Etika, privatnost i zaštita intelektualne svojine

Etika

Pod etikom (moralom) podrazumevamo niz principa ispravnog i neispravnog, na osnovu kojih formiramo svoje ponašanje odnosno skup pravila ponašanja i vođenja poslova koje bi ljudi trebalo da poštuju. S obzirom da nije uvek jasno šta je ispravno a šta ne, mnoge kompanije i organizacije stvaraju sopstvene grupe pravila – etičke kodekse. **Etički kodeks** je skup principa koji članovima kompanije ili organizacije služe kao odrednica prilikom donošenja odluka. Jedno od osnovnih načela etike su odgovornost za sopstvene postupke odnosno činjenica da pojedinac prihvata da snosi posledice za svoje odluke i ponašanje. Osim toga, veoma važni aspekti etike i svakog etičkog kodeksa su poštovanje privatnosti i prava drugih, poštovanje prava svojine, savesnog odnosa prema imovini, lično poštenje, itd.

Treba naglastiti da etiku ne treba poistovećivati sa zakonima, jer ono što je nemoralno ne mora u svakom slučaju biti i nezakonito, i obrnuto. Neka od etičkih pitanja, vezana za informatički sektor, su npr. da li zaposleni mogu da računar i softver kompanije koriste u privatne svrhe ili da li preko službene e-mail adrese mogu da razmenjuju privatne poruke, imaju li pravo rukovodioci kompanije da čitaju te poruke, itd.

Privatnost

Jedno od ključnih etičkih pitanja je i pitanje privatnosti. **Privatnost** je pravo pojednica da ne bude uznemiravan i da bude oslobođen od bilo kakvog i bilo čijeg uplitanja u lične stvari [Turban]. Privatnost informacija je pravo pojednica da odredi kada i u kojoj meri informacije o njemu mogu da se preuzmu i da se distribuiraju drugima.

Napredak informaciono-komunikacionih tehnologija poslednjih godina omogućava efikasno prikupljanje i čuvanje velike količine podataka o svakom pojedincu ili organizaciji. Gotovo svakodnevno ljudi ostavljaju svoje podatke ne samo u okviru zvaničnih institucija (državni organi kao što su školstvo, zdravstvo, policija, sudstvo, opštinska administracija, zatim banke, osiguravajuća društva, trgovine), već vrlo često i putem interneta. Svakodnevno korišćenje mobilnog telefona ostavlja trag u bazi podataka mobilnog operatera, koji ne samo da zna sa kim i koliko dugo je korisnik razgovarao, već i lokaciju sa koje je razgovarao i kuda se kretao i kada nije razgovarao (u nekim zemljama se smatra se je poznavanje lokacije korisnika na osnovu signala sa njegovog mobilnog telefona nedozvoljeno zadiranje u privatnost pojednica; ipak ova karakteristika se pokazala kao vrlo korisna u pronaženju nestalih lica u slučajevima prirodnih katastrofa ili otmica). Korišćenje kreditne kartice na bankomatu, u prodavnici ili na internetu takođe ostavlja jasan trag i mnoštvo ličnih informacija. U našoj zemlji od 2005. godine, pri Udruženju banaka Srbije, radi Kreditni biro, u kome se prikupljaju informacije o svim odobrenim kreditima i kreditnim karticama korisnika na teritoriji Srbije, tako da banka, pri odobravanju novog kredita, uvek prvo zatraži izveštaj za klijenta od Kreditnog biroa, kako bi procenila njegovu kreditnu sposobnost za novi kredit. Svi navedeni podaci mogu bili ukradeni iz centralnih baza ili na neki drugi način zloupotrebljeni, ozbiljno narušavajući privatnost ljudi.

