im aktivnosti promenile prirodu, oni su i dalje ostali jedna od najkompaktnijih grupa "informatičara". Istovremeno su i posebna grupa kompjuterske mafije koja, čineći kriminal "belih kragi", biva često u fokusu interesovanja. I pored spektakularnih upada u razne, a naročito posebno dobro čuvane, informacione sisteme, koji dovode do širenja njihove slave, tihi neovlašćeni, nasilni, ulasci u sisteme sa podacima koji pripadaju domenu privatnosti ili poverljivosti dovode do njihove sve žešće osude. U rasponu između pouzdanosti i privatnosti, neautorizovani "pogled" u sistem deluje sasvim bez opravdanja.

### 3.2.2. Pojam hakinga

<sup>115</sup> Denning P., *Computers Under Attack, Intruders, Worms, and Viruses*, New York, ACM Press, 1990., str. 143 - 185.

<sup>116</sup> Cornwall H., op. cit., str. 324.

<sup>117</sup> Drakulić M., Drakulić R., *Hakerska etika u kontekstu profesionalne etike informatičara*, II naučni skup Tehnologija, kultura i razvoj, Herceg Novi, 1995.

Kao pojava, haking je postao stvarni problem tek u poslednjih desetak godina, ali se razvija i raste veoma brzo. Mišljenja o hakingu su veoma različita<sup>118</sup>. Tako, npr., **jedno** od njih je polazi od toga da je haking proces u kome neka osoba (haker) sprovodi nelegalan upad u kompjuterski ili komunikacioni sistem i tamo čita podatke, ostavlja poruke, startuje programe, briše ili ispravlja programe i informacije<sup>119</sup>, a po **drugom**, haking je takav pristup kompjuterskom ili komunikacionom sistemu za koji ne postoji dozvola njegovog vlasnika<sup>120</sup>.

U suštini, termin hacker u **originalnom značenju** označava svakoga ko je veoma zainteresovan da nauči sve o kompjuterskim sistemima i njihovom korišćenju na novi i "pametn" način, te mnogi kompjuterski entuzijasti sebe zovu hakerima u, ovom, nepežorativnom značenju<sup>121</sup>. Međutim, hakeri su i pojedinci ili grupe koje probijaju zaštitu okruženja kompjuterskog sistema, specijalnog on-line servisa, čineći to iz malicioznosti ili netrpeljivosti, ali često i iz političkih razloga<sup>122</sup>. Hacker isto tako označava i svakog programera koji eksploatiše, proverava ili dovodi kompjuterske i komunikacione sisteme do kranjih granica, bez obzira na posledice. Pokatkad to može dovesti i do uništenja ili sabotaze vrednih podataka, kao i velikih šteta<sup>123</sup>. Vrlo slično je i odredjenje da je to neautorizovani pristup sistemu ili bazi podataka od strane neautorizovane osobe<sup>124</sup>.

**Haking je neautorizovani, nasilni pristup, odnosno pokušaj pristupa sistemu (kompjuterskom, komunikacionom), a hacker je osoba koja ima znanje,**

<sup>118</sup> Uglavnom su se pri definisanju iskristalisala dva polazišta: **jedno**, za koje je ključni pojam haking, i **drugo**, koje se bazira na određivanju pojma hakera, pa na osnovu toga i aktivnosti kojima se bave. Iako na prvi pogled različita ova polazišta imaju isti rezultat: dolaze do odredjenja pojmova haking i hacker. Pri samom određivanju sadržine ovih pojmova jedna se grupa autora orijentiše ka opštem odredjenju ne upuštajući se u posledice, niti u motivaciju, dok kod drugih se pokušava dati, manje ili više, iscrpna lista objekata napada i motiva koji do njih dovode

<sup>119</sup> Samociuk M., op. cit., str. 151., definiše **haking** kao *neovlašćeni pristup kompjuterskim ili komunikacionim sistemima, posle koga osoba pretražuje sistem, ostavlja poruke, startuje programe, briše, modifikuje ili krade programe i informacije*.

<sup>120</sup> Bainbridge D., Computers and the Law, London, Pitman Publishing, 1990., str. 138.; Sterling B., op. cit., navodi da je za američku policiju haking svaki napad izvršen sa, preko, kroz ili protiv kompjutera.

<sup>121</sup> Denning D., op. cit., str. 25.

<sup>122</sup> Peckitt R., Computers In General Practice, Wilmslow, Sigma Press, 1989., str. 136.

<sup>123</sup> Grupa autora, Organizing for Computer Crime: Investigation and Prosecuting, National Institute of Justice USA, 1990., str. 7 i 8.

<sup>124</sup> Peckitt R., op. cit., str. 136.

*sposobnosti i želje da u potpunosti neovlašćeno koristi tuđe kompjuterske i komunikacione sisteme*<sup>125</sup>.

Iz ovog odredjenja, a i prirode ove aktivnosti proističu sledeće **karakteristike**:

1. to je **neautorizovani i brižljivo planirani pristup** (sve redje su posledica slučajnosti ili lutanja, kao što je to bilo u početku);
2. to je **nasilan pristup**, što znači da je u pitanju probijanje zaštite sistema;
3. taj pristup se realizuje kroz **upad u sistem**, pri čemu se termin “upad” koristi za označavanje raznih metoda i tehnika **provaljivanja**<sup>126</sup>;
4. upadi u sistem baziraju se na **visokom profesionalnom znanju**;
5. činjenjem samog hakinga, haker, po pravilu, **istovremeno čini i druga dela**: špijunaže<sup>127</sup>, prevare, kradje usluga<sup>128</sup>, sabotaze, ubacivanje virusa, manipulacije i zloupotrebe sistema (komunikacijskog i kompjuterskog), pronevere;
6. haking može činiti **jedna osoba ili grupa**, pri čemu je sve učestalija pojava organizovanog hakinga od strane veoma velikih grupa hakera;
7. **mesto provale**, po pravilu, **je udaljeno** od mesta gde se sam haker nalazi;
8. kad se jednom nadje u sistemu haker se **ponaša kao autorizovani korisnik**;
9. **orudje** su mu posebni programi (npr. traganje za lozinkama), **objekt** su sistemi i njihov sadržaj, a **posledice** raznovrsne;
10. **motivacija je specifična i raznovrsna** (od pomoći onima koji su u nevolji do terorizma); i
11. mnogi slučajevi hakinga imaju **široke razmere i internacionalizuju** se zbog lakog prevazilaženja lokalnih, gradskih, državnih i međukontinentalnih prostora.

<sup>125</sup> Dorothy Denning je **hakera definisala kao osobu koja provaljuje u sisteme i koristi resurse bez naknade**. O tome više Denning D., A Dialog on Hacking and Security, Edicija: Computers Under Attack, Intruders, Worms, and Viruses, New York, ACM Press, 1990., str. 421 - 439.

<sup>126</sup> Termin **provala** u pravu **vezan je za teške kradje**.

<sup>127</sup> Veoma veliki broj hakerskih upada imaju za krajnje odredište vladine i vojne baze širom sveta, a naročito su pod udarom SAD, Japan, Francuska, Nemačka, mada ni druge države nisu ostale pošteđene. Tako je poznat slučaj *Tristan* (1985.) kada je 20 Nemačkih hakera uspešno razbilo zaštitu *Tsukuba High Energy Institute*, već iduće godine prošetali su se EDP sistemima, kao i glavnim računarom *Lawrence Berkeley Laboratory*, koristeći ga, potom, za ulaske u mnoge vojne i državne sisteme. Naknadno se uspostavilo da je u pitanju grupa koja je tesno bila povezana sa KGB.

<sup>128</sup> Holandska hakerska grupa nazvana *Paranoia* početkom 1995. godine otkrila je *BSyKb* kod na osnovu koga je dešifrovala TV signale *Videocrypt - coded signal*-a dovodeći u opasnost originalnost potpisa o plaćanju.

Dakle, ovaj proces uletanja u sisteme prate veoma opasni incidenti, kao što su: upadi u vojni sistem, uništavanje satelitskog televizijskog transmitera, kolaps komunikacijske mreže (npr. evropske), i slično.

### 3.2.3. Tipovi hakinga

Jasno je da su ne samo kompjuterska, već i sva elektronska sredstva postala meta hakera. Dela koja predstavljaju haking mogu se podeliti na različite kategorije zavisno od motiva, ciljeva i načina upada. Njih izvršavaju amateri ili profesionalni kriminalci. Zbog toga se haking prevashodno deli na<sup>129</sup>: **1) amaterski**, i **2) profesionalni**.

Osim ovih moguće je postojanje i drugih **vrsta hakinga**. Tako, haking može biti:

1. po nameri: **dobronamerni** i/ili **maliciozni**;
2. po cilju: **čitanje, uništenje, menjanje, distribuiranje, fabrikovanje podataka, ostavljanje poruke, startovanje programa bez dozvole, brisanje ili ispravljanje programa i podataka**;
3. po počiniocima: **pojedinci** i/ili **grupe**;
4. po mestu odakle je napad krenuo: **eksterni** i **interni**;
5. po realizovanju od strane grupe: **organizovano** i/ili **stihijski**.

Bilo kojoj vrsti hakerski napadi pripadali sigurno je da će imati **tendenciju rasta i da će biti sve raznovrsniji**.

#### 3.2.3.1. Amaterski haking

Postojbina hakinga uopšte, pa i amatreskog, je SAD. Prvi takav zabeleženi slučaj desio se još ranih 60-ih godina na *M.I.T.* i predstavlja, u stvari, prapočetak hakinga i sadašnjih računarskih virusa<sup>130</sup> (program koje je tada hakingom ubačen bio je "*cookie monster*").

<sup>129</sup> Samociuk M., op. cit., str. 152.

<sup>130</sup> Spafford E. H., Heaphy K. A., Ferbach D. J., op. cit., str. 318.

Danas, hakeri entuzijaste uglavnom imaju jedan, redje više, objekata napada. Osnovna odlika amaterskog hakinga je što je to, po pravilu, **delo mladih ljudi** (hakeri - amateri obično imaju od 17 do 25 god., mada je uočena pojava snižavanja ove starosne granice na 13 ili čak manje godina), i **oni ne nanose, odnosno ne žele da nanose, neke stvarne štete** (ili bar to ne čine namerno) **svojim upadom u sistem**<sup>131</sup>. Mada u ovoj kategoriji postoji još jedna grupa hakera kojima je glavni cilj da **razbiju sigurnosni sistem**<sup>132</sup>. Oni sate i sate provode u proučavanju sistema obezbeđenja posebno zaštićenih kompjuterskih sistema i pronalaženju načina za rušenje te zaštite<sup>133</sup>. Smatra se da je broj ovih hakera - amatera - eksperata, relativno veliki (npr., u V. Britaniji, to je od 10 do 20% od ukupnog broja hakera). Sam stav hakera-amatera ilustruje njihovu "naivnost", u kojoj oni, detinjasto, žele da demonstriraju svoju pamet i visprenost upadom u određeni sistem i slabosti obezbeđenja tog sistema, a istovremeno da ostanu nekažnjeni jer to nisu uradili sa namerom da prouzrokuju štetu.

Naravno, ni kod hakera - amatera nije sve tako ružičasto. Ne mali broj među njima su i vandali koji upadom u sistem žele da nanesu štete, uspire sistem, obrišu podatke, onemoguće korisnike, a, takodje, i izvrše sabotažu određenog sistema.

Znači, hakeri - amateri najčešće žele da ispune jedan i/ili više od sledećih ciljeva<sup>134</sup>:

- **da pronadju** dovoljno izazovni sistem i poigraju se sa njim;
- **da dobiju pristup sistemu** i pretraže ga da bi zadovoljili znatiželju i dokazali svoja znanja i sposobnosti;
- **da pronadju neku novu, zanimljivu igricu** u sistemu kako bi se igrali;
- **da unište ili modifikuju podatke, ubace viruse i virusolike programe ili da ostave neku, najčešće šaljivu, poruku;**

Način ispunjenja cilja je različit i raznovrstan, te ih je teško otkriti. Pogotovo što ih ima mnogo i što jedan haker - amater više puta pokušava upad u sistem dok mu pokušaj ne uspe. Zanimljivo je da se oni retko vraćaju istom sistemu, tako da je i to

<sup>131</sup> Forester T., Morrison P., op. cit., str. 46.

<sup>132</sup> Samociuk M., op. cit., str. 153.

<sup>133</sup> Tako je, npr. 27 marta 1995. godine jedan haker, čije ime nije oblavljeno, poslao poruku Centru za elektronsko podnošenje poreskih prijava u Kaliforniji, da sistem bezbednosti Centra ima ozbiljnih propusta, jer je otkrio password i login identifikacije, koje su se nalazile u sistemu. Korišćenjem lozinki i identifikacija ušao je u bazu. O tome više: Collinson H., op. cit., str. 117 - 121.

<sup>134</sup> Grover D., The protection of computer software - its technology and application, Cambridge, Cambridge University Press, 1989., str. 152.

otazavajuća okolnost za otkrivanje. Jedini putokaz je njihova hvalisavost na osnovu koje se, dugotrajnim i mukotrpnim istragama, može ponekad doći do počinioca.

### 3.2.3.2. *Profesionalni haking*

Ma koliko na prvi pogled amaterski haking izgledao kao opasna pojava, teška za otkrivanje i kontrolu, ipak pojava profesionalnog hakinga postaje nešto od čega treba stvarno ozbiljno zazirati. Ovaj tip hakinga čine lica koja vrše kriminalnu delatnost upada u sistem, kao stalno zanimanje i koja im služi kao osnovni ili ključni izvor sredstava za život. Pri tom, profesionalnim hakerima upadi i "vršljanja" po sistemima ne predstavljaju nikakvu moralnu dilemu niti povredu neke moralne vrednosti. Kao i drugi profesionalni kriminalci i hakeri - profesionalci ne osećaju grižu savesti i ne kaju se za svoje upade. Čak, naprotiv.

Najčešće se udružuju u:

- *političke ili subverzivne grupe* za oštećavanje i iskrivljavanje informacija;
- *grupe za industrijsku špijunažu* koje teže da se domognu vrednih informacija koje mogu skupo prodati;
- *"spasiteljske" grupe* koje teže da ublaže određene nestašice (vere, novca i/ili robe); i
- *grupe za obavljanje bilo kog tipičnog kriminaliteta.*

Za ovaj tip hakinga je **karakteristično**:

1. **da su napadi brižljivo i dugotrajno planirani**, uz studiozno analiziranje prethodnih sopstvenih i tuđih iskustava (kriminalci sa stručnom literaturom i menjelima);
2. **da najčešće napadaju iste ili slične vrste sistema**, mada to mogu biti "politropni" napadi;
3. **da hakuju vešto, spretno** i na način koji će biti ne samo efikasan nego i najmanje rizičan za otkrivanje upada i njih samih;
4. **da napade češće izvršava grupa**, nego pojedinac, pri tom grupe imaju sopstvenu informativnu mrežu, časopise, radi međusobnog obaveštavanja o "podvizima";
5. **da počinioci poseduju veliko tehničko znanje** i "dobru" motivaciju za takav čin; i
6. **da su "ulozi" vrlo veliki** (transakcije ogromnih suma novca, upadi u izuzetno značajne sisteme, naročito za nacionalnu bezbednost ili transnacionalne korporacije koje predstavljaju centre političke,

ekonomske, finansijske i sl. moći), pa su i posledice velikih razmera, a "dobiti" poprilične.

Činjenica je, da je kompjuterski kriminalitet mnogo lakši način dolaska do novca, od obične i danas veoma zastarele oružane pljačke banaka. Putem korupcije i ucene, posedovanjem određenih informacija bez sumnje se može lepo živeti. Međutim, **profesionalni haking se često pojavljuje i kao upozorenje** na terorističke akcije<sup>135</sup>, političke i poslovne sabotaze, nelojalnu konkurenciju, flagrantna kršenja ljudskih prava ili prevare velikih, često i međunarodnih, razmera organizovane od raznih subjekata, a realizovane od strane "kompjuterske mafije" specijalno angažovane i izuzetno plaćene za realizovanje ovih poslova<sup>136</sup>.

Zanimljivo je da se profesionalni haking sve češće pojavljuje u formi **organizovanog kriminala** uključivanjem kompjutera u organizovanu prostituciju, pornografiju<sup>137</sup>, rasturanje droge<sup>138</sup>, prikupljanje i rasturanje kradene robe, kladjenje, pranje novca, bskrupulozno zalenašenje ili uterivanje dugova. Tako se hakeri - profesionalci udružuju u razne grupe, bande, ili "udruženja" sa namerom i ciljem da se hakingom bave kao redovnom profesijom. Najčešće se formiraju lažne firme iza kojih hakerska grupa obavlja svoju nedozvoljenu aktivnost. Oni koriste kompjutere firme za otkrivanje šifri, a u fiktivnom nudjenju proizvoda i usluga prikrivaju stvarne namere. Međutim, ne treba zanemariti ni organizovane grupe za haking koje se ne prikrivaju, već time hvale i ponose. Takva je čuvena nemačka grupa *Computer Chaos Club*, američke *Quasi Moto*, *8BBS*, *Neon Knights of North, West, East and South*, *Pitare-80*, *Nu Prometheus*, naravno i jedna od najpoznatijih *Legion of Doom* (nastala spajanjem *Legion of Hackers* i *Legion of Doom*), i mnoge druge.

Za organizovani profesionalni haking **karakteristično** je:

**1. da su to čvrste, dobro organizovane i osmišljene grupe;**

<sup>135</sup> Tako je grupa hakera iz Hanovera između 1986. i 1989. godine provaljivala u dobro čuvane vojne podatke sa idejom "da treba nešto učiniti za svetski mir" i "jednakost među blokovima", dostavljajući podatke Pentagona sovjetskoj tajnoj službi. Nakon otkrivanja ova je grupa došla i pred sud. Bio je to prvi slučaj suđenja hakera zbog špijunaže. O tome više kod" Vodinić V., op. cit., str. 330 i 331.

<sup>136</sup> Forester T., Morrison P., op. cit., str. 46.

<sup>137</sup> Javnost Kanade pre par godina bila je uzburkana slučajem korišćenja kompjuterski poslatih biltena za transmisiju pornografije. U Filadelfiji je odeljenje za seksualni kriminal policije pratilo prenos dečije pornografije, a isto tako je i FBI bio uključen u istragu u Oklahomi. O tome više u materijalu Ministarstva pravde SAD, str. 10 i 11.

<sup>138</sup> Upadi u policijske sisteme služe za praćenje akcija i dobijanje podataka o oduzetim količinama droge, potkizivačima, mestima nabavke, kao i za anonimno komuniciranje između dilera.

