SOCIO-KULTURNI PRISTOP K RABAM INFORMACIJSKO-KOMUNIKACIJSKIH TEHNOLOGIJ KOT INTERDISCIPLINARNI OKVIR ZA PSIHOLOGIJO NOVIH TEHNOLOGIJ.

Primer analize razmer varnosti v računalniško posredovani komunikaciji.

Marko Habjan
Melikova 7, SI-1000 Ljubljana

IZVLEČEK

Kapitalistična produkcija se prilagaja današnji »varni verziji« družbe tako, da varnost kot vrednoto naredi dostopno na prostem trgu; jo torej komodificira, »poblagovlja« v potrošne dobrine, predvsem kot lastnost informacijsko-komunikacijske tehnologije. Organizacijski premik družbe, ki tej verziji sledi, se je začel izvajati kot projekt high-technology restrukturiranja družbe. Gnan je bil skupaj s strani vladnih in korporacijskih sektorjev, in je bil rezultat načrtnega uvajanja novih tehnologij: izvedel se je kot samouresničujoča prerokba realnosti, ki so jo napovedovali teoretiki informacijske družbe. A je impliciral nepričakovan in nepredviden obrat, saj rabe tehnologije upravljalski in korporacijski »tehnokrati« ne obvladujejo več popolnoma, kljub temu, da tehnologijo nenehno reproducirajo in jo izpopolnjujejo. Zaradi (pre)obilja informacij in proste izmenjave znanja ter izkušenj po tehnoloških poteh lahko danes ljudje izvajajo horizontalne do-it-yourself *ovinke mimo hierarhično strukturiranih računalniških varnostnih sistemov, ki jih prej niso mogli izvajati. Varnostni posegi tehnokratov, ob »primerni« medijski podpor seveda, v oblikovanju družbene percepcije tveganja občutek tveganja samo ojačajo ali oslabijo, ne pa šele povzročijo občutek tveganja. Ti posegi so v sklopu centralizirane in hierarhizirane birokratske paradigme upravljanja z umom in telesi velikega števila svetovne populacije, kjer država - če se osredotočimo konkretno nanjo - v dani ekonomski racionalnosti s svojimi občimi mikrostrategijami in multiformnimi taktikami oblasti fiksira vsakega individuuma (v lastni svobodi) posebej v pravno osebo. V takšnih razmerah se nahajata domači uporabnik in uporabnica, kar povzroča njuno negotovost. Strahovi, ki se pri rabi porajajo, so disproporcionalni do stvarnih pričakovanj glede učinkov rabe tehnologij ter se nazadnje premestijo še na vse druge tehnološke*

objekte. Percepcije tveganja, ideje o varnosti in kontroverze o tehnologiji, nimajo kaj dosti skupnega z znanstvenimi empiričnimi dokazi, ampak so raje oblikovane na podlagi kulturnih podmen in domnev o ranljivosti človeka, nazadnje povzročijo, da se v »kulturi zlorabe« vse prehitro spregleduje ključni pogoj, namreč, da si ranljivost zaradi lastne nevednosti ljudje povzročijo sami, oz. jim jo, namerno, zaradi njihove nevednosti in nesposobnosti spoprijeti se s problemi, povzročijo drugi prav zato, ker (to) vedo. V procesu viktimizacije se je torej pač lažje že v naprej videti kot žrtev, zlati v primeru, ko bo patologija zlorabe verjetno imela učinek postati samo-uresničujoča prerokba. Od tod končno izpeljujemo še interdisciplinarno načelo, da mora tudi znanost proučevanja človekove osebnosti vedno upoštevati socio-kulturne razmere in ideološke značilnosti, vpisane v tehnologijo, ki določajo načine rab IKT.

Ključne besede: varnost, vrednota, kapitalizem, informacijsko-komunikacijska tehnologija, nadzor, identiteta, politika, ideologija, javnost, paradigma upravljanja, nacionalna država, mrežna struktura moči, negotov domači uporabnik/uporabnica, družbena neenakost in izključenost, demokracija, medčloveški odnosi, heker, viktimizacija, interdisciplinarnost.

UVOD:
VARNOST KOT KOMODIFICIRANA VREDNOTA V DRUŽBENIH RAZMERJIH »HIGH-TECH« KAPITALISTIČNE PRODUKCIJE.

Rastoči trendi v globalizaciji: institucionalizacija virtualnega,[1] računalniška socializacija ter kulturalizacija tržne ekonomije (ko postaja kultura ena od glavnih sfer tržišča: *softwarska* industrija zabave, množični medijski izdelki, šport itd.), predstavljajo tri poenotujoče forme sodobne družbenosti. Ena od posledic teh trendov je **prevrednotenje** - med drugim tudi vzpon »vse bolj pomembnih« vrednot varnosti.[2] Kapitalistična produkcija se prilagaja današnji »varni verziji« družbe tako, da varnost kot vrednoto naredi dostopno na prostem trgu; jo torej komodificira, »poblagovlja« v potrošne dobrine. Ker pristojni centri moči sami/edini odrejajo standarde varnosti, ker ne-varnosti ustvarjajo pač drugi, je možnost »biti varen« samo ena in edina: ker nismo varni, se zavarujemo s ponujenimi rešitvami ali pa ostanemo ranljivi v ne-varnosti. V takšni, tržni paradigmi »informacijske« družbe, je logika, ki se »prodaja«, sledeča: z institucionaliziranjem univerzalnih varnih praks, ki omogočajo varno izvajanje partikularnih interesov, dosežemo relativno varnost za vse uporabnike/uporabnice enako. S tem pa odpravljamo tudi družbene neenakosti. Kapitalistični produkcijski sistem torej »kar sam« dela v skupnem interesu. Ali rečeno v teoriji ideologije: sam ideološko reproducira pogoje za svojo produkcijo, s tem, da jo razširja na potrošnjo oz. jo prilagaja končnemu cilju, tj. konsumpciji.

