

Zakonodaja iz področja kriptografije v Sloveniji

Maja Markovčič
Fakulteta za matematiko in fiziko
September 2001

Povzetek

Zaščita podatkov je področje, ki se dandanes zadeva vsakega človeka. Naši osebni podatki so shranjeni v računalnikih. V sestavku najprej pogledamo, koliko Slovence to področje zanima in koliko so s to problematiko seznanjeni. V nadaljevanju sta predstavljena dva sprejeta zakona, na koncu pa na kratko pogledamo primerjavo z ostalimi državami.

Vsebina

1. Uvod – zanimanje za kriptografijo pri nas
2. Razvoj kriptografije v Sloveniji
3. Zakonodaja s področja kriptografije
 - 3.1 Kako zakonodaja sledi razvoju kriptografije
 - 3.2 Zakon o elektronskem poslovanju in elektronskem podpisu
 - 3.3 Komentariji na zakon
 - 3.4 Zakon o izvozu blaga z dvojno rabo
4. Kako je drugje
5. Zaključek
6. Viri

1. Uvod – zanimanje za kriptografijo pri nas

Skoraj vsa področja človekovega delovanja so dandanes določena z zakoni. Le ti se dotaknejo tudi tistih stvari, ki jih večina ljudi niti ne pozna. Mogoče bi lahko tako rekli na nek način tudi za kriptografijo. Zakaj?

Naredila sem mini raziskavico in nekaj svojih znancev vprašala, če vedo, kaj je kriptografija in ali se jim zdi pomembno, da je uzakonjena. Odgovori so se seveda razlikovali glede na starost in seveda na področja delovanja vprašanega. Računalničarji so v glavnem vedeli, kaj je to, bila pa sem malo razočarana nad svojimi kolegi matematiki, ampak resnici na ljubo tudi jaz do pred nekaj leti nisem o tem vedela nič. Čeprav bi strokovnjaki moji raziskavi lahko očitali kar nekaj pomanjklivosti (od subjektivnosti do nereprezentativnosti vzorca), bi lahko zaključila, da je beseda KRIPTOGRAFIJA večini Slovencev neznana. Drugi del besede nekatere zavede in vso stvar povežejo z grafiko. Zanimiv odgovor sem dobila od laika iz področja informatike, ki mi je dejal, da je to najbrž nekaj v zvezi z geografijo in bi bilo najbrž kar pametno, da zakoni uredijo tudi 'te reči'. Ob podatku, da je kriptografija področje, ki se v grobem povedano ukvarja z zaščito podatkov in zasebnostjo, so si bili vsi na novo poučeni enotnega mnenja, da mora biti zakonodaja tu natančno določena. Varnost podatkov je stvar, ki ljudem v času razvijajoče tehnologije vedno več pomeni.

Torej, ker je predmet naše raziskave tesno povezan z računalništvom in seveda internetom, so se moji nadaljnji poskusi, kje bi našla kaj o tem, držali predvsem spletnih strani. Srečo sem najprej

poskusila z nekaj najbolj priljubljenimi in splošnimi stranmi v Sloveniji: matkurja.com, slovista.net in slowwwenia.com.

Pri prvi me je ključna beseda KRIPTOGRAFIJA pripeljala na domačo stran našega profesorja Aleksandra Jurišiča in na stran seminarja iz kriptografije, katere avtor je ravno tako naš profesor. Seveda s tem nisem bila zadovoljna, ker je to, da bi se v Sloveniji za kriptografijo zanimal le naš profesor, le malo verjetno.

Slovista (najpopolnejši iskalec slovenskega interneta, kot se imenujejo) se je izkazal za uspešnejšega. S svojimi 39 zadetki je razkril, da je interes le nekoliko večji. Skozi pregled teh strani bi moj sogovornik iz raziskave težko našel kakšen uporaben zemljevid in geografske podatke, lahko pa bi dobil veliko uporabnih informacij. Tu bi zvedel, kaj so osnove, cilji in sredstva kriptografije. Ugotovi lahko, da kriptografija omogoča tudi enostavne opravke, kot so poslovanje z banko, saj pri SKB-Net trdijo: "Kriptografija, usmerjevalniki, požarni zidovi, interne kontrole, uporabnikova identifikacijska številka, identifikacijska kartica, ... vse to zagotavlja varno uporabo SKB NET-a."