2. da su predviđene da **deluju duže vreme**, mada se mogu pojaviti i kao “leteće”;
3. da **imaju izgradjen sistem sopstvenih normi i standarda**, baziran na negaciji posebnih, viših vrednosti, čak i ljudskog života;
4. da su im nazivi, po pravilu, **parodije** na: velike korporacije (*Fortune 500*, *Belcor*, *IBM Syndicate*, *SABRE*, *Anarchy company* i sl.); vladine službe, organizacije i agencije (*NASA Elite*, *NATO Association*) ili pokrete u muzici i subkulturi (hipije, pankere), kao i na prave kriminalce (*Apple mafia*). Ne retko ove organizovane grupe teže da **prikriju ili upozore na svoju delatnost** kroz identifikaciju sa klubovima i krugovima (*Club X*, *Elite Hackers Club*, *Circle of Death*) ili kroz **poetske opise hakerskih aktivnosti** (*Autostopers*, *Stow-away*)<sup>139</sup>;
5. **organizacija im je manje hijerarhizovana nego kod drugog organizovanog kriminaliteta**, jer su im znanja i veštine visoke i prilično ujednačene;
6. sama **grupa je izuzetno operativna**, sposobna za brzo manipulisanje i efikasno brisanje tragova, tim više što se lako premeštaju;
7. **obavljanje hakinga predstavlja samo osnovu za vršenje drugih kriminalnih aktivnosti** - ucenjivanje, terorizam, sabotaze, špijunaže, pretnje, zastrašivanja;
8. ne retko su **povezani i sa ovlašćenim korisnicima, licima koja sprovode zakon, poitičarima i liderima političkih stranaka i frakcija**, tako da postaju veoma moćan politički i ekonomski faktor;
9. **za sada su manje međusobno suprotstavljene**, po čemu se razlikuju od drugih organizovanih grupa, i često pomažu jedni drugima protiv svih ostalih; i
10. **sve izraženija internacionalizacija i povezivanje** sa sličnim grupama u drugim zemljama i sa drugih kontinenata.

Dakle, opasnost nije mala i raste istom brzinom kako se razvijaju nove tehnologije.

#### 3.2.4. Ko, zašto i gde hakuje?

---

<sup>139</sup> Sterling B., op. cit.

Hakera ima više različitih kategorija<sup>140</sup> zavisno od razloga zbog kojih upade preduzimaju<sup>141</sup>:

**Prvo. *Hakeri su oni koji uživaju u učenju*** (mahom studenti i djaci, mada ni drugim kategorijama ovo nije strano) o detaljima sistema (kompjuterskog, komunikacionog) i kako da povećaju njegove mogućnosti, nasuprot većini korisnika koji uče samo minimum onoga što je neophodno.

**Drugo. *Hakeri su oni koji sa entuzijazmom programiraju*** i u tome više uživaju (mahom studenti i djaci, a potom profesionalci), nego da o njemu teoretišu. Naravno, oni su i izuzetno dobri u tome.

**Treće. *To su prevashodno oni koji su sposobni da cene hakerske vrednosti*** (svi sem kriminalaca).

**Četvrto. *Hakeri su eksperti za pojedine vrste programa*** (profesionalci).

**Pet. *Oni su i eksperti svake vrste*** (profesionalci).

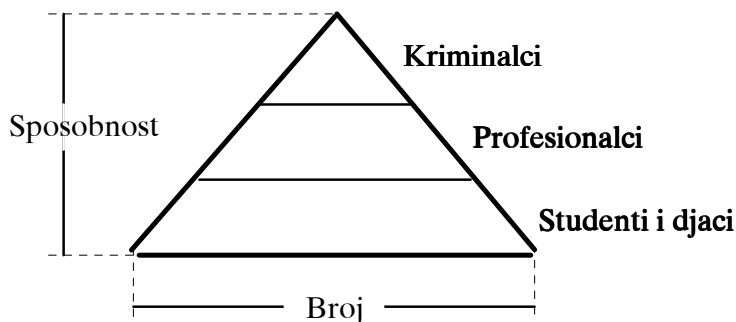
**Šesto. *To su i maliciozni ljubopitljivi nametljivci*** (kriminalci) koji pokušavaju da otkriju informacije njuškajući unaokolo, u cilju postizanja koristi (ekonomske, političke, lične) ili nanošenja štete (uništenjem, otkrivanjem i sl.)<sup>142</sup>.

Na osnovu ovih odredjenja prepoznaju se **tri** najčešće **kategorije počinilaca hakinga**:

<sup>140</sup> Raymond E., Steel G., The New Hacker's Dictionary, Cambridge, MIT Press MA., 1991., str. 8.

<sup>141</sup> Johnson G. D., op. cit., str. 110; Drakulić M., Drakulić R., op. cit., str.136 - 153.

<sup>142</sup> Forester T., Morrison P., op. cit., str. 78.



Zavisno od toga ko hakuje različiti su i razlozi zbog čega se to radi. Sa aspekta **samih hakera** to se čini zbog toga što su mladi, znatiželjni, spremni na učenje i istraživanje granica sistema i mreža i zbog profesionalne zainteresovanosti i izazova, postizanja određenih "zlona" ili "dobronamernih" ciljeva (kriminalnih).

Sociolozi, psiholozi, profesionalni informatičari, profesori informatike i računarstva, kao i mnogi drugi stručnjaci pokušavaju da razgrnu velove u koje je haking zamotan. Najčešće se na pitanje - zašto? - daju sledeći odgovori:

1. radi **odgonetanja** mnogobrojnih intelektualnih izazova, pojedinci pokušavaju da reše, bar, neke od njih (kompjuterski i telekomunikacioni sistemi su neistražene teritorije koje čekaju da budu otkrivene);
2. radi **povećanje uzbudjenja** pri upadu i mogućnostima otkrivanja;
3. to je **odgovor na izazov** (mnogi hakeri smatraju da je ne samo zabavno testirati granice sistema, već i mogućnosti prbijanja svih zaštita);
4. radi **postizanja većeg ugleda i slave u kompjuterskom podzemlju, čija su oni** (po sopstvenom mišljenju) **elita** jer je to i način za postizanje određenog statusa i solidne pozicije (saopštiti, a naročito pokazati drugim hakerima svoje aktivnosti i podvige koji su izvedeni sa posebnom veštinom, lukavošću, tajnošću). Posebno je važno dokazati i pokazati posedovanje zabranjenog znanja, toliko bitnog za ovo podzemlje, pošto im ono otvara sva "sigurnosna vrata i lokote";
5. radi **mržnje prema vlasti i autoritetima**, naročito u slučajevima kad se sumnja da postoje određena kršenja, prekoračenja ili neizvršenja ovlašćenja koja imaju vladina ili međunarodna tela i organi;
6. radi **osvete**, najčešće od strane odbijenog kandidata na konkursu za posao da bi dokazao da je sposobniji od izabranog, kao i uvredjenog, otpušenog, ili nedovoljno cenjenog;
7. radi ne bez osnove **verovanja u mogućnost dobijanja dobro plaćenih i visoko cenjenih zaposlenja**, ne retko predstavlja i razlog dopuštanja da

budu uhvaćeni (tako je haker koji je bio poznat kao *Brain Dead* i koji je provaljivao u vladine, policijske i poslovne sisteme prilikom hapšenja izjavio: "hapšenje je za hakera prvi značajan korak u karijeri ka cilju postizanja visoko plaćenog konsultanta bezbednosti". Ovom je rečenicom on izneo mišljenje i većine od 74 hakera koji su 1995. godine uhapšeni u SAD-u)<sup>143</sup>;

8. radi postojanja **posebnog stila življenja** socijalno neadekvatnih, inače intelektualno sposobnih, pojedinaca. Ovaj stil nazivan "**kompjuterskim sindromom**" (kompjuterska psihoza), naročito napada muške adolescente između 14 i 17 godina starosti. Oni su obično samouki, uživaju u intelektualnim igrama, seksualno neaktivni, a možda zanemaruju i ličnu higijenu<sup>144</sup>. Ovi mladi ljudi često ne mogu ni da naprave razliku između realnog sveta i kompjuterski dočaranog, pa otuda, ne retko, za svakodnevno sporazumevanje koriste programski jezik;
9. njim se **supstituu komunikacije** u kojima kompjuteri zamenjuju ljude, jer ne zahtevaju međusobne i kompleksne odnose kao što je to slučaj sa ljudima;
10. kompjuteri su medijumi koji su **preokrenuli** mnogo što šta: u statusu pojedinca (kao što je sedenje u čelo stola), govoru tela (klimanje glavom, mrgodjenje), obezbeđenju neke vrste društvene anonimnosti te se menja način odlučivanja u grupi (dokazano je da kompjuterske konferencije omogućavaju ravnopravno učešće i ohrabruju nesigurne i sramežljive, dok se komunikacijom, putem elektronske pošte, anulira iskaz osećanja na licu, način izgovaranja poruke koji može imati uticaja na njeno tumačenje i sl.);
11. kao i radioamaterstvo, odlazanje na utakmice i sl. **haking postaje hobi i opsesija**, mada kada je zlonameran, sličan je destrukciji;
12. to je **porok** koji izaziva zavisnost koja u potpunosti zaokuplja hakera, kao alkohol alkoholičara, droga narkomana i od koje se teško može osloboditi, a lako postaje ovisan;
13. mnogi hakeri koristeći samo malo opreme (modem, PC, neke komunikacione softvere) **svojom dovrtljivošću uspevaju da prodru "u budućnost"**, te otuda primedbe da haking prouzrokuje male intelektualne izazove, ali velike mogućnosti, čine se preteranim, mada, donekle, i stoje. Za mnoge hakerske aktivnosti nije neophodna genijalnost, već znanje i spretnost. Međutim, neki od njih se ipak ne mogu realizovati bez izuzetne inteligencije i izvesne doze genijalnosti, usled čega se hakerima pridodaje osobina genijalaca;

<sup>143</sup> Collinson H., op cit., str. 215 - 220.

<sup>144</sup> Raymond E., Steel G., op. cit., str. 96.

14. to je svojevrsni oblik **deljenja pravde**, pri čemu se osećaj za nju remeti načinom na koji se ona realizuje (dilema da li su hakeri moderni Robin Hudovi ili samo moderni pljačkaši? i dalje ostaje nerešena). To je, dakle, nalaženje opravdanja za negativne aktivnost i pokušaj pravdanja pred sopstvenom savešću.

Naravno, ovo su samo neki od razloga koji dovode do **hakerske groznice**. Njen osnov je “zadovoljavanje svoje duhovne potrebe i veoma izražene želje za znanjem, statusom i moći”<sup>145</sup>.

Kao najčešći objekti upada, generalno uzevši (na osnovu podataka o izvršenom hakovanju), pojavljuju se:

- *kreditno dobro stojeće organizacije*;
- *kreditne agencije*;
- *univerzitetske instalacije*;
- *banke i finansijski servisi*;
- *novine* (dnevni listovi i časopisi);
- *elektronska pošta*;
- *vladini kompjuteriski i komunikacioni sistemi* (naročito vojni, policijski, ministarstava);
- *domaće i internacionalne kompjuterske mreže*;
- *PTT sistemi*;
- *kancelarijski informacioni sistemi*; i
- *EDI servisi*.

Ne retko se dešava da se uhvate tuđe i nepoznate "budne oči" u poverljivim sistemima. Pojave se s vremena na vreme i nestanu. Ne prave štetu. Poruka je jasna - pretnja će rasti, a njeno otklanjanje će koštati mnogo više nego zaštita koju sprovode eksperti<sup>146</sup>.

### 3.2.5. *Kako hakeri ulaze u sisteme?*

---

<sup>145</sup> Sterling B., op. cit.

<sup>146</sup> Drakulić M., Drakulić R., op. cit., str. 147.

Ulasku u sistem, naročito kad su u pitanju hakeri profesionalci, prethode određene pripreme i planirane akcije. Prva dva koraka pre hakerskog upada vezana su za: **skupljanje obaveštenja i pokušaj upada.**

**Prethodno obaveštavanje o sistemu**, zavisno od tipa hakinga, bazirano je na raznim tehnikama. Ono što je karakteristično je, da se koriste podacima za koje se u sistemima smatra da su nebitni za zaštitu, pošto se ona, uglavnom, orijentiše na lozinke. Zaboravlja se da hakerima svaka informacija o sistemu može poslužiti za pronalaženje praznina i "rupa". Tako, prethodna obaveštavanja hakeri o sistemu retko dobijaju slučajno. Ona su češće proistekla iz<sup>147</sup>:

**1. primene "oportunističkih" tehnika:**

- ◆ *prislušivanjem razgovora* (u barovima, restoranima, taksiju, telefonskih i sl.) zaposlenih ili korisnika i/ili
- ◆ *direktnim ispitivanjem*

**2. pretraživanjem novina, publikacija i BBS-ova**<sup>148</sup>;

**3. pretraživanjem pošte** (elektronske ili obične);

**4. prekopavanjem i preturanjem po otpacima i djubretu;**

**5. lažnim predstavljanjem** (javljanje na konkurs, studentska ispitivanja, izigravanjem "zaboravnih" korisnika);

**6. zaustavljanjem komunikacija:**

- ◆ *zaustavljanjem "glasa"*
- ◆ *izvlačenjem podataka, telefonskih veza i teleksa*
- ◆ *skupljanjem elektromagnetne radijacije iz jedinica vizuelnog displeja*
- ◆ *zaustavljanjem satelitskih ili mikrotalasnih transmisija*<sup>149</sup>

**7. kradjom;**

**8. podmićivanjem, iznudjivanjem i iskorišćavanjem:**

- ◆ *kockarskih strasti*
- ◆ *materijalnih problema*
- ◆ *ogromnih troškova vezanih za enormne medicinske račune*
- ◆ *ekstremnih nezadovoljstva zaposlenih*
- ◆ *korišćenjem alkohola, droge i sličnih zloupotreba.*

<sup>147</sup> Grover D., op. cit., str. 156 - 160.

<sup>148</sup> Po Sterling-u BBS su velike biblioteke "zabranjenog znanja" koje koriste hakeri da bi došli do određenih informacija i uputstva za "rad". Tako su u SAD-u 1991. godini naročito bili popularni BBS-ovi koji su obavještavali o: hakingu Američke banke; pregledu hakinga; hakingu Londonske banke; kako hakerisati; informatoru hakinga; osnovama hakinga; priručniku hakinga; tehnikama hakinga; rečniku hakinga; haking Mtc kreditne kompanije i sl.

<sup>149</sup> Japanci su u toku 1995. godine iskazali ozbiljnu zabrinutost zbog vojne i industrijske špijunaže koja se realizuje "presretanjem" elektromagnetnih talasa. Ministarstvo pošta i telekomunikacija naručilo je posebnu studiju o načinima prevencije od takve špijunaže, Communication, Vol. 38., no. 1/95., str. 10.

Kada je prikupio dovoljno obaveštenja o sistemu u koji želi da upadne, **haker pokušava da u njega udje**, koristeći se svim slabostima<sup>150</sup> i greškama u dizajnu, implementaciji i operacionalizaciji zaštitnog sistema<sup>151</sup>. Tehnike koje mu stoje na raspolaganju su raznovrsne, a izbor pada na one koje najviše odgovaraju njegovim (redje njenim) mogućnostima, sposobnostima, znanju i veštinama. Najčešće su to auto - biranje, korišćenjem posebnog modema ili prosto korišćenjem telefonskih brojeva ili komunikacionih linija za koje je ranije dobio odgovarajuća obaveštenja. Pored ovih tehnika, hakeri koriste i protokole, log - on procedure ili otkrivene korisničke *IDs* i lozinke.

Kad je ušao u sistem **haker pokušava da dobije privilegije** najvišeg nivoa kako bi mogao da ukrade, modifikuje ili uništi podatke ili pokušava da krađom tuđih korisničkih *IDs* i lozinke, u sistem unese programe koji će ga zaustaviti (usporiti i potpuno zaustaviti), oštetiti, ili uništiti. Za to mu služe odgovarajuće metode i tehnike od trapdoor-a, bombi, ansihronih napada, salami tehnike, do ubacivanja virusolikih i crvolikih programa.

### 3.2.6. Otkrivanje, istraga i prevencija - da li su mogući?

Da bi se haking mogao otkriti nužno je ispunjenje određenih pretpostavki. To su prevashodno: postojanje i korišćenje softvera sa programom za dobro "uhodjenje", redovno nadgledanje sistemskih ulazaka i praćenje svih signala. Iako deluju sasvim logične, ove radnje, i kad se kontinuirano preduzimaju, mogu, uglavnom, **najaviti da je posetilac u sistemu**, a često je to *post festum* ulaska. Znači, otkrivanje je veoma teško i, ne retko, svedeno samo na konstataciju o postojanju uljeza.

**Istraga** je, zato, **izuzetno otežana**, pa se i karakteristike koje inače prate kompjuterski kriminal u slučaju hakinga još multipliciraju i komplikuju. Naročito:

<sup>150</sup> Po podacima koje su izneti u časopisu Computers & Security (Collinson H., op. cit., str. 409 - 414.) od 300 ispitanih trgovačkih kompanija i firmi za vođenje knjigovodstva u V. Britaniji, 1/3. je priznala da nema nikakvu zaštitu od neovlašćenog eksternog pristupa, 1/5 je izjavila da je nesposobna za detekciju takvih pristupa. Okolnosti su teže ako se ima u vidu da su računi nekih od ovih firmi vredni desetine i stotine miliona funti, a da 90% njih čuva podatke i file-ove svojih klijenata iako nemaju zaštitu.

<sup>151</sup> Jedan od najslikovitijih primera su dva propusta u sigurnosti Interneta koje su obelodanjene januara 1995. godine. Slabosti je 1994. godine otkrio Kevin Mitnick, koji je inače višestruki osuđivani haker u povratu, napavši kompjuter poznatog eksperta za kompjutersku sigurnost, Tsutom Shimomura. Više o tome u diplomskom radu Tatjane Zlatković.

1. **što su počinioci veoma vešti i inteligentni**, lukavo izbegavajući otkrivanje<sup>152</sup>, izuzetno brzo uništavajući dokaze, i sl;
2. **što postoji vremenska i prostorna udaljenost**<sup>153</sup>;
3. **što većina žrtvi prikriva napade**, neobaveštavajući istražne organe;
4. **što sudski procesi dugo traju**, uz često krajnje neizvesne rezultate, i izuzetno niske kaucije<sup>154</sup>.