Ko raziskujemo sodobne informacijsko-komunikacijske fenomene, ne odpravljamo, ukinjamo ali zamenjujemo česa »starega«, modernega, z »novim«, »postmodernim«, ampak zgolj retroaktivno preoblikuje naravo predobstoječih pojavov, povezanih z informacijsko-komunikacijsko tehnologijo (IKT). Če soglašamo, da je osnovni metodološki problem vseh družbenih raziskav *konstrukcija objekta* raziskave, potem s tem tudi dopuščamo sprožitev takšnih spoznavnih rezov, ki jih iz

[1] Institucionalizacija kot proces družbene interakcije, v katerem nastajajo relativno stabilna pravila in načini za zadovoljevanje temeljnih družbenih potreb. V današnjem času postaja vedno več področij človekovega življenja in dela medializiranih z računalniško posredovano komunikacijo – od tod izraz »institucionalizacija virtualnega«.

[2] V izdaji *Glasila podjetja Microsoft* ***Microsoft Info*** (2002: 3), ki je tematsko posvečena varnosti, se uvodni članek začne z naslovom »Varnost – vrednota številka ena!«. Avtor članka med drugim zapiše: »Morebiti kar premalo cenimo varnost okolja, v katerem živimo. Za naše računalnike žal to ne velja. Nenehno so izpostavljeni nevarnostim, ki jih prinaša vpetost v svetovna omrežja.« Avtor tega članka si upa dodati, da pa prav nič bolj kot nevarnostim, ki jih prinaša vpetost v »globalno« okolje, v katerem živimo.

poprejšnjih teoretskih perspektiv in/ali znanstvenih paradigem ne moremo ustrezno podpreti, sprejeti ali razložiti. Takšen »neuspeh« je neposredni rezultat uspešne teoretske intervencije v objekte raziskovalne problematike, saj z ustvaritvijo nove zgodovinske realnosti premaknemo koordinate okvira realnosti. Če se navežemo na začetek, za ilustracijo uporabimo »desno-usmerjeni« politični premik k svobodni iniciativi (*free-enterprise*) od zgodnjih sedemdesetih let naprej, ko so »informacijsko revolucijo« imeli za projekt *high-technology* restrukturiranja družbe, gnanega skupaj s strani vladnih in korporacijskih sektorjev vsepovsod v naprednem (poznem, rečemo danes) kapitalizmu:

> Postindustrijska tehnokracija […] je nosila znamenje povezanosti z vladno birokracijo. Informacijska revolucija, bolj prilagojena klimi thatcherisma in reaganisma, to odpravlja. Tehnokracijo je nadomestila visoka tehnologija, človeka organizacije inteligentne mašine, eksperte ekspertni sistemi, inteligenco umetna inteligenca, ogromne računalnike mikroračunalniki, piramidne hierarhije distribucijskimi sistemi, osrednjo pisarno kiberprostor (Dyer-Witheford, 1999: 21-22).

Ta organizacijski premik je bil rezultat načrtnega uvajanja novih tehnologij, se je izvedel kot samouresničujoča prerokba realnosti, ki so jo napovedovali teoretiki informacijske družbe (ibid.: 22). A je impliciral nepričakovan in nepredviden obrat: »tehnologija se je obrnila proti tehnokraciji« (ibid., op. 30, 242). Današnji upravljalski in korporacijski »tehnokrati« rabe tehnologije **ne obvladujejo** več popolnoma, kljub temu, da tehnologijo nenehno reproducirajo in jo izpopolnjujejo. Trhlost fetišiziranja »Moorovega zakon«[3] »*hardware* kapitalizma« dokazuje njegovo nasprotje, tj. slab *software* (Lanier, 2000: spletni dokument). Poleg tega še celo nekateri vodilni v industriji IT priznavajo, da gre razvoj, npr. v proizvodnji mikroprocesorjev za osebne računalnike, naprej predvsem zaradi tehnoloških zmogljivosti in zmožnosti, ne pa zaradi potreb ali zahtev uporabnikov, ki – vsaj nekateri – to s pridom izkoriščajo. Hkrati se je pokazalo, da birokratski nadzor in posredovanje trga v menjavi nista več nujno učinkovita niti prisotna. Ti dve dejstvi sta zelo pomembno pri **vprašanju varnosti**: zaradi (pre)obilja informacij in proste izmenjave znanja ter izkušenj po tehnoloških poteh lahko izvajamo horizontalne *do-it-yourself* ovinke mimo hierarhično

[3] »Hardverska plat računalnikov še naprej postaja eksponencialno boljša in cenejša, kar je znano kot 'Moorov zakon'«. Da bo kvalitativne in kvantitativne vidike informacijskih sistemov neizogibno pospešil Moorov zakon, je eno do petih prepričanj »kibernetskih totalitaristov« (Lanier, 2000: spletni dokument).

strukturiranih računalniških varnostnih sistemov, ki jih prej nismo mogli izvajati. Zato morajo skrbniki teh sistemov vedno znova vpeljevati popolnoma nove metode nadzora za zagotavljanja varnosti. V tej, za »klasične tehnokrate« bolj negativno determinirani paradigmi varnosti, smo klasični webrovski birokratski »idealni tip« družbenega nadzora, kateremu smo se v preteklosti tako zelo približevali, a ga nikoli dosegli, kot »idealni« in kot »tip« moderne paradigme družbene organizacije že presegli ter tudi že preživeli. Zato neprestanemu **preseganju** in **prežitku ideala** skuša slediti tudi sodobna (bio)politika »diktature varnosti«, kjer so za »idealno« varnost nenehno potrebni nenehni popravki, intervencije, izboljšave; torej: tehnološka (kulturna) kolonizacija primarnega življenjskega okolja (narave) kot način oblikovanja sodobne družbene identitete v kulturi disfunkcionalnih presežkov.[4] Takšni posegi, ob »primerni« medijski podpori seveda, pa v oblikovanju percepcije tveganja družbeni občutek tveganja samo ojačajo ali oslabijo, ne pa šele povzročijo občutek tveganja (Furedi, 1997: 52). V javnosti izzovejo že implicirane in efektivne popularne strahove, konstantno prisotne ob vsakem »napredku« (tehnološke intervencije v telo, škodljivi učinki tehnologij v družbenem vsakdanu in tveganja v do sedaj neokrnjeni naravi, ki jih prej ni bilo ipd). Ti strahovi so **disproporcionalni** do stvarnih pričakovanj glede učinkov tehnologij ter se nazadnje premestijo še na vse druge tehnološke objekte. Napačne predstave, ki so največkrat posledica slabe obveščenosti javnosti, izzovejo strahove »pred neznanim« ter špekulacije o omejitvah, ki jih laična javnost zahteva glede trenutnega stanja in nadaljnjega tehnološkega razvoja ter aplikacij tehnologij. Znanost je (še vedno) negotova glede vpliva na zdravje ljudi: glede »možne« škodljivosti »stranskih učinkov« elektro-magnetnega sevanja baznih postaj in mobilnih telefonov npr., katerih jakost signalov anten je nižja od strogo arbitrarnih »mejnih vrednosti«, »smernic« ali »priporočil« za zagotavljanje varnosti, znanost zagotavlja, da »ni verjetna«, da (še) ni nekih empiričnih dokazov, ki bi upravičili škodljiv vpliv. Politika je (vedno bolj) brez neke učinkovite in avtonomne iniciative, da