Po pridobljenih osnovah lahko posameznik tu dobi tudi nadaljnje informacije o digitalnem podpisu, varstvu elektronske zasebnosti, varnosti elektronskega poslovanja in nenazadnje tudi zve, kaj je to DES in PGP (program za kodiranje elektronskih sporočil, datotek ali celotnega diska). Meni osebno je bila zanimiva stran Centra vlade za informatiko, ker sem tu dobila največ informacij o zakonodaji.

Četudi sem na slovisti dobila že kar nekaj materiala, sem vseeno pogledala še na slowwwenio.com. Tu je na voljo PGP 6.02i, podjetje Infotehna d.o.o. pa ponuja PenOp, celovit sistem za elektronski podpis s pomočjo grafične tablice in elektronskega peresa.

Zanimanje torej je. Poglejmo sedaj, koliko je bilo na tem področju pri nas narejenega in kaj se obeta.

2. Razvoj kriptografije v Sloveniji

Kriptografija le ni tako mlada veda, kot se zdi. Zaščita podatkov, zasebnost, kode. To so problemi, ki so belili človeške glave že davno pred izumom računalnika. Ker je naša država očitno veliko mlajša, je bil razvoj večino pogojen s politiko in razvitostjo države, kateri smo trenutno pripadali. Trenutno bi o velikem zaostanku in seveda o velikem naskoku pred drugimi težko govorili.

V članku z naslovom Nove naloge in pomen kriptografije avtor Rado Ključevšek trdi: »Država se mora opreti na lastno znanje in sama skrbeti za razvoj šifrirne opreme za svoje potrebe. Ni nujno, da ves razvoj za lastne potrebe poteka v okviru državne uprave, boljše je celo, da poteka tudi v podjetjih v Sloveniji, a mora biti ves državno nadzorovan ter mora zadostovati strogim varnostnim merilom.« Najbrž so državni uradniki drugačnega mnenja, saj so nove kartice zdravstvenega zavarovanja last tuje firme.

Avtorju članka bo mogoče v uteho, da za celoten sistem elektronskega poslovanja (in s tem seveda tudi za zaščito) skoraj v vseh slovenskih bankah skrbi naše podjetje Zaslon, ki je pred kratkim prišel v last nekoliko večjega Hermes Softlab-a. Omenjeni Zaslon je avtor Klika, ki ga velika večina Slovencev po dokaj odmevni reklamni akciji pozna vsaj po imenu.

V razvoj kriptografije pri nas se ne bi posebno speščala. Raje pogledjmo, kako je z razvojem zakonodaje iz tega področja.

3. Zakonodaja iz področja Kriptografije

3.1 Kako zakonodaja sledi razvoju kriptografije

Na tem področju je bila narejena še ena raziskava, kjer se v nasprotju z mojo lahko zanesemo na rezultate, saj je bila bistveno bolj strokovno izvedena. Potekala je februarja, leta 1996. Predmet te raziskave so bili pravniki, njihova računalniška osveščenost in poznavanje osnovnih kriptografskih pojmov. Ankete so izpolnjevali pravniki iz različnih področij, kot so odvetniki, pravniki v gospodarstvu, uprava, pravosodje, notarji, osebe iz pravnega svetovanja in drugi. Poslane so jim bile po pošti. Ker le 9% vprašanih ne uporablja računalnika, so sklepali, da so na anketo odgovorili predvsem tisti, ki ga uporabljajo.

Poleg vprašanj o uporabi modema in elektronske pošte so bila nekatera tudi na temo elektronskega podpisa. Navedla bom podatke, ki so objavljeni na spletni strani z naslovom: Elektronski podpis – Usklajevanje tehnoloških in pravnih rešitev pri pravnem poslovanju, avtorja mag Janeza Topliška.

