INŠTITUT ZA KRIMINOLOGIJO
*pri Pravni fakulteti v Ljubljani*

*Urednik*: doc. dr. Aleš Završnik

*Avtorji*: dr. Matej Kovačič
mag. David Modic
Marko Rusjan
dr. Liljana Selinšek
spec. Janko Šavnik
doc. dr. Aleš Završnik

*Naslov*: Kriminaliteta in tehnologija: Kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon?

*Izdal in založil*: Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani
*Za izdajatelja*: prof. dr. Matjaž Jager

*Recenzenta*: prof. dr. Katja Filipčič
prof. dr. Katja Šugman Stubbs

*Tisk*: Oblikovanje Pika Škraba s.p.
*Naklada*: 200 izvodov

Prvi natis
Ljubljana, 2010

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

343.9:004.056(082)

KRIMINALITETA in tehnologija : kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon? / [avtorji Matej Kovačič ... et al.] ; Aleš Završnik, urednik. - 1. natis. - Ljubljana : Inštitut za kriminologijo pri Pravni fakulteti, 2010

ISBN 978-961-6503-16-7
1. Kovačič, Matej, 1974- 2. Završnik, Aleš
252127744

**INŠTITUT ZA KRIMINOLOGIJO**
**pri Pravni fakulteti v Ljubljani**

# KRIMINALITETA IN TEHNOLOGIJA

## Kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon?

**ALEŠ ZAVRŠNIK**
**Urednik**

**Ljubljana 2010**

# Kazalo

# Spremna beseda: Življenje kot tehnološki in nadzorstveni višek

Pozor! Knjiga, ki nemo ždi pred vami, si nedvomno zasluži, da jo vzamete v roke (če je seveda že niste) in jo preberete. Razlogov, ki utemeljujejo njeno privlačnost, vsekakor ne manjka. To, kar najbrž najprej pritegne pogled (in, domnevam, tudi vaše zanimanje), je predvsem nesporna aktualnost in večplastna kontroverznost obravnavanih tematskih sklopov, ki jih je mogoče, čeravno le zelo v grobem, zgostiti v vprašanje, kako najnovejša tehnološka »čudesa« (namreč raznovrstni – zakonski in nezakonski – otroci informacijske in komunikacijske »revolucije«) spreminjajo delovanje neformalnega in formalnega družbenega nadzorstva ter življenjske prakse (in »teorije«) njegovih človeških/podružbljenih objektov ali subjektov (in sicer bodisi normalnih bodisi odklonskih ali celo kriminalnih). Bolj ali manj dramatične, predvsem pa nenehno in z osupljivo naglico porajajoče se novosti, ki jih v kompleksni sferi (pro)aktivnih in reaktivnih kontrolnih mehanizmov generira vročičen znanstveni in tehnološki razvoj – in ki tako ali drugače (pri)zadevajo domala vse člane (post)modernih kapitalističnih formacij –, so gotovo dovolj očitne (in zatorej tudi splošno zaznane), neprimerno bolj problematičen pa je njihov značaj (oziroma vrednostni predznak in, ne nazadnje, »smiselnost«). No, in prav v tem pogledu je delo »Kriminologija in tehnologija« še posebej dragoceno, saj pogumno orje teoretsko ledino (vsaj v tukajšnjem družboslovnem/kriminološkem prostoru) in ponuja kopico pretanjenih terminoloških in konceptualnih orodij, s pomočjo katerih se je gotovo lažje orientirati v kaotičnem in (omni)kriznem postmodernem svetu.

»Tehnično omogočeno in okrepljeno nadzorovanje« – ta (resda nekoliko okorna) sintagma je bržkone še najbolj ustrezen prevod angleške besede *surveillance* – je dandanes vse bolj »organsko« vpeto v vsakdanje življenjske rutine (npr. v sferi dela, potrošniških aktivnosti, izobraževanja in transporta). Vsakovrstna tehnična krama, ki se kopiči v mogočnih orožarnah javnih in zasebnih nadzorovalcev (večjih ali manjših »orwellovskih bratov«), je največkrat v službi preventivnega (na prvi pogled amoralnega, apolitičnega, instrumentalno racionalnega ali pragmatičnega) situacijskega »inženiringa« oziroma sistemske integracije ali koordinacije (tj. zagotavljanja tekočega, čim manj tveganega ali motenega funkcioniranja institucij, procesov in aranžmajev). Toda pozor. Ko steče beseda o vlogi »visoke« (in konec koncev tudi »nižje«) tehnologije pri zagotavljanju varnosti, se pogosto najprej pomisli na pospešeno vključevanje tehničnih naprav v permanentno vojno zoper terorizem in kriminaliteto. Ob tem pa vseeno ne bi smeli prezreti nemara še dosti pomembnejše vojne, namreč tiste – praviloma skrbno in sistematično zanikane ali utajene (oziroma ideološko/kulturno »normalizirane«), na katero se lepi pridevnik »razredna«. Tu seveda ne gre zgolj za tehnični nadzor na »delovnem mestu« (ta »kategorija« postaja sicer časovno in prostorsko čedalje bolj nedoločljiva, še zlasti na področju »nematerialnega« dela). Upoštevati je namreč treba, da se je ravno po zaslugi osupljivega znanstvenega in tehnološkega razvoja izrazito povečala kolektivna moč kapitala v razmerju do prodajalcev »delovne sile« (na globalni in lokalni ravni). Uvajanje tehnologije – podkleteno z reorganizacijo (»racionalizacijo«) delovnih procesov in prestrukturiranjem podjetij – je povzročilo izredno povečanje produktivnosti (gospodarstvo lahko izdela veliko več blaga z dosti manj človeškega dela). *In abstracto* je to gotovo razveseljiv, celo hvale vreden dosežek, saj »načeloma« omogoča krajšanje delovnega časa,

izboljšanje delovnih razmer ter povečanje individualne in kolektivne blaginje (pravzaprav že kar strukturno rešitev »ekonomskega problema« v klasičnem ali tradicionalnem pomenu tega pojma). Vendar pa se to – presenečenje? – ni zgodilo. Poveč(ev)anje produktivnosti je dejansko blagoslov predvsem za relativno tanko (in strukturno privilegirano) manjšino, npr. v obliki povečanih dividend (za delničarje), groteskno nabreklih dohodkov (za vodilne uslužbence, menedžerje in druge predstavnike novodobne delavske elite, tj. strokovnjake v »sektorju znanja«) ter razširjenih možnosti za izsiljevanje, zastraševanje, izkoriščanje, manipuliranje, nadzorovanje in poniževanje bolj ali manj običajnih prodajalcev delovne sile (ki medsebojno tekmujejo za »dobrino vseh dobrin«, plačano zaposlitev). Po drugi – neprimerno temačnejši – strani pa se povečanje produktivnosti (po zaslugi avtomatizacije, informatizacije in racionalizacije) kaže kot vrtoglava strukturna brezposelnost, povečevanje »presežne« populacije (ki je barbarski kapitalistični stroj ne potrebuje več niti v vlogi Marxove razvpite »rezervne armade«), družbenoekonomska negotovost (in z njo spete slutnje o posameznikovi lahki, tako rekoč hipni zamenljivosti/nadomestljivosti ali celo odvečnosti in sramotnem padcu na dno statusne piramide), »prekarnost« (ne le značilno postfordističnih) delovnih razmerij, stopnjevane zahteve po fleksibilnosti, lojalnosti, mobilnosti, učinkovitosti, konkurenčnosti in »vseživljenjskem izobraževanju« delovne sile (»liberalnih sužnjev«), intenzivna in ekstenzivna ekspanzija delovnih obremenitev, krčenje delavskih pravic (in navsezadnje tudi mezde), politična nemoč (ali celo obupanost) …

Vidimo torej, da je tehnologija – najbolj milo rečeno – neke vrste mešani blagoslov, pojav z nič koliko obrazov. Po eni strani zbuja vtis, da »je čedalje več mogoče« (ali da bo, *in extremis*, nemara že prav kmalu skoraj »vse mogoče«), po drugi strani pa je precej težko prezreti dejstvo, da je tudi »vse več nemožnega«. Tehnologija povečuje družbeno in človeško moč in silo, obenem pa tudi odvisnost, nebogljenost in vsakovrstne utvare (ter nenazadnje otipljivo ekološko škodo). Danes je redkeje kot nekoč slišati optimistične (utopične?) napovedi, da bosta znanost in tehnika prej ali slej odrešili človeštvo (oziroma vsaj osvobodili ljudi od heteronomnega, nujnega, telesno in duševno utrudljivega in celo škodljivega ali »zgolj« nevšečnega, dolgočasnega, duhomornega in zoprnega dela). Vseeno pa se na tehnologijo še vedno obešajo precejšnja pričakovanja ali vsaj pretežno pozitivne vrednostne konotacije (z drugimi besedami: skepse, kritike, posmehovanje, zadržanost ali zavračanje tehničnih čudes so pogosto dojeti kot znamenje posameznikove mentalne omejenosti, civilizacijske zaostalosti, topoumne konservativnosti, mračnega nazadnjaštva, sovražnosti do napredka, zatohle provincialnosti, tipično postmoderne »nepismenosti« ali »neizobraženosti«, obžalovanja vredne nekompetentnosti, otežene zaposljivosti ali pač zgolj bizarne ekstravagance in bahaškega snobizma). Kakor koli že, zgodovinske in aktualne izkušnje vendarle kažejo, da tehnologija (navzlic kopici njenih nesporno pozitivnih reperkusij) ni – in pravzaprav niti ne more samodejno biti – »panaceja« za osrednje družbene (in za tudi individualne ali eksistencialne) probleme (ti so – če to hočemo ali ne – po svoji naravi predvsem kulturni/ideološki, politični/pravni in etični). Še huje, zdi se, da so ljudje s pomočjo tehnologije doslej uspeli storiti bržkone celo več slabega kakor dobrega. Oziroma: znanstveni/tehnološki razvoj (ki ga zaenkrat usmerjajo predvsem interesi kapitala oziroma »odtujenih« središč politične in ekonomske moči) po vsej verjetnosti ne moreta ustvariti niti boljšega sveta, niti boljše družbe, niti boljših ljudi (kaj šele »nadljudi«!),

gotovo pa lahko zelo pomembno prispeva h *good way of life*, kakršnega prikazuje in oglašuje kapitalistična propaganda, in to vsekakor zelo prepričljivo in tudi uspešno (»kvazi luksuzna tehnika narodu, bogastvo, moč, prestiž in oblast bogatašem!«).

Za konec le še to: iskrene čestitke uredniku in tudi avtorju dveh izjemno zanimivih in tehtnih prispevkov, tj. Alešu Završniku, čigar zavidljive znanstvenoraziskovalne in teoretske zmožnosti/sposobnosti so se sicer tukajšnji bralski javnosti razodele že v delu »Homo criminalis: upodobitve zločinskega subjekta v visokotehnološki družbi tveganja«. In seveda: prav take čestitke in pohvale tudi vsem drugim avtorjem, ki so s svojimi poglobljenimi analizami pojavov, kot so hekerstvo, nigerijska prevarantska pisma, digitalni dokazi v kazenskem postopku in forenzika mobilnih telefonov, soustvarili knjigo, katere spremne besede je tu konec.

V Ljubljani, 20. avgusta 2010. Prof. dr. Zoran Kanduč

# O avtorjih

**Matej Kovačič**, doktor znanosti, strokovni sodelavec v Centru za raziskovanje javnega mnenja in množičnih komunikacij na Fakulteti za družbene vede Univerze v Ljubljani in asistent za področje družboslovne informatike in metodologije. V okviru raziskovalnega dela se ukvarja tudi z vprašanji zasebnosti in nadzora v virtualnem prostoru ter kiberkriminala, rezultat tega pa sta knjigi Zasebnost na internetu (2003) in Nadzor in zasebnost v informacijski družbi (2006) ter poglavje z naslovom Zasebnost in hramba prometnih podatkov v mobilni telefoniji v monografski publikaciji Mobilne refleksije (2007).

**David Modic**, univerzitetni diplomirani socialni pedagog, magister znanosti, je doktorski študent Univerze v Exetru, kjer je tudi zaposlen. Vrsto let že raziskuje virtualne skupnosti, procese odločanja v virtualnem svetu, viktimizacijo, samoprijavo in virtualno patologijo. Poleg naštetega je David Modic tudi certificiran psihoterapevtski svetovalec transakcijske analize in član angleške HEA (*Higher Education Authority*). Večino svoje raziskovalne dejavnosti opravlja v Veliki Britaniji.

**Marko Rusjan**, univerzitetni diplomirani pravnik, podiplomski študent na Pravni fakulteti Univerze v Ljubljani. Področja njegovega zanimanja in raziskovanja so kibernetska kriminaliteta, igre na srečo, teoretska kriminologija, strah pred kriminaliteto in politična filozofija.

**Liljana Selinšek** je doktorica pravnih znanosti, od 1.6.2010 zaposlena kot svetovalka v uradu informacijskega pooblaščenca, pred tem pa je poučevala kazensko pravo na Pravni fakulteti Univerze v Mariboru. Njena ožja pravna specializacija je področje kazenskega prava (materialni in procesni del), ukvarja pa se tudi s pravom o prekrških. Ta področja v zadnjem času povezuje z vprašanji varstva osebnih podatkov in dostopa do informacij javnega značaja, vseskozi pa se pri svojem delu trudi v pravni kontekst čimbolj konstruktivno vplesti razvoj informacijske tehnologije.

**Janko Šavnik**, spec., *Certified Computer Examiner* (CCE), sodni izvedenec za informacijsko varnost in računalniško forenziko, zaposlen kot upravitelj varovanja informacij v Hypo Alpe-Adria-Bank d.d., sicer pa član strokovnega sveta Inštituta za forenziko informacijskih tehnologij (IFIT).

**Aleš Završnik** je doktor pravnih znanosti, docent za kriminologijo na Pravni fakulteti Univerze v Ljubljani in znanstveni sodelavec na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani. Je član upravnega odbora COST *Action* IS0807 *Living in Surveillance Societies* in projekta COST *Action* IS0801 *Cyberbullying.* Ukvarja se s preučevanjem učinkov informacijske tehnologije na kriminaliteto in nadzorovanje, v letu 2009 je izdal knjigo *Homo criminalis: upodobitve zločinskega subjekta v visokotehnološki družbi tveganja* in vodil programski in organizacijski odbor konference *Kibernetska kriminaliteta in digitalna forenzika*.

# Zahvala urednika

Knjiga prikazuje del nove raziskovalne poti Inštituta za kriminologijo pri Pravni fakulteti v Ljubljani, ki se nanaša na proučevanje vplivov novih tehnologij na kriminaliteto in odklonskost ter družbeno odzivanje na kriminalne in druge odklonske pojave v svetu, znanem kot raziskovalno polje *Kriminaliteta in tehnologija*. Ta združuje znanja s področja kazenskega (materialnega in procesnega) prava, kriminologije, prava človekovih pravic, prava policijskih pooblastil, prava telekomunikacij, varnostnih študij in digitalne forenzike.

Knjiga je kulminacija daljšega sodelovanja avtorjev, ki s(m)o v preteklosti sodelovali pri več raziskovalnih projektih s področja kazenskega prava in kibernetske kriminalitete na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani. O kriminaliteti in tehnologiji smo tudi javno razpravljali na konferenci *Kibernetska kriminaliteta in digitalna forenzika*, ki je potekala 4. junija 2009 na Pravni fakulteti v Ljubljani, in se je nanašala na specifičen segment raziskovalnega področja *kriminaliteta in tehnologija*: na *kibernetsko kriminaliteto* kot novo obliko kriminalitete v informacijski dobi in *digitalno forenziko*, disciplino, ki se ukvarja z odkrivanjem in analizo digitalnih sledov v elektronskih napravah. Konferenco sta organizirala Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani kot nosilna inštitucija in Inštitut za forenziko informacijskih tehnologij, združila pa je petnajst najvidnejših slovenskih predavateljev in gostov iz Velike Britanije in Madžarske. Knjiga je zato rezultat odličnega sodelovanja avtorjev pri skupnih raziskovalnih projektih raznovrstnih oblik, saj je le tako mogoče zagotoviti konsistentno in koherentno obravnavo multidisciplinarnih raziskovalnih izzivov.

Hvaležno zahvalo ob izdaji knjige izrekam Agenciji za raziskovalno dejavnost RS, ki je podprla projekt *Nadzorovanje in kaznovanje v informacijski družbi: Kibernetska kriminaliteta in nadzorstveni učinki informacijske tehnologije*, št. J5-0269, ki teče od leta 2008 na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani pod vodstvom prof. dr. Renate Salecl. S tem Agencija ni samo zagotovila potrebna finančna sredstva za raziskovanje, temveč je omogočila sinergije med doslej ločenim »svetom prava« in »svetom tehnike« na občutljivem, dinamičnem področju nadzora in zasebnosti, ter novih vrst in oblik kriminalitete in odzivanja nanjo, kakor tudi razvoj posebnega raziskovalnega področja *kriminaliteta in tehnologija* v Republiki Sloveniji.

Zahvaljujem se tudi Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani, predvsem profesorici Renati Salecl za dopuščanje velike mere raziskovalne svobode, ki je edino lahko vodila k novi še neprehojeni raziskovalni poti, in direktorju, profesorju Matjažu Jagru, za razumevajoče finančno vodenje tudi tega projekta. Hvala recenzentom za njihovo dodatno delo in hvala profesorju Zoranu Kanduču za spremne misli, ter Marinki Milenkovič, Ivanki Sket in Mojci M. Plesničar, MSc., ki so pomagale uredniku pri jezikovnem urejanju delov besedila. Vsi ste pripomogli k sklepnim dejanjem pri pripravi knjige, za kar se vam iskreno zahvaljujem.

Največjo zahvalo dolgujem avtorjem prispevkov. V veselje mi je bilo sodelovati z vami. Hvala vam za upoštevanje pripomb in predvsem vašo potrpežljivost pri nemara res dolgem procesu znanstvenega objavljanja v RS. Z vami si želim produktivnega sodelovanja tudi v bodoče, saj, kot kaže, dilem na novem križišču *tehnologija in*

*kriminaliteta* v »tehnološki družbi«, ki si želi biti »družba znanja« in ki želi učinke vpliva tehnike na družbo tudi razumeti, ne bo kmalu zmanjkalo.

V Ljubljani, 24. avgusta 2010 Doc. dr. Aleš Završnik

# Kriminaliteta in tehnologija: uvod

**Aleš Završnik**

Namen knjige je proučiti, kako informacijska tehnologija (IT) in zanjo značilen postopek digitalizacije, tj. pretvorbe (reprezentacije) predmetov, oseb, prostorov in informacij v digitalne podatke, spreminja štiri med seboj antagonistično povezane pojave: nadzor in zasebnost (I. in II. del) ter izvrševanje kaznivih dejanj (III. del) in kazenskopravno reakcijo nanje (IV. del). V knjigi se izogibamo determinističnemu razumevanju tehnologije, ki bi bila razumljena kot sama po sebi »slaba« ali »dobra«. Ko je enkrat umeščena v delovanje kompleksnih družbenih fenomenov, kot so družbeno nadzorovanje in zasebnost, izvrševanje kaznivih dejanj in kazenskopravno reagiranje na kriminaliteto, je lahko »zdravilo« za zagate teh fenomenov, lahko pa povzroči še večje težave od tistih, ki jih s pomočjo IT poskušamo rešiti.

## IT kot Pandorina skrinjica in panaceja kazenskega pregona in zasebnosti

Informacijska tehnologija po eni strani omogoča učinkovita »zdravila« pri odkrivanju kaznivih dejanj in pregonu domnevnih storilcev: omogoča okrepljeno (preventivno) policijsko obveščevalno dejavnost (na primer s številnimi zbirkami podatkov in njihovo izmenjavo pri čezmejnem nadzoru, izmenjavo podatkov o potnikih, o finančnih transakcijah), omogoča odkrivanje (resničnih ali namišljenih, a zato nič manj družbeno mobilizacijskih) kriminalnih tveganj, zmanjšuje kriminalne priložnosti s tehničnim onemogočanjem (»arhitekturo«, Lessig),[1] na primer pri zaščiti pravic intelektualne lastnine s tehničnimi blokadami in ukrepi oziroma shemami za digitalno upravljanje avtorskih (in drugih) pravic (*Digital Rights Management*). Poleg krepitve kriminalitetnega prevencijskega delovanja olajšuje sodno procesiranje že odkritih domnevnih storilcev kaznivih dejanj: omogoča avtomatizacijo zamudnih rutinskih opravil pravosodne uprave z elektronskimi vpisniki, pospešuje organizacijsko-tehnična opravila v sodnih postopkih z elektronskimi spisi, s celovitim upravljanjem sodnih primerov z informacijskimi sodnimi upravljavskimi sistemi (*Court Case Management Systems*) ali s proizvodi umetne inteligence[2] ter omogoča uporabo vsenavzočnih digitalnih sledi v dokazne namene, čemur služi računalniška forenzika. IT omogoča bolj

[1] Lessig 1999.

[2] V Braziliji za manjše prekrške uvajajo shemo »Pravičnost na kolesih«, obliko elektronskega sojenja s programi umetne inteligence (po Graham-Rowe 2000). Strojno učenje, ki prepoznava obraze, posnema človeške zakonitosti prepoznavanja obrazov in je presenetljivo točno, ugotavljajo psihologi. Glej Kagian *et al.* 2008. O možnostih umetne inteligence v pravu glej v Koritnik, Grah Whatmough 2010.

učinkovito varstvo zasebnosti, na primer komunikacijske zasebnosti z (vedno bolj dostopnimi in brezplačnimi) sistemi za kriptiranje komunikacij.

IT je na drugi strani pogosto Pandorina skrinjica, ker omogoča zlorabe ali preprosto »v praksi« ne deluje tako, kot bi si njeni apologeti želeli. Priča smo obsežnim podatkovnim zbirkam osebnih podatkov, ki »puščajo« (na primer odtekanje informacij o zdravstvenih podatkih v VB). Intenzivno rudarjenje po podatkovnih zbirkah in kreiranje novih metapodatkov (o podatkih) in trgovanje z osebnimi podatki[3] so Pandorina skrinjica novih zlorab. Raziskovalci vedno bolj (so)glasno ugotavljajo, da sta obstoječa intenziteta profiliranja in internetnega nadzora nesorazmerni,[4] da videonadzorni sistemi javnega prostora ne odvračajo storilcev kaznivih dejanj[5] in da sicer tehnološko policijsko delovanje (»*technopolicing*«) ne deluje.[6] Invazivni kriminalitetni prevencijski ukrepi (na primer protiteroristično navdahnjeni regulatorni ukrepi, kot je obvezna hramba prometnih podatkov) povzročajo občutno kolateralno škodo, saj omogočajo sistematično, ubikvitarno in permanentno zbiranje podatkov o posamezniku in njihovo shranjevanje za morebitne bodoče (v trenutku zbiranja) še neznane namene. Kako razumeti te kontradiktorne ocene?

[3] Kanaley 1999.

[4] Brown in Korff analizirata, kako IT krepi policijsko delovanje. Tehnologije, ki omogočajo opazovanje posameznika, oblikovanje in analiziranje podatkovnih zbirk o prometnih podatkih, povezanih s telefonskimi klici in komunikacijami po elektronski pošti in oddaljeno preiskovanje računalnikov preko vohunskih programov, vodijo po njunem mnenju v nov »podatkovni nadzor« (angl. »*dataveillance*«). Navedene aktivnosti kršijo številne temeljne človekove pravice, temeljna načela pravne in demokratične države, onemogočajo (in ne pospešujejo) mednarodno pravno pomoč in sodelovanje ter sprožajo številne ustavnopravne izzive. Tehnološke možnosti, ki so na voljo policiji na področju nedoločnega »boja zoper terorizem«, vodijo do absurdnih razsežnosti rudarjenja po podatkovnih zbirkah, ki pogosto vodijo do »napačnih zadetkov«, tj. pozitivnih, a napačnih iskalnih rezultatov o osebah, ki nimajo nobene povezave s terorističnimi dejavnostmi, temveč zgolj ustrezajo v programe vgrajenim stereotipom. Po Brown, Korff 2009.

[5] Douglas Smith 2009; Hempel, Töpfer 2009; Leman-Langlois 2008b.

[6] Leman-Langlois 2008a.

## IT je politika z drugimi sredstvi

Uvodno zagato predstavlja že narava IT, tj. način, kako razumemo njeno povezanost z vrednotami. IT običajno ne presojamo na enak način kot družbene fenomene. »Zdravorazumsko« se nam IT zdi kot nekaj, kar je bliže naravnim kot družbenim zakonom, saj jo zaradi delovanja po fizikalnih zakonitostih dojemamo kot nekaj, kar bolj poznajo inženirji in tehniki kot pa družboslovci, ki so zgolj njeni »uporabniki«. Zato posameznih tehnologiji pri uvedbi v družbeno (upo)rabo ne vrednotimo samih po sebi, večinoma presojamo njene neposredne učinke (zlasti učinkovitost, računsko hitrost). Tehnična sofisticiranost posamičnih tehničnih proizvodov, ki sicer res delujejo po fizikalnih zakonih, pa ničesar ne pove o tem, kakšne učinke imajo ti proizvodi na družbene odnose, na razmerja moči v družbi, na pravičnost, enakost, porazdeljenost družbenega bogastva, varnost in odgovornost, potem ko so ti proizvodi enkrat umeščeni v družbene institucije in družbene procese, ter morda še pomembneje, kakšne vrednote posamični (tehnično-nadzorstveni) proizvodi utelešajo.

Tehnološki proizvodi so že pri svojem nastajanju in pred umestitvijo v družbeno okolje oblikovani na način, ki ni odvisen le od fizikalnih zakonitosti. Bistveno bolj, kot običajno domnevamo, so odvisni od družbe, njenih gospodarskih, političnih in kulturnih značilnosti. Že bolj preprosti predmeti »vsakodnevnega življenja« (kot je steklenica za vodo) so rezultat kulturne zaznave (v primeru steklenice za vodo tega, kaj pomeni »kulturno« shranjevanje vode), gospodarske učinkovitosti (da je steklenico v določeni družbi v določenem zgodovinskem trenutku sploh mogoče izdelati glede na cene produkcijskih dejavnikov) in družbene moči relevantnih subjektov (na primer ekonomske moči steklarn nasproti proizvajalkam polimerov). *A fortiori* to velja za bolj kompleksne tehnične proizvode, kot sta internet ali video nadzorovanje. Pri tem je dodatna spremenljivka, ki otežuje abstraktno oceno o (ne)primernosti vnosa tehničnih pomagal v družbeno prakso, raznolikost družbenih okolij, kamor so ti predmeti umeščeni.

Vsak tehnični proizvod je zato takšen (in ne drugačen) ne zgolj zaradi tehnološkega razvoja in tehnološke optimalnosti, temveč zato, ker je v določenih družbenih okoliščinah glede na gospodarske, kulturne, politične in druge značilnosti družbe obveljal za »pravega«. Tehnološko proizvedene oblike kriminalitete in tehnološko okrepljeni odzivi nanjo so zato gordijski vozel političnih in gospodarskih interesov, pravnih pravil in tehnološkega razvoja, so križišče interesov različnih akterjev, od policije, zasebne varnostne industrije in forenzičnih strokovnjakov, in odražajo masovne individualne želje, geopolitične strategije in druge oblike moči.[7]

Ni samo zločin družbeni proizvod, kot so v kriminologiji pokazale teorija etiketiranja, simbolični interakcionizem, mentalizem, dekonstruktivizem in kritična kriminologija, temveč so to tudi različni tehnološki proizvodi, od interneta, videonadzornih sistemov, satelitske GPS navigacije, elektronskega cestninjenja in drugi tehnični predmeti, uporabljeni pri sodobnem nadzoru. Leman-Langlois[8] zato pravilno ugotavlja, da tehnologijo predstavljajo objekti, ki jih ni lahko opazovati ali meriti, ker so tudi to sociološki objekti: spreminja jih kultura in tudi sami povratno spreminjajo kulturo. V sodo-

[7] Po Leman-Langlois 2008a: 4.

[8] *Ibidem*: 2.

bni kulturi nezaupanja in proizvajanja vedno novih tveganj, ki nas domnevno ogrožajo, zato tudi trivialni predmeti postajajo varnostna zadeva.

Študije znanosti in tehnologije ugotavljajo, da je »tehnologija politika z drugimi sredstvi« in da je »tehnologija aktivnost na daljavo«. V specifični kulturi strahu in nezaupanja po terorističnih napadih v New Yorku, Londonu in Madridu v začetku 21. stoletja, tako vsakodnevni predmeti in vsakodnevne dejavnosti spreminjajo »ontološki status«. Neyland[9] ugotavlja, da so nahrbtniki in druga prtljaga (bodisi pripeta na človeka, posebej v Londonu, bodisi zapuščena – posebej na letališčih), plastične vrečke, parkirani avtomobili, voda in druge tekočine (na letališčih), vožnja s podzemno železnico, delo v visokih stolpnicah itn. zamenjali svoj družbeni pomen. Iz vsakodnevnih predmetov, prostorov in aktivnosti so se preoblikovali v kategorije suma, v nekaj, o čemer bi nas moralo skrbeti. Ti predmeti so spremenili svoj »ontološki status« – potencialno lahko status nevarnega predmeta prejme prav vsak predmet – in vplivajo na to, o čem naj razmišljamo, kako naj se vedemo, kako naj se reorganizirajo institucije in preoblikujejo odnosi med različnimi enotami v organizacijah.[10]

[9] Neyland 2009.

[10] Z etnografskimi študijami pisemskih pošiljk je Neyland ugotovil, da so zaradi groženj s »pismi-bombami« (antraks) pisemske pošiljke postale razumljene v kategorijah tveganja. Ti trivialni predmeti so dobili svoje specifične tarče (majhne in srednjevelike sprejemne pisarne), zaradi njih pa se je spremenilo tudi delovanje subjektov, ki naj bi preusmerili svoje aktivnosti in prevzeli nove odgovornosti za upravljanje s temi tveganji. Zaradi objektov (predmetov, aktivnosti), ki so spremenili svoj »ontoloških status«, so se družbeni odnosi premrežili. Predmeti in aktivnosti, pogreznjeni v vsakdanjost, ki jim doslej nismo naklonili nobene pozornosti, so na ta način dvignjeni iz vsakdanjosti v kategorije, ki po novem potrebujejo veliko pozornosti in zahtevajo preobrat trdovratnih in rutiniziranih družbenih odnosov. Po Neyland 2009: 38.

## IT ima Janusov obraz

Pomen IT za kriminaliteto in odzivanje nanjo ter za družbeno nadzorovanje in zagotavljanje zasebnosti učinkuje v obe smeri: predstavlja panacejo in Pandorino skrinjico, ima Janusov obraz.

V povezavi s kriminaliteto in odzivanjem nanjo moramo IT razumeti na več načinov:[11] (1) tehnologija omogoča nove načine izvrševanja kaznivih dejanj (tehnološki pripomočki omogočajo učinkovito, hitro in prožno dogovarjanje storilcev pri izvrševanju kaznivih dejanj, policijsko sledenje geografsko razpršenim in mobilnim članom kriminalne združbe pa je zelo težavno); (2) a tehnologija omogoča tudi novo in bolj učinkovito odzivanje na kriminaliteto, saj krepi (širi in poglablja) policijsko moč (satelitska navigacija omogoča policistom slediti označenim predmetom in vozilom na daljavo, zbiranje prometnih podatkov omogoča obsežno rudarjenje, vzorčenje, profiliranje, videonadzor omogoča preverjanje dogajanja na kraju zločina brez nezanesljivih izpovedb prič in v dejanskem času, v katerem se nekaj dogaja); (3) tehnologija predstavlja novo grožnjo nacionalni varnosti (»kibernetski cunami« bi v »informacijski družbi« ogrozil kritično nacionalno infrastrukturo (dobavo električne energije, vodovodne sisteme, vse vrste prometa itn.); (4) a tehnologija ponuja tudi nove možnosti za zaščito nacionalne varnosti, saj zbirke podatkov o številnih rutinah našega vsakdana (na primer o finančnih transakcijah, fizičnem gibanju, elektronskih komunikacijah, potrošnji) omogočajo izjemne možnosti preventivnega in obveščevalnega delovanja represivnih organov, ki se usmerja na vsakogar izmed nas; (5) zato pa tehnologija predstavlja tudi nove možnosti za kršenje temeljnih človekovih pravic in svoboščin z nediskriminatornim nadzorom slehernika (na primer z videonadzornimi kamerami, »pametnimi« dokumenti), posege v zasebnost, kršitve domneve nedolžnosti, privilegij zoper samoobtožbo in drugih kazenskih procesnih kavtel; (6) a tudi nove možnosti za zaščito temeljnih človekovih pravic in svoboščin (na primer avtomatizirani identifikacijski sistemi omogočajo nediskriminatorno delovanje, kar omogoča enakopravno obravnavo tudi morebiti diskriminiranih družbenih manjšin).

Pomen IT za nadzorovanje in zasebnost enako učinkuje v obe smeri. Tehnično (p)o(d)krepljen nadzor je konstantno (ves čas) in ubikvitarno (vsepovsod) navzoč. Danes res ni več »prostora, kamor bi se skrili« (O'Harrow).[12] A tudi cena za izločitev bi bila velika – izločitev iz vseh osrednjih družbenih procesov.[13] Nadzor zato sam po sebi ni slab: uporaba radio-frekvenčnih čipov (angl. *Radio-Frequency Identification Tag* oziroma *RFID tag*) v zdravstvene namene ni a priori sporna.[14] Možnost izdelave »aleksandrijske« knjižnice, ki bi zbrala kulturno dediščino sveta, se zdi kar pogoj »svobodne kulture«. Lyon[15] zato poudarja, da tehnično okrepljen nadzor omogoča ena-

[11] Leman-Langlois 2008a: 2–3.

[12] O'Harrow 2005.

[13] Bond 2009.

[14] Zdravljenje na domu namesto institucionalizacije (hospitalizacije) bolnika s pomočjo tehnologije, glej Stout 2008.

[15] Lyon 2002.

kost in varnost, pa tudi ogroža varnost. Je del skrbi za človeka in tudi njegove kontrole.[16] Podobno Ball in Webster[17] menita, da je sodobno nadzorovanje »paradoksno«, ker hkrati ovira in omogoča. »Paradoks nadzorovanja« je, da je invazivno, se vsiljuje in nadleguje, a tudi krepi in omogoča oblikovanje človeka kot državljana.[18] Pogoj vključitve v skupnost je mogoč le s podreditvijo nadzoru, evidentiranju, klasificiranju (na primer prebivališča za potrebe obdavčenja), a v zameno posameznik prejme priložnosti, pravice in storitve (na primer volilno pravico, socialne pomoči).

Ta dvojnost kaže na nezadostnost trditve, da sodobno tehnično okrepljeno nadzorovanje ogroža zasebnost. Res je tudi nasprotno. Povečane zahteve po zasebnosti generirajo vedno nove oblike nadzora, ki naj zagotovijo, da druge izločamo in da omejimo dostop do sebe in do informacij o sebi.[19] Na primer, zahteva po povečani zasebnosti v lastnem domu je proizvedla nadzor prostora v obliki ključavnic. Vsaj pred dvema desetletjema na slovenskem podeželju ni bilo mogoče najti zaklenjenih domov, če so bili tam prebivajoči doma. Danes pa je že do vhodnih vrat vedno teže priti, saj nas pričakajo »videofon« naprave že pri mejnih ograjah. Pričakovanja po »nepropustnem« varovanju zasebnosti so tista, ki povečujejo nadzor. Ta pa povratno omogoča tudi večje posege v zasebnost – a ne »naše«, temveč zasebnosti »drugih«.

Zasebnost je nemogoče enkrat za vselej definirati, njeno pojmovanje se razlikuje med različnimi družbami in spreminja v času. Za njeno sodobno pojmovanje je ključno, da je prežeta s posesivnim individualizmom,[20] zasebno lastnino in dvomljivim pojmovanjem osebe kot avtonomne, od družbe ločene »entitete«. *Homo clausus* je utvara, kot je pokazal Elias,[21] saj je posameznik močno vpet v družbenosimbolno matrico (celokup institucij, jezika in ritualov).

Pri pojmovanju zasebnosti danes po eni strani opažamo trend njenega večjega poudarjanja (na primer ustanavljamo nove državne institucije, kot je Informacijski pooblaščenec), po drugi strani pa mu prihaja nasproti trend vedno večjega razgaljevanja zasebnosti. Oba trenda kažeta, da gre za vzpostavljanje novega ravnotežja med posameznikom in družbo, do novega načina, kako se posameznik dojema v odnosu do družbenega in v množici. Ker želi komoditeto, se zasebnosti tudi odpoveduje. Zato Leman-Langlois[22] prepričljivo sklepa, da postaja zasebnost valuta, s katero trgujemo na trgu: v zameno za popuste pri nakupovanju dovolimo trgovcem zbirati podatke o naših nakupih (potrošniško profiliranje je zato *stricto sensu* pravno nesporno, saj temelji na »svobodnem pristanku« posameznika), v zameno za hiter *check-in* na letališču dopustimo zbiranje podatkov o naših biometričnih (telesnih) značilnostih (na primer

[16] Lyon 2007: 3.

[17] Ball, Webster 2003: 12.

[18] Ball, Webster 2003: 12.

[19] Lyon 2002.

[20] Lyon 1994.

[21] Elias 2001.

[22] Leman-Langlois 2008c.

prstnega odtisa na *fast-track* programih, kakršen je na primer na letališču Amsterdam-Schiphol).

Solove[23] za sodobni čas prav tako ugotavlja, da prihaja do redefinicije zasebnosti, še posebej do novih nians v njenem pojmovanju pri »*Google* generaciji«. Strah, da so mlajši uporabniki izgubili vrednostni kompas pri varovanju lastne zasebnosti, kaže tudi na nerazumevanje njihove strukturne vloge v sodobnem zahodnem svetu. Zahteve po »prodornosti«, neskrupulozni tekmovalnosti in (samo)promociji so temeljne zahteve v »kulturi narcisizma« (Lasch). Danes ne gre več za to, da nas panoptični »Veliki brat« gleda, temveč za to, kar Mathiesen[24] imenuje sinoptikon: množica opazuje peščico – elito v podobi »zvezdnikov« v »družbi spektakla«. Če so iz Benthamovega sveta vsi želeli zbežati pred nevidno nadzorno instanco, v sinoptikonu želimo vsi biti vidni, v središču, »na ogled«. V dobi tekoče moderne (Bauman), karnevalske skupnosti, družbe spektakla, kulture narcisizma (Lasch) oziroma oznamčene družbe (Klein) so se spremenili sami subjekti. Upanje, da se bomo jutri spet srečali, je danes izgubilo velik del svoje verodostojnosti.[25] Verjetnejša je možnost, da bo to, kar bomo srečali jutri, naše lastno telo, ki bo vpeto v dokaj drugačne družbene okoliščine, v radikalno spremenjeno družino, razred, sosesko in družbo sodelavcev. Z drugimi besedami: kar je bilo v določenem trenutku zanimiv osebni podatek, postane v novih družbenih vlogah, družbenih kontekstih in sredinah le še pričevanje o neki preteklosti muzealne vrednosti.

Zasebnosti, ki jo IT domnevno ogroža, ne moremo pojmovati kot nekaj, kar obstaja zgolj tam, kjer ni kopice osebnih podatkov. Osebni podatki so tu in vedno več jih je. To pa avtomatično še ne pomeni, da je naše zasebnosti kaj manj. Paradoksalno, a pomemben je naš nadzor nad tem, kako se informacije razširjajo. Bolj ko lahko sami vplivamo na razširjanje naših osebnih podatkov, bolj je življenje v naši družbi bližje skupnosti enakopravnih posameznikov. To je tudi razlog, da spletna socialna omrežja ne ogrožajo avtomatično zasebnosti njihovih uporabnikov. Uporabniki tam res razgaljujejo številne zasebne podatke, kar daje vtis o popolni odpovedi zasebnosti, a vendar raziskave kažejo,[26] da uporabniki ohranjajo precejšno mero nadzora nad razširjanjem podatkov, z zelo redkimi izjemami, ki oznanijo informacije, kot so telefonske številke in naslovi prebivališč.

[23] Solove 2007.

[24] Mathiesen 1997.

[25] Bauman 2002.

[26] Jones *et al.* 2008.

## Vznik prevencijske pravičnosti

Informacijska tehnologija spreminja kriminaliteto in odzivanje nanjo. Kriminaliteto spreminja v dveh ozirih: kot sredstvo za izvrševanje kaznivih dejanj spreminja kriminalne priložnosti in olajšuje izvrševanje (obstoječih oblik) kaznivih dejanj,[27] kot (nov) objekt napada pa nastopa v obliki (nove) kibernetske kriminalitete.[28]

Odzivanje na kriminaliteto zaradi informacijskotehnoloških pripomočkov pa kaže, da so spremembe pri reakciji na kriminaliteto tako korenite, da presegajo pomen sprememb v kriminaliteti. Z drugimi besedami, tehnološko podkrepljena reakcija na kriminaliteto, ki naj bi bila rešitev za »problem kriminalitete«, postaja nov problem zase: namesto, da bi reševala težave, ustvarja nove.

Delovanje akterjev kazenskopravnega sistema in novih zasebnih akterjev zagotavljanja varnosti se vedno bolj usmerja na zgodnje označevalce ali tveganja za nastanek kazenskopravnega primera. Te spremembe, ki jih je IT povzročila v »boju« zoper kriminaliteto, zaokrožajo nov koncept t. i. »prevencijske pravičnosti« (angl. »*preemptive justice*«),[29] ki širi in poglablja[30] nadzorovanje našega »vsakodnevnega« življenja.[31] Kaj pravzaprav ta koncept prinaša novega glede na doslejšnje prevencijsko kriminalitetno politično delovanje akterjev kazenskopravnega sistema?

Prevencijska pravičnost je nasledek (stare) modernistične težnje po dominaciji in obvladovanju vedno številčnejših vidikov posameznikovega življenja, večjih delov sveta, žive narave in populacije ter vredno(s)tnega imperializma. Je nasledek ideje, da je svet mogoče razumeti, če ga le dovolj nadrobno analiziramo in razstavimo na manjše (sestavne) dele, da bi ga naposled ukrojili po našem vnaprej zamišljenem načrtu. Te modernistične težnje IT z možnostjo malodane neskončnega beleženja, zbiranja, shranjevanja in analiziranja osebnih podatkov pomaga uresničevati. Sintetiziranje velike količine podatkov z računalniki naj bi nam omogočilo razumeti vedno bolj kompleksen

---

[27] Organizacija in delitev kriminalnega dela sta se spremenili v treh ozirih: (1) posamezniku tehnologija nudi večji nadzor nad izvedbo kriminalnega dejanja, tako da lahko kaznivo dejanje izvršijo tudi posamezniki, ki pred tem niso imeli zadostnih virov in sredstev (na primer organizacijske, finančne moči) za izvedbo dejanja; (2) oblikujejo se nove oblike kriminalne organizacije preko sodelovanja različnih specializiranih skupin (na primer pri kibernetični kriminaliteti je novo sodelovanje (dotlej ločenih) skupin hekerjev, oblikovalcev računalnikih virusov in pošiljateljev nezaželene pošte, tako da tisti, ki okužijo računalnike s Trojanskimi konji, o tem obveščajo skupine, ki pošiljajo neželeno pošto, kar privede do tega, da je te računalnike mogoče »ugrabiti« in uporabiti kot *zombije*); (3) spremembe, ki se nanašajo na izgubo in/ali pridobitev novih veščin (t. i. *deskilling & reskilling effect*). Po Wall 2007: 39–44.

[28] Prava kibernetska kriminaliteta je tista, ki bi v skladu s testom transformacije (oziroma eliminacije) prenehala obstajati, če bi kibernetski prostor ne obstajal. Po Wall 2007: 34 in nasl.

[29] Tako Zedner 2007, Brown in Korff 2009, McCulloch in Pickering 2009.

[30] Tezo o širjenju in poglabljanju nadzora v Ball, Webster 2003.

[31] Teza o nadzoru običajnega vsakdana (trivialnih predmetov, aktivnosti in/ali prostorov) v Haggerty in Ericson 2000, Staples 2000, Lyon 2001, Franko Aas, Oppen Gundhus, Mork Lomell 2009.

svet in ga celo enkrat za vselej »prebrati« (na primer s superračunalniki podprtimi projekti, kot je bil Projekt človeški genom).

Z usmerjenostjo »na površino«, tj. z načini uporabe IT, ki od uporabnika ne zahtevajo poznavanja temeljev njenega delovanja (na primer, ko preklapljamo med različnimi virtualnimi »okni« znanje dvojiškega jezika ni potrebno in lahko ostajamo »na površini«), s svojo decentralizirano strukturo omreženih računalnikov pa IT hkrati tudi ruši svet moderne. Z ustvarjanjem »uporabnikov«, ki delujejo »na površini«, ne da bi jim bilo potrebno razumeti dogajanje »za zaslonom«, postaja sodobno računalništvo metafora sodobnega (postmodernističnega) pogleda na svet.[32] Torej razumevanja, po katerem sveta ni več mogoče do konca razložiti z eno in edino metateorijo, ki bi omogočala deduktivno izpeljavo preostalih pravil, tudi tistih za urejanje družbe in upravljanje z javnimi zadevami. Svet je preveč kompleksen, da bi ga enkrat za vselej do konca razumeli, zato ostanimo »na površini« in tam »upravljajmo« z viri, ki jih imamo, je osrednja implicitna predpostavka novega odnosa do sveta.

Po drugi strani pa narava kibernetskega prostora predstavlja tudi zgled decentraliziranega, večplastnega, horizontalno upravljanega prostora, ki nakazuje na možnosti novega načina upravljanja skupnih zadev na svetovni ravni onkraj režima nacionalnih držav združenih v okornem OZN.[33] Kiberprostor (IT) »grozi«, da bo zbrisal meje časa, prostora, lastnine, obstoječih hierarhij, medosebne meje in meje med državami.[34] Je nekje vmes med starim modernim in novim postmodernim, krepi potenciale moderne in že kaže obrise novega postmodernega sveta. Kako se to kaže v razumevanju kriminalitete in v reakciji nanjo?

---

[32] Turkle 1995.

[33] Za Delmas-Marty je upravljanje kibernetskega prostora paradigmatski primer svetovne vladavine oziroma možnosti (siceršnje) »svetovne družbene pogodbe«, »svetovnega razdruženega reda« ali »postnacionalne konstelacije«, ki bi delovala na različnih ravneh (nacionalni, regionalni in svetovni) in vključevala celoto (državnih in nedržavnih) akterjev, déležnikov (držav, industrije, akademije in civilne družbe). Za kaj takega meni, da je potrebna »mondalizacija« prava, ki jo opredeli drugače od globalizacije, ki označuje globalno razširjanje kapitala oziroma ekonomskega delovanja, in poleg nje vključuje tudi globalno razširitev temeljnih človekovih pravic »druge generacije« (ekonomskih in socialnih pravic). Po Delmas-Marty 2008.

[34] Meje časa IT briše, ker deluje hipno, njene »računske« kapacitete obdelovanja podatkov se eksponentno povečujejo, informacije se pretakajo v »realnem času«. Meje prostora briše, ker omogoča prenos podatkov na globalni ravni in preko obstoječih meja. Obstoječe hierarhije moči ruši, ker opolnomoči različne akterje civilne družbe od posameznikov do korporacij, meje lastnine briše, ker omogoča uživanje kulturnih dobrin, ki jih je bilo potrebno po dosedanjih poslovnih modelih distribucije plačevati, medosebne meje briše, ker omogoča osebni stik, kjer doslej ni bil mogoč. Meje med državami briše kibernetski prostor, ker so aktivnosti v njem praviloma čezmejne in uhajajo tradicionalnim konceptom delitve prostora po nacionalnih državah, ker kibernetski prostor nima centralnega upravljavskega organa, iz katerega bi bilo mogoče obvladovati periferijo sistema, temveč njegove številne infrastrukturne plasti upravlja decentralizirano več organizacij, ki so sestavljene iz različnih déležnikov (držav, industrije, uporabnikov) in v okviru različnih jurisdikcij, njihovo delovanje pa poteka po različnih pravilih (državnih predpisih, samoregulativnih iniciativah in nadnacionalnih vladnih in nevladnih aktih različnih stopenj obligatornosti). Glej Marx 2008.

Značilnost prevencijske pravičnosti, ki ne bi bile mogoče brez sodobnih zmogljivosti IT, je, da spreminja (liberalen in na konceptu človekovih pravic zasnovan) pravni okvir za uporabo sile v zunanji in notranji politiki držav (in drugih akterjev pri zagotavljanju varnosti). Kot reakcija na teroristične napade je nova »pravičnostna« paradigma, na področju politično bolj gnetljivega mednarodnega prava, legitimirala novo obliko »kirurških napadov«[35] prevencijske narave,[36] v obliki vojaškega posredovanja na tujem ozemlju, ki naj bi jih opravičevala »neposredna grožnja napada z orožjem za množično uničevanje«. »Vojna proti terorizmu« je bila močan generator prevencijske pravičnosti.[37] Kasneje se je z doktrino o nuji »zaprtja posameznika, za katerega obstaja vsaj odstotek verjetnosti, da je vpleten v teroristični napad«, idejnega očeta Dicka Cheneya, razširila v prevencijski kazenski pregon.[38] Zanj je značilno nižanje dokaznih standardov v obliki »prevencijskih obtožb«, razširjene so možnosti sojenja brez porote, večje so možnosti izključitve javnosti na sojenju in možnosti nerazkritja dokazov obrambi, če je to v interesu nacionalne varnosti, dokazni standardi se znižajo – na primer za obsodilno sodbo namesto standarda »onkraj razumnega dvoma«[39] zadostuje (nižji) civilnopravni standard »ravnotežje verjetnosti«,[40] možen je daljši pripor še pred vložitvijo obtožnice itn.

Te korenite spremembe, ki jih IT omogoča z izjemnimi računskimi kapacitetami evidentiranja, hranjenja in obdelovanja podatkov o vsakodnevnih predmetih, prostorih in posameznikovih aktivnostih, so nas po oceni Zedner privedle v »pred-kriminalno družbo«.[41]

Glavna premika, ki nas vodita iz »po-kriminalne družbe«[42] v »pred-kriminalno družbo«, sta dva.[43] Prvič, iz osredotočenosti na preteklo kaznivo dejanje, ki se očita in dokazuje obdolžencu, se delovanje akterjev kazenskega pregona premika k dokazovanju (neke stopnje) verjetnosti storitve kaznivega dejanja v prihodnosti. Zločin je razumljen kot tveganje ali potencialna izguba, prakse soočanja z zločinom so prevencijske narave, varnost pa komoditeta, ki se prodaja za profit. Glavni pojmi (koncepti) tega obrata so (aktuarski) izračuni, tveganja, negotovost, nadzorovanje, varnostni ukrepi, pazljivost, prevencija in zagotavljanje varnosti.

---

[35] Angl. *surgical strikes*.

[36] Angl. *pre-emptive strikes*.

[37] McCulloch, Pickering 2009.

[38] Angl. *pre-emptive prosecution*.

[39] Angl. *beyond reasonable doubt*.

[40] Angl. *balance of probabilities*.

[41] Oznaka »pred-kriminalen« (angl. *pre-crime*) izvira iz romana *Minority Report* (Philip K. Dick, 1956) in istoimenskega filma (Steven Spielberg, 2002), kjer družbo varujejo pred kriminaliteto t. i. »*pre-crime units*«, enote, ki ne preiskujejo že izvršenih kaznivih dejanj, temveč odkrivajo storilce bodočih kaznivih dejanj. Glej več v Zedner 2007.

[42] Angl. *post-crime society* označuje glavno usmeritev akterjev kazenskopravnega sistema na preiskovanje že storjenih (preteklih) kaznivih dejanj in na kazenski pregon domnevnih storilcev.

[43] Zedner 2007.

To anticipiranje tveganj seveda ni povsem nova orientacija v kriminalitetni politiki modernih kaznovalnih sistemov. A raziskovalci ugotavljajo, da so podatkovne zbirke postale središčne za delovanje akterjev kazenskopravnega sistema,[44] da se je paradigma policijskega delovanja korenito spremenila[45] in da so velike količine podatkov (v posamičnem kazenskem primeru tudi več terabajtov), ki se nanašajo na številne vidike posameznikovega življenja, ki jih doslej (bodisi iz fizičnih bodisi iz ekonomskih razlogov) ni bilo mogoče sistematično beležiti in analizirati (na primer vzorce gibanja, potrošnje, denarnih tokov, komunikacije itn.), proizvodnja novih podatkov o posamezniku (ki se jih sam morda niti ne zaveda) z rudarjenjem in povezovanjem različnih podatkovnih zbirk, danes nekaj povsem novega. Obveščevalno policijsko delovanje je postalo prototip sodobnega policijskega dela.[46]

Drugič, premik v osredotočanju na prihodnost je pospremljen še s sektorskim premikom.[47] Varnosti ne zagotavlja več le država, temveč v vedno večji meri tudi zasebni sektor: zasebna varnostna industrija in civilna družba v obliki programov, ki stremijo k vključevanju slehernika in poudarjajo samozaščitno vedenje, pozorno čuječnost, pa tudi organizacijsko in finančno soudeležbo pri zagotavljanju reda in miru (na primer zagotavljanje varnosti v skupnosti – *community policing*). Delitev dela poteka tako, da zasebni sektor na »prostovoljen« in podjetniški način sodeluje pri izvajanju nadzora še preden se zgodi kaznivo dejanje, za aktivnosti po storjenem kaznivem dejanju pa (še) skrbijo državni akterji.[48]

Posledica obeh premikov je, da ukrepov (zlasti protiteroristično navdahnjene) kriminalitetne politike ni več mogoče umestiti v okvir konvencionalnih prevencijskih kriminalitetnopolitičnih ukrepov. Prihaja do mešanja državnih in zasebnih akterjev pri zagotavljanju varnosti in reda (tj. javnega in zasebnega interesa pri monopolizaciji sile, kar je konstitutiven element suverena), protiteroristični ukrepi združujejo nacionalno varnost s pregonom kriminalitete, prihaja tudi do zamegljevanja zunanje in notranje prisilne moči države.[49] Elemente kazenskopravnega boja zoper kriminaliteto se združuje z elementi nacionalne varnosti, policijske sile pa z vojaškimi in obveščevalnimi

---

[44] Garfinkel zato govori o ZDA kot o narodu podatkovnih zbirk (angl. *database nation*). Teh ne oblikuje le država, temveč številni zasebni akterji, ki so vstopili v mehanizme zagotavljanja varnosti (korporacije in podjetja, nevladne organizacije) in intenzivirajo zbiranje informacij o posamezniku. V Garfinkel 2001.

[45] Lemieux 2008.

[46] Lemieux 2008.

[47] Zedner 2007: 262.

[48] Delitev ni povsem natančna, saj tudi policija izvaja (prevencijske) dejavnosti, ki so potencialno nevarne in bi lahko vodile v kriminaliteto, v odzivanju na že storjena kazniva dejanja (in tudi v vojskovanju) pa so tudi prisotni zasebniki: zasebni detektivi, zasebne vojske, zasebni forenzični laboratoriji, ki naj bi bili bolj neodvisni od državnih itn.

[49] Kader, vreden zaposlitve, niso psihologi, socialni delavci in drugi »psi-« eksperti socialne države. Podatek o *National Security Agency* (ZDA) je, da zaposluje največje število matematikov na svetu, takoj za jezikoslovci in tehnološkimi eksperti. Glej Priest, Arkin 2010.

zmogljivostmi države.[50] Meje med kriminaliteto, terorizmom in vojskovanjem zato postajajo zaradi transformativnih učinkov IT vedno težje določljive.[51] Vedno težje postaja ločevati[52] med akterji kazenskopravnega sistema in organi nacionalne varnosti, med kriminalitetno politiko in obveščevalno politiko, med policijskim in vojaškim posredovanjem, med organi kazenskega pregona in obveščevalnimi agencijami, med nacionalnimi in mednarodnimi oblikami uveljavljanja kazenskega prava ter med lokalnimi in mednarodnimi kriminalnimi dejavnostmi in organizacijami.[53]

IT industrija je ključno sredstvo za vzpostavitev »pred-kriminalitetne« (*pre-crime*) paradigme. Eksponentno rastoča zmogljivost zbiranja, shranjevanja in procesiranja podatkov ji omogoča vrtoglave donose.[54] Politiki pa z uporabo novih tehnologij iskanja sledov prihodnjega zločina dokazujejo, da nekaj vendarle počno v boju zoper kriminaliteto, breme zagotavljanja varnosti pa prenašajo na civilno družbo.

* * *

Knjiga v prvem delu obravnava vpliv IT na tehnično (p)o(d)krepljeno nadzorovanje (angl. *surveillance*). IT spreminja intenziteto nadzora (omogoča intenzivnejše – globlje in širše nadzorovanje),[55] kraj in čas nadzora (omogoča ubikvitarno in permanentno nadzorovanje), ter subjekte in objekte nadzora (nadzornik ni več le država, ki je tradicionalno razumljen »Veliki brat«, temveč tudi korporacije, podjetja in posamezniki, ki s(m)o postali novi »mali bratci« in na razne načine nadzorujemo drug drugega in državo; objekti nadzora – nadzorovani pa so poleg individualno določenih oseb vedno bolj tudi agregati (vzorci) posameznikov,[56] »nevarni« predmeti in aktivnosti,[57] ki so do

[50] Po McCulloch, Pickering 2009.

[51] Thomas, Loader 2000: 3.

[52] Tako Marx 2008.

[53] Sodobne »informacijske vojne« se močno razlikujejo od »industrijskega vojskovanja«: ni več množične mobilizacije, vojaki postajajo »*knowledge warriors*« (Toffler & Toffler), vojne so »instantne« (Castells), načrtovanje operacij postane natančno s pomočjo teorije iger in simulacij, napadi so »kirurški«, z letali brez človeške posadke, zato je govor o »post-militarnih družbah« (Show) in »post-heroični« vojaški politiki (Luttwalk). Po Webster 2003: 100–105.

[54] Rast zasebne varnostne industrije je dobro razpoznavna po ekonomskih kazalnikih. ZDA je v času predsedovanja Clintona odobrila 1,46 milijarde dolarjev za boj proti grožnji kibernetskega terorizma. V Avstraliji je maja 2001 znašal proračun za varovanje »kritične informacijske infrastrukture« 2 milijona dolarjev, se potrojil na 6 milijonov dolarjev leta 2002, nato pa v štirih letih zrasel na 24,9 milijone dolarjev (po Yar 2009: 198). Zasebna varnost najbolj nabreka v ekonomsko najbolj razvitih državah: v VB je po podatkih *The British Security Industry Association* 600.000 ljudi zaposlenih v zasebni varnostni industriji, kjer se »obrača« 5 milijard funtov (l. 2004), videonadzorstveni sektor je zrasel s 84 milijard (l. 1993) na 509 milijard (l. 2005) funtov, vrednost človeškega varovanja je poraslo s 530 milijonov (l. 1993) na 1557 (l. 2005) milijonov funtov. Po Zedner 2007.

[55] Ball, Webster 2003.

[56] Feeley, Simon 1992.

nedavna veljali za povsem neproblematične). V tem delu nas zanimajo tudi novi načini nadzora, za katere je značilno, da so manj opazni, avtomatizirani in potisnjeni v vsakdanje rutine, omogočajo pa bolj invaziven nadzor (na primer »neopazno« profiliranje potrošnikov) ter vprašanje povezanosti tehnično okrepljenega nadzora z drugimi sodobnimi družbenimi pojavi.

Tehnično intenziviran nadzor je v veliki meri posledica dveh velikih kriminalitetno-političnih premikov v začetku 21. stoletja, »boja proti terorizmu« in nastajajočega prevencijskega modela pravičnosti, ki pozornost akterjev sodobnih okcidentalnih kazenskopravnih sistemov obrača v prihodnost. Akterji kazenskopravnega sistema nimajo več za nalogo »zgolj« odkrivati že storjenih kaznivih dejanj in preganjati domnevnih storilcev, temveč tudi preventivno obveščevalno delovati, da do kaznivih dejanj sploh ne bi prišlo, kar utemeljeno navaja na misel, da iz »pokriminalitetne družbe« (angl. *post-crime society*) vstopamo v »predkriminalitetno družbo« (angl. *pre-crime society*).[58]

Zasebnost, ki jo informacijska tehnologija ogroža in hkrati tudi omogoča ščititi, je antipod družbenega nadzorovanja in je obravnavana v drugem delu knjige. Na splošni (definicijski) ravni se še vedno zastavlja vprašanje, kaj sploh zasebnost je, oziroma, kje je »prava mera« stičišča zasebnosti in nadzora, ki sta relativni, v času in prostoru spremenljivi kategoriji. Posameznik je nujno vpet v družbene institucije in procese in je zato po eni strani »vraščenost« posameznika v družbeno-simbolno matrico pogoj njegovega duševnega samouresničenja in »zdravja«. Izven družbe bi ostal psihotično vase zavrteno bitje in nema žival. Po drugi strani pa vsi potrebujemo »prostor zase«, želimo »biti pri sebi« in v določenih družbenih situacijah utemeljeno pričakujemo zasebnost. Zasebnost, ki je odnos do drugega, je pravzaprav garant posameznikovega »normalnega« duševnega razvoja in tudi »zdravja«. Ta »paradoks zasebnosti« se kaže tudi v razmerju do družbenega nadzorovanja. Zasebnost je še vedno pogosto razumljena na enosmeren vzročnoposledični način, kot da povečan nadzor nujno ogroža zasebnost. Navedeno drži, a prepogosto se spregleda, da so ravno povečane zahteve po zasebnosti in tega, da nas »pustijo pri miru«, tiste, ki generirajo več nadzora. Zahteva po več zasebnosti je hkrati zahteva po več nadzora.

Knjiga se zasebnosti loteva z analizo specifične vrste zasebnosti, tj. komunikacijske zasebnosti na delovnem mestu, ki je specifičen in izrazito asimetričen prostor družbene moči. Zasebnost na/pri delu je ključna za naša življenja, saj večino in vedno več časa preživimo ravno na delovnem mestu. Podjetja so postala novi subjekti družbene moči, ki preraščajo moč nacionalnih držav, in so aktivni in invazivni subjekti nadzora našega vsakdana. Kar je ključno v času fleksibilnih in prekarnih zaposlitev sodobnega časa je tudi, da se nadzorovano delovno »mesto«, ki je bil tradicionalno ločen kraj in čas dela, (pre)pogosto razteza daleč izven delovnega okolja in delovnega časa, kar odnose družbene moči med delavcem in delodajalcem še bolj nagiba v korist drugega. Zasebnost na delovnem mestu se tako kaže kot trdnjava ohranitve človečnosti na prostoru in v času, ki okupira večino naših življenj. Prispevek prikaže, kako različno je pravica do zasebnosti razumljena v ameriškem pravnem redu in v Evropi, kakšno je

---

[57] Neyland 2009.

[58] Zedner 2007.

razmerje med pravico do zasebnosti zaposlenega in lastninsko pravico delodajalca, ter kako komunikacijsko zasebnost pravno varujemo v Sloveniji.

Pri spremembah, ki jih informacijska tehnologija sproža pri načinih izvrševanja kaznivih dejanj, oblikah in vrstah kriminalitete, knjiga v tretjem delu analizira hekerstvo (tretje poglavje) in poseben tip internetne goljufije (četrto poglavje). Hekerstvo (kot družbeno-kulturni fenomen) je bilo z novo pokapitalistično etiko motor nastanka kiberprostora. S časom je pod vplivi »močne in vplivne« koalicije varnostne industrije in velikih proizvajalk programske opreme spremenilo družbeno etiketo tako, da so dejanja hekerjev postala označena kot naivna, utopična in vedno pogosteje tudi zločinska. Etika darovalne ekonomije, vzajemnosti in solidarnosti, ki je prvotno naselila kiberprostor, se je iz kiberprostora izselila, ko je ta postal »veliko nakupovalno središče«. Kljub izgonu pa hekerstvo ostaja alternativna politična sila, ki jo kaže naprej gojiti. Predstavlja pomembno (redko) ogledalo kapitalističnemu sistemu gospodarstva in njegovim škodljivim psihološkim, ekološkim in solidarnostnim reperkusijam.

Nigerijska prevarantska pisma (goljufije »tipa 419«), ki jih knjiga pretresa v četrtem poglavju, kažejo drug sklop sprememb, ki jih je IT povzročila kriminaliteti. Ocene o naravi teh sprememb se (na abstraktni ravni) gibljejo od ocen, da smo zaradi IT priča zgolj »staremu vinu v novih steklenicah« (Grabosky),[59] torej da se že znane fenomenološke oblike kriminalitete pojavljajo le v novi obliki (kar je potrebno storiti, je »raztegniti« pravna pravila na nove dejanske situacije), do ocen, da gre za »novo vino, za katerega še nimamo steklenic« (Wall).[60] Zato naj bi potrebovali nove koncepte in nova pravna pravila. A ta dilema je bolj kot z razumevanjem fenomenologije in novosti povezana s simbolno-ideološkim kategoriziranjem (etiketiranjem), ki naj priskrbi (ali odvrne) pozornost kriminologov, pravnikov, sociologov, socialnih psihologov, pedagogov, komunikologov, sistemskih varnostnih inženirjev, forenzikov in akterjev kazenskopravnega sistema na spremembe v kriminaliteti. V knjigi so zato prikazani mehanika prevar »tipa 419«, tipičen potek nigerijske prevare in psihološki mehanizmi njenih udeležencev, ter družbene razmere v Nigeriji (in njena umeščenost v svetu in posebej v odnosu do zahodnega sveta), ki so ugodno gojišče za prevare tega tipa. Podani so tudi napotki, kako se tovrstnim viktimizacijam izogniti.

Nigerijska prevarantska pisma so (konkretno) po eni strani »staro vino v novih steklenicah«, goljufije, ki so umeščene globoko v kapitalistično logiko prilaščanja. Po drugi strani pa so »novo vino«, saj gre za goljufije velikega obsega, ki zlorabljajo globalni domet interneta, avtomatizacijo izvrševanja kaznivih dejanj, kjer računalnik opravlja rutinsko delo masovnega pošiljanja e-pošte, za posledico pa imajo masovne viktimizacije; te so sicer lahko na individualni ravni bagatelne in si ne zaslužijo intervencije represivnega državnega aparata (na primer goljufija v vrednosti enega centa), a so lahko zelo resne na agregatni ravni (na primer z izvedbo 100 milijonov goljufij v vrednosti enega centa), lahko pa so tudi na individualni ravni »totalne«, tako da posameznik v mehaniki »drobnih korakov« izgubi svoje celotno premoženje.

Informacijska tehnologija ni spremenila le kriminalitete, temveč tudi odzivanje nanjo in temu je namenjen četrti del knjige. Subjekti formalnega družbenega nadzora, ki

[59] Grabosky 2001.

[60] Wall 1999.

so v središču analize, že upoštevajo dejstvo (ali bi to vsaj morali), da v »informacijski družbi« v digitalni obliki nastane ali je vanjo pretvorjenih vedno več dejavnosti (komunikacij, poslovnih procesov, kulturnih dobrin itn.) in da so številne naše aktivnosti malodane vedno zabeležene in evidentirane v digitalni obliki. Digitalni dokazi bodo imeli v (vseh) sodnih postopkih vedno pomembnejšo dokazno vlogo. Učinkovitost kazenskega pregona je zato že danes vedno bolj odvisna od policijske sposobnosti pridobiti, zavarovati in izvesti pravno veljavno analizo digitalnih sledi, kvaliteta kazenskih postopkov pa od tožilskih in odvetniških sposobnosti postaviti relevantna vprašanja ekspertom digitalne forenzike, ter od sodniškega poznavanja načinov delovanja (omreženih) digitalnih naprav in posledično primernega vrednotenja digitalnih dokazov.

Knjiga prikaže osnove digitalnih dokazov in temeljna načela forenzike digitalnih (elektronskih) naprav, veljavno kazenskoprocesno ureditev pridobivanja, ohranitve in pregleda digitalnih dokazov in posebej specifike forenzike mobilnih telefonov. Pomen tega dela knjige je velik tudi zaradi izjemno velikega razkoraka med družbeno in policijsko/pravosodno realnostjo v stopnji uporabe digitalne tehnologije. Stopnja informatiziranosti slovenske družbe je namreč še vedno v ostrem kontrastu s pomenom in vlogo digitalne forenzike v kazenskih postopkih. Slovenija je med relativno dobro razvitimi informacijskimi družbami: delež gospodinjstev z osebnim računalnikom znaša 70 odstotkov, z mobilnim telefonom 94 odstotkov, z dostopom do interneta s širokopasovno internetno povezavo pa 56 odstotkov (podatki za leto 2009).[61] Tudi opremljenost podjetij z IT je velika: vsa podjetja z več kot 250 zaposlenimi uporabljajo računalnike, imajo dostop do interneta in lastno spletno stran (podatki za leto 2009). Delež podjetij, ki imajo več kot 10 zaposlenih in uporabljajo računalnike, je malenkost manjši in znaša 98 odstotkov, podjetij, ki imajo dostop do interneta, je 96 odstotkov, tistih z lastno spletno stranjo pa je 69 odstotkov.

Če te podatke primerjamo s podatki o uporabi metod digitalne forenzike v policijski praksi, vidimo, da smo priča dvem različnim kulturam, od katerih je le ena digitalna. Selinšek[62] namreč navaja, da so metode digitalne forenzike v policijski praksi izjemno redek preiskovalni pristop: v letih 2001–2006 je policija skupaj na državno tožilstvo vložila ovadbe za 487.957 kaznivih dejanj, računalniško opremo pa je preiskala v 212 primerih, kar znaša 0,043 odstotka primerov. To kaže, da je policijsko delo še zelo daleč od distopičnih scenarijev, ki jih pooseblja metafora policijskega »Velikega brata«, in da če kdo, so sodobni subjekti nadzora, ki se zlahka izogibajo represivni moči države, »mali bratci« v obliki podjetij in korporacij, ki močno prehitevajo svojega starejšega sorojenca, ki naj bi ščitil javne interese.

Forenzika digitalnih (elektronskih) naprav (računalniška forenzika) je zato postopek, za katerega je pričakovati, da bo vedno pogostejši v vseh vrstah sodnih postopkov, izveden na iniciativo vseh strank postopka.

V knjigi je digitalni forenzični postopek natančneje opredeljen: to je postopek pridobivanja, ohranitve, pregleda, analize in predstavitve digitalni dokazov. Knjiga natančno analizira slovensko ureditev prvih treh faz postopka v kazenskem postopku

---

[61] Podatki za leto 2006: delež gospodinjstev z osebnim računalnikom 65%, z mobilnim telefonom 90%, z dostopom do interneta s širokopasovno internetno povezavo 34%. Po Statistični letopis 2006 in 2009.

[62] Po Selinšek 2008: 51.

(zaseg, zavarovanje, preiskava), kot so določene v noveli zakona o kazenskem postopku ZKP-J. Poleg tega velja spomniti, da bo forenzične preiskave v skladu s splošnimi pravili sicer res izvedel specialist strokovnjak v vlogi sodnega izvedenca za računalniško forenziko. A vrednost teh dokazov je podvržena načelu proste presoje dokazov, kar zahteva od strank postopka in sodišča poznavanje in razumevanje digitalnega forenzičnega postopka. Zanašanje na pomoč izvedenca zato ne bo zadostovalo za preseganje opisanega digitalnega razkoraka. V knjigi je poudarjeno, da preveliki upi, položeni v shranjene impulze, ki so »izjemno hlapljivi«, ali preveliko nezaupanje in nepoznavanje delovanja IT, vodijo v sodne odločitve, ki bodo odtujene od družbene realnosti. V tem delu knjiga obravnava še nekatere nove zanimive situacije: kdaj je mogoče uporabiti *plain view* doktrino pri brskanju po elektronskih napravah, kdaj upravičeno pričakujemo zasebnost na (iz računalnika) izbrisanih podatkih (saj na primer prestavljanje podatkov v »koš« na namizju računalnika in sukcesivno praznjenje »koša«, še ne pomeni, da podatkov iz naprave ni več mogoče priklicati), kakšna je vrednost dokazov, pridobljenih s strani zasebnih subjektov, ter vrednost zaseženih naprav in zavarovanih podatkov s strani drugih državnih organov?

Knjiga v zadnjem poglavju četrtega dela obravnava specifično temo forenzike mobilnih telefonov, ki bo v pravosodni praksi v bodoče vedno pogostejši in morda tudi najpogostejši primer računalniške forenzike. Forenzika mobilnih telefonov je zaradi konverzije različnih tehnologij v eno mobilno terminalsko napravo, ki ji bolj iz navade kot opisno korektno še vedno pravimo mobilni *telefon*, paradigmatičen primer računalniške forenzike. Mobilni telefoni so terminalske naprave, ki so hkrati računalniki (z urejevalniki besedil, odjemalci elektronske pošte, internetnimi brskalniki, organizatorji, telefonskimi imeniki, slovarji itn.), fotoaparati in kamere, GPS navigacijske naprave, radijski in televizijski sprejemniki, predvajalniki glasbe, filmov in elektronskih knjig itn. Vloga sodnega izvedenca za računalniško forenziko, kot jo predstavi sodni izvedenec, je zato toliko bolj ključna za zbliževanje sveta tehnike s svetom prava in je relevantna za udeležence vseh vrst sodnih postopkov, kjer bo potrebno ugotoviti dejstva o naših življenjih, ki pa so praviloma nekje pustila digitalno sled.

Na koncu je potrebno (samo)kritično dodati, da je *Kriminaliteta in tehnologija* prvi osnutek novega zemljevida razmišljanj o vplivih sodobnega tehnološkega razvoja na križišče nadzora in zasebnosti ter transformativne moči informacijske tehnologije na kriminaliteto in odzivanja nanjo, ter da ne predstavlja zaključene ali nemara hermetično zaprte analize vseh možnih vplivov IT. Knjiga ne obravnava pomena biotehnologije ali nevroznanosti na kriminaliteto, na primer vpliva znanosti o možganih na odzivanje na kriminaliteto, ki »preti«, da bo zamajala temeljno načelo subjektivne (krivdne) odgovornosti. Poglavje o nadzoru izpušča analizo posamičnih oblik nadzora, poglavje o zasebnosti obravnavo drugih vrst zasebnosti, poglavje o kibernetski kriminaliteti ne obravnava vseh možnih oblik te vrste kriminalitete, poglavje o digitalni forenziki pa tudi ne vseh (kazensko)pravno relevantnih podtem in tudi ne vseh oblik računalniške forenzike. Ta vprašanja so prav tako zelo pomembna, a njihova celovita obravnava bi terjala vsaj štiri knjige. Poleg tega bi bil namen izdelati publikacijo o vseh možnih vplivih IT na izbrane štiri sklope tudi prevzeten, (še bolj) podvržen »zastarljivosti«, besedilo pa usojeno na večni »delovni osnutek«.

Cilj pričujoče publikacije je prikazati razvoj domače znanosti na tem področju, ki le postopoma in z zastoji reflektira skokovit tehnološki razvoj. To pa je kritika, ki v celoti

zadeva vse družboslovne znanosti, ki bi morale kritično vrednotiti tehnološki napredek in posamične v osrednje družbene institucije in procese umeščene proizvode. Družboslovne vede žal le s težavo in zastoji sledijo tehnološkemu napredku, ki je postal glavni *doping* svetovne kapitalistične nadvlade, kar pa je tudi odraz drugorazrednega mesta, ki ga v tehnološki »družbi znanja« zaseda družboslovje, ki mu pogosto pripadejo zgolj (finančne, kadrovske idr.) drobtine z mize *Science*.

# Viri in literatura


1. Ball, K.; Webster, F. (eds.) (2003). **The Intensification of Surveillance. Crime, Terrorism and Warfare in the Information Age**. London, Sterlin Virginia: Pluto Press.
2. Bauman, Z. (2002). **Tekoča moderna**. Ljubljana: Založba /*cf. (Rdeča zbirka).
3. Bond, D. (2009). **Erasing David**. Dokumentarni film. Po URL: http://erasingdavid.com/, dostop dne 12.7.2010.
4. Brown, I.; Korff, D. (2009). Terrorism and the Proportionality of Internet Surveillance. **European Journal of Criminology**, let. 6, št. 2, s. 119–134.
5. Delmas-Marty, M. (2008). **Preureditev oblasti: domišljijske sile prava**. (Ivanka Sket – prevajalka, Alenka Šelih – avtorica dodatnega besedila). Ljubljana: GV založba (Zbirka Pravna obzorja; 36).
6. Douglas Smith, G.J. (2009). Empowered watchers or disempowered workers? The ambiguities of power within technologies of security. V: K. Franko Aas, H. Oppen Gundhus, H. Mork Lomell (eds.), **Technologies of inSecurity: the surveillance of everyday life**. Abingdon, New York: Routledge-Cavendish, s. 125–146.
7. Elias, N. (2001). **O procesu civiliziranja: sociogenetske in psihogenetske raziskave.** Zvezek 2. Ljubljana: Založba /*cf. (Rdeča zbirka).
8. Feeley, M.; Simon, J. (1992). The New Penology: Notes on the Emerging Strategy of Corrections and its Implications. **Criminology**, let. 30, št. 4, s. 449–474.
9. Garfinkel, S. (2001). **Database Nation: the death of privacy in the 21st century**. Sebastopol (CA): O'Reilly.
10. Grabosky, P. (2001). Computer Crime: A Criminological Overview. V: **Forum on Crime and Society**, let. 1, št. 1. New York: United Nations Publications, s. 35–53.
11. Graham-Rowe, D. (2000). Trial by Laptop: An Electronic Judge on Wheels Delivers Instant Justice. **New Scientist**, 29. april.
12. Haggerrty, K. D.; Ericson, R. V. (2000). The surveillant assemblage. **British Journal of Sociology**, let. 51, št. 4, s. 605–622.
13. Hempel, L.; Töpfer, E. (2009). The surveillance consensus: Reviewing the politics of CCTV in three European countries. **European Journal of Criminology**, let. 6, št. 2, s. 157–177.
14. Jones, S.; Millermaier, S.; Goya-Martinez, M.; Schuler, J. (2008). Whose space is MySpace? A content analysis of MySpace profiles. **First Monday**, let. 13, št. 9. Po URL: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2202/2024 dostop 7.6.2010.
15. Kagian, A.; Dror, G.; Leyvand, T.; Meilijson, I.; Cohen-Or, D.; Ruppin, E. (2008). A machine learning predictor of facial attractiveness revealing human-like psychophysical biases. **Vision Research**, št. 48, s. 235–243. Po URL: http://www.cs.tau.ac.il/~ruppin/amit.pdf, dostop 14.7.2010.

16. Kanaley, R. (1999). »States« Sale of Data: At What Price? Philadelphia Inquirer, 13.6., s. A01, **Philadelphia Inquirer**. Po URL: http://rp.ratiosemper .com/group/reality_pump/message/11175, dostop 15.3.2010.
17. Koritnik, B.; Grah Whatmough, A. (2010). Umetna inteligenca v pravu. **Pravna praksa**, št. 10, z dne 11.3.2010, s. 22–27.
18. Leman-Langlois, S. (2008a). Intruduction: technocrime. V: S. Leman-Langlois (ed.), **Technocrime: Technology, crime and social control**. Cullompton, Devon, Portland: Willan Publishing, s. 1–13.
19. Leman-Langlois, S. (2008b). The local impact of police videosurveillance on the social construction of security. V: S. Leman-Langlois (ed.), **Technocrime: Technology, crime and social control**. Cullompton, Devon, Portland: Willan Publishing, s. 27–45.
20. Leman-Langlois, S. (2008c). Privacy as currency: crime, information and control in cyberspace. V: S. Leman-Langlois (ed.), **Technocrime: Technology, crime and social control**. Cullompton, Devon, Portland: Willan Publishing, s. 112–138.
21. Lemieux, F. (2008). Information technology and criminal intelligence: a comparative perspective. V: S. Leman-Langlois (ed.), **Technocrime. Technology, crime and social control**. Cullompton [England], Portland, Or.: Willan Publishing, s. 139–168.
22. Lessig, L. (1999). **Code and other laws of cyberspace**. New York: Basic Books.
23. Lyon, D. (1994). **The Electronic Eye: The Rise of Surveillance Society**. Cambridge: Polity Press.
24. Lyon, D. (2001). **Surveillance Society: Monitoring Everyday Life**. Buckingham: Open University Press.
25. Lyon, D. (2002). Surveillance Studies: Understanding visibility, mobility and the phenetic fix. **Surveillance & Society**, let. 1, št. 1, s. 1–7.
26. Lyon, D. (2007). **Surveillance Studies: An Overview**. Cambridge, Malden: Polity Press.
27. Marx, G.T. (2008). Something's happening here and we are there. V: S. Leman-Langlois (ed.), **Technocrime. Technology, crime and social control**. Cullompton [England], Portland, Or.: Willan Publishing, s. vii–xix.
28. Mathiesen, T. (1997). The viewer society: Foucault's »Panopticon« revisited. **Theoretical Criminology**, let. 1, št. 2, s. 215–234.
29. McCulloch, J.; Pickering, S. (2009). Pre-Crime and Counter-Terrorism. Imagining Future Crime in the 'War on Terror'. **British Journal of Criminology**, let. 49, št. 5, s. 628–645.
30. Neyland, D. (2009). Mundane terror and the threat of everyday objects. V: K. Franko Aas, H. Oppen Gundhus, H. Mork Lomell (eds.), **Technologies of inSecurity: the surveillance of everyday life**. Abingdon, New York: Routledge-Cavendish, s. 21–41.
31. O'Harrow, R. (2005). **No place to Hide**. New York: Free Press.
32. Priest, D.; Arkin, W.M. (2010). Top Secret America. **Washington Post**, 21.7.2010. Po URL: http://projects.washingtonpost.com/top-secret-america/ articles/, dostop 1.8.2010.

33. Selinšek, L. (2008). Digitalna forenzika v kazenskih postopkih. V: L. Selinšek (ur.), **Digitalna forenzika v kazenskih postopkih**. Ljubljana: GV Založba, s. 13–64.
34. Solove, D.J. (2007). **The Future of Reputation: Gossip, Rumor, and Privacy on the Internet**. New Haven, London: Yale University Press. Po URL: http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/text.htm, dostop 1.7.2010.
35. Staples, W. G. (2000). **Everyday Surveillance. Vigilance and visibility in postmodern life**. Lanham: Rowman & Littlefield.
36. Statistični letopis 2006. Po URL: http://www.stat.si/letopis/LetopisPrva Stran.aspx, 30.6.2010, dostop 15.6.2010.
37. Statistični letopis 2009. Po URL: http://www.stat.si/letopis/LetopisPrva Stran.aspx, 30.6.2010, dostop 15.6.2010.
38. Stout, H. (2008). Technologies Help Adult Children Monitor Aging Parents. **The New York Times**, 28.7.2010. Po URL: http://www.nytimes.com /2010/07/29/garden/29parents.html?_r=3, dostop 2.8.2010.
39. Thomas, D.; Loader, B. (2000). Introduction – cyber crime: law enforcement, security and surveillance in the information age. V: D. Thomas, B. Loader (eds.), **Cyber crime: Law Enforcement, Security and Surveillance in the Information Age**. London: Routledge.
40. Turkle, S. (1995). **Life on the Screen: identity in the age of the Internet**. New York: Simon & Schuster.
41. Yar, M. (2009). Computer crime control as industry: virtual insecurity and the market for private policing. V: K. Aas Franko, H. Oppen Gundhus, H. Mork Lomell, eds., **Technologies of InSecurity: The surveillance of everyday life**. Abingdon, New York: Routledge-Cavendish, s. 189–204.
42. Wall, D.S. (1999). Cybercrimes: New wine, no bottles? V: P. Davies, P. Francis, V. Jupp (eds), **Invisible Crimes: Their Victims and their Regulation**, London: MacMillan, s. 105–139.
43. Wall, D.S. (2007). **Cybercrime: The Transformation of Crime in the Information Age**. Cambridge, Malden: Politiy Press.
44. Webster, F. (2003). Information Warfare, Surveillance and Human Rights. V: F. Webster, K. Ball (eds.), **The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age**, London: Pluto Press, s. 90–111.
45. Zedner, L. (2007). Pre-crime and post-criminology? **Theoretical Criminology**, let. 11, št. 2, s. 261–281.

# I. NOVE TEHNOLOGIJE V SISTEMIH DRUŽBENEGA NADZORSTVA

## 1 Nadzorstvene študije v kulturi bajtov: kaj je »novo« nadzorovanje?

**Aleš Završnik**

### Parabola o vsakodnevnosti tehničnega nadzora

Srečanja s tehnično okrepljenim nadzorom (angl. *surveillance*) so postala neizbežna. Nove oblike tehničnega nadzora segajo vse od oblik, ki so že povsem »naturalizirane« in del »normalnih«, »vsakodnevnih« rutin našega življenja (na primer videonadzor na avtocestah), preko »mejnih« oblik, ki se jim podvržemo le, če v zameno nekaj pridobimo (na primer soglašamo z zbiranjem naših osebnih podatkov za dodatni popust v trgovini), do oblik, ki (še vedno) »šokirajo našo zavest« (na primer varnostno preslikovanje tipa *body-screening* na letališču, ki nas malodane »sleče«). Na kakšne načine se kaže penetracija in naturalizacija tehničnega nadzora v vsakodnevne rutine našega življenja, je razvidno iz opisa nekega dne v življenju našega junaka Žana:

Žanu zjutraj zazvoni budilka v mobilnem telefonu. Izklopi nadležen zvok in nastavi priljubljeno radijsko postajo na sprejemniku, povezanem v optično omrežje novega ponudnika, ki mu ponuja še 200 TV programov, videoteko na »oddaljen način« in brezplačne pogovore znotraj fiksnega in domačega mobilnega omrežja. Ker bo v službo prišel prepozno, pokliče kolega, naj ga nikar ne čakajo in začnejo s sestankom. Svoj osnutek jim bo poslal čez pet minut po e-pošti. Preveri gretje radiatorja in zmanjša jakost, saj ves dan nikogar ne bo doma. Ker želi, da je toplo, ko se vrne domov, nastavi časovnik tako, da bo lahko reguliral gretje na daljavo. Po kopalniški rutini preveri prenosnik, ki je vso noč nalagal tri dokumentarne filme preteklega leta; najbrž nobenega izmed njih ne bo utegnil pogledati, a »za vsak slučaj«. Odpre elektronsko pošto, odpošlje osnutek in preveri nova sporočila. Zlasti ga zanima, kdaj bo dobava v spletni trgovini naročenega sesalnika. Zaenkrat je prejel le avtomatično generirano e-sporočilo, da se mu bodo posvetili v »najkrajšem možnem času«. Odhiti iz stanovanja.

Pred vhodom v blok stoji pismonoša in zvoni stanovalcem, ki pospremijo Žanov odhod prek domofona. Soseda mu prek zvočnika zapiska, naj se zvečer oglasi na sestanku nadzornega odbora skupnosti stanovalcev. »Aha....«, ji zagodrnja in hiti naprej. Razmišlja, ali naj se odpravi z avtomobilom ali z mestnim avtobusom: najbrž je kartica Urbana »prazna«, pomisli in izbere avto. Hitro je na avtocesti, pritisne na plin. Saj ve, da je pod videonadzorom, a ker je gneča, pospešuje, v predoru ga preseneti bliskavica. Tudi 10 km/h več je lahko preveč. Končno je pred službeno garažo, kjer z daljinskim

upravljavcem odpre vrata, ob tem pa po videosistemu pozdravi vratarja. Ob vhodu v dvigalo ga pospremi varnostna kamera, v veži nadstropja, kjer dela, pa z RFID kartico potrdi svoj prihod.

Zdaj si oddahne, ura tiktaka. »Spet bodo nadure, ponovno minus«, si zagodrnja. »Morda pa je kriva kartica in potrebujem novo«, išče izgovore. Tajnico zaprosi, naj preknjiži stanje na novo kartico. Pohiti v pisarno, vklopi računalnik, kjer se mu zažene prikaz nujnih opravil za tekoči delovni dan. Elektronska pošta se precej časa nalaga, ponovno bo nekaj ur porabil za odgovore. Ko po službenem telefonu opravi nekaj telefonskih pogovorov, pokliče ženo na zasebni mobilni telefon.

Po nekaj urah na delovnem mestu prične s popravljanjem osnutka za novo sejo. Iz skupnega strežnika pridobi starejša poročila sodelavcev, saj tam hranijo varnostne kopije. Panično pomisli, ali to, kar zdaj tipka na računalniku, kdo beleži in opazuje njegovo zmedo. Zdaj ve, da je oddaljen dostop do njegovega službenega računalnika mogoč, saj mu je administratorka na njegovo prošnjo sama naložila popravek programa SPSS, še ko je bila v tujini. »Gotovo ne«, si misli. A ve, da nadzor na delovnem mestu ne pozna meja, saj je bral o nadzoru japonskih bančnih uslužbenk, ki jim s pomočjo video tehnologije merijo izraz na obrazu tako, da jih računalnik opozori, če ne izražajo zadovoljive stopnje vedrine.

Med odmorom si ogleda stanje svojega spletnega nakupa. Iz trgovine mu javljajo, da njegovo plačilo ni bilo izvedeno, ker je vnesel napačne podatke o kreditni kartici. Javi, da bo plačal »po povzetju«. Preko spletne strani hotels.com poišče na digitalnem zemljevidu kongresni center srečanja v ZDA, ki se ga bo udeležil naslednji mesec, in v njegovi bližini izvede rezervacijo hotelske sobe. Zahtevajo številko kreditne kartice, zdaj je bolj previden pri vnosu številk. Na elektronski naslov, ki ga pusti ob rezervaciji, takoj prejme potrdilo o rezervaciji in dve ponudbi – za najem avtomobila in masažo. »Hitro so me našli!«, si misli. Zbere se in nadaljuje.

Po koncu službe Žan registrira svoj odhod z novo kartico. Stanje ur je občutno boljše, ne ve zakaj, a se ne sprašuje preveč. Odhiti v trgovino, kupi nekaj živil in peno za britje. Plača s kartico, v naglici odtipka napačno PIN kodo, in se poti, ko čakajoči bolščijo pod njegove prste. Ko odhaja iz trgovine, sproži alarm. Varnostniki ga povabijo v stransko sobo pri skladišču. Kmalu ugotovijo, da prodajalka iz škatle pene za britje ni odstranila RFID oznake. Opravičijo se ne, saj samo opravljajo svoje delo. »Saj razumete?!«, zasliši, ko nejevoljno odhaja. »Tako se ravna z »zvestimi« kupci?!«, mu švigne po glavi.

Na poti proti domu se ustavi še v lekarni, da bi dvignil zdravila za nosečo ženo. Ker nima njene zdravstvene kartice, zdravil ne dobi.

Proti večeru se z ženo odpravita na pregled nuhalne svetline njunega prihajajočega bitja: spol določen, verjetnost kromosomskih napak majhna. Osebje jima prijazno ponudi storitev shranjevanja matičnih celic, ker ta »rešujejo življenja«. Bosta razmislita. Zvečer preverja elektronsko pošto, brska po internetu o matičnih celicah in izpolnjuje obrazec na elektronskem sistemu za izdajo dovoljenj za potovanje za vstop v ZDA. Prebere, da bo moral pri vstopu dovoliti odvzem prstnih odtisov in pristati na fotografiranje. Informacije o tem, da ga bodo tudi posneli, ko bo govoril na mejni kontroli, ni nikjer...

Prigoda na več mestih, kot ste bralci opazili, odstira rutinski, (bolj ali manj) naturaliziran (junak ima dvome o nekaterih oblikah nadzora), intenziviran, avtomatiziran in

tehničen (digitaliziran) nadzor: (1) nadzor mobilnega telefona, ki ga je s triangulacijo mogoče locirati in pridobiti druge prometne podatke, ustvarjene pri njegovi uporabi; (2) nadzor nad preneseno vsebino v radio/TV sprejemnik; (3) izdelki »pametne hiše« (ogrevanje stanovanja) omogočajo povezavo in nadzor na daljavo; (4) računalnik, povezan na internet, omogoča sledljivost slehernega »klika miške« (kaj, kdaj, kako dolgo, od kje dostopa uporabnik do spletnih strani – obvezna hramba prometnih in lokacijskih podatkov, ter podatkov o naročnikih); (5) videonadzorovanje cestnega sveta, javnih prostorov in zasebnih premis (domofon, nadzor službenih prostorov in vožnje na avtocesti), omogočajo slikovno, zvočno snemanje, tudi obojestransko komunikacijo, lahko je opremljeno s sistemi za prepoznavanje obrazov ali za analizo vzorcev gibanja; (6) nadzor cestnega sveta vsebuje tudi sisteme za merjenje hitrosti vozil, pretočnosti prometa, protipožarne senzorje v predorih, sisteme za prepoznavanje registrskih tablic, vozila je mogoče locirati preko satelitske navigacije, sistemov elektronskega cestninjenja, sistemov za preprečevanje kraj vozil prek GSM omrežij; (7) nadzor na delovnem mestu: registriranje službene prisotnosti in gibanje po službenih prostorih je nadzorovano z RFID karticami, v službi je ponekod nadzorovano psihofizično stanje delavca (na primer alkoholiziranosti) ali celo nadzor z detektorji laži ali razpoloženja (emocionalno delo), GPS nadzorovanje delovnim sredstvom in spremljanje njihovega delovanja (na primer lociranje službenih vozil in načina njihove uporabe, na primer koliko voznik obrablja zavore), računalniški programi nadzirajo frekvenco tipkanja; (8) pri nakupih v spletnih trgovinah profilirajo nakupe uporabnikov, obiskovanje spletnih strani, (9) potrošniško nadzorovanje: »kartice zvestobe« v trgovini, elektronsko označevanje izdelkov z RFID čipi, ki omogočajo sledljivost izdelkov, njihovo evidenco in preprečevanje ponarejanja (t. i. »internet stvari«); (10) zdravstveni podatki, združeni v podatkovne zbirke, do katerih je mogoče dostopati s »pametnimi karticami«, omogočajo zdravstveno profiliranje »tveganosti« posameznika; (11) bančni podatki in finančne transakcije: mogoče jih je izvajati po elektronski poti, banke analizirajo finančne tokove, poročajo »sumljive« transakcije uradom za preprečevanje pranja denarja, podatki se lahko izmenjujejo med državami (na primer na podlagi sporazuma o izmenjavi bančnih podatkov evropskih državljanov v sistemu Swift z ZDA); (12) »pametne« ID kartice in dokumenti, ki jih imamo pri sebi, vsebujejo biometrične podatke (na primer prstni odtis, fotografijo obraza); (13) pri državnem (mejnem) nadzoru prihaja do kopičenja podatkov (na primer odvzemi prstnih odtisov, digitaliziranje fotografij obraza in posnetki glasu), izmenjave podatkov o letalskih potnikih, uporaba biometričnih podatkov za hitrejše prehajanje med varnostnimi točkami (na primer digitalizirane šarenice na letališču Amsterdam Schiphol, kjer naš lik prestopa na poti v ZDA); (14) na telo usmerjene tehnologije, kot na primer varnostno telesno preslikovanje (angl. *body-screening*) na letališčih, senzorji frekvence utripa srca (angl. *heartbeat machine*) in drugo kopičenje bioloških informacij o posamezniku (na primer matičnih celic, bank DNK itn.).

Parabola tudi kaže, da obstajajo številna mesta upora tehničnemu nadzoru, in da je tehnološko nadzorovanje lahko tudi povsem neuporabno. Sodoben tehnično okrepljen nadzor namreč pogosto ne dosega distopičnih (pogosto paranoidnih) scenarijev iz romanov kot sta Orwellov *1984* in Huxleyjev *Krasni novi svet*: kaj če bi Žanu RFID kartico za evidentiranje službene prisotnosti odčital njegov sodelavec ali če je tajnica v sistemu za beleženje prisotnosti naknadno popravila izračun prisotnih ur ob menjavi

kartice? Ali na primer, za slovenske razmere značilen primer, ko je računalniško evidenco o prometu izdanih računov, ki teoretično omogoča popoln davčni nadzor nad poslovanjem podjetja, mogoče nepooblaščeno spreminjati? Ali v primeru, ko videonadzorniki preprosto pozabijo vklopiti snemalnik, ali pa so videoposnetki dobri (za »razumnega človeka«), a sodišče oceni, da niso pravno zadosten dokaz o nekem dejstvu? Kaj pa, če je radar hitrosti v predoru zgolj prevara, če so varnostne kamere v dvigalu zgolj prazna očesa?

Ti primeri kažejo, da je tehnologija nadzora vedno umeščena v družbeno okolje. Tam je njena uporaba lahko povsem drugačna od prvotno zamišljene, njena učinkovitost je lahko velika, majhna, povsem izostane ali celo negativna, tj. z negativnimi eksternalijami, ko povzroča več družbene škode kot koristi. Družbeni (kulturni, pravni, etični) učinki IT so zato nekaj, kar je šele potrebno proučiti potem, ko so tehnologije nadzora že umeščene v družbeno-kulturni kontekst. Ker tehnologije spreminjajo kulturo, res pa je tudi obratno: kultura spreminja razumevanje, pomen in učinke v družbene procese in družbene institucije umeščenih tehnologij.

# Kulturni transformativni učinki IT: posredni vpliv IT na nadzorovanje

## Kult informacij

IT spreminja kulturo (in obratno) in družbeni podsistemi, vključno z mnogovrstnimi oblikami družbenega nadzora in sistemom kazenskega pravosodja, so neizogibno deležni kulturnih transformativnih učinkov IT.[1] Poglejmo, kako lahko IT spreminja kulturo?

Roszak[2] v študiji *Kult informacij* ugotavlja, da se je pomen informacij v sodobni tehnološki družbi bistveno povečal. Informacije so postale visoko cenjene, delo z njimi pa osrednjega pomena pri upravljanju družbe.

Arhivsko administrativno delo in druga podobna dela, povezana z informacijami, so bila v preteklosti nizko vrednotena. Bila so sicer potrebna, saj so zbiranje, shranjevanje in analiza informacij tudi v preteklosti predstavljali podlago za družbeno odločanje. Centri družbene moči (zgodnje države in imperiji) so se lahko oblikovali šele, ko so uspešno pobirali davke, monopolizirali sredstva fizičnega prisiljevanja in monopolizirali sredstva mobilnosti prebivalstva (sposobnost nadzirati populacijo, tj. odločati o tem, ali, kdaj in za koliko časa sme posameznik zapustiti določeno območje pod suverenostjo, kar danes poznamo v obliki potnih listov, zelenih kart in vizumskih režimov).[3] Vse tri funkcije suverena je bilo v zgodovini mogoče izvrševati z zbiranjem, shranjevanjem in analizo informacij: pobiranju davkov so služili popisi nepremičnega in premičnega premoženja (v preteklosti »glav živine« in pridelkov, danes osebnih dohodkov, nepremičnin itn.), monopolizaciji sredstev fizičnega prisiljevanja in mobilnosti pa je služilo označevanje oseb (pravni režimi imen in priimkov), registri prebivalcev, matične knjige o rojstvih, smrtih, statusnih spremembah, evidence o kaznovanosti ipd. Vse to je omogočalo nadzor nad populacijo in zagotovilo posameznikovo prispevanje skupnosti (suverenu), zagotavljalo konformno vedenje in naposled omogočilo tudi izločitev neposlušnih članov iz skupnosti.

Z nastankom države blaginje (angl. *welfare state*) v 19. stoletju pa v industrijsko razvitih delih sveta nastanejo številne nove administrativne naloge, ki povečajo pomen zbiranja, shranjevanja in analize podatkov. Namesto tradicionalne avtoritete (patriarha, fevdalca) v moderni državi nastopi pravna avtoriteta, povezana z delovanjem birokratskega aparata. Razvoj javne šole in izobraževalnega sistema, zdravstvenega sistema, socialnih zavarovanj in socialnih pomoči pa so zahtevali vedno več podatkov o posamezniku (identifikatorjev): evidence o šolskih ocenah, o pridobljeni izobrazbi, o dohodkih, o prejeti socialni pomoči, o zdravstvenem stanju, o odsotnostih z dela in iz

[1] Zavoljo jasnosti argumenta, da IT spreminja kulturo, ta pa načine razumevanja in soočanja s kriminaliteto, se na tem mestu ne spuščamo v vzajemno vplivanje akterjev družbenega nadzora, ki povratno tudi sami sooblikujejo in spreminjajo kulturo. Povezava je vzajemna, saj so akterji družbenega nadzora sestavni del »kulture« odziva na kriminaliteto in ne obstajajo zunaj družbeno-simbolne matrice.

[2] Roszak 1994.

[3] Torpey 2000.

šole, o službenih poteh, dohodkih, pridobljenih izven delovnega razmerja in drugih dohodkih so podlaga za odločitve birokratskega aparata. To zahteva precizne metode shranjevanja, arhiviranja in dokumentiranja, ki omogočajo enostaven priklic za kasnejšo uporabo, privedlo pa je v vedno bolj centralno vodenje zbirk podatkov, da bi se zagotovila večja učinkovitost in moč, ki bi segala preko vedno večjega razpona časa in prostora. Rastoč birokratski aparat države blaginje je tako deloval po objektiviziranih racionalnih pravilih. Max Weber je ob tem zgodnjemu nabrekanju birokratskega aparata ugotavljal, da zbiranje informacij v moderni državi postaja ne le sredstvo, temveč tudi cilj sam po sebi. Od tod strah pred birokratizacijo in tem, da se bodo raznovrstne življenjske izkušnje preoblikovale v številčne abstrakcije in odtujile ljudi. Od tod izvira tudi kritika instrumentalne racionalnosti, ki je nujni sestavni del birokratskega delovanja, a ki sama zase ne more zagotoviti »pravilnega« stanja stvari in »pravične« družbe.

Zbiranje, shranjevanje in analiza podatkov postane nujni del izpolnjevanja obljub države blaginje, njene implicitne zaveze, da je treba družbo čim bolj natančno razumeti – to pa je mogoče zgolj z detajlnim seciranjem vsakodnevnega življenja slehernika – in jo naposled ukrojiti po »naši podobi«.

Z razvojem IT se je pomen informacij povečal še v večji meri, kot je napovedoval Weber. Informacije so postale proizvod zase, s katerim se v informacijski »družbi znanja« trguje, in se jih pravno ščiti. Informacije so poseben kapital,[4] vrednost podjetij se v »družbi znanja« meri po njihovem »*know-how*« in ne v stvarnih produkcijskih faktorjih (strojih, zemljiščih). Informacije postanejo valuta,[5] s katero plačujemo za lastno komoditeto, ko na primer na letališču pustimo prstne odtise, da nam ne bi bilo potrebno čakati v vrsti, njihova uporaba je na koncu zaščitena tudi s kazenskim pravom.

Danes naj bi zato prešli od kulture atomov h kulturi bitov (Negroponte).[6] Za ta prehod so značilni konflikti med obema kulturama, kakršen je konflikt med zagovorniki in nasprotniki kriminalizacije kršitev pravic intelektualne lastnine: prvi ostajajo v (moderni) kulturi atomov, drugi pa v (postmoderni) kulturi bitov. Če smo v moderni kulturi tovorili snovi (atome), kar je bilo počasno, težko in okolju neprijazno početje, meni Negroponte,[7] danes potujejo računalniški podatki (biti). Včasih so bile kulturne (nematerialne) dobrine prav tako del sfere atomov, saj smo kulturo (njene proizvode) sporočali prek atomov: ideje, zgodbe, glasbo, filme smo prelili v/na fizične nosilce, na papir in v knjige, na kasete, vinil, CD, DVD plošče in druge nosilce podatkov. Tudi nematerialne (kulturne) dobrine je bilo potrebno pretovoriti, jih skladiščiti, pripeljati v drug kraj, razložiti... V knjižnicah si je bilo mogoče nematerialne dobrine skoraj brezplačno izposoditi, a vendarle je imel knjigo naenkrat v posesti zgolj en uporabnik knjižnice, preostali so morali počakati v vrsti.

V kulturi bitov tovorjenje snovi, da bi prenesli kulturne dobrine (znanje, glasbo, filme) ni več potrebno. Pošljemo jih lahko po digitalni poti z minimalnimi stroški neomejenemu številu naslovnikov, ne da bi z izdelavo »duplikatov« kvaliteta slabela. Digitalna knjižnica tehnično omogoča, da se njene zaloge prenašajo na daljavo. Obisk

[4] Roszak 1994: 8.

[5] Leman-Langlois 2008c.

[6] Negroponte 1996.

[7] Negroponte 1996.

njenih prostorov ni več potreben, gradiva si lahko izposodijo vsi uporabniki knjižnice hkrati.

Toda prehod iz kulture atomov v kulturo bitov še ni izpeljan. Pravno vrednotenje ostaja pretežno v kulturi atomov. Na primer, vrednotenje pretoka nematerialnih dobrin v pravu intelektualne lastnine se le počasi spreminja, kazenskopravno varovanje kršitev pravic intelektualne lastnine ostaja v kulturi atomov.[8] »Biti digitalen« ne pomeni, da se dejansko prenosi bitov vršijo hitreje (ali da se sploh vršijo) kot prenosi atomov. Zuckerman[9] tako prepričljivo ugotavlja, da danes uporabljamo ustekleničeno vodo (atome) s Fidžija, ne pa njihovih lokalnih časopisov po internetu (bite). Internetna infrastruktura sicer omogoča globalno omreženje, a so vsebine, ki jih dejansko spremljamo, homogene: ne beremo prosto dostopnih časopisov na internetu iz drugih kulturnih okolij ali tistih na drugi strani političnega spektra, temveč pregledujemo lokalno, ideološko in vrednostno nam bližje vsebine. Naš (idejni, kulturni, vrednostni) svet se zaradi tokov bitov ni oplemenitil z drugačnimi svetovi. Postal je še bolj homogen in zavrten vase. Glavnina bitov potuje le med ZDA in zahodno Evropo, preostali svet pa je v omrežju manj udeležen. Tok bitov je kvečjemu podoben toku atomov: najgostejši prenosi digitalnih podatkov se ujemajo z najgostejšim letalskim prometom. Spletna socialna omrežja, ki omogočajo ohranjati v stiku fizično ločene ljudi, zato ne pomenijo tudi zbliževanja različnosti (kultur, jezikov ali vrednostnih orientacij): skupine internetnih »prijateljev« so vedno interesno, vrednostno, razredno in še kako drugače homogene druščine.

## Računalniška »ontologija«

»Kult informacij«, ki hvali domnevno objektivne informacije, ki ležijo v neosebnih podatkovnih zbirkah in računalniških mrežah, je preko sprememb v kulturi prodrl tudi v načine razmišljanja o kriminaliteti in v mehanizme reagiranja nanjo. Podatkovne zbirke so postale središče delovanja pravnih odločevalcev in Garfinkel[10] govori o »nacijah podatkovnih zbirk« (angl. *database nation*). V delovanju kazenskopravnih sistemov se to kaže v spremembi paradigme policijskega dela, meni Lemieux.[11] Zbiranje, shranjevanje, analiziranje ter izmenjava podatkov in informacij o kaznivih dejanjih in storilcih, danes sicer ni nekaj povsem novega in ni značilnost zgolj sodobnega policijskega dela. A vendarle velike količine podatkov (v posamičnem kazenskem primeru tudi več terabajtov), podatkov, ki se nanašajo na številne vidike posameznikovega (trivialnega, vsakodnevnega) življenja, ki jih doslej (bodisi iz fizičnih bodisi iz ekonomskih razlogov) ni bilo mogoče sistematično beležiti in analizirati (na primer vzorce gibanja, potrošnje, denarnih tokov, komunikacije itn.), proizvodnja novih podatkov o posamezniku (ki se jih sam morda niti ne zaveda) z rudarjenjem in povezovanjem različnih podatkovnih

[8] Pravo intelektualne lastnine se dejansko postopno prilagaja, dober primer predstavlja sistem licenc *Creative Commons*, ki omogočajo intenziteto avtorskopravne zaščite *á la carte* glede na želje avtorja.

[9] Zuckerman 2010.

[10] Po Garfinkel 2001.

[11] Lemieux 2008.

zbirk, so danes nekaj povsem novega. Obveščevalno policijsko delovanje je zato po njegovem mnenju[12] pridobilo na pomenu in predstavlja prototip sodobnega policijskega dela. Vse oblike policijskega dela, vključno s policijskim patruljiranjem, naj bi pridobile tudi obveščevalne sestavine.

»Računalniško ontologijo« uteleša nova filozofija odzivanja na kriminaliteto, ki se odraža preko metod dela, kakršna je kartografiranje kriminalitete.[13] Aktuarski sistem COMPSTAT,[14] ki je v uporabi pri policijskem delu v ZDA in VB, ni »le« računalniški program, temveč »organizacijsko upravljavsko orodje, večplasten dinamičen pristop, ki zasleduje cilje, kot so zmanjševanje kriminalitete, povečevanje kvalitete življenja in upravljanje s človeškimi viri in materialnimi sredstvi«.[15] Njegove glavne naloge so policijsko-obveščevalne narave: določanje »kriminalitetnih žariščnih točk« (angl. *crime hotspots*), identifikacija incidentov po času, dnevu in lokaciji. Njegov cilj je odkriti v preteklosti neopažene vzorce kriminalnih dejavnosti. Program na elektronskem zemljevidu (tipa *Google maps*) prikaže vrste kaznivih dejanj, podatke o žrtvah, *modus operandi* storilcev, podatke o osumljenih v soseski ipd., kar korenito spreminja fokus policijskega dela.[16]

Spremembe v proizvodnji vednosti, ki jih je IT izzvala, so opazne tudi v načinu osmišljanja kriminalitete. Franko Aas[17] meni, da so orodja za oceno tveganj, podatkovne zbirke in algoritmi postali osnova védenja o zločinu in o kaznih. Ti vplivajo na konstrukcijo prestopnikove identitete in identitete tistih, ki odločajo. Računalniške podatkovne zbirke so kot diskurzi, lingvistične konfiguracije, ki konstituirajo posameznika. Avtorica zato meni, da je s tem, ko se je v kaznovalnem sistemu povečal pomen računalniških podatkovnih zbirk, tudi v penalno kulturo vstopila »računalniška ontologija«. Ontologijo pripovedi posameznika (na primer žrtve, osumljenca) vse bolj nadomešča ontologija podatkovne zbirke. V takšni kulturi niso več ključne policijske poizvedbe v lokalnem okolju, zaslišanja oseb z osebnim kontaktom, temveč analize podatkov v informacijskih sistemih, do katerih dostopajo policisti med patruljiranjem z omreženimi računalniki v vozilih. To spreminja postopke oblikovanja prestopnikove identitete, spreminja zgodbe o nasilju, bolečini, socialni deprivaciji in frustraciji. Te zgodbe, ki so predstavljene v novih »računalniških« parametrih, niso več enake zgodbe.

---

[12] Ob tem trendu, ko obveščevalno policijsko delo prodira v vse oblike policijskega dela, pa je značilen tudi pojav povsem novih policijskih enot: v VB *Forward Intelligence Teams* (FIT), katerih delo je zbirati podatke o posameznikih na javnih zborovanjih. To so uniformirani policisti, ki so »oboroženi« s kamerami in napravami za zvočno snemanje. Glavni očitek proti takšnim oblikam nadzora je, da omejuje svobodo združevanja in da »pred-inkriminira« protestnike, novinarje in fotografe. Ti sicer niso napravili nobenega prekrška, a so evidentirani in označeni kot »problematični«.

[13] Angl. *crime-mapping techniques*.

[14] Angl. *COMPuter STATistics* ali *COMParative STATistics*.

[15] Po Wikipedia, URL: http://en.wikipedia.org/wiki/CompStat, dostop 28.6.2010.

[16] Primer kartografiranja kriminalitete v Los Angelesu je dostopen na URL: http://www.lapdcrimemaps.org/, dostop 28.6.2010.

[17] Franko Aas 2005.

V naravi podatkovnih zbirk je, da vsebujejo zgoščene, nelinearne in nepovezane informacije. Tam ni (pri)povednosti z začetkom, sredino in zaključkom, ki bi bila racionalno argumentirana. »Zgodbo« uredi vsakokratni uporabnik podatkovne zbirke, ki poljubno uredi podatke. S tem pa prihaja do opuščanja »globinskega« razumevanja kriminalitete (etiologije), poudarjena je potreba po aktivnosti in delovanju.

Podobno se zaradi IT spreminja vloga sodnika v sistemih, kjer so v uporabi informatizirani sistemi odmere kazni (angl. *sentencing information systems*). Prvotna ideja informatizacije kaznovalnih tablic je bila legitimna, cilj je bil zagotoviti enotno sodno prakso pri izrekanju kazenskih sankcij in s tem zagotoviti enakost pred zakonom. A sodnikova vloga se je v teh sistemih popolnoma spremenila. Če je sojenje pred uvedbo informatiziranih smernic zahtevalo, da sodnik razume pripovedi udeleženih, in da sam oblikuje pripoved o spornem primeru, informacijske kaznovalne smernice že vsebujejo navodila o tem, kako kaznovati. Vsebujejo vednost o tem, koliko naj posamičen parameter primera prispeva k izrečeni kazni, in ne zahtevajo razmišljujočega in reflektirajočega sodnika. Prihaja torej do oblikovanja nove »moči brez pripovedi«.[18]

## Družba tehnopolisa

Računalniki in njihove mreže omogočajo nove metode spoznavanja sveta in generirajo novo razumevanje sveta, a vendar, ali to pomeni, da tehnologija stopa na mesto kulture?

Postman[19] o teh spremembah pesimistično meni, da načelo učinkovitosti, ki je generator razvoja IT, vodi do odmiranja kulture. Meni, da se »kultura umika tehnologiji«, ki stopa na njeno mesto. Sodoben odnos do tehnologije naj bi se namreč bistveno razlikoval od preteklih razmerij družbe do tehnoloških orodij: (1) »družbe uporabnice orodij« so tehnologijo uporabljale za dosego specifičnih namenov, a ves univerzum posameznika je ostajal osredotočen na religijo in družino, (2) v družbah »tehnokracije« je obstajala vera v napredek in izboljševanje posameznikovih sposobnosti, ki naj jih tehnologija krepi. Tehnologija je bila razumljena kot orodje, ki naj poveča posameznikovo zmožnost obvladovanja narave, cilj znanosti pa, kot je menil Bacon,[20] dvigniti človeštvo nad naravo; (3) v »tehnopolisu« pa tehnologija prevzame osrednjo vlogo. Učinkovitost postane (osrednja) vrednota, ljudje imajo preveč (in ne premalo) informacij, zlasti o trivialnih podrobnostih vsakdana drugih, tehnološko posredovane življenjske izkušnje pa postanejo bolj cenjene od neposrednih – na primer izkušnja posrednega (tehnološko posredovanega) »sprehajanja« po mestu v računalniški kopiji tipa *Google Maps Street View*, z vsemi ojačevalci čutil, možnostmi hipnega pridobivanja informacij o zgodovini kraja, njegovih posebnostih ipd., postane bolj razburljiva od resničnega (fizičnega) obiska mesta.

Ta pesimistični pogled na tehnopolis, kjer naj bi se kultura umaknila tehnologiji, pa spregleda dejstvo, da nam tehnologija zunaj kulture sploh ni dana. V kulturi nastajajo potrebe, želje, interesi, ki naj jim tehnologija streže in jih naslovi. Bolj kot teza o umiku kulture je zato prepričljiva teza o spremembi kulture (o transformativnih učinkih IT).

---

[18] Franko Aas 2005.

[19] Postman 1993.

[20] Bacon, 1996.

Tehnični sistemi lahko podpirajo instrumentalne vrednote, kot so funkcionalnost, učinkovitost, zanesljivost in priročnost za uporabo, kot trdi Postman, a lahko podpirajo tudi druge moralne in politične vrednote, ki so nam (morebiti) bliže.[21]

V študijah znanosti in tehnologije o tem, ali tehnologija sploh lahko vsebuje vrednote, obstajata dve teoriji. Teorija o nevtralnosti tehnologije trdi, da imajo tehnični proizvodi sicer lahko občutne učinke na družbeno in politično življenje in lahko dajejo prednost določenim družbenim, moralnim ali političnim vrednotam pred drugimi.[22] A zanika, da bi bili ti učinki značilnost samega tehničnega sistema. To so posledice rabe tehnologij. Tehnologije pojmuje zgolj kot orodja za dosego človeškega namena: moralnost in politika ležita v ljudeh in ne v njihovih orodjih.

Druga teorija pa trdi,[23] da so tehnični proizvodi lahko neposredni nosilci vrednot in lahko sistematično prispevajo k realizaciji ali onemogočanju družbenih, etičnih in političnih vrednot. Zavzema se za to, da bi snovalci tehnologij imeli jasno izraženo dolžnost, da pri zasnovi tehnoloških predmetov vključujejo vrednote, kot so svoboda, avtonomija, sožitje in varnost, ker tehnološki sistemi implicitno krepijo določene vrednote. Ključna je ugotovitev, da tehnološki artefakti utelešajo vrednote in da ima tehnična zasnova tudi vrednostno dimenzijo. Vprašanje danes zato ni, ali je tehnologija že stopila na mesto, ki pripada kulturi, temveč v kakšni kulturi živimo, da daje prednost vrednotam učinkovitosti pred drugimi bolj družbeno inkluzivnimi vrednotami.

Računalniki predstavljajo novo razvojno fazo v razvoju kulture, ki se je ločila od »resničnega«, in proizvedla alternativo in ne kopijo resničnega. Ključno je zato računalnike misliti kot kulturne proizvode, ki nam pomagajo na nov način razumeti nas same, sodobne družbene razmere, odnose in institucije. Računalniki so (lahko) močna metafora, kako razumeti sodobni svet. Če je ta, od Loytardovega spisa iz leta 1979 dalje,[24] označen kot postmoderen, so računalniki metafora, meni Turkle,[25] ki nam pomaga razumeti postmodernistične teorije (teorije Lacana, Derridaja, Deleuza, Guattarija). Računalniki in njihove decentralizirane mreže tudi rušijo doslejšnje hierarhije moči, državne meje in piramidalno urejenost sveta (nacionalnih držav in njihovih srečanj v OZN). Predstavljajo (paradigmatične) predmete sodobnega časa: če smo »težko moderno«[26] mislili preko predmetov, kot je tekoči trak, in govorili o »fordistični« družbi (množične kulture, *en mass* proizvodnje in drugih nasledkov te tehnologije – organizacije življenja v »fabriki« in monogamni družini), je »postmoderno« potrebno misliti preko računalnikov in njihovih mrež. Na kakšen način?

[21] Flanagan, Howe, Nissenbaum 2008.

[22] Flanagan, Howe, Nissenbaum 2008: 347

[23] Glej še MacKenzie, Wajcman 1985.

[24] Lyotard 1984.

[25] Po Turkle 1995.

[26] Bauman 2002.

## Računalnik kot metafora postmodernizma

Postmodernistični odnos do sveta, navdahnjen z računalniki, se odraža v prvi vrsti v našem razumevanju človeka kot biološkega bitja. Možgani so v sodobni (nevro)znanosti razumljeni kot organ za »procesiranje« informacij, kot osrednji »računalnik« z nevroni (sestavnimi deli), ki se povezujejo v »mreže«, med njimi pa z učenjem prihaja do »premreženja« (vzpostavljanja novih povezav). Te konceptualizacije človeka kot »biološkega stroja« zrcalijo infrastrukturo interneta. Tudi ta je decentraliziran sistem, ki povezuje računalnike v mreže, med katerimi podatkovni paketki potujejo po različnih poteh, kar računalnike vedno znova »premreži« na unikaten način. Računalniško prebiranje genov v sodobni genetiki ima prav tako za cilj učinkovito zdraviti z »reprogramiranjem« genskega materiala. Človeško bitje je dojeto kot (pred)programiran človek-stroj. Računalniški dualizem strojne in programske opreme (angl. *hardware* in *software*) se prenaša na človeka tudi s ponazarjanjem razlike med možgani in duhom (angl. *brain* in *mind*).

Računalniki na opisane načine sprožajo nove reprezentacije življenja, novo razumevanje posameznika, služijo nam kot zrcala in spreminjajo načine, kako razmišljamo o sebi, o drugih in o družbi. Turkle[27] zato prepričljivo meni, da so računalniki »paradigmatski postmodernistični predmeti«, ki utelešajo novo postmoderno teorijo in jo postavljajo na »realna tla«. Poglejmo, kako in kakšen »ontološki« pomen je računalnik imel skozi kratko, a bliskovito zgodovino.

»Ontologija« računalnikov v družbi ni bila vedno enaka. V 60. letih prejšnjega stoletja, v času »trde« moderne, so bili računalniki razumljeni kot računske naprave. Prvi računalniki so bili sicer občutno večji od običajnega kalkulatorja, a po svoji osnovni funkciji so bili razumljeni kot računski stroji. V tej »modernistični računalniški estetiki« (Turkle) je bilo programiranje pojmovano kot linearna računalniška dejavnost, kot nekaj, kar je mogoče narediti prav ali narobe, *tertium non datur*. Ta »prav« je določalo notranje računsko bistvo računalnika in predstavljalo tudi vodilo za razmišljanje o ekonomiji, psihologiji in družbi. Računske ideje so bile v »trdi« moderni predstavljene kot ena izmed velikih modernih meta-pripovedi, zgodb o tem, kako svet deluje. Če ga želimo razumeti, ga je potrebno razstaviti na manjše in bolj enostavne sestavne dele in jih nato natančno analizirati.

Kasnejša usmeritev v programiranju se je preusmerila od linearnega programiranja (na primer v operacijskih sistemih tipa DOS) k simulaciji, navigaciji in interakciji. Novo »računalniško estetiko« bolje opisujejo postmodernistične teorije. Računalniki od uporabnika ne zahtevajo več poznavanja tehnične plati delovanja računalnika in dvojiškega računalniškega jezika. Uporabniška raven je danes postala raven aplikacij in vmesnikov (kot so na primer operacijski sistemi *MS Windows*, *Mac OS X* ali *Linux*), kjer lahko na namizju opazujemo ikone, kot so »koš«, »moji dokumenti« in druge poljubno ustvarjene »mape«. Seveda vemo, da »koš« v resnici ni koš in niti ni kopija pravega koša, ampak zgolj simulacija, ki ne obstaja v resničnosti. A za našo uporabo zadostuje osredotočenost »na površino« (na »mape« na namizju), na simulacijo, ki jo uporabnik aktivno sooblikuje. V računalnikih seveda še vedno obstaja raven bitov in bajtov, potujočih elektronov, brez katerih računalnik ne bi obstajal. A sprememba, ki

[27] Turkle 1995: 18.

smo ji priča, se nanaša na osredotočenost programiranja in raven uporabe, kjer znanje o bitih in bajtih ni potrebno. Od »modernistične kulture kalkulacije« smo prešli v »postmodernistično kulturo simulacije«.[28]

Sprememba iz kulture kalkulacije v kulturo simulacije je hkrati osrednja tema postmodernizma, ki trdi, da živimo v družbi simulakra in da označevalec predhodi označencu. Ta premik ne zadeva samo računalnikov, temveč tudi medosebne odnose, naše samorazumevanje, razumevanje družbe, vključno z vlogo, namenom in smislom delovanja kazenskopravnih sistemov in kriminalitetnopolitičnih usmeritev. Značilnost te »paradigme« je, da vzroki kriminalitete, ki ležijo skriti »zadaj« za kaznivim dejanjem, in ki so bili v preteklosti razumljeni kot njegov simptom, niso več v ospredju kaznovalne oblasti. To zanima, kako upravljati in voditi sisteme »na površini«, kako upravljati z odklonsko populacijo, zanima jo učinkovitost, ki jo je mogoče neposredno meriti, performans, ki daje takojšnje in merljive rezultate, kar vedno pogosteje vodi v »javno-zasebna« partnerstva ali kar v privatizacijo državnih (pravosodnih) nalog. Franko Aas[29] identificira takšne premike v pravnih sistemih, kjer poznajo računalniške programe za izbiro in odmero kazenskih sankcij, in jih imenuje odmera kazni »na površini« (angl. »s*entencing-at-a-distance*«). Ta ponazarja premik od individualiziranega k »tarifnemu« kaznovanju, kjer je namesto presoje sodnika ključen računalniški program. Ta specifična tehnologija pa je le paradigmatični primer tega, da danes izkušnje življenja in kulture pridobivamo na veliko večji razdalji kot kdajkoli poprej, da delujemo na razdaljo (angl. *action-at-a-distance*, Rose in Miller) in živimo »kulturo z razdalje« (angl. *culture-at-a-distance*, Lash).

IT spreminja kulturo in s tem posredno spreminja mehanizme družbenega nadzorovanja. Oblike neformalnega in formalnega družbenega nadzora pa spreminja tudi bolj neposredno in te spremembe so predmet nove renesanse nadzorstvenih študij.

[28] Turkle 1995.

[29] Franko Aas 2005.

# Študije »novega« nadzorovanja: neposredna uporaba IT v nadzorovanju

### IT v neformalnih in formalnih oblikah družbenega nadzorovanja

Neformalne oblike družbenega nadzora spreminja IT na več načinov. Tehnični pripomočki nadzora so dostopni tudi državljanom, ki danes lahko vohunijo drug za drugim in z lastnim zalezovanjem tudi kršijo človekove pravice drugih, a tudi tako, da vohunijo za državo in ji gledajo pod prste. Nova tehnična oprema (kot so cenovno dostopne kamere, mikrofoni, mobilni telefoni) in novi prostori (internet) so spremenili enopomensko definicijo nadzorovanja – vsakdo lahko malodane povsod in v vsakem trenutku snema ali kako drugače nadzoruje drugega. To amatersko nadzorovanje zato kaže, kot meni Koskela,[30] da so tehnično okrepljen nadzor »ugrabili« državljani. Amatersko nadzorovanje omogoča kritično rabo, na primer snemanje policijskega ali vojaškega nasilja, ki bi sicer ostalo javnosti skrito, kot je bilo mučenje zaprtih »sovražnih bojevnikov« v zaporu Abu Ghraib v Bagdadu, ko je fotografija vojakinje Lynndie England z golim zapornikom na povodcu obkrožila svet, ali na primer povratnega snemanja policijskega dela kot odgovor na nove policijske enote, ki so opremljene s snemalnimi napravami kot so v VB *Forward Intelligence Teams*.[31]

Tehnologije nadzora spreminjajo neformalne oblike družbenega nadzora, ker vsebujejo možnost, da jih uporabimo kot sredstvo nasprotnega vohunjenja, gledanja pod prste tistim, ki naj bi nas nadzorovali (angl. »*counter-surveillance*«).[32] Bistvo tiranije, kakršno ponazarja Orwellov Veliki brat, je v tem, da tisti »zgoraj« (nadzorniki) gledajo in pri tem niso vidni, s čimer se lahko izognejo odgovornosti za svoje početje. Prav demokratizacija in dostopnost tehnologij pa omogočata, da so skupine z družbeno močjo pod večjim nadzorom in pritiskom javnosti in da upoštevajo pravila strokovnosti, saj jih lahko v nasprotnem primeru državljani tudi pokličejo na odgovornost in jim na koncu (po pravni poti ali z revolucionarnim nasiljem) odvzamejo moč. IT zato ni vnaprej slaba in naperjena zoper posameznika. Pod pogled postavlja tudi tiste, ki so bili doslej skriti. Gibanje »vseprisotnega pogleda« (fr. »*sousveillance*«) Steva Manna[33] se zavzema ravno za to, da bi državljani prevzeli nalogo gledanja »od spodaj« in s tem potrjevanja, da so suvereni sami, in ne brezupniki, ki jim vladajo drugi.

Formalne oblike družbenega nadzora, med katerimi osrednjo mesto zavzema kazenskopravni sistem, se bolj neposredno spreminjajo z vnosom konkretnih informacijsko-tehničnih proizvodov v mehanizme izvajanja oblasti. Vplivi IT se kažejo po celotnem spektru formalnega družbenega nadzorstva: v prevencijskih programih in ukrepih,

---

[30] Koskela 2009.

[31] *FITwatch* iniciativa združuje ljudi, ki opazujejo, snemajo in dokumentirajo policijsko nadzorovanje pri demonstracijah in opozarjajo na sporne policijske nadzorstvene prakse, ki temeljijo na »kategoričnem sumu«, njihov cilj pa je zagotoviti anonimnost in zasebnost tistih, ki na legitimen način izražajo svoje politično nestrinjanje. Glej Swain, Apple 2009.

[32] Brin 2009.

[33] Mann 2002.

čemur služijo tehnologije, kot so nadzorne kamere, hramba prometnih podatkov v javnih telekomunikacijskih omrežjih, nadzor nad potniki z *body-scannerji* ipd.; v postopkih odkrivanja kaznivih dejanj in pregona storilcev;[34] v pravosodni upravi (na primer koncept e-pravosodja zaokroža poskuse obvladovanja pripada zadev na sodišča in avtomatizacije organizacijsko-tehničnih zadev z videokonferenčnimi zaslišanji oseb, vključuje sisteme elektronskih sodnih spisov, elektronskega vročanja in podobnih oblik informatizacije notranjega poslovanja sodišč); v izvedbi dokaznih postopkov, v vodenju glavnih obravnav in opravi posamičnih procesnih dejanj (z novimi vrstami dokazov, kot so vedno pogostejši DNK dokazi, virtualnimi animacijami ali dokazi »nedolžnosti« z nevrološkimi preslikovanji možganov s fMRI tehnikami) ter v novih oblik kazenskih sankcij, kot je na primer elektronsko (GPS) sledenje.[35] Analiza vseh teh sprememb presega namen tega prispevka, a te spremembe so implicitno vključene v temeljne premike družbenega nadzorstva, ki so privedli do renesanse nadzorstvenih študij, osredotočenih na »novo« tehnično okrepljeno nadzorovanje.

## Kaj so »nove« nadzorstvene študije?

Sodobne nadzorstvene študije so eklektična, multidisciplinarna in »mednarodna« znanstvena disciplina, ki se osredotoča na pojav povečanega zbiranja, shranjevanja, posredovanja, preverjanja in uporabljanja osebnih podatkov kot sredstva vplivanja in upravljanja s posamezniki in populacijami. Ti postopki lahko obsegajo fizično opazovanje, a danes vedno pogosteje tudi druge oblike avtomatiziranega (računalniškega) evidentiranja, ki niso le vizualne narave. Obsegajo primere, ko posameznik ni ničesar osumljen in bi bil to razlog nanj osredotočenega nadzora, temveč postane objekt nadzora zgolj zato, ker je v tranzitu ali se nahaja na določenem kraju ali v kontekstu.[36] Namesto posebej sumljivih posameznikov se »nov« nadzor izvaja nad vzorci populacije, posebnimi kategorijami vedenja, ki same po sebi niso kaznive. Zato ni nujno, da se opazujejo detajli opazovane enote, lahko se nadzoruje tokove enot. Postopki »novega« nadzora danes doživljajo renesanso preučevanja zato, ker se povezujejo z ideologijo, teorijo in prakso zagotavljanja varnosti v družbi, in ker s selektivnim nadzorom in močjo kategorizacije (t. i. teza o nadzoru kot obliki »družbenega sortiranja«)[37] vplivajo na neenakost (predvsem njeno povečevanje) v družbi.

Označba *nadzorstvene* študije je glede na značilnosti in dimenzije »novega« nadzora nenatančna. Opisno jih bolj natančno opredeljujemo kot študije, ki se osredotočajo na tehnično (p)o(d)krepljen nadzor. V angleščini ločnico ponazarja razlika med *surveillance* in *control*, ki ju v slovenski jezik prevajamo z nadzor(ovanje). A tudi to

[34] *Twitter* in *Facebook* sta že postala ključna vira policije za pridobivanje informacij o prestopnikih v »realnem času«. Po Hooper 2009.

[35] James 1979.

[36] Lyon 2002.

[37] Lyon 2003.

razlikovanje ne obsega vseh novih dimenzij nadzora.[38] Marx[39] opozarja, da *Oxford Dictionary* pojem *surveillance* opredeljuje takole: »To je opazovanje, še posebej sumljivih ljudi«. A sodobno nadzorovanje obsega v manjši meri (finančno in personalno potratno) vizualno opazovanje. Vidljivost (tj. opazovanje) je sicer res osrednja težnja sodobnih oblik nadzora in (tudi zato) postajamo »civilizacija pogleda« (Wajcman),[40] ki si domišlja, da je vse bivajoče mogoče postaviti na ogled – česar ne vidimo, kot da ne obstaja. A vidljivost je le metafora vednosti in ne opisni pojem sodobnih oblik nadzora. Poleg tehnologij, ki povečujejo »vidljivost« objektov nadzora, obstajajo tehnologije nadzora, ki se zanašajo na nevizualne oblike beleženja, kot so avditivno (sluh), olfaktorno (vonj) in taktilno (dotik) nadzorovanje. Dodatna značilnost »novega« nadzora je dimenzija preračunavanja, povezovanja in vzorčenja podatkov. Nadzoruje, meri in beleži se kontekste: prostore, specifična obdobja, mreže in sisteme.[41]

Sodobno nadzorovanje se nanaša na posameznike, kot že omenjeno, ki niso prav ničesar osumljeni. Opazovani so zato, ker so del nadzorovane množice, del nadzorovanega prostora (na primer nadzor gibanja potnikov na letališču), uporabljajo določeno tehnologijo (na primer internet) ali so v toku (na primer ljudi, ki so v toku prek državnih meja, pa tudi podob in sporočil, ki so v toku preko telefonov, interneta). Cilj »novega« nadzora je nadzirati kategorije oseb, predmetov, prostorov in tokov. Te spremembe v (predpostavljenem ali domnevanem) sumu zato Marx[42] poimenuje kot prevlado »kategoričnega suma«. Temeljno načelo pri uporabi sodobnih nadzornih tehnologij namreč ni načelo nedolžnosti, temveč krivde: vsakdo je domnevno kriv, dokler ga nadzorni sistem ne preveri in izloči.

Pri sodobnem nadzoru ne gre le za opazovanje drugih, temveč tudi (ali še vedno) za samoopazovanje in samonadzor (v smislu »foucaultovskih« disciplin in v smislu tehničnega nadzora telesa, kot so na primer testi alkoholiziranosti, nameščeni v vozilih). Sodobno nadzorovanje tudi ne predpostavlja fizične bližine, kot to zahtevajo starejše oblike optičnega opazovanja, lahko se izvaja na daljavo (na primer preko satelitskega sistema).

Temeljni učinek »novega« nadzora je, da postavlja dnevno življenje sodobnika pod konstantni nadzor (časovna neomejenost),[43] ki poteka preko novih tehnologij. Nadzor ni več le specifičen (nanašajoč se na določljivo osebo) in ni namenjen le specifičnemu namenu, temveč je rutinski (načini zbiranja osebnih podatkov so rutinizirani kot

---

[38] Dodaten zaplet pri razlikovanju v angleškem jeziku je tudi ta, da je kardinalno delo Foucaulta *Nadzorovanje in kaznovanje* iz *Surveiller et punir*, sicer po posvetovanju s Foucaultom, prevedeno v angleški jezik kot *Control and punishment* (in ne *Surveillance and Punishment*). Poleg tega je njegova knjiga posvečena tudi tretjem pojmu – disciplinam (in disciplinski družbi). Glej Jones 2005.

[39] Po Marx 2002.

[40] Wajcman 2010.

[41] Marx 2002.

[42] Marx 1988.

[43] Lyon 2002: 2.

»normalen« del življenja)[44] in sistematičen (ne le spontan ali občasen). Usmerjanje pozornosti na osebne podatke se izvaja za namen vplivanja, upravljanja, zaščite ali usmerjanja ljudi. Lahko je osebno ali posredovano z informacijsko tehnologijo in praviloma vključuje razmerja moči (v katerih so nadzorniki privilegirani pred nadziranimi).[45]

Te značilnosti »novega« nadzora sodobne nadzorstvene študije opazujejo multidisciplinarno,[46] tako da združujejo epistemološke reze in pojme več tradicionalno ločenih disciplin. So pa tudi »čez-disciplinske« (angl. *cross-disciplinary*) narave,[47] ker ustvarjajo novo raziskovalno polje, ki »preči« obstoječe konceptualizacije. Združujejo raziskovalce sociologije, politologije, študij znanosti in tehnologije, kriminologije, antropologije, komunikologije, (sociologije) prava, pa tudi zgodovine, filozofije in socialne psihologije, naravoslovnih ved (posebej računalništva in informatike) ter drugih specifičnih študij (porabništva, družbenih gibanj, globalizacije in dela). Osrednja raziskovalna vprašanja sodobnih nadzorstvenih študij so: kje je mogoče najti nove oblike nadzorovanja, kako (v kakšnem smislu in ali sploh) je informacijska tehnologija intenzivirala nadzorovanje, zakaj ga je intenzivirala, kakšne so posledice ali implikacije vedno bolj skrupuloznega »pogleda« (pa tudi zvočnega, termičnega in še kakšnega »bolščanja« in povečevanja vednosti o posamezniku), kdaj je nadzorovanje legitimno (kot del skrbi za sočloveka), kdaj pa prerašča v oblastno izkazovanje (pre)moči, ter tudi vprašanja upora: kakšne so oblike upora, onemogočanja ali subvertiranja (izkrivljanja) nadzornih mehanizmov, ki so v »teoriji« razumljeni kot vsemogočni »orwellovski« Veliki brat, a se v »praksi« izjalovijo, izkažejo za povsem neuporabne, potratne in zavajajoče?

## Nadzor v moderni

Nadzor (angl. *surveillance*) je star, kot je stara družba. A v moderni je po Giddensu[48] nadzor postal osrednjega pomena. Opazovanje, beleženje in popisovanje pojavov (vseh vrst), njihovo označevanje in kategoriziranje ter analiziranje s ciljem vplivati na prihodnjo dinamiko opazovanega »pojava«, je temeljna značilnost moderne. Te vrste nadzor je bil konstitutiven za nastanek moderne države, ki je ravno s pomočjo (moderne) znanosti, ki se je zavezala racionalnemu (strukturiranemu, vrednostno nepristranskemu, objektivnemu) »pogledu«, uspela obvladati in vzpostaviti nove mehanizme izvajanja oblasti nad drugimi deli narave in »Drugimi« družbenimi skupinami (bodisi s kolonializmom tujih dežel bodisi z vrednostnim imperializmom kot kolonializmom »z drugimi sredstvi«). Nadzor kot akumulacija informacij z neposredno supervizijo družbenega življenja je zato po Giddensu nekaj, kar nasploh konstituira moderno kot civilizacijsko-kulturni fenomen.

---

[44] Lyon 2007: 7.

[45] Lyon 2007: 13–16.

[46] Po Goold 2009.

[47] Po Lyon 2002.

[48] Giddens 1985: 13.

Zato ni presenetljivo, da so se z nadzorom ukvarjali in ga reflektirali vsi klasiki sociološke misli. Karl Marx je opozoril na moderne discipline kapitalistične supervizije, na nadzor delavcev, ločitev mentalnih in ročnih opravil (delitev dela), kar je omogočilo podrejanje dela kapitalu. Max Weber je opozoril na vojaško-birokratsko nadzorovanje z beleženjem in hrambo podatkov v dosjejih. Vojaška organizacija in militarizacija je omogočila nastanek moderne države, novi način delovanja vojske (hierarhija položajev in odgovornosti, racionalizacija, delitev dela, način odrejanja nalog) pa se je prenesel iz vojske v civilno birokratsko organizacijo. Ta je za svoje delovanje intenzivirala postopke monitoringa, popisovanja in kategoriziranja. Emil Durkheim pa je opozoril na trend intenziviranega nadzora, ki ga zaradi vse večje socialne razslojenosti in družbene neenakosti, ki generira kriminaliteto, izvajajo vladajoči s povečanim nadzorom marginaliziranih in prikrajšanih posameznikov in skupin.

Današnja renesansa v preučevanju »novega« nadzora gradi na teh spoznanjih. Marxova teorija služi analizam nadzora delavcev, Durkheimova analiza je aktualna pri analizi policijskega nadzora in nadzora v zvezi z delovanjem akterjev kazenskopravnega sistema, Webrova pa v analizah vojaškega nadzora, ki je sploh omogočil nastanek nacionalnih držav in birokratske (upravne) administracije.[49] A vendarle, zakaj klasične sociološke misli niso zadostne pri analizah vseh sodobnih dimenzij nadzora?

## »Novi« nadzor v postmoderni

Moderne teorije nadzorovanja, ki jim pripadajo Marx, Weber in Durkheim, se ločijo od postmodernih po tem, da razumejo nadzorovanje kot izraz kapitalističnega podjetništva, birokratske organizacije, nacionalne države, težke industrijske »mehanizacije« in razvoja nove vrste solidarnosti, ki vključuje manj »zaupanja« ali vsaj drugačne vrste zaupanja med ljudmi v moderni »družbi tujcev« (Simmel).[50] Torej, kjer nadzorovanje (angl. *surveillance*) postane nadomestek za različne oblike (predmodernih) zaupnih razmerij. Postmoderne teorije nadzorovanja se nasprotno ukvarjajo z novimi oblikami vidljivosti in oprezanja za nevarnostmi (tveganji) in poudarjajo, da so temeljne značilnosti sodobnega nadzorovanja (1) tehnološka omogočenost, (2) usmerjenost na telo, (3) vsakodnevnost in (4) univerzalnost.[51]

### Tehnična okrepitev nadzora

Nove teorije nadzorovanja v ospredje postavljajo (digitalno) informacijsko tehnologijo (IT). IT postopke »gledanja« (v dobesednem pomenu in v pomenu pridobivanja nove vednosti) podvrže avtomatizaciji. Deluje tako, da raznovrstne »bitnosti« (od predmetov, ljudi in naravnih pojavov, biološko-kemične sestave živih bitij do simbolne komunikacije in vzorcev fizičnega gibanja navedenih »entitet«) pretvori v digitalni jezik. Telesa, biološki in družbeni procesi, komunikacija, dražljaji vseh vrst in tudi naravni pojavi

[49] Dandeker 1990.

[50] Simmel 1950.

[51] Lyon 2007: 51, 55.

izven dosega človeškega senzoričnega aparata (na primer frekvence elektromagnetnega valovanja, ki jih s »prostim očesom« ne zaznamo), postanejo digitalni podatki. Ta digitalizacija postavi opazovane »bitnosti« na skupni imenovalec dvojiškega jezika, s tem pa omogoča objektivizacijo in analizo podatkov.

Za izvajanje družbenega nadzora je pri tem pomembnih več pojavov, najpogosteje analizirani pa je družbeni vpliv oblikovanja »digitalnih dvojnikov«,[52] digitalnega sebstva oziroma digitalnih identitet, ki imajo odločilno vlogo pri družbenem odločanju o pravicah in obveznostih posameznika in pri njegovem nastopanju v pravnem prometu. Ti dvojniki so izredno trdoživi in posameznik jih lahko le stežka ovrže v dolgotrajnih postopkih preverjanja istovetnosti. Za razliko od osebe, »digitalni dvojnik nikoli ne laže«.[53] Zato je v družbenem nadzoru podatek, ki so ga nadzorniki pridobili na primer iz vizumskega informacijskega sistema, pomembnejši od osebne izpovedi imigranta, ki trdi drugače, kot o njem »govori« podatkovna zbirka: da je že zaprosil za azil in da se mora na meji obrniti. Podatki, nakopičeni v podatkovnih zbirkah, imajo veliko moč pri družbenem odločanju in zbirke nastopajo kot samostojni »diskurzi«.[54]

## Na telo usmerjeni nadzor

»Novo« nadzorovanje je usmerjeno na telo, kjer naj bi se skrivala (vsa oziroma za oblastno odločanje relevantna) resnica o posamezniku. Telo je v procesu digitalne pretvorbe izvrženo iz družbenega konteksta in je objektivizirano. Na primer, tehnologije, kot so detektorji laži (uporabljani pri preiskovanju kaznivih dejanj in pri nadzoru zaposlenih na delovnem mestu), naprave za varnostno preslikovanje teles na letališčih ali za termično opazovanje potnikov za morebitno preveliko telesno aktivnost, ki naj bi odražala skrb zbujajoče (kriminogeno) psihološko stanje, tehnike preslikovanja možganov, ki naj bi pripomogle k odkrivanju krivde v kazenskih postopkih ipd. naprave, so usmerjene na telesa in ne omogočajo upoštevanja (vsebine) osebnih izpovedi ali družbenega konteksta. Zato dekontekstualizirajo (na primer detektorji laži ne zaznajo stresne situacije oziroma okoljskih spremenljivk) in objektivizirajo telesa.

Vidljivost telesa se tudi nepretrgoma povečuje: vidimo lahko pod obleko (na primer pri letališkem *body-screeningu*), pod kožo (na primer s tehnikami preslikovanja možganov), merimo lahko kemične procese (na primer preko elektronske zapestnice na daljavo ugotavljamo električno prevodnost kože pogojno odpuščenega obsojenca in njegovo morebitno alkoholiziranost). V nekaterih kontekstih je vidljivost teles konstantna (na primer pri videonadzorovanju javnih površin). Telo je vir zelo uporabnih podatkov za številne subjekte nadzora: za zunanje agente (državo, korporacije) in tudi za sam subjekt – prakse konstantnega nadzora telesne teže, maščob, krvnega tlaka, holesterola in drugih snovi so nekaj povsem novega v dobi nadzora, usmerjenega na telo, ko je telo potrebno gnesti v kulturno sprejemljive »skulpture-stroje«.

[52] Poster 1996.

[53] Franko Aas 2005.

[54] Poster 1996.

## Vsakodnevnost nadzora

Vsakodnevnost »novega« nadzora se nanaša na dejstvo, da je nadzor postal »normalen« del življenja slehernika in da ne prihaja več do osredotočanja na posameznika le v specifičnih primerih (na primer zaradi interesov kazenskega postopka ali zagotavljanja delovne discipline). Nadzorovane kategorije se oblikujejo tudi glede na geodemografske stile, psihološke razlike, izobrazbene in zdravstvene razlike. Nadzor se razteza tudi v čas pred rojstvom posameznika. Tako se (pro)natalisti zavzemajo za prenatalno zdravje (nosečnic) pa tudi »zdrav« življenjski slog potencialnih (bodočih) staršev, kjer je potrebno nadzorovati prehrano, gibanje ipd.

»Vsakodnevnost« novega nadzora se odraža v udomačitvi (naturalizaciji) omenjenih posamičnih oblik nadzora. Videonadzorovanje otrok z video varuškami (*nanny cams*) ali s senzorji za zaznavanje premikanja in dihanja je postalo del ideologije starševske skrbi za otrokovo dobrobit. Prav tako oblikovanje podatkovnih zbirk o otrocih, s katerimi je mogoče preverjati, koliko sadja je otrok zaužil dnevno.[55] Videonadzor javnih površini je tipičen primer tehnologije, ki je postala v VB (svetovni velesili videonadzora) med prebivalci povsem sprejemljiv ukrep za zagotavljanje varnosti. Murakami Wood in Webster[56] pa ugotavljata, da smo priča normalizaciji tudi drugih oblik tehnično okrepljenega nadzora v Evropi. Ta normalizacija je po njunem mnenju posledica globalizacije nadzorovanja, domestifikacije varnosti in velike želje EU, da bi kreirala svojevrstno politiko in prevzela vodilno vlogo pri zagotavljanju varnosti.

## Univerzalnost nadzora

Univerzalnost »novega« nadzora pomeni, da nihče ni več imun na novo »bolščanje«. Z ukrepi, kot so hramba prometnih podatkov v javnih telekomunikacijskih omrežjih, videonadzorovanje javnega prostora, elektronsko označevanje izdelkov (RFID oznake), smo vsi ujeti v tehnično nadzorovanje. Čeprav je tudi res, da uporaba tako shranjenih podatkov ni nikoli sorazmerna po vsem družbenem polju. Dejanske družbene posledice tako zbranih podatkov niso sorazmerne, saj imajo politično vplivne skupine in posamezniki sredstva, da se lahko učinkom »vsenavzočnega« nadzora tudi izognejo. To, da se imamo kam skriti, je postal luksuzna dobrina, ki si jo lahko zagotovijo le premožni in vplivni, čeprav je cena za takšen izhod popoln (notranji) nadzor (na primer zatekanje v varovane ograjene skupnosti).

Paradoksalno je, da nas ravno IT, ki omogoča komoditeto in olajšuje življenje (kdo pa želi čakati pred cestninsko postajo, če nam elektronsko cestninjenje omogoča vožnjo brez ustavljanja?), postavlja pod nadzor. A ključno vprašanje je, zakaj je tehnologija nadzora postavljena v okolje na način, ki omogoča komoditeto in tudi nadzor (v primeru elektronskega cestninjenja to pomeni, zakaj ga sploh potrebujemo, če lahko enak cilj (komoditeto) dosežemo z drugimi sredstvi, na primer z višjimi cenami goriva ali vozil).

[55] Roberts 2006.

[56] Murakami Wood, Webster 2009.

## Motivi »novega« nadzora

Na sodobno nadzorovanje je mogoče gledati z vidika motivov nadzora, torej tega, zakaj sploh prihaja do nadzorovanja. Glede na razloge za nadzor je mogoče razčleniti štiri kategorije nadzora: (1) »kategorični sum« (Marx)[57] se nanaša na nadzorovanje, ki je posledica osredotočanja kazenskopravnih sistemov na grožnje, ki lahko privedejo do kriminalitete; (2) »kategorično zapeljevanje« (Lyon)[58] najdemo v potrošništvu, pri katerem smo v nadzorovanje pritegnjeni z metodami potrošniškega zapeljevanja, bleščečih predmetov, trgovskih »svetišč« in zvezdniškega blišča. Vsebina tega nadzora je evidentiranje in analiza vedenja potrošnikov (na primer s karticami zvestobe ali s programi zvestih letalskih potnikov, ki omogočajo detajlno beleženje navad in oblikovanje potrošnikovega profila), cilja pa na nadaljnje zapeljevanje posameznika v trošenje; (3) »kategorična skrb« (Ball in Webster)[59] se nanaša na nadzorovalne prakse, ki so povezane s skrbjo za človeka, z njegovim zdravjem in socialnimi storitvami (na primer z digitaliziranimi zdravniškimi kartotekami, pametnimi e-zdravstvenimi karticami ali čipi, s katerimi je mogoče na oddaljen način hitro dostopati do zdravstvenih podatkov). Temelj teh oblik nadzora je skrb za posameznika, a hkrati tovrstne skrbstvene tehnologije omogočajo identifikacijo »rizičnih skupin«, kar ima lahko za posledico »družbeno sortiranje« in diskriminacijo: rizične osebe se težje zdravstveno zavarujejo, zavarovalnice jim (lahko) naprtijo večje zavarovalne premije, so težje zaposljive ipd.; (4) »kategorično izpostavljanje« (Mathiesen)[60] pa se nanaša na nadzor sodobnih medijev v »množični kulturi«. Ti so pogosto invazivni pri svojem nadzoru »javnih« oseb ter kreativni pri oblikovanju »mnenjskih voditeljev« in »zvezdnikov«. Gre za nadzor, ki ga žene zabavljaška kultura, ki prodira v novice kot *infotainment*, ki hkrati informira in zabava, ter kot *securitainmnet*,[61] ki zabava in uči gledalce nadzornih tehnik.

[57] Marx 1988.

[58] Lyon 1994.

[59] Ball, Webster 2003: 4.

[60] Mathiesen 1997.

[61] Andrejevic 2010.

## Subjekti »novega« nadzora

Pomemben vidik »nove« povečane transparentnosti posameznika je širitev (skupaj z objekti nadzora) subjektov nadzora. Informacijska tehnologija je spremenila moč organov odkrivanja in pregona kaznivih dejanj,[62] povečala pa je tudi nadzorstveno moč civilne družbe: podjetij, korporacij in državljanov. Opolnomočeni državljani danes povratno nadzorujejo nadzornike v inverznem nadzoru (angl. *counter-surveillance*). Ljudje sami sodelujemo pri izvajanju nadzora s tehničnimi pomagali v večji meri kot doslej in »vsakodnevnost« nadzora[63] ne pomeni, da se je povečal le nadzor množice, temveč da nadzorujemo tudi sami. Koskela[64] pripisuje moč množice v proizvodnji nadzorovanja tehničnemu razvoju nove opreme (videonadzorne opreme, kamer, mobilnih telefonov ipd.)[65] in novim prostorom nadzora – virtualnemu prostoru. Vsakodnevni nadzor je danes povečan v obe smeri, nadzorniki intenzivirajo nadzor nadzorovanih skupin in tudi nadzorovani vračajo pogled nadzornikom.[66] Ta sinoptični vidik nadzora (Mathiesen) se je danes okrepil: nadzor množice v panoptikonu danes krepi ideologija varnosti, ki postavlja zahteve po vse večjem nadzoru oseb, predmetov in prostorov, a na drugi strani so nadzor manjšine nad večino (sinoptizem) okrepili množični mediji, ki večini na ogled postavljajo trivialne detajle »javnih oseb«, zvezdnikov, voditeljev in drugih »medijskih« osebnosti.

Korporacije so okrepile nadzor nad posameznikom v vlogi zaposlenega delavca in v vlogi potrošnika. Kot delavci smo nadzorovani s tehničnimi merilniki prihoda/odhoda v službo, z videonadzorom službenih prostorov, z nadzorom elektronskih in drugih telekomunikacij itn., kot potrošniki pa smo profilirani z oblikovanjem metapodatkov o nakupovalnih vzorcih, s tarčnimi internetnim marketingom, z beleženjem in analiziranjem spletnih obiskov, z uporabo plačilnih kartic itn. Med močne subjekte »novega« tehnično (p)o(d)krepljenega nadzora civilne družbe sodijo telekomunikacijska podjetja (pogosto monopolni subjekti na »odprtem trgu«), ponudniki prenosa digitalnih vsebin, ponudniki spletnih socialnih omrežij (*Facebook* ipd.), spletne trgovine (*Amazon* ipd.) in avkcijske strani (*eBay* ipd.), finančni posredniki (*PayPal* ipd.) in banke, infrastrukturni upravljavci (na primer upravljavci cestnega sveta, komunalna podjetja z nadzorom porabe vode, elektrike, plina in tudi naše »pridelave« vrste, količine, kraja in časa kopičenja odpadkov). Subjekti tehničnega nadzora so tudi druge skrbstvene institucije, kot so šole, ki postajajo »brezgotovinske« šole, kjer je mogoče plačevati malico in registrirati prisotnost učencev pri pouku s »pametnimi« karticami, s čimer naj bi omogočili zgodnjo intervencijo ob znakih »bodočih težav«.

---

[62] Moč tehničnih pomagal v praksi pogosto kaže tudi na nemoč: tehnologija ne deluje, kamere so zastarale in s slabo ločljivostjo slike, ki ne zadostuje za uporabo pred sodiščem, zadetki nadzora so napačni itn. Več o tem, kako je moč akterjev kazenskega pravosodja kljub tehnologiji šibka in zakaj je popoln policijski nadzor utopija v Manning 2008.

[63] Tako Haggerty in Ericson 2000; Staples 2000; Lyon 2001; Ball, Webster 2003.

[64] Koskela 2009: 149.

[65] Cena kamere svinčnika (*Mini DVR Video Pen*) je na primer 49,99$. Glej Amazon.com.

[66] Glej Koskela 2009: 147, ter Mathiesen 1997.

Moč tradicionalnih subjektov nadzora se na nacionalni in nadnacionalni (EU) ravni kaže v množici zbirk osebnih podatkov. V ZDA so vzpostavili nove »Fuzijske centre« (v sestavi *U.S. Department of Justice*), katerih naloga je zbirati informacije od vladnih virov, njihovih partnerjev in zasebnega sektorja, ter številnih javnih podatkovnih zbirk. Tipi podatkov, ki jih iščejo in analizirajo, so se nevarno razširili, saj vsebujejo ne le podatke, relevantne za kazenskopravno-obveščevalno delo, temveč tudi podatke javnega in zasebnega sektorja. V njih delujejo akterji kazenskopravnega sistema skupaj z drugimi vladnimi »entitetami« civilnega in vojaškega značaja in s člani zasebnega sektorja. V oblikovanju podatkovnih zbirk z biometričnimi podatki je ZDA še bolj invazivna. Na primer, za državljane članic EU je po programu *US Visit Program* obvezna registracija v sistemu ESTA najmanj 72 ur pred začetkom potovanja, vključno z odvzemom prstnih odtisov, fotografijo obraza in odvzemom biometričnih značilnosti glasu pred vstopom v ZDA, kar tvori kar tridimenzionalni govoreči »digitalni dvojnik« posameznika.

Na ravni Evropske unije obstajajo obsežne podatkovne zbirke, ki kažejo posebej močno uzurpacijo nadzorstvene moči EU. Evropski sistemi za zbiranje, hrambo ali čezmejno izmenjavo osebnih podatkov za namene pregona kaznivih dejanj ali upravljanja migracij so naslednji:[67] (1) *ukrepi za krepitev schengenskega območja in carinske unije*: (a) schengenski informacijski sistem druge generacije (SIS II), (b) EURODAC podatkovna zbirka prstnih odtisov, (c) vizumski informacijski sistem (VIS), (č) elektronski sistem za izmenjavo podatkov o izpopolnjenih informacijah o letalskih in ladijskih potnikih (*Advance Passenger Information System* – API), (d) konvencija Naples o medsebojni pomoči in sodelovanju med carinskimi upravami omogoča izmenjavo carinskih podatkov, (e) carinski informacijski sistem (CIS) s podatkovno zbirko FIDE; (2) *ukrepi za preprečevanje in boj zoper terorizem in druge oblike resne čezmejne kriminalitete*: (f) »Švedska pobuda« (2006) omogoča izmenjavo podatkov med državami članicami, (g) prümska pogodba (2008) govori o poglobitvi čezmejne izmenjave podatkov o DNK, prstnih odtisih, avtomobilskih registrskih podatkih in posameznikih, osumljenih terorizma, (h) direktiva o hrambi podatkov zavezuje ponudnike telefonskih in internetnih storitev, da hranijo prometne in lokacijske podatke, ter podatke o naročnikih, obstajajo pa še, (i) evropska informacijska kaznovalna evidenca (ECRIS), (j) za boj zoper pranje denarja in financiranje terorizma obveščevalne enote FIU (*Financial Intelligence Units*), (k) pisarne konfiskacije s kaznivimi dejanji pridobljene premoženjske koristi (AROs) in (l) evropska in nacionalne platforme za boj proti kibernetski kriminaliteti; (3) *EU agenciji z nalogo pomoči državam članicam pri prevenciji in boju zoper težje oblike čezmejne kriminalitete*, ki hranijo osebne podatke sta (m) Europol, (n) Eurojust; (4) *mednarodna dogovora o prevenciji in boju zoper terorizem in druge težje oblike čezmejne kriminalitete*, ki omogočata izmenjavo osebnih podatkov, (o) sporazum za posredovanje podatkov o letalskih potnikih (*Passenger Name Records* – PNR) z ZDA, Kanado in Avstralijo in (p) sporazum o izmenjavi bančnih podatkov prek sistema SWIFT z ZDA (TFTP); (5) *Stockholmski akcijski načrt* pa predvideva (vsaj) še: (r) nov PNR paket leta 2011, (s) vstopno-izstopni sistem za drža-

[67] Ukrepi za zbiranje, shranjevanje in čezmejno izmenjavo osebnih podatkov za namene boja proti kriminaliteti ali upravljanja migracij po Komunikaciji Komisije Parlamentu in Svetu EU *Overview of information management in the area of freedom, security and justice*.

vljane tretjih držav, ki vstopajo v EU (EES), in (š) program registriranih potnikov (RTP).

Države članice EU so dolžne oblikovati tudi zbirke, ki vsebujejo biometrične podatke. Na ravni držav članic EU in na ravni EU obstajajo vsaj naslednje zbirke biometričnih podatkov:[68] (a) zbirke biometričnih značilnosti za namene izdajanja potnih listin in potovalnih dokumentov, tako da ti vsebujejo pomnilniške medije, ki vsebujejo podobo obraza in prstne odtise, (b) dovoljenja za prebivanje za državljane tretjih držav morajo vsebovati nosilec za shranjevanje podatkov o podobi obraza in dveh podobah prstnih odtisov, (c) vizumski informacijski sistem (VIS) na ravni EU vsebuje daktiloskopske podatke prosilcev za vizume, (č) Schengenski informacijski sistem (SIS II) na ravni EU in z možnimi kopijami podatkov v državah članicah vsebuje digitalizirane fotografije in prstne odtise, (d) v Eurodac sistem za določanje države, ki je odgovorna za obravnavanje prošenj za azil, se vnašajo prstni odtisi prosilcev za azil in ilegalnih migrantov, (e) sistemi za olajševanje prehoda meje za dobroverne potnike, ki se poskusno izvajajo na nekaterih letališčih, uporabljajo biometrične podatke o podobi obraza in prstnem odtisu.

Krepitev nacionalnih in nadnacionalnih podatkovnih zbirk oblikujejo »skrivnostno državo« v državi: v ZDA nastaja »*Top Secret America*«,[69] v EU pa se stare oblike zbiranja, shranjevanja in izmenjave informacij dopolnjujejo in dodajajo nove na ravni držav članic in na ravni EU.

Ključno za mrežo subjektov »novega« nadzora je, da se je državi pridružila močna »civilna družba« – gospodarski subjekti, kot so mednarodne korporacije, veliki trgovci, marketinške agencije. Ključno za ta nadzor je, da s pravnimi »očali« ni viden, saj je pri zbiranju, obdelovanju in posredovanju podatkov praviloma zadoščeno vsem pravnim določilom o varstvu osebnih podatkov. A hipertrofija, sicer pravno dopuščenega zbiranja osebnih podatkov, generira nastanek novih in novih zbirk osebnih podatkov, komoditeta sodobnega potrošnika pa vodi v nove in nove »prostovoljne« odpovedi zasebnosti.[70] Tovrstna hipertrofija sicer s pravnim »certifikatom« ozaljšanega postopka zbiranja osebnih podatkov žal dolgoročno ni vzdržna, je etično nesprejemljiva in potencialno nevarna, ker predstavlja močne skušnjave za zlorabe, katerih posledic ne bi bilo mogoče popraviti. Zna se zgoditi, da se naenkrat zbudimo v novi družbi.

---

[68] Po Janc 2009.

[69] Kritično o širjenju zaupnega sistema nadzorovanja v ZDA, ki ima 854.000 zaposlenih, v Priest, Arkin 2010.

[70] Glej programe zvestih letalskih potnikov, kartice »zvestobe« (popustov) ipd. zapeljive produkte.

### Značilnosti »novega« nadzora

Značilnost sodobnega nadzora je, da omogoča močno povečano vidljivost posameznika, da je mobilen in da omogoča klasifikacije.[71] Digitalni obrat, ki je nastal z razvojem IT, sodobno nadzorovanje spreminja v bolj subtilno, a hkrati bolj intenzivno.[72] Tehnično avtomatiziran nadzor nadomešča pomanjkljivo, muhavo in z željo prežeto človeško opazovanje. Omogoča tudi obsežne primerjave in klasificiranje podatkov, ki so bili doslej sicer zbrani, a hranjeni ločeno na nepovezanih lokacijah in v različnih oblikah (lastnoročnih zapisih, mikrofilmih, mikrofiših, kasetah, CDjih idr. nosilcih podatkov). »Vidljivost« se je povečala tudi zaradi izpostavljenosti več pogledom hkrati, kar je privedlo do »korenikastega« razširjanja nadzora.[73]

Povečana vidljivost je posledica dejstva, da zbiranje osebnih podatkov transcendira meje in ovire doslejšnje vidljivosti, in sicer: (1) geografske razdalje (na primer satelitski nadzor), (2) svetlobo oziroma vidljivost (nadzor je mogoč ponoči, ker je mogoče prestrezati dele elektromagnetnega valovanja, ki ne sodi v vidni spekter), (3) kožo (na primer preslikovanje možganov s tehnikami funkcionalne magnetne resonance, z rentgenom, s tehnologijo visokega milimetrskega valovanja[74]), (4) čas (nadzor je mogoč v dejanskem času, ko se nekaj dogaja) in (5) velikost (nadzorovati je mogoče pojave od mikroskopskih in vse do nano velikosti).

Sodobni nadzor omogoča tudi transcendenco umetnih meja: (a) zidov (na primer termično nadzorovanje stavb za prisotnost oseb), (b) drugih materialov (na primer zapiske Ratka Mladiča so organi pregona odkrili z napravami gledanja skozi les in beton),[75] (c) zapečatenih ovojnic itd. Običajne ovire doslejšnje vidljivosti, ki so v preteklosti preprečevale zbiranje ali pretok osebnih podatkov, so danes (ob dovoljšnjih resursih subjektov nadzora) padle.[76]

Informacijske tehnologije nadzora imajo zato trojne učinke: so globlje, širše in bolj neopazne pri zbiranju podatkov od starejših metod. Globlje so, ker omogočajo zbiranje vedno bolj intimnih detajlov o posamezniku in ustvarjanje nove vednosti o posamezniku. Širše so, ker omogočajo nadzor nad vidiki posameznikovega življenja, ki jih do sedaj ni bilo mogoče sistematično beležiti, shranjevati in analizirati, bolj neopazne (fizično neinvazivne) pa zato, ker posameznik niti ne more z običajnimi sredstvi zaznati nadzora, ki se izvaja nad njim (t. i. *»low level« intelligence*).[77]

---

[71] Po Lyon 2002.

[72] Po Koskela 2009: 150.

[73] Po Haggerty, Ericson 2000.

[74] Angl. *Millimeter-wave imaging-technology*.

[75] Simons 2010.

[76] Marx 2002.

[77] Glej Podbregar, Ivanuša 2010.

Če povzamemo doslej nanizane novosti »novega« nadzora, so njegove temeljne značilnosti: (povečana) vidljivost posameznika, mobilnost nadzora, klasificiranje,[78] (tehnična) sofisticiranost,[79] trend širjenja in večja invazivnost. »Novi« nadzor se od »tradicionalnega« razlikuje po naslednjih dimenzijah:[80]

| **Dimenzija** | **Tradicionalni nadzor** | **»Novi« nadzor** |
|---|---|---|
| Uporabljena čutila | »Običajna«, neokrepljena | Tehnološko okrepljena |
| Vidljivost (zbirk podatkov, subjektov nadzora, lokacij nadzora) | Vidni | Manj vidni ali nevidni |
| Soglasje | Manjši delež nehotnega | Večji delež nehotnega |
| Stroški | Dražje | Cenejše |
| Integracija | Zbiranje podatkov je posebna, ločena dejavnost | Zbiranje podatkov je vpeto v rutinske dejavnosti |
| Prisilnost | »Trši« (bolj prisilno) | »Mehkejši« (manj prisilno) |
| Lokacija nadzornika | Na kraju dogajanja | Tudi oddaljeno |
| Nadzornik | Človek, žival | Stroj |
| Kraj zbranih podatkov | Pri nadzorniku, lokalno | Pri tretjih osebah, pogosto se podatki selijo |
| Objekt nadzora | Posameznik | Posameznik in kategorije ljudi |
| Časovno obdobje nadzora | Sedanjost | Preteklost, sedanjost, Prihodnost |
| Časovno osredotočanje nadzora | Posamična točka ali v Presledkih | Kontinuiran |
| Dostopnost podatkov | Z odlogom | V dejanskem času, v katerem se nekaj dogaja |
| Dostopnost tehnologije | Nesorazmerno dostopna (tehnologija bolj dostopna elitam) | Bolj dostopna (demokratizirana) |
| Kontekst nadzora | Kontekstualiziran | Akontekstualiziran |
| Globina | Manj intenziven | Bolj intenziven |
| Širina | Manj intenziven | Bolj intenziven |
| Objekt nadzora | Poudarek na znanih posameznikih | Poudarek tudi na anonimnih posameznikih, množici, agregatih, tokovih |
| Razmerje med sebstvom in vednostjo nadzornika | Višje (kar ve nadzornik, ve verjetno tudi nadzorovani) | Nižje (nadzornik ve, kar nadzorovani ne nujno pozna) |
| Realističnost proizvoda nadzora | Neposredna podoba | Tudi simulacije |

[78] Tako Lyon 1994.

[79] Na primer Goold 2009.

[80] Po Marx 2002.

| Dimenzija | Tradicionalni nadzor | »Novi« nadzor |
|---|---|---|
| Oblika proizvoda nadzora | Posamični medij (pisni ali Numerični) | Večpredstavnost (zmožnost posredovati informacije z besedilom, sliko, gibljivo sliko, zvokom) |
| Analiza podatkov | Težje organizirati, shranjevati, priklicati, analizirati | Lažje organizirati, shranjevati, priklicati, analizirati |
| Povezovanje podatkov | Ločeni in težje primerljivi podatki (različne oblike, različne lokacije) | Lažje primerljivi, povezljivi podatki več vrst (optični, slušni, tekstovni, numerični) |
| Posredovanje podatkov | Težje poslati in sprejemati | Lažje poslati in sprejemati |

### Kritike nadzorstvene družbe in upor nadzoru

Družbeno nadzorovanje ni bilo nikoli statično. V preteklosti je neformalen nadzor in moč nadzorovanih množic omogočala praksa govoric, danes pa se ljudje prilagajajo novim mehanizmom nadzora in na primer prevzemajo aktivno vlogo pri proizvodnji in cirkulaciji avdio- in videoposnetkov.[81] Po Foucaultu moč generira tudi odpore moči. Digitalna moč nadzora zato ne povečuje le zmogljivosti avtoritet in elit, temveč prinaša tudi emancipatorni potencial. Oblikuje »kompleksne mreže odnosov moči in odporov«.[82]

Prva kritika teoretiziranja o nadzorstveni družbi se nanaša na dejstvo, da se razmišljanje o nadzorstveni družbi preveč zgleduje po distopičnih novelah, kot sta Orwellov *1984* in Huxleyjev *Krasni novi svet*. Literarna fikcija je prikazala potencial nevarnega razvoja prihodnje družbe, a ta fikcija ni povsem pravilna zgodovina prihodnosti. Sodobno nadzorovanje je preveč razpršeno, objekti nadzora pogosto v drugih družbenih situacijah nastopajo kot subjekti nadzora. Namesto »Velikega brata«, ki centralno obvladuje poživinjeno množico, imamo danes veliko malih »bratcev«.

Slabost sodobnih nadzorstvih študij zato je, da se pretežno ukvarjajo z analizo vsemogočega nadzora, ki poteka od zgoraj navzdol, od nadzorstvene institucije k nadzorovanemu posamezniku, manj pa je spraševanja o tem, kakšen je odziv nadzorovanega. Lyon[83] na primer opozarja na preveliko osredotočenost nadzorstvenih študij na sisteme, njihove zmogljivosti in na vsemogočne tehnologije. Pri tem pa zanemarjajo subjekte, analizo aktivnosti tistih, ki delujejo v teh aranžmajih nadzora. Nadzorovani so namreč mesto izvajanja oblasti, a to ne pomeni, da so pasivni objekti. So aktivni subjekti in subjekti želje, ki reflektirajo prakse nadzora, jim skušajo uiti, se jim izogniti,

[81] Po Tinic 2006.

[82] Green 1999: 27.

[83] Lyon 2007: 92.

vrniti pogled in tudi opozoriti na nelegitimne, diskriminirajoče ali kako drugače nepravične prakse nadzora.[84]

Upor nadzoru bolj konkretno odražajo aktivnosti nevladnih organizacij, kot so *Privacy International*, *Electronic Frontier Foundation*, *Digital Rights* ali *Big Brother Awards* – ta podeljuje nagrade in sramoti vladne in korporacijske posege v zasebnost. Ali umetniške skupine, ki vzpostavljajo cone, kjer ni nadzora (na primer tako, da izdelujejo načrte mestnih ulic, ki niso pod videonadzorom, t. i. *iSee* poti) ali računalniške simulacije, kako uiti sistemom za avtomatično prepoznavo obraza z drugačno pričesko in ličenjem.[85] Cilji teh skupin so krepiti zavest o nadzorovanju, ki se izvaja brez soglasja posameznika, in to za cilje, na katere nadzor niti nima vpliva, saj sredstva nadzora pogosto niso kos nalogi, ki naj bi jo domnevno izpolnjevala (na primer videonadzor javnih površin na zmanjšanje kriminalitete nima vpliva).[86] Njihov cilj je tudi povečati nadzor nad represivnimi organi (na primer t. i. »*cop watching*«) in vse bolj tudi nad nezakonitimi praksami delodajalcev.

Prakse upora dobivajo različna teoretična osmišljanja: Mann meni,[87] da gre za gibanje »*sousveillance*«, ki ga opredeli kot reflekcionizem, kar pomeni uporabo zatiralskih orodij zoper zatiralce same. Drugi avtorji te prakse označujejo kot »inverzno nadzorovanje« ali sobivanje nadzora in protinadzora (angl. »*co-veillance*«). Monahan[88] pa »proti-nadzorovanje« (angl. *counter-surveillance*) opredeljuje kot namensko in taktično uporabo ter motenje nadzornih tehnologij z namenom izzvati asimetrije institucionalne moči. Koskela[89] govori o »ugrabitvi« nadzorovanja. Ugotavlja,[90] da se nadzorovani upirajo pogledu in tudi sami opazujejo in vračajo opazovanje. Yar[91] pa v analizi študij videonadzorovanja, torej konkretne tehnologije nadzora, ugotavlja, da te študije zanemarjajo možne aktivne vloge nadzorovanih. Dejansko se nadzorovani emocionalno odzivajo na kamere in najdejo številne načine subvertiranja nadzora in izogibanja pogledu kamere. Na primer, poulični igralci v New Yorku svoje performanse izvajajo na krajih, ki ga snemajo kamere in tako subvertirajo učinke moči, ki naj bi bili homogeni. Študije odpora torej v pomembnem vidiku dopolnjujejo teoretiziranje o nadzorstveni družbi, ko se ukvarjajo s tem, kako razumeti odnos nadzorovanih do nadzora.

Rizično mesto sistemov nadzora, kjer ti lahko odpovedo, pa niso le nadzorovani, temveč tudi nadzorniki. Tudi ti so subjekti želje, subverzije, refleksije, ki lahko onemogočijo in subvertirajo vzpostavitev »orwellovskega« nadzornega stolpa. To je druga pomanjkljivost v teoretiziranju sodobnega tehnično okrepljenega nadzora. Mesto

---

[84] Ball 2003.

[85] Glej Harvey 2010.

[86] Tako Leman-Langlois 2008b, Hempel, Töpfer 2009.

[87] Mann 2002: 534.

[88] Monahan 2006.

[89] Koskela 2009.

[90] Koskela 2003.

[91] Yar 2003.

nadzornika predstavlja tudi mesto tveganja za delovanje nadzornih mehanizmov, saj lahko ruši, preobraža ali subvertira učinke totalitarizirajočih institucij nadzora. Orwellov nadzorni *telescreen* v praksi zato ni tako vsemogočen, kot bi oblikovalci sodobnih varnostnih politik to želeli. Mesto nadzornika je kontingentno, tekoče in nepredvidljivo.

Videonadzorni sistemi, opozarja Douglas Smith,[92] v praksi še zdaleč ne povečujejo gotovosti v negotovem svetu. Njihov učinek je, da proizvajajo ontologije negotovosti: fragmentirajo vsakodnevno življenje, povzročajo neenakosti in povečujejo negotovosti. Nadzorniki gledajo tudi kaj drugega (ali predvsem kaj drugega) od tega, kar naj bi nadzorovali, so podrejeni imperativom kapitala (njihova služba ima notranjo dinamiko, ki jih dela podrejene drugim akterjem, zlasti so pri svojem delovanju odvisni od pomoči policije in varnostnikov, ki dejansko ukrepajo na podlagi nadzornikovih opozoril) in so pogosto impotentni (vse, kar lahko storijo je, da opazujejo, kaj se dogaja na opazovanem kraju). Podobno za uporabo sodobnih tehnologij pri opravljanju policijskega dela ugotavlja Manning.[93] Dejansko policijsko delovanje je še vedno usmerjeno v tradicionalne naloge in tehnično dovršeno delovanje policije ostaja neizvedljivo v praksi. Tehnologija ni dovolj zanesljiva, v policiji potekajo boji za moč in vpliv posamičnih izobrazbenih skupin, zaposleni ne kažejo interesa za uporabo tehnologije, če pa so motivirani za njeno uporabo, tehnološke rešitve pogosto niso kompatibilne in generirajo več dela, kot ga pomagajo opraviti. Realnost policijskega dela je še zelo daleč od tega, da bi bila »visoko-tehnološka«.

Oznaka »nova nadzorstvena družba« je, tretjič, tudi zelo splošna, saj ne odraža dejstva, da je nadzor zgodovinsko, prostorsko in kulturno pogojen. Sodobne študije nadzorovanja se zgledujejo po anglo-ameriškem kulturnem okolju in na nadzorovanje se gleda z anglo-ameriškimi očali.[94] Murakami Wood[95] na primer primerja Japonski nadzor s tistim v VB in upravičeno trdi, da ni nujno, da je »nadzorstvena družba«, ki jo lahko opazujemo na različnih krajih in v različni intenziteti, sploh v čemerkoli še enaka družba. Lahko gre za popolnoma drugačne oblike nadzora, drugačne mreže subjektov in objektov nadzora. Kritika praznosti teze o nadzorstveni družbi prihaja tudi iz Francije,[96] kjer so postavili osnovne pojme, v katerih danes razmišljamo o nadzoru (od Foucaulta prek Deleuza do Bigoja). Sodobno teoretiziranje ostaja anglocentrično, predvsem so na voljo analize, ki se nanašajo na VB, ZDA, Kanado, le deloma še Nemčijo in skandinavske države.[97] Vzhodna, južna in osrednja Evropa, kot da tehnično okrepljenega nadzora ne bi poznala. Geografska ločnica sodobnih nadzorstvenih študij, ki so dobile zagon z razvojem informacijske tehnologije, danes v veliki meri poteka po mejah železne zavese. A prisluškovanje, opazovanje, sledenje ipd. so nekaj, kar so tajne službe vedno počele in kar je postalo po padcu berlinskega zidu vsaj v »vzhodnem bloku« dostopno javnosti in danes etiketirano kot barbarski unikum, ki mu na zahodu

[92] Douglas Smith 2009: 145.

[93] Manning 2008.

[94] Goold 2009: 116.

[95] Murakami Wood 2009.

[96] Klauser 2009.

[97] Glej Murakami Wood, Webster 2009.

naj ne bi bilo najti vzporednic. Kot kaže, je razlika med teoretiziranjem o tehnološko okrepljenem nadzoru med »blokoma«, v veliki meri še posledica dejstva, da je država v »vzhodnem bloku« še vedno dojeta kot demon, ki ga je potrebno omejiti in oslabeti. Tako je postala plen gospodarskih elit, ki prisesane na državna (javna) sredstva kopičijo svojo moč. Nove tehnologije nadzora preveč in prepogosto neutemeljeno zareverberirajo strah pred premočno »očetovsko« državo, zato tudi niso bile uvedene v tolikšni meri. Kar je lahko dobro (vsaj na primer videonadzorne revolucije po vzoru VB ne potrebujemo, čeprav lahko pride do nas preko EU) in slabo (saj nam državo četverijo jezdeci gospodarske elite, civilne družbe, politični vplivneži in njihove oprode). Analiza zasebnih subjektov »novega« nadzora v »vzhodnem bloku« je torej ključna naloga prihodnjih »novih« nadzorstvenih študij tehnično okrepljenega nadzora.

# Viri in literatura


1. Andrejevic, M. (2010). Reading the Surface: Body Language and Surveillance, **Culture Unbound**, let. 2, s. 15–36. Po URL: http://www.cultureunbound.ep.liu.se/v2/a03/cu10v2a3.pdf, dostop 15.7.2010.
2. Bacon, F. (1996). **Francis Bacon: a critical edition of the major works**. Oxford, New York: Oxford University Press.
3. Ball, K. (2003). Power, control and computer-based performance monitoring: Repertoires, resistance and subjectivities. V: D. Lyon (ed.), **Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination**, London and New York: Routledge.
4. Ball, K.; Webster, F. (2003). The intensification of surveillance. V: K. Ball, F. Webster (eds.), **The Intensification of Surveillance: Crime, terrorism and warfare in the information age**. London: Pluto Press, s. 1–15.
5. Bauman, Z. (2002). **Tekoča moderna**. Ljubljana: Založba /*cf. (Rdeča zbirka).
6. Brin, D. (2009). Crime and lawfulness in the age of all-seeing techno-humanity. V: S. Leman-Langlois (ed.), **Technocrime. Technology, crime and social control**. Cullompton [England], Portland, Or.: Willan Publishing, s. 14–26.
7. Clapham, C. (1982). **Private Patronage and Public Power: Political Clientelism in the Modern State**. London: Collins.
8. Dandker, C. (1990). **Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day**. Cambridge: Polity Press.
9. Douglas Smith, G.J. (2009). Empowered watchers or disempowered workers? The ambiguities of power within technologies of security. V: K. Franko Aas, H. Oppen Gundhus, H. Mork Lomell (eds.), **Technologies of inSecurity: the surveillance of everyday life**. Abingdon, New York: Routledge-Cavendish, s. 125–146.
10. Flanagan, M.; Howe, D.C.; Nissenbaum, H. (2008). Emobodying Values in Technology: Theory and Practice. V: J. van den Hoven, J. Weckert (eds.), **Information Technology and Moral Philosophy**, Cambridge: Cambridge University Press, s. 322–353.
11. Franko Aas, K. (2005). **Sentencing in the Age of Information: From Faust to Macintosh**. London, Sydney, Portland, Oregon: The GlassHouse Press.
12. Garfinkel, S. (2001). **Database Nation: the death of privacy in the 21st century**. Sebastopol (CA): O'Reilly.
13. Giddens, A. (1985). **The Nation-State and Violence**. Cambridge: Polity.
14. Goold, B.J. (2009). Editorial. Making Sense of Surveillance in Europe. **European Journal of Criminology**, let. 6, št. 2, s. 115–117.
15. Green, S. (1999). A plague on the Panopticon: Surveillance and power in the global information society. **Information, Communication and Society**, let. 2, s. 26–44.
16. Haggerty, K.D.; Ericson, R.V. (2000). The surveillant assemblage. **British Journal of Sociology**, let 51, št. 4, s. 23–45.

17. Harvey, A. (2010). **How to Hide from Machines**. Po URL: http://ahprojects.com/blog/146, http://ahprojects.com/c/itp/thesis, dostop 1.7.2010.
18. Hempel, L.; Töpfer, E. (2009). The surveillance consensus: Reviewing the politics of CCTV in three European countries. **European Journal of Criminology**, let. 6, št. 2 , s. 157–177.
19. Hooper, (2009). Protesters, police go on-line in G-20 battle. **CNN**, 27.marec. Po URL: http://edition.cnn.com/2009/WORLD/europe/03/26/g20.protests.social.networking/index.html#cnnSTCText, dostop 1.8.2010.
20. James, A. (1979). Sentenced to Surveillance? **Probation Journal**, let. 26, št. 1, s. 15–20.
21. Janc, G. (2009). Zbirke biometričnih značilnosti v EU. **Pravna praksa**, št. 6, s. 16–19.
22. Jones, R. (2005). Surveillance. V: Hale *et al.* (eds.), **Criminology,** Oxford: Oxford University Press, s. 471–492.
23. Klauser, F. R. (2009). »Lost« Surveillance Studies: a discussion of French research on CCTV. **Surveillance and Society**, let. 6, št. 1, s. 23–31.
24. Komunikacija Komisije EU Parlamentu in Svetu (2010). **Overview of information management in the area of freedom, security and justice**, Brussels, 20.7.2010, COM(2010)385 final.
25. Koskela, H. (2003). »Cam era«: The contemporary urban panopticon. **Surveillance and Society**, let. 1, št. 3, s. 292–313.
26. Koskela, H. (2009). Hijacking surveillance? The new moral landscapes of amateur photographing. V: K. Franko Aas, H. Oppen Gundhus, H. Mork Lomell (eds.), **Technologies of (In)Security: the surveillance of everyday life**. Abingdon, New York: Routledge-Cavendish, s. 147–167.
27. Leman-Langlois, S. (2008b). The local impact of police videosurveillance on the social construction of security. V: S. Leman-Langlois (ed.), **Technocrime: Technology, crime and social control**, Cullompton, Devon, Portland: Willan Publishing, s. 27–45.
28. Leman-Langlois, S. (2008c). Privacy as currency: crime, information and control in cyberspace. V: S. Leman-Langlois (ed.), **Technocrime: Technology, crime and social control**, Cullompton, Devon, Portland: Willan Publishing, s. 112–138.
29. Lemieux, F. (2008). Information technology and criminal intelligence: a comparative perspective. V: S. Leman-Langlois (ed.), **Technocrime: Technology, crime and social control**, Cullompton, Devon, Portland: Willan Publishing, s. 139 –168.
30. Lyon, D. (1994). **The Electronic Eye: The Rise of Surveillance Society**. Minneapolis: University of Minnesota Press.
31. Lyon, D. (2001). **Surveillance Society: Monitoring everyday life**. Buckingham: Open University Press.
32. Lyon, D. (2002). Editorial. Surveillance Studies: Understanding visibility, mobility and the phenetic fix. **Surveillance and Society**, let. 1, št. 1, s. 1–7.
33. Lyon, D. (ed.) (2003). **Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination**. London and New York: Routledge.

34. Lyon, D. (2007). **Surveillance Studies: An Overview**. Cambridge, Malden: Polity Press.
35. Lyotard, J.-F. (1984). **The Postmodern Condition: A Report on Knowledge**. Manchester: Manchester University Press.
36. MacKenzie, D.; Wajcman, J. (1985). **The social shaping of technology**. Milton Keynes, UK: Open University Press.
37. Mann, S. (2002). »Reflectionism« and »diffusionism«: New tactics for deconstructing the video surveillance superhighway. V: T.Y. Levin, U. Frohne, P. Wiebel (eds.), **Rhetorics of Surveillance from Bentham to Big Brother**, Karlsruhe: ZKM Centre for Art and Media, s. 531–543.
38. Manning, P.K. (2008). A view of surveillance. V: S. Leman-Langlois (ed.). **Technocrime. Technology, crime and social control**, Cullompton [England], Portland, Or.: Willan Publishing, s. 209–242.
39. Marx, G.T. (1988). **Undercover: Police Surveillance in America**. Berkeley: University of California Press.
40. Marx, G.T. (2002). What is new about the »new surveillance«? Classifying for change and continuity. **Surveillance and Society**, let. 1, št. 1, s. 9–29.
41. Mathiesen, T. (1997). The viewer society: Foucault's »Panopticon« revisited. **Theoretical Criminology**, let. 1, št. 2, s. 215–234.
42. Monahan, T. (2006). Counter-surveillance as political intervention? **Social Semiotics**, let. 16, št. 4, s. 515–534.
43. Murakami Wood, D. (2009). The »Surveillance Society«: Questions of History, Place and Culture. **European Journal of Criminology**, let. 6, št. 2, s. 179–194.
44. Murakami Wood, D.; Webster, C.W. (2009). **Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of a Bad Example**. Po URL: http://www.tcd.ie/Statistics/egpa/docs/2009/Webster.pdf, dostop 23.7.2010.
45. Negroponte, N. (1996). **Being Digital**. New York: Vintage books.
46. Podbregar, I.; Ivanuša, T. (2010). Javni viri in analitika v obveščevalni dejavnosti. **Revija za kriminalistiko in kriminologijo**, let. 61, št. 2, s. 191–198.
47. Poster, M. (1996). Databases as discourse or electronic interpellations. V: D. Lyon, E. Zureik (eds.), **Computers, Surveillance and Privacy**, Minneapolis: University of Minnesota Press.
48. Postman, N. (1993). **Technopoly: the surrender of culture to technology**. New York: Vintage Books.
49. Priest, D.; Arkin, W.M. (2010). Top Secret America. **Washington Post**, 21.7. Po URL: http://projects.washingtonpost.com/top-secret-america/articles/, dostop 16.7.2010.
50. Roberts, Y. (2006). Beware the parent trap. **Guardian**, 29. junij. Po URL: http://www.guardian.co.uk/commentisfree/2006/jun/29/comment.children, dostop 17.7.2010.
51. Roszak, T. (1994). **The Cult of Information: A Neo-Luddite Treatise on High-Tech, Artificial Intelligence, and the True Art of Thinking**. Berkeley and Los Angeles: University of California Press.

52. Selinšek, L. (2008). Digitalna forenzika v kazenskih postopkih. V: L. Selinšek (ur.), **Digitalna forenzika v kazenskih postopkih**, Ljubljana: GV Založba, s. 13–64.
53. Simmel, G. (1950). The metropolis and mental life. V: K.H. Wolff (ed.), **The Sociology of Georg Simmel**, Glencoe, IL: Free Press.
54. Simons, M. (2010). Data on Balkan Wars Found in Home of Suspect. **The New York Times**, 10.7. Po URL: http://www.nytimes.com/2010/07/11/world/europe/11mladic.html?_r=4, dostop 20.7.2010.
55. Staples, W.G. (2000). **Everyday Surveillance. Vigilance and visibility in postmodern life**. Lanham: rowman & Littlefield.
56. Swain, V.; Apple, E. (2009). Watching you watching me. **Guardian**, 15. marec. Po URL: http://www.guardian.co.uk/commentisfree/libertycentral/2009/mar/13/surveillance-police-protest, dostop 15.7.2010.
57. Tinic, S. (2006). (En)visioning the televisual audience: Revisiting questions of power in the age of interactive television. V: K.D. Haggerty, R.V. Ericson (eds.), **The New Politics of Surveillance and Visibility**, Toronto: University of Toronto Press, s. 308–326.
58. Torpey, J. (2000). **The Invention of the Passport: Surveillance, Citizenship and the State**. Cambridge: Cambridge University Press.
59. Turkle, S. (1995). **Life on the Screen: identity in the age of the Internet**. New York: Simon & Schuster.
60. Wajcman, G. (2010). **L'oeil absolu**. Paris: Denoël (Médiations).
61. Weber, M. (1987). **Economy and Society**, 2 vol. Berkely, CA: University of California Press.
62. Yar, M. (2003). Panoptic Power and the Pathologisation of Vision: Critical Reflections on the Foucauldian Thesis. **Surveillance and Society**, let. 1, št. 3, s. 254–271.
63. Zuckerman, E. (2010). Listening to global voices. **TEDGlobal**, julij 2010. Po URL: http://www.ted.com/talks/ethan_zuckerman.html, dostop 17.7.2010.

# II. ZASEBNOST V DIGITALNI DOBI

## 2 Komunikacijska zasebnost na delovnem mestu

**Matej Kovačič**

### Uvod

Pri vprašanju zasebnosti na delovnem mestu v praksi pogosto naletimo na argumentacijo delodajalcev, češ, zaposleni uporablja opremo podjetja, v službi je plačan za opravljanje svojega dela, kako torej lahko na delovnem mestu pričakuje zasebnost? Če je delodajalec lastnik komunikacijske opreme (telefona, računalnika) in delovnega časa zaposlenega – ali torej nima pravice preveriti ali zaposleni dela, ali pa morda »zapravlja« čas podjetja oziroma morda celo krade poslovne skrivnosti?

Vprašanje je vsekakor na mestu, a odgovor na vprašanje ali zaposleni na delovnem mestu lahko pričakuje spoštovanje zasebnosti, je odvisen predvsem od razumevanja vloge zaposlenega. Pri tem sta se v svetu uveljavila dva pristopa. Prvi, »ameriški« pristop zaposlenega na delovnem mestu vidi predvsem kot delojemalca, ki uporablja opremo, ki je last delodajalca, v delovnem času je plačan s strani delodajalca in zato službenih komunikacijskih sredstev in službenega časa ne sme »zlorabljati« v zasebne namene. Na drugi strani imamo t. i. »evropski« pristop, ki zaposlenega na delovnem mestu ne vidi samo kot delavca, pač pa tudi kot človeško bitje, ki ima kot tak tudi določene (človekove) pravice. Ob vsem skupaj se v primeru nadzora na delovnem mestu postavlja še vprašanje pravic t. i. tretjih oseb (z nadzorom komunikacij zaposlenega nadzorujemo tudi komunikacije njegovih zunanjih komunikacijskih partnerjev). Pri vsem skupaj je pomembno tudi vprašanje sorazmernosti (se pravi kolikšen obseg nadzora je sprejemljiv in še opravičljiv oziroma ali zaželenega cilja ni mogoče doseči z blažjimi sredstvi), saj je po eni strani jasno, da ima zaposleni tudi na delovnem mestu interes za čim večjo zasebnostjo, po drugi strani pa je nesporen tudi interes delodajalca po racionalni rabi službenih sredstev in delovnega časa.

## Ameriški pristop

Ameriška zakonodaja je koncipirana kot sistem negativnih svoboščin, zato je pravica do zasebnosti posameznikov nasproti državi bistveno bolj zavarovana kot nasproti delodajalcem. Zasebnost na delovnem mestu v ZDA v splošnem ni dojeta kot pravica, temveč bolj kot boniteta.

Ameriški delodajalci zato o zaposlenih zbirajo številne podatke, posebej problematično pa je, da pogosto ne zagotavljajo točnosti in zaupnosti podatkov, posameznikom pa pogosto tudi ne omogočijo, da bi napačne podatke lahko popravili. Obseg nadzora na delovnem mestu se v ZDA v zadnjem desetletju precej povečuje, postaja pa tudi čedalje bolj rutinski. Kot je leta 2001 ugotovil Schulman, je razlog za premik nadzorovanja od zgolj nekaj »problematičnih« posameznikov proti nadzoru celotne populacije zaposlenih ta, da je zdaj celotna delovna sila sumljiva, podjetja pa so čedalje bolj zaskrbljena zaradi t. i. »internih groženj« (Schulman, 2001). Z nadzorom se podjetja v ZDA želijo zaščititi tako pred odtekanjem različnih poslovnih skrivnosti kot tudi pred odškodninskimi tožbami zaradi neprimernega ravnanja zaposlenih. Pomemben faktor pri povečevanju nadzora pa predstavlja tudi agresivno trženje nadzornih sistemov s strani proizvajalcev in prodajalcev tovrstne opreme.

Leta 1986 so v ZDA sprejeli *Electronic Communication Privacy Act*[1] (ECPA), ki obravnava prisluškovanje elektronskim komunikacijam. ECPA v prvem poglavju, znanem tudi pod imenom *Wiretap Act*, prepoveduje prestrezanje elektronskih telekomunikacij, pri čemer je »prestrezanje« definirano kot »*zaznavanje izžarevanja [signala] (angl.* aural*) ali druga pridobitev vsebine žice oziroma elektronske ali ustne komunikacije, ki poteka s pomočjo uporabe kakršnekoli elektronske, mehanične ali druge naprave*«.[2] Bistveno pri tem je, da je prestrezanje definirano kot dejavnost, ki poteka hkrati s prenosom. Problem sodobne tehnologije – konkretno, nadzora elektronske pošte – pa je, da prestrezanje elektronske pošte ni nujno sočasno. Delodajalec namreč lahko dostopi do strežnika, v katerem je elektronsko sporočilo *shranjeno*, in s tem zaobide prepoved sočasnega prestrezanja. ECPA namreč v drugem poglavju, znanem pod imenom *Stored Communications Act*, ki prepoveduje dostop do shranjenih elektronskih sporočil brez soglasja nadzorovane osebe, iz prepovedi eksplicitno izključuje »*osebe, ki zagotavljajo (angl.* to provide*) žično ali elektronsko komunikacijsko storitev*«. Tako so iz prepovedi ECPA izvzeti delodajalci, ki imajo v lasti komunikacijsko opremo podjetja (Sinrod, 2004).

ECPA delodajalcem tudi sicer dovoljuje nadzor komunikacij (tudi telefonskih), a le, če zadevajo poslovanje podjetja. V primeru telefonskih pogovorov se tak nadzor v praksi izvaja tako, da lahko delodajalec zakonito nekaj časa posluša pogovor, da ugotovi, ali gre za poslovni ali zasebni pogovor (ACLU, 2003). Če je pri telefonskem pogovoru poslušanje še možno časovno omejiti, pa dostop do elektronske pošte ne more biti delen ali časovno omejen, pač pa delodajalec lahko naenkrat vpogleda v celotno sporočilo.

[1] Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986).

[2] *Ibidem*.

Zato je nadzor elektronske pošte laže upravičiti. Vsekakor pa velja, da lahko kot pogoj za zaposlitev delodajalci zahtevajo soglasje za nadzor v (skoraj) kakršnemkoli obsegu in v tem primeru je nadzor komunikacij zaposlenega povsem zakonit. V nadaljevanju si poglejmo nekaj primerov, ki to ilustrirajo.

Leta 1990 je administratorka elektronskega poštnega sistema podjetja Epson, Alana Shoars, ugotovila, da eden izmed direktorjev prebira elektronsko pošto zaposlenih. Temu je nasprotovala, zato so jo odpustili. Shoarsova je vložila tožbo, vendar se je podjetje branilo, da je sistem za elektronsko pošto v njihovi lasti in imajo zato pravico, da ga upravljajo in nadzorujejo, ali se uporablja samo v delovne namene ali ne. Kalifornijsko sodišče je nato 1992 v primeru *Shoars proti Epson America Inc*.[3] presodilo, da ustava ščiti samo informacije, ki so osebne, ne pa tudi poslovnih komunikacij, Shoarsova pa je uporabljala opremo, ki je bila v lasti podjetja (Sykes, 1999: 140). Njena pritožba je bila zavrnjena.

Podobna je bila tudi odločitev v primeru *Bonita P. Bourke, et. al. proti Nissan Motor Corporation*,[4] ko je leta 1993 kalifornijsko prizivno sodišče razsodilo, da vpogled v elektronsko sporočilo, ki ga je uslužbenka poslala po omrežju podjetja, ne pomeni neupravičenega vdora v njeno zasebnost, saj je uslužbenka predhodno podpisala izjavo, v kateri se je zavezala, da bo elektronsko pošto uporabljala zgolj v službene namene (Klemenčič, 2003: 137). Podobna je bila tudi razsodba v primeru *McLaren proti Microsoft*[5] iz leta 1999. V tem primeru je podjetje pregledalo z geslom šifrirano elektronsko pošto zaposlenega, shranjeno v osebnem imeniku ter na podlagi vsebine sporočil zaposlenega (ki je bil obtožen spolnega nadlegovanja) odpustilo. Zaposleni je sprožil sodni spor, a sodišče je v razsodbi dalo prav delodajalcu, in sicer z obrazložitvijo, da je interes delodajalca, da prepreči pošiljanje neprimerne elektronske pošte, nad interesom zaposlenega do zasebnosti (Klemenčič, 2003: 137).

Kaj je neprimerno, pa je pogosto stvar presoje delodajalca. Na to kaže primer zaposlenega v podjetju Pillsbury. Zaposleni Michael Smyth je namreč leta 1994 enemu izmed sodelavcev poslal elektronsko sporočilo, v katerem je zapisal, da so njegovi predpostavljeni *»zahrbtne barabe«*. Ker so le-ti spremljali komunikacijo svojih zaposlenih, so ga odpustili z obrazložitvijo, da so bili njegovi komentarji neustrezni in neprofesionalni. Smyth se je pritožil na sodišče in trdil, da so mu v podjetju zagotovili zasebnost komunikacij, podjetje pa je trdilo nasprotno. Zvezno sodišče je primer zavrglo (in s tem dalo prav delodajalcu) z obrazložitvijo, da tudi če bi podjetje zaposlenemu res obljubilo tajnost komunikacij, sporno dejanje ne posega v oškodovančevo zasebnost na nepošten način (Sykes, 1999: 141).

Problem nejasne in zastarele zakonodaje pa je postal precej očiten v primeru *U. S. proti Councilman*.[6] Šlo je za primer ponudnika brezplačne elektronske pošte, ki je prestrezal elektronsko pošto svojih uporabnikov (brez njihove vednosti). Podjetje, ki se je sicer ukvarjalo s prodajo rabljenih knjig, je namreč svojim strankam ponudilo brezpla-

[3] Shoars v. Epson America Inc., No. (SWC) II2749 (Cal App. Dep't. Super. Ct. Dec 8, 1992).

[4] Bonita P. Bourke, et. al. v. Nissan Motor Corporation, No. 68-705 (Cal. Ct. App., 1993).

[5] McLaren v. Microsoft, No. 05-97-00824 (Tex. Ct. App. 28. maj, 1999).

[6] United States of America v. Bradford C. Councilman, No. 03-1383 (1st Cir., June 29, 2004).

čne poštne predale, nato pa prestrezalo elektronsko pošto, ki so jo njihove stranke prejemale od konkurenčne prodajalne knjig, podjetja Amazon. Prestrezanje so izvajali misleč, da je na podlagi ECPA zakonito. S tem je podjetje hotelo ugotoviti, katere knjige njihove stranke kupujejo pri konkurenci in po kakšnih cenah, posledično pa si pridobiti tržno prednost. Dejstvo je, da je ECPA precej nejasen in 29. junija 2004 ameriško prizivno sodišče prvega okrožja najprej razsodilo, da je takšno prestrezanje elektronske pošte zakonito. Odločitev je bila nato avgusta 2005 revidirana in okrožno sodišče v Massachusettsu je presodilo, da nadzor elektronske pošte v takih primerih ni dovoljen (EPIC, 2005).

Kot torej vidimo, je nadzor komunikacij, zaposlenih v ZDA, precej razširjen, zakonodaja pa nadzor na delovnem mestu v veliki meri dovoljuje. Vendar pa je tovrsten nadzor lahko dvorezen. Posledica pretiranega nadzora je pogosto lahko obravnava posameznikov bolj v smislu nekakšnega inventarja in manj kot avtonomnih človeških bitij. Uporaba elektronskih identifikacijskih kartic je zgolj zunanji znak take obravnave, posegi delodajalcev v telesno zasebnost (urinski, krvni in genski testi) pa odpirajo tudi vprašanja človekovega dostojanstva in avtonomije na delovnem mestu. Nekateri avtorji so mnenja, da vohunjenje za elektronsko pošto zaposlenih uničuje občutek skupnosti na delovnem mestu (Whitaker, 1999: 105), to pa verjetno vpliva tudi na lojalnost podjetju. Zato se upravičeno zastavlja vprašanje ali nadzorovanje zaposlenih sploh dosega svoj cilj – preprečevanje odtekanja informacij – in ali se delodajalci problema lojalnosti zaposlenih morda ne lotevajo na napačen način in z napačnimi sredstvi.

## Evropski pristop

Povsem drugačen pristop do zasebnosti na delovnem mestu pa velja v Evropi. V zvezi z nadzorom na delovnem mestu sta verjetno najpomembnejši odločitvi Evropskega sodišča za človekove pravice *Halford proti Združenemu kraljestvu*[7] iz leta 1997 ter *Copland proti Združenemu kraljestvu*[8] iz leta 2007.

Ga. Halford, uslužbenka policije, je proti svojemu delodajalcu leta 1990 sprožila postopek zaradi diskriminacije na delovnem mestu. V svoji pisarni je imela dva telefona, od katerih je bil eden namenjen za zasebno uporabo, glede uporabe telefonov pa ji niso bile naložene nikakršne omejitve. Halfordova je kasneje ugotovila, da je njen delodajalec nadzoroval telefonske klice iz njenega službenega telefona (pa tudi domačega telefona) in sicer z namenom, da bi zbrali gradivo za svojo obrambo v postopku zaradi diskriminacije. Zadeva je prišla na *Evropsko sodišče za človekove pravice*, ki je presodilo, da je v tem primeru šlo za kršitev 8. člena *Evropske konvencije o človekovih pravicah*.[9] V razsodbi je izrecno zapisalo, da zaposleni na delovnem mestu upravičeno pričakuje zasebnost.

Podobna je bila odločitev tudi v primeru *Copland proti Združenemu kraljestvu*[10] iz leta 2007. V tem primeru je nadrejeni delavke Lynette Copland pregledoval izpiske telefonskih številk, ki jih je klicala med delovnim časom ter sezname spletnih strani, ki jih obiskovala. Nadzor naj bi se vršil z namenom ugotavljanja, ali delavka službena sredstva uporablja za zasebne namene. Da jo nadzorujejo, je ugotovila šele, ko so iz njenega podjetja kontaktirali njeno pastorko ter jo vprašali, zakaj pošilja elektronsko pošto na službeni e-poštni naslov Coplandove. Tudi ta primer je prišel na *Evropsko sodišče za človekove pravice*, ki je leta 2007 presodilo, da je tudi v tem primeru šlo za kršitev 8. člena *Evropske konvencije o človekovih pravicah*[11] in da je torej delodajalec neupravičeno posegal v njeno zasebnost.

*Evropsko sodišče za človekove pravice* je v primeru presodilo, da varstvo zasebnosti velja tako za telefonske komunikacije, kot tudi za elektronsko pošto in uporabo interneta, in da je iz stališča varstva zasebnosti irelevantno ali gre za zasebno ali za službeno komunikacijsko sredstvo. Prav tako so presodili, da kršitev predstavlja že samo zbiranje in obdelava prometnih podatkov in s tem potrdili, da so prometni podatki inte-

---

[7] Halford v. Velika Britanija, odločba z dne 25. 6. 1997.

[8] Copland v. Velika Britanija, odločba z dne 3. 4. 2007.

[9] Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin, spremenjena s protokoli št. 3, 5 in 8 ter dopolnjena s protokolom št. 2, ter njeni protokoli št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, »Mednarodne pogodbe«, št. 7/1994, 13. 6. 1994. Konvencijo je državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6.1994.

[10] Copland v. Velika Britanija, odločba z dne 3. 4. 2007.

[11] Glej op. 9.

gralni element komunikacij. Kršitev zasebnosti torej ni »le« vpogled v vsebino komunikacij, pač pa tudi vpogled v prometne podatke. Nadalje so v razsodbi zapisali, da je iz stališča varstva zasebnosti irelevantno ali so bili podatki »zgolj« zbrani, ali pa so bili tudi razkriti tretjim osebam oziroma uporabljeni proti pritožnici. S tem so se postavili na stališče, da je sporen že sam akt posega, ne pa šele morebitni kasnejši pregled oziroma obdelava prestreženih podatkov in komunikacij s strani tretje osebe. Pomemben element sodbe je bilo tudi dejstvo, da delavka ni bila vnaprej opozorjena, kdaj in v kakšnih primerih lahko delodajalec nadzira elektronsko pošto zaposlenih in je zato po mnenju sodišča lahko upravičeno pričakovala zasebnost na svojih službenih komunikacijskih sredstvih.

Evropski pristop k varovanju komunikacijske zasebnosti se kaže tudi v nekaterih drugih primerih. *Evropsko sodišče za človekove pravice* je leta 1998 v primeru *Lambert proti Franciji*[12] jasno poudarilo, da glede tajnosti komunikacij ni razlike med lastnim telefonskim priključkom ali telefonskim priključkom tretje osebe, istega leta pa v primeru *Kopp proti Švici*[13] tudi, da so zaščiteni tudi klici iz poslovnih prostorov ter v poslovne prostore.

Zanimiva je tudi razsodba (in predvsem njena utemeljitev) *Kasacijskega sodišča Francije* v primeru *Societe Nikon France, SA v. Onof*[14] št. 99–42.942 iz leta 2001. V tem primeru je namreč delodajalec preiskal računalnik zaposlenega, zaradi suma, da leta krši konkurenčno prepoved. V okviru preiskave je delodajalec pregledal in prekopiral dve mapi na računalniku zaposlenega (označeni z imenom »osebno« in »fax«), pri čemer so ugotovili, da je zaposleni uporabljal računalnik za neslužbene namene in kršil konkurenčno prepoved, čeprav je bilo to z notranjimi pravili organizacije prepovedano. Na podlagi tega so ga odpustili.

Zaposleni se je pritožil, in *Kasacijsko sodišče Francije* je presodilo, da ima delavec tudi med delovnim časom in na delovnem mestu pravico do zasebnosti in tajnosti komunikacij. Pri tem so izrecno zapisali, da:

»*delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema preko službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen Evropske konvencije o človekovih pravicah ... To velja ne glede na to, ali je bil delavec vnaprej seznanjen, da službenega računalnika ne sme uporabljati v neslužbene namene... Podjetje ali druge ustanove ne smejo biti mesta, kjer bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, kjer temeljne človekove pravice nimajo veljave ... Menimo, da je splošna popolna prepoved uporabe e-pošte v neslužbene namene nerealna in krši pravno načelo sorazmernosti.*« (Klemenčič, 2002: 402.)

Odločitev kaže na to, da – kot ugotavlja Klemenčič – »*se domet pravice do komunikacijske zasebnosti ne ustavi zgolj pri zagotavljanju zaupnosti vsebine sporočanja in podatkov, povezanih z njo, ampak hkrati prepoveduje tudi nesorazmerne prepovedi komuniciranja z zunanjim svetom*« (Klemenčič, 2002: 395). Dejstvo namreč je, da

[12] Lambert v. Francija, odločba z dne 24. 8. 1998.

[13] Kopp v. Švica, odločba z dne 25. 3. 1998.

[14] Societe Nikon France v. M. Onof, Cass. soc., 2. oktober 2001, Bull Civ. V, No. 291.

*Priporočilo Sveta Evrope št. R(89) 2*[15] določa, da imajo zaposleni na delovnem mestu pravico do vzpostavljanja osebnih in socialnih stikov. Podobno stališče je zavzelo tudi *Evropsko sodišče za človekove pravice* v primeru *Niemietz proti Nemčiji*[16] leta 1992, ko je zapisalo da mora »*spoštovanje zasebnega življenja vsebovati tudi določeno stopnjo pravice do vzpostavljanja in razvijanja odnosov z drugimi človeškimi bitji*«. Ter: »*poleg tega se zdi, da ni načelnega razloga, zakaj bi ta pojem 'zasebnega življenja' izključeval profesionalne ali poslovne dejavnosti [posameznika]...*«

Podobno stališče glede omejitev nadzora na delovnem mestu je Kasacijsko sodišče Francije zavzelo tudi v primeru *Philippe K. v. Cathnet*-Science.[17] V primeru je delodajalec na mizi zaposlenega po naključju našel erotične fotografije, zaradi česar so posumili, da ima zaposleni na računalniku shranjene pornografske vsebine. Sledila je preiskava računalnika, na katerem so res našli pornografske vsebine in posledično zaposlenega odpustili. Nižja sodišča so odločitev delodajalca podprla, *Kasacijsko sodišče Francije* pa je presodilo, da sum prisotnosti pornografije na računalniku ne predstavlja opravičljivega razloga za preiskavo (Cate, 2007).

Vse to kaže na to, da evropska pravna ureditev na delovnem mestu zaposlenemu priznava bistveno širši krog komunikacijske zasebnosti kot ameriška pravna ureditev, hkrati pa tudi prepoveduje pretirano omejevanje komunikacij z drugimi. Glede nadzora komunikacij na delovnem mestu tako velja, da mora biti zaposleni vnaprej seznanjen s pravili delodajalca glede uporabe telefona, elektronske pošte in interneta, hkrati pa si delodajalec ne more privoščiti pretiranega omejevanja pravice do zasebnosti in pravice do komunikacije z zunanjim svetom.

Praviloma tudi velja, da se mora zaposleni z nadzorom strinjati oziroma mora biti nadzor objektivno opravičljiv in sorazmeren. Glede strinjanja velja poudariti, da je zaposleni nasproti delodajalcu seveda v podrejenem položaju, zato mora biti strinjanje prostovoljno in brez prisile. *Article 29 Working Party* je tako v svojem mnenju *Opinion 8/2001* iz septembra 2001 zapisala, da »*če zaposleni nima možnosti, da [obdelavo osebnih podatkov] zavrne, to ni soglasje. Soglasje mora biti vedno prostovoljno. Torej mora imeti zaposleni tudi možnost preklicati soglasje brez negativnih posledic*« (Article 29 Working Party, 2001).

Po mnenju *Article 29 Working Party* je obdelava osebnih podatkov zaposlenega objektivno opravičljiva le na primer zaradi izpolnjevanja pogodbenih obveznosti oziroma spoštovanja zakonskih zahtev (na primer obdelava osebnih podatkov o plačah, posredovanje podatkov davčni upravi), zaradi zasledovanja zakonitih interesov delodajalca, razen kadar taki interesi ne prevladajo nad temeljnimi pravicami zaposlenega (potrebno je torej najti ravnovesje med interesi delodajalca in zaposlenih) ali na primer zaradi zagotavljanja vitalnih interesov zaposlenega (na primer zagotavljanje varnosti pri

[15] Svet ministrov Sveta Evrope. 1989. Priporočilo Sveta Evrope št. R(89) 2 o varstvu osebnih podatkov, uporabljanih za zaposlovanje (Recommendation No. R (89) 2 on the protection of personal data used for employment purposes), sprejeto 18 januarja 1989.

[16] Niemietz v. ZR Nemčija, odločba z dne 16. 12. 1992.

[17] Philippe K. v. Cathnet-Science, Cour de Cassation, Chambre Sociale, Arret No. 1089 FS-P+B+R+1, Pourvoi No. J-03-40.017, 5/17/05.

delu). Omejevanje pravice do zasebnosti na delovnem mestu je torej mogoče le izjemoma (Article 29 Working Party, 2001).

Velja tudi poudariti, da vse navedeno ne velja le za vsebino komunikacij, pač pa tudi za obravnavo prometnih podatkov (podatkov o klicih oziroma prejemnikih sporočil, in vseh drugih podatkov, ki ne predstavljajo vsebine komunikacije). Evropska pravna ureditev namreč prometne podatke obravnava precej drugače kot ameriška pravna ureditev. *Vrhovno sodišče ZDA* je tako leta 1979 v primeru *Smith proti Maryland*[18] presodilo, da prometni podatki o telefonskih pogovorih niso zaščiteni s Četrtim amandmajem ameriške ustave,[19] s čimer so uvedli ločevanje prometnih podatkov od same vsebine komunikacije. Drugačno stališče pa je zavzelo *Evropsko sodišče za človekove pravice*, ki je v primeru *Malone proti Veliki Britaniji*[20] leta 1984 presodilo, da so prometni podatki integralni element telefonskih komunikacij in kot taki tudi uživajo pravno varstvo.

Poleg tega pa je potrebno izpostaviti še dejstvo, da nadzor s strani delodajalca lahko predstavlja tudi kršitev interesa t. i. tretjih oseb, torej oseb, ki komunicirajo z zaposlenim in morda niti ne vedo, da gre za službeno komunikacijsko sredstvo ter da delodajalec nadzoruje komunikacije zaposlenega, s katerim so v stiku (Klemenčič, 2001: 188–189). Ta problem je zelo očiten pri morebitnem nadzorovanju službenih mobilnih telefonov, kjer je možnosti za razlikovanje med službenim in zasebnim komunikacijskim sredstvom še manj.

[18] Smith v. Maryland, 242 U.S. 735 (1979).

[19] 4. amandma, Listina svoboščin (*Bill of Rights*), 1791.

[20] Malone v. Velika Britanija, odločba z dne 02. 08. 1984.

## Zasebnost na delovnem mestu v Sloveniji

Podoben odnos do zasebnosti na delovnem mestu kot ga ima *Evropsko sodišče za človekove pravice*, ima tudi slovenska pravna ureditev. Vendar pa ima slovenski pravni red neko specifiko, zaradi katere je komunikacijska zasebnost v Sloveniji še nekoliko bolj zaščitena kot na splošno v Evropi. Ustava RS namreč v 37. členu določa, da »*samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo, ali potek kazenskega postopka ali za varnost države.*«[21]

Slovenska ustava torej za posege v komunikacijsko zasebnost zahteva ustrezno zakonsko podlago in predvsem sodno odredbo. Oktobra 2008 je tako *Ustavno sodišče* v razsodbi Up-106/05[22] presodilo, da poseg v svobodo komuniciranja ni dovoljen brez predhodnega dovoljenja sodišča. V primeru je sicer šlo za preiskavo zakonito zasežene mobilnega telefona in SIM kartice v kazenskem postopku brez (dodatne) odredbe sodišča. V razsodbi je *Ustavno sodišče* poudarilo tudi stališče, da je treba predmet varstva komunikacijske zasebnosti razlagati širše, in sicer tako, da le-ta vključuje tudi prometne podatke, ki so sestavni del komunikacije.

Visoke standarde za posege v zasebnost je *Ustavno sodišče* postavilo tudi v odločbi Up-472/02[23] iz oktobra 2004. Šlo je za odločanje v primeru snemanja pogovora s strani zasebnika in uporabi tega posnetka v poznejšem civilnem sodnem postopku. Sodišče je v odločitvi zapisalo:

»*Poseg v pravico do zasebnosti bi bil pod določenimi pogoji dopusten, vendar bi morale biti v pravnem postopku za izvedbo dokaza, pridobljenega s kršitvijo pravice do zasebnosti, posebej utemeljene okoliščine. Izvedba takega dokaza bi morala imeti poseben namen za izvrševanje neke ustavno zavarovane pravice. V takem primeru mora sodišče upoštevati načelo sorazmernosti in skrbno prisoditi, kateri pravici je treba dati prednost.*«[24]

Po mnenju sodišča namreč:

»*Posnetka oziroma tonskega zapisa telefonskega pogovora tudi ni mogoče enačiti z zapiski o pogovoru. Gre namreč za bistveno kakovostno razliko... Kot je bilo že poudarjeno, daje tonski zapis oblast nad tujo osebo oziroma njeno osebno dobrino, ker omogoča ponovitev (vnovično predvajanje). Če je torej to storjeno brez vednosti prizadete osebe, je s tem poseženo v izključno pravico osebe, da sama razpolaga s svojo besedo oziroma z glasom.*«.[25]

Slovenska sodna praksa se tako praviloma postavlja na stran posameznika, kar kaže tudi odločitev Upravnega sodišča RS, s katero je le-to zaposlenemu priznalo pravico do varstva zasebnosti pri uporabi službenih mobilnih telefonov (Klemenčič, 2003: 137). V

---

[21] Ustava Republike Slovenije, Uradni list RS, št. 33/91-I, 42/97, 66/2000, 24/03, 69/04 in 68/06.

[22] Odločba Ustavnega sodišča RS, št. Up-106/05, Uradni list RS, št. 100/2008.

[23] Odločba Ustavnega sodišča RS, št. Up-472/02, Uradni list RS, št. 114/2004.

[24] *Ibidem*.

[25] Odločba Ustavnega sodišča RS, št. Up-472/02, Uradni list RS, št. 114/2004.

razsodbi U702/99[26] je *Upravno sodišče* presodilo, da se varstvo zasebnosti, zagotovljeno v 37. členu Ustave RS,[27] nanaša tudi na službene telefone, pridobitev in uporaba izpiskov telefonskih klicev službenega telefona pa predstavlja kršitev. V obrazložitvi sodbe so zapisali:

»*Sodišče je glede na ugovor tožene stranke, da je šlo za službene telefone, ugotovilo, da pojem tajnosti pisem in drugih občil zajema tako zasebne kot tudi službene komunikacije. Zaupnost razmerij, v katere vstopa posameznik, ne more biti uporabljena kot kriterij, ki bi določal obseg zaščite komunikacijske zasebnosti. ... Pojem zasebno življenje torej vsebuje tako zasebne kot tudi službene telefonske linije, zaradi česar ni pomembna lastnina ali pripadnost določenega telekomunikacijskega sredstva. To varstvo je dano vsem osebam in ni mogoče slediti navedbi tožene stranke, da to ne velja za tožnike, ki so uporabljali mobilne telefone v lasti tožene stranke. Lastninski koncept zasebnosti, to je pristop z vidika dejstva, čigavo je komunikacijsko sredstvo, ki je bilo nadzirano, ni relevanten. Tudi Ustava RS ne ločuje zasebnosti v zasebni in službeni sferi.*«[28]

Glede obsega pravice do zasebnosti na delovnem mestu je sicer jasno, da je odvisen tako od delovnih nalog, ki jih zaposleni opravlja (na primer rokovanje s tajnimi podatki, itd.) in zahtev delovnega mesta (po na primer varovanju poslovnih skrivnosti), za nadzor pa je bistveno, da je transparenten in sorazmeren. Nadzor komunikacij zaposlenega zaradi ugotavljanja ali zaposleni morda ne »zapravlja« časa podjetja za zasebne namene ni ne sorazmeren, ne potreben. Za odpoved pogodbe o zaposlitvi namreč zadostuje že to, da delavec ni opravil dodeljenih nalog. Ali jih ni opravil zaradi pretirane uporabe interneta, elektronske pošte in telefona v neslužbene namena ali pa iz drugih razlogov, pa je ob vsem skupaj povsem irelevantno.

Ob tem določene posege v zasebnost – tudi na delovnem mestu – sankcionira in prepoveduje tako kazenska, kot tudi zakonodaja, ki se nanaša na varstvo osebnih podatkov.

---

[26] Sodba Upravnega sodišča št. U 702/99 z dne 21. 3. 2000.

[27] Ustava Republike Slovenije, Uradni list RS, št. 33/91-I, 42/97, 66/2000, 24/03, 69/04 in 68/06.

[28] Sodba Upravnega sodišča št. U 702/99 z dne 21. 3. 2000.

## Sklep

Pri vprašanju zasebnosti na delovnem mestu prihaja do trka lastninske pravice delodajalca in pravice do zasebnosti zaposlenega. Evropska pravna praksa se je postavila na stališče, da lastninska pravica ne prevlada samodejno nad pravico do zasebnosti, kar pomeni, da je pravico do zasebnosti potrebno (vsaj do določene mere) spoštovati tudi na delovnem mestu. Seveda pa je jasno, da tudi pravica do zasebnosti ni absolutna in tudi ta ne more prevladati nad lastninsko pravico delodajalca. Pomembni pa so tudi družbeni in psihološki vidiki. Pretiran nadzor namreč lahko omejuje kreativnost, motivacijo in lojalnost zaposlenega, zato na določeni točki lahko postane celo kontraproduktiven.

Ravno zaradi kolizije zgoraj omenjenih pravic pa je jasno, da bo vprašanje zasebnosti na delovnem mestu v prihodnosti sprožalo še številne polemike. Na to nakazuje tudi v začetku leta 2009 na Finskem sprejeta novela zakona o varstvu podatkov in elektronskih komunikacij,[29] ki delodajalcem v primeru suma kraje poslovnih skrivnosti daje pravico, do vpogleda v prometne podatke službene elektronske pošte zaposlenih (European Digital Rights, 2008). Zakon je že v fazi predloga požel precej kritik, številni pravni strokovnjaki pa so mnenja, da je protiustaven in morda tudi v neskladju z *Evropsko konvencijo o človekovih pravicah*.[30] Posegi v zasebnost morajo namreč imeti ustrezno zakonsko podlago, hkrati pa morajo biti tudi nujni v demokratični družbi oziroma sorazmerni. In ravno vprašanja sorazmernosti, ter soglasja zaposlenega oziroma prisile delodajalca so tista, ki bodo v prihodnosti zakoličila obseg pravice do zasebnosti na delovnem mestu.

[29] Novela zakona je znana tudi pod imenom »Lex Nokia«. Za sprejem zakona naj bi namreč lobiralo podjetje Nokia, ki pa je to zanikalo.

[30] Glej op. 9.

# Viri in literatura


1. ACLU (2003). **Privacy in America: Electronic Monitoring**. Po URL: http://www.aclu.org/Privacy/Privacy.cfm?ID=14170&c=132, dostop 19. 4. 2005.
2. Bogataj, M. (ur.) (2003). **Internet in pravo**. Ljubljana: Pravna fakulteta.
3. Cate, H. F. (2007). European Court of Human Rights Expands Privacy Protections: Copland v. United Kingdom. **ASIL Insights**, let. 11, izdaja 21, 6. avgust. Po URL: http://www.asil.org/insights070806.cfm, dostop 28. 10. 2009.
4. EPIC (2005). **United States v. Councilman**. Po URL: http://epic.org/privacy/councilman/, dostop 1.10. 2009.
5. European Digital Rights (2008). Snooping law, »Lex Nokia«, proceeding slowly but surely in Finland. **EDRi-gram**, št. 6.24, 17. december 2008. Po URL: http://www.edri.org/edri-gram/number6.24/nokia-law-finland-snooping, dostop 20. 10. 2009.
6. Klemenčič, G. (2001). Varstvo elektronske zasebnosti. V: M. Potrč (ur.), **Internet in pravo**, Ljubljana: Pasadena, s. 129–191.
7. Klemenčič, G. (2002). 37. člen (varstvo tajnosti pisem in drugih občil). V: L. Šturm (ur.), **Komentar ustave republike Slovenije**, Ljubljana: Fakulteta za podiplomske državne in evropske študije, s. 391–408
8. Klemenčič, G. (2003). Internet in pravica do zasebnosti. V: M. Bogataj (ur.), Internet in pravo, Ljubljana: Pravna fakulteta, s. 101–141.
9. Potrč, M. (ur.) (2001). **Internet in pravo**. Ljubljana: Pasadena.
10. Schulman, A. (2001). **The Extent of Systematic Monitoring of Employee E-mail and Internet Use**. Po URL: http://www.sonic.net/~undoc/extent.htm, dostop 17. 1. 2004).
11. Sinrod, J. E. (2004). **E-Legal: Employer Access to Employee E-Mails**. Law.com, 27. januar. Po URL: http://www.duanemorris.com/articles/print/article1479. pdf, dostop 11. 6. 2004.
12. Sykes, J. C. (1999). **The End Of Privacy**. New York: St. Martin's Press.
13. Šturm, L. (ur.) (2002). **Komentar ustave republike Slovenije**. Ljubljana: Fakulteta za podiplomske državne in evropske študije.
14. Whitaker, R. (1999). **The End of Privacy**. New York: The New Press.


***Pravni dokumenti ZDA***


1. 4. amandma, Listina svoboščin (Bill of Rights), 1791.
2. Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986).
3. Bonita P. Bourke, et. al. v. Nissan Motor Corporation, No. 68-705 (Cal.Ct.App.1993).
4. McLaren v. Microsoft, No. 05-97-00824 (Tex. Ct. App. 28. maj, 1999).
5. Smith v. Maryland, 242 U.S. 735 (1979).
6. Shoars v. Epson America Inc., No. (SWC) II2749 (Cal App. Dep't. Super. Ct. Dec 8, 1992).
7. United States of America v. Bradford C. Councilman, No. 03-1383 (1st Cir., June 29, 2004).

***Odločitve Evropskega sodišča za človekove pravice***

1. Copland v. Velika Britanija, odločba z dne 3. 4. 2007.
2. Halford v. Velika Britanija, odločba z dne 25. 6. 1997.
3. Kopp v. Švica, odločba z dne 25. 3. 1998.
4. Lambert v. Francija, odločba z dne 24. 8. 1998.
5. Malone v. Velika Britanija, odločba z dne 02. 08. 1984.
6. Niemietz v. ZR Nemčija, odločba z dne 16. 12. 1992.

***Odločitve Kasacijskega sodišča Francije***

1. Philippe K. v. Cathnet-Science, Cour de Cassation, Chambre Sociale, Arret No. 1089 FS-P+B+R+1, Pourvoi No. J-03-40.017, 5/17/05.
2. Societe Nikon France v. M. Onof, Cass. soc., 2. oktober 2001, Bull Civ. V, No. 291.

***Dokumenti Sveta Evrope***

1. Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin, spremenjena s protokoli št. 3, 5 in 8 ter dopolnjena s protokolom št. 2, ter njeni protokoli št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, »Mednarodne pogodbe«, št. 7/1994, 13. 6. 1994. Konvencijo je državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.
2. Svet ministrov Sveta Evrope. 1989. Priporočilo Sveta Evrope št. R(89) 2 o varstvu osebnih podatkov, uporabljanih za zaposlovanje (*Recommendation No. R (89) 2 on the protection of personal data used for employment purposes*), sprejeto 18 januarja 1989.

***Dokumenti EU***

1. Article 29 Working Party on Data Protection. 2001. Opinion 8/2001 on the processing of personal data in the employment context, iz dne 13. septembra 2001. Po URL: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf, dostop 28. 10. 2009.

***Slovenski pravni dokumenti***

1. Ustava Republike Slovenije, Uradni list RS, št. 33/91-I, 42/97, 66/2000, 24/03, 69/04 in 68/06.
2. Sodba Upravnega sodišča št. U 702/99 z dne 21. 3. 2000.
3. Odločba Ustavnega sodišča RS, št. Up-472/02, Uradni list RS, št. 114/2004.
4. Odločba Ustavnega sodišča RS, št. Up-106/05, Uradni list RS, št. 100/2008.

# III. KIBERNETSKA KRIMINALITETA

## 3 Hekerstvo kot izziv in upor

**Marko Rusjan**

### Uvod

V članku skušam prikazati življenje in navade avtohtonih prebivalcev medmrežja hekerjev. Prostor, poimenovan kiberprostor, ki so ga pomagali vzpostaviti, so postopoma kolonizirale horde iskalcev dobička, novih tržnih niš in presežne vrednosti. V tem procesu so se nekateri hekerji odločili za upor, drugi so sprejeli nova pravila in novega gospodarja, tretji so sprejeli nova pravila, vendar ne novega gospodarja, ter stopili na pota prepovedanega služenja denarja.

Kazniva in druga odklonska dejanja niso določena z večnimi Božjimi ali naravnimi zakoni, temveč so določena znotraj vsakokratne družbe. Kiberprostor je področje, ki se stalno spreminja, pravila delovanja so zaradi spremembe tehnologij nestalna in tako lahko na kršitve pozitivnega prava gledamo predvsem s stališča kulturnih, ideoloških, razrednih in ekonomskih bojev akterjev tega prostora. Kiberprostor namreč ni preslikava realnega prostora, temveč vesolje, ki se širi, in katerega kolonizacija (torej vzpostavitev jurisdikcije nad celotnim ozemljem) ni končana.

Hekerji so s strani medijev hkrati glorificirani in demonizirani. Na eni strani imamo podobo dobrih, pridnih, vzornih računalničarjev, ki pomagajo državni oblasti odkrivati njene nasprotnike, ki ogrožajo celotni družbeni red in mir. Po drugi strani pa imamo podobo psihopatskih, na trenutke neracionalnih, na trenutke preračunljivih hekerjev, katerih smisel življenja je greniti naša življenja. Namen članka je prikazati del filozofije hekerjev in njihovega načina delovanja v odnosu do pravnega režima, ki skuša na medmrežju vzpostaviti enaka pravila delovanja, kot so v realnem, materialnem svetu. Za vzpostavljanje teh pravil pa mora država uporabiti svojo represivno moč. Pri tem pa lahko usodno oslabi potenciale informacijske tehnologije.

## Opredelitev hekerstva

Drugi oziroma tretji svet[1] kiberprostor prinaša drugačna »pravila igre« kot smo jih vajeni iz vsakdanjega življenja v fizičnem svetu. Svet, ki ga je ustvarila povezava osebnih računalnikov v svetovno mrežo, ponuja neštete možnosti in prinaša s tem tudi veliko nevarnosti. Sovpada s pojavom globalnega gospodarstva,[2] ki se je razvilo v drugi polovici 20. stoletja. Primerno poimenovana ekonomija je svojo manifestacijo dobila z oblikovanjem ločenega borznega indeksa za informacijske tehnologije *Nasdaq* na njujorški borzi. Kiberprostor pa ni samo prostor, podvržen tržnim zakonitostim. Njegov nastanek ni oblikoval trg, temveč želja strokovnjakov po sodelovanju na daljavo in čim hitrejšemu izmenjevanju podatkov.[3] Kiberprostor je tako predvsem prostor skupnosti, v katerih se srečujejo realne in izmišljene identitete. Šele v drugi fazi se začne komercializacija interneta. In prav ta prevladujoča tendenca po ureditvi prostora, ki bi bil predvsem trg in šele nato vse drugo, skuša postaviti svoja pravila, pisana po nareku velikih korporacij, ki skušajo monopolizirati del kiberprostora. Preoblikovanje kiberprostora v »veliko nakupovalno središče« šele omogoča večanje razsežnosti pojava kiberkriminalitete.

Pred vsemi temi procesi pa je hekerstvo, ki ni samo produkt nastanka kiberprostora, temveč je soudeleženo pri njegovem nastanku. Preden lahko začnemo razpravljati o hekerstvu kot početju, ki stopica po tenki meji med pravnim in protipravnim, moramo definirati to početje. Le ob zamejitvi tega pojma lahko ustrezno opredelimo njegove značilnosti, preteklost in prihodnost. Wang v *Steal this computer book 4.0* smatra, da je hekerstvo obstajalo že pred pojavom računalnika in da lahko pod hekerstvo uvrstimo tudi vdiranje v zapuščene hiše ali prisluškovanje telefonom. Hekanje tako ni samo manipulacija računalnikov, temveč se lahko izvaja na različne načine. Hekanje vključuje analizo sistema, da spoznamo njegovo delovanje, igranje z njim, da se ga naučimo nadzorovati in v zadnjem stadiju sistem tako zmanipulirati, da prevzamemo nadzor nad njim.

Heker je največkrat označen za nevarnega posameznika, ki s svojim početjem ogroža varnost delovanja interneta in računalniških sistemov. Javna podoba, oblikovana z medijsko histerijo, njeno potrebo po ustvarjanju strahov, je nekakšna Frankensteinova pošast, sestavljena iz podob o »špeglarskih« čudakih, zagrenjenih samotnih volkov,

---

[1] Primernejša se mi zdi oznaka tretji svet, kajti prvi svet je svet resničnega, tega kar dejansko je, neodvisnega od naše zmožnosti zaznavanja, drugi svet je svet zaznavanega v katerem zavestno delujemo, tretji svet pa je svet, ki ga je ustvaril drugi svet.

[2] Globalno gospodarstvo razlikujemo od svetovnega gospodarstva, ki je obstajalo že 500 let. Bistvena značilnost globalnega gospodarstva je sposobnost delovanja kot enota v realnem času v svetovnem obsegu. Največji zagon razvoju je poleg tehnologije dala politika deregulacije in liberalizacije svetovnih trgov.

[3] Charles Herzeld, ki je bil direktor DARPA-a (*Defence Advanced Research Projects Agency*), zanika legendo, da naj bi internet nastal zaradi potrebe po komuniciranju v primeru jedrske vojne. Internet naj bi razvili zaradi potrebe po povezavi z zmogljivimi računalniki, ki jih je bilo v zgodnjih šestdesetih relativno majhno število, veliko raziskovalcev pa je bilo geografsko oddaljenih od njih.

računalniških zasvojencev, ki se želijo maščevati celemu svetu z ustvarjanjem in širjenjem uničujočih virusov. Demonizacija hekerjev je pretvorila popularno podobo norega znanstvenika[4] v podobo bedečega, od ljudi odtujenega računalničarja, ki ima raje stroje kot ljudi. Tako kot se je spreminjala podoba kiberprostora z nezadržno komercializacijo, tako so postajali neodvisni hekerji vedno bolj nepotrebni. Njihova nepotrebnost za delovanje ekonomskega sistema se je pokazala s tem, da so iz dobrih čudakov postali javni škodljivci, poleg tega pa so zaradi domnevne odvisnosti od računalnikov postali tudi predmet medicinalizacije s strani psihiatrije.[5]

Še širša opredelitev hekerstva je v Hekerskem manifestu. Heker je tu predstavljen kot predstavnik novega družbenega razreda, kateremu nasproti stoji razred vektorske elite.[6] Nova ekonomija določa nova razredna razmerja med neposrednimi proizvajalci in lastniki proizvajalnih sredstev. Neposredni proizvajalec je heker, ki svoje delo prodaja vektorskemu razredu.[7] Kvalitativno razliko z industrijskim delavcem predstavlja heker

---

[4] Doba znanstvenega pozitivizma 19. stoletja je prinesla veliko literarnih del, ki opisujejo bolj ali manj posrečene znanstvene poskuse. Privlačnost podobe norega znanstvenika odraža Stevensonova povest o Dr. Jekillu in Mr. Hydu, ko znanstvenikov poskus naredi iz človeka pošast, ki ogroža ostale. Na začetku 21. stoletja je prevladujoča tehnologija informacijska, kar se kaže tudi v popularni kulturi, ki najbolj vpliva na oblikovanje javnih podob in novih stereotipov. Heker tako pridobi različne vloge, od sovražnika človeštva do Robin Hooda informacijske družbe.

[5] Reed prikaže, kako je bila postavljena odvisnost od računalnikov in interneta ob bok klasičnim odvisnostim kot na primer droge, alkohol in novejšim kot je odvisnost od igranja na srečo. Z odvisnostjo se pojmuje obnašanje, ki škodi delovanju racionalnega osebka v družbi. Začetni strah pred računalniki je bil premagan s prepričevanjem uporabnikov, da lahko zmerno in pravilno uporabljamo stroje. Kajti tak način uporabe zagotavlja »neodklonsko« uporabo računalnikov. »Psihologizacija odvisniškega obnašanja in pretvorba uporabe računalnika v komercialne namene za produktivno delo, tržne produkte in aktivne potrošnike. Na primer praksa obravnavanje uporabe računalnika kot zdravstvenega problema in ločitev uporabe računalnika na »zdravo« in »nezdravo« odgovarja ločitvi med upravljanjem s pravicami intelektualne lastnine in računalniškim hekanjem.« Reed, str. 138.

Zanimivo, da edina slovenska ambulanta za zdravljenje odvisnosti, delujoča v okviru Zdravstvenega doma Nova Gorica, zdravi poleg odvisnosti od iger na srečo tudi odvisnost od interneta in odvisnost od glasbe. Izbor zajema sodobne »grešne« aktivnosti, pretirano zadrževanje pri teh opravilih, ki odvrača ljudi od normalnega delovanja v produkcijskih vlogah na delovnem mestu in reprodukcijskih vlogah v družini. Nenazadnje pa tudi od skrbi za duhovno zdravje (*sic*).

[6] Avtor McKenzie sledi Marxovi teoriji o razredni vojni, ki od nastanka razredne družbe predpostavlja konflikt interesov med dvema prevladujočima razredoma, od katerega je eden vladajoči, drugi pa temu podrejen. Razrede določa način produkcije. Prav tako pa je odločilna oblika, ki jo zavzame lastnina. »Ko zasebna lastnina napreduje od zemlje h kapitalu in naprej od informacije, lastnina sama postaja čedalje abstraktnejša. Kapital kot lastnina osvobodi zemljo prostorske fiksiranosti. Informacija kot lastnina osvobodi kapital fiksiranosti na posamezen objekt.« McKenzie, str. 28.

[7] Hek je obstajal že prej, v drugih družbeno ekonomskih ureditvah, vendar šele v informacijski dobi zasede osrednje mesto. »Pod posestniško ali kapitalistično vladavino je svoboden in nekoristen hek zatiran ali marginaliziran, sicer pa ohranja svojo lastno ekonomijo daru. Pod vektorialistično vladavino je hek deležen dejavnega spodbujanja in snubljenja, vendar

v tem, da so njegovi možgani del proizvajalnega sredstva. Ta del proizvajalnega sredstva postaja vedno bolj pomemben v primerjavi s stroji, v našem primeru računalniki in omrežje, s tem pa tudi hekerski razred pridobiva na moči v svoji razredni poziciji proti vektorskemu razredu. Castells[8] meni, da je postal človeški um prvič v zgodovini neposredna proizvajalna sila, ne pa samo bistveni element proizvajalnega sistema.

Za trenutek opustimo obravnavanje hekerskega delovanja v kontekstu dovoljenega in prepovedanega, ne zanima nas pozitivnopravno označevanje posameznih dejanj. Hekerja določa želja po obdelavi informacij, s katerimi dosega različne cilje. Internetni prostor je nastal kot prostor vzajemnega sodelovanja med udeleženci v mreži. Hekerska etična načela so določala prosto izmenjavo informacij in prepoved monopoliziranja znanja. Večina hekerjev je z odporom sprejela novo prakso, ki jo je sprožil Bill Gates, ustanovitelj Microsofta, s sodelavci, ko ni hotel več deliti računalniške kode z ostalimi, ker jo je želel tržiti. Ta nasilni presek z dotedanjo prakso predstavlja izvorni zločin, ki pa s časom postane zakon. Kiberprostor, do tedaj še prostor neomejene svobode in ekonomije daru, začenjajo kolonizirati podjetniki. Kiberprostor doživi ponovitev prvotne akumulacije kapitala, ki jo je realni svet že doživel. Država sledi ekonomizaciji teritorija z uvedbo zakonodaje, ki ščiti na novo postavljeno stanje. Tako za nazaj legalizira prisvojitev skupne lastnine in kriminalizira dotedanje svobodne prakse.[9] Hkrati pa poteka tudi proces digitalizacije vsebin iz realnega prostora, ki so v le tem prostoru že pravno in tudi fizično zaščitene. Vendar pa sam pojav digitalizacije ni tako dramatično nevaren za obstoj kapitalističnega načina produkcije. Prvič, digitalizirani kiberprostor je samo ena dimenzija človekovega bivanja, ki ne more obstati brez realnega materialnega življenja, v katerem deluje vse po starih ekonomskih pravilih omejenosti dobrin, in drugič, kulturne produkte uporablja le del človeštva, kar je posledica neenakomernega gospodarskega razvoja.[10] Kljub temu se kulturna industrija sooča z nevarnostjo izgubo dobička, kajti digitalizirane dobrine so zaživele svoje svobodno življenje, katerih reprodukcija je neobvladljiva. Sistem sicer lahko tehnično nadzoruje ves promet na medmrežju, ne more pa preprečiti dogajanja brez radikalnega posega v samo delovanje medmrežja ali pa z radikalno punitivno politiko, ki bi s pomočjo splošne prevencije učinkovala na obnašanje uporabnikov medmrežja.

V kiberprostoru pa to blago z dematerializacijo izgubi fizično zaščito in njeno nematerialno obliko lahko ščiti samo še pravo. In na teh mejnih točkah prihaja do pravnih spopadov med predstavniki kulturne industrije, ki skuša s pomočjo avtorskih pravic akumulirati kapital, in hekerji ter tehnološke industrije na drugi strani, ki skušajo

---

samo pod predznakom poblagovljene proizvodnje. Za hekerja je tragedija prvega v tem, da je zapostavljen, in tragedija drugega v tem, da ni zapostavljen.« McKenzie, str. 94.

[8] »Nove informacijske tehnologije niso samo orodja za uporabo, temveč tudi procesi, ki se jih razvija. Uporabnik in izdelovalec je lahko hkrati v eni osebi. Tako lahko uporabniki prevzamejo nadzor nad tehnologijo kot je to v primeru interneta.« Castells, str. 31.

[9] Takšna je praksa proste izmenjave datotek s pomočjo programskih orodij.

[10] Po nekaterih marksističnih teorijah je neenakomerna razvitost nujna za delovanje kapitalističnega sistema, saj omogoča ustvarjanje dobička na račun cenovnih razlik delovne sile in surovin med različno razvitimi področjih. Primerjaj teorijo svetovnega sistema, teorijo akumulacije kapitala Rose Luxemburg, teorijo imperializma V.I. Lenina.

čim bolje izkoristiti možnosti nove tehnologije. Prvi za svoje osebne koristi in zanimanja, drugi za svojo akumulacijo kapitala. Spopad pa se ne odvija samo v okviru pravnega diskurza na sodiščih, temveč tudi na političnem polju.[11]

Spopad pa odloča, kakšna bo ureditev interneta. Ali bo struktura medmrežja ostala nehierarhična in necentralizirana, univerzalna in odprta? Ali pa bo vedno bolj omejena, kot kažejo znaki od kitajskega velikega požarnega zidu, do načrtov vojske ZDA za bojne spopade v kiberprostoru in do razvoja večtirnega omrežja, ki bo privilegiral promet korporacij, ki bodo pripravljene plačati več, medtem ko bodo ostali na ta račun počasnejši.

Za potrebe tega prispevka pa je najpomembnejša opredelitev kazenskega prava do hekerstva, kje so tisti preseki, ki določajo hekerstvo kot protipravno delovanje. Predvsem pa, ali hekerstvo vstopa na področje prepovedanega, ali pa se prepovedano širi na področje delovanja hekerstva, s procesom, ki ga imenujemo kriminalizacija. Nenazadnje pa tudi, koliko se sploh uspe kazensko pravo prilagajati spremembam, ki jih povzroča nova tehnološka revolucija. Če sprejmemo tezo, da kazensko pravo predvsem izvršuje želje in potrebe družbenega sistema, ki le-to potrebuje za sankcioniranje in preprečevanje motečih dejanj, potem gre tudi za vprašanje, kako se odziva kapitalistični gospodarski sistem na tehnološke spremembe.[12]

Problem uvrstitve hekerstva med škodljive ali koristne prakse Wall[13] razreši z delitvijo na »dobre« in »slabe« hekerje, ki naj bi jih določalo njihov namen in posledice njihovega delovanja. Tako naj bi dobri (angl. *white hats*) hekerji z vdori le širili svoje znanje in pomagali pri odpravi varnostnih lukenj. Tako se tudi izboljšujejo odprtokodni programi, kot je na primer spletni brskalnik Firefox. Na nasprotni strani pa slabi hekerji (angl. *black hats*) skušajo poškodovati sisteme ali pa se finančno protipravno okoristiti. Wall tako raje uporabi termin *crack* za zlonamerni *hack*. Z uporabo tega termina strogo loči med obema praksama. Kljub temu pa ostajajo sive cone, v kateri se gibljejo hekerji, ki v imenu »Dobrega« napadajo »Zlo«. Z napadom na državni strežnik države, ki doka-

---

[11] Junija 2009 je bil prvič izvoljen predstavnik švedske Piratske stranke v Evropski parlament. Uspeh je bil spodbujen tudi z nedavno odločitvijo švedskega sodišča o kaznovanju švedskega spletnega portala *Pirate Bay* zaradi kršenja avtorskih pravic. *Pirate Bay* je spletni portal, ki omogoča iskanje torrentov, s pomočjo katerih poteka izmenjava datotek preko interneta. Odločitev je razdelila švedsko javnost, še toliko bolj, ko je kasneje postalo v javnosti znano, da je sodnik, ki je odločal v zadevi, povezan z organizacijami, ki se borijo za večjo zaščito avtorskih pravic. Vprašanje pa je, koliko gre v primeru tega volilnega uspeha za glasove protesta, koliko pa za dejansko podporo politični usmeritvi, ki daje večji pomen svobodi na internetu kot pa zaščiti avtorskih pravic. Dodatno kompleksnost situacije predstavlja tudi profitna (oziroma bolje ne - neprofitna) usmerjenost portala *Pirate Bay* in vrednostna ter ideološka heterogenost Piratske stranke. Več o teh vprašanjih primerjaj Söderberg.

[12] Če sprejmemo Marxovo tezo, da je pravni red del družbene nadstavbe, produkcijska razmerja pa so del družbene baze, potem mora biti pravni red pravi odraz razmerij med produkcijskimi faktorji, delom in kapitalom. Če pa pravni red zaostaja za spremembami v produkcijskih razmerjih, kot se to kaže prav na področju nematerialne ekonomije, ki ne pozna več klasičnih reprodukcijskih problemov in omejenosti dobrin, potem vladajoči razred s pomočjo ideologije vsiljuje lažne vrednote in pravne norme. Podrobneje glej Poulantzas, str. 31.

[13] Wall.

zano sistemsko krši človekove pravice, skuša heker opozoriti na zločine, ki jih izvaja država, hkrati pa sam krši zakonodajo in povzroča škodo. Ali je takšen heker beli ali črni klobuk? Kiberprostor presega državne meje in državno jurisdikcijo, zato je vrednotenje etičnosti delovanja v njem nemogoče oceniti v razmerju do pozitivnega prava, kajti legitimnost tega prava ni povsod enaka. Poleg tega se Evropejcu lahko zdijo pozitivne pravne norme nekje v Aziji krivične in jih tudi zaradi tega ne upošteva. In obratno seveda.[14]

Opredeliti je potrebno tudi motiv hekerjev za njihovo delovanje. Anketa, ki so jo opravili raziskovalci med izraelskimi hekerji, je pokazala, kateri so najpogostejši vzroki za njihovo delovanje (od najpogostejšega do najredkejšega odgovora): 1) zabava, vznemirjenje, 2) radovednost, 3) računalniško znanje, 4) ekonomski razlogi (ideološko nasprotovanje, pomanjkanje denarja, denarna nagrada), 5) verjetnost kazenskega pregona, 6) pomanjkanje škodljivih namenov, 7) nezavedanje kršitev, 8) voyeurizem, 9) maščevanje in 10) preprostost dejanja.[15] Hekerji so večinoma mladi moški, ki ljubijo nove izzive in tvegano početje. Pri tem se ne razlikujejo veliko od povprečnega storilca kaznivih dejanj. Niti se njihove vrednote in težnje razlikujejo veliko od vrednot in želja sodobne družbe. Želja po zabavi,[16] odkrivanje novosti, notranje zadovoljstvo so enake tako pri hekerjih kot pri ostalih. Razlika je le v področju delovanja, ki pri hekerjih pomeni kršenje pravnih norm. Toda ravno tem pravnim normam hekerji odrekajo legitimnost. Internet je dojet kot območje popolne svobode, v katerem ne sme biti ovir za hekerja. Kršenje omejitev je izziv, ki se mu je težko upreti. Heker se norčuje iz tehnoloških in pravnih ovir, ki jih postavljajo podjetja in državni organi. Vznemirjenje ob tovrstnem početju se dopolnjuje tudi z načelnim nasprotovanjem zapiranja sistemov zaradi zasebnosti ali zavarovanja dobička podjetij.

In nenazadnje je hekerstvo parazitska dejavnost, ker zahteva gostujoči sistem, v katerem lahko deluje. Ker pa je heker parazit, samo izkorišča delovanje sistema in možnosti, ki jih le ta ponuja. Hkrati pa ne sodeluje pri delovanju in nadgradnji sistema, kot to počnejo nekdanji hekerji, ki so začeli svoje usluge prodajati industriji, in ki jih Taylor imenuje *microserfs*.[17]

---

[14] Medtem ko morajo biti pravila za nemoteno delovanje svetovnega medmrežja enotne, pozitivno materialno pravo posamezne države ohranja svoje specifičnosti. Različne tradicije tako vplivajo na različno ureditev spornih ravnanj. Ob tem pride do kulturnih in vrednostnih konfliktov. In tudi do konflikta med načelom univerzalnosti človekovih pravic in načelom multikulturnosti. Konec koncev določene države ne priznavajo obstoja določenim spletnim stranem in jih s pomočjo cenzure naredijo nedostopne za svoje državljane. Najboljša tehnična orodja je na tem področju razvila Kitajska.

[15] Podrobneje Turgeman – Goldschmidt, str. 12-18.

[16] Hekerstvo obravnava tudi teorija igre, ki smatra, da je delovanje hekerjev kot igra, ki poteka na internetu. Elementi igre kot so gibanje, pretočnost, spremembe in nepredvidljivost so prisotni v zavesti hekerjev.

[17] Taylor uporablja ta termin za označevanje hekerjev, ki deluje s komercialnimi nameni, največkrat za večja podjetja. Povzel ga je po romanu Douglasa Couplanda Microserfs, ki opisuje delo pri Microsoftu. Taylor, str. 629.

## Pojavne oblike hekerstva

Hekerskih oblik delovanja je ogromno, težko bi vse našteli, ne da bi ob tem katere od njih tudi izpustili. Hitri razvoj tehnologije nenehno sproža nove variacije hekerskih modus operandi. Pri našem pregledu se bomo osredotočili samo na nekatere najbolj značilne in pomembne.

### Socialni inženiring[18]

Najbolj razširjen in priljubljen način vdiranja v sisteme in protipravno okoriščanje je socialni inženiring. Cilj napada so informacije o osebah, ki nam bodo služile za pridobivanje zaupanja teh oseb, s pomočjo katerih bomo nato lahko prišli v zaščiteni sistem. Na zvit in premišljen način pridemo do želenih informacij. Heker mora pri tem uporabiti svoje znanje o človekovi psihologiji, kajti njegovo poznavanje tehnologije je uporabno šele v naslednji stopnji, ko bo pridobljene podatke uporabil. Izkorišča človeško lastnost, da zaupamo ljudem, ki nam ponudijo pomoč.

Pri socialnem inženiringu je tveganje zelo majhno. Če poskus ni uspešen, samo prekineš zvezo in ni nevarnosti, da bi zaradi tega bil preganjan. Tudi preprečiti je zelo težko. V tem primeru ne pomaga tehnološka zaščita, vse je odvisno od izkušenj, znanja in previdnosti osebja, ki sprejema telefonske klice. Ravno zaradi tega so najbolj na udaru osebe, ki so najmanj tehnično izobražene. Heker napade »šibki člen« in od njega pridobi potrebne podatke, na primer gesla za vstop v sistem, ne da bi žrtev sploh opazila, da je viktimizirana. Napad se tako odvija nevidno, škodo se ugotovi šele kasneje. Ker čas dogodka ni znan, je težko najti sledi do storilca. Dodatna nevarnost je v tem, da žrtev ne ve, da nekdo zlorablja njeno zaupanje in se lahko podobna dejanja ponavljajo.

Napadalec najprej preuči žrtev, da si s pomočjo osebnih podatkov pridobi zaupanje. Priljubljena taktika je *dumpster diving*, brskanje po odpadkih podjetja, v katerih skuša najti heker koristne podatke, ki mu bodo omogočili pridobiti zaupanje cilja napada.

### Hektivizem

Hektivizem je skovanka iz besed hekerstvo in aktivizem. Pomeni družbeno politični aktivizem, ki se poslužuje informacijske tehnologije. Pri tem lahko uporablja zakonita ali pa protipravna sredstva. Paleta ciljev, za katere se različni hektivisti zavzemajo, je mavrična, segajo od komunističnega dojemanja skupne nematerialne lastnine in liberalističnega pogleda na svobodo delovanja na internetu do islamistične in neonacistične propagande na drugi strani.[19] Aktivisti so lahko že brez hekerstva

[18] Socialni inženiring kot prakso hekerjev moramo ločiti od socialnega inženiringa državnih oblasti, ki so z njegovo pomočjo skušale oblikovati novo družbo drugačnih, spremenjenih posameznikov kot na primer fašistični in socialistični projekti.

[19] Na tej točki bi sicer lahko zamejili termin hektivizem in v to vključili le hekerje, ki politično delovanje umeščajo v kontekst borbe za svobodo na medmrežju, ne pa da samo uporabljajo novo tehnologijo za širitev idej, ki niso neposredno vezane na problematiko delovanja medmrežja. Tako je lahko objavljanje na spletnih straneh samo uporaba nove tehnologije za

kriminalizirani. V kolikor so njihovi cilji v nasprotju z zakonodajo določene države[20] ali pa državni organi diskrecijsko odločijo, da je njihovo delovanje protipravno, je njihovo delovanje že obravnavno kot kriminaliteta. V drugem primeru pa je lahko njihova usmeritev povsem sprejemljiva za pravni red, vendar pa so njihove metode protipravne.[21]

Uporaba informacijske tehnologije omogoča aktivistom učinkovit način širjenja svojih idej med ljudmi. Poleg tega internet nudi velik učinek za majhen denarni vložek, kar je velik korak naprej od obdobja pred razmahom interneta, ko so bile potrebne večje vsote denarja za odmevnejše kampanje osveščanja javnosti.

Kljub prednostim uporabe novih tehnologij pa hektivizem ni razvil vseh svojih potencialov iz dveh razlogov:

1. Večina hekerjev je v svojem aktivizmu osredotočenih na vprašanje dostopnosti tehnologije, ob tem pa zanemarjajo vprašanje uporabe tehnologije kot orodja za doseganje političnih in socialnih ciljev; na primer problem odprtokodnih ali zaprtokodnih programov kot osrednja tema bojev.[22]

2. Protikulturne hekerske težnje so se vključile v korporativni kapitalizem s preobrazbo hekerjev v potrošnike in z uporabo njihovega znanja in volje. Razvoj interneta predstavlja tudi zmanjšanje programske (»softwarske«) heterogenosti, tako da za večino vsakdanjih delovanj ni potrebno iskati izvirnih rešitev, temveč so produkti že izpopolnjeni. Tako se odstotek ljudi, ki imajo neko uporabno računalniško znanje, zmanjšuje, povečuje se odstotek ljudi, ki so navadni potrošniki tehnologije. Poleg potrošnje pa so seveda za kapitalistično gospodarstvo koristni vsi, ki imajo uporabno znanje za kreiranje novih produktov za nove in stare potrošnike.

Nasprotno takšni kritiki pa Taylor[23] smatra ravno hektivizem za povratek k začetni hekerski etiki in njihovi zavzetosti za spreminjanje in odpiranje tehnologije. Ravno hektivizem naj bi se izognil pastem tehnološkega fetišizma, ki usmerja pozornost hekerja samo na delovanje tehnologije, brez zavedanja o družbenih učinkih tega delovanja.

Po 11.9.2001 je boj proti terorizmu vključil tudi boj proti kiberterorizmu. Ohlapnost, fluidnost in nedefiniranost tega pojma omogoča boj proti vsakršnim motnjam svetovnega prometa podatkov. Vlade posameznih držav ustanavljajo posebne

---

širjenje informacij in torej klasično aktivistično dejanje, napad določene skupine na spletno stran druge skupine ali državnega organa s pomočjo botnetov pa je že hektivistično dejanje.

[20] V primeru sovražnega govora organizacije ali skupine že s samo objavo na svoji spletni strani kršijo zakonodajo, ki prepoveduje širjenje nestrpnosti in spodbujanja sovraštva do družbenih skupin ali posameznikov. Ob tem je sama tehnična postavitev na spletno stran povsem v skladu z zakonodajo, neskladna pa je objava na spletni strani.

[21] Preoblikovanje tuje spletne strani na kateri se znajde sporočilo organizacije ali skupine je v nasprotju z zakonom, ni pa sama vsebina protipravna. Seveda je možna tudi kombinacija obojega, da je tako vdor v spletno stran kot tudi vsebina objave protipravna.

[22] Odgovor na ta očitek bi bil, da boj za odprto kodo pomeni boj za odprto okolje na internetu, ki edino omogoča obstoj svobode v kiberprostoru. Boj za odprto kodo je tako boj za neovirano širjenje informacij in sodelovanja.

[23] Taylor, str. 627.

oddelke za borbo na svetovnem spletu, velikokrat ti oddelki spadajo na vojaško področje. Ob tem obstaja velika nevarnost nadaljnje militarizacije boja proti kriminaliteti. S tem preidemo iz kazenskopravnega diskurza, ki je namenjen preganjanju storjenih kaznivih dejanj, k vojaškemu diskurzu, ki obravnava določen pojav kot varnostni problem. Tudi vojna strategija zahteva povsem drugačen pristop kot policijska strategija.

Že omenjena nedefiniranost termina kiberterorizem omogoča možnost ne samo borbe proti političnim skupinam, ki uporabljajo hekerske metode za povzročanje večje škode in ogrožanje varnosti ljudi, temveč tudi preganjanje političnih skupin, ki skušajo s prepovedanimi metodami nenasilno opozarjati na svoje cilje. Ker je boj proti terorizmu univerzalen, kar pomeni, da vse države uporabljajo podobne metode, si tudi države poljubno lahko opredelijo, kdo je za njih terorist oziroma kiberterorist. V večini držav ne veljajo relativno visoki standardi svobode govora in političnega ali nevladnega delovanja,[24] tako da se na seznamu »informacijskih teroristov«, zlahka znajdejo tudi nevladne organizacije, ki se ukvarjajo s človekovimi pravicami in pri tem uporabljajo tudi internetno tehnologijo.[25]

Metode delovanja hacktivistov:

- *Visual sit-in* predstavlja virtualno različico klasičnega *sit-ina,* ki predpostavlja nenasilno fizično okupacijo določenega prostora, povezanega s ciljem protesta, s strani protestnikov. Ena prvih takšnih akcij je bila akcija podpornikov indijanskih upornikov zapatistov, ki so uporabili poseben program *Flood Net*, preko katerega so sprožali periodične zahtevke po dostopu do spletne strani mehiške vlade. S tem so dosegli blokado delovanja strani, saj njen strežnik ni bil zmožen odgovoriti na vse zahtevke.

- *Bombardiranje z elektronsko pošto* je masovno pošiljanje elektronske pošte na določen naslov in s tem blokiranje njegovega normalnega delovanja.

Hektivizem ima prihodnost, če se bo znal zavedati nevarnosti prevelike identifikacije s tehnološkim aspektom protesta. Sposobnost povezovanja novih tehnoloških praks s tradicionalnimi in indigenskimi kulturnimi viri je pri tem odločilna. Zunanje omejitve hektivizma pa je stopnja represije, ki jo bodo državni organi uporabili v domnevnem boju proti terorizmu.

[24] Zanimiv je primer strežnika Tor, postavljenega s strani posameznikov, ki omogoča anonimno delovanje na internetu, saj ne beleži IP-ju uporabnikov. S tem omogoča izognitev nadzoru in preprekam za dostop do spletnih strani, ki se jih določeni državni režimi poslužujejo.

[25] Ob vseh pomanjkljivosti koncepta e-demokracije pa prav tehnološka prednost interneta omogoča širjenje informacij z nizkimi stroški. Ekonomska diskriminacija političnih strank je s tem delno odpravljena oziroma se vsaj njena stopnja zniža. Seveda pa vse to ni vedno povšeči vladajočim političnim in gospodarskim elitam, ki lahko z represijo, trdo roko zatirajo tovrstno delovanje. Najuspešnejša pri izvajanju cenzure na svetovnem spletu je Kitajska, ki je razvila že zelo močne filtre za spletne brskalnike.

## Piratstvo

Medtem ko je vdiranje v sisteme in socialni inženiring početje, ki po eni strani povzroča nevšečnosti, po drugi strani daje nove tržne možnosti za varnostno industrijo. Precej večjo škodo in paniko sistemu in kulturni industriji povzroča nedovoljeno širjenje nematerialnih produktov kot so računalniški programi, glasba, filmi, knjige, računalniške igre itd. Simptomatično je, da povprečen uporabnik interneta obravnava hekerske vdore kot zločin in nevarnost, piratstvo pa se mu navadno ne zdi problematično in se tudi sam poslužuje uporabe nedovoljenih kopij, pripadniki kulturne industrije, na primer filmske družbe in glasbene založbe, pa v škodi, ki jim je povzročena, vidijo najhujši zločin. Preprostost širjenja datotek po medmrežju povzroča visok porast prometa. Pri tem ni potrebno nikakršno hekersko znanje. Pomembna pa je vloga hekerjev pri vzpostavljanju vedno boljših *peer to peer* (p2p) povezav, ki so hkrati hitrejša in čim manj nadzorovana s strani državnih organov. Temeljno hekersko načelo je svoboden pretok informacij in vse oblike nematerialnih kulturnih produktov so zapisane v obliki informacije.

Kulturna industrija je polagala velike upe v razvoj interneta, saj je predstavljal nov medij za prodajo njenih produktov. »Scenarij je namreč predvideval, da bosta možnost prevajanja vsakovrstnih vsebin (glasbene, filmske, besedilne, radijskih in televizijskih programov) v diskretne enote digitalne informacije (bit) in njena distribucija uporabnikom preko mreže »inteligentnih« terminalov (torej računalnikov, združenih s klasičnimi mediji) neizogibno pripeljali do oblikovanja enotnega integriranega sistema prodaje novic, zabave in kulture stotinam milijonov naročnikov po vsem svetu.«[26] Načrt je naletel na dve veliki oviri v obliki uporabnikov interneta, ki so želeli, da ostane interaktiven sistem, ne pa samo medij oddajanja, druga ovira pa je težavno zagotavljanje spoštovanja pravic intelektualne lastnine. V ZDA je bil leta 1998 sprejet zakon DMCA (*Digital Millenium Copyright Act*), ki je zavaroval pravice kulturne industrije, poslabšal pa je položaj tehnološke industrije. Zakon je predvideval strožje varovanje pravic. Instrumenti so razširitev področja dejavnosti, ki so jih imeli za nezakonite, ter poostritev kazenskih sankcij za tovrstne dejavnosti. Kritiki so zakonu očitali, da:

»1. onemogoča znanstveno in tehnološko raziskovanje in tako upočasnjuje inovacije;

2. zavira tekmovalnost in monopolom lajša nadzor nad trgom,

3. krči pravice potrošnikov in tako brezobzirno omejuje njihove zmožnosti, da prosto uporabljajo izdelke, ki so jih zakonito kupili (tako imenovana pravica do poštene rabe (*fair use*))«.[27]

Začel se je boj med kulturno industrijo in tehnološko industrijo ter med kulturno industrijo in potrošniki. Razvpiti primer Napster je prinesel Pirovo zmago kulturni industriji. Sodišče je obsodilo podjetje Napster, ker je izmenjava datotek potekala preko njihovih strežnikov. Napster bi namreč lahko na svojem strežniku preprečil nezakonito izmenjavo. Tudi kot odgovor na to odločitev sodišča so se p2p omrežja razvila, tako da

[26] Formenti, str. 15.

[27] Formenti, str. 16.

promet ne poteka preko centralnega strežnika, ampak neposredno med računalniki.[28] S tem je možnost preprečevanja in kaznovanja nedovoljenega prometa z datotekami zelo zmanjšana. Promet je težje izslediti, težko je preprečiti nadaljnjo uporabo programske opreme tistim, ki so si jo že naložili na svoje računalnike in preprečiti nezakonito rabo tehnologije, saj omrežje nima centraliziranega nadzora. p2p omrežje nima fizične centrale, obstaja samo v virtualnem svetu.

Rešitve v okviru situacijske prevencije so različne, vendar omejujejo možnosti uporabe produkta in mu s tem zmanjšujejo uporabno vrednost. Zgoščenke, ki imajo onemogočeno kopiranje, kršijo pravico potrošnika, da si ustvari lastno varnostno kopijo. Prepoved uporabe programov p2p onemogoča prosto izmenjavo datotek, ki niso zaščitene z avtorskimi pravicami. Poleg bi se pojavili ilegalni programi, katerih delovanje je praktično nemogoče preprečiti brez totalnega nadzora prometa interneta. Kar ponovno predstavlja poseg v koncept zaščite osebnih podatkov.

Drugi ukrep v boju proti kršenju avtorskih pravic so drakonske kazenske sankcije. Že sam zakon DMCA prinaša stroge kazni, nekateri predlogi v zadnjih nekaj letih pa so še bolj skrajni. Ameriški poslanci in senatorji se med drugim zavzemajo za odobritev hekerskih napadov s strani podjetij v računalnike domnevnih kandidatov, za uničenje računalnikov tistih, ki nezakonito snemajo z omrežij p2p in za zaporne kazni za vse študente, ki si izmenjujejo glasbene datoteke, ter zaporne kazni tudi za tiste, ki samo ponujajo datoteke prek p2p. Namen preganjanja posameznih izmenjevalcev datotek je prestrašiti vse uporabnike interneta in jih odvrniti od uporabe omrežij p2p. Pregoni so pospešili razvoj naslednjega rodu izmenjevalnih omrežij, ki zagotavljajo bistveno več anonimnosti in so skoraj neodvisna od posameznih strežnikov, ki bi jih bilo mogoče izslediti in zapreti. Konec junija 2005 pa je ameriško Vrhovno sodišče odločilo, da so lahko spletna omrežja za izmenjavo datotek pravno odgovorna zaradi omogočanja nepooblaščene izmenjave avtorskih del.[29] Hkrati s poostrenimi kaznimi so podaljšali dolžino trajanja avtorske pravice za 20 let.

Dogajanje po 11. septembru 2001 je pospešilo izvoz vsebine DMCA v ostale države sveta. Potreba po represivnem preprečevanju kiberkriminalitete *in bianco carta* prestrašene javnosti je povzročila povečan nadzor nad prometom na internetu, ki ga vsebuje tudi razvpiti *Patriotic Act*.[30] Širjenje ameriške suverenosti preko meja kot prevencija pa je bilo možno le z izvozom zakona DMCA. Z gospodarskimi kupčijami so ZDA pri nekaterih dosegle sprejem zakonov o avtorskih pravicah, ki služijo interesom njihove kulturne industrije.

V Evropski uniji je bila leta 2001 sprejeta Direktiva o avtorskih pravicah (*European Union Copyright Directive* – EUCD). Direktiva je po vsebini precej podobna

---

[28] »Omrežje p2p so namreč ustvarili hekerji, ki so hoteli ustvariti horizontalne in demokratične mreže, zaščitene pred cenzurami in pred političnim nadzorom kot tudi pred tržnimi manipulacijami.« Formenti, str. 20.

[29] Kučić v Formenti, str. 197.

[30] »Tako na primer eden od členov Patriotic Act, ki je bil sprejet takoj po 11. septembru, jasno predvideva, da se vsako informatično hudodelstvo, storjeno na ameriških tleh (za izpolnitev tega pogoja zadostuje, da zaščitene informacije preko ameriškega strežnika le potujejo!), tudi če ga zagreši tujec, ki živi v tujini (glej primer Skilarov, s katerim smo se ukvarjali prej), lahko kaznuje v ZDA.« Formenti, str. 38.

ameriškemu zakonu, čeprav dopušča možnost izdelave lastne kopije. Do leta 2005 v Sloveniji ni bil sprožen noben kazenski postopek zaradi izmenjevanje preko p2p, saj niti slovenski varuhi interesov glasbenih založnikov (zavod IPF in združenje SAZAS) niso sprožili postopka, prav tako še niso imeli probleme ponudniki internetnih storitev, zahteve predstavnikov ameriških lastnikov avtorskih pravic pa ignorirajo.[31] Vendar pa je leta 2004 slovenska policija zasegla strežnike in računalnike državljanu Slovenije, ki je postavil zelo uspešno p2p zadevo imenovano Supernova. Zaradi policijskega zastraševanja je umaknil mrežo s spleta. Leta 2005 je državni tožilec obvestil osumljenca, da je ustavil kazenski pregon.

Pomembno je poudariti nekomercialno naravo brezplačnega izmenjevanja datotek. Razlike med klasičnim piratstvom in izmenjavo datotek je, da se v drugem primeru izogne industriji pretiranega nadzora in kot prvotna glasbena industrija preprosto izkorišča novo obliko razširjanja vsebine, vendar pa v primerjavi s kabelsko TV nihče ne prodaja vsebine, ki se na ta način izmenjuje.[32] Klasično piratstvo je fizično razmnoževanje materialnih nosilcev medijskih vsebin. Glasbena industrija ocenjuje, da zaradi fizičnega piratstva letno izgubi 4,6 milijarde dolarjev.[33] Lessig poudari tri bistvene značilnosti izmenjave p2p, preko katerih lahko potegnemo ločnico s klasičnim piratstvom:

- izogne se industriji pretiranega nadzora,
- kot prvotna glasbena industrija preprosto izkorišča novo obliko razširjanja vsebine,
- v primerjavi s kabelsko TV nihče ne prodaja vsebine, ki se na ta način izmenjuje.

Varovana pravna dobrina je potencialni dobiček, ki ga kulturna industrija izgublja zaradi brezplačne izmenjave datotek. Pri tem trčimo na problem določitve višine te škode. Ker naj bi kazensko pravo po načelu *ultima ratio* posegalo v izmenjavo dobrin, je potrebno ugotoviti ali gre res za tako veliko škodo, ki je povzročena žrtvam. Študije učinka izmenjave datotek obravnavajo korelacijo med količinami izmenjanih datotek in količino prodanih nosilcev medijskih vsebin (z glasbo, filmi ali računalniškimi igricami). Dejstvo je, da je upadla prodaja nosilcev, in da se povečuje število uporabnikov p2p omrežij. Vendar ta korelacije še ne dokazuje, da samo ta tehnologija vpliva na prodajo. Raziskave navajajo še nekatere druge faktorje, ki vplivajo na trg kulturnih produktov. Med njimi so nenormalno povečana prodaja v 90-ih, ko so potrošniki zamenjali medij – zamenjava vinilnih plošč za zgoščenke, povečana prodaja DVD-jev s filmi in računalniških igric (sprememba potrošniške usmeritve od glasbe k drugim oblikam zabave) in cene samih produktov. Raziskave tudi kažejo pozitivno korelacijo med možnostjo izmenjave glasbenih datotek in prodajo nosilcev glasbe. Večina delavcev v glasbeni industriji naj bi dosegala boljše prodaje, medtem ko naj bi škodo nosile

[31] Drugje po Evropi je ameriško fonografsko združenje obtožilo skoraj 5000 evropskih državljanov in od njih iztožilo od 3000 do 5000 evrov. Kučić, str. 194.

[32] Lessig, str. 83.

[33] Navedeno po Lessigu, str. 79. Ocena je bila podana v letu 2003. Domnevamo lahko, da se je ocena povečala, saj kljub večjemu kazensko pravnemu preganjanju hkrati tudi narašča trg kulturne industrije s pomočjo novega srednjega razreda v azijskih državah.

predvsem največje zvezde, ki prodajo največ.[34] Tako da lahko izmenjava datotek deluje tudi podobno kot progresivna davčna lestvica, saj nekaj prihodka izgubijo milijonarske zvezde in multinacionalne založbe, medtem ko pridobijo manjši glasbeni izvajalci in založbice, kar v ekonomski govorici pomeni glasbeni delavci in mala podjetja.

## Odgovor varnostne industrije na hekersko »nevarnost«

Prosti trg varnostnih storitev se hitro odziva na nove varnostne izzive. Novi načini hekerskih zlorab izzovejo odgovor industrije v novem varnostnem produktu, naj bo to v obliki programja ali strokovnega usposabljanja. Ker varnostna industrija deluje na podlagi povpraševanja, je njena usmeritev po vzdrževanju povpraševanja. Povpraševanje temelji na občutku stranke, ali je možnost, da postane viktimizirana. Varnostnim izzivom so podvržena predvsem podjetja, katerim vsaka motnja v delovanju informacijskega sistema predstavlja velik strošek. Tako so podjetja pripravljena vložiti v varnostni sistem, ki jim omogoča nemoteno delovanje in zagotavlja relativno varnost. Na ravni tehnične zaščite to ni problematično, problem se pojavi pri napadih s pomočjo socialnega inženiringa. Zaščita pred tovrstnimi napadi je možna le s strokovnim usposabljanjem celotnega osebja. Ker je želja varnostne industrije, da je povpraševanje po njenih produktih čim večje, skuša aktivno spodbuditi tovrstno povpraševanje. Kar lahko doseže na dva načina. Prvi, zakonsko nesporen, je propagiranje svojih produktov na tak način, da dobi stranka občutek, da to nujno potrebuje za normalno delovanje. Nakup tovrstnega blaga kot je na primer antivirusni program postane obvezen strošek, tako kot na primer zavarovalna polica. Drugi način pa je protipraven, v svojem bistvu hekerski, saj lahko sproži napad na sistem podjetja in ga na ta način prisili, da nakupi prav njihovo programsko opremo. Podjetja se seveda pri tem poslužijo hekerjev, ki niso povezani formalno z njimi, ampak jim lahko plačujejo za usluge. Ko ima informacijski sistem enkrat določeno programsko opremo, je majhna verjetnost, da bo kasneje prišlo do zamenjave te programske opreme za programsko opremo drugega proizvajalca, saj to pomeni stroške nakupa in usposabljanja osebja.

Posamezniki so veliko manj zaščitene, saj večina ne vlaga veliko v zaščito svojih osebnih računalnikov. Vendar so tudi manj zanimive tarče za hekerje, ki se želijo materialno okoristiti, ali pa jim je izziv povzročiti večjo nezgodo. Posamezniki so tako predvsem podvrženi virusom, trojanskim konjem, spywareom in podobni nesnagi, ki povzroča motnje v delovanju računalnika.

[34] V kampanjah okoli Napsterja so največje glasbene zvezde nastopile proti izmenjavi glasbe kot piratstvu, na primer Metallica in Madonna, medtem ko so manj znani glasbeni ustvarjalci, na primer Chumbawamba, podpirali možnost svobodne izmenjave glasbe.

## Nevarnosti pretiranega varnostnega omejevanja interneta

Glavne točke boja na medmrežju so vprašanja avtorskih pravic, terorizma in kriminalitete. Ta boj določa koordinate omejevanja svobode na internetu. Od začetne utopične skupnosti hekerjev, ki ni poznala omejitev, temveč je služila predvsem sodelovanju in izmenjavi informacij, skuša država vzpostaviti nadzorne mehanizme, ki bodo omogočili nadaljnjo akumulacijo kapitala s koriščenjem avtorskih pravic[35] in hitrejšo prodajo klasičnih materialnih dobrin in finančnih produktov.

Kriminologija je že v preteklosti poskrbela za soočenje s primerjavo med nevarnostjo ulične kriminalitete in kriminalitete »močnih«, torej pripadnikov vladajočih slojev ali državnih organov. Podobna situacija se pojavlja tudi v kiberprostoru. Posameznik je lahko žrtev hekerskega napada, škodljivega ravnanja, goljufije ali kraje. Hkrati pa je tudi izpostavljen nadzorovanju, saj s svojim početjem pušča za seboj sledove. Kopičijo se podatki o naših potrošniških navadah, politični usmeritvi, spolnih preferencah itd. Za temi podatki poteka lov med kiberkriminalci, podjetji in državnimi represivnimi organi. Medtem ko prvi želijo izrabiti podatke za izvršitev posamičnega kaznivega dejanja, podjetja skušajo prepoznati naše potrošniške navade in nas napasti s propagando, ali pa celo skušajo ustvariti nove potrebe s pomočjo podatkov, ki jih imajo na razpolago, državni organi pa skušajo imeti čim enostavnejši dostop do vseh podatkov, ki bi jim lahko služili pri pregonu osumljencev kaznivih dejanj ali pa v borbi proti potencialnim varnostnim problemom, kot je dandanes terorizem. Premajhna ozaveščenost uporabnikov spleta prinaša dodaten problem, saj večina misli, da nima kaj skrivati. Pri tem pa se ne zavedajo, da lahko nekdo uporabi še tako nedolžno navado obiskovanja določene spletne strani ali iskanja določenih podatkov za svoje načrte.[36]

[35] Avtorska pravica je lastninska pravica, ki se v nematerialnem okolju sooča s problemom onemogočanja svobodne reprodukcije informacije. Zgodovinsko je avtorska pravica vezana na materialnega nosilca, na primer knjigo. V kiberprostoru pa se skuša avtorska pravica vezati na nematerialne nosilce. Tehnološki napredek je v tem primeru premagal omejenost dobrin in omogoča neskončno reprodukcijo, lastnina pa temelji na omejenosti dobrin.

[36] Google je spletna stran, ki dobiva monopolni položaj v konkurenci iskalnikov na internetu. Tako v svojih bazah kopičijo ogromne količine podatkov o iskanju na netu. Ena novejših storitev je *Google Books*, ki omogoča branje digitaliziranih knjižnih del. Ob tem pa se beležijo podatki, katere knjige smo prebirali. Ni tako zelo fantastična domneva o posebnem »index prohibitorumu« knjig, ki bi si ga sestavile posamezne države za borbo proti sovražnikom države. V kolikor bi državni organi pridobili podatke od Googla o vaših bralnih navadah, ki bi vključevala prebiranje »problematičnih« knjig, bi se lahko znašli na seznamu osumljenih za pregon ali kakšnega drugega nepravnega načina državnega boja. Naloga internetne civilne družbe, katere pomemben del so tudi hekerji, je, da skuša takšne zadeve preprečiti in doseči takšno pravno ureditev, ki bi tovrstne zlorabe zbiranja podatkov preprečila.

# Sklep

Prehod v informacijsko družbo je prinesel s seboj tudi nove vrednote in materialne pogoje oziroma bolje rečeno, nematerialne pogoje. Heker je postal najprej junak, ki prinaša vedno novo znanje za izboljšanje delovanja sistema, kasneje pa postane zaradi svoje avtonomne narave in etike osovražen s strani sistema in njegovega propagandnega stroja – kulturne industrije. Ker heker verjame, da so njegova načela na prvem mestu, veliko pred pravnimi normami, ki v veliko primerih neustrezno capljajo za dejanskim dogajanjem, pride v konflikt s pravnim redom. Dosleden heker ima le dve izbire, ali se pridruži sistemu ali pa deluje samostojno še naprej in s tem tvega odgovor represivnega dela sistema.

Prakse, ki so sporne in velikokrat tudi preganjane, so v članku le na kratko predstavljene, saj bi njihova podrobnejša razčlemba zahtevala veliko več prostora. Ostajajo pa vprašanja varnosti, intelektualne lastnine in odprtosti interneta ključna vprašanja, ki določajo prihodnost kiberprostora. In z njim delijo usodo tudi hekerji, ki bodo na svoj način sooblikovali njegovo delovanje. Le skrajni distopični scenarij družbe prihodnosti, v kateri bi bile informacije popolnoma nadzorovane in usmerjene, za hekerje ne bi bilo prostora. Vendar v takšni družbi ne bi bilo prostora tudi za svobodno voljo, pravico svobode govora, pravico svobodnega združevanja. To pa je prevelika cena boja proti kriminaliteti in »terorizmu« za zagotavljanje varnosti in pravic zasebne lastnine. Hekerji nam kažejo alternativno pot, ki temelji na odprtosti in prosti izmenjavi nematerialne, informacijske lastnine. Z vrednotami vzajemnosti in solidarnosti, ki so pogosto skregane s prevladujoči načeli kapitalističnega gospodarstva. Kar pa je predvsem pokazatelj, da informacijska tehnologija prinaša drugačne temelje za preureditev ekonomskih struktur v celotnem gospodarstvu, tako realnem kot kiber.

## Literatura


1. Castells, M. (2000). **The Rise Of The Network Society**. Oxford: Blackwell.
2. Formenti, C. (2005). **Ne-ekonomija: Digitalna ekonomija in paradoksi intelektualne lastnine**. Ljubljana: Krtina.
3. Halpin, H. **The Immaterial Aristocracy of the Internet**. Po URL: http://www.metamute.org/en/Immaterial-Aristocracy-of-the-Internet.
4. Kee, J. **Social Engineering: Manipulating the Source**. Po URL: http://www.sans. org/reading_room/whitepapers/engineering/social_engineering_manipulating_the_source_32914.
5. Kučić, J. L. (2005). Prihodnost v vzvratnem ogledalu. V: C. Formenti, **Ne-ekonomija: Digitalna ekonomija in paradoksi intelektualne lastnine**, Ljubljana: Krtina, s. 193–212.
6. Lazzarato, M. (2006). Immaterial Labour. **Theory out of Bounds**, let. 7. University of Minnesota Press, s. 133–147.
7. Lessig, L. (2005). **Svobodna kultura: Narava in prihodnost ustvarjalnosti**. Ljubljana: Krtina.
8. McKenzie, W. (2008). **Hekerski manifest**. Ljubljana: Maska.
9. Poulantzas, N. (2008). Marxist Examinations of the Contemporary State and Law and the Question of the »Alternative«. V: N. Poulantzas, **The Poulantzas Reader: Marxism, Law and the State**, London: Verso, s. 25–46.
10. Reed, L. (2002). Governing (through) the Internet: The discourse on pathological computer use as mobilized knowledge. **European Journal of Cultural Studies**, let. 5, št. 2, s. 131–153.
11. Söderberg, J. **Trouble on the High Seas**. Po URL: http://www.metamute.org/en/ trouble_on_the_high_seas.
12. Taylor, P.A. (2005). From hackers to hacktivists: speed bumps on the global superhighway? **New Media Society**, let. 7, št. 5, s. 625–646.
13. Taylor, P. A. (1999). **Hackers: Crime in the Digital Sublime**. London: Routledge.
14. Turgeman – Goldschmidt, O. (2005). Hacker's Accounts: Hacking as a Social Entertainment. **Social Science Computer Review**, let. 23, št. 1, s. 8–23.
15. Wall, D.S. (2008). **Cybercrime: The Transformation of Crime in the Information Age**. Cambridge: Polity Press.
16. Wang, W. (2006). **Steal this computer book 4.0: what they won't tell you about the Internet**. No Starch Press.
17. Yar, M. (2006). **Cybercrime and Society**. Sage: London.
18. Yar, M. (2008). The rhetorics and myths of anti-piracy campaigns: criminalization, moral pedagogy and capitalist property relations in the classroom. **New Media Society**, let. 10, št. 4, s. 605–623.
19. **Google Book Search Settlement and Reader Privacy**. Po URL: http://www.eff.org/ issues/privacy/google-book-search-settlement.

# 4 Nigerijska prevarantska pisma

**David Modic**

»*Če ne bi bilo požrešnih, naivnih in kriminalno*
*nastrojenih žrtev, ki bi rade žele tisto,*
*česar niso posejale, ne bi bilo prevar tipa 419.*«
Nigerijska ambasada v Washingtonu, l. 2003

## Uvod

Izraz Nigerijska prevarantska pisma oziroma pisma 419 morda ni takoj prepoznaven. Vendar če jih definiramo opisno – tista elektronska sporočila, kjer vas nekdo v polomljeni angleščini obvesti, da vam je bogati stric (čigar obstoj je bil do sedaj za vas popolna skrivnost) zapustil milijone dolarjev v obliki zlatih palic in vse, kar stoji na poti med vami in užitkarskim življenjem, je plačilo majhne akontacije –, naenkrat vemo mnogo več o temi tega članka. Nigerijska prevarantska pisma so postala nekaj povsem običajnega v naših poštnih nabiralnikih, postala so del vsakdana. Zvedavi bralec bo z nejevero vprašal, ali sploh še kdo nasede tako prozornemu poskusu prevare. Raziskave kažejo, da nigerijska pisma še vedno prinašajo dobiček tistim, ki jih pošiljajo.

V tem članku bomo odgovorili na vprašanja o zgodovini tako prevar kot prevarantov, o tipični strukturi nigerijskih pisem in o tem, zakaj so tako uspešna.

## Demografski podatki

Medmrežje je marca 2009 po podatkih podjetja *Internet World Stats*[1] štelo dobro milijardo in pol uporabnikov. Ta podatek je sicer bolj kot ne posledica ugibanja – ko doma uporabljamo dostop do Medmrežja, smo od zunaj videti kot en sam uporabnik, čeprav v istem trenutku sin igra *World of Warcraft*, medtem ko oče po avto.netu išče nov družinski karavan, mama pa preko *Facebooka* meče ovce v prijateljice. Aha, bo rekel kritični bralec, kaj pa če preštejemo število uporabnikov glede na unikatne poštne naslove? Tudi to ni tako preprosto, kot se zdi, saj ima veliko uporabnikov več kot en naslov (na primer službenega in zasebnega). No, pa dovolj o nezanesljivosti Medmrežne statistike – tisto, kar lahko dokaj zanesljivo trdimo je, da Medmrežje uporablja *vsaj* milijarda in pol uporabnikov, kar pomeni, da je skupina tarč za prevarante ogromna.

Sicer gotovo nismo vsi uporabniki Medmrežja dovolj naivni ali pohlepni, da bi nas obljube o neslutenem bogastvu prepričale, da smo mogoče tokrat prav mi naleteli na zlato žilo, na tisto priložnost, ki pride samo enkrat v življenju in nas bo osvobodila dnevne tlake.

V Sloveniji ni mogoče z lahkoto najti podatkov o tem, koliko denarja Slovenci letno izgubijo zaradi prevar, v Veliki Britaniji pa spletne prevare nanesejo prevarantom

[1] Glej URL http://www.internetworldstats.com/stats.htm.

okroglih tri in pol milijarde funtov na leto (Fischer, Lea in Evans, 2008). V Združenih državah so nigerijska prevarantska pisma v letu 2007 povzročila skoraj štiri in pol milijarde dolarjev škode po podatkih nizozemske raziskovalne organizacije *Ultrascan Advanced Global Investigations*.[2] Ultrascan je v letu 2009 sledil tristo tisoč aktivnim pošiljateljem nigerijskih prevarantskih pisem. V letu 2005 je ameriški *Secret Service* ustanovil posebno delovno skupino z imenom operacija 4-1-9 (angl. *4-1-9 operation*). V istem letu je skupina prestregla tristo do petsto nigerijskih prevarantskih pisem na dan. V tem času je skupino klicalo v povprečju sto potencialnih žrtev na dan (Dyrud, 2005).

Raziskave so pokazale, da lahko prevaranti pričakujejo, da bodo posamezniki odgovorili na eno pismo od vsakih sto poslanih. Od tistih, ki so odgovorili na prevarantsko pismo, pa bo vsaj en posameznik na vsakih sto poslal denar. Preprosto povedano so nigerijska prevarantska pisma uspešna v približno 1‰ primerov, torej eno na vsakih tisoč (prav tam). Če upoštevamo podatek o tristo tisoč aktivnih pošiljateljih in če ohlapno računamo, da vsak izmed njih pošlje samo eno pismo na teden novemu uporabniku, jih še vedno *oseminštirideset na dan* ((300.000/1000)/7) zasluži na tuj račun. Glede na to, da je povprečna izguba na posameznika in prevaro v Združenih državah le malo manj kot petnajst tisoč dolarjev (*Fraud Trends January - June 2009*, 2009), se nehamo čuditi nad tako velikimi izgubami na letni ravni.

Nigerijska prevarantska pisma sicer segajo še v čas pred masovno uporabo elektronske pošte – leta 1998 so ameriške oblasti na newyorškem letališču JFK zasegle in uničile *skoraj dva in pol milijona* nigerijskih prevarantskih pisem v *3 mesecih* (Dyrud, 2005).

## Zakaj Nigerija?

Kritični bralec bo sedaj rekel, da menda nigerijskih prevarantskih pisem ne pošiljajo samo Nigerijci. Ne? Morda presenetljivo praktično vsa nigerijska prevarantska pisma izvirajo iz Nigerije. Razlogov za to je več.

Na makroekonomskem nivoju prebivalci Nigerije niso bogati, dasiravno Nigerija izvaža nafto in njene derivate. Naftni koncerni so v lasti tujih korporacij, tako da so avtohtoni prebivalci izločeni iz krogov, ki žanjejo dobiček. Še več, največji tuji prilivi, ki jih letno zasluži Nigerija, pridejo iz naslova nigerijskih prevarantskih pisem (Oyesanya, 2004).

Na mikroekonomskem nivoju gre za početje, ki je zelo dobro plačano, opravlja pa ga kader, ki je visokoizobražen. Zakaj pa so potem pisma napisana v polomljeni angleščini, bo rekel pozorni bralec. Zato, da verjamemo, da imamo opravka z nepismenimi bedaki, ki niso dovolj inteligentni, da bi nas prinašali okoli. O tem več kasneje. Prevare so se masovno začele izvajati v osemdesetih letih prejšnjega stoletja, potem ko je Nigerija obubožala zaradi izjemno nizkih cen nafte na svetovnih trgih. Tuje korporacije so pokupile naftna podjetja in na cesti se je znašel dobršen del visokoizobraženega kadra, ki se je soočal z realno možnostjo, da bodo postali brezdomci in umrli od lakote (Zuckoff, 2005). Ta univerzitetno izobraženi kader se organizira in prične izdelovati in pošiljati nigerijska prevarantska pisma po vsem svetu (Dyrud, 2005). Raziskave kažejo,

[2] Glej URL: http://www.ultrascan.nl.

da gre za organizirani kriminal, ki ga vodijo odvetniki, računovodje in diplomirani kemiki (prav tam).

Če pojav zbanaliziramo, gre za posel, enak kateremu koli drugemu (seveda s to razliko, da ta ni zakonit). Zaposleni so organizirani v piramidni shemi, kjer tisti pri vrhu dobro zaslužijo, tisti, ki pa so šele začeli, pa upajo na zaslužek kasneje. Vodilni kader novači mlade diplomante in maturante – pred univerzo se pripeljejo v črnem mercedesu, odpeljejo potencialne novince v svojo vilo na obali in jim rečejo: »Vidiš, vse tole je lahko tvoje, če boš trdo delal zame.« Novinci masovno pošiljajo elektronsko pošto in ko jim nekdo odgovori, o tem obvestijo nadrejene, ki prevzamejo prevaro (Zuckoff, 2005).

Dodatna olajševalna okoliščina za storilce je, da nigerijska vlada običajno ne preganja storilcev. Vsakih nekaj let kakšen izmed vladnih uradnikov zatrdi, da bodo tokrat res pričeli s pregonom (Moses, 2009), vendar do sedaj kakšnega večjega učinka ali obsežne akcije ni bilo. Na to stanje močno vplivata dva dejavnika. Pošiljatelji prevarantskih pisem so zvezdniki v očeh nigerijskega slehernika. Javnost jih vidi kot moderne Robine Hoode, ki bogatašem iz razvitega sveta jemljejo denar, ker si ga ti tako ali tako ne zaslužijo (Dixon, 2005). Drugi pomembni dejavnik pa je, da Nigerija kotira pri vrhu svetovne korupcijske lestvice – ocenjena je z 1,9 na lestvici od 1 do 10 in samo Bangladeš je ocenjen kot bolj skorumpiran v svetovnem merilu (Cukier, Nesselroth in Cody, 2007). Tako kaže, da nigerijska vlada ne čuti prehude potrebe, da bi zajezila reko nigerijskih prevarantskih pisem, ki se valijo na Zahod.

Izraz *prevare* ali *pisma 419* izhaja iz 419. člena nigerijskega kazenskega zakonika (38. poglavje), ki se nanaša na prevare (Dyrud, 2005; Zuckoff, 2005).

## Mehanika prevar 419

Etiološko gledano pisma 419 v svoji mehaniki niso posebno inventivna. Splošno gledano jih lahko uvrstimo v t. i. sheme predhodnega plačila (angl. *advance fee schemes*), kjer v zameno za kasnejšo (fiktivno) veliko pridobitev žrtev najprej vloži nekaj svojih sredstev (Cukier et al., 2007). To pomeni, da obstoj Medmrežja seveda ni ključen za tovrstne prevare – čisto navadna pošta ravno tako deluje.

Prvi zabeleženi primeri tovrstnih prevar segajo v 16. stoletje. Gre za t. i. pisma španskega zapornika, katerih tarče so bili angleški aristokrati. Prejeli so pismo bogatega fiktivnega sonarodnjaka, ki naj bi bil zaprt v Španiji. Na prostost naj bi ga španske oblasti izpustile šele, ko bi plačal določen znesek. Zaprti Anglež naj bi bil sicer zelo premožen, vendar naj bi trenutno ne imel dostopa do svojih sredstev in zato za pomoč prosi prejemnika pisma. Takoj, ko bo denar dobil in predal svojim ječarjem, naj bi ga ti izpustili in ko se bo vrnil nazaj v rodno Anglijo, bo svojemu dobrotniku *izposojeni* denar *seveda* povrnil z obrestmi *(Zuckoff, 2005).* Verjetno ni potrebno posebej poudarjati, da se za fiktivnim španskim zapornikom izgubi vsaka sled, takoj ko mu dobrotnik odpošlje zaprošena sredstva.

Mehansko gledano torej ne gre za veliko spremembo. Bogati sonarodnjak ne obstaja, tako kot ne obstaja bogati stric iz Nigerije. Denar, ki ga žrtev pošlje v upanju, da bo bogato poplačana v prihodnosti, ostane v žepih storilcev, ki potem izginejo. V primeru nigerijskih prevarantskih pisem velja povedati še to, da v skoraj vseh primerih ne gre za enkraten znesek, temveč za veliko število majhnih vsot, ki so razporejene čez daljše časovno obdobje.

Naslove žrtev storilci pridobijo s spletnih forumov, spletnih seznamov zaposlenih v podjetjih in t. i. liste lahkoverneže (angl. *sucker-lists*), kamor žrtev najhitreje pride tako, da odgovori na kako pismo 419 ali pa dejansko tudi pošlje denar (Dyrud, 2005). Storilci sami si med seboj prevzemajo žrtve in nič neobičajnega ni, če se nekdo v relativno kratkem času zaplete v več prevar naenkrat.

Ko je žrtev enkrat v sistemu, prične dobivati večje količine neželene pošte. Dyrudova je v času svoje raziskave dobivala v povprečju enajst pisem 419 na mesec (prav tam).

## Tipični potek nigerijske prevare

Pisma 419 so večinoma napisana v polomljeni angleščini. Tak zavajajoči stil je izbran namenoma, saj zaziba žrtev v lažni občutek varnosti, ko si misli, da ga nekdo, ki niti ne zna angleško, že ne bo prinesel naokrog (Cukier et al., 2007).

Kljub temu da se, globalno gledano, nigerijska pisma v vsebini razlikujejo med seboj, vseeno lahko poiščemo njihove skupne točke.

Pošiljatelj žrtvi vedno obljublja dobiček v prihodnosti. Znesek je odvisen od tipa pisma, ravno tako valuta (zlato, dolarji ipd.). Za to, da bi posameznik lahko prišel do nagrade, pa mora najprej plačati določene dajatve. Žrtev dobi pismo »visokega državnega uradnika«, ki je lahko bankir, odvetnik, vdova vojaškega diktatorja, kraljev nezakonski sin ipd. Ta žrtvi pove, da ima dostop do večje količine denarja, kot je na primer dediščina, bančni račun preminulega vojnega zločinca, rezervna sredstva vojaškega diktatorja ali kaj podobnega. Da bi prišel do denarja, pa uradnik potrebuje sredstva za davščine, koleke, plačilo odvetniški pisarni, carinske dajatve in tako naprej.

V zadnjem času se pojavlja vedno več pisem nigerijskih »lepotic«, ki po zmenkarskih spletnih straneh iščejo osamljene, premožne samske moške in se dogovarjajo za zmenke. V primeru, da žrtev v vabo zagrize, mu povedo, da bi se rade dobile z njim v njegovi državi, kar pa pomeni, da potrebujejo denar za letalsko karto, vizo, najemnino za stanovanje, podkupnine uradnikov in tako naprej. Slike, ki jih prevaranti uporabljajo, so ponavadi nigerijske manekenke ali TV-voditeljice.

Druga različica, ki se pojavlja v zadnjem času, so nigerijski »študenti«, ki bi radi najeli stanovanje v tuji državi, na primer Združenih državah Amerike. Lastniku nepremičnine sporočijo, da bi radi plačali najemnino nekaj mesecev vnaprej preko »podjetja«, ki jim plačuje šolnino, zato bi najraje najemodajalcu poslali ček dotičnega podjetja. Ker ne bi radi tega počeli večkrat in ker še nimajo odprtega bančnega računa v državi, ki jo kanijo obiskati, bodo poslali ček v večjem znesku, ki bo vključeval tudi denar za letalsko karto, potne stroške ipd. Razložijo, da bi bilo najbolj preprosto, če bi nato najemodajalec unovčil ček in jim del zneska poslal nazaj. Žrtev ček unovči, del denarja pošlje nazaj, nakar se izkaže, da je bil ček ponarejen, banka zahteva denar nazaj, »študent« pa ne odgovarja več na klice in elektronsko pošto.

Tretja različica, še posebej veliko uporabljana v letu 2008 je, da nekdo dobi elektronsko pošto prijatelja, ki naj bi bil na poslovnem potovanju v Nigeriji ali na Nizozemskem. Gre dejansko za osebo, ki jo žrtev pozna. Ta prijatelj naj bi bil okraden, izgubil je denarnico, prenosni računalnik, potni list, letalsko karto, vse. Tudi mobilni telefon, zato res nima smisla, da bi ga poskušali priklicati. Sedaj prosi za pomoč žrtev, ki naj mu pošlje manjšo vsoto denarja, za letalsko karto in nadomestilo potnega lista.

Ker sam nima nobenih osebnih dokumentov, je srečal prijaznega Nigerijca, ki mu je dovolil, da uporabi njegov bančni račun ali pa naslov za potovalne čeke. Zgodba je lahko tudi resnična, do te mere, da so prijatelja res okradli in v primeru, da ga poskušate priklicati, nihče ne dviga telefona ali pa vam odgovori storilec. Vendar denar ali potovalni čeki ponavadi ne pridejo do prijatelja.

Ena od različic predvideva, da se žrtev razglasi kot zakoniti dedič premoženja, ki ostaja v nigerijski banki, druga, da žrtev ustanovi podjetje v Nigeriji, ki naj bi potem izdalo račun za sredstva, tretja, da odpre bančni račun v Nigeriji, kamor naj bi se sredstva pretočila.

Po prvem plačilu mora žrtev plačati samo še eno dajatev, da se dokoplje do denarja. In za drugim plačilom spet samo še eno in tako naprej (Cukier et al., 2007). V vseh pismih je končni dobiček že skoraj na dlani in tisto, kar bo pridobljeno, daleč odtehta začetni vložek.

Gre za t. i. pomoto izgubljenega plačila (angl. *sunk cost fallacy*) (Arkes in Ayton, 1999; Arkes in Blumer, 1985). V ekonomiji se izraz izgubljeno plačilo (angl. *sunk cost*) uporablja, ko govorimo o nekem znesku, ki ga ne bomo več dobili nazaj. Zanimivo je, da ljudje v določenem trenutku prenehamo razmišljati racionalno in rečemo: »Kamor je šel bik, naj gre še štrik.« V primeru nigerijskih prevarantskih pisem to pomeni, da žrtev v neki točki oceni, da mora nujno dobiti obljubljeno nagrado, saj je v transakcijo vložila že toliko denarja, da se ji preprosto ne izplača prenehati, saj ve, da, če neha, zagotovo ne bo dobila nič. Tako, nič kaj racionalno, še naprej plačuje, navkljub temu da izgublja vedno več.

Če žrtev nima denarja, ji storilec ponudi možnost unovčenja njegovih (ponarejenih) čekov. Pri tej transakciji žrtev običajno vrne 90% denarja storilcu, 10% pa zadrži zase, vendar v končni fazi tudi tistih 10% porabi za razne dajatve (Rusch, 1999).

Unovčevanje ponarejenih čekov je kaznivo dejanje, kar na eleganten način pripelje do tega, da je žrtev naenkrat soudeležena pri pranju denarja in obenem predmet kazenskega pregona v domači državi.

V vmesnem času žrtev dobi *ogromne* količine dokumentov, opremljenih z državnimi grbi in pomembnimi žigi. Včasih je eden od dokumentov tudi pooblastilo za razpolaganje s celotnim žrtvinim premoženjem. Ker je pisem – dopisov, dokumentov, aneksov in potrdil tako veliko, se lahko zgodi, da žrtev podpiše tudi tako pooblastilo. Poznamo primere, v katerih je žrtev podpisala tovrstno pooblastilo in nekaj mesecev kasneje ugotovila, da je »njen pravni zastopnik« prodal hišo, v kateri živi z družino, in da se morajo izseliti.

Ob tem je treba poudariti, da ni nujno, da so dokumenti, ki jih žrtev dobiva, ponarejeni. Kot je že bilo omenjeno v tem članku, je korupcija v Nigeriji tako vseprisotna, da je povsem mogoče, da gre za pristne dokumente, ki jih je podpisal skorumpirani predstavnik oblasti, ali pa da je državni uradnik proti plačilu »posodil« žige in formularje storilcu. Lahko mu je tudi oddal svojo pisarno za nekaj ur. V več primerih so tako žrtve zares obiskale nigerijske »uradnike« v Nigeriji, v »njihovih pisarnah«, v času uradnih ur (Cukier et al., 2007). Tako se ne gre zanašati na to, da je tisto, kar vidimo, tudi dejansko realna situacija.

V več primerih so storilci žrtve prestregli že kar na letališču v Lagosu in jih v »državnih« limuzinah odpeljali do »državne palače«, kjer so v neki naključni pisarni opravili primopredajo papirjev ali denarja, jih odpeljali v »hotel« in jih tam pustili. Ko

se je izkazalo, da denarja v resnici ni, so bili storilci že davno daleč stran, žrtev pa deset tisoč kilometrov stran od doma v hotelski sobi v revnem predelu mesta, kamor taksiji ne vozijo.

Končnica prevare se lahko izteče tako, da je žrtev povabljena nekam v tujino (Lagos, Amsterdam in London so najbolj pogosti cilji poti), kjer sreča svoje storilce v živo. V tej točki lahko žrtev ubijejo, če se izkaže, da nima več nobenih sredstev in je v tem smislu povsem nekoristna za storilce. Lahko jo ugrabijo in zahtevajo odkupnino od sorodnikov ali prijateljev. Lahko pa ji dajo kovček pobarvanega »denarja«, ki bi ga bilo treba samo še »oprati«. Pred očmi žrtve »operejo« en sam stodolarski bankovec, ki je v resnici edini resnični denar v kovčku, magična tekočina pa je v resnici zabarvana solna raztopina. Seveda tekočina, nujna za razbarvanje, ni zastonj, zato bi morala žrtev plačati le še čisto zadnji znesek in oditi z »denarjem«. Kasneje v hotelski sobi žrtev ugotovi, da je razbarvani denar ponarejen ali pa da gre za časopisni papir, narezan v obliki denarja (prav tam).

## Psihološki mehanizmi, povezani s pismi 419

Poti prepričevanja (angl. *routes to persuasion*) (Langenderfer in Shimp, 2001; SanJosé-Cabezudo, Gutiérrez-Arranz, in Gutiérrez-Cillán, 2009) so pomemben del pri procesu odločanja. Gre za vprašanje, na kakšen način nekoga prepričamo, da si izbere določeno opcijo. Poznamo dve poti – *centralno* oziroma neposredno, kjer naj bi sistemski in logični argumenti pripeljali do ugodne reakcije in spodbudili osebo na drugi strani, da globoko razmisli in sprejme optimalno izbiro (Fischer et al., 2008). Po domače povedano gre za tehniko, kjer so karte na mizi in kjer računamo, da bo teža naših argumentov prepričala posameznika. Druga pot je t. i. *periferna* oziroma posredna, kjer iščemo bližnjice in emocionalne reakcije, ki naj spodbudijo osebo na drugi strani, da ne razmišlja, ampak se preprosto strinja z nami (prav tam).

Verjetno ni potrebno posebej poudarjati, da se prevaranti raje poslužujejo perifernih poti – le malo verjetno je, da se bo nekdo pustil prevarati, če mu storilec vnaprej in jasno da vedeti, da bo na koncu ostal brez vsega in da ga bodo bodisi zaprli v lastni državi bodisi ubili v Nigeriji.

Storilci torej igrajo na karto čustev, bodisi religioznih (… *sama Božja volja je bila, da sem vas našel* …), bodisi zaščitniških (… *pomagajte mi, ubogi osamljeni in zapuščeni vdovi* …), bodisi grabežljivih (… *denar bova delila 50:50. Pomislite, že naslednji teden imate na računu lahko 50 milijonov dolarjev* …), bodisi odrešitvenih (… *nikoli več ne boste revni niti vi, niti vaši otroci* …), bodisi povsem mesenih (… *tako rada bi se te dotaknila in s prsti šla skozi tvoje lase* …).

Periferne poti prepričevanja so problematične ravno zato, ker zapeljejo žrtev stran od racionalnega odločanja. V našem primeru je njihov cilj, da se žrtev nikoli ne vpraša, zakaj je bila izbrana ravno ona in kako to, da do danes ni še nikoli slišala za svojega bogatega preminulega nigerijskega sorodnika.

Sama nigerijska prevara je zasnovana tako, da pokrije čim več faktorjev, zato je v resnici znotraj sebe manj kot konsistentna. Tisti posamezniki, ki tako nekonsistentnost odkrijejo, običajno odstopijo od prevare, razen v primeru, kjer verjamejo, da lahko prevarajo prevaranta, kar pa je v resnici v nekaterih primerih cilj prevaranta. Torej ne to, da

bo na koncu sam prevaran, ampak, da žrtev misli, da ji bo uspelo. Raziskave kažejo, da je pretirana samozavest najpomembnejši faktor uspešnosti prevare.

Dodaten element, ki vpliva na uspešnost prevare, še posebej pri starejših posameznikih, je dejstvo, da se vsaj nekdo ukvarja z njimi (Langenderfer in Shimp, 2001). Starejši posamezniki večkrat vedo, da jih nekdo izrablja, vendar jih vodita dva elementa: ne bi radi izneverili pričakovanj storilca, saj je to nevzgojeno in nesramno, obenem pa si želijo socialne interakcije – na nek izkrivljen način plačajo storitev, torej to, da se nekdo ukvarja z njimi. Na tem mestu naj poudarim, da ne želim omalovaževati starejše populacije – če je že kaj narobe s tem zatečenim stanjem, je narobe to, da se otroci in svojci ne ukvarjajo s svojimi starši ali sorodniki.

Ob tem je zanimivo, da se tveganje za izrabo poveča v obeh mejnih položajih: pri neizkušenosti ob uporabi medija (Medmrežja) posamezniki pričakujejo, da bodo prevarani, zato tudi so, obenem pa se ne zavedajo, kaj vse se jim na Medmrežju lahko zgodi; tveganje za viktimizacijo pa se poveča tudi ob dobrem poznavanju medija, saj v tem primeru posamezniki niso tako pozorni oziroma imajo lažen občutek samozavesti (Dutton in Shepherd, 2004), kar zniža njihov prag nezaupljivosti.

Nigerijska pisma v sebi skrivajo elemente pravljičnosti (Cukier et al., 2007) – pomislite: od posameznika pričakujejo, da postane nekritičen – kljub temu, da pisma na začetku skoraj nikoli niso naslovljena nanj osebno, naj bi še vedno verjel, da je ravno on tisti izbranec, milijonti obiskovalec neke spletne strani, naključno izžrebani posameznik, ki je zadel na loteriji, čeprav ni kupil srečke. V večini pisem najdemo nejasne namige na tretjo osebo, ki naj bi potencialno žrtev priporočila prevarantu, kar sicer preusmeri sum od prevaranta (ki očitno hoče samo dobro) na to, ponavadi neznano tretjo osebo, ki je žrtev izbrala iz nekega magičnega razloga (prav tam). Realistično gledano bi v primeru, ko bi nam nekdo res hotel podariti milijon funtov, ta dobrotnik verjetno vložil vsaj toliko truda, da bi odkril, kako nam je v resnici ime.

Večina pisem 419 vsebuje reference na tekoče dogodke, skupaj s spletnimi naslovi. Običajno se nanašajo na naravne ali humanitarne nesreče (prav tam). Gre za kršenje verige zaupanja – storilec ponudi verodostojni vir in na ta način sebe naredi bolj verodostojnega – *saj piše v New York Timesu, da je bogati vojaški diktator res umrl, torej ni vrag, da žrtvi ne bi pisala vdova pravkar pokojnega*.

Če gledamo na pisma 419 s stališča dramske strukture, vidimo, da skoraj brez izjeme vsebujejo stereotipne zgodbe, ki v grobem sledijo več mitom.

Prvo bi lahko poimenovali »od trnja do zvezd« – storilec se ponavadi predstavi kot slehernik, ki je vse življenje garal v neki duhomorni službi (bančni uradnik, odvetnik, gradbenik) ali pa kot neuslišana, zatirana vojaška vdova, ki se ni strinjala z moževimi neetično manj sprejemljivimi dejanji, vendar je pač nikoli nihče ni upošteval. Oba sta imela srečo samo enkrat v življenju, ko sta naletela na bogastvo, ki ga sedaj ponujata drugemu malemu človeku – žrtvi. Zgodba je efektivna ne več nivojih – po eni strani vzbuja sočustvovanje in po drugi identifikacijo. Občutek, da smo v neki stvari skupaj, da se borimo proti skupnemu sovražniku, ki ga predstavlja kar nepošteni svet, ki ne poskrbi za male ljudi, kot sta storilec in žrtev. Storilec sporoča žrtvi, da tudi malim ljudem lahko uspe, če držijo skupaj – vse to pa bi bilo morda dolgoročno bolj efektno, če bi storilec res nameraval delovati v dobro žrtve.

Drugi tak mit je »vreča zlata na koncu mavrice« – vedno gre za nek znesek ali dobiček, ki je nesorazmeren z dejanskim vložkom in bi pomenil zelo dobro kupčijo za

žrtev, če bi končna transakcija v resnici obstajala. V tem smislu prevarant računa tudi na posameznikov pohlep in nemoralno naravo, *češ, pa kaj, če si nečesa ne zaslužim, vse, kar lahko dobim od sveta, mi tako ali tako pripada*. Če bi žrtev razmišljala o tem, kaj si v resnici zasluži in koga ta posel oškoduje, bi nasedla veliko težje. Od tod izhaja izraz, da je težko prevarati poštenega človeka (Duffield in Grabosky, 2001).

Liki, ki nastopajo v nigerijskih pismih, ravno tako sledijo mitom in arhetipom: od Robina Hooda (Dixon, 2005) – na primer gradbinec, ki mu država noče poplačati njegovega znoja in solza, rabi žrtvino pomoč pri trganju denarja iz krempljev bogatašev, ker bi rad nahranil svojo sedemčlansko družino – do princeske v težavah, ki išče princa na belem konju (Cukier et al., 2007) – na primer hčerka plemenskega poglavarja, ki potrebuje denar za pobeg iz države, ki je *tako* kruta do žensk (fiktivna fotografija priložena) pa do dobre vile (prav tam) – starejše ženske, ki je podedovala ogromno denarja, vendar se ne znajde s financami in bi raje videla, da bi z denarjem upravljala žrtev, dobiček pa bi si nato delila na pol.

Nagrada, ki jo storilec ponuja, je brez izjeme večja, kot bi si jo usluga, ki jo rabi, zaslužila. Gre za obrnjeni socialnopsihološki mehanizem recipročnosti (Rusch, 1999): družbeno prilagojeni posamezniki čutimo potrebo po tem, da bi poravnali račune – če nam nekdo naredi uslugo, bi jo radi vrnili, raziskave pa so pokazale, da se čutimo obvezane vrniti uslugo, tudi če je v našo škodo in nesorazmerna s prejšnjo uslugo (prav tam). Pri pismih 419 gre za ravno obratno situacijo: končno je žrtev del skupine tistih, ki dobijo več, kot izgubijo. Tudi ta percepcija nenadnega in nepričakovanega srečnega naključja preprečuje žrtvi, da bi se predolgo mudila pri detajlih, ki bi ob bolj pozornem pregledu razkrinkali storilca in pomanjkljive temelje prevare (Cukier et al., 2007).

## Kaj storiti?

V preteklosti so se preventivni mehanizmi izkazali za dokaj neuspešne. Za to obstaja več razlogov – Medmrežje kot ogromna tvorba, največja zakladnica informacij na svetu, onemogoča lahek dostop do prav teh informacij, ki jih hrani. Mehanske rešitve na tehnološkem nivoju bodisi niso efektivne bodisi niso praktične (na primer izklop Nigerije iz Medmrežja), saj bi pomenile odtujevanje pravic tistim, ki niso naredili ničesar nemoralnega ali nezakonitega. Na nivoju posameznika je morda najbolj efektivna rešitev razmišljanje o tem, da *nič na tem svetu ni zastonj*. Na nivoju skupin so se v zadnjih letih pojavile združbe posameznikov, ki *varajo prevarante* (angl. *scaming the scamers*). Člani teh skupin pravijo, da to počnejo zato, da zapravljajo čas storilcem, ki potem nimajo časa izrabljati lahkovernosti ostalih uporabnikov Medmrežja. V resnici verjetno to počnejo za zabavo. Velikokrat so te kontraprevare skrajno elaborirane in njihovi avtorji vpeljujejo vanje več fiktivnih likov, občasno tudi fiktivne nigerijske prevarante, pravnike, vodje policijskih skupin ipd. Taka dopisovanja lahko trajajo tudi po več mesecev, arhivi pa so javno dostopni na svetovnem spletu. Bralec, ki ima čas in voljo, lahko obišče spletne strani www.419eater.com ali www.scambuster419.co.uk za nekaj uric brezskrbne zabave.

# Zaključek

Gotovo je, da so pisci nigerijskih prevarantskih pisem razvili sistem brez večjih lukenj. Osredotočeni so na ogromno ciljno skupino, tudi če so skrajno neuspešni in njihove prevare uspejo samo enkrat na vsakih tisoč primerov, še vedno živijo zelo lagodno. Marketinške strategije jim nudijo obilo materiala za snovanje boljših in boljših lažnih ponudb. Pregovor pravi, da upanje umre zadnje, in tako bodo vedno imeli na voljo ljudi, ki bodo upali. Upali, da se je ravno njim nasmehnila sreča. Upali, da bodo obogateli brez kakršnega koli predhodnega vložka. Upali, da je na koncu mavrice res vreča zlata. Pisci pisem 419 se zanašajo na to, da bomo ljudje zase vedno verjeli, brez trohice dvoma, da smo nekaj posebnega, da si zaslužimo biti boljši kot ostali, da je v vesolju vse urejeno v točki, ko zaslužimo na račun drugega. Ironično je, da tako storilci, kot žrtve verjamejo isto, vendar v našem primeru storilci te fantazije sebi tudi potrjujejo, seveda na račun žrtev.

## Literatura


1. Arkes, H. R. in Ayton, P. (1999). The sunk cost and Concorde effects: Are humans less rational than lower animals? **Psychological Bulletin**, let. 125, št. 5, s. 591–600.
2. Arkes, H. R. in Blumer, C. (1985). The psychology of sunk cost. **Organizational Behavior and Human Decision Processes**, let. 35, št. 1, s. 124–140.
3. Cukier, W. L., Nesselroth, E. J., in Cody, S. (2007). **Genre, Narrative and the "Nigerian Letter" in Electronic Mail**. Paper presented at the 40th Annual Hawaii International Conference on System Sciences (HICSS'07). Po URL: http://www2.computer.org /portal/web/csdl/proceedings/h#5.
4. Dixon, R. (2005, 20.10.). 'I Will Eat Your Dollars'. **LA Times**, s. 3. Po URL: http://www.latimes.com/news/nationworld/columnone/la-fg-dollars20-2005oct20,0,4514097,full.story.
5. Duffield, G. M. in Grabosky, P. N. (2001). The psychology of fraud. **Trends and issues in crime and criminal justice**, marec, št. 199, s. 1–6.
6. Dutton, W. H., in Shepherd, A. (2004). **Confidence and risk on the Internet**. Oxford: Oxford Internet Institute.
7. Dyrud, M. A. (2005). **I Brought You a Good News: An Analysis of Nigerian 419 Letters**. Paper presented at the 70th Annual Convention of The Association for Business Communication. Po URL: http://www.businesscommunication.org/conventions/ Proceedings/2005/PDFs/07ABC05.pdf.
8. Fischer, P., Lea, S. in Evans, K. (2008). **The Psychology of Scams: Provoking and Commiting Errors of Judgement. Research for the Office of Fair Trading**. Exeter, UK: University of Exeter.
9. **Fraud Trends January - June 2009**. (2009). (Advisory). Washington, DC: National Consumer League.
10. Langenderfer, J. in Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. **Psychology and Marketing**, let. 18, št. 7, s. 763–783.
11. Moses, A. (2009). **Hardline Nigerian official pledges to arrest the 419 scammers**, 1.09.2009. Po URL: http://www.theage.com.au/technology/security/hardline-nigerian-official-pledges-to-arrest-the-419-scammers-20090901-f65d.html, dostop 20.9.2009.
12. Oyesanya, F. (2004). **Nigerian Internet 419 on the Loose**. Po URL: http://www. nigeriavillagesquare.com/articles/femi-oyesanya/nigerian-internet-419-on-the-loose-13.html, dostop 28.9.2009.
13. Rusch, J. J. (1999). **The "Social Engineering" of Internet Fraud**. Paper presented at the Internet Global Summit - INET 99. Po URL: http://www.isoc.org/isoc/conferences /inet/99/proceedings/3g/3g_2.htm.
14. SanJosé-Cabezudo, R., Gutiérrez-Arranz, A. M. in Gutiérrez-Cillán, J. (2009). The Combined Influence of Central and Peripheral Routes in the Online Persuasion Process. **CyberPsychology & Behavior**, let. 12, št. 3, s. 299–308.

15. Zuckoff, M. (2005). Annals of Crime: The Perfect Mark. **The New Yorker**, 15. maj, s. 36–42. Po URL: http://www.newyorker.com /archive/2006/05/15/060515fa_fact?current Page=all.

# IV. DIGITALNI DOKAZI IN RAČUNALNIŠKA FORENZIKA

## 5 Digitalni dokazi v kazenskem postopku: pogledi na aktualna vprašanja

**Liljana Selinšek**

### Uvod

Digitalni dokazi so vrsta elektronskih dokazov,[1] ki zaradi svoje vseprisotnosti postajajo čedalje bolj pomembno dokazno sredstvo tudi v kazenskih postopkih, kar je posledica digitalizacije vsakdanjega življenja, pa tudi uporabe elektronskih naprav v povezavi s kriminalnimi aktivnostmi. Že v 80. letih prejšnjega stoletja se je napovedovalo, da bo forenzično računalništvo oziroma digitalna forenzika postala integralni del večine kazenskih preiskav,[2] sedaj pa se to v čedalje več državah tudi dejansko dogaja.

Digitalni dokazi (za razliko od analognih[3]) pravosodnim sistemom po svetu povzročajo težave. Ti dokazi so lahko relevantno dokazno sredstvo praktično v vseh pravnih postopkih, saj so pravni dogodki, ki se lahko dokazujejo z njimi, številni. Predvsem je treba poudariti, da digitalni dokazi niso povezani izključno z računalniško kriminaliteto oziroma s t. i. *high-tech crime*. Koristni so lahko tudi pri dokazovanju na primer pogodbene volje ali drugih relevantnih elementov v civilnopravnih zadevah; v

[1] S pravnega vidika se elektronski dokaz najpogosteje definira kot *proizvod analogne naprave ali podatek v digitalni obliki, ki je ustvarjen, spremenjen, shranjen ali povezan s kakršnokoli napravo, računalnikom ali računalniškim sistemom ali ki se prenaša preko komunikacijskega sistema in je relevanten za proces razsojanja* (prim. Mason, s. XXXV). Elektronski dokaz je torej splošni izraz za digitalne in analogne dokaze, pogosto pa se uporablja kar kot sopomenka za digitalni dokaz.

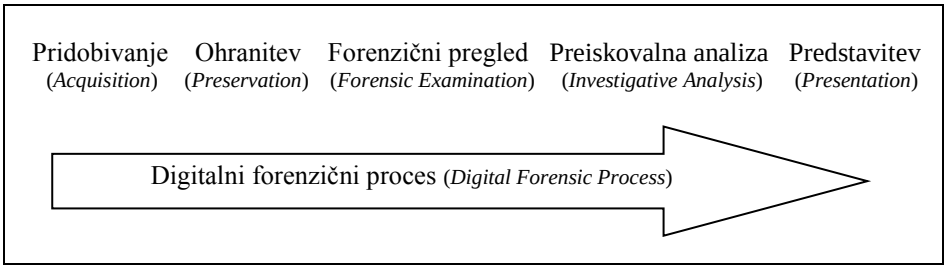
[2] Prim. McKemmish, s. 3.

[3] Dokazi v analogni obliki praviloma niso problematični za razumevanje. Sem sodijo na primer vinilne plošče, avdio kasete, fotografski negativi ipd., skratka stvari, ki smo jih navajeni in vemo, kako delujejo. Analogni fotoaparat na primer ustvari primarni dokaz (posnetek določene situacije) v obliki negativa, izvedeni dokaz pa dobimo v obliki razvite fotografije. Znano je, da je podatke v analogni obliki mogoče prirediti in ponarediti, vendar to terja precej truda, ponaredkov oziroma prirejenih dokazov pa praviloma ni težko opaziti oziroma odkriti. Ravno nasprotno je z digitalnimi dokazi: le-te je razmeroma enostavno spremeniti oziroma prirediti, kar pa je pogosto zelo težko ali celo nemogoče odkriti.

kazenskih zadevah pa razen za dokazovanje dejanj, ki pomenijo neposredno zlorabo računalniške in/ali informacijsko-komunikacijske tehnologije tudi za dokazovanje številnih drugih kaznivih dejanj, ki niso nujno povezana s to tehnologijo, je pa bila v konkretnem primeru pri dejanju tako ali drugače prisotna ali uporabljena.[4] Ker so digitalni dokazi danes praktično povsod, je pomembno, da so posamezniki, ki delujejo znotraj širšega kroga pravosodja, seznanjeni z njihovo naravo in posebnostmi.

Kar se tiče kazenskega postopka, se je Slovenija oktobra 2009 pridružila zaenkrat ne prav širokemu krogu držav, ki imajo v kazenskih postopkovnikih posebna pravila o zasegu elektronskih naprav, zavarovanju podatkov v njih in njihovi preiskavi. Z novelo ZKP-J[5] sta bila v Zakon o kazenskem postopku (dalje ZKP[6]) vnesena člena 219.a in 223.a, ki določata osnovne smernice v zvezi s pridobivanjem digitalnih dokazov, s čimer je zakonodajalec pripoznal dejstvo, da za kazenski postopek praviloma ni bistvena fizična naprava, ampak podatki na njej.[7]

Digitalni forenzični proces poteka po naslednjih fazah:[8]




Z novelo ZKP-J so bile v zakonodajo vnesene določbe, ki se nanašajo na prve tri faze (pridobivanje, ohranitev in forenzični pregled). Preiskovalna analiza in predstavitev izsledkov digitalne forenzične preiskave (oziroma digitalnih dokazov) pa poteka po splošnih kriminalističnih pravilih oziroma pravilih dokaznega prava ter pravilih o izvedenstvu in pričanju.

Že uvodoma je treba zapisati, da je področje digitalne forenzike in s tem tudi digitalnih dokazov zelo fleksibilno in hitro se spreminjajoče, zato je na zakonski ravni primerno definirati le temeljne smernice in morebitne omejitve v zvezi s posameznimi procesnimi dejanji, povezanimi z digitalnimi dokazi. To je slovenski zakonodajalec storil z novelo ZKP-J, kar pa je le prvi korak. Podrobnosti v zvezi s pridobivanjem, analizo in predstavitvijo digitalnih dokazov bi bilo primerno urediti oziroma izdati v obliki

[4] Z digitalnimi dokazi se lahko dokazujejo tudi na primer goljufije, ponarejanje listin, lažni stečaji, neupravičena proizvodnja in promet s prepovedanimi drogami, davčne zatajitve, nevestno delo v službi, tatvine, kršitve tajnosti občil, zlorabe osebnih podatkov ipd.

[5] Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku, Ur.l. RS št. 77/2009.

[6] Zakon o kazenskem postopku, ZKP-UPB4, Ur.l. RS št 32/2007 in Ur.l. RS št. 68/2008 in 77/2009.

[7] Prim. Kovačič, s. 1.

[8] Prim. Bianchi in Pollit, s. 85.

navodil, prilagojenih funkciji posameznega organa (optimalno bi bilo pripraviti ločena navodila o digitalnih dokazih za policijo, za tožilstvo in za sodišča). Prednost takega pristopa je v tem, da so navodila precej bolj fleksibilna od zakona in je z njimi lažje slediti hitremu tehnološkemu napredku ter razvoju teorije in prakse na področju digitalne forenzike. Navodila bi lahko v obliki na primer podzakonskega akta izdal kateri od državnih organov, lahko pa bi jih pripravila tudi kakšna specializirana institucija. Bolj kot to, kdo bo navodila izdal, je pomembno, da so pripravljena strokovno in da so kratka, jasna in izražena na način, razumljiv naslovnikom.[9]

V tem prispevku skušamo s pomočjo primerjalne metode izpostaviti nekatera vprašanja in dileme, ki se pojavljajo v zvezi z digitalnimi dokazi v kazenskih postopkih. Poudarek je na domači pravni ureditvi in tuji sodni praksi (ker domače ni prav veliko).

[9] Na svetovnem spletu je dostopnih kar nekaj dokumentov, ki bi lahko predstavljali dober vzorec pri oblikovanju navodil za policijo in širše področje slovenskega pravosodja. Več o tem gl. Bernard in ostali, s. 56.

## Temeljno o digitalnih dokazih

V osnovi bi lahko digitalne dokaze razdelili v dve skupini: 1) na digitalne dokaze, shranjene v elektronski (računalniški) obliki, in 2) na digitalne dokaze, ustvarjene s strani računalniškega programa ali operacijskega sistema. Dokazi, shranjeni v elektronski obliki, so dokumenti in drugi podatki, ki jih je ustvaril posameznik in so v konkretnem primeru pač shranjeni na primer na trdem disku (fiktivni računi ali drugi dokumenti, elektronska pošta s sporno vsebino ipd.). Tovrstni dokazi lahko vsebujejo in potrjujejo izjavo, namero, željo, voljo določene osebe. Dokazi, ustvarjeni z računalniškim programom, pa kažejo na določeno dejavnost v računalniškem ali drugem informacijskem sistemu (na primer vstop v določeno računalniško omrežje ali sistem, opravljen telefonski klic ipd.) ali pa dokumentirajo določeno stanje ali dogodek (na primer digitalna fotografija, posnetek z digitalno kamero ipd). Kar se tiče vprašanja, ali gre za neposredne (*direct*) ali posredne (*circumstantial, indirect*) dokaze,[10] lahko digitalni dokazi predstavljajo oboje. Na primer zapis prijave (*computer logon record*) je neposredni dokaz, da je bil določen račun (*account*) uporabljen za dostop v računalniški sistem v določenem času, a le posredni dokaz za to, da je dejanje izvršil imetnik tega računa. Obstaja namreč možnost, da je imetnikov račun (zlo)/(upo)rabil nekdo drug, zato bodo potrebni še drugi dokazi za to, da je bil prav imetnik računa tisti, ki je v določenem času vstopil v določen računalniški sistem.[11]

S pravnega vidika se pogosto poudarja, da digitalni dokaz ni v bistvu nič drugačen od teksta v papirnem dokumentu, zato obstajajo mnenja, da naj bi bili ti dokazi podvrženi enakim pravilom, ki se uporabljajo za dokumentarne dokaze. Vendar zadeva ni tako preprosta. Dejstvo je, da je tudi digitalni dokaz v prvi vrsti dokaz[12] in zato zanj ne morejo veljati drugačna *temeljna pravila* kot za ostale dokaze. Da se lahko uporabi na sodišču, mora dokaz v splošnem izpolnjevati dva pogoja: 1) biti mora pravno dopusten in 2) imeti mora ustrezno dokazno vrednost. To v celoti velja tudi za digitalne dokaze. Vendar pa je za pravilno ovrednotenje pravne dopustnosti in dokazne vrednosti potrebno upoštevati značilnosti digitalnih dokazov, zaradi katerih imajo bistveno drugačno dejansko naravo od klasičnih dokazov.[13] Predvsem ameriška sodišča so na

---

[10] Neposredni (direktni) dokazi neposredno kažejo na odločilna pravna dejstva, posredni dokazi pa kažejo na to s pomočjo indicev oziroma logičnega sklepanja. Prim. Dežman in Erbežnik, s. 540.

[11] Prim. Casey, s. 179.

[12] Dokaz je v pravnem smislu vir spoznanja o kakem pomembnem dejstvu oziroma sinonim za logično in izkustveno sprejemljivo trditev o obstoju kakega pravno pomembnega dejstva. Gl. Dežman in Erbežnik, s. 539.

[13] Chaikin izpostavlja na primer naslednje pomembne okoliščine, povezane z digitalnimi dokazi: 1) poseganje v digitalne zapise (vstavljanje, spreminjanje, brisanje) je tako enostavno, da lahko do tega pride tudi po naključju, 2) tudi strokovna forenzična preiskava ne bo nujno pokazala, ali je bilo poseženo v določen digitalni zapis, 3) ne obstajajo splošno sprejeti standardi za najboljšo prakso na področju forenzičnih postopkov v zvezi z digitalnimi dokazi, niti za potrebno izobrazbo in strokovno izpopolnjevanje digitalnih forenzičnih preiskovalcev in 4)

podlagi lastnih napak sčasoma uspela ugotoviti, da digitalni dokazi vendarle ne morejo biti vedno (o)vrednoteni enako kot klasični dokazi, ampak zaradi svojih tehničnih karakteristik[14] oziroma posebnosti terjajo drugačen pristop pri ocenjevanju, pa tudi vrednotenju pravne dopustnosti ter dokazne vrednosti.

Da so pravno dopustno dokazno sredstvo na sodišču, morajo biti digitalni dokazi pridobljeni, shranjeni in analizirani ob upoštevanju vseh standardov, ki jih za postopanje z dokazi v širšem smislu določata Ustava RS in ZKP. Dokazi, pridobljeni na nedovoljen način, so predmet izločitve oziroma ekskluzije.[15] Če je bila preiskava elektronske naprave opravljena brez odredbe sodišča ali v nasprotju z njo ali brez pisne privolitve imetnika ter znanih in dosegljivih uporabnikov elektronske naprave, sodišče na podlagi izrecne določbe enajstega odstavka 223.a člena ZKP svoje odločbe ne sme opreti na zapisnik o preiskavi in na tako pridobljene podatke, kar pomeni, da pridobljeni digitalni dokazi niso pravno dopustni.

Standardi pravičnega sojenja pa zahtevajo, da se tudi na zakonit način pridobljeni digitalni dokazi pravilno ovrednotijo,[16] saj je napačna informacija v obliki dokaza v kazenskem postopku lahko celo bolj škodljiva od odsotnosti vsakršnega dokaza. Kar se tiče dokazne vrednosti digitalnih dokazov, pri nas enako kot za vse ostale dokaze velja načelo proste presoje dokazov. Če želi biti sicer prosta ocena dokaza pravilna, pa je nujno poznavanje in upoštevanje narave digitalnih dokazov.

Pri klasičnih dokazih dejstvo, da prestanejo ekskluzijski test, praviloma pomeni visoko dokazno vrednost. Ob zakonitem zasegu ali drugačni pridobitvi klasičnega dokaza zagotavljanje njegove integritete in verodostojnosti namreč praviloma ni problematično. Pri digitalnih dokazih pa ni nujno tako. Poudariti je treba, da dokaz v postopku ni nosilec digitalnega dokaza kot fizični predmet, ampak je dokaz informacija, zabeležena na takšnem predmetu. Zavarovanje in ohranjanje teh informacij oziroma dokazov utegne biti zelo kompliciran in je pogosto najbolj ključna faza v postopku s

---

sodoben svet je čedalje bolj odvisen od digitalnih podatkov, količina digitalnih dokazov pa ima pomemben vpliv na preiskovalne postopke. Prim. Chaikin, s. 241–243.

[14] Digitalni dokazi so pogosto v obliki, ki ni neposredno berljiva, zato v večini primerov ne moremo videti podatkov, ki jih vsebuje nosilec digitalnega dokaza. Da postane dokaz dostopen (berljiv), je potrebna strojna in programska računalniška oprema, pogosto pa tudi znanje in pomoč digitalnega forenzika, pri čemer je treba vedeti, kaj takega strokovnjaka sploh vprašati. Scheetz, s. 14.

[15] Na podlagi drugega odstavka 18. člena ZKP sodišče ne sme opreti sodne odločbe na dokaze, ki so bili pridobljeni s kršitvijo ustavno določenih človekovih pravic in temeljnih svoboščin, kot tudi ne na dokaze, ki so bili pridobljeni s kršitvijo določb kazenskega postopka in je zanje v ZKP določeno, da se sodna odločba nanje ne more opreti, ali ki so bili pridobljeni na podlagi takega nedovoljenega dokaza

[16] Podobno kot pri ostalih tipih dokazov (listinah, pričanju ipd.) je relevantnost digitalnega dokaza odvisna od tega, od kje dokaz izvira, kako je bil ustvarjen in kaj se skuša z njim dokazati. Zlasti materialni dokazi, ki sami zase dokazujejo to, kar je njihova vsebina, so lahko v veliko pomoč pri iskanju resnice v posameznem primeru (na primer digitalne fotografije v kazenskem postopku zaradi otroške pornografije, elektronska pošta v primeru preiskave internetne goljufije ipd.).

temi dokazi. Če pride tukaj do napake, je dokaz izgubljen najmanj zaradi dvoma v njegovo zanesljivost oziroma verodostojnost (integriteto).[17]

Praktično gledano, digitalni dokaz ni nič drugega kot serija elektronskih impulzov, shranjenih v bolj ali manj stabilni obliki. Ti shranjeni impulzi *so* dokaz – ko oziroma če pride do njihove spremembe (do te pa lahko pride zelo hitro),[18] njihova dokazna vrednost postane vprašljiva in lahko zbledi ali pa je odvisna od dodatne presoje narave spremembe. Ker so digitalni dokazi »izjemno hlapljivi« (*highly volatile*), je njihova dokazna vrednost torej v veliki meri odvisna od strokovnosti tistega, ki te dokaze zavaruje in nato zbira in analizira.

Z uveljavitvijo novele ZKP-J so se obrambi v zvezi z digitalnimi dokazi razmeroma zožile možnosti izpodbijanja njihove pravne dopustnosti zaradi postopka, po katerem je bil pridobljen. Še vedno pa zaradi njegove narave obstajajo razmeroma široke možnosti zbujanja dvoma v zanesljivost oziroma relevantnost digitalnega dokaza, s čimer se seveda niža dokazna vrednost in ob morebitni odsotnosti preostalih dokazov zmanjšujejo možnosti za obsodilno sodbo. Ocena vrednosti oziroma zanesljivosti digitalnega dokaza je v konkretnem primeru torej lahko odločilnega pomena; da je pravilna, pa pogosto terja precejšnjo mero razgledanosti sodnika na področju sodobne informacijsko-telekomunikacijske tehnologije. Kot rečeno, so tudi digitalni dokazi predmet proste presoje dokazov, se pravi, da sodišče pri presoji njihove dokazne vrednosti ni vezano na nobena določila o tem, kako oceniti vrednost posameznega dokaza, ampak ta ocena poteka po pravilih logičnega sklepanja in analiziranja.

V tuji literaturi se poudarjajo zlasti trije elementi,[19] na katere je treba biti izrazito pozoren pri presoji dokazne vrednosti digitalnih dokazov. To so: [20]

---

[17] Scheetz, s. 26. Računalniki v ozadju izvajajo številne procese, kar morajo digitalni forenziki brez izjeme in natančno upoštevati pri zavarovanju oziroma pridobivanju digitalnih dokazov, sicer ti ne bodