ZASEBNOST IN INTERNET

Franci Pivec

Izvleček

Zasebnost, posebej informacijska zasebnost je s pojavom interneta doživela nove oblike ogrožanja. Pravne ureditve evropskih držav so to zaznale z različno intenzivnostjo, velikega pomena pa so v tem pogledu mednarodne konvencije (OZN, EU, OECD). Opazno je neskladje med normativno podobo in realnim stanjem, ker v mnogih državah ne izvajajo dosledno niti lastnih niti mednarodnih predpisov, kar je pogostoma povezano s politiko nadzorovanja ljudi in organizacij. Poseben primer je varovanje informacijske zasebnosti na delovnih mestih, ki so vse pogosteje opremljena z internetom. Še bolj ogroža informacijsko zasebnost nezaželena uporaba nadležne elektronske pošte za komercialne namene («spam«). Nedvomno pa za ogrožanje zasebnosti ni kriva informacijska tehnologija sama po sebi, pač pa so krivi ljudje, ki z njo razpolagajo.

Abstract

With the appearance of the Internet, privacy, especially information privacy, has been confronted with new forms of threat. The state laws in different countries perceived this phenomenon with diverse levels of intensity, though international conventions regarding this issue play a very important role here (OZN, EU, OECD). An apparent disharmony is seen between the prescribed image and the real life situation, since in many countries neither the country's own regulations, nor the international ones are observed consequently, which is often connected with the policy to control people and organisations. A special case is the protection of information privacy at work, where the workplaces are increasingly equipped with the Internet. Another, even more menacing threat to the information privacy is sending "spam", which is unsolicited email. Undoubtedly, the information technology in itself is not the culprit in jeopardising the privacy; it is the people using it that are to blame.

■■■

I. Internet in zakonodaja o varovanju zasebnosti v evropskih državah

Varovanje zasebnosti v svetu elektronskih informacij je v pravnih ureditvah seveda nov pojav. Prvi korak je bil narejen v nemški deželi Hessen leta 1970, Švedska pa je leta 1974 kot prva država zastavila celovit sistem pravnega varovanja.

Zasebnost sama po sebi je bila že zdavnaj prepoznana kot pomembna človekova pravica, ki je pogosto zajamčena tudi z ustavo. Kot takšna je sprejeta tudi v mednarodnem pravu in v OZN, OECD in EU ali Svetu Evrope je bilo sprejetih kar nekaj konvencij, preko katerih je ta pravni element pridobil ustrezno mesto tudi v nacionalnih ureditvah.

Uveljavljanje in razvoj informacijske tehnologije v državni upravi, zdravstvu, transportnih sistemih, bančništvu dramatično povečuje zbiranje informacij o posamezniku in zasebnost ni bila še nikoli tako načeta kot danes. Internet dejansko pomeni:

- da so z globalizacijo padle geografske bariere,
- da je zavladala splošna konvergenca med informacijskimi sistemi,
- da se z multimedijo medsebojno prelivajo tudi formati podatkov.

Komunikacijski kanali so se neznansko razširili in pospešili, s tem pa tudi možnosti prestrezanja osebnih sporočil in poseganja v zasebnost. Internet je razširil možnosti intenzivnega nadzorovanja. Tudi manj razvite države si silno prizadevajo pridobiti kar najsodobnejša orodja za nadzorovanje elektronskih komunikacij in – verjeli ali ne – izdatki za te nakupe so že presegli obseg trgovine z orožjem.(1)

Pravica do zasebnosti najpreprosteje pomeni, da te »pustijo pri miru«. Gre za mejo, preko katere se skupnost ne sme vtikati v življenje posameznikov in v njihove medsebojne odnose. Lahko govorimo o

- telesni zasebnosti, ki zadeva varovanje fizične osebe pred neželenimi telesnimi intervencijami;
- teritorialni zasebnosti, ki zadeva poseganje v okolje domovanja, delovnega mesta, javnega prostora;
- zasebnosti komuniciranja, ki zadeva nedotakljivost pošte, telefona, elektronskih sporočil;
- informacijski zasebnosti, ki zadeva zbiranje in obdelovanje osebnih podatkov.

Zasebnost je skratka pravica posameznika, da je zavarovan pred vsiljevanjem v njegovo osebno življenje ali odnose ter družino, bodisi v neposrednem fizičnem smislu, bodisi z objavo informacij o tem.(2)

Bilo bi zelo presenetljivo, če ta pravica ne bi bila vključena v Splošno deklaracijo o človekovih pravicah ali v Mednarodno konvencijo o civilnih in političnih pravicah. Evropa je pravico varovanja zasebnosti opredelila z Rimsko konvencijo o varovanju človekovih pravic in temeljnih svoboščin. Še posebej se je skrb za varovanje zasebnosti v Evropi okrepila po letu 1980, ko je bila v Svetu Evrope sprejeta Konvencija o varovanju osebnosti v zvezi z avtomatsko obdelavo osebnih podatkov.(3) Na tej osnovi so kasneje nastale direktive Evropskega parlamenta o pretoku osebnih podatkov (4) ter o varovanju zasebnosti v telekomunikacijah.(5) Ljudem v EU bi morala biti na tej podlagi zajamčena

- pravica izvedeti, od kod informacija, ki jih zadeva, izvira;
- pravica do popravka nepravilne informacije;
- pravica do izvzetja osebnih podatkov iz neželenih obdelav;
- pravica, da je v določenih okoliščinah uporaba osebnih podatkov dopustna le na podlagi izrecne privolitve.