Mnenje o elektronskem podpisu prehaja od velikega nezaupanja do kar precejšnjega zaupanja v posameznih primerih. Ker kar visok odstotek vprašanih, ki nima stališča ali pa niso odgovorili (32% - 34%) lahko vidimo, da pravniki zelo slabo poznajo tehnologijo elektronskega podpisovanja. Da elektronsko sporočilo lahko pravno zadostno podpišemo na elektronski način, meni le 41% pravnikov in le 25% jih meni, da je elektronski podpis enako učinkovit kot lastnoročni.

19% pravnikov meni, da lahko na elektronski vlogi z osebnimi podatki vložnika izpustimo podpis vsake vrste in ker jih kar 58% meni, da ni tako, to nakazuje, da le bolj zaupajo ročnim podpisom in niso za tako imenovano "nepapirno poslovanje".

7% pravnikov se strinja, da je možnost elektronskega podpisa v slovenskih predpisih predvidena, vendar bi bilo bolje kakšen neposredni primer tudi najti. Izvajalci te raziskave so sklepali, da so vprašani najbrž s tem mislili, da možnost elektronskega podpisa v slovenskih predpisih ni izrecno izključena. Več kot polovica vprašanih na to vprašanje ni znala odgovoriti ali pa se ni opredelila (57%).

Kar 72% anketiranih se strinja s tem, da bi se morali pri elektronskem podpisovanju prilagoditi pravnim rešitvam, ki bodo uveljavljene izven Slovenije.

Tuje rešitve utegnejo vplivati tudi na uporabo šifrirnih tehnik pri zasebnem elektronskem poslovanju v Sloveniji. V splošnem imajo slovenski pravniki do šifriranja je podoben odnos kot njihovi kolegi v ZDA, čeprav je pri nas seveda večji delež neopredeljenih. Vsekakor je to posledica dejstva, da je praksa šifriranja zasebnih elektronskih sporočil v Sloveniji razmeroma neznana. Dobra polovica, kar 58% pravnikov, je naklonjena zasebni uporabi šifriranja in pravijo, da za elektronsko sporočanje ne bi smeli postavljati strožjih omejitev, kakršne veljajo za pisma.

Naj pravo počaka, da bo postala tehnologija elektronskega podpisovanja popolnoma zanesljiva, meni polovica pravnikov (52%). Raziskovalci so ugotovili, da bi bil ta odstotek bistveno večji in bi bili pravniki elektronskemu podpisu bolj naklonjeni, če bi jim konkretno pokazali kakšen zanesljiv način elektronskega podpisovanja. Pravniki resno občutijo pomanjkljivo poznavanje tehnologij elektronskega poslovanja, saj skoraj vsi (91%) menijo, da bi morali pravnike že med rednim študijem seznaniti z elektronskim poslovanjem. Če iz katerega koli razloga tega usposabljanja ne bi mogli vključiti v redni pravni študij, ostaja dejstvo, da bi pravniki ob vstopu v poklic elektronsko poslovanje že radi poznali.

Pravniki imajo na internetu na voljo kar obširen slovarček pojmov iz 'kriptografskega prava', vendar pa najbrž konkreten primer in uporaba prikažeta boljšo sliko, s katero bi si tudi oni lažje oblikovali svoje mnenje.

3.2 Zakon o elektronskem poslovanju in elektronskem podpisu

Iz pravnega stališča sta za področje kriptografije najpomembnejša elektronsko poslovanje in elektronski podpis. Čeprav digitalni podpis kot smo že videli ne sodi v ustaljeno prakso naših pravnikov, imajo pripravljen osnutek na to temo. Tudi elektronsko poslovanje postaja vedno bolj popularno, vsaj na področju trgovine, saj že kar nekaj potrošnikov naroča izdelke preko računalniških povezav. S takšno ponudbo se pri nas lahko pohvali tudi Mercator.