[4] V življenjskih razmerah sodobnega sveta, v katerih je človek s kulturnimi inovacijami že tako presegel »…meje 'naravne' stopnje popolnosti, se pravi, da [je] stopi[l] čez to, kar lahko doseže zgolj z lastnimi viri« (Simmel, 2000: 68), izgleda, da bodo vse bodoče inovacije vse bolj in bolj nesmiselne, disfunkcionalne, tj. vedno manj koristne za osnovno funkcijo – preživetje (ker zaradi dviga kvalitete življenja niti ni več nobene potrebe po kulturnih inovacijah), in da bo človek preoblikoval preko vseh - kolikor toliko še - racionalnih meja ne le svojo »naravo«, ampak tudi zunanji svet, da na koncu ne bo ostalo sploh nič več »naravnega«. Seveda je to le teoretična futuristična napoved v dikciji kulturne kritike poznega kapitalizma, ki pa vseeno ima neke realne empirične osnove – vsaj kot izhodišče za teoretiziranje v nadaljevanju.

bi z ustreznimi prioritetami in intervencijami glede tveganja pomirila strahove v javnosti, ki sledijo nenehnemu prevrednotenju ideala varnosti. Scenarij »strahu« je v družbi torej popoln: tveganje javnosti ni empirično, ampak je najprej trancsendentalno, vedno komplementarno teoretično vkalkulirano.

PARADIGMA NADZORA *VERSUS* RAZLIČNE MOŽNOSTI RABE TEHNOLOGIJ

V poznem dvajsetem stoletju in na prehodu in v enaindvajsetem stoletju smo priče silovitim poskusom vzpostavitve nadzora nad **materialnimi tokovi** informacijsko-komunikacijskih tehnologij v procesu privatiziranja komunikacijke infrastrukture s strani velikih svetovnih monopolnih korporacij, multinacionalk, transnacionalnih blokov in nadzora nacionalne države s podeljevanjem koncesij. Slednja si prizadeva za upravljanje tokov s fleksibilnimi in horizontalnimi tržnimi deregulacijami, prvi pa nato z uvajanjem novih potrošniških praks, kar se, recimo, kaže v pripustitvi produkcijskih sil in produkcijskih odnosov v formi t. i. »*e*-ekonomije« in »*m*-ekonomije« v socio-ekonomsko bazo družbe. Vsi omenjeni subjekti legitimirajo svoje postopke s komplementarnimi drakonskimi (zakonskimi, *copyright* in patentnimi) pravnimi predpisi v pravno-politični družbeni nadgradnji. Vendar ti predpisi kot taki še vedno ostajajo del moderne centralizirane in hierarhizirane **birokratske paradigme upravljanja** z umom in telesi velikega števila svetovne populacije, kjer država – če se osredotočimo konkretno nanjo - v dani ekonomski racionalnosti s svojimi občimi mikrostrategijami in multiformnimi taktikami oblasti fiksira vsakega individuuma (v lastni svobodi) posebej v pravno osebo.[5] V tej paradigmi nadzora upravljalci življenje otežujejo, ga nasilno zadržujejo v fiksni coni in ga delajo še bolj restriktivnega, internet pa, kot vemo, nasprotno, implicira potencialne zmožnosti, da življenje napravimo lažje: »Informacije so zato, da si jih ljudje med seboj delijo, ne pa prodajajo. Znanje je dar, ne pa blago, namenjeno prodaji« (Barbrook, 2002: spletni dokument). Zaradi tega očitnega strukturnega protislovja med neoliberalnim kapitalizmom in nacionalno državo[6] ter uporabniki in uporabnicami, ali še drugače: nasprotja med posameznim in občim (interesom),

[5] V prvi vrsti sta takšni osnovi za instrumentalni nivo upravljalske oblasti ameriški »The Digital Millennium Copyright Act« in evropska »The EU Copyright Directive«, ustrezna konceptualna referenca tem taktikam in tehnikam pa je Foucaultov spis (1991) z naslovom *Governmentality.*

[6] Sodobna protislovja med neoliberalnim kapitalizmom in nacionalno državo puščamo ob strani za kakšno drugo priložnost.