Napisane pravice so bolj malo vredne, če nihče ne odgovarja za njihovo izvajanje, zato so članice EU obvezane ustanoviti instanco, ki je posamezniku na voljo pri uveljavljanju pravice varovanja informacijske zasebnosti. Najbolj aktualne teme v evropski ureditvi varovanja osebnih podatkov so danes:

- Uporaba matične številke, ki jo kritiki označujejo le za vidni vrh ledene gore, ki ob uporabi pametne kartice pomeni definitivni konec romantičnega obdobja zasebnosti.
- Biometrika na podlagi digitalizacije osebnih fizičnih značilnosti za identifikacijo in preverjanje, ki zajema skeniranje mrežnice, geometrijo dlani, prstne odtise, prepoznavanje glasu, DNA ...
- Nadzorovanje komunikacij, pri čemer praviloma sodelujejo telekomunikacijske firme, ki celo prilagajajo svoje sisteme, da so »prisluškovalno prijazni«. Glede tega se tudi specializirane ustanove razvitih držav »nesebično trudijo«, da nove demokracije ne bi preveč zaostale.
- Poseben dosežek na tem področju, ki je pred meseci prišel v javnost, je projekt ECHELON, ki pa je dejansko že precej stara stvar, izhajajoča iz pakta Quadripartite, sklenjenega kmalu po Drugi svetovni vojni. Z njim so uvedli standardizacijo v obveščevalno dejavnost in angleški Menwith Hill, ki je »pokril« Evropo, je le ena od točk v svetovni mreži, ki jo povezuje Fort Meade v Marylandu. Z metodo ključnih besed so pod nadzorom praktično vse elektronske komunikacije.(6)
- Televizija zaprtega kroga postaja v razvitih državah tako običajna kot javna razsvetljava. Hranjenje in obdelava video-posnetkov je velika industrija, ki zanesljivo sega na področje zasebnosti, ne da bi se znali varovati pred zlorabami. Televizijske predstave s posnetki »skrite kamere« so iz leta bolj zabavne in bolj zaskrbljujoče.
- Nadzorovanje delovnih mest, posebej računalniških delovnih postaj, kjer so možnosti pridobivanja osebnih podatkov praktično neomejene. Delojemalci se seveda upirajo, toda večina delodajalcev se takega nadzora poslužuje, pri čemer jih podpira tudi znamenita American Management Association.(7)
- Nepooblaščeno in nadležno pošiljanje komercialne elektronske pošte, kar je ponekod zajelo že takšne razsežnosti, da resno ogroža informacijsko zasebnost uporabnikov interneta.

Nadzorovalni sistemi se naglo prilagajajo novi tehnologiji in ni dvoma, da rutinsko pregledujejo tudi celotni internet. Zakonodaja tega »še ni vzela«, zato se lahko nadzorovalne agencije s ponudniki servisov interneta dogovarjajo precej prosto. Le-ti imajo sicer tudi druge razloge, da se nasproti uporabnikom poslužujejo tehnologije »cookie cutter«*, pride pa to prav še komu drugemu, ki se mu ne zdi potrebno spoštovati zasebnosti.

Obstaja vrsta mednarodnih civilnih združenj, ki se nočejo sprijazniti s stanjem na področju varovanja zasebnosti, še posebej varovanja osebnih podatkov. Za izhodišče smo si izbrali dve poročili takšnih združenj in sicer:

- poročilo Electronic Privacy Center (EPIC) »Surfer Beware: Personal Privacy and the Internet«(8) ter
- poročilo Global Internet Liberty Campaign (GILC) »Privacy and Human Rights. An International Survey of Privacy Laws and Practice«(9)

Takoj lahko ugotovimo očitno razliko med državami, kjer varovanje osebnih podatkov res funkcionira, in državami, kjer si dajo opraviti le z videzom zakonodaje, pravica zasebnosti pa je kvečjemu municija v političnih obračunavanjih. Vse dokler prenos baz osebnih podatkov preko meje ni potreben in si pač le znotraj ene države drug drugemu delajo škodo, se nihče zunaj preveč ne razburja. Ko pa bodo siceršnje integracije narekovale tudi vzajemno uporabo osebnih podatkov, bo pa sodelovanja hitro konec, če država ne bo mogla jamčiti primernega, ne le papirnega, ampak praktičnega varovanja podatkov. Slepomišenje pri tem ni mogoče, ker so praktična ravnanja na tem področju pod stalnim nadzorom največjih obveščevalnih služb. Če te lahko v neki državi za vsakim vogalom pridejo do zaupnih podatkov, bodo svojim

* *"Cookies" so keksi, ki jih prilepijo na elektronske dokumente, da jim lahko sledijo po internetu in seveda tudi po računalnikih.*

delodajalcem zanesljivo odsvetovale tesnejše povezovanje. V tem je tudi smisel nenehnega pregledovanja in poročanja o stanju varovanja zasebnosti. Dodaten problem ima marsikatera država nekdanjega vzhodnega bloka, kjer še vedno prevladujejo razkošne navade KGB, ki jih sedaj opravičujejo z bojem proti organiziranemu kriminalu, kar pa le-temu očitno nič ne škodi.(10)

V nekaterih državah bolj vljudno (Združeno kraljestvo), v drugih kar nasilno (Rusija), povsod pa z opazno vnemo, se policije vrtijo okoli ponudnikov storitev na internetu. Nadzor si zamišljajo podobno kot pri mobilni telefoniji, kjer slovenski novinarji sploh niso edini osumljeni prisluškovanja (Irska, Švica, Portugalska, Slovaška ...). Posebno poglavje je ilegalna prodaja zbirk osebnih podatkov, npr.:

- češki uradniki s podatki servisirajo prodajalce Pampers pleničk in Always vložkov,
- španska Telefonica nepooblaščeno prodaja podatke o telefonskih naročnikih,
- v baltskih republikah je mogoče za bagatelo kupiti vsakršen seznam,

Madžarsko vrhovno sodišče je ukinilo matično številko državljanov kot neustavno. Na Poljskem je to PESEL, kjer se je od leta 1975 nabrala ena največjih zbirk osebnih podatkov na svetu, se pa sedaj divje prepirajo kaj bi z njo. Aktualna je zadeva z grško matično številko, pri kateri EU ne pusti dodajanja šifre o veroizpovedi. Inverzija se je zgodila v Luksemburgu, kjer sta ZDA in EU skupaj izposlovali ukinitev absolutne tajnosti bančnih računov. Dve državi – Nizozemska in Norveška – sta v zadnjem času opravili obširne parlamentarne preiskave o odnosu države (posebej tajnih služb) do zasebnosti in prislovični permisivnosti navkljub so ugotovili, da so živeli pod nebrzdanim nadzorom z vsemi sredstvi, za kar ni bilo nobene legalne osnove.

Posnemanja vredna je Švedska, kjer je Stevan Dedijer na univerzi v Lundu pred dvema desetletjema ustanovil prvo katedro za obveščevalno dejavnost na svetu, njena vlada pa že od leta 1776 ne pozna pojma »tajni akti«.