Na osnovu svih ovih podataka moguće je napraviti digitalni dosije pojednica, odnosno elektronski opis korisnika i njegovih navika. U nekim zemljama, pre svega SAD, postoje kompanije koje rade na kreiranju profila odnosno digitalnih dosijea pojedinaca, na osnovu najrazličitijih informacija, počev od prezimena i imena, adrese, matičnog broja, obrazovanja, posedovanih nekretnina i vozila, preko finansijske aktivnosti (računi, kartice i transakcije u bankama) do elemenata policijskog dosijea odnosno podataka o eventualnim prekršajima. Podaci se prikupljaju za najrazličitijih mesta i integrišu u jedinstveni dosije pojedinca, koji zatim kompanija prodaje drugim kompanijama (npr. za proveru podataka o potencijalnim

kandidatima za zaposlenje) ili organizacijama (ovi podaci se mogu koristiti i kao osnova u nekim istragama i sudskim postupcima).

Sam pristup internetu takođe ostavlja mnoštvo podataka o korisniku (setite se samo koliko puta ste popunjavali razne formulare prilikom registracije na neki sajt). I ovde postoje kompanije koje prikupljaju podatke o korisnicima interneta, njihovim e-mail adresama, navikama, sajtovima koje posećuju i proizvodima i uslugama koje kupuju na internetu, i ovako prikupljene podatke često prodaju drugim kompanijama koje onda korisnicima nude proizvode i usluge za koje su potencijalno zainteresovani.

S tim u vezi navedimo još jedan primer narušavanja privatnosti, a to je neželjena elektronska pošta (spam, junk e-mail), koja najčešće služi za reklamiranje proizvoda i usluga. Preko 50% spam poruka se odnosi na reklamiranje farmaceutskih proizvoda. Spam je vrlo ozbiljan problem, jer osim što dosađuje korisnicima, oduzima i vreme i novac, pre svega zbog pada produktivnosti, zagušenja sistema elektronske pošte, angažovanja dodatnog memorijskog prostora, korišćenja anti-spam softvera, a neke spam poruke mogu sadržati i crve i viruse. Pojedne kompanije i poruke nude mogućnost skidanja sa mailing liste, i prekida daljeg prijema neželjene pošte, ali to nije slučaj sa svim porukama.

Još jedno od važnih pitanja vezano za privatnost zaposlenih i etiku je i elektronski nadzor. Naime, mnoge kompanije, ali i vladine institucije, nadziru rad svojih zaposlenih, odnosno njihovu elektronsku poštu, sajtove koje posećuju za vreme radnog vremena (u SAD, više od tri četvrtine organizacija), čak i kontrolišu sadržaj njihovih službenih računara. Pitanje je da li je na ovaj način ugrožena privatnost pojednica ili je to legitimna aktivnost poslodavca i vlasnika informatičkih resursa. U svakom slučaju, treba naći pravi balans između lične privatnosti i opštih interesa, naročito kada se vodi računa o nacionalnoj bezbednosti.

U narušavanje privatnosti spada i iznošenje neistina o nekoj osobi ili instituciji. Naime, na raznim sajtovima društvenih mreža (Facebook, MySpace, Twitter, itd) ili blogovima, moguće je postaviti neistinite ili uvredljive informacije o nekoj osobi, na koje ona ne može da utiče niti ih demantuje. S obzirom na karakter (mreža bez granica) i rasprostranjenost Interneta teško je i pravno se zaštititi od ovakvih napada, jer sajtovi i njihovi serveri mogu biti postavljeni u udaljenim zemljama. U Americi, skoro polovina kompanija pri zapošljavanju novih kandidata koristi internet i Google kako bi saznali više informacija o njima i ukoliko postoje neke neprimerene i neprijatne informacije, iako možda netačne, one mogu presudno uticati na stav poslodavca.

Ozbiljne kompanije znaju da moraju da poštuju pravo privatnosti svake osobe i zato nije retkost da donose sopstvenu politiku ili **kodeks privatnosti**, koji sadrži skup smernica na zaštiti privatnosti kupaca, klijenata i zaposlenih. Ispravno definisana i primenjena politika privatnosti može pomoći kompanijama da izbegnu pravne probleme. U praksi postoje dva modela po kojima kompanija omogućava klijentu da se ogradi, odnosno onemogući kompaniji dalje prikupljanje ili slanje informacija, uključujući i reklamni materijal.