Ne retko istraga uopšte ne daje rezultate, čime se još više ohrabruju hakeri da nastave sa aktivnostima. Da bi se, bar, obezbedile osnovne pretpostavke za istragu nužno je rešiti, na odgovarajući način, i posebne probleme koji se odnose na kompetenciju istražitelja, kompleksnost istrage i kompleksnost prava<sup>155</sup>. **Posebno je važno da se istraga dobro pripremi, da se sprovede od strane kompetentnih i posebno obučanih istražitelja** (često su u pitanju eksterni, u mnogim zemljama, posebni odredi policije ili njima odgovarajući organi, sa ekspertima u informatici i kriminalistici)<sup>156</sup>. Zanimljivo je da se porastom "hakerske industrije" stvara i jedno novo

<sup>152</sup> Tako je u avgustu 1986. godine u laboratoriji *LBL* u SAD-u konstatovan upad hakera. Ova laboratorija izvršavala je i ugovorene obaveze za vojsku, te je upad bio krajnje zabrinjavajući. Počela je istraga. Istražni organi su pustili uljeza da nastavi sa aktivnostima pomno beležeći sve njegove aktivnosti. Praćenje je trajalo godinu dana. Hacker je ne samo šetao sistemom *LBL*-a već je upotrebio njihov kompjuter za upade u druge univerzitetske, poslovne i vojne sisteme. Maskiranje je bilo vešto izvedeno i rezultiralo sa pokušajima prodora u 450 kompjutera. U 30 je uspeo da udje. Sistemi su javljali greške, koji su nakon izvesnog vremena identifikovani kao napadi. Praćenjem su istražitelji otkrili mnoge njegove osobenosti, od stila programiranja, do brzine u reakcijama na različite zahteve različitih operativnih sistema. Međutim, praćenje je bilo izuzetno teško. Počele su igre "mačke i miša" (mada je pitanje, u početku, bilo ko je miš?). U jednom trenutku, postavljena je zamka sa lažnim file-om u kome su se kao strogo poverljive pojavile adrese elektronske pošte i nekoliko poruka od nepostojećeg sekretara *LBL*-a. Ovom file-u nije niko, sem vlasnika i sistem inženjera, mogao pristupiti. Postavljeni su i posebni alarmi. Nakon nekog vremena alarmi su pokazali prisustvo uljeza. Posle sata čitanja, koliko je haker bio u file-u, kompletirani su podaci o tragovima. Nakon mesec dana stiglo je i anonimno pismo iz Nemačke na nepostojećeg sekretara. Krug se zatvarao. Počela je saradnja između američkih i nemačkih istražnih organa, univerziteta, *LBL*-a, nemačkog PTT-a, koji su nakon teškog puta došli do odredišta - 1989. godine uhapšeni su Marcus H i Peter C, kao osumnjičeni za inkriminisane radnje. Slučaj je završen sa **kaznom od 20 meseci zatvora, uz mogućnost uslovnog oslobađanja i novčanom kaznom od 10.000 maraka**. O celom postupku više kod: Mandell M, *The West German Hacker Incident and Other Intrusions*, Edicija: *Computers Under Attack, Intruders, Worms, and Viruses*, str. 150 - 156.

<sup>153</sup> Članovi australijske hakerske grupe *Dave* uhapšeni su 1990. godine, iako su kompjuterske provale počeli da vrše po Americi i Australiji 1988. godine iz Australije.

<sup>154</sup> Tako je, npr., jedan škotski student, kome je trebalo da počne sudjenje za delo hakinga, otputovao u SAD na svetski kongres hakera (1995.). Na kongresu je, između ostalog, 200 hakera iz Evrope, Amerike i Azije, raspravljano i o sličnim problemima. O tome više kod Collinson H., op. cit., str. 409 - 414.

<sup>155</sup> Pallmer I. C., Potter G. A., op. cit., str. 182.

<sup>156</sup> Tako je, npr., u SAD objavljena lista profesionalnih asocijacija koje se bave istragom i hvatanjem kompjuterskih kriminalaca. Ova lista od 11 privatnih i javnih asocijacija, obuhvata njihove adrese, telefone, specijalnost i imena lica za kontakte. Takođe, daju se i brojevi telefona policijskih istražitelja po gradovima, kao što i mnoge veće softverske firme daju posebne telefone na koje mogu da se jave njihovi korisnici koji imaju probleme sa nekim od dela kompjuterskog kriminaliteta.

zanimanje - **lovci na hakere** (*hacker - trackers*) koji se nalaze u okviru policije, vladinih agencija ili su, čak, i privatni istražitelji. Oni sve više bivaju pozivani da prate hakerske tragove i pronalaze počiniocce. Tako je jedan specijalizovani lovac na hakere u okviru *Royal Canadian Mounted Police* posle višemesečnog praćenja pronašao 23-eg programera koji je uleteo u *SFU's* kompjuter godinu dana pre. Ovaj slučaj ukazuje istovremeno i na jednu specifičnost istrage ovih dela - višemesečno, pa nekad i višegodišnje istraživanje, koje prevashodno uključuje korišćenje komunikacionih sistema i čekanje vesti u biltenima ili međusobnim elektronskim vezama kojim se kriminalci služe za međusobnu komunikaciju. Zato istražitelji moraju, sem strpljenjem, biti snabdeveni i istrajnošću da pregledaju ogromne količine kompjuterizovanih podataka kako bi našli tragove i dokaze. Pored toga, istražitelji, kad je ovaj tip kriminaliteta u pitanju, moraju biti u tesnoj vezi sa žrtvom, što pokatkad i nije baš tako jednostavno. Poseban problem vezan je za promenu klasičnog policijskog, odn. istražnog, "rada", jer se zahteva i dobro poznavanje tehničkih pravila i karakteristika. No, to svakako ne isključuje ni uobičajene metode i tehnike otkrivanja i praćenja<sup>157</sup>.

Naravno, kompleksnost istrage ogleda se i u brojnosti veza i terminala sa kojih su ulasci hakerskih uljeza mogući. **Naročito alarmantan postaje problem širenja mreža** u koje se, pored organizacija i vladinih institucija, povezuju i pojedinci, te je veoma teško kontrolisati sve korisnike i zainteresovane. Pri tom, ne treba zanemariti ni činjenicu da je izuzetno mali broj hakera stvarno i bio uhvaćen, a posebno i to da su **dokazi veoma često bili sporni** tako da su uhvaćeni hakeri bivali puštani na slobodu bez kazne<sup>158</sup>. To je često bila **posledica**:

- ◆ *gubljenja važnih podataka zbog promene napajanja* dok je manipulacija sa podacima trajala;
- ◆ *osetljivosti kompjutera na pomeranja* (sem ako nije u pitanju notebook) zbog kojih se može desiti da dodje do uništenja podataka;
- ◆ *prolaska kroz, npr. sigurnosna vrata i oštećenje disketa*;
- ◆ *nepažljive izmene podataka od strane istražitelja nestručnim ili nemarnim rukovanjem sa kompjuterom*;
- ◆ *istovetnosti kopija i teškim dokazivanjem originala* i sl.

Što se, pak, pravne kompleksnosti tiče, ona enormno raste samim specifičnostima i mnoštvom varijanti načina izvršenja ovih kriminoidnih radnji.

<sup>157</sup> Grupa autora, op. cit., str. 18 - 20.

<sup>158</sup> Jedan od njih je i Craig Naidorf koji je pušten bez obzira što su njegovi upadi u Bell-ove sisteme trebali da se završe sa 65 godina zatvora, velikim novčanom kaznom, kao i kaznom društveno korisnog rada.

Da bi se haking donekle sprečio nužno je **preduzeti i odgovarajuće preventivne mere**. To su aktivnosti kojima organizacija treba da preduhitri potencijalne uljeze. Prevažodno, ove se aktivnosti moraju odnositi na kontrolu izvora podataka iz kojih hakeri crpe svoja obaveštenja o sistemu i njegovim slabostima. Kontrola mora obuhvatiti i identifikaciju lica i lozinki, sigurnost operativnog sistema, softversku kontrolu pristupa, kontrolu baza podataka i kontrolu mreže. Pored toga, tu su i aktivnosti vezane za analizu rizika, kao i redukciju motivacije, naročito zaposlenih (koji iznose podatke i informacije o sistemu i njegovim slabostima van organizacije). Takodje, te će se redukcije odnositi i na korisnike i sva ona treća lica koja mogu posredno doći do takvih podataka<sup>159</sup>.

#### 4.      **Zaštita od virusa i hakinga**

##### 4.1.    *Pravna zaštita od kompjuterskog kriminaliteta*

Da bi se obezbedila zaštita od kompjuterskog kriminaliteta, pa i od hakinga ili virusa, nužno je preduzimanje kompleksa mehanizama i mera. Dugo su jedna od najslabijih karika sigurnosti bile pravne mere i mehanizmi. Medjutim, dešavaju se određeni pomaci.

Naime, mnoge zemlje počele su donositi ili je u toku postupak donošenja posebnih zakona, odnosno novela postojećih krivičnih zakona kojima se reguliše ova problematika<sup>160</sup>. Osim toga, pri OECD-u i Evropskoj Uniji posebni komiteti istražuju probleme i pripremaju odgovarajuće međunarodne akte kako bi se obezbedila unifikacija i harmonizacija nacionalnih prava zemalja članica. Naravno, sve ove aktivnosti ne bi bile potpune kada im se ne bi pridružile i one vezane za OUN, koja pokušava da kanališe čitavu nabujalu reku problema vezanih za ovu vrstu kriminaliteta.

<sup>159</sup> Grover D., op. cit. str.170 - 173.

<sup>160</sup> Gemingnani M., Viruses and Criminal Law, Edicija: Computers Under Attack, Intruders, Worms, and Viruses, New York, ACM Press, 1990., str. 490.

#### 4.1.1. *Kompjuterski kriminalitet i nacionalni propisi zaštite*

Kompjuterskog kriminalitet je ozbiljan i stvaran izazov za pravne sisteme. U početku, sasvim prirodno, nije bilo baš mnogo zemalja koje su dela ovog kriminaliteta uvrstile u svoja nacionalna zakonodavstva. Bilo je, ali je i dalje prisutno, prilično lutanje oko načina i predmeta regulisanja. Najteže je bilo odgovoriti na pitanja: pod čega podvesti radnje i aktivnosti vezane za ovaj specifični kriminalitet i kako ga u odgovarajućim zakonima definisati? Rešenja su bila razna. No, sigurno je jedno - zbog ovog kriminaliteta sve je evidentnija potreba za modernizacijom zakonodavstva, naročito krivičnog, kao i procesnog. Poseban je problem bio koje rešenje bi trebalo prihvatiti i kakve kazne predvideti? Uglavnom se prihvata jedno od sledećih rešenja:

- ◆ *obezbediti da postojeći propisi obuhvate adekvatno odredjenje pojedinih tipova ovog kriminaliteta*, sa svim obeležjima i karakteristikama, kao i odgovarajućim sankcijama, unoseći nove ili modifikujući postojeće odredbe; ili
- ◆ *doneti posebne, sui generis, zakone* ukoliko to pravni sistem zemlje dozvoljava; ili
- ◆ *kombinovati oba rešenja.*

U početku je izgledalo da će prvo rešenje postati opšte prihvaćeno, jer se činilo lakšim i boljim modernizovati pravo, prevashodno krivično i procesno, pa potom i ono koje obezbeđuje zaštitu podataka. Pogotovo što su neke od aktivnosti veoma mnogo podsećale na klasična krivična dela. Međutim, ni to nije dugo potrajalo i sve se intenzivnije razmišljalo o drugoj soluciji. Tim više, što je i SAD, postojbina ovog kriminaliteta, prihvatila upravo nju. Iako najkompletnije, trećem rešenju nije pribeglo mnogo zemalja zbog njegove izuzetne složenosti. A kako su se aktivnosti odvijale može, kao primer, poslužiti SAD.

**Američki kongres** je maja 1986. godine izglasao dva zakona: *Zakon o kompjuterskoj prevari i zloupotrebi (Computer Fraud and Abuse Act)* i **Zakon o privatnosti elektronskih komunikacija** (*Electronic Communications Privacy Act*). Na osnovu ovih zakona, svaki pokušaj neovlašćenog menjanja podatka na kompjuterima druge države smatra se federalnim prekršajem<sup>161</sup>. Prisluškivanje elektronske pošte i elektronska pljačka (presretanje elektronskog transfera novca), takodje, je kažnjivo. Prvi prekršaj je kažnjiv sa 5, a drugi sa 10 godina zatvora. Osim toga predviđena je i kazna do 20 godina zatvora za pristup informacijama čije

<sup>161</sup> Word G. H., Shriver R. F., op. cit., str. 96.

neautorizovano otkrivanje predstavlja opasnost za, npr., odbranu zemlje. Osim kazni zatvora, zakoni predviđaju i novčane kazne koje se kreću od 5.000 do 100.000 dolara, kao i meru društveno korisnog rada, odn. određeni broj sati ovog rada. Zakoni su federalnog karaktera, što znači da važe samo ako prekršaj predje granice makar jedne od federalnih država. Time je obezbeđeno pravo svake države da donosi zakone kakve želi.

14. jula 1988. predstavnik Kalifornije predložio je **Zakon o iskorenjavanju računarskih virusa** (*Computer Virus Eradication Act*) prema kome se svako ko namerno ubaci u program naredbe koje izazivaju razne štete korisnicima u toku rada tog programa, kao i onaj koji takav program prosledi nekom drugom, bez upozorenja, izlaže građanskim i krivičnim kaznama.

Krajem iste godine **šest velikih softverskih kompanija** pokušava da se izbori za zakon koji bi stvaraoce virusa slao u zatvor do 10 godina. Ove firme su formirale **Savet proizvođača softvera** (*Software Development Council*), koje, u saradnji sa nekoliko advokatskih firmi, radi na izradi modela zakona o računarskim virusima koje bi trebalo da bude prihvaćen širom sveta.

*Predložene kazne* su sledeće:

- ♦ za stvaraoce virusa koji uništava podatke - **\$ 1000 ili 3 meseca zatvora**;
- ♦ za ugrožavanje javne bezbednosti ili zdravlja - **\$ 10.000 ili 1 godinu zatvora**; i
- ♦ za bilo kakve po život opasne efekte virusa - **10 godina zatvora**.

Godinu dana kasnije **Udruženje proizvođača računarske i poslovne opreme**, sa sedištem u Vašingtonu, tražilo je od vlade SAD-a da goni kreatore računarskih virusa. U pismu senatskom *Podkomitetu za tehnologiju i nauku* tražilo se da Kongres donese antivirusne zakone zasnovane na činjenici samog postojanja kriminalnog ponašanja, pri čemu se zanemarivala uloga opreme i tehnika koji se koristi za zlodelo kreiranja i plasiranja virusa. Oni zahtevaju i da se sudske i istražne institucije obučavaju za gonjenje kompjuterskog kriminaliteta, da se povezuju kompanije u računarskoj industriji na zajedničkom poslu zaštitnih sredstava i, konačno, da se vrhunski prioritet da istraživanjima na području virusa uz vodeću ulogu *Instituta za standarde i tehnologiju*.

Shvatajući opasnost od slobodnog uplitanja u računarske sisteme i mreže, izvestan broj federalnih država je doneo posebne zakonske (krivične) amandmane. Tako, npr. član 502. **Krivičnog zakona Kalifornije** jasno definiše prava

korisnika računarskog sistema u cilju sprečavanja neovlašćenog pristupa i upotrebe određenih delova sistema i podataka. Na osnovu njega su u martu 1988. god. osuđena dvojica Pakistanaca, braća Bazit i Amdžat Alvi, koji su razorili 40% kapaciteta računarskog sistema univerziteta u Delaveru. Naime, njih dvojica su omogućila telefonski prodor svog softverskog proizvoda nazvanog *SCORES*, u *EDSN* mrežu (*Electronic Data System Network*), koji ju je i razorio.

Naravno, što se hakinga tiče, policijska i sudska statistika ukazuju da broj slučajeva raste, a istovremeno, da se sve više zemalja uključuje među one koje su ovo delo predvidele u svom krivičnom zakonodavstvu<sup>162</sup>. Primera radi, treba pogledati podatke iz SR Nemačke i Holandije:

**Policijska i sudska kriminalna statistika SR Nemačke**

| godina                               | 1987. | 1988. | 1989. | 1990. | 1991. | 1992. |
|--------------------------------------|-------|-------|-------|-------|-------|-------|
| registrovani slučajevi / osumnjičeni | 49/43 | 54/64 | 68/60 | 77/57 | 61/31 | 75/46 |
| pokrenuti slučajevi / osuđeni        | 1/1   | 4/2   | 4/1   | 1/0   | 1/0   |       |

**Holandsko ministarstvo policije**

| godina                 | 1987. | 1988. | 1989. | 1990. | 1991. |
|------------------------|-------|-------|-------|-------|-------|
| registrovani slučajevi | 1     | 4     | 9     | 11    | 95    |

S druge strane, sve je veći i broj zemalja koje nisu informaciono vodeće, ali su donele odgovarajuće propise vezane za ovaj kriminalitet.

<sup>162</sup> Mohrenschlager M., Hacking: To Criminalize Or Not? - Suggestions For The Legislature, *Computer & Security* 14 (1995) 103 - 112; Gordon S., Technologically Enabled Crime: Shifting Paradigms for the Year 2000, *Computers & Security*, no. 14 (1995), str. 391 - 402; Cobbs J., Writer F., Canadian Computer Crime Legislation: A Review, Datapro Systems, Hardware & Software, CD, 1994.; Tantam M., European Computer Misuse Legislation, Datapro Systems, Hardware & Software, CD, 1994; Sharpe D., Asia - Pacific Computer Misuse Legislation, Datapro Systems, Hardware & Software, CD, 1994; Rasch M., Computer Criminal Law and Federal Sentencing Guidelines, Datapro Systems, Hardware & Software, CD, 1994.

**Zaštita kompjuterskih i telekomunikacionih sistema  
od pojedinih dela kompjuterskog kriminaliteta (virusa i hakinga)**

| zemlja     | godina   | naziv akta   | delo  |
|------------|--|--|---|
| Arkanzas   | 1987.  | Krivični zakon   | kompjuterski prestup  |
| Austrija   | 1987.  | Zakon o zaštiti podat.   | povreda prava   |
| Australija | 1988<br>poslednja<br>modifika<br>cija<br>1995. | Amandman o zaštiti<br>kompjuteru i podataka<br>Komonvelta i<br>korišćenja mogućnosti<br>Komonvelta | krivotvorenje dokumenata<br>neautorizovani pristup podacima<br>uništenje nakon ili u toku pristupa podacima<br>neautorizovano korišćenje kompjutera ili<br>prenosnika<br>uništenje u toku ili nakon pristupa podacima<br>korišćenjem kompjutera ili prenosnika  |
| Belgija    | 1990.  | Krivični zakon   | nedozvoljeni pristup<br>oštećenje<br>manipulacija sa podacima ili komp. proramima<br>modifikacija podataka ili komp. programa   |
| Danska     | 1985.  | Krivični zakon   | nezakonito ponašanje pristupom informacijama<br>ili programima drugih   |
| Filipini   |  | Krivični zakon   | neautorizovani pristup kompjuteriz. bazama<br>neautorizovano unošenje podataka u kompjutere<br>kradja informacija   |
| Florida    | 1978.  | Krivični zakon   | prestupi protiv korisnika kompjutera  |
| Francuska  | 1988.  | Krivični zakon -<br>poglavlje III -<br>nesumljivi<br>kompjuterski napadi                           | neautorizovani pristup podacima i sistemima za<br>automatsku obradu podataka<br>ometanje operacija sistema za obradu podataka<br>ometanje integriteta i autentičnosti podataka<br>krivotvorenja svakog oblika kompjuterizovanih<br>dokumenata   |
| Holandija  | 1993.  | Krivični zakon   | nameran i nezakonit pristup automatizovanim<br>sistemima ili delovima sistema<br>kompjuterski prekršaji izvršenja naknadnih<br>kopija ili zapisa za sebe ili drugog, skladištenje<br>podataka u AOP kojim se stiče dobit<br>nezakonitim pristupom<br>kompjuterski prekršaji zloupotreba telekomu.<br>infrastrukture |
|            | 1993.  | Zakon o kompjutersk.<br>kriminalu  | oticanje podataka u komunikacijama, komp.<br>špijunaža i oštećenje podataka   |
| Hong Kong  |  | Uredba o kradji  | kradja i napadi na imovinu  |
| Indonezija |  | Krivični zakon   | oštećenje<br>namerno odavanje bilo koje tajne   |
| Italija    | 1994.  | Krivični zakon   | haking u nezaštićene sisteme<br>širenje virusa<br>trgovina password-ima<br>oštećenje nacionalnog informacionog sistema  |

|              |                    |  |   |
|--------------|--------------------|--|---|
| Japan        | 1987.              | Krivični zakon   | “prekid kompjuterskog poslovanja” - uništenjem kompjutera koji se koristi za obavljanje poslova   |
| Južna Koreja |                    | reforma Krivičnog zakona   | nelegalno primanje ili otkrivanje informacija prevare pomoću kompjutera<br>kompjuterska sabotaža  |
| Kanada       | 1985.              | Krivični zakon   | neautorizovano korišćenje kompjutera, zlodela na podacima   |
| Malezija     |                    | Krivični zakon - klasična kriv. dela sa elementima vezanim za kompjutere | krada<br>prevare<br>podvale   |
| Nemačka SR   | 1986.<br><br>1988. | Krivični zakon deo o zaštiti od ekonomskog kriminaliteta<br><br>dopuna   | neovlašćeno dobijanje tuđih zaštićenih podataka<br>neautorizovani pristup podacima smeštenim na elektronskim ili magnetnim medijumima ili koji nisu direktno vidljivi<br>kompjuterska zloupotreba<br>oštećenje operacija obrade podataka<br>kradja dokumenata<br>špijuniranje podataka (haking) |
| Novi Zeland  | 1990.              | Krivični zakon   | direktni ili indirektni neautorizovani pristup bilo kom kompjuterskom sistemu<br>oštećenje, uništenje ili modifikovanje podataka  |
| Norveška     | 1987.              | Krivični zakon   | razbijanje zaštite ili postizanje dobiti neautor. pristupom program. i podacima uskladišenih ili transmits. elektron. ili na drugi tehnički način   |
| Poljska      | 1993.              | Predlog Krivičnog zakona   | neautorizovan pristup infor. vršenjem prekršaja na elektron. magn. ili drugim specijalnim medijumima<br>korišćenje vizuelnih i drugih specijalnih medijumima za nedozvoljene svrhe<br>otkrivanje trećim licima informacija sačuvanih na magn. elektronskim i sl. medijumima                     |
| SAD          | 1984.<br>1986.     | Federalni Zakon o komp. prevarama i zloupotrebama                        | neautorizovani pristup kompjuteru ili njegovo korišćenje u nedozvoljene svrhe   |
| Singapur     |                    | Predlog akta   | secificirana dela kriminala vezanog za kompjutere   |
| Slovačka     | 1990.              | Krivični zakon   | povrede autorskih prava na komp. programima<br>prevare<br>neautorizovano korišćenje tuđe svojine- koja se odnosi na kompjutere<br>kršenje privatnosti<br>prikazivanje ekonomskih i poslovnih podataka (uplitanje, unošenje)   |

|                        |                                    |   |  |
|------------------------|------------------------------------|---|--|
| Švedska                | 1973.<br>1986.<br>1990.<br>1986.   | Zakon o podacima<br><br>Krivični zakon                                  | prekršaj zbog neautorizovanog pristupa zapisima u elektronskoj obradi podataka<br><br>prevare sa neautorizovanim manipulacijama informacionim procesima<br>nelojalnost prema rukovodiocu, neautorizovano korišćenje i povrede podataka |
|                        | 1992.<br>1994.<br>stupili na snagu | Komisija eksperata predlaže dopunu Zakona o podacima i Krivičnog zakona | haking<br>oštećenja podataka<br>krivitvorenje elektronskih dokumenata<br>trgovina password-ima   |
| Tajland                |                                    | Krivični zakon  | haking<br>ucene i iznudjivanja   |
| Tajvan                 | 1991.                              | Krivični zakon  | zaštita svake poslovne tajne ugrađene u računarski program   |
|                        | 1992.                              | Gradjanski zakonik  | zaštita poslovne ili industrijske tajne<br>zaštita od uništenja  |
| Velika, Britanija      | 1990.                              | Zakon o kompjuterskim zloupotrebama                                     | povreda korišćenjem bilo koje funkcije kompjutera sa namerom da se obezbedi pristup programima ili podacima koji se nalaze u bilo kom kompjuteru, neautoriz. pristup ili namera da se to uradi   |
| Viktorija (Australija) | 1988.                              | Zakon o kompjut. kriminalu  | zaštita KS od nezakonitog ulaza ili izlaza   |
| Virdžinija             |                                    | Zakon Virdžinije  | kompjuterski prekršaji (prestupi)  |

Podaci o zakonodavnim aktivnostima ukazuju da se ubacivanje i distribuiranje virusa i haking kao krivična dela, prekršaj ili prestup predviđa:

- ◆ *krivičnim zakonima*, i/ili
- ◆ *zakonima o zaštiti podataka* (uopšte ili ličnih), i/ili
- ◆ *posebnim zakonima*.

Kad su u pitanju sankcije mnoga zakonodavstva su pošla od različitih mogućnosti. U **jednoj grupi** zemalja (odredjene federalne države SAD, Florida, Arkanzas; Australija) pošlo se od *zaštite sistema i podataka* i predvidele kao inkriminisane radnje svi “namerni, svesni i neovlašćeni pristupi kompjuterima, kompjuterskom sistemu, komunikacionoj mreži ili podacima”. **Druge su zemlje** (npr. Danska, Švedska, Velika Britanija) za polazište imale *bezbednost i integritet podataka* i odredile kao kažnjive: neovlašćene pristupe za snimanje obrade elektronskih podataka, tuđim ličnim informacijama, programima, sistemima za obradu podataka, ili iniciranje da kompjuteri izvrše funkciju koja će obezbediti pristup podacima ili programima smeštenim na kompjuteru (a to bude uradjeno svesno i neovlašćeno). Naravno, posebno su zanačajna presretanja podataka kompjuterskim prisluškivanjem, ako se obavlja:

bespravno i tehničkim sredstvima. Objekt su komunikacije sa i u kompjuterskom sistemu ili mreži (po predlogu posebnog Komiteta Saveta Evrope). I, **treća grupa zemalja** (npr. Austrija, Kanada, Virdžinija u SAD, Francuska) polazi od *koncepta štete* i predviđa da ona nastaje: protivzakonitim i neovlašćenim korišćenjem kompjutera, kompjuterske mreže ili sistema za: privremeno ili trajno uklanjanje podataka ili softvera; prouzrokovanje kvarova ili zastoja brisanje ili menjanje podataka i programa; stvaranje ili menjanje finansijskih sredstava ili elektronskog transfera novca; prouzrokovanje fizičku štetu; korišćenje kompjuterskog sistema za izvršenje prekršaja, prevaru za pristup i zadržavanje u sistemu.

Sankcije su različite i kreću se od *novčanih kazni* (npr. Holandija 25.000 guldena, SAD 100.000 dolara) do *zatvora*, pri čemu se zatvor predviđa u trajanju od nekoliko meseci (npr. Danska 6 meseci, Kanada 6 meseci), do 20 godina (SAD), ali najviše njih predviđa maksimalnu kaznu od 10 godina (Kanada, V. Britanija, Holandija) zavisno od težine dela i stava zemlje prema ovom tipu kriminaliteta. Po neki zakoni, uz osnovnu kaznu, predviđaju i *meru bezbednosti* - društveno korisni rad u odredjenom trajanju (SAD).

#### 4.1.2. Kompjuterski kriminalitet i medjunarodna zaštita

Pravni sistemi, sudska praksa i sve aktivnosti vezane za otkrivanje, gonjenje i hvatanje počinilaca krivičnih dela našli su se pred ozbiljnim izazovom narastajuće pojave kompjuterskog kriminaliteta. Sve više zemalja donosi odgovarajuće nacionalne propise, ali time problem još uvek nije rešen. On se sve intenzivnije prenosi na medjunarodnu scenu. **Kompjuterski kriminalitet postaje novi oblik transnacionalnog kriminaliteta što zahteva izuzetno veliku medjunarodnu saradnju.** Medjutim, medjunarodna saradnja prolazi kroz mnogobrojne tunele nerazumevanja i nagomilanih dilema i problema koje bi trebalo brzo i efikasno rešavati. Medju mnogima, kao najznačajniji, izdvajaju se sledeći problemi<sup>163</sup>:

- ◆ *pomankanje globalne saglasnosti oko načina tretiranja i savladavanja ovog kriminaliteta;*
- ◆ *pomankanje globalne saglasnosti oko pravnog definisanja kriminalnih ponašanja;*
- ◆ *pomankanje ekspertiza u oblasti policijske, proceduralne i sudske aktivnosti;*

---

<sup>163</sup> UN Manual.

- ◆ *neodgovarajući način odredjivanja pravnih ovlašćenja u istragama pristupa kompjuterskim sistemima, uključujući i zaplenu kompjuterizovanih podataka;*
- ◆ *pomankanje harmonizacije različitih nacionalnih proceduralnih prava uključujući i isledjivanje ovog kriminaliteta;*
- ◆ *transnacionalni karakter mnogih dela kompjuterskog kriminaliteta;*
- ◆ *pomankanje dogovora oko saradnje u ekstadiciji i međusobnom pomaganju, kao i sinhronizaciji različitih pravnih mehanizama međunarodne saradnje, jer postojeće stanje ne može, na odgovarajući način, obuhvatiti svu dinamičnost i specifičnost ovih dela i teškoće oko sprovođenja istrage.*

Većina od ovih problema prisutna je od početka 80-ih, kada su i počeli prvi koraci u međunarodnoj saradnji veznoj za kompjuterski kriminalitet. A ta saradnja je počela prvo u okviru OECD-a, te se prenela na Evropsku Uniju i, naravno, pokrenula odgovarajuće mehanizme i aktivnosti OUN-a.

#### Hronologija međunarodnih aktivnosti

| Godina | Organizacija           | Aktivnosit i dokument   |
|--------|------------------------|---|
| 1983.  | OECD<br>Ad hoc Komitet | počela priprema posebne studije o mogućnostima internacionalizacije i harmonizacije krivičnog prava u vezi sa kompjuterskim kriminalitetom i zloupotrebama  |
| 1985.  | OECD<br>Komitet        | predlaže zemljama članicama da kompjuterske prevare treba da se kriminalizuju i budu predviđene nacionalnim krivičnim zakonima  |
| 1985.  | OUN                    | VII kongres: Zaštita od kriminala i tretmanu počinitelja<br>Generalni sekretar podnosi izveštaj: Predlog međunarodnih akcija protiv oblika kriminala identifikovanog u Milan planu akcija, u kom su paragrafi 42 - 44 posvećeni kompjuterskom kriminalitetu |
| 1985.  | EZ                     | osniva se Posebni komitet eksperata za kriminal vezan za kompjutere<br>Saveta Evrope<br>ovaj Komitet raspravlja pravne probleme ovog kriminaliteta  |
| 1986.  | OECD                   | objavljivanje studije: Kriminalitet vezan za kompjutere: analiza i pravna politika<br>predlaže se lista radnji koje zahtevaju jednako odredjivanje u zemljama članicama<br>osnivanje Komiteta za politiku vezanu za informacije, kompjutere i komunikacije  |
| 1986.  | Evropski Savet         | pokreće izradu sopstvene studije sa smernicama za dalji rad i rešavanje problema  |
| 1989.  | EZ<br>Savet Evrope     | usvaja Preporuku No. R(89)9 o kriminalitetu vezanom za kompjutere   |
| 1990.  | OUN                    | sastanak predstavnika Azijsko - pacifičkog regiona, u pripremi za VIII  |

|       |  |  |
|-------|--|--|
|       | Havana   | kongres, raspravlja se o uticaju tehnološkog progresa na kompjuterski kriminalitet<br>12 plenarna sednica VIII kongres: Zaštita od kriminala i tretman počinitelja, na kome predstavnici Kanade podnose predlog Rezolucije o kompjuterskom kriminalitetu<br>13 plenarna sednica - zemlje članice usvajaju Rezoluciju o kompjuterskom kriminalitetu |
| 1992. | OECD   | donosi skup smernica za ostvarivanje sigurnosti informacionih sistema u kojima značajno mesto ima i savladavanje kompjuterskog kriminaliteta   |
| 1992. | Savet Evrope                                     | pokreće studiju koja se odnosi na međunarodnu saradnju u vezi sa kompjuterskim kriminalitetom i informacionoj tehnologiji  |
| 1992. | Međunarodno udruženje krivičnog prava Wursburg   | donosi Rezoluciju vezanu za kompjuterski kriminalitet na konferenciji o kompjuterskom kriminalitetu na kojoj učestvuju delegacije zemalja Severne i Latinske Amerike, Zapadne Evrope, Srednjeg Istoka i Afrike   |
| 1994. | OUN  | Predlog Rezolucije na osnovu analiza i rada OECD i EZ i donose se smernice   |
| 1995. | EZ<br>Evropski savet                             | donosi Preporuku No. R(95)13. o sagledavanju problema u krivičnom procesnom pravu vezanim za informacionu tehnologiju  |
| 1996. | EZ<br>Pravni savetodavni odbor Evropske Komisije | organizuje Kongres o kompjuterskom kriminalitetu, novembra   |

Dakle, od međunarodnih dokumenata za rešavanje brojnih pitanja ovog specifičnog fenomena svakako da poseban značaj imaju: Rezolucija UN o kompjuterskom kriminalitetu<sup>164</sup>; Preporuka o kriminalitetu vezanom za kompjutere i Preporuka o sagledavanju problema u krivičnom procesnom pravu vezanim za informacionu tehnologiju.

**Rezolucijom o kompjuterskom kriminalitetu VIII Kongresa OUN** (*Resolution on Computer-related Crime on the 8th United National Congress on Crime and Treatment of Offenders*) predlažu se sledeće mere<sup>165</sup>:

- 1. modernizacija prava i procedura** u smislu obezbedjenja da postojeća krivična dela i prava obuhvate adekvatno osiguranje dokaza u sudskim sporovima i ukoliko je nužno menjaju svoja prava na odredjeni način; ukoliko to pravo nedostaje primenjivati opšta pravila prihvaćena ovim aktom u skladu sa sofisticirano formom aktivnosti kompjuterskih kriminalaca; i, naravno, pri donošenju novih propisa početi od rezultata do

<sup>164</sup> Rezoluciju VIII kongresa prihvatila je Generalna skupština OUN u Rezoluciji 45/121.

<sup>165</sup> UN Manual.

kojih je došla posebna Komisija za kompjuterski kriminalitet Komiteta OUN-a;

2. **poblošanje kompjuterske sigurnosti i preduzimanja preventivnih mera zaštite**, vodeći računa o problemima vezanim za: zaštitu privatnosti, ljudskih prava i osnovnih sloboda i svakom regulatorskom mehanizmu koji se odnosi na korišćenje računara;
3. **prihvatanje mera kojima će se ljudi ubediti o nužnosti zaštite od kompjuterskog kriminaliteta**;
4. **usvajanje mera neophodne obuke svih učesnika u procesu kažnjavanja vezanog za kompjuterski kriminalitet**, počevši od sudija, službenika i članova tela odgovornih za zaštitu, istragu i presudjivanje počinocima ovog kriminala;
5. **izrada i prihvatanje seta normi kompjuterske etike**, pri čemu se očekuje potpuna saradnja sa zainteresovanim organizacijama i asocijacijama i **obavezno uključivanje ovih principa i normi u redovno obrazovanje i obuku u informatici**; i
6. **prihvatanje politike da žrtve kompjuterskog kriminaliteta** koje podpadaju pod **Deklaraciju o osnovnim principima pravde za žrtve kriminala i zloupotreba OUN-a**, budu uključene u restituisanje i legalizaciju zahteva i mera za njihovo **ohrabrenje u obaveštavanju** (za to predviđenih tela) **o pretrpljenom napadu**.

Ono što je posebno ovom Rezolucijom usvojeno je preporuka Komitetu OUN-a da uspostavi međunarodnu saradnju u pripremi i izradi smernica i standarda koji će pomoći zemljama članicama u dogovaranju oko istraživanja i analize novih načina otkrivanja, praćenja i gonjenja kompjuterskih kriminalaca u budućnosti.

**Preporuka o kriminalitetu vezanom za kompjutere** i (*Recommendation No. R(89) 9 on computer-relating crime*) posebno je bitna jer daje klasifikaciju dela ovog kriminala, sa osnovnim karakteristikama<sup>166</sup>.

**Preporuka o sagledavanju problema u krivičnom procesnom pravu vezanim za informacionu tehnologiju** (*Recommendation No. R(95)13 concerning problems of criminal procedure law connected with information technology*) sadrži sedam delova: pretres i zaplena; tehnički nadzor; obaveze u saradnji sa istražnim organima; elektronski dokazi; korišćenje kriptografije; istraživanje,

<sup>166</sup> Navedene podele iz ove Preporuke date su u okviru 3. Tipična dela kompjuterskog kriminaliteta, ove knjige.

statistika i obuka; kao i međunarodna kooperacija<sup>167</sup>. Osnovni putokazi koje sadrži ova Preporuka su:

1. **nacionalna krivična prava moraju predvideti i dozvoliti istražnim organima pretragu kompjuterskog sistema i zaplenu podataka**, pri čemu se podaci koji se automatski obrađuju funkcionalno tretiraju kao tradicionalni dokumenti;
2. **mora se dozvoliti tenički nadzor u svrhu sprovođenja istrage**, prekidanjem telekomunikacija ako je to nužno i svim drugim potrebnim raspoloživim tehničkim merama za prikupljanje i odašiljanje podataka bitnih za sprovođenje istrage;
3. **obavezuju se svi subjekti koji dolaze u dodir sa istražnim organima da im omoguće lakše sprovođenje istrage**, pristupom sistemima ili vezama, a u tom cilju se obavezuju i operateri da stalno kontrolišu svoje kompjuterske sisteme i evidentiraju proveru kako bi mogli ove podatke dostaviti istražnim organima, a posebno oni u javnim i privatnim mrežama dužni su preduzimati mere sigurnosti koje će onemogućavati neovlašćeni pristup i o tome, uredno vodjene, podatke dostavljati za potrebe istrage;
4. **podaci u elektronskom obliku za prikupljanje, čuvanje i prikazivanje dokaza obezbediće se na način na koji se najbolje osigurava njihov integritet** i smatraće se autentičnim, u domaćem i međunarodnom sprovođenju istrage, uz stalnu obavezu razvijanja teničkih metoda za rukovanje njima;
5. **radi minimiziranja negativnih efekata korišćiće se kriptografija u istražnim postupcima**, ali tako da to ne utiče na legitimnost;
6. **za potrebe razvoja daljeg sagledavanja uticaja informacione tehnologije oformljene nacionalne komisije za krivična dela će se kontinuirano uključivati u praćenje ovog novog fenomena**. Za tu svrhu nužno je uspostavljanje posebnih specijalizovanih jedinica koje će se, uz stalnu obuku od strane specijalnih eksperata, uključivati u otkrivanje i praćenje ove pojave;
7. **nužna je međunarodna saradnja u identifikaciji izvora opasnosti**, naročito ukoliko su napadnuti kompjuterski sistemi locirani na različitim teritorijama i podpadaju pod različite jurisdikcije. Zbog nužnosti brzog reagovanja, mora se omogućiti pretraživanje sistema i zaplenu podataka, kao i zaustavljanje telekomunikacija.