II. Internet na delovnem mestu in pravica zasebnosti

Ameriški Svet za delovno pravo je že leta 1996 posvetil svojo letno konferenco v Ashevillu problemom varovanja zasebnosti delojemalcev, ki imajo na svojem delovnem mestu povezavo z internetom.(11) S tem so odprli novo stran v reguliranju delovnih razmerij, ki je iz leta v leto bolj aktualna tudi za druge države. Tudi za Slovenijo, če upoštevamo zadnje podatke iz longitudinalne raziskave Raba interneta v Sloveniji, po kateri ima dostop do interneta 96% velikih podjetij, 89% srednjih, 77% majhnih in 66% zelo majhnih.(12) Gre zanesljivo za najbolj razširjeno tehnološko inovacijo, ob kateri nas morajo zanimati tudi socialne posledice.

Zanimivo je, da so Gallupovi podatki za ZDA v letu 1996 vsaj za srednja in majhna podjetja občutno nižji kot naši za leto 1999, kar pomeni, da je svetovni razvoj interneta res izredno pospešen. Ocenjujemo, da ta trenutek internet uporablja več kot 300 milijonov ljudi, od tega preko polovice samo za elektronsko pošto. Raziskava v 500 največjih svetovnih družbah je pokazala, da zaposleni z dostopom do interneta v povprečju porabijo 1,2 ure na dan za elektronsko pošto (30% več kot 1,2 ure, 12% pa več kot 2 uri). Prestrezanje sporočil po internetu je približno enako pogosto kot pri mobilni telefoniji – vsekakor je tega več znotraj firme (44%) kot zunaj firme (14%).

Študija American Civil Liberties Union je pokazala, da delodajalci nadzorujejo približno polovico vseh elektronskih sporočil in računalniških zapisov zaposlenih. V telekomunikacijskih firmah, zavarovalnicah in bankah pa je ta delež še znatno višji (80%). Seveda pri tem prihaja do kršitev pravice zasebnosti zaposlenega, varovanja osebnih podatkov, pravice sindikatov do kontaktiranja svojih članov ...

Na osnovi sodne prakse so najpogostejše tožbe proti delodajalcem, ki se nanašajo na:

- nedopustno vpletanje v zasebnost,
- zlorabo imena in podobe,
- nedopustno publiciteto zasebnega življenja,
- publiciteto, ki neosnovano postavlja v napačno luč pred javnostjo.

Sodišča pa niso pretirano navdušena za brezpogojno varovanje pravice zasebnosti delojemalca. Pri Nissanu sodelavka, ki je tožila firmo zaradi seksualnega vznemirjanja preko interneta, ni uspela, ker se je firma zavarovala s pisnimi izjavami, da bodo vsi zaposleni internet uporabljali le za službene potrebe. Sodišče tudi ni podprlo tožbe delojemalca, ki so mu v njegovi odsotnosti »prebrskali« njegov službeni PC, saj so to utemeljili s potrebo delovnega procesa. Firma pa je plačala kazen v primeru, ko so na ta način pridobili podatek o zdravstvenem stanju zaposlenega, do katerega niso bili upravičeni.

Pogostno je zmotno prepričanje delojemalcev, da jim izbira gesla jamči zasebnost v omrežju, dejansko pa delodajalci obvladujejo vsa gesla. Seveda bi bilo etično, če bi ljudem to tudi odkrito povedali. Ko gre za internet v javnih službah, je nadzorovanje lahko upravičeno tudi z »višjimi interesi« in delojemalec bo moral dokazati, da je varovanje njegove zasebnosti nekega izrecnega pomena.

Uvajalka elektronske pošte pri Epsonu je tožila lastno firmo, ker je na tečaju zagotavljala, da je zaupnost komuniciranja preko interneta samoumevna,

potem pa je odkrila, da je resnica drugačna. Sodišče je presodilo, da gre za utemeljeno nadziranje delovnega procesa, česar gospa ni razumela. Noben zakon ne zagotavlja splošne zasebnosti elektronske pošte na delovnem mestu. Ponudniki sistema elektronske pošte imajo, nasprotno, izrecno pravico prestrezati komunikacije na svojih sredstvih, če gre za vzdrževanje sistema ali za preprečevanje škode na premoženju. Delodajalec v firmi z internetom je praviloma tudi ponudnik internetnega servisa zaposlenim in vse ostalo postane jasno samo po sebi.

V servisu za rezervacije letalskih vozovnic American so ugotovili, da nekdo opravlja rezervacije »na zalogo«, na koncu pa vozovnice ostajajo neprodane. »Razkrinkana« firma jih je tožila zaradi prestrezanja informacij, a sodišče je dalo prednost lastniškemu interesu pred interesom zasebnosti. Tudi sistemi nadzorovanja kvalitete v firmah so primerna osnova za legalno prestrezanje komunikacij zaposlenih, ki bi se morali tega zavedati.

Sklicevanje na to, da so preko interneta firme dopustne le službene komunikacije, sproža dve različni ravnanji: kontekstualno ali vsebinsko. Sodišča praviloma vedno odobrijo prestrezanje komunikacij do točke, ko je mogoče določiti, ali gre za službeno ali privatno potrebo. Delodajalci pa radi sežejo preko te meje in nadzirajo celotne vsebine sporočil, kar sodniki težje sprejmejo, če ni podpisano vnaprejšnje soglasje prizadetega (formular ob sklenitvi zaposlitvene pogodbe). Nekateri sindikati predlagajo, da bi nadzorovanje uredili odvisno od dobe zaposlitve v firmi: prvih 6 mesecev popoln nadzor, prvih 5 let po dve uri tedensko, po petih letih pa nadzora ni več.

Dejansko zadeva za delodajalce ni čisto preprosta, saj jih lahko nerazsodnost njihovih zaposlenih na internetu spravi v velike težave. Slavni Bill Gates je plačal 2,2 milijona, ker so »mačoti« iz tehnološkega oddelka preko omrežja firme s seksualnimi opolzkostmi prizadeli sodelavke v informacijskem oddelku. Takšnih primerov pa je še cel kup. Pri Chevronu je bila firma obsojena na 2 milijona zaradi žaljivega kviza na njenem omrežju o tem, zakaj je pivo boljše od žensk? Prodigy je plačal, ker je nekdo preko njihove oglasne deske nesramno ozmerjal neko znano osebo.

Nadzorovanje interneta opravičujejo delodajalci tudi s tem, ker se z neskončno lahkostjo dogajajo izdaje poslovnih skrivnosti. Borland je na ta način prestregel sporočilo konkurenčni firmi, ki mu je povzročilo znatno škodo. Sodišče je sprejelo dokaz in oglobilo tako »izdajalca« kot konkurenčno firmo.