Na spletni strani Centra Vlade za informatiko je osnutek zakona o elektronskem poslovanju – delovno besedilo z datumom 2.6.1999. Prvi člen določa, da je to zakon, ki ureja elektronsko poslovanje ter uporabo podatkov v elektronski ali podobni obliki in uporabo elektronskega podpisa v pravnem prometu. V drugem členu so pravno definirani pojmi.

V nadaljevanju se najprej dotaknejo elektronskega poslovanja. V četrtem členu je zapisano, da se elektronskemu sporočilu ne sme odreči veljavnosti samo zato, ker je v elektronski obliki. Nadalje se ukvarjajo z elektronskimi sporočili, predvsem tem, kdaj se posamezno sporočilo šteje za poslano in kdaj za prejeto.

Zanimiv je zopet 12. člen, ki pravi, da se elektronskemu sporočilu kot dokaznemu sredstvu v sodnih, upravnih in drugih postopkih ne sme odreči veljavnosti samo zato, ker je v elektronski obliki.

Tudi pri elektronskem podpisu je najprej člen, ki mu daje veljavo: "Elektronskemu podpisu se ne sme odreči veljavnosti samo zaradi elektronske oblike, ali ker ne temelji na ustreznem overitvenem potrdilu ali na overitvenem potrdilu, ki ga izdaja ustanova za overjanje po tem zakonu."

Elektronski podpis se šteje za ustrezen, če podpisana oseba soglaša s podatki v vsebini in če je ta metoda primerno zanesljiva namenu, zaradi katerega je bilo elektronsko sporočilo ustvarjeno. Zakon določi tudi kaj so primerne tehnologije in varovala za uporabo vseh opravil v zvezi z elektronskim podpisovanjem. V nadaljevanju kar nekaj prostora nameni pravilom overjanja elektronskih podpisov.

Zakon torej določa pogoje, ki jih morajo izpolnjevati ponudniki in uporabniki storitev. Ti pogoji se navezujejo na overjanje, tehnične zadeve za varno elektronsko podpisovanje, obliko kvalificiranih digitalnih potrdil, ureja odgovornost vpletenih subjektov in določa obliko nadzora ponudnikov storitev.

Na koncu zakona so opisane še kazenske določbe, ki se nanašajo predvsem na ustanove za overjanje (kazni so od 200 000 do 5 000 000) in na posamezne osebe, če se ne držijo členov v zakonu (od 50 000 do 450 000).

Zakon je bil sprejet junija leta 2000.

3.3 Komentariji na zakon

Odmevi na zgoraj opisani zakon niso bili nič kaj spodbujajoči. Očitajo mu, da je bil oblikovan v zaprtem krogu in da sploh ni možno izvedeti, katero ekipo "strokovnjakov" se je ukvarjala s tem.

Zanesljivo je možno reči, da tako ne delajo nikjer v tujini. Tam resno razpravljajo že o enotnih metodoloških pristopih sodelujočih ekip. V ZDA naj bi obstajal za več kot eno stran dolg seznam najpomembnejših oseb, ki so pripravljale besedilo enotnega zakona o e-transakcijah.

Na Merkurjevih dnevih '99 v Naklem je bilo prvo posvetovanje diplomantov in magistrantov elektronskega poslovanja. Tam so poleg podanih kritik na osnutek zakona o elektronskem poslovanju in digitalnem podpisu skritizirali tudi računalniško osveščenost naših pravnikov: "Čeprav je mnoga razmerja pri e-poslovanju možno presojudi po veljavnih pravilih, bi morala slovenska pravna stroka sistematizirati "pravo e-poslovanja v Sloveniji", saj bi to prispevalo k bolj sistematičnemu delu in k večji pravni preglednosti. Medtem ko imajo nekatere tuje pravne šole že desetletje posebne študijske usmeritve za e-poslovanje ali vsaj redne specializirane seminarje, je slišati neverjetno, da slovenski pravni fakulteti te aktivnosti zožujeta in ne skrbita za razvoj pravnih kadrov, ki jih bo sodobno e-poslovanje še kako potrebovalo."

Kljub omenjenim kritikam je naš zakon o elektronskem poslovanju eden izmed prvih v Evropi. Ne gre zanemariti, da smo v teoriji korak pred drugimi. In kako je s prakso? Andy Grove, direktor Intela, trdi da bodo v petih letih vsa podjetja internetna podjetja ali pa sploh ne bodo več podjetja. To je napoved in za naše razmere mogoče celo nekoliko pretirana, medtem ko je stanje trenutno tako: 90% velikih in 78% malih podjetij je trenutno priključenih na internet. Vendar pa – ali to pomeni, da smo pripravljeni na elektronsko poslovanje? Razlika med tistimi, ki so na internetu in tistimi, ki pravijo, da poslujejo preko njega, je zelo velika. Verjetno pa je tudi pri tistih, ki poslujejo preko interneta, to mnogokrat zreducirano na pošiljanje elektronske pošte in na poslovanje z Agencijo za plačilni promet.

Nekoliko se stvari naprej premikajo v izobraževanju. Za delavce v računovodstvu in finančah so seminarji in izobraževanja stalnice. Poleg običajnih tem (davki, zakonodaja s področja financ...) se jim je pred kratkim priključilo tudi elektronsko poslovanje. Učijo jih osnovnih pojmov in način dela.

Situacija se spreminja iz dneva v dan. Najbrž bodo računalniki in poslovanje prek njih najbolj stopili v ospredje, ko bo na delovna mesta prišla generacija rojena ob računalnikih. Sama se nekako ne štejem še v to generacijo, pa še nisem zaposlena. Današnji otroci, ki se poleg hoje in govora že v rani mladosti učijo osnovnih veščin računalnika, v sebi ne bodo imeli tistega strahu in nezaupanja v elektroniko. Ko bodo na pohodu oni, se zna razvoj elektronskega poslovanja še toliko bolj pospešiti in zaviti v smeri, ki jih trenutno sploh še ne vidimo.

3.4 Zakon o izvozu blaga z dvojno rabo

Poglejmo kako je z izvozom kripto opreme.

Za laike, ki se v pravo šele uvajamo, besedna zveza blago z dvojno rabo bolj malo pomeni. V drugem členu zakona je razlaga izrazov, kjer piše, da je blago z dvojno rabo blago in tehnologija, ki se lahko uporablja tako v civilne, kot tudi vojaške namene. Natančnejši opis se glasi: blago, ki se v celoti ali po delih uporablja oziroma lahko nameni za uporabo v zvezi z razvojem, proizvodnjo, upravljanjem, delovanjem, vzdrževanjem, skladiščenjem, odkrivanjem, identifikacijo in širjenjem kemičnega, biološkega ali jedrskega orožja. Poleg tega se ne sme uporabljati za razvoj, proizvodnjo, vzdrževanje in skladiščenje izstrelkov, sposobnih nositi takšno orožje.

Za tako blago velja, da se ga lahko izvaža le na podlagi dovoljenja, ki ga izda ministrstvo, pristojno za ekonomske odnose s tujino, poleg tega pa mora pred izdajo odločbe zahtevati obvezno mnenje ministrstev pristojnih za zunanje zadeve, notranje zadeve in obrambo.

Zakon veleva, da se izda dovoljenje za vsak posamičen izvoz, z veljavnostjo največ enega leta. Zahtevek za dovoljenje mora vsebovati opisan namen končne uporabe blaga, ter izjavo končnega uporabnika, da bo blago uporabljeno le za namene, ki so navedeni v zahtevku in ne bo ponovno izvoženo v tretjo državo, brez soglasja države izvoznika.

Kazenske določbe zakona o izvozu blaga z dvojno rabo nihajo od 300.000 SIT pa tja do 20.000.000, odvisno od tega kdo je kršil in kakšne vrste je prekršek.