Znači, značajni koraci u međunarodnoj saradnji i regulaciji su učinjeni - čekaju realizaciju na nacionalnom planu.

<sup>167</sup> Tekst Preporuke preuzet sa Interneta.

#### 4.1.3. *Kompjuterski kriminalitet po našem pravu*

**U našoj zemlji ne postoji zakon koji bi bio ekvivalentan navedenim zakonima i prihvaćenim rešenjima**, odnosno koji bi tretirao pitanja kreiranja i širenja računarskih virusa i kažnjavanja hakera za učinjena dela hakinga, jer do pre nekoliko godina ni sami programi nisu bili zakonski zaštićeni. Za verovati je, da će se sa sve većom primenom računara i ozbiljnijim i studioznijim pristupom ovom problemu uskoro i kod nas neminovno postaviti pitanje zakonske zaštite podataka, kompjuterskih sistema i mreža od svih onih aktivnosti koje su u drugim zemljama svrstane u kompjuterski kriminalitet, te da će, vremenom, biti doneti i odgovarajući pravni akti.

Znači, pojava i najeza raznih vrsta virusa i sve češći upadi hakera u kompjuterske i komunikacione sisteme svakako je opasnost i realnost koja pretila i nama. Da bi se opasnost sprečila i posledice umanjile, neophodno je preduzimanje niza mera i izgradnja većeg broja mehanizama. U preventivnom delovanju, pored tehničkih i organizacionih mera, značajnu ulogu imaju i pravne mere i mehanizmi, dok u lečenju posledica i kažnjavanju počinilaca najefikasnije su krivičnopravne sankcije. Pri tom, je neophodno preduzeti sledeće aktivnosti:

**Prvo. Novelirati i uskladiti naše zakone**, naročito krivične (mada pored njih trebalo bi doneti i zakone o zaštiti podataka u kojima bi se predvideli i ovi oblici njihove zloupotrebe, kao i novelirati radno zakonodavstvo) i **odgovarajuće podzakonske akte** uvođenjem nekih oblika hakinga (profesionalnog npr.) i virusa u krivična dela i/ili teže povrede radnih obaveza (ukoliko su učinjena od strane zaposlenih). Pri pripremi i izradi ovih novela neophodno je posebno voditi računa o preporukama donetim od strane odgovarajućih međunarodnih strukovnih udruženja i tela međunarodnih organizacija, kao i iskustvima informaciono razvijenih zemalja.

**Drugo. Predvideti stroge sankcije** - od kazne zatvora do novčanih kazni i zabrane vršenja delatnosti, kao i otpuštanje sa posla ukoliko su dela učinjena na radnom mestu ili su propuštene preventivne mere. Svaka od ovih kazni, zavisno od težine dela, treba da bude veoma stroga (za neka kvalifikovana dela kumulativno primenjivati kazne zatvora, novčane kazne i zabranu vršenja delatnosti) kako bi se, pored kažnjavanja počinilca, moglo zastrašujuće delovati i na potencijalne počinioc.

**Treće.** S obzirom na otežano otkrivanje dela kompjuterskog kriminaliteta **neophodno je osposobiti odgovarajuće institucije** (organe otkrivanja i gonjenja), **ali i odredjene profile informatičara - profesionalaca** koji bi mogli preventivno delovati u organizacijama i institucijama u kojima se ovi sistemi nalaze. Jedna od mogućih

aktivnosti je i predviđanje radnih mesta u okviru kojih bi se obavljali poslovi obezbeđenja sigurnosti IS. To sigurno ne bi trebalo da umanji ni ulogu menadžera koji bi, pored razumevanja opasnosti koje prete IS, trebalo i da koordiniraju aktivnost i za njihovo sprečavanje i otklanjanje. Svakako da ne bi trebalo zaboraviti ni na **pravosudne organe** koji, zbog nepoznavanja ove problematike, imaju ozbiljnih problema da završe već započete slučajeve ili će ih imati u rešavanju budućih.

**Četvrto. Nužno bi bilo formiranje odgovarajućeg ekspernog tela** (Komiteta, Odbora, Komisije) koje bi istraživalo uzroke i počiniocce, analiziralo tipove i karakteristike samih aktivnosti, i naravno, predlagalo odgovarajuće mere (pravne, organizacione i druge) za rešavanje i sprečavanje ovog kriminaliteta.

**Peto.** Sigurno da bi bilo oportuno i **medjusobno povezivanje** svih takvih institucija i organa i njihovo uključivanje u internacionalne organe, organizacije i institucije.

**Šesto. Nužno je evidentirati, pratiti i istraživati ove pojave** - što bi trebalo da obavljaju odgovarajuće organizacije (od statističkih zavoda do naučnih instituta i institucija) i organi, ali i udruženi veći proizvođači softvera i pružaoci informacionih usluga.

**Sedmo. Trebalo bi postepeno i postupno ostvariti saradnju sa žrtvama** i stvarati odgovarajuće uslove za njihovu bolju saradnju i prijavljivanje počinjenih ili pokušanih dela neautorizovanog pristupa sistemima i "ubacivanja" virusa.

I na kraju, neophodno je konstatovati da se sa pojavom fenomena kakvi su haking i virusi moramo suočiti, jer je došlo vreme kada ih moramo rešavati.

#### 4.2. *Etika i zaštita od kompjuterskog kriminaliteta*

Razvoj i primena kompjuterske i komunikacione tehnologije donela je i niz etičkih dilema. Kad je u pitanju ove tehnologije, etičke norme se postavljaju u prvi plan kod njihove primene od: **strane raznih subjekata** koji sa njom dolaze u dodir i vezu i **posebnih grupa profesionalnih informatičara**.

U prvom slučaju, glavni problem pojavljuje se u izgradjivanju i primeni opštih etičkih postulata i normi, odnosno onih koje važe za sve koji dodju u situacije za

koje su ove norme primenljive. To se naročito odnosi na sve one koji se mogu pojaviti kao **aktivni ili pasivni subjekti**<sup>168</sup> korišćenja određenog kompjuterskog programa, korišćenja ili negiranja korišćenja kompjuterskih servisa, kradje, haking, zaražavanje virusima, ažurnost i tačnost podataka i informacija, itd. Posebne etičke dileme pojavljuju se u situacijama korišćenja ove tehnologije u političke i vojne svrhe, kao i za razna praćenja ljudi. Rešavanje ovih dilema naročito je važno, jer bi trebalo da:

1. **formuliše** ponašanja pojedinaca i grupa u određenim situacijama;
2. **kanališe** moguće negativne konotacije primene kompjuterske i komunikacione tehnologije u odnosu na njegove tvorce i pasivne subjekte protiv kojih se on može usmeriti;
3. **definiše** određene situacije u kojima su etičke norme prioritete, ako ne i jedine; i
4. **ukazuje** na moguće zloupotrebe koje nisu pravom predviđene i sankcionisane.

Primeri radi, zbog navodne "više" potrebe mogu se od raznih političkih stranaka ili grupa prikupljati "poverljivi" podaci čijom kombinacijom mogu nastati teške posledice po pojedince ili druge grupe. Njihova upotreba ne mora biti regulisana pravom. Pitanje je etičkih normi da li će se to i desiti. Slično je sa mnogim zdravstvenim podacima. Neki od njih su takvi da bi se ugrozila bezbednost pojedinaca ukoliko "procure", a neki ako ostanu tajna. Oni koji do njih dodju, npr. iz naučnih razloga (a nisu lekari) na legalan način dolaze u situaciju da ako ih objave mogu izazvati paniku, a ako ih ne objave stvaraju znatne teškoće, npr. u sprečavanju zaraze. Od pojedinaca i njihove procene, šta je dobro a šta ne, zavisi i kako će se ove dileme rešavati.

Poseban problem predstavljaju virusi za koje su se duže vremena postavljala pitanja da li su kriminal, greška ili oboje. Naročito je problematična granica na kojoj se odvaja dozvoljena kompjuterska igrarija od destruktivne obesti ili namerne zločinačke aktivnosti. Izgadjivanje etičkih normi i principa u ovoj oblasti osobito je važno, ne samo zbog epidemioloških razmera koje ova pojava dobija, već i za sve one slučajeve koji se direktno ne kose sa pravom, ali mogu predstavljati i predstavljaju neodgovarajuća ponašanja.

Upravo u domen etičkih normi ulazi i slučaj "Beogradske grupe hakera" i uloge koju je modemska veza "Sezam" odigrala. Naime, da li su povredjene neke etičke norme kad se radilo o organizovanom "hakingu" u Beogradu bez obzira na njegov pozitivni kontekst. Da li je i sama aktivnost protiv nekih etičkih pravila ponašanja, i, u stvari, da li ona i postoje?

---

<sup>168</sup> Samociuk M., op. cit., str. 153.

Sva ova pitanja teško da mogu dobiti odgovore, naročito pozitivne, jer:

- a. **mnoge situacije kod nas još se nisu pojavile** pa je bilo i nemoguće formirati neki od etičkih sudova o njima;
- b. **malobrojni slučajevi za koje se zna nisu omogućili definisanje određenih etičkih principa**, čak, bi se moglo reći da je tendencija upravo suprotna;
- c. našim relativno slabo razvijenim uslovima za primenu ovih tehnologija **čini se da je više odgovaralo stvaranje takvih principa i etičkih normi koje su dozvoljavale sve ono što pravom nije bilo regulisano i predviđeno kao zabranjeno**, bez obzira na generalnu pozitivnost ovog principa, pa otuda i postojanje npr. sasvim "normalnih" situacija kopiranja, prepravljanja, poklanjanja računarskih programa na bilo koji način nabavljenih iz inostranstva ili podizanjem na pijedestal heroja svih onih koji su uspjeli da "prevare" kompjuter dajući pogrešne, zastarele ili prepravljene podatke. Ovakva ponašanja su naročito dolazila u prvi plan kad su se pojavljivali određeni subjekti, naročito pojedinci, u relaciji sa bilo kojim državnim organima;
- d. naše uobičajene težnje da u svemu budemo sami sebi dovoljni, pa inostrane vrednosti i iskustva, ma koliko oni pozitivni bili, **nisu prihvatani niti primenjivani**.

Iako je značajno izgradjivanje i primenjivanje etičkih principa i normi za subjekte koji koriste kompjutersku tehnologiju, ili na bilo koji način imaju sa njima vezu, ipak ono što bi moralo biti **prioritetno je izgradnja i primena ovih principa i normi prvenstveno od strane informatičara**. Njima su dostupne sve komponente sistema tako da je sasvim razumljivo da se oni pojavljuju kao posebno kritična grupa. Medjutim, profesija informatičara novijeg je datuma te se još uvek bori sa izgradnjom takvog kodeksa. Neke profesije, kao što su lekari ili pravnici već vekovima su uspostavljale međusobno povezana etička pravila i imale dovoljno vremena za proveru njihove adekvatnosti, kompletnosti, primenljivosti. Informatičari nisu imali ni vremena niti društveni status koji bi im pomogao da to ostvare. Naime, ova profesija, za razliku od nekih klasičnih, gotovo da nema nikakav društveni status. Najčešće se njihov status poistovećuje sa statusom inženjera, a oni su mahom u "ulozi zaposlenih koje rade za druge, a ne za sebe"<sup>169</sup>. Pored toga, pozicija "nadmoći" u koju informatičari sami stavljaju sebe u odnosu na druge doprinosi velikoj sumnjičavosti i netrpeljivosti, te otežava situaciju. U takvim uslovima izgradnja etičkog kodeksa je umnogome otežana. Svakako tome doprinosi i neshvatanje značaja oformljenih etičkih sudova i definisanih principa od strane samih informatičara.

<sup>169</sup> Forester T., Morrison P., op. cit., str. 17.

Ipak, grupe entuzijasta okupljene u profesionalne asocijacije pokušavaju da se ova stanja prevaziđu i tako, 1972. godine, nastaje **Kodeks profesionalnog ponašanja ACM** (*The Association for Computing Machinery*). To je jedan od prvih takvih kodeksa informatičara. On je, pre svega, imao za cilj uspostavljanje pravila kojima će se omogućiti priznanje profesije informatičara od strane drugih profesija uz istovremeno regulisanje određenih ponašanja članova ove organizacije koja bi mogla dovesti do gubitka poverenja od strane drugih<sup>170</sup>. Međutim, razvoj KT i pojava virusa, hakinga, softverskog piratstva, raznih oblika invazije na privatnost i mnogih drugih problema otvorili su i nove dileme i izmenjali stavove u odnosu na određene oblike ponašanja. To je oktobra 1992. godine dovelo do usvajanja revizije i noveliranog **Kodeksa etike i profesionalnog ponašanja** (*Code of Ethics and Professional Conduct*)<sup>171</sup>, ali i donošenja novih od starne drugih organizacija kao što su **IEEE** (*Institute of Electrical and Electronics Engineers*), **BCS** (*British Computer Society*), **IFIP** (*International Federation for Informing Processing*). No, i pored postojanja drugih kodeksa ipak najveći značaj, a i najkompletija odredjenja, ima ACM-ov.

Dakle, maja 1992. godine u časopisu *Communication of the ACM* pojavljuje se Predlog Kodeksa etike i profesionalnog ponašanja *ACM*. Predlog je formulisala posebna interesna grupa **SIGCAS** (*Special Interest Group on Computer and Society*). Ova verzija Predloga imala je 25 članova grupisanih u četiri dela (opšti moralni imperativi, posebne profesionalne odgovornosti, organizacioni imperativi rukovodilaca i poštovanje Kodeksa). Četvrti deo obuhvatao je i posebno Uputstvo pripremljeno da objašnjava pojmove upotrebljene u Kodeksu, a za koje se očekuje da će biti češće menjani, saglasno razvoju tehnologije i novim pojavama i sadržajima. Osim toga, na kraju je štampan formular predloga koje je trebalo da popune svi članovi *ACM* (članovi koji glasaju, članovi asocijacije i članovi studenti) ukoliko imaju određene komentare. Na osnovu svega toga 16 oktobra iste godine *Izvršni Savet ACM* usvojio je Kodeks sa 24 imperativa i Uputstvom:

### 1. Opšti moralni imperativi

- 1.1. **Doprinositi društvu i blagostanju ljudi** - osnovni cilj je minimiziranje negativnih posledica rada kompjuterskih sistema, naročito onih koje predstavljaju pretnju zdravlju i sigurnosti. Prilikom projektovanja i uvođenja sistema mora se obezbediti njihovo korišćenje na društveno odgovarajući način.
- 1.2. **Izbegavati nanošenje štete drugima** - pod štetom se podrazumevaju povrede ili negativne posledice koje nastaju za korisnike, zaposlene,

<sup>170</sup> Anderson R., Johnson D., Gotterbarn., Perrolle J., Using the New ACM Code of Ethics in Decision Making, *Communications of the ACM*, vol. 36., no. 2/93, str. 98 - 107.

<sup>171</sup> ACM Code of Ethics and Professional Conduct, *Communication of the ACM*, vol. 35., no. 5/92. str. 94 - 100.

poslodavce i ostale, kao što su nepoželjno gubljene informacija, gubitak ili oštećenje imovine i neželjene uticaje na okruženje. Informatičar ima obavezu da signalizira na moguće opasnosti kao što su: modifikacije ili uništenje podataka i programa, pojava kompjuterskih virusa i sl.

- 1.3. **Biti častan i istinoljubiv** - poštenu informatičar neće namerno lagati ili obmanjivati u vezi sistema ili njegovog projekta, naročito o mogućnostima i ograničenjima sistema, kao ni o svojim kvalifikacijama, i sl.
  - 1.4. **Biti pošten i nediskriminativan** - osnovna ideja ovog člana je tolerancija i jednaka prava za sve bez obzira na rasu, pol, veru, starost, hendikepiranost ili nacionalno poreklo.
  - 1.5. **Poštovati svojinska prava naročito autorska i patentna** - povrede patentnih ili autorskih prava, kao i poslovne tajne i ugovora o licenci u većini slučajeva su pravno nedozvoljeni, a tamo gde to nije, u suprotnosti su sa profesionalnim ponašanjem. Kopiranje softvera može biti samo sa dozvolom autora, a slično je i sa umnožavanjem drugih materijala.
  - 1.6. **Priznavati moralna prava na intelektualnoj svojini** - svaki informatičar obavezan je da zaštiti integritet autora dela intelektualne svojine, osobito ne sme "pozajmljivati" ideje ili koristiti dela bez vidljive naznake autora, čak ni onda kada ona nisu pravno na odgovarajući način zaštićena.
  - 1.7. **Poštovati privatnost drugih** - obaveza informatičara je da štiti privatnost i integritet podataka koji se odnose na pojedince. Faktički, to je poštovanje prava na informacionu privatnost.
  - 1.8. **Poštovati poverljivost** - pretpostavlja respektovanje od strane zaposlenih, klijenta i korisnika svih zahtevanih obaveza vezanih za poverljivosti informacija.
- 2. Specifična profesionalna odgovornost**
- 2.1. **Težiti da se ostvori najviši kvalitet, efektivnost i dostojanstvo procesa i proizvoda profesionalnog rada** - svaki profesionalac mora težiti kvalitetu i biti svestan negativnih posledica prouzrokovanih slabim kvalitetom sistema.
  - 2.2. **Steći i održati profesionalnu kompetenciju** - profesionalac mora učestvovati u formiranju standarda za odgovarajuće nivoe kompetencije i težiti njihovom održavanju, a to se postiže kroz pojedinačne studije, učešćem na seminarima, konferencijama i kursovima, kao i uključenjem u rad staleških organizacija.
  - 2.3. **Znati i poštovati postojeće različitosti prava u svom profesionalnom radu** - član asocijacije mora se ponašati po postojećem lokalnom, regionalnom, nacionalnom i međunarodnom

pravu osim ako mu osnovni etički principi to ne dozvoljavaju. Takođe, on mora poštovati politike i prakse organizacija čiji je član. Ukoliko se neko suprotstavi pravu ili pravilima, jer ih smatra neetičnim ili to čini iz nekog drugog razloga, mora prihvatiti kompletnu odgovornost za te svoje radnje i njihove posledice.