lahko to protislovje poimenuje kot **'tehnokonflikt'** med **svobodo** in **nadzorom**. Udeleženci v tem konfliktu nas z ene strani neprestano prepričujejo, da je internet enostavno tehnološka nadgradnja starega medijskega sistema s pripadajočo pravno-politično legitimiteto, z druge o prostem internetskem izmenjevanju datotek in prostem programju (*free software*) kot znanilcu dekomodificirane družbe (»*software* komunizem«), s tretje o nujnosti in apriornosti načina uvajanja *e-in nekaj pač* storitev »informacijske družbe«, s četrte o koristnosti »odprte kode« za državne uprave itd. Kar koli pač zainteresirane strani trdijo v obrambo svojih stališč, gre za nadzor nad **dvojno mrežno strukturo moči**: (**a**) nad digitalno, tj. osnovno, najnižjo plastjo, internetno infrastrukturo z *bandwidth* posegi glede preklapljanja, širine in hitrosti prenosa ter nadzorovanja pretakajočih se podatkovnih paketkov; in (**b**) z inherentno zvezano družbeno strukturo, tj. sfero, naddoločeno z načinom materialne produkcije in reprodukcije. Če to strukturo povežemo še s tokovi semiotične uporabnosti podob in možnostmi cirkulacije blag, zadobijo digitalizirane oblike blag ideološki smisel in pomen nematerialne (re)produkcije, ki jo nekateri diskurzi tako radi zagovarjajo, v sferi virtualnega zato, ker nove tehnologije omogočajo neskončno digitalno predelovanje, kopiranje, replikacijo in simulacijo ter distribucijo vseh digitaliziranih oblik kot zgolj pogojno transformiranih, virtualni blag. Termin »pogojno transformiranih« vpeljujemo, ker ima virtualni objekti izvor vedno že v »materialni eksistenci« *off-line* sveta: ravno materialne lastnosti realnih objektov so tiste, ki tvorijo virtualni diskurz o teh objektih. Ko si nekdo s svetovnega spleta prenese glasbo v MP3 formatu na svoj računalnik, jo verjetno želi poslušati, kar pa je čim bolj kvalitetno najbrž želel tudi pred mrežnim načinom prenosa in poslušanja. Glasba je še vedno glasba, nov je torej samo način, ki ustvari jedro *tehnokonflikta*. Če stvar še nekoliko nadaljujemo, se pretok digitalnih vsebin, merjenih v M(ega)B(itih) na koncu vedno nekako legitimizira z nekim učinkovitim pravno-političnim diskurzom in proporcionalno kompenzira (najmanj ugodno, če si pravno-formalno prepoznan kot »pirat«). To pa nasprotuje prvotnemu nazoru odprtosti in prostemu širjenju kulturnih inovacij, ki je bil prvinska (nagonska, »naravna«) podlaga za javno vpeljavo interneta kot nehegemonega medija, tistega, ki ne sledi nomadski vojaški strategiji ARPANET-a ter oblastniški želji po redu in nadzoru vsega, kar je prosto (trg, komunikacija in dar).

VARNOST POSAMEZNIKA JE DRUŽBENO POGOJENA IN MU POSREDOVANA Z REPREZENTACIJAMI »VERZIJ« VARNOSTI

V neposredni povezavi s konfliktom, ki smo ga ravnokar »materialistično« utemeljevali, so percepcije tveganja, ideje o varnosti in kontroverze o tehnologiji, ki nimajo kaj dosti skupnega z znanstvenimi empiričnimi dokazi, ampak so raje oblikovane na podlagi kulturnih podmen in domnev o ranljivosti človeka. Izhajajo prav iz pogojne transformacije, zaradi katere ljudje prehitro menijo, da so v virtualnem osvobojeni vseh spon realnega sveta. Poznavalec razmer, »Internet engineering task force« (*Delo* 29.9.2002: spletni dokument), zatrjuje, da je »varnost zgolj iluzija«:

> Internet je zlepljen s protokolom BGP [Border Gateway Protocol], ki ga uporabljajo internetni ponudniki in operaterji, da vedo, kdo uporablja kateri del številskega prostora in kako usmerja promet. Vendar je protokol sam povsem nezavarovan. Veliko težav nastane že zato, ker operaterji in skrbniki teh omrežij naredijo napake – pomislite, kaj se lahko zgodi šele, če kdo ta omrežja namerno zlorablja! Zgodi se, da promet nepravilno usmerjajo ali – še huje – da ga usmerijo v »črno luknjo«. To pomeni, da se del internetnega prometa kar izgubi in ga je treba znova poslati. No, paketi se ne izgubijo, le pojavijo se na napačnem mestu, kjer jih usmerjevalniki pač zavržejo… [...] Ko smo raziskali zakaj, smo ugotovili, da se to dogaja zaradi napak pa tudi zaradi poskusov, ki so nepredvideno ušli tudi v odprto, javno internetno okolje. Jasno pa je, da bi take »napake« lahko kdo povzročil tudi namerno.

Nadaljuje, da je varnost pogosto prepuščena uporabnikom samim. Zato se nam kar samo postavi sledeče vprašanje: ali se le-ti točno zaradi takšne »osamitve« in ideološkega utemeljevanja virtualnih praks delovanja zavedajo vprašanja varnosti. Še pomembnejše je morda vprašanje, v kolikšni meri zaupajo programju, ki ga imajo naloženega na svojih računalnikih, in ki bi jim varnost pravzaprav moral zagotoviti. Odgovore na ti vprašanji moramo iskati v nakazanem ideološkem razmerju med imaginarnimi predstavami, ki jih glede varnosti uporabniki in uporabnice interneta imajo in njihovimi realnimi eksistenčnimi razmerami (varnosti), v katerih do interneta dostopajo (in naprej do vsebin ter storitev v kiberprostoru). Ponujene rešitve namreč temeljijo točno na **nemoči** osamljenega domačega uporabnika oz. uporabnice (ibid.):

> Slabo pa je, da uporabniki enostavno ne znajo vzpostaviti sistema varovanja. Zato smo v dvomih – najbolje je varovati podatke v uporabniških sistemih, vendar uporabniki takih sistemov ne znajo upravljati in vzdrževati. Ali jim lahko kako pomagamo? Pogosto lahko.

> Družba 3com denimo, ena večjih izdelovalk omrežne opreme za potrošnike in omrežnih kartic za računalnike, je že začela v svoje izdelke vgrajevati varnostne protokole, ki omogočajo vzdrževanje na daljavo, obenem pa zagotavljajo varovanje podatkov pri uporabnikih. Tem ni treba vedeti ničesar. A to je uporabno zgolj v podjetjih in velikih organizacijah – domačim uporabnikom takšne rešitve še ne zagotavljajo varnosti.