Prvi model, model ograđivanja (opt-out model), dozvoljava kompaniji da prikuplja lične podatke klijenta ili da mu šalje razne informacije, sve dok kupac ne zatraži da to prekine. Najčešće na dnu reklamnih e-mail poruka se nalazi link na kome se klijent nože da se odjavi sa mailing liste, tj. prekine dalju komunikaciju sa kompanijom. Ovaj model je zastupljen u SAD.

Kod drugog modela, modela pristanka (opt-in modela), kompanijama je zabranjeno da prikupljanju lične podatke klijenata ili da im šalju reklamne poruke ili informacije sve dok klijent to lično ne odobri, najčešće prijavljivanjem na sajtu kompanije ili potvrđivanjem primljene poruke od kompanije. Ovaj model je znatno prihvatljiviji zagovornicima zaštite privatnosti i zastupljeniji je u Evropi.

Jedan od velikih problema je nepostojanje jedinstvenih standarda i zakona u pogledu zaštite privatnosti, na svetskom nivou. Iako u mnogim zemljama postoje zakoni o zaštiti privatnosti, koji obuhvataju i informatički aspekt, ovi zakoni su često neusklađeni, a i s obzirom da se sadržaji na internetu koji se pregledaju u jednoj zemlji mogu nalaziti na serverema koji su u nekoj drugoj zemlji, opravdano je pitanje ko i koje zakone može i treba da primeni. Takođe, mnoge multinacionalne kompanije mogu imati problema u prilagođavanju svog poslovanja lokalnim zakonima o privatnosti i bezbednosti, kao i u prenosu podataka o klijentima iz jedne zemlje u drugu.

Intelektualna svojina

Jedno od ključnih savremenih pitanja u oblasti informaciono-komunikacionih tehnologija, ne samo etičko već i pravno, je pitanje zaštite intelektualne svojine. Pod intelektualnom svojinom porazumevamo implementirano znanje i intelektualni rad vlasnika, koje je zaštićeno zakonima o zaštiti poslovnih tajni, patenata i autorskih prava.

Poslovna tajna je intelektualni rad grupe ili pojednica, kao što je poslovni plan (npr. strateški plan razvoja kompanije), koji je tajna kompanije i nije zasnovan samo na javno dostupnim informacijama. Patent je dokument kojim se vlasniku garantuje ekskluzivno pravo na korišćenje otkrića (izuma ili procesa) u nekom vremenskom periodu (najčešće 20 godina). Patenti se registruju u nacionalnim institucijama (zavodima) za patente, a štite se posebim zakonima.

Autorska prava (Copyright) su prava zagarantovana zakonom, koja stvaraocu intelektualne svojine garantuju vlasništvo nad svojinom kao i sva prava koja iz toga proističu (npr. vlasnik ima pravo da naplaćuje kopiranje ili korišćenje njegovog dela).

U oblasti informaciono-komunikacionih tehnologija dva najznačajnija oblika intelektualne svojine su softver i multimedijski sadržaji u digitalnom obliku. Pod digitalnom piraterijom se podrazumeva izrada nelegalnih kopija digitalnih proizvoda i informacija, zaštićenih autorskim pravima.