- 2.4. **Prihvatati i sprovoditi odgovarajuće profesionalne ocene** - kvalitetan rad zavisi od ocena i kritika profesionalne javnosti, ali kad god je to moguće član treba i da odgovarajući kritički osvrt na rad drugih.
- 2.5. **Dati odgovarajući i potpuni doprinos razvoju kompjuterskih sistema i njihovim uticajima, uključujući i analizu mogućih rizika** - od informatičara se očekuje da će biti perceptivan, temeljan i objektivan pri razvoju, preporučivanju ili prezentiranju opisa i alternativa sistema. S obzirom da je u pitanju posebno poverenje koje im se ukazuje oni imaju i posebne odgovornosti u obezbeđenju objektivne i verodostojne ocene koje prezentiraju zaposlenima, klijentima, korisnicima ili okruženju. Kad je u pitanju ocena vrednosti oni moraju identifikovati i sve postojeće i relevantne konflikte interesa i upozoravati na moguće štete ili bilo koji znak opasnosti.
- 2.6. **Poštovati ugovore, sporazume i prihvaćene odgovornosti** - profesionalac mora poštovati obaveze predviđene ugovorom. Prihvatanje sporazuma moralo bi biti samo nakon serioznih razmatranja i ukazivanja na rizike poslodavcima ili klijentu. Ako je preuzeo obaveze mora obezbediti da sistem funkcioniše kako je predviđeno. Ukoliko ne može u potpunosti zadovoljiti definisane zahteve, mora odlučiti da li će tražiti promenu sporazuma jer druga strana nije u obavezi da je prihvati. Ako se ne prihvati promena sporazuma onda je za dalje bitan njegov etički sud, a i on mora biti svestan svih konsekvenci.
- 2.7. **Doprinositi opštem razumevanju kompjuterizacije i njenih posledica** - profesionalac je u obavezi da svoje tehničko znanje razmenjuje sa okruženjem doprinoseći razumevanju kompjuterizacije, objašnjavajući njen uticaj i ograničenja.
- 2.8. **Pristupati kompjuterskim i komunikacionim resursima samo kad postoje ovlašćenja za to** - pojedinac ili organizacija može ograničiti pristup svojoj opremi (računarima, komunikacijama, softveru, podacima) sve dok to ne predstavlja diskriminaciju, jer neautorizovani pristup može dovesti do njihovog oštećenja što predstavlja nanošenje štete. Drugim rečima, niko bez dozvole ne sme pristupiti ili koristiti tuđi kompjuterski sistem, softver ili podatke.

### 3. Organizacioni imperativi rukovodilaca

- 3.1. **Jasno iskazati odgovornosti svakog člana organizacije i podsticati potpuno prihvatanje tih odgovornosti** - pošto svaka organizacija ima uticaj na okruženje njoj pripadaju i određene odgovornosti. Zato svaki rukovodilac mora podsticati njeno potpuno prihvatanje od strane zaposlenih, jer se time podiže kvalitet.
  - 3.2. **Rukovoditi zaposlenima i ostalim resursima pri projektovanju i izgradnji IS tako da to poboljša kvalitet radnih uslova** - rukovodioci su odgovorni da kompjuterski sistem poboljšava, a ne degradira, kvalitet radnih uslova. Kada se uvode računari mora se voditi računa o ličnom i profesionalnom razvoju, fizičkoj sigurnosti i dostojanstvu svih zaposlenih. Pri projektovanju sistema i uslova rada uvek se moraju uzimati u obzir odgovarajući ergonomski standardi.
  - 3.3. **Priznati i podržavati adekvatno i autorizovano korišćenje kompjutera i komunikacija u organizaciji** - računarski sistemi mogu postati moćna orudja za nanošenje štete, ali oni mogu i doprinosti dobrobiti organizacije, pa su rukovodioci dužni da jasno definišu njihovo korišćenje. Treba težiti da broj i tip ovih ograničenja bude minimalan, da bi se postigao najveći mogući efekat.
  - 3.4. **Obezbediti da korisnici i svi oni koji očekuju da im sistem zadovolji potrebe jasno iskažu svoje zahteve tokom pripreme i projektovanja** - kasnije, sistem treba da potvrdi zadovoljenje postavljenih zahteva.
  - 3.5. **Uskladiti i podržati sve one politike koje štite dostojanstvo korisnika i svih drugih koji dolaze u kontakt sa kompjuterskim sistemom** - projektovanje i implementacija sistema koji namerno ili slučajno dominiraju nad pojedincima ili grupama su etički neprihvatljivi.
  - 3.6. **Stvoriti mogućnosti članovima organizacije za učenje o principima i ograničenjima kompjuterskih sistema** - omogućavanje usavršavanja je osnova za ostvarivanje optimalnih rezultata svih zaposlenih, jer profesionalac mora biti upoznat sa opasnostima koje donose sistemi projektovani na pojednostavljenim modelima, nemogućnostima prihvatanja ili projektovanja sistema u svim radnim uslovima itd.
- 4. Poštovanje Kodeksa**
- 4.1. **Podržati i promovisati principe ovog Kodeksa** - budućnost profesije informatičara zavisi od tehničkih karakteristika i etičkih principa.
  - 4.2. **Tretirati kršenje ovog Kodeksa kao neadekvatno članstvu asocijacije** - prihvatanje ovog etičkog kodeksa od strane profesionalaca je dobrovoljno. Medjutim, ako se član ponaša suprotno Kodeksu, članstvo mu može prestati.

Pri tom, treba istaći tri bitne činjenice: **prvo**, ovi kodeksi usvojeni od velikog broja članova organizacija u SAD, V. Britaniji i u mnogim drugim zemljama, postaju principi koji imaju realne mogućnosti da postanu opšti; **drugo**, međutim, pravila koja formiraju organizacije tipa *ACM*, iako imaju izuzetnu ulogu i značaj, s obzirom da nisu snabdevena rigoroznim sankcijama, često ostaju samo gola proklamacija i "skup lepih želja"; i **treće**, parafrazirajući Bernarda Šoa da su "profesije zavere protiv ljudi" formulisanjem ovakvih etičkih pravila karakterističnih za informatičare stvaraju se istovremeno i uslovi za formiranje info-tehnokratije, koja zatvorena u svoje okvire predstavlja "koncentrat moći" i stvarnu opasnost<sup>172</sup>.

Izgradjivanje i primenjivanje etičkih principa i normi za subjekte koji koriste i komunikacionu tehnologiju ili na bilo koji način imaju sa njima vezu, a prvenstveno od strane informatičara, je značajno. **Nepostojanje kodeksa etičkih normi kod nas stvara razne mogućnosti zloupotreba koje informatičari mogu nekažnjeno činiti neosudjivani, naročito ne od pripadnika sopstvene profesije.** Sigurno da bi situacija bila mnogo jasnija kad bi se računi za neke poslove i akcije polagali pred Etičkim sudom časti i kad bi izrečene osude značile gubitak posla, nemogućnost bavljenja profesijom i sl. Tada bi i kvalitet rada i odgovornost za sopstvene greške, neznanje ili nemarnosti bile sasvim drugačije nego do sada. Odbacivanje ili osudjivanje od ljudi iz sopstvene "branše" ponekad je mnogo teže nego izdržavanje kazne zatvora ili plaćanje za nanetu materijalnu štetu. O tome treba svakako dobro razmisliti i određene korake predvideti. Tim više, što nam vreme ne ide na ruku i što ignorisanje ovakvih potreba znači i mirenje sa postojećim.

S druge strane i **hakeri** imaju svoj **Kodeks etičkih normi** (*Hacker ethic*)<sup>173</sup>. Između 70-ih i 80-ih prve generacije hakera su se oduševljavale pričama iz naučne fantastike koje su u sebi nosile "mrvice" hakerske etike u avanturama iz kibernetičkog prostora (*Cyberspace*), a koja će se artikulirati za nešto manje od jedne decenije u obostranom intervjuu između osobe pod pseudonimom **Frank Drake**, editora poznatog podzemnog časopisa *W.O.R.M.*, i **Dorothy Denning**, priznatog stručnjaka za sigurnost sistema i autora više knjiga iz ove oblasti. Intervjui su obavljani elektronskom poštom. Kasnije će stavovi F. Drake-a postati okosnica hakerske etike koje se danas pridržavaju hackeri, frekeri i krakeri, pri čemu je bitno istaći da su mnoge premise date i u objašnjenju Pamele Kane i Deborah Johnson<sup>174</sup>, koje ukazuju na

<sup>172</sup> Drakulić M., Drakulić R., U susret profesionalnoj etici informatičara - bliska budućnost ili iluzija, XXI Jugoslovenski simpozijum za operaciona istraživanja, Kotor 1994., zbornik radova SYM OP IS '94.

<sup>173</sup> Drakulić M., Drakulić R., Hakerska etika u kontekstu profesionalne etike informatičara, Zbornik radova: II naučni skup, Tehnologija, razvoj i kultura, Herceg Novi, 1996. str. 136 - 153.

<sup>174</sup> Johnson D., Computer Ethics, Englewood Cliffs, Prentice Hall, 1994., str. 103 - 124.

transformaciju naučne fantastike u hakersku filosofiju. Osnovni postulati ove etike su formulisani kroz sledećih šest pravila:

**1) Sve informacije treba da budu slobodne.** Ovo je najzanimljiviji i najvažniji argument hakera, i polazi od konstatacije da ako su sve informacije slobodne znači da su i nesvojinske, a ako su nesvojinske ne postoji ni potreba za zaštitom. Jedina zamerka je što sve informacije za sada nisu slobodne. Ovaj zahtev nosi jak intuitivni apel, posebno ako se ima u vidu fundamentalna uloga koju informacije imaju u životu svakog pojedinca. Informacije su potrebne za većinu stvari u životu, a količina i kvalitet informacija su pretpostavka kvaliteta odluke. Zapravo, svi argumenti o slobodi informacija su veoma uopšteni. Oni ne pokazuju da je potrebna sloboda svih informacija; ne pokazuju da je sloboda informacija najveća od svih vrednosti; ne pokazuju da se slobodom informacija ne može nikad trgovati. Medjutim, u mnogim zemljama postoji trgovina slobodom informacija u odredjenim oblastima u korist drugih vrednosti.

**Tri** su oblasti u kojima se nužno **prekida trgovina slobodnim informacijama**. *Prva je oblast konkurencije. Druga oblast je nacionalna sigurnosti.* Ona je izuzetno delikatna oblast, jer ciljevi nacionalnog (državnog) interesa zahtevaju čuvanje odredjenih informacija, kao strogo poverljivih, kako bi zemlja mogla nastaviti željene aktivnosti u međunarodnim i nacionalnim poslovima. Naravno, to se mora uravnotežiti u odnosu na odgovornost države prema svojim građanima<sup>175</sup>. *Treće područje je privatnost*<sup>176</sup>. Jasno je da pojedinac ima pravo na privatnost i u krajnjem slučaju baš u ovoj oblasti života postoji potreba za restrikcijama slobodnih tokova informacija.

Bez obzira na serioznost ovih protivargumenta mora se konstatovati i činjenica da hakeri ne greše uvek u zaključcima. Oni uvidjaju enormne potencijale kompjuterske tehnologije i, u vezi s tim, najvažniji hakerski zahtev - oslobodite informacije - potkrepljuju stavom da o informacionim sistemima treba razmišljati kao o javnim bibliotekama koje opstaju zbog značaja skupljenih informacija koje se u njima nalaze i kojima svaki građanin može pristupiti bez troškova i teškoća. Ipak, tamo gde hakeri greše je stav da sve informacije treba da budu slobodne, bez odredjivanja razlika

<sup>175</sup> Robertson G., Freedom, The Individual and the Law - Privacy, London, Penguin Book, 1993., str. 122 - 148.

<sup>176</sup> Michael J., Individual Rights and the Law in Britain - Privacy, Oxford, The Law Society, 1995., str. 265 - 301; Spafford E. H., Are Computers Hacker Break - ins Ethical?, The Journal of Systems and Software, no. 17/92, str. 41 - 47; Sipior J. C., Burke T. W., The Ethical and Legal Quandary of Email Privacy, Communication of the ACM, vol. 38, no. 12, December 1995, str. 48 - 54; Weisband S. P., Reinig B. A., Managing Users Perceptions of Email Privacy, Communication of the ACM, vol. 38, no. 12, December 1995, str. 40 - 47; Milberg S. J., Burke S. J., Smith H. J., Kalman E. A., Values, Personal Information Privacy, and Regulatory Approaches, Communication of the ACM, vol. 38, no. 12, December 1995, str. 65 - 74.

između tipova informacija i u pretpostavci da ni jedna druga vrednost ne treba da bude u raskoraku sa vrednošću slobodne informacije.

**2) Provale ukazuju na probleme onima koji mogu nešto da učine u vezi sigurnosti, kao i onima koji uslužuju kompjutersku "zajednicu".** Sa ovim argumentom hakeri tvrde da njihovo ponašanje čini nešto dobro. Robert Morris bazirao je svoju odbranu upravo na ovim osnovama. Pažljivim ispitivanjem može se konstatovati da je ovo slab argument za mnoge slučajeve. Još je manje prihvatljivo da je ono što rade hakeri analogno usluzi. To neodoljivo podseća na obrazloženje slično onome da radi brige o sigurnosti komšija pojedinci imaju pravo da upadaju u njihove domove da bi ispitali da li su obezbeđeni od provale. Svakako da se ne mogu usvojiti ovakvi argumenti vezani za provalnike, kao ni slični vezani za hakere. Takođe, on-line upadi, i u slučaju kada su učinjeni u cilju skretanja pažnje na mane bezbednosti, je gubljenje vremena i novca, vršenje pritiska na pojedince i organizacije da investiraju u zaštitu. Mnogi nemaju sredstva da poboljšaju sistem ili ugrade čvršću zaštitu.

**3) Hakeri ne čine štetu, odnosno ne čine štetu bez krajnje potrebe i ne menjaju ništa, oni uče.** Prvi deo ovog argumenta može se lako odbaciti, jer ne sme se zaboraviti i da su nefizička oštećenja ipak šteta, a sasvim je jasno da ljudi trpe štete od aktivnosti hakera. Ako pojedinci imaju pravo vlasništva i pravo na privatnost, onda su oni oštećeni kada im se ova prava napadaju. Šta više, hakeri mogu činiti i fizička oštećenja. Postoji mogućnost da hakeri udju u bolničke sisteme u kojima su pacijenti životno zavisni od njihovog rada ili u sisteme procesne industrije u kojima su radnici u fizičkoj opasnosti od hemikalija ili eksplozija. Hacker u takvoj situaciji ubacujući crva usporava sistem, a zna se da je za kontrolisani proces kritično vreme, jer ugrožava živote i zdravlje.

Odbrana hakera da oni uče o kompjuterskim i komunikacionim sistemima je neadekvatna. Hakeri uče mnogo o sistemima iz svojih hakerskih aktivnosti, ali i iz drugih, tako da se teško može pokazati da hakeri čine dobra dela. Da li je svaka aktivnost u kojoj se unapređuje učenje samim tim i dobra? Da li je haking jedini način za učenje o računarima? Da li je haking najbolji ili samo dobar način učenja o KT?

Nekoliko primera čini lakim odgovor na prvo od pitanja. Davanje elektro šokova učenicima kad pogreše odgovor može ubrzati učenje, ali to, svakako, nije dobar metod. Možda bi vezivanje djaka za žice kroz koje protiče električna energija dalo dobre rezultate u učenju o opasnostima od hvatanja golih žica, ali teško da bi bilo dobro. Zato i učenja kroz haking ne čini haking dobrim. Haking svakako nije jedini način učenja o kompjuterima.

Čak i kad se radi o sigurnosti haking verovatno nije najbolji način za njeno učenje, ali istini za volju, nema evidencije koja bi govorila koji bi to bio. Zbog sve veće zainteresovanosti za sigurnošću, možda bi se nešto važno i moglo naučiti od razmišljanja nekog ko pokušava da upadne u sistem. Ovakvo iskustvo bi moglo da

pomogne kompjuterskim polaznicima, ali samo uz predhodno dobijanje dozvola od onih koji poseduju sistem, tako da prava ne bi bila nasilno ugrožena, a i šteta ne bi bila naneta. Takve vežbe se nerado preporučuju zato što one ohrabruju stavove da je "zabavno" upadati u sisteme. Poenta je u odnosu hakinga, kao unapredjenja učenja, i negativnih konsekvenci. Ono što je dobro za hakere zlo je za druge jer su ugrožena njihova prava (privatnosti, vlasništva). A ovaj stav hakera da cilj opravdava sredstvo teško da se može prihvatiti.

**4) Hakeri upadaju u sisteme da bi osmatrali zloupotrebe podataka** i sa distance omogućili odbranu od Velikog brata. Ovaj argument upućuje na problem građanskih sloboda, a omogućuje hakerima da sebe predstavljaju kao zaštnike - štite tamo gde ne postoji adekvatna zaštita od strane formalnih autoriteta. Hakeri navode da štite, nekakvom vrstom zaštite, od toga. Osvajajući neautorizovanim pristupom državne ili komercijalne sisteme mogu uočiti kada je i kakva zloupotreba učinjena i to otkriti javnosti. Na taj način će biti u mogućnosti da uzbune javnost da bi zaustavili zloupotrebu.

Hakeri su u pravu kada govore da je neophodna zaštita protiv zloupotreba podataka i Velikog brata. Ali je pitanje da li je cena tolerisanja hakera veća od efekata njihove zaštite. Drugim rečima, da li hakeri rešavaju problem ili ga čine još gorim?

Mada ovaj hakerski argument jeste bitan, jer ukazuje na problem u kibernetском prostoru, ipak, izgleda kontraproduktivno da se uspeh zaštite veže za tolerisanje i opraštanje hakerisanja. Oslobađanje jednog problema pravljenjem drugih može dovesti i da se kibernetски prostor napuni nekontrolisanim brojem "zaštitnika" koji bezglavo njime tumaraju. Zašto bi briga o zloupotrebi podataka i prikrivenoj prismotri zbog "viših" ili komercijalnih interesa bila vića od zabrinutosti zbog zaštitnika koji mogu odlučiti da, u ime zaštite, nekontrolisano zaviruju u fajlove ili da lutaju po sistemima? Ovo je, ipak, grub i skup metod za izlaženje na kraj sa problemom za koji postoje i druga rešenja. Dakle, ako se postavi pitanje o najboljem načinu za sprečavanje zloupotreba podataka i državne on-line prismotre, ipak postoji više opcija umesto hakinga.

**5) Hakeri nikad ne odaju druge hakere**, što je gotovo "uobičajeno" kad su u pitanju određene, kompaktne, grupe ili slojevi, koji se međusobno čuvaju i štite. Ako se uzme u obzir i da se radi o grupi koja je na granici između legalnog i, češće, nelegalnog, onda je, čak, ovakav stav sasvim opravdan. Tim više što i kod mafije postoji ovakva obaveza, gotovo, smrtni greh. S druge strane, većina onih koji nisu zlonamerni (F. Drake smatra da je, kao i kod svega drugog, 90% hakera rdjavo i da je svega 10% intelektualna elita) veruje u dobro koje čini te je krajnje necelishodno da se međusobno odaju. Jasno je da neće ni npr. advokat bezrezervno otkriti nepoštenog kolegu, već će ga sakriti od očiju i suda javnosti, a optužiti unutar Etičkog suda advokatske komore. Odluke ovog Suda mogu biti teže i rigoroznije nego

redovnih sudova<sup>177</sup>. Naravno, to uglavnom ima smisla ukoliko se radi o hakerima ispod 18 godina, jer iznad toga oni postaju profesionalci i kriminalci i pridržavaju se upravo "zaveta ćutanja" mafije u punom smislu<sup>178</sup>.