Le kako je potem mogoče, da dobri poznavalci varnosti, recimo jim *hekerji*, ki so kot potencialni ustvarjalci nevarnosti prvi na listi osumljenih, izhajajo večinoma prav iz vrst **domačih** uporabnikov in uporabnic? Ker kljub veliki zapletenosti varnostnih programskih sistemov sami iščejo in tudi najdejo 'varnostne luknje', za katere industrija varnosti računalniške programske opreme še ne ve ali jih ne zna pravočasno sama popraviti. Ker ravno oni presegajo to iluzijo varnosti, kot edino alternativo njihovemu početju pa upravljalci ponudijo le takojšnjo kriminalizacijo njihovega početja.[7] Citirani računalniški strokovnjak 'puščanje lukenj' varnostnih sistemov sicer vidi kot glavni vzrok, »da ne gre za pravo varnost, ampak zgolj za iluzijo o njej«, vendar kot rešitev ponudi klasični obrazec **pastorale**: sledite rešitvam družb, standardom mednarodnih organizacij, odločitvam vlad ipd.; torej sledite *Gospodarju*, *Drugemu*, *Microsoftu*, moderni upravljalski oblasti, tj. modernim pedagogizirajočim pastirjem, ki z vodenjem, usmerjanjem in upravljanjem ravnanja poskrbijo hkrati za čredo in vsako ovčico posebej. Domači potrošniki prav zato živijo v (navadno) preveč optimistični predstavi, npr. o odgovornosti, ki da jo do njih proizvajalci/prodajalci imajo, in zato površno sledijo rešitvam, 'varnostnim zaplatam', ki jih *softwarska* in *hardwarska* industrija neprestano dodaja svojim (slabim) izdelkom ali pa jih sploh ne znajo izkoristiti. Na koncu jih vse skupaj prisili k temu, »da kupijo res varne izdelke« (ibid.) – že videna strategija dane ekonomske racionalnosti v enem od pristopov programske industrije, kjer je namen zastonj (*free*) verzij

[7] Eden najslavnejših, skoraj že mitološki arhetip hekerjev preteklega desetletja, je verjetno Kevin Mitnick. FBI ga je po večletnem preganjanju leta 1995 zaprla zaradi kraje programske opreme različnim računalniškim podjetjem in južnokarolinški univerzi. Januarja 2000 so Mitnicka pogojno izpustili, od takrat pa se preživlja s svojimi veščinami tako, da piše in svetuje na temo računalniške varnosti. O tem dogodku je Hollywood posnel tudi »presenetljivo objektiven film« (*Delo*, 12.9.2002: 10). Mitnick je napisal tudi knjigo, kjer z izmišljenimi primeri - zaradi omejitev pogojne izpustitve in sodne odločbe, ki mu prepoveduje finančno okoriščanje s pripovedmi o svojih zločinih - opisuje zvijače za prelisičenje omrežnih vzdrževalcev, da hekerjem razkrijejo gesla, enkripcijske ključe in druge varnostne podrobnosti. Pri nas je bil leta 2003 podobno aktualen primer računalniškega samouka Roberta Škulja iz Kranja, ki je odkril, da računalniški sistem *Klik* Ljubljanske banke ne deluje dobro in da ga sami ne znajo (ali nočejo?) popraviti. Z banko se je menda nekaj mesecev pogajal, da bi jim prodal svoj »protisistem«, banka pa ga je naposled zaradi izsiljevanja ovadila. Škulja so nemudoma aretirali ter mu pobrali računalniške programe. Resnico je poznal resda najbolj pokojni Škulj sam, a je primer dovolj poučen in zgovoren.

programskih aplikacij ta, da frustrirajo in spodbodejo uporabnike in uporabnice, da nazadnje kupijo »boljše« verzije. Poleg tega se lahko še kritično zamislimo o učinkovitosti nedomišljene, apriorne in samoumevne umestitve »novega« računalniškega, digitalnega organizacijskega stila informacijskih in distribucijskih sistemov v »stare« organizacijske strukture, ki se izvaja s prilagajanjem delovnih postopkov kupljenim programskim rešitvam (in ne ravno obratno). Klasično teoretsko je tradicionalne organizacijske strukture opredelil že Max Weber s konceptom racionalnih »idealnih tipov« rigidne, piramidne birokratske organizacije (za splošen prikaz, polemiko z Webrom in zaton birokracije glej npr. Haralambos, Holborn, 1999: 279-296). Ker pa smo zgoraj z možnostjo eliminacije tradicionalnih hierarhij znotraj sodobnih organizacijskih struktur pokazali, da potrebujemo dobro teorijo »nove« družbene organizacije, bi lahko bilo primerno izhodišče nemara prav Deleuzov in Guattrarijev koncept rizoma (2000), umeščen v horizontalno komunikacijsko in varnostno samo-organizacijsko strukturo. Razmerje med področjem (birokratske) državne uprave, deloma tudi upravami svetovnih korporacij in multinacionalk na eni strani ter na drugi strani samim sebi ali kvečjemu rešitvam drugih prepuščenimi internetnimi galjoti - večina domačih uporabnikov in uporabnic, tako ali drugače (ne)soočenih z vprašanjem varnosti -, predstavlja še zelo odprto vprašanje varnosti, ki ga skušamo podrobneje misliti in konceptualizirati v nadaljevanju. Frank Furedi (1997: 68) k temu problemu pristopa z eno od značilnosti sodobnih družb, ko v eni od glavnih tez v knjigi *Culture of Fear* ugotavlja,

> da kadar v drže in načine vedenja ne moremo biti več prepričani, so izkušnje, ki so bile doslej relativno samoumevne, postale poslej pojmovane kot tvegane.