Softverska piraterija

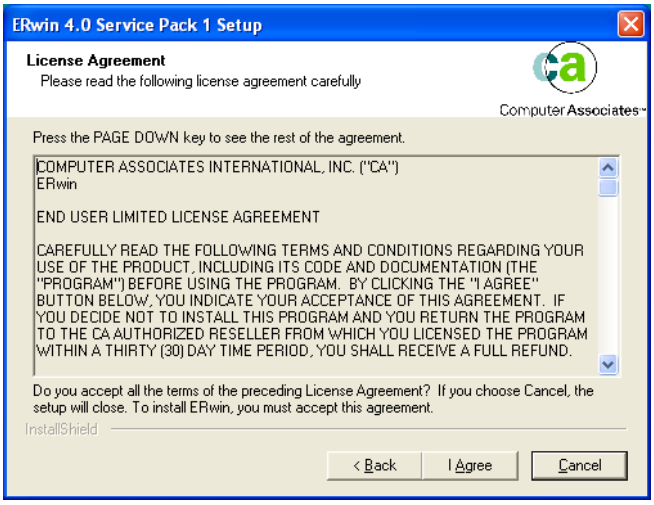
Softverska piraterija se odnosi na izradu nelegalnih kopija softvera, i predstavlja jedan od najozbiljnijih problema u savremenom informatičkom društvu. U SAD postoji zakon koji štiti autorska prava nad računarskim softverom, kojim se obezbeđuje zaštita izvornog programskog kôda, ali se ovim zakonom ne štite neki drugi sastavni delovi softvera kao što su padajući meniji ili ikone. Naravno, kopiranje softverskog programa bez plaćanja vlasniku je kršenje autorskih prava. Treba istaći da korisnik kupovinom softvera kupuje samo licencu odnosno pravo korišćenja softvera, ali ne i pravo distribucije tj. nije dozvoljeno davati kupljeni softver drugome kako bi ga on instalirao na svom računaru.

U našoj zemlji je u decembru 2009. godine usvojen novi Zakon o autorskim i srodnim pravima, kojim se pod autorskim delom smatraju i „računarski programi u bilo kojem obliku njihovog izražavanja, uključujući i pripremni materijal za njihovu izradu“. Po ovom Zakonu, autorska prava traju doživotno, ali i 70 godina posle smrti autora, a sva autorska prava se prenose njegovim naslednicima. Ovim Zakonom su osim definicije autorskih prava propisana sva prava koja iz njih proističu, kao i sva sredstva njihove zaštite, pa su tako na primer za izradu i puštanje u promet nelegalnih kopija softvera, ali i njihovo korišćenje, propisane visoke novčane kazne.

Procenjuje se da danas oko 40% svih personalnih računara u svetu radi pomoću ilegalnog softvera (u SAD oko 25%, u Evropi oko 35%). Kao zemlje sa najvećim procentom ilegalnog softvera ističu se Vijetnam, Kina, Indonezija, Ukrajina i Rusija, u kojima više od 85% softvera predstavljaju nelegalne kopije.

U našoj zemlji je do 2000. godine, zbog nepostojanja adekvatne zakonske zaštite ili neprimenjivanja postojećih propisa, gotovo 99% korišćenog softvera bilo ilegalno. Danas se situacija menja, i procenjuje se da je taj procenat u Srbiji oko 75%, pri čemu je ovaj procenat u poslovnom sektoru manji, zbog viših kazni i kontrola od strane Poreske uprave, koja je u našoj zemlji zadužena za kontrolu legalnosti softvera u posedu pravnih lica. Inače, u našoj zemlji se softverska piraterija tretira kao ozbiljan privredni prekršaj, po prirodi prestupa sličan utaji poreza.

Prilikom instalacije softvera, u jednom od početnih koraka, korisnik „potpisuje ugovor“ sa proizvođačem, kojim se obavezuje na poštovanje svih obaveza i načina upotrebe softvera koje proizvođač propisuje. Ovaj ugovor je poznat pod nazivom Ugovor krajnjeg korisnika o korišćenju licence (EULA – End User Licence Agreement), i na slici 1 je prikazan jedan primer. Ugovor se obično „potpisuje“ klikom na opciju „I agree“ ili „Accept“, bez čega nije moguće nastaviti instalaciju softvera.