**6) Hakeri nikad ne bi smeli da upadaju u sisteme bolnica ili nekih humanitarnih, npr. dečjih, institucija.** Pravilo je proisteklo iz masovne osude hakerskih upada u ove sisteme i raznih upozorenja na etičke implikacije ovakvih akcija. Tim više, što su se mnoge grupe javno hvalile (preko svojih časopisa, elektronske pošte) na ove upade, a što je izazvalo bes i opravdane pogrome. Ako nigde nije bila jasna granica između hakerskog dobra i zla ovde je ona postala evidentna. Ni slučaj kada je grupa hakera upala u jedan bolnički sistem ne bi li pomogla siromašnim pacijentima, koji nisu bili u mogućnosti da plate skupe terapije usled čega je dolazilo do rapidnog pogoršanja njihovog zdravlja, nije naišao na opšte odobravanje. To upravo podseća na eutanaziju ili kradje zbog dobročinstva. Sukobila se "pravičnost", kojoj teže hakeri, sa pravdom, kojoj teži društvo, a sprovode je pravnici. Kompleksnost ovih dilema ukazala je na nespremnost društva da da adekvatne etičke i pravne odgovore na ovo i slična pitanja.

Dakle, hakere treba, ponekad, posmatrati kao "dobronamerne čuvarе savesti". Bez njih ne bi moglo biti ni istinske kontrole informacionih sistema i podataka koji se u njima nalaze, često i bez dozvole i bez znanja onih na koje se odnose. Mogućnost njihovog upada i "prodora" predstavlja potencijalnu opasnost za vlasnike sistema, naročito u slučajevima kada se u bazi nalaze nedozvoljeni podaci koji se pred regularnom kontrolom skrivaju ili sklanjaju. Neočekivani napadi ni otkuda mogu se završiti obelodanjivanjem u odgovarajućim časopisima, ali i porukama koje se šalju mrežama, i koje, čak, mogu stići i do policije i drugih službi otkrivanja, praćenja i kažnjavanja. Naročito kad je ugroženo pravo na privatnost i informacionu privatnost. U većini zemalja predviđena su posebna tela koja prate ispravnost tretmana podataka o ličnosti i koja mogu preduzimati mere i pokretati sudske postupke protiv prekršilaca. Ukoliko hakeri takvim telima pošalju informacije o prekršiocima ili takve informacije pošalju "subjektima" podataka, pa oni pokrenu odgovarajuće postupke, tada je hakerska pozitivistička uloga "čuvara savesti" odigrana na pravi način.

Medjutim, negativne posledice hakovanja mnogo su veće od pozitivnih, **te je i status hakera blizak kompjuterskom podzemlju i oni sličniji kriminalcima nego dobročiniteljima**. No, postojanje ove etike, bar, unekoliko menja njihovu filosofiju i stil ponašanja i može ih približiti informatičarima.

<sup>177</sup> Drakulić M., A Step by Step Toward the Sollution - Social, Legal and Ehical Dilemmas of IT in Yugoslavija, Zbornik radova: XIII međunarodni simpozijum Komjuter na sveučilištu, Cavtat, 1991.

<sup>178</sup> Upravo na to ukazuje Drake F., u pomenutom intervjuu.

# LITERATURA

1. ACM Code of Ethics and Professional Conduct, Communication of the ACM, vol. 35., no. 5/92.
2. Aharonian G., Setting The Record Straight On Patents, Communication of ACM, vol. 34., no.1/93.
3. AIPPI, Resolution of Protection on the Computer Software and Integrated Circuit, Report Expert Committee, 1986.
4. Anderson R., Johnson D., Gotterbarn., Perrolle J., Using the New ACM Code of Ethics in Decision Making, Communications of the ACM, vol. 36., no. 2/93.
5. Anderson R., Why Cryptosystems Fail, Communications of the ACM, vol. 37., no. 11/94.
6. Arazi B., Interleaving security and efficiency considerations in the design of inexpensive IC cards, IEE Proceedings Computers and Digital Technologies, vol. 141, no. 5/94.
7. Arsić Z., Patentnopravna zaštita kompjuterskog programa, Zbornik radova, Novi Sad, Pravni fakultet u Novom Sadu, 1988.
8. Backer J. B., Introduction to Computer Crime, North-Holland, Elsevir, 1984.
9. Bainbridge D., Computers and the Law, London, Pitman Publishing, 1990.
10. Bartoš M., Međunarodno javno pravo, ugovorno pravo, Beograd, Službeni list SFRJ, 1986.
11. Beer T. A. L., National secrecy interest versus public access.
12. Bell D., The post-industrial society: a conceptual scheme, edicija Evolution of an Information Society, London, Aslib, 1987.
13. Bender C., Computer Law: Evidence and Procedure, 1978.; Bigelow, Computers and Law: An Introductory Handbook, 1966.
14. Bernachi R., Frank P., Statland N., Bernacchi On Computer Law, A Guide to the Legal and Management Aspects of Computer Technology, Boston, Little, Brown & Company, 1986.
15. Besarović V., Pravo industrijske svojine i autorsko pravo, Beograd, NIO Poslovna politika, 1984.
16. Besarović V., Prednosti autorsko-pravne zaštite računarskih programa, Beograd, Anali Pravnog fakulteta u Beogradu, br. 2-3/89.
17. Besarović V., Savremeni koncept prava industrijske svojine, edicija: Pravo industrijske svojine, Beograd, Savez inženjera i tehničara Jugoslavije, 1988.
18. Bogša A., Kratka istorija prvih dvadeset pet godina Svetske organizacije za zaštitu intelektualne svojine, Patentni glasnik, br. 2/93.
19. Bogićević Č., Nedoželjena konkurencija u radnom pravu, Privreda i pravo, br. 3-6/95.
20. Borchardt K. D., The ABC of Community Law, Luxembourg, Office for official publications of the European Communities, 1994.
21. Brown J., The current status of copyright protection for computer software and some patent parallels, London, A Frank Cass Professional Journal, Computer Law & Practice, br. 5/90.
22. Brum M., Implementation of European Data Protection Directive: The View from Denmark.
23. Burket H., Theories of information in the law, Journal of Law and Information Science, br. 2/82.
24. Burkill G., Reverse compilation of computer programs and its permissibility under the Bern Convention, A Frank Cass Professional Journal, Computer Law & Practice, no. 4/90.
25. Burnside J. W. K., The Fundamentals of Computer Technology, edicija: Essays on Computer Law, Melbourne, Longman Cheshire Pty Limited, 1990.
26. Business and Information Modeling, Trade/WP.4/R. 1090, 1994.
27. Canadian computer litigation: where we are and where we are going? - trade secret protection for information technology, 1996.
28. Cartwright P., Product Safety and Consumer Protection, The Modern Law Business, no. 58/95.
29. Catala P., Answers five questions, Agora, br. 6/83.
30. Chalton S., Gaskill, S., Data Protection Law, London, Sweet & Maxwell, 1988.
31. Chance C., Information Technology 1992, Amsterdam, Chliford Chance Publication, 1990.
32. Clark P., Hoffman L., BITS: A Smartcard Protected Operating System, Communications of the ACM, vol. 37., no. 11/94.

33. Cobbs J., Writer F., Canadian Computer Crime Legislation: A Review, Datapro Systems, Hardware & Software, CD, 1994.
34. Coldwell R. A., Computer Crime: A Social Perspective, Edicija: Essays on Computer Law, Melbourne, Longman Chechire Pty. Lim., 1990.
35. Collins W. R., Miller W. K., Spielman J. B., Wherrey P., How Good Is Good Enough?, Communication of ACM, vol. 37, no. 1/94.
36. Comments on the EC Data Protection Directive: The View from Sweden; Lloyd I., Introduction to the Data Protection Special Feature.
37. Commission of the European Communities, Brussels, 13. may 1992, COM (92) 24 Final - SYN 393.
38. Commission of the European Communities, Green Paper: Copyright and Related Rights in Information Society, Brussels, COM(95)182 final.
39. Commission of the European Communities, Proposal for a Council Directive on legal the protection of databases, COM (92), 24 Final - SYN 393.
40. Commission of the European Communities, White Paper: Growth Competitiveness, Employment - the Challenges and Ways Forward into Twenty - first Century, Corfu, ISBN 92-826-74, 1994.
41. Computer Software & Intellectual Property, Background paper, Office of Technology Assessment, Congress of United States, 1990.
42. Copyright Act of 1976., US.
43. Cornwall H., Data Theft, Computer Fraud, Industrial Espionage and Information Crime, London, A Mandarin Paperback, 1993.
44. Council Directive 92/100/EEC on rental and lending right and on certain rights related to copyright in field of intellectual property.
45. Council Directive 92/250/EEC on legal protection of computer programs.
46. Council Directive 93/98/EEC Of 29 October 1993 harmonizing the term of protection of copyright and certain rights, Official Journal of European Communities, no. L 290/9.
47. Council Directive 93/98/EEC harmonizing the term of protection of copyright and certain related rights.
48. Council Directive 95/46/EC on protection of individuals with regard to processing of personal data and the free movement of such data.
49. Council Directive on the legal protection of databases, Official Journal of the European Communities of 27/3/96 no L 77.
50. Council Directive on the Legal Protection of Topographies of Semiconductor Products (87/54/EEC).
51. Daler T., Gulbrandsen R., Melgard B., Sjolstad T., Security Of Information And Data, Chichester, Ellis Horwood Limited, 1989.
52. Denning D., A Dialog on Hacking and Security, Edicija: Computers Under Attack, Intruders, Worms, and Viruses, New York, ACM Press, 1990.
53. Denning D., The United States v. Craig Neidorf, Communications of ACM, vol. 34., No. 3/91.
54. Denning P., What is Software Quality?, Communications of ACM, vol. 35., br. 1/92.
55. Djordjević Ž., Stanković V., Obligaciono pravo, Beograd, Naučna knjiga, 1987.
56. Djurović R., Medjunarodno privredno pravo, Beograd, Savremena administracija, 1991.
57. Dossick S., User - Interface Copyrights: Obstacles to Innovation, IEEE Technology and Security Magazine, Fall 1994.
58. Doswell R., A Guide to Computer Crime Investigation, Edicija: A Handbook of Computer Security, London, Kogan Page, 1990.
59. Drakulić M., A Step by Step Toward the Sollution - Social, Legal and Ehical Dilemmas of IT in Yugoslavija, Zbornik radova: XIII medjunarodni simpozijum Komjuter na sveučilištu, Cavtat, 1991.
60. Drakulić M., Drakulić R., Hakerska etika u kontekstu profesionalne etike informatičara, Zbornik radova: II naučni skup, Tehnologija, razvoj i kultura, Herceg Novi, 1996.
61. Drakulić M., Drakulić R., U susret profesionalnoj etici informatičara - bliska budućnost ili iluzija, XXI Jugoslovenski simpozijum za operaciona istraživanja, Kotor 1994., zbornik radova SYM OP IS '94.
62. Drakulić M., GATT i Medjunarodni trgovinski aspekti prava na intelektualnu svojinu - konsekvence Urugvajске runde, Zbornik radova: Zlatibor, IV Medjunarodni Simpozijum SYM - ORG '95.

63. Drakulić M., Informacione tehnologije i privatnost, Kotor, zbornik radova sa XXI SYM-OP-IS'94.
64. Drakulić M., Kompjutersko pravo, Beograd, MST Gajić, 1992.
65. Drakulić M., Milovanović A., Nelojalna konkurencija u pravu Evropske Unije, Vrnjačka Banja, Zbornik radova: V međunarodni simpozijum SYM ORG '95.
66. Drakulić M., Modus vivendi pravne sigurnosti informacionih sistema, Zbornik radova sa: II međunarodnog simpozijuma, Menadžement i organizacija, Kopaonik 1992.
67. Drakulić M., Osnovi Poslovnog prava, Beograd, FON, 1995.
68. Drakulić M., Pravna zaštita baza podataka, Donji Milanovac, Zbornik radova: XI naučno-stručni skup Info-Teh '96, 1996.
69. Drakulić M., Pravna zaštita kompjuterskih programa, D. Milanovac, Zbornik radova: 10. YU Info-Teh '95, 1995.
70. Drakulić M., Pravni aspekti zaštite podataka u organizaciji, Beograd, I stručni skup: Zaštita podataka u računarskim sistemima, 1995.
71. Drakulić M., Pravo intelektualne svojine i zaštita topografija integrisanih kola, Beograd, Info, br. 6/95.
72. Drakulić R., Drakulić M., Mogućnosr IT prismotre - uzrok tehnostresa, Zbornik radova sa naučnog skupa: "Tehnologija, kultura i razvoj", Beograd, 1994.
73. Dreier T., Development of the Protection of Semiconductor Integrated Circuits, IIC, vol. 19., no. 4/88.
74. Dworkin G., The Patentability of Computer Software, edicija: Computer Law, London, Blackstone Press Limited, 1990.
75. Dyson E., Intellectual Property in the Net, Release, 1.0. 12./94.
76. Eaton J., Smithers J., Curan S., This is IT, A Manager's Guide to Information Technology, Oxford, Philip Allan, 1988.
77. Edwards E., Savage N., Walden I., Information Technology & The Law, Basingstoke, Macmillan Publicers LTD., 1990.
78. Eisenberg T., Gries D., Hartmanis J., Holcimb D., M. Stuart Lynn, T. Santaro, The Cornell Commission: On Morris and Warm, Edicija: Computers Under Attack, Intruders, Worms, and Viruses, New York, ACM Press, 1990.
79. Erdelez S., Kompjutersko pravo, informatičko pravo ili informacijsko pravo, Pravni vjesnik, br. 6/90.
80. Erdelez S., Prikaz i analiza autorskopravne zaštite računarskoh programa u SFRJ, Zakonitost, br. 7 - 9/90.
81. European Convention for the Protection of Human Rights and Fundamental Freedoms.
82. Everest G., Database Management, Objectives, System Functions, and Administration, New York, McGraw-Hill Book Company, 1986.
83. Evropski model EDI sporazuma Komisije EEZ o pravnim aspektima EDI, 1994, Beograd, Yu EDI forum, br. 2/94.
84. F - PROT Professional, Update Bulletin, Data Fellows, Finland, 1994.
85. Fakes A., Choosing your computer law counsel, Information Management Review, vol. 15, no. 4/88.
86. Fižgar A., O zaštiti podataka u društvenom sistemu informisanja, Beograd, Anali Pravnog fakulteta u Beogradu, br. 3 - 4/85.
87. Fidoten R., The Ethics of Information Resources, Dallas, Dallas Publ., 1990.
88. Fiedler H., A structured approach to the teaching of information policy and information law, edicija: Computer and Law, Rome, Council of Europe, 1985.
89. Fisher N., Intellectual Property Rights on the Internet (Political Topic for Succession), may 1996.
90. Forester T., Morrison P., Computer Ethics, Cautionary Tales and Ethical Dilemmas in Computing, London, Basil Blackwell, 1994.
91. Frankel Y., Herzberg A., Karger P., Krawczyk H., Kunzinger C., Yung M., Security Issues in a CDOD Wireless Network, IEEE Personal Communications, vol. 2., no. 4/95.
92. Freed R., A lawyer's guide through the computer maze, The Practical Lawyer, no. 7/60.
93. Garner R., Clipper's hidden agenda, Open Computing, vol. 11., no. 8/94.
94. GATT, Agreement of Trade-Related Aspects of Intellectual Property Rights of GATT, 1994.
95. Gemingnani M., Viruses and Criminal Law, Edicija: Computers Under Attack, Intruders, Worms, and Viruses, New York, ACM Press, 1990.

96. Ginsburg J., Kernochan J., One Hundred and Two Years Later: The US Joins The Bern Convention, RIDA, no. 141/189.
97. Goodman S. E., Press L. I., Computing in Vietnam: An Asian Tiger in the Rough, Communication of the ACM, vol.38., no.1/95.
98. Goodman S. E., Press L., International Perspectives: Computing in Vietnam: An Asian Tiger in the Rough, Communication of the ACM, vol. 38., no. 1/95.
99. Gordon S., Technologically Enabled Crime: Shifting Paradigms for the Year 2000, Computer & Security, 14 (1995).
100. Gordon S., Technologically Enabled Crime: Shifting Paradigms for the Year 2000, Computers & Security, no. 14 (1995).
101. Grebović D., Aspekti bezbednosti i EDI, Beograd, EDI i EDIFACT standardi, Brezovica, II YU EDI konferencija, 1994.
102. Greenop D., Shaping the European Information Society, British Telecommunications Engineering, vol. 14., 3/95.
103. Group on the Information Society to the Corfu European Council, Brussels, 1994.
104. Grover D., The protection of computer software - its technology and applications, Cambridge, Cambridge University Press, 1989.
105. Grupa autora, Organizing for Computer Crime: Investigation and Prosecuting, National Institute of Justice USA, 1990.
106. Guideline 3 for Data Protection Act 1984., London, The Data Protection Registrar, 1992.
107. Haynes C., The Computer Virus Protection Handbook, San Francisco, Sybex, 1990.
108. Heardnden K., Computer - Linked Crime - What is Happening?, edicija: A Handbook of Computer Security, London, Kogan Page, 1990.
109. Heinlein E., Principles of Information System Security, Computer & Security, no. 14/95.
110. Henderson G. F., Intellectual Property: Litigation, Legislation and Education : A Study of the Canadian Intellectual Property and Legation System, 1996.
111. Herweg R., Bases of Computer Viruses, Koln, Datakontext - Verlag, 1991.
112. Hill S., Smith M., Risk Management & Corporate Security, A Viable Leadership And Business Solution Designed To Enhance Corporations In The Emerging Marketplace, Computers & Security, Vol. 14., no. 2/95.
113. Hussson P., The TEDIS EDI & ISDN Initiative, Online's Conference, Hamburg, 1995 -02-6/10.
114. Ignjatović Dj., Pojmovno odredjenje kompjuterskog kriminaliteta, Anali Pravnog fakulteta u Beogradu, br.1-3/91.
115. Information Technology Trends in Central and Eastern Europe, Deloitte Touche Tohmatsu International, IDOM, 1994/1995.
116. Intellectual Property Issues in Software, Washington, National Academy Press, 1992.
117. Internal Organization and Operating Procedures for Completion of the Work Program on Legal Questions and Other Legal Issues, Trade/WP.4/R. 1071, juli 1994.
118. Johnson D., Computer Ethics, Englewood Cliffs, Prentice Hall, 1994.
119. Jovanović P., Pitanje ugovora o radu i radnog odnosa povodom predloga Zakona, Privreda i pravo, br. 3-6/95.
120. Kandić-Popović Z., Krivično-pravna zaštita privatnog života, Beograd, Anali Pravnog fakulteta u Beogradu, br. 4/88.
121. Kane P., V.I.R.U.S. Protection, Vital Information Resources Under Siege, Includes dr Panda Utilites, New York, Bantam Books, 1989.
122. Karsperson, EC Data Protection Directive, Impact on Dutch Data Protection Law; Clark, Data Protection in Republic Ireland.
123. Kavran D., Laws And Regulations Of Informations Systems Development And Operation, UN, 1987.
124. Kavran D., Pravo i regulacija zaštite podataka u informacionim sistemima, I stručni skup: Zaštita podataka u računarskim sistemima, Beograd, 1995.
125. Kavran D., Uloga prava u razvoju i funkcionisanju informacionih sistema, Beograd, Anali Pravnog fakulteta u Beogradu, br. 2 - 3/89.