V družini, na delovnem mestu, doma, na potovanju, na javnih mestih združevanja, celo pri rokovanju in v ljubezni. Za subjekta je torej pomembno, kako zaznava »razmere« (varnosti), v katerih se znajde, ne pa kakšne realno so. Od tega je odvisno, kako se na razmere odziva, kakšna so njegova samozaščitna dejanja (če so), kaj si o povzročiteljih razmer misli, kakšno stališče do njih zavzame (do hekerjev, teroristov, muslimanov, tujcev, brezdomcev, »norih krav«, »pedrov«, »čefurjev« ipd.). Moralo nizkih pričakovanj najbolj nazorno prikaže tale stavek: »Ko danes ljudje rečejo heker, s tem mislijo terorist« (RGS, 2002: spletni dokument). Zato smemo zaključiti, da ima teorija ideologije (Althusser, 2000: 84 in naprej) tudi v rizomatičnem kontekstu

materialnih tokov IT ideološke učinke, še zlasti pa v tehnološko posredovanem kiberprostoru, kjer zmeraj že obstaja možnost (»ideologija nima zgodovine«), da ideologija uspešno »interpelira individuume v subjekte« medijsko posredovane in digitalno konstruirane družbene realnosti. Natančneje: v subjekte *Kalifornijske ideologije*, v kateri si individui predstavljajo svoje realne eksistenčne razmere zgolj v imaginarni formi tehnološke osvoboditve, posvečenosti in bogastva (Barbrook, Cameron, 2001: spletni dokument).

SODOBNO DRUŽBENO PROTISLOVJE: DOMINANTNA RABA TEHNOLOGIJE KOT GENERATOR DRUŽBENIH RAZLIK IN NEENAKOSTI, NE PA NAROBE

Neizogibna posledica razmerij družbene neenakosti in izključenosti je povečanje kvantitativnega in kvalitativnega razlikovanja med ljudmi, v našem primeru med ljudmi, ki si lahko privoščijo tehnologije in tistimi, ki si tega ne morejo. Neenakosti in razlike med razvitimi in nerazvitimi državami, ki izhajajo iz prisotnosti novih tehnologij kot kazalcem stopnje razvoja informacijske družbe, so strokovnjaki po celem svetu poenostavljeno označili za »digitalni prepad« (*digital divide*). Razmišljajo, kako bi ga premagali, pri tem pa spregledajo, da prepad ne bo odpravljen samo s kvantitativnim povečanjem in uvajanjem »bolj dostopne« IKT v družbo (javno npr. z *internet cafe-ji*, privatno z omogočanjem brezplačne rabe IKT najrevnejšim družbenim slojem, kot to počnejo ponekod v Veliki Britaniji), uvajanjem izobraževalnih programov (osnovne pismenosti) ter do državljanov »prijaznih« *e*-storitev ipd. Za uporabnika in uporabnico je smiselno delo z IKT (tj. tisto s pozitivnimi rezultati) kompleksna zmes socialnih, kulturnih, psiholoških, ekonomskih, političnih in predvsem osebnih, pragmatičnih razlogov. Če jih ljudje, zlasti teh zadnjih, nimajo ali jih v internetu ne najdejo, ga pač prostovoljno ne uporabljajo. Zato bo/je premostitev prepada dolgotrajen, če ne celo nemogoč proces nezavedne absorbcije tehnokulture in zavestnega izkustvenega pridobivanja znanja ter iskanja ugodja s pomočjo IKT. Vendar: če vpeljevanje rabe IKT implicirajo izenačujočo vlogo v intervencijah za socialno vključenost in enakost, potem je tu na mestu vsaj še tole politično vprašanje glede uniformnosti: ali so prizadevanja za socialno vključenost kot obveza za omogočanje in čim širši dostop do interneta res demokratična in družbi nujno potrebna? »Zakaj pa bi morali 'vsi' uporabljati internet, računalnike, DVD, mobilno telefonijo, kabelsko televizijo ipd.?« je vzorec dikcije, v kateri se sprašujejo

neuporabniki IKT. To vprašanje ne izraža njihove eksplicitne nenaklonjenosti do tehnologije kot take, ampak so (razumljivo) prej nenaklonjeni publiciteti, ki jih obkroža. Če dodamo še »realne eksistenčne razmere« pretiranih stroškov za dostop do interneta (tudi pri »zastonj« dostopu), spontane policijske globalizacije in totalizacije, totalne kontrole in destrukcije privatnosti s pomočjo IKT (npr. nad elektronsko pošto zaposlenih), terorja varnosti, zlasti pa anti-demokratičnosti tehnopolitičnega sistema *e*-demokracije,[8] potem smemo takšne razmere opisati kot mikro-učinke aparatov varnosti, na katere se opira sodobna upravljalska oblast, ko nam v istem hipu zagotavlja varnost v obstoječi informacijsko-komunikacijski infrastrukturi. A le ni vse tako *orwellovsko* distopično: na podlagi družbenih gibanj lahko predvidevamo, da se v panoptikomu oblasti brez centra, v »oblasti brez oblasti«, katere podlaga so (teoretično) vsi strežniki, vključeni v medmrežje,[9] nahaja mnoštvo pragmatičnih interesov zainteresiranih družbenih skupin, organizacij in posameznikov, ki vidijo v internetu zlasti priložnost za ekspresijo lastne konkurenčnosti in lastnih interesov, pa čeprav se njih interesi medsebojno celo frontalno izključujejo - kar je le en paradoks globalne uniformnosti (s katerim pa ni pravzaprav nič narobe – nasprotno, zagotavlja pestrost in raznolikost). V takšnih družbenih razmerah je varnost kot dominanta postala hkrati blago in fetiš, ne pa vrednota pravičnosti, ki odpravlja neenakosti za vse različne ljudi enako. Kritično-razmišljujoči posamezniki in posameznice se tega zavedajo in skušajo samostojno delovati, znajo refleksivno uporabljati tehnologijo. Večji problem pa takšna praksa predstavlja tistim uporabnikom in uporabnicam, ki se zaradi izgubljenosti v »svobodni« izbiri[10] potrošniške družbe in nemoči v digitalnem tipu panoptičnega nadzora počutijo že tako ali drugače negotovi. V njim lastnim aktivnostim jim grozijo