Slika 1. Ugovor krajnjeg korisnika o korišćenju licence (EULA)

Iako ni jedan po postojećih metoda ne garantuje potpunu zaštitu, danas se u svetu najčešće primenjuju sledeće metode borbe protiv piraterije:

- zaštita autorskih prava,
- zaštita od kopiranja,
- licenciranje po mestu upotrebe.

Već je navedeno da se autorska prava štite zakonima, a da su za njihovo spovođenje zadužene državne institucije. Softverskom piraterijom nisu pogođeni samo proizvođači softvera, zbog nenaplaćene cene, već i država, zbog nenaplaćenog poreza. Svako delo zaštićeno autorskim pravima treba da na vidnom mestu ima označeno obaveštenje o time, kao i godinu njegovog objavljivanja i ime ili naziv vlasnika. U svetu je uobičajeno da se iza naziva proizvoda zaštićenog autorskim pravom postavlja oznaka ©, od reči Copyright.

Tehnike zaštite od kopiranja se sastoje u primeni hardverskih i softverskih karakterstika koje sprečavaju pokušaje kopiranja ili kopirani softver čine nepouzdanim. Iako su do sada isprobane mnoge tehnike

kojima bi se onemogućilo neovlašćeno kopiranje i korišćenje softvera (npr. DVD diskovi se zaštićuju digitalnim „omotačima“ (wrappers), koji onemogućavaju njihovo kopiranje), pokazalo se da ni jedna od njih ne daje potpunu sigurnost. Zbog toga većina proizvođača odustaje od ove metode i više se oslanja na preostale dve.

Za potrebe pre svega kompanija i organizacija sa velikim brojem korisnika, a i u cilju suzbijanja piraterije, neki proizvođači softvera nude mogućnost licenciranja po mestu upotrebe (site licencing). U ovom slučaju, korisnik (kompanija ili organizacija), na osnovu ugovora sa proizvođačem, dobija jedan primerak instalacionog diska i prateće dokumentacije, a dobija dozvolu za instalaciju softvera na onoliko računara koliko je licenci platila. Korisnik je dužan da vodi računa o imenima korisnika kojima je licenca dodeljena kao i o računarima i mrežama koji ovaj softver koriste. Na ovaj način, kupci dobijaju mogućnost da pod znatno povoljnijim uslovima (cena niža i do 50% od pojedinačne kupovine), dođu do potrebnog broja kopija softvera, a proizvođači brže šire svoju korisničku mrežu i lakše ulaze u velike kompanije.

Takođe, neke softverske kompanije u cilju širenja svojih proizvoda i vezivanja potencijalno novih klijenata, često svoje proizvode ustupaju potpuno besplatno za nekomercijalne svrhe. Na primer, većina kompanija koje proizvode razvojne alate i sisteme za kreiranje aplikacija, besplatno daju svoj softver na korišćenje univerzitetima i fakultetima, u nadi da će studenti po završetku studija u firmama u kojima se budu zaposlili, tražiti da rade sa softverom na koji su navikli odnosno koji dobro poznaju još sa studija.

Treba istaći da je poslednjih godina u usponu tzv. koncept otvorenog kôda (Open Source), po kome proizvođači softvera ustupaju besplatno na korišćenje svoje proizvode. Primeri za ovaj koncept su operativni sistem Linux, softverski paket OpenOffice.org, veb server Apache, itd.

Piraterija digitalnih sadržaja

Drugi važan segment, po prihodima i značajniji, je piraterija digitalnih sadržaja. Naime, razvojem informacione tehnologije postalo je vrlo jednostavno praviti kopije različitih digitalnih sadržaja (najčešće muzike i filmova, ali i knjiga u elektronskom obliku, slika, članaka, itd.) čak i na kućnim računarima. Ovaj oblik piraterije najčešće se vrši putem Interneta ili kopiranjem sadržaja na CD ili DVD disk. Napomenimo da se i ovi oblici autorskih prava, štite već navedenim Zakonom o autorskim i srodnim pravima.