4. Kako je drugje

Prvi zakon o elektronskem podpisu je bil sprejet leta 1995 v ZDA v zvezni državi Utah. Leta 1996 je komisija Združenih narodov za mednarodno gospodarsko pravo (UNCITRAL) sprejela Modelni zakon o elektronskem poslovanju. Po njem so se zgledovali tudi oblikovalci slovenskega zakona.

V Evropi so bili prvi Nemci. Zakon so sprejeli leta 1997, sledile pa so še nekatere države, kot sta na primer Italija in Avstrija. Da bi članice Evropske unije poenotile zakonodaje o elektronskem poslovanju in o elektronskih podpisih, je unija konec leta 1999 sprejela direktivo z naslovom Okvir unije za elektronske podpise (A Community Framework for Electronic Signatures). Določila direktive morajo države članice udejaniti na državni ravni do 19. junija 2001. Direktiva obravnava vse vrste elektronskih podpisov, vendar izpostavlja tiste, ki imajo pod določenimi enako pravno veljavo, kot lastnoročni podpis pri dokumentih v papirni obliki.

Slovenski zakon je v skladu z direktivo Evropske unije. Lastnoročnemu podpisu je enakovreden samo varen elektronski podpis, ki je overovljen s kvalificiranim potrdilom.

Tehnologija varovanja podatkov v elektronskem poslovanju se hitro spreminja. Ravno zato so zakoni iz tega področja tehnološko nevtralni. V tem ne izstopa niti slovenski. Naš zakon izvažanja kripto opreme kot smo videli ne prepoveduje, ampak le omejuje. Potrebno je najbrž kar nekaj birokracije za dokazovanje, da se oprema ne bo uporabljala za vojaške namene. Za primerjavo, v ZDA in Kanadi smatrajo kripto opremo za vojaško in so zato izvozne omejitve kar hude, a so jih jeseni leta 99 precej omilili. Nekatere države (npr. Češka) so podpisnice sporazuma, ki omejuje izvoz kripto opreme, a Slovenija tega (še) ni podpisala. Članica Nata Slovenija tudi še ni, situacija se bo pa najbrž spet spremenila, ko se bomo priključili tej vojaški zvezi.

5. Zaključek

Sestavek, ki ste ga ravnokar prebrali, je nastajal kar dolgo časa. Zanimivo pri tem je, da je tema takšna, ki iz dneva v dan prinaša spremembe. V času od začetka pisanja do zaključka smo Slovenci dobili e – redovalnice. Kmalu se nam obetajo terminali, ki bodo marsikomu prihranili nepotrebno čakanje ob birokratičnih opravkih. S pomočjo terminalov naj bi dobili razna potrdila (o državljanstvu, o stalnem prebivališču, družinskih članih...).

Novosti k sreči prihajajo. Marsikaj nam bodo olajšale. Zavedati se je treba, da sodobna tehnologija poleg prednosti prinaša tudi določen strah. Vedno več naših podatkov bo na voljo spretnim hekerjem, vendar mislim, da lahko zaupamo državi in njenem zakonskem stroju, da nas bo pred tem varovala kolikor bo v njeni moči. Poleg tega pa lahko računamo tudi na to, da je verjetnost, da bi se kdo spravil ravno na nas, zelo majhna.

6. Viri

- [1] Tomaž Klobučar, Elektronski podpisi, Monitor oktober 2000
- [2] Rudi Tavčar, Želja po zmagi ali le boj za preživetje, Relacije december 2000
- [3] Državni zbor, Zakon o izvozu blaga z dvojno rabo
http://www.sigov.si/dz/si/aktualno/spremljanje_zakonodaje/sprejeti_zakoni/sprejeti_zakoni.html
- [4] Državni zbor, Zakon o elektronskem poslovanju in elektronskem podpisu
- [5] Jay Worthington, Interview with Eben Moglen Junij 2000
- [6] Referat na Merkurjevih dnevih'99, Pravno urejanje elektronskega poslovanja po svetu in v Sloveniji, September 99 (<http://www2.arnes.si/~rzjtopl/slo/Merkur99.htm>)