126. Kirby M., Access to information and privacy: the ten information commandments, *Government Information Quarterly*, no. 3/86.
127. Klitzke A., Trade Secrets: Important Quasi - Property Rights, *The Business Lawyer*, no. 4/86.
128. Knoppers J., Information law and information management, *Information Management Review*, br. 1/86.
129. Kotov V., Project Start, *Communications of the ACM*, vol. 34., no. 6/91.
130. Krčevinac S., Informacione tehnologije u centralnoj i istočnoj Evropi, Donji Milanovac, Zbornik radova sa XI Info -Teh, 1996.
131. Krivični zakon republike Srbije, Službeni glasnik RC, br. 26/77; 43/77; 20/79; 24/84; 39/86; 51/87/6/89; 42/89; 21/90; 49/93; 67/93; 47/94.
132. Krivični zakon Savezne Republike Jugoslavije, Službeni list SFRJ, br. 44/76; 34/84; 57/89; 3/90; 38/90.
133. Krušić M., Iskustva GSUP-a Beograd u otkrivanju novih pojava oblika krivičnih dela iz oblasti privrednog kriminaliteta u poslovnim bankama, *Bezbednost*, br. 2/86.
134. Lazarević B., Drakulić M., Razvoj informacionog sistema kao inovativna delatnost, Edicija: Menadžment u funkciji inovacija, Beograd, Centar za menadžment Univerziteta u Beogradu, 1995.
135. Legal Aspects of Trade Data Interchange, Trade/WP.4/R. 1096., od 22 jula 1994.
136. Lehman B., Baker J., Oblon M., Intellectual Property and National Information Infrastructure (The White Paper).
137. Leonard P., Contracting with Staff and Consultants in Information Industry, Edicija: Essays on Computer Law, Melbourne, Longman Chechire PTY Limited, 1990.
138. Lilić S. i grupa autora, Zaštita podataka u kompjuterizovanim informacionim sistemima, uporedno-pravna analiza, Beograd, Institut za uporedno pravo, 1987.
139. Lilić S., Izazov pravne informatike, *Informatika, privreda, pravo*, br. 1/90.
140. Lilić S., *Pravna informatika*, Beograd, Zavod za izdavanje udžbenika i nastavnih sredstava, 1991.
141. Lipner S., Kalman S., *Computer Law, Cases and Materials*, Columbus, Merrill Publishing Company, 1989.
142. Lloyd I., *Information Technology Law*, London, Batterworth, 1993.
143. Lobel F., *Foiling The System Breakers*, New York, McGraw Hill Book Company, 1986.
144. Lopandić D., Janjević M., Ugovor o Evropskoj uniji, od Rima do Mastrohta, Beograd, Međunarodna politika, Pravni fakultet, Fakultet političkih nauka, Institut ekonomskih nauka, Evropski pokret u Srbiji, 1995.
145. Mandell M., The West German Hacker Incident and Other Intrusions, Edicija: Computers Under Attack, Intruders, Worms, and Viruses.
146. Manigodić M., Robni i uslužni žigovi, Beograd, Pronalazaštvo, 1989.
147. Manley W, II, Shrode W., Critical Issues in Business Conduct, Legal, Ethical and Social Challenges for the 1990s, New York, Quorum Book, 1989.
148. Marković N., Zaštita ličnih podataka, I stručni skup: Zaštita podataka u računarskim sistemima, Beograd, Savez inženjera i tehničara Srbije, 1995.
149. Marković S., Obrazloženje Nacrta Zakona o autorskom pravu i susednim pravima, Savezno ministarstvo za razvoj, nauku i životnu sredinu, septembar, 1995.
150. Martin J., *Information Engineering*, Washington, Prentice Hall, 1990.
151. Marx P., The legal risk of using information as a comparative weapon, *Information Management Review*, no. 8/87.
152. Mathijsen P. S. R. F., *A Guide to European Union Law*, London, Sweet & Maxwell, 1995.
153. Mawrey R., Salmon K., *Computers and the Law*, Oxford, BSP Professional Books, 1988.
154. McDonagh M., Access to public sector information: the Australian experience.
155. McFarlane G., *A Practical Introduction to Copyright*, London, Waterlow Publishers, 1989.
156. McKnight G., *Computer Crime*, London, Michael Joseph, 1973.
157. Mecanović I., Informatičko pravo - nova grana prava u nastajanju, *Pravni vjesnik*, br. 6/90.
158. Michael J., Individual Rights and the Law in Britain - Privacy, Oxford, The Law Society, 1995.
159. Milberg S. J., Burke S. J., Smith H. J., Kalman E. A., Values, Personal Information Privacy, and Regulatory Approaches, *Communication of the ACM*, vol. 38, no. 12/95.

160. Milberg S. J., Burke S. J., Smith H. J., Kalman E. A., Values, Personal Information Privacy, and Regulatory Approaches, *Communication of the ACM*, vol. 38, no. 12/95.
161. Milić D., Komentar Zakona o autorskom pravu, sa sudskom praksom, Beograd, Službeni list, 1987.
162. Miller J., Recent Developments in Computer Law in New Zeland, edicija: Essays on Computer Law, Melbourne, Longman Professional, 1990.
163. Milošević M., Elektronska razmena podataka u Evropskoj Uniji, III YU EDI konferencija, Beograd, 1995.
164. Mohrenschlager M., Hacking: To Criminalize Or Not? - Suggestions For The Legislature, *Computers & Security*, Vol. 14., no. 2/95.
165. Muftić S., Sigurnost kompjuterskih sistema, Sarajevo, Zavod za ekonomsko planiranje, 1979.
166. Murphy B., The International Politics of New Information Technology, London, Crom Helm, 1986.
167. Mylott T., Computer Law for Computer Professionals, New York, Prentice Hall, 1984.
168. Nedin Z., Pravne prepreke razvoju EDI, Brezovica, Prva Yu EDI konferencija, 1993.
169. Nikolić D., Pravo, informacija, Novi Sad, Narodna tehnika Vojvodine, 1990.
170. Norderhaug T., Oberding J., Designing a web of intellectual property, *Computer Networks and ISDN Systems*, no. 27/95.
171. Norton H., Informatics In Europe, Manchester, NCC Blackwell, 1991.
172. Norton H., Informatics In Europe, Preparing for the Global Market, Oxford, NCC Blackwell, 1991.
173. Pallmer I. C., Potter G. A., Computer Security Risk Management, London, Jessica Kinglley Publishers, 1989.
174. Parać Z., Kompjuterski program - autorsko djelo i u jugoslovenskom autorskopravnom režimu, Zbornik referata: Posvetovanja Pravni aspekti varstva in uporabe računalniških programov in podatkovnih baz, Nova Gorica, 1988.
175. Pariska Konvencija za zaštitu industrijske svojine, od 20 marta 1983., Medjunarodni ugovori i drugi sporazumi, Službeni list SFRJ, br. 20/74.
176. Parker D., Computer Abuse, Perpetrators and Vulnerabilities of Computer System, Menlo Park California, Stanford Research Institute, 1995.
177. Parker D., Demonstrating the Elements of Information Security with Treats, National Computer Security Conference, Baltimore, 1995.
178. Parker D., Fighting Computer Crime, New York, Charles Scribner's Sons, 1988.
179. Pearson E. H., White A., Recent Developments In Computer Law in the US, edicija: Essays of Computer Law, Melbourne, Longman Professional, 1990.
180. Peckitt R., Computers In General Practice, Wilmslow, Sigma Press, 1989.
181. Peritt H. H., Reinventing Government Through Information Technology.
182. Petrović S., Jirić V., Zaštita podataka u automatizovanim informacionim sistemima, Beograd, Naučna knjiga, 1986.
183. Pfleeger C., Security in Computing, Engelwood Clifts, Prentice - Hall International, inc., 1989.
184. Powers M., Chenel P., Crow G., Structured Systems Development, Analysis, Design, Implementation, Boston, Boyd&Fraster Publishing Company, 1990.
185. Prednacrt zakona o pravnoj zaštiti topografija integrisanih kola, Savezno ministarstvo za razvoj, nauku i životnu sredinu, Savezni zavod za intelektualnu svojinu, avgusta 1996.
186. Prednacrt Zakona o autorskom pravu i susednim pravima, Beograd, 1994.
187. Press L., Personnel Computers and the World Software Market, *Communications of the ACM*, vol.34., no. 34/91.
188. Prinsley M., S. Baxster, The proposed European Directive on the legal protection of computer programs, London, A Frank Cass Professional Journal, *Computer Law & Practice*, no. 6/90.
189. Rasch M., Computer Criminal Law and Federal Sentencing Guidelines, Datapro Systems, Hardware & Software, CD, 1994.
190. Raymond E., Steel G., The New Hacker's Dictionary, Cambridge, MIT Press MA., 1991.
191. Recommendation to Member States OJ. 1981. L 246/31.
192. Reed C., Computer Law, London, Bleckstone Press Limited, 1993.
193. Reichman J. H., Uticaj TRIPS Nacrta ugovora na konkurentnost zemalja u razvoju na integrisanom svetskom tržištu, Patentni glasnik, br. 1/94.

194. Report of Intellectual Property Rights Sub - Group on Intellectual Property Rights to the DTI Multimedia Industry Advisory Group, UK, 1995.
195. Reports on the Working Conference of the EC Data Protection Directive, Hanover, 1996.
196. Rickestone S., Copyright and Data Bases, Edicija: Essays on Computer Law, Melbourne, Longman Chechire PTY Limited, 1990.
197. Roberts R., Compute!'s Computer Viruses, Greensboro, Compute! Books, 1988.
198. Roberts R., Kane P., Compute!'s Computer Security, Greensboro, Compute! Books, 1989.
199. Robertson G., Freedom, The Individual and the Law - Privacy, London, Penguin Book, 1993.
200. Rotenberg M., Communications Privacy: Implications For Network Design, Communication, vol. 36, no. 8/93.
201. Samociuk M., Hacking, Edicija: The Protection of Computer Software - its technology and applications, Cambridge, Cambridge University Press, The British Computer Society, 1989.
202. Samuelson P., Computers Viruses and Worms: Wrong, Crime, or Both, Edicija: Computers Under Attack, Intruders, Worms, and Viruses, New York, ACM Press, 1990.
203. Samuelson P., Copyright Law and Electronic Compilations of Data, Communications of the ACM, no. 2/92.
204. Samuelson P., Denber M., Glushko N., Developments on the Intellectual Property Front, Communication of ACM, vol. 34, no. 6/92.
205. Samuelson P., First Amendment Rights For Information Providers, Communication, vol. 34, no. 6/91.
206. Samuelson P., How to Interpret the Lotus Design (And How Not To), Communications of ACM, no. 11/90.
207. Samuelson P., The Ups and Downs of Look and Feel, Communications of ACM, vol. 43, no. 4/93.
208. Savić N., Pitić G., Vodič za beli papir Evropske unije, Beograd, Poslovni krug, 1995.
209. Savić Z., Potpis i potvrđivanje verodostojnosti dokumenata, Brezovica, Druga YUEDI konferencija, 1994.
210. Savić Z., Razvoj sistema zaštite informacij u EDI okruženju, III YU EDI Konferencija, Beograd, 1995.
211. Saxby S., The role of law in the development of the information society, Pravni vijesnik, br. 6/90.
212. Scott M., Computer Law, New York, Wiley Law Publications, 1987.
213. Seipel P., Computing Law: perspectives on the new legal discipline, Stockholm, Liberfoerlag, 1977.
214. Seipel P., Public access to public -held information and dissemination policy - the Swedish experience.
215. Sharpe D., Asia - Pacific Computer Misuse Legislation, Datapro Systems, Hardware & Software, CD, 1994.
216. Shirey R., Security Requirements for network management data, Computer Standards & Interfaces, no. 17/95.
217. Sieber U., The Handbook on Computer Crime, Chichester, John Wiley & Sons, 1986.
218. Sieber U., The International Handbook Of Computer Crime, Chichester, John Wiley&Sons, 1991.
219. Simsons J. F., Semiconductor Chip Protection and Sui Generis Legislation, edicija: Essays on Computer Law, Melbourne, Longman Chechire Pty Limited, 1990.
220. Singleton S., Introduction to Competition Law, Pitman Publishing, London, 1992.
221. Sipior J. C., Burke T. W., The Ethical and Legal Quandary of Email Privacy, Communication of the ACM, vol. 38, no. 12/95.
222. Sipior J. C., Burke T. W., The Ethical and Legal Quandary of Email Privacy, Communication of the ACM, vol. 38, no. 12, December 1995.
223. Smith D., Simon S., Cautilli L., Trials of Wireless, Secure Electronic Mail, IEEE Personal Communications, vol. 2., no. 4/95.
224. Spafford E. H., Are Computers Hacker Break - ins Ethical?, The Journal of Systems and Software, no. 17/92.
225. Spafford E. H., Heaphy K. A., Ferbach D. J., A Computer Virus Primer, Edicija: Computers Under Attack, Intruders, Worms, and Viruses, New York, ACM Press, 1990.
226. Sterling B., The Hackers Crashdown: Law and Disorder on the Electronic Frontier, electronic book, 1994.

227. Stoch J. F., Hupp J. A., The Worm Programs - Early Experience with a Distributed Computation, edicija Computers Under Attack, Intruders, Worms, and Viruses, New York, ACM Press, 1990.
228. Stojčić Z., EDI i razlozi njene primene, Brezovica, Prva YU EDI konferencija, 1993.
229. Stojković G., Drakulić M., Da li haking i virusi prete i našim informacionim sistemima, Zbornik radova sa II međunarodnog simpozijuma Menadžment i organizacija, Kopaonik, 1991.
230. Šturm L., Pravni aspekti zaštite podataka u savremenim informacionim sistemima, Beograd, Anali Pravnog fakulteta u Beogradu, br. 6/86.
231. Tamaki Y., Zaštita poslovnih tajni u Japanu, Podlistak Patentnog glasnika, br. 1/93.
232. Tantam M., European Computer Misuse Legislation, Datapro Systems, Hardware & Software, CD, 1994.
233. Tapper C., Computer Law, London, Longman, 1989.
234. Tapper C., Legal Problems Posed by Computers International Consideration, edicija: Essays on Computer Law, Melbourne, Longman Professional, 1990.
235. Totić B., Nacrt Ugovora o rešavanju sporova između država u oblasti intelektualne svojine, Patentni glasnik, br. 1/92.
236. Treaty on the Protection of Intellectual Property in Respect of Integrated.
237. United Nations Manual on the prevention and control of computer-related.
238. Unković D., Strategija i tehnika zaštite poslovnih tajni, Beograd, Savremena administracija, 1989.
239. Uredba o obezbeđenju i zaštiti informacionih sistema državnih organa, čl. 4., Službeni glasnik SRS, br. 41/90.
240. Uredba o ratifikaciji Pariska konvencija za zaštitu industrijske svojine, Službeni list SFRJ, Međunarodni ugovori i drugi sporazumi, br. 5/74.
241. US Copyright Act, As Amended.
242. Ustavni zakon doneti su na Saveznom veću Savezne skupštine SFRJ 27 aprila 1992, a objavljeni u Službenom listu SRJ, br. 1/92.
243. Vasiljević M., Trgovinsko pravo, Beograd, ABC Glas, 1992.
244. Vebber D., Patents and Trade Marks for Hardware and Software, edicija: Essays on Computer Law, Melbourne, Longman Professional, Pty, 1990.
245. Velašević D., Jovanović Z., Gajin S., Milojević I., Sigurnost i zaštita u računarskim mrežama, Zbornik radova sa I stručnog skupa: Zaštita podataka u računarskim sistemima, Beograd, 1995.
246. Velašević D., Osnovni pojmovi i struktura zaštite podataka u računarskim sistemima, I stručni skup: Zaštita podataka u računarskim sistemima, Beograd, 1995.
247. Velašević D., Problemi i analiza zaštite podataka u računarskim sistemima; XI naučno - stručni skup Info - Teh '96, Donji Milanovac, 1996.
248. Vilus J., Evropski model EDI sporazume, (prevod), Yu EDI Forum, br. 2/94,
249. Vilus J., Gradjanskopravna odgovornost učesnika u EDI prenosima, Brezovica, Druga YU EDI konferencija, 1994.
250. Vodinelić V., Metodika otkrivanja, dokazivanja i razjašnjavanja računarskog kriminaliteta, Priručnik, 4/90.
251. Walden I, EDI and the Law, London, Bienheim Online, 1989.
252. Weatherill S., Cases and Materials on the EC Law, London, Blackstone Press Limited, 1992..
253. Weinberg G., Geller D., Computer Information Systems, An Introduction to Data Processing, Boston, Little, Brown and Company, 1985.
254. Weisband S. P., Reinig B. A., Managing Users Perceptions of Email Privacy, Communication of the ACM, vol. 38, no. 12/95.
255. Weissenberg P., Opening Speech, Conference: Access To Public Information: A Key To Commercial Growth And Electronic Democracy, Stockholm, 1996.
256. White S. R., Chese D. M., Kuo C. J., Copin with Computer Viruses and Related Problems, Research Report online version on CHESŠIBM.COM, 1989.
257. Whitfild N., Net Answers, Personal Computer World, 1996.
258. Wiebe A., Harmonization of Data Protection Law in Europe, Report on the Working Conference of the EC Data Protection Directive, Hanover, 1996.
259. Wilkes J., Privacy and Authentication Needs of PCs, IEEE Personal Communications, vol. 2. no. 4/95.

260. WIPO, Model Provisions on the Computer Software, Industrial Property, 1977.
261. WIPO, Treaty on the Protection of Intellectual Property in Respect of Integrated Circuits, 1989.
262. Wolfe H., Computer Security: For Fun and Profit, Computer & Security, no. 14/95.
263. Wolinsky C., Sylvester J., Privacy in the Telecommunications Age, Communication, vol. 35, no. 2/92.
264. Word G. H., Shriver R. F., Computer Crime Techniques Prevention, Illinois, Bankers Publishing Co., 1987.
265. World H. G., Shriver F. R., Computer Crime Techniques Prevention, Rolling Meadows, Bankers Publishing Company, 1989.
266. Zakon o autorskom pravu, Službeni list SFRJ, br. 19/78; 24/86; 21/90.
267. Zakon o društvenom sistemu informisanja Srbije, Službeni glasnik SRS, br. 49/89.
268. Zakon o informacionom sistemu Republike Srbije, Službeni glasnik RS, br. 12/96.
269. Zakon o izmenama i dopunama Zakona o radnim odnosima, Službeni glasnik RS, br. 24/96.
270. Zakon o osnovama radnog odnosa, Službeni list SRJ, br. 29/96.
271. Zakon o osnovama društvenog sistema informisanja i o informacionom sistemu federacije, Službeni list SFRJ, br. 68/81.
272. Zakon o patentima, Službeni list SR Jugoslavije, br. 15/95.
273. Zakon o preduzećima, Službeni list SRJ, br. 29/96.
274. Zakon o suzbijanju nelojalne utakmice i monopolističkih sporazuma, Službeni list SFRJ, br. 32/74.
275. Zakon o trgovini, Službeni list SRJ, br. 32/93.
276. Zakona o izmenama i dopunama Krivičnog zakona Republike Srbije, Službeni Glasnik R.S., br. 47/94.
277. Zakon o izmenama Krivičnog zakona Socijalističke Republike promenjen je naziv u Krivični zakon Republike Srbije, Službeni glasnik RC, br. 42/92.
278. Zlatković T., Haking kao kompjuterski kriminal, diplomski rad, Beograd, FON, 1996.
279. Živanović T., Krivično pravo, Beograd, Gundulić, 1935.