Razvojem tehnologije i padom cena komponenti, danas smo u situaciji da gotovo svaki PC računar ima DVD rezač, koji omogućava narezivanje sadržaja u digitalnom obliku na CD ili DVD disk, tako da gotovo svako može vrlo jednostavno da napravi nelegalnu kopiju originalnog muzičkog CD-a ili filma na DVD-u. Osobe koje se gotovo profesionalno bave ovim oblikom piraterije, pokušavaju da i po svim ostalim karakteristikama (slika na CD-u, omot, itd.) njihova kopija bude istovetna originalnom izdanju, tako da ljudi često nisu ni svesni da kupuju nelegalne kopije.

Razvojem brzih internet veza, omogućeno je da osobe potpuno besplatno i za kratko vreme dođu do željenog filma ili muzike. Krajem 1990-tih i početkom ovog veka postojali su brojni sajtovi nastali prvenstveno radi distribucije digitalnih sadržaja. Jedan od najpopularnijih je bio Napster, koji je 1999. godine kreirao tada 19-godišnji Amerikanac Shawn Fanning i koji je bio jedan od prvih koji je nudio mogućnost razmene muzike i filmova putem Interneta. Sajt je vrlo brzo stekao veliku popularnost, pre svega kod mladih, jer su se sa njega, osim inače besplatnih sadržaja, mogle preuzeti i kopije komercijalnih sadržaja, za koje bi inače bilo neophodno platiti. Popularnost je čak išla dotle da su neki univerziteti u SAD zabranili korišćenje Napstera na svojim mrežama, jer je prenos podataka sa ovog sajta bio toliko intenzivan da je zagušio akademsku mrežu i onemogućio bilo kakav rad. Princip rada je bio takav da bi nakon preuzimanja softvera sa sajta, i instalacije na svom računaru, korisnici mogli da pretražuju ogromnu bazu sa digitalnim sadržajima, pre svega pesmama u mp3 formatu, jednostavnim unošenjem naziva

izvođača ili pesme. Na osnovu dobijenih rezultata pretrage, korisnik je mogao da se odluči koji će fajl da preuzme i za par minuta bi ga, potpuno besplatno, imao na svom hard disku, sa koga je mogao da se preslušava ili kopira dalje, na CD diskove ili mp3 plejere.

Naravno, ubrzo su reagovale muzičke i filmske kompanije, navodeći da im ovo kršenje autorskih prava ugrožava poslovanje i da im je prodaja značajno opala i sud je ubrzo zabranio rad Napstera i sličnih sajtova ili apikacija (npr. Kazaa).

Jedan od najvećih problema Napstera je što je sve digitalne sadržaje držao na svojim serverima, odakle su bili preuzimani, tako da je pravnicima bilo lako da dokažu kršenje autorskih prava i dobiju pokrenute tužbe. Zato se posle Napstera razvio novi oblik ove piraterije, a to je korišćenje aplikacija koje služe za ostvarivanje veze i direktnu razmenu podataka, odnosno prenos fajlova između dva računara (peer-to-peer). Naime, instalacijom ovog softvera, korisnik može da priloži neke digitalne sadržaje sa svog računara i postavi ih dostupnim ostalim korisnicima (file sharing). Takođe, može da pretražuje šta su ostali korisnici postavili dostupnim, i da ove sadržaje preuzima direktno na svoj računar. S obzirom da se ostvaruje direktna veza dva korisnika, odnosno da server proizvođača softvera učestvuje samo u uspostavljanju veze, ali ne i u prenosu fajlova (prenos ide direktno sa računara na računar korisnika koji mogu biti sa različitih krajeva sveta), to je znatno teže dokazati odnosno optužiti proizvođača ovakvog softvera za kršenje autorskih prava. Najpoznatiji softveri za peer-to-peer razmenu fajlova su BitTorrent, eMule, eDonkey, Gnutella, itd.