Internet, ki se mu praktično ne morejo več izogniti, pa spravlja v škripce poklice, v katerih veljajo etična načela varovanja zaupnosti klientov: advokati, zdravniki, duhovniki ... Pri internetu ni zanesljivega jamstva, da zapisa ni kdo prestregel. A popolnoma enako je pri mobilni telefoniji, kjer je začuda zadržkov precej manj.

Pri nas še ni bilo slišati pritožb sindikatov, češ da jih omejujejo pri rabi interneta v firmah, v svetu pa to že postaja torišče sindikalnega boja. Za ameriške delodajalce je sindikat izrecna »nevarnost za firmo« in ga tako tudi obravnavajo ter preprečujejo neomejeno komuniciranje z zaposlenimi preko interneta na delovnem mestu. Ker morajo spoštovati tudi zvezni zakon o delovnih razmerjih, se praviloma odločajo za omogočanje dostopa do oglasne deske v firmi, ki je zaposleni ne morejo brati med delovnim časom.

Da bi se izognili rizikom, ki jih prinaša internet, se firme trudijo z definiranjem razvidne internetne politike in pravilnikov o uporabi interneta. Izhodišče je dejstvo, da so delodajalci lastniki in upravljalci interneta v firmi. Iz tega sledi naslednje:

1. Zaposleni morajo vedeti, da je sistem namenjen službeni rabi, zato ga firma nadzira kot vsako drugo delovno sredstvo. To načelo naj se izpiše na ekranu vsakič, ko se delojemalec priključi.
2. Opozoriti je treba, da bo uporabnik sam odgovarjal za vsakršno neprimerno komunikacijo – žalitve, obscenost.
3. Ni treba omejevati delodajalčevega vpogleda v sistem – prav vse je lahko v funkciji poslovanja.
4. Pri uporabi ni izjem, ne za dobrodelne, ne za rekreativne, osebne, sindikalne ali druge namene. Vse to naj pokrije oglasna deska, za katero poskrbi delodajalec.
5. Opozoriti je treba, da tudi sprotno brisanje zapisov ni ovira za njihovo nadziranje.
6. Delojemalci naj podpišejo soglasje o pravici delodajalca, da pregleduje informacije v sistemu.
7. Kršitve so razlog za uvedbo disciplinskega postopka.
8. Delodajalec zajamčeno nima nobenega drugega razloga za nadzorovanje interneta kot zgolj poslovni interes.
9. Informacije se vedno sporočajo le tistim, ki se jih neposredno tičejo, kar zmanjšuje nevarnost neprevidnih objav in njihovih posledic.

Povsem jasno je, da se pri nas odnosi v zvezi z internetom na delovnem mestu še niso izoblikovali. Ni nujno, da bodo povzete izkušnje od drugod obveljale tudi v Sloveniji, saj se to področje nasploh zelo hitro spreminja. Lahko pa bi se izognili kakšni od težav, če bi dovolj zgodaj odprli razpravo o teh temah, kar je tudi namen tega prispevka.

III. Ogrožanje zasebnosti v trgovini na internetu (nadležna pošta)

Vsakomur, ki uporablja internet, je znan pojav nezaželenih sporočil, ki kradejo elektronski prostor,

čas in pozornost. V spletnem prostoru jim pravijo »spam« (menda so si ga izmislili v Monty Pyton's Flying Circus), mi pa predlagamo izraz »nadležna pošta«.

Tipično za nadležno pošto je: (13)

- da vam jo pošilja nekdo, s katerim doslej niste imeli nikakršnega odnosa;
- da so sporočila praviloma polresnice, torej zavajajoča;
- da ni mogoče identificirati osebe, ki stoji izza sporočila;
- firma, ki nastopa v sporočilu, ima navadno zveneče ime, ki spominja na nekaj, a ko natančneje premislite, zanjo še niste slišali.

Nadležna pošta ima seveda zagovornike, ki trdijo, da je to pač oblika elektronskega neposrednega trženja in se je treba nanj privaditi. Če koga moti, pa naj jo zbriše! Stvar pa ni tako preprosta in glede na razširjenost gre za enega najhujših napadov na informacijsko zasebnost uporabnikov interneta. Po zmernih ocenah znaša nadležna pošta 5-15% elektronske pošte.(14) Po bolj napetih ocenah pa celo 30%.(15)

Nadležna pošta je neznansko ceneno oglaševanje, saj lahko navaden PC, povezan v internet z 28,8 Kb modemom sproducira 100 elektronskih sporočil na minuto. V mesecu dni je to 26 milijonov sporočil, kar pošiljatelja stane vsega 4000 SIT. Kdo bi se temu odrekel? A na drugi strani za prejemnika stvar ni poceni in tudi preprosti klik na "delete" stroškov ne zmanjša. Za brisanje milijona takih sporočil je potrebnega mesec dni klikanja. Povprečni uporabnik interneta na leto za brisanje nadležne pošte porabi več kot dve uri. Za nadležno pošto plača uporabnik tudi lastniku poštnega strežnika, kjer je običajna tarifa od 5000 do 40.000 SIT mesečno. Bolj ko je internet zamašen z nadležno pošto, višjo hitrost zvez si je treba naročiti in večja je najemnina.

Stroški nastajajo tudi pri ponudnikih internetnih storitev oz. pri upravljalcih sistemov elektronske pošte. Skrivaštvo pošiljateljev nadležne pošte večkratno povečuje obseg dejavnosti skrbnikov. Neredko kot povratni naslov navedejo nič krivega uporabnika, ki se mu začnejo dogajati nenavadne, drage in časovno potratne stvari.

Morda sploh največja škoda pa je finančno neizmerljiva in pomeni diskreditiranje interneta kot resne komunikacije.

Največje težave na internetu povzroča naslednja nadležna pošta:

- piramide, ki vabijo k neverjetnim zaslužkom z minimalnimi vložki;
- ponudbe proizvajalcev nadležne pošte, da po določenih cenah izvedejo oglaševanje za naročnike;
- verižna pisma z bolj ali manj bedastimi izgovori;
- ponudbe za delo na domu, ki so običajno nelegalne;
- ponudbe shujševalnih pripomočkov, zdravstveni nasveti ipd., večinoma pravno problematične;
- pridobivanje vplačil za fiktivne agencije za neposredno trženje;
- lažne investicijske ponudbe;
- počitniške ponudbe po nizkih cenah, ki se šele v hotelu izkažejo za neresnične;
- itd...

Nadležna pošta je postala problem že v omrežju ARPA konec sedemdesetih. V osemdesetih so največjo zgago povzročala verižna pisma, ki so dejansko drugo ime za prve viruse na internetu. Ob takratnih zmogljivostih (in ceni!) računalniškega spomina je bilo katastrofalno, da je sporočilce 2 Kb po štirih kolenih že naraslo na 20 Mb, v petem ali šestem kolenu pa se je računalnik sesul.

Toliko kot nadležna pošta je star tudi odpor proti njej. V vrsti primerov je bila uporabljena taktika »zob za zob«. Kralju »spama« Jeffu Slatonu, ki je javno opravičeval vznemirjanje vseh telefonskih naročnikov, je znani moderator Patrick Towson vrnil tako, da so mu vsi telefonski naročniki nasuli sporočila v njegov računalnik in ga zadušili. Danes je znano, da borci proti nadležni pošti agresivneje kršijo zakone od samih pošiljateljev.

Za tehnološko podporo nadležne pošte ni lepšega kot cenena (ali celo brezplačna) internetna povezava. Ta pošta je največja grožnja za obstoj subvencioniranih akademskih omrežij. Nadalje je potrebno razpolagati s čim obsežnejšo adremo elektronskih naslovov, ki se jih odkupuje ali krade. Programi za razpošiljanje pošte so preprosti in poceni. Preostane še aranžman za zbiranje vplačil, ki mora biti primerno prikrit. Gre torej za sila preprost posel, ki se bo v bodočnosti še širil in slej kot prej zajel okolja, ki so ta trenutek še slabo pokrita z nadležno pošto.

Nadležna pošta je vsekakor družbeno vprašanje, zato je normalno, da ob njem pomislimo na pravne vidike. Pegasus je primer licencirane programske opreme, ki preprečuje zlorabljanje elektronske pošte. Pri roki je seveda odškodninska tožba za škodo, ki jo povzroči nadležna pošta, vendar pot do poplačila ni lahka. Potrebna je širša organizacija in na ta način je družba R&D Associates dosegla svoje, kar je videti na njihovi spletni strani http://www.kclink.com/spam>. Podobno so se problema lotili v združenju Citizens Inc., ki izstavlja račune pošiljateljem pošte za uporabo poštnih nabiralnikov, telefonov in računalnikov. Uspešni so tudi nekateri veliki ponudniki internetnih servisov, ki jih nadležne pošiljke diskreditirajo pri naročnikih: Juno Online je na ta način izterjal 5 milijonov odškodnine, Hotmail pa blizu pol milijona.(16)

Uspešnih je bilo nekaj kazenskih ovadb, ki zvečine izhajajo iz prevar, vsebovanih v nadležni pošti, ali navajajo vdore v zasebne informacijske sisteme.

V Sloveniji še nisem slišal za organizirano koalicijo proti nezaželenim komercialnim sporočilom. Ne verjamem, da bi bili prejemniki pri nas kaj manj občutljivi, pač pa trgovci še niso prav dojeli, kaj se jim z internetom ponuja. To je nedvomno srečna okoliščina, saj je že ali pa bo še na voljo cel kup brezplačnih orodij za boj proti nadležni pošti, za katera so poskrbela številna združenja prizadetih uporabnikov interneta. Enako pomembno pa je informiranje javnosti o problematičnih straneh vsiljivega elektronskega trgovanja, saj ga sicer ljudje vse preradi razumejo kot normalno stanje.

Po ameriškem vzoru je bila leta 1999 ustanovljena EuroCAUCE. (17) Njeno poslanstvo je izboriti zakonodajo, ki bo omejila škodljivo razsežnost nadležne pošte. Mobilizacijska parola za pridobivanja članstva je »Ne pustite se imeti za norca!«. Na njeni spletni strani so na voljo tudi brezplačna orodja za boj proti nadležni pošti.

Pri vsem tem ne gre zgolj za individualno vznemirjenost in jezo, pač pa ima nadležna pošta tudi narodnogospodarsko razsežnost: nobelovec Ronald Coase je dokazal – kar prebivalci bivših socialističnih držav vemo iz izkušnje – da nesankcionirano porazdeljevanje stroškov med nedolžne plačnike na koncu vedno privede do razpada ekonomskega sistema. Na ta način se namreč usodno deformirajo kriteriji učinkovitosti trga – nevidne roke, ki uravnava ponudbo in povpraševanje. Do nadležne pošte je treba biti moralno neizprosen: kraja je kraja, tudi če gre v posameznem primeru za majhen denar. Pet tolarjev ni nič, a če jih ukradeš slehernemu Slovencu, je to veličasten mercedes.

Za razliko od delojemalcev, ki vsaj vedo, kdo in kako zbira podatke o njih na internetu, sodobni potrošniki o tem nimajo pojma. Vedo le, da je njihov poštni nabiralnik na internetu zamašen z nezaželeno pošto. Nelegalno zbiranje in obdelovanje osebnih podatkov za tržno rabo je dodatno zaskrbljujoče, ker ni razmejeno od politične rabe. CCN, eden največjih svetovnih ponudnikov osebnih podatkov (43 milijonov naslovov posameznikov, 18 milijon naslovov gospodinjstev, 30 milijonov finančnih izkazov itd...) odkrito kupuje volilne sezname strank in jih najbrž tudi prodaja. Pri pametnih karticah, ki nam tako priročno olajšujejo nakupovanje, je dobro pomisliti, kaj vse izdajatelji vedo o nas, da lahko jamčijo za našo solidnost. Obvladati tržišče dejansko pomeni razpolagati z informacijami o kupcih. Orwell si ni predstavljal, da sploh ne bo država tista, ki bo nakopičila največ podatkov o ljudeh, ampak bodo to trgovci.

Vidmar in Flaherty sta na tej podlagi naredila daljnosežne sklepe, da se je tudi potrošnja preselila v sfero prisile in da živimo zgolj v iluziji svobodne izbire v trgovini, dejansko pa si prodajalci izberejo nas in proti temu ne moremo skoraj nič. V anketi se 70% potrošnikov zaveda problematičnosti situacije, ko firme kupujejo podatke o potrošnikih.(18) K temu bi imel kaj dodati tudi Jürgen Habermas, da se je namreč zrušila pravična kupoprodajna pogodba, ki je temelj meščanske demokracije.

IV. Sklepna razmišljanja o vplivu interneta na varovanje zasebnosti

Že od osemdesetih let sem so računalniki in preko njih kontrola informacij nesporno glavni način nadzorovanja ljudi.(19) Roger Clarke ugotavlja, da se je nadzorovanje (surveillance) na ta način preoblikovalo v podatkovno nadzorovanje (dataveillance). Pa vendar bi bil sklep, da računalniki sami določajo obseg nadzorovanja ljudi, napačen. Ob vsem kopičenju zapletene opreme še vedno ni nihče presegel svetovnih rekorderjev v nadzorovanju Stalina, Maocetunga, Pol Pota ali Honneckerja, ki so vse skupaj delali »peš«. Bolj kot tehnologija botrujejo sodobnemu nadzorovalnemu naskoku na zasebnost zaslužki: v izogib finančnim rizikom je treba informacijsko obvladati čim več spremenljivk – konkurenco, zaposlene, potrošnike, stroške, cene, tečaje... Tudi države se ravnajo po tej logiki in praviloma nihče nima večjih baz osebnih podatkov od davčnih uprav. Iz tega sledi, da bi bil vsakršen tehnološki determinizem glede ogrožanja zasebnosti neutemeljen in vedno se je treba vprašati, kakšne namene imajo institucije, ki posedujejo informacijsko tehnologijo.

Čeprav govorimo o osebnih računalnikih, stroji dejansko niso naravnani na osebo, ampak jih takšne naredimo mi sami. Po zasnovi pa nas računalnik, enako kot štedilnik ali brivnik, obravnava le kot anonimnega uporabnika. V začetnem obdobju interneta tudi ni bilo nobenih tehničnih postopkov za zagotavljanje kontrole komuniciranja, ampak je veljalo, da je to treba urediti s socialnimi pravili. (Nadzor dostopa je prišel šele z večuporabniškimi sistemi.) Nadzorovalno funkcijo dobi računalnik izključno v kontekstu institucije, kar se ujema s Feenbergovo ugotovitvijo, da so stroji tako ali tako le epifenomeni širših socialnih procesov.(20) Tudi človekova zasebnost je dejansko institucionalna komponenta in oboje skupaj tvori človekovo identiteto.(21) Vstop informacijske tehnologije v to razmerje je povzročil bistveno spremembo in pojavila se je »digitalna persona«.(22)

Pretresljivo je spoznanje, da nas ta podatkovna podoba, nekakšen alter-ego, vse bolj obvladuje.(23) Ljudje slutijo, da se o njihovem »dobrem imenu« odloča na odtujen način in jih je tega strah. Pošten pogled iz oči v oči je smešen preostanek preživelih običajev. Sedaj smo prisiljeni svojo odtujeno digitalno podobo ponujati v zamenjavo za družbeno priznanje,

na podlagi katerega lahko računamo z možnostjo zaposlitve, najema kredita, medicinske pomoči itd... Položaj »dodatka k stroju« ima zgodovinske vzporednice in neredke so tudi reakcije, ki spominjajo na ludizem v začetkih industrijske revolucije. Kot je šlo za zmoto takrat, je tudi danes po sredi nerazumevanje vloge tehnologije, ki ne more odgovarjati za sprevrženost institucij.(24)

Ali informacijska tehnologija res napeljuje vodo na mlin centralizacije oblasti, celo nove avtoritarnosti? V prvem obdobju razvoj računalništva tja do osemdesetih se je splošno potrjeval Groschev zakon, da večji ko so računalniki, bolj so učinkoviti. Prevladovala je zvezdna struktura organizacije, z velikim računalnikom v centru ter bolj ali manj neumnimi terminali na periferiji. Načelo »večje je boljše« se prilega centralističnemu upravljanju s podatki, hierarhični strukturi organizacije in avtoritarnemu načinu vodenja.(25) Tak pristop tudi predpostavlja, da obstajajo superiorni posamezniki, ki obvladujejo neuko čredo, kar je računalnikarjem sila prijalo, pa če so si to priznali ali ne. (Takoj so se tudi oblekli v bele halje, kar je običajen statusni simbol privilegiranih poklicev.) Prvi veliki projekti informacijskih centrov so se nanašali na preštevanje, razvrščanje, analiziranje, nadzorovanje itd. množic ljudi. Nastali so sistemi identifikacije, vseobsežni registri ter centralna državna telesa za upravljanje s posvečeno informacijsko tehnologijo. Če realnost ni bila primerna za računalniško obdelavo, so jo kar malo popravili in približali »duhu časa«.

Zgodila pa se je velika sprememba v razvoju informacijske tehnologije. Apple, IBM/PC in Macintosh so se bliskovito uveljavili na vseh koncih in krajih. Sistemski inženirji (v belih haljah) so preko noči izgubili moč odločanja o tem, kdo, kaj in kdaj bo delal na računalniku. Ne le, da PC ni več legitimiral centralizirane, avtoritarne oblasti, ampak jo je začel močno spodjedati. Velikanski razvoj je naredila komunikacijska tehnologija, ki je omogočila povezovanje računalnikov v neskončna ploska omrežja, s čemer je padla prejšnja hierarhična zvezdna struktura pametnega procesorja in butastih terminalov.

Internet prinaša zelo drugačno kulturo od tiste, ki je vladala v zvezdnih omrežjih, saj priznava imaginacijo in svobodo ter odpira nove možnosti samoizobraževanja, druženja itd... Ironija je, da je nastanek interneta sponzorirala vojska. Po drugi strani pa so prav tam prvi naleteli na omejitve centralizma ter spoznali njegovo ranljivost. Internet je prispodoba stabilnosti, robustnosti in redundance.(26) ZDA so si na tej osnovi zagotovile nov razvojni ciklus, Sovjetska Zveza s PC-ji v »samizdatu« in »inter-njetom« pa je propadla.

Zasebnost je večinoma razumljena kot pravica, kar povzroča težave, saj je pravica načelno zmeraj absolutni standard in jo imaš ali pa je nimaš. V resnici je stvar veliko bolj slojevita. Varovanje zasebnosti je proces iskanja ustreznega ravnovesja med zasebnostjo in mnogoštevilnimi konkurenčnimi interesi. Zelo pogosta je napačna izključna usmerjenost na varovanje podatkov, namesto na varovanje integritete ljudi, ki se jih podatki tičejo.(27) Še bolj zožene opredelitve varovanja podatkov se poslužujejo informatiki, ki v tej zvezi govorijo le o načinu preprečevanja, da bi nepooblaščene osebe spreminjale podatke v bazah podatkov ali v fazi njihovega prenosa.

Kot je država postopoma izgubljala monopol nad informacijsko tehnologijo, je začela tudi iskati izgovore, da ne more več jamčiti varovanja osebnih podatkov. Clintonova administracija je začela previdno razlagati, da so tudi osebne informacije pač le tržno blago in morajo biti prepuščene tržni samoregulaciji. Zasebnost se je znašla na »brisanem prostoru« med etiko in ekonomijo. Etika trdi, da gre pri zasebnosti za fundamentalno vrednoto in ne za nekaj, kar si posameznik kupi. Ekonomija pa ugotavlja, da se z osebnimi informacijami dejansko trguje in jim ljudje mirno določajo tržno ceno.(28) Se pa znajo tudi ekonomisti sami v zvezi z zasebnostjo zaplezati: obenem ko trdijo, da je treba vse informacije obravnavati kot blago na trgu – kar pomeni, da si jih eni lahko privoščijo, drugi pa ne – v svojih tržnih modelih izključujejo varovanje informacijske zasebnosti kot anomalijo, saj morajo biti vse informacije brezplačno na voljo vsem. Ni mogoče izključiti možnosti, da se bo pojavil model varovanja zasebnosti, ki bo deloval po logiki tržnih pravil.

Sicer pa je Michael Rubin že na začetku razmaha informacijske tehnologije zasejal dvom, ali nas koncept zasebnosti sploh usposablja za spoprijem z novimi oblikami nadzorovanja. Avtonomni individualizem je postal veliko razkošje in si ga lahko privoščijo, kupijo le najbogatejši, revni pa se mu »prostovoljno« odpovedujejo, ker je zanje predrag.(29) Ali naj na tem temelji neka temeljna pravica?

Zunaj primarnih skupin smo ljudje navajeni na anonimnost. Na ta način nakupujemo, potujemo, se zabavamo, participiramo v javnosti, izražamo verska čustva, morda tudi uporabljamo posebno vrsto zdravstvenih storitev ... Anonimna je tista človekova transakcija, ki ne pušča za seboj podatka, povezljivega z določenim posameznikom. K anonimnosti nas navajajo družbene vrednote ali tudi izogibanje osebni odgovornosti.

Vrsta transakcij pa predpostavlja osebno preverjanje: naročanje blaga in storitev, udeležba v formalnih postopkih pred sodišči ali upravnimi organi, pridobivanje občutljivih podatkov itd... Priče smo vse hujšemu pritisku v smeri pretvarjanja anonimnih v preverjene transakcije, kar je posledica:

- naraščanja števila socialnih institucij,
- povečevanja razdalje med institucijami in posamezniki,
- upadanja zaupanja med ljudmi,
- povečanih zmogljivosti informacijske tehnologije.

Podatkovna intenzivnost družbenega življenja se je na prelomu stoletja neznansko povečala in tudi to sproža nelagodje in občutek ogrožene zasebnosti. Očitna je želja umikanja v anonimnost, čemur je mogoče ustreči na način psevdonimnosti. Pri psevdonimni transakciji ni neposrednega identifikatorja, pod posebnimi pogoji pa je identifikacija možna s pomočjo zaprtih indeksov. Za to je potrebno pravno, organizacijsko in tehnično varovanje, kar ni nobena posebna težava. Vrsta ljudi ima ne le željo, ampak utemeljeno potrebo po takšni psevdonimnosti, saj bi po tej poti zmanjšali tveganja, katerim so iz teh ali onih razlogov izpostavljeni.

Pojavila se je tudi nova tehnologija PET (Privacy-EnhancingTechnology), kar je tehnični in organizacijski koncept, ki pomaga varovati zasebnost uporabnikov interneta. Označujejo jo tudi kot »agenta za anonimizacijo« ali »agenta za psevdonimizacijo«.(30)

Ali nas lahko PET reši? So tudi opozorila, da gre predaleč in da so možne kriminalne zlorabe. Sedaj se še redko uporablja, ker mora programsko opremo uporabnik sam najti na internetu in jo tudi obvladati. Morda pa bi morali ponudniki internetnih storitev PET nuditi svojim strankam v običajnem paketu storitev?(31)

Zadnja leta se je zelo razširilo razpravljanje o etiki interneta. K temu so prispevale afere v zvezi s pedofilstvom, pornografijo, kršitvami copyrighta ... Kazensko preganjanje kršiteljev ni učinkovito. Srečujemo pa se s protislovno situacijo, ko je na voljo vse več orodij za cenzuriranje interneta, hvalimo pa tudi Digital Freedom Network za prebijanje kitajske cenzure. Omemba cenzure upravičeno vzpodbudi ogorčene proteste, čeprav Charles Oppenheim zagotavlja, da nobena cenzura v resnici ne more ogroziti interneta, saj je narejen, da bi preživel atomsko vojno.(32)

Enostavni klik na »send« je za mnoge neobvladljiva skušnjava, da se s svojimi sporočili prenaglijo. Kopičijo se žalitve, klevete, kraje avtorstva ... Prodigy je poizkušal stvari izboljšati s preprostim postopkom, da med klikom in dejanskim odhodom sporočila preteče obveznih 10 minut, ko odpošiljatelj lahko še malo premisli o posledicah in zadevo popravi.

Tudi ko je komunikacija na internetu organizirana v elektronskih diskusijskih skupinah (EDG), so njihovi moderatorji pred resnimi etičnimi dilemami, do katere meje posegati v sporočila. Ali naj zahtevajo popravke prispevkov? Ali naj izločijo prispevke, ki so za kogarkoli potencialno žaljivi? Ali naj uveljavijo načelo preprečevanja družbene škodljivosti? Koncept varovanja zasebnosti jim pri tem ne pomaga prav veliko. Svoje izhodišče morajo nujno razširiti na etiko interneta.(33)

Electronic Privacy Information Center (EPIC) je pregledal 100 najbolj obiskanih spletnih strani, ki zajemajo tudi osebne podatke, in ugotavljal, ali se ozirajo na zasebnost ali ne. Skoraj polovica jih zbira osebne podatke, ne da bi posameznike o tem kaj vprašali. Le 17 je takih, ki na svojih straneh omenijo pojem zasebnosti in lahko dobrohotno sklepamo, da so na ta element vsaj pomislili. Vsi drugi pa nič in med temi so tako znamenita imena kot Geocities, Excite, New York Times, Lycos in še mnogi drugi.

Še najmanj preseneča, da je do skoraj enakega rezultata prišla ameriška Zvezna trgovinska komisija, ki je za leto 1998 ugotovila, da je 92% komercialnih spletnih strani zbiralo osebne podatke o potrošnikih, a le 14% od njih je imelo njihovo privolitev. Nekateri nudijo tudi prodajne popuste, če se kupec pusti popisati, kar je nedvomno etično problematičen pritisk na revne ljudi.(34)

Že od samih začetkov računalništva je znano zdravilo za mnoge od »bacilov«, ki najedajo informacijsko zasebnost – to je šifriranje sporočil. Z njo pa trčimo v jedro problema zasebnosti, ki se mu reče nadzorovanje. Včasi preprosto ni več jasno, ali se zakonodaja o varovanju osebnih podatkov ne sprejema prav zato, da bi onemogočila to najučinkovitejše sredstvo varovanja informacijske zasebnosti? V nekateri državah si dajo agencije za varovanje podatkov največ opraviti s preganjanjem šifriranja. Vprašanje gotovo ni preprosto, saj se s stopnjo družbene razvitosti povečujejo tudi riziki, pred katerimi se je treba kolikor mogoče učinkovito zavarovati. V to očitno spada tudi nadzorovanje interneta, čemur dajejo državni organi praviloma prednost pred varovanjem zasebnosti.

Viri

1 Big Brother Incorporated, Privacy International *http://www.privacy.org/pi/reports/*

2 Report of the Committee on Privacy and Related Matters, David Calcutt QC, 1990. Cmnd. 1102, London: HMSO

3 Convention on the protection of individuals with regard to the automatic processing of personal data. Convention, ETS no. 108, Strasbourg, 1981. *http://www.coe.fr/eng/legaltxt/108e.htm*

4 Directive 95/46/EC of the European Parliament and the Council of 24. Oct. 1995 on the protection of individuals with regard to the processing of personal data and on free movement of such data. *http://www.odpr.org/restofit/Legislation/Directive/Directive_Contents.html*

5 Directive 97/66 /EC of the European Parliament and the Council of 15. Dec. 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. *http://www2.echo.lu/legal/en/dataprot/protection.html*

6 European Parliament, Scientific and technological options assesment (STOA), An appraisal of technologies of political control, 6. Jan. 1998. *http://jya.com/stoa-atpc.htm*

7 American Management Association, Report on electronic monitoring&surveillance,1997. *http://www.amanet.org/survey/elec97.htm*

8 *http://www.epic.org/reports/surfer-beware.html*

9 *http://www.gilc.nl/privacy/survey/intro.html*

10 Banisar, David Excerpt from US State Department Report worldwide privacy abuses. *http://www.privacy.org/pi/reports 1995_hranalysis.html*

11 Dichter, S. Mark and Burchart S. Michael Electronic interaction in the workplace: monitoring, retrieving and storing employee communications in the internet age. *http://www.mlb.com/speech1.html*

12 Kelbl, Barbara in Vehovar, Vasja RIS99 – podjetja, FDV/CMI Ljubljana, marec 2000.

13 Cranor,L.F. and LaMachia, B.A. Spam! Communication of the ACM, 41(8) 1998.

14 Schwartz, A. and Garfinkel, S. Stoping spam, Sebastopol/CA: O'relly 1998.

15 *http://www.cauce.org/about/problem.shtml*

16 Sorkin, David *http://host1.jmls.edu/cyber/cases.html*

17 EuroCAUCE *http://www.euro.cauce.org/en/index.html*

18 Vidmar, Neil and Flaherty, David Concern for personal privacy in an electronic age. Journal of Communication, 35, 1986.

19 Marx, T. Gary and Reichman, Nancy Routinizing the discovery of secrets: computers as informants. American Behavioral Scientist, 27(4), 1984.

20 Feenberg, Andrew Alternative modernity: the technical turn in philosophy and social theory. Berkeley: University of California Press, 1995.

21 Agre, E. Philip The architecture of identity: embedding privacy in market institution. Informations, Communications and Society 2(1), 1999. *http://dlis.gseis.ucla.edu/people/pagre/architecture.html*

22 Clarke, Roger The digital persona and its application to data surveillance. The Information Society, 10(2), 1994.

23 Laudon, C. Kenneth Dossier society: value choices in the design of national information systems. New York: Columbia University Press, 1986.

24 Lyon, David New technology and the limits of ludism. Science and Culture, 7, 1989.

25 Clarke, Roger The eras of dataveillance, prispevek na konferenci Computers, Freedom & Privacy – Chicago, marec 1994. *http://www.anu.edu.au/people/Roger.Clarke/DV/NotesDVEras.html*

26 Clarke, Roger Information technology: weapon of authoritarianism or tool of democracy? Predavanje na IFIP World Congress, Hamburg, 1994. *http://www.anu.edu.eu/people/Roger.Clarke/DV/PaperAuthism.html*

27 Clarke, Roger Introduction to dataveillance and information privacy, and definitions of terms. *http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html*

28 Kang, Jerry Information privacy in cyberspace transactions, Stanford Law Review 50(4) 1998.

29 Rubin, Michael Guilty until proven innocent. Information Management Review 2(1) 1998.

30 Cranor, Lorrie Faith »Internet privacy«, Communication of the ACM, 42(2), 1999.

31 Tavani, Herman PET's, E-commerce, and ethics. CPSR Newsletter, 18(2), 2000.

32 Oppenheim, Charles The legal and regulatory environment for electronic information. Tetbury: Informatics Ltd., 1999.

33 Buchanan, A. Elisabeth and Netiva Caftori Ethics in technology. CPSR Newsletter, 18(2), 2000.

34 Spinello, Richard Moralty and law in cyberspace. Sudbury/MA: Jones and Barlet Publishers, 2000.

◆

Franci Pivec je diplomiral iz filozofije in sociologije. V bibliografiji prevladujejo dela o organizacijskih in sociooloških vidikih šolstva. Zadnja leta, ko je zaposlen na Institutu informacijskih znanosti v Mariboru, pa je objavil več študij, povezanih s pojavom informacijske družbe. Je tudi član posebne interesne skupine za informacijsko etiko pri IFIP ter aktivno deluje v FID.

◆