[8] Javni vložek (*input*) v *e*-demokracijo je s strani zagovornikov tehnopolitičnega sistema zamišljen predvsem kot agora, javni forum različnih diskusij v kiberprostoru, ki pa so največkrat brez kakršnih koli posledic za formiranje politike v obstoječih tradicionalnih političnih institucijah. Torej je takšna politična komunikacija predvsem sama sebi namen, udeleženci in udeleženke v *e*-demokraciji pa so »pasivno aktivni« v razmerju do politike. Podobno bi bile tudi *e*-volitve reducirane na sam tehnični proces pred pravo politično substanco, volivec in volivka pa na pasivnega subjekta ideologije v politiki kot redefiniranem procesu tehničnih transakcij, kjer se ga oz. se jo z IKT zaslepi, preusmeri pozornost in odvrne od prave participativnosti v sodobni politiki, čeprav se zdi ravno obratno: demokracijo IKT med ljudi širi, jo dela bolj dostopno, odprto in povezujočo. Vendar bistveno vprašanje ostaja: povezujočo s čim (ali kom)? *Cf*. Starr (2002: spletni dokument), »Connecting to what?«.

[9] Teoretski model oblasti kot centralne urejevalne fantazme, ki prikriva večjo razvejano in prikrito koncentracijo sodobnih tehnoloških postopkov in strategij nadzorovanja, ki prevevajo celoto kiberprostora.

[10] V novih tipih kapitalizma prisilna izbira dejansko izgine in jo nadomesti njen goli videz, podoba To je povečalo produkcijo in obstoj nepredvidljivih potreb in zahtev, tj. pomenov, zavedanj in identitet, kar je samo še povečalo negotovost potrošnikov (glede možnosti svobodne izbire).

nevarnosti informacijskih varnostnih sistemov, saj jim predstavljajo travmatično-nesimbolizirano realno jedro. Pred »nevarnostmi« neprestano bežijo v »varni« zaklon tehno-simbolizirane realnosti in si v formuli *utajitve* realno zamišljajo situacijo nekako takole: »Saj vem, da obstajajo možnosti hekerskega vdora v moj računalnik, pa vendarle mislim, da se to meni ne more storiti« S tem pa so že, kot opozarja Furedi (2002: 85), degradirani na raven, kjer so vsi medčloveški odnosi potencialno toksični, zato potrebujejo skrbno upravljanje in nadzor ekspertov, svetovalcev, terapevtov in drugih.

SOCIOLOŠKE IMPLIKACIJE »KULTURE STRAHU« ZA NADALJNE PSIHOLOŠKE INTERVENCIJE

'Hekerska forma' je obči konstitutivni strukturni element »virtualnega razreda«, sloja »navadnih« uporabnikov in uporabnic IKT, a je prav hekerska skupnost z njim že v konfliktu, ker je njihov intelektualni izziv, pri nekaterih seveda tudi interes za pragmatično okoriščanje na način, ki je v iskanju ugodja nasproten instrumentalnim ciljem birokracije, prevelik, ker v svojem početju resnično uživajo in se zabavajo ali pa se okoriščajo bolj kot drugi. Hekerje nikakor ne romantiziramo kot osamljene kontrakulturne heroje, saj to že počne *kiberpunk* literatura. S hekersko formo zgolj mislimo načine, s katerimi se organizirajo »ritualne« prakse komuniciranja in delovanja s pomočjo povezovanja z računalniki in računalniškimi mrežami. Spremljajoči medijski diskurz moralne panike in strokovni diskurzi, ki so odgovorni za promocijo IKT pa so nereprezentativni promotorji! Zakaj? Resnični računalniški/internetni navdušenci kot »pravi« uporabniki in uporabnice so tisti, ki znajo napraviti kaj sami. Njih je sorazmerno malo, saj se programska in računalniška industrija proti njim pravno-formalno »bojujeta«, ker s »krekanjem« programa ali predelavo *Xboxa* pastorali seveda ne sledijo, vendar vsaj vedo, kako programska ali strojna oprema deluje in znajo zraven še izkoristiti »skrite« potenciale tehnične opreme, ki obdelana ali predelana celo bolje deluje![11] S tem, kar počno, z **iz-rabo IKT** oni postavljajo standarde varnost, ne pa nevarnost(i) - je naša poglavitna, osrednja teza. Biti predan računalnikom, imeti zmožnosti in sposobnosti za rabo

[11] Na alternativne načine rabe in prakse izkoriščanja tehnične opreme smo samo pokazali, ne pa tudi raziskali, kako do takšnih praks pride. Na tem mestu dajemo poudarek konceptualizaciji socialne percepcije varnosti IKT.

tehnologije, biti entuziast, čeprav v očeh okolice »čudak«, torej biti »*geek*« še ni nič narobe (razen tega, da med uporabniki tako moški kot ženski delež med *geeki* preživita preveč časa ob računalnikih, na ta način pa zanemarjata druge socialne aktivnosti). To potrjuje v računalništvo sprejeta javna označevalna praksa/lingvistična raba tega izraza, ki kaže na večjo družbeno odobritev početja in toleranco *geek-ov* kot pri rabi izraza »heker«, kaj šele »kreker«, katerih početje se ne tolerira ter se celo kriminalizira. Jedro problema se ustvari, ker heker v splošnem vključuje jasno razmejene in bolj močne, čvrste kompetence glede izrabe IKT, ki jih *geek* takšnih nima! *Geek* preprosto sledi dominantni rabi, ki jo sicer zelo dobro obvlada, heker pa poleg tega razvija še nove, alternativne rabe, ki so večkrat izven dominantnih okvirov.[12] Odrejanje simbolne, družbeno-kulturno pogojene meje med sprejemljivim in nesprejemljivim, ki se časovno-prostorsko spreminja glede na interese dominantne družbene skupine oz. elite virtualnega novega razreda, je tudi eden od vzrokov, da v današnji kulturi prevladuje perspektiva varnostnih razmer kot historični cikel razmerja med preteklostjo in prihodnostjo, v katerem smo vseskozi že bili, smo in bomo nenehno v nevarnosti, kjer so ljudje »[…] spodbujani, da se vidijo raje kot žrtve […] kot pa samo-determinirajoči dejavniki«. Živimo v kulturi, kjer človeška bitja niso samo žrtve škode iz preteklosti, ampak jim je tudi usojeno, da poškodujejo bodoče generacije (Furedi, 1997: 89). Poleg tega je tudi njim samim škoda v prihodnosti že usojena, všteta, anticipirana, če ne bodo uporabljali uradne pomoči edino kompetentnih svetovalcev (*cf*. podpoglavje »Nesposobni ljudje«, ibid.: 91-95). V »kulturi zlorabe« se vse prehitro spregleduje ključni pogoj, namreč, da si ranljivost zaradi lastne nevednosti ljudje povzročijo sami, oz. jim jo, namerno, zaradi njihove nevednosti in nesposobnosti spoprijeti se s problemi, povzročijo drugi prav zato, ker (to) vedo. V procesu viktimizacije se je pač lažje že v naprej videti kot žrtev, zlati v primeru, ko »bo patologija zlorabe verjetno imela učinek postati samo-uresničujoča prerokba« (90).

[12] Hekerje se v medijskih konstruktih realnosti, željnih spektaklov, ki se radi prodajajo, velikokrat predstavlja izrazito stereotipno: od hitre hrane predebele, mozoljave, zanemarjene mladeniče (ne pa mladenke!) ter kot statusno frustrirane študente tehničnih usmeritev, ki s svojim funkcionalnim znanjem in spretnostmi deviantno reflektirajo svoj družbeni položaj: nedokončan izobraževalni proces ipd. Zato želijo na tak način svetu in sebi dokazati, da so »pravi« strokovnjaki. S takšnimi podobami in oznakami pa se v javnosti ne daje možnosti prodora novejših ugotovitvev sociologije, ki v informacijski družbi zaznava premik od statusa k funkciji in k individualnim življenjskim projektom.

ZAKLJUČEK: SOCIO-KULTURNI PRISTOP K RABAM IKT KOT INTERDISCIPLINARNI OKVIR PSIHOLOGIJE NOVIH TEHNOLOGIJ

Naj na tej točki našo intervencijo zaustavimo, ne pa tudi končamo, ker smo s prikazano analizo vseskozi odpirali sledi k interdisciplinarnemu pristopu, ko problematiko varnosti v informacijsko-komunikacijskih mrežah obravnavamo v perspektivi **rabe** IKT. Želeli smo pokazati, da struktura globalnega sistema kapitalistične *high-tech* produkcije določa družbeno strukturo na način, ki povzroči temeljni razcep varnost/ne-varnost na individualni, uporabniški ravni. Tu se uporabnik in uporabnica prepoznavata kot žrtvi, kar bistveno naddoloči njuno osebnost. Iz tega sledi napotilo, da mora tudi znanost proučevanja človekove osebnosti vedno upoštevati socio-kulturne razmere in ideološke značilnosti, vpisane v tehnologijo, ki določajo načine rab IKT.

BIBLIOGRAFIJA

Althusser, Louis (2000), »Ideologija in ideološki aparati države«, v: Izbrani spisi, Ljubljana: Založba /**cf.*, str. 53-110.

Barbrook, Richard, Cameron, Andy (2001), »Californian Ideology: critique of West Coast cyber-libertarianism« <http://www.hrc.wmin.ac.uk/hrc/theory/californianIdeo/index/t.4.2> [še dostopno 25.4.2002].

Barbrook, Richard (2002), »GIVING IS RECEIVING«, *nettime mailing list* 10.10.2002 <http://amsterdam.nettime.org/Lists-Archives/nettime-l-0210/msg00033.html> [še dostopno 14.10.2002].

Deleuze, Gileles, Guattari, Felix (2000), Micelij, Koper: Hyperion.

Dyer-Witherford, Nick (1999), Cyber-Marx : cycles and circuits of struggle in high-technology capitalism, Urbana in Chicago: University of Illinois press.

Foucault, Michel (1991), »Governmentality«, v: Burchell, Graham, Collin Gordon in Peter Miller (ur.), The Foucault Effect, Harvester Wheatsheaf: Hertfordshire, str. 87-104.

Furedi, Frank (1997), Culture of Fear, Risk-talkin and the Morality of Low Expectation, London in Washington: CASSELL.

Haralambos, Michael, Holborn, Martin (1999), Sociologija : teme in pogledi, Ljubljana: DZS.

»Kevin Mitnick napisal knjigo«, nadnaslov »*Računalniška varnost*«, Delo, 12.9.2002, str. 10.

Lanier, Jaron (2000), »One-Half of a Manifesto. Why stupid software will save the future from neo-Darwinian machines«, *Wired* 8.12.2000, <http://wired.com/wired/archive/8.12/lanier.html> [še dostopno 8.5.2001].

Microsoft Info (2002), Glasilo podjetja Microsoft, letnik 8, številka 2 / december, Ljubljana: Microsoft d.o.o.

RGS (2002), »How We Made Our Own 'Carnivore'«, *nettime mailing list* 17.6.2002 <http://amsterdam.nettime.org/Lists-Archives/nettime-l-0206/msg00088.html> [še dostopno 21.6.2002].

Simmel, Georg (2000), Izbrani spisi o kulturi, Ljubljana: Studia Humanitatis.

Starr, Sandy (2002), »Connecting to what?«, *spiked* 15.1.2002 <http://www.spiked-online.com/Articles/00000002D3AE.htm> [še dostopno 16.7.2002].

»Varnost je zgolj iluzija«, nadnaslov »Intervju: dr. Steven Kent, Internet engineering task force«, *Delo* 29.9.2002, na spletnih straneh intervju na naslovu <http://dpp.delo.si/Apps/WebObjects/DeloGPortal.woa/41/wo/5m7z21OpkzIm3XoxOHASxx1TnkX/0.6.0.1.4.1.3.6.1> [še dostopno 19.10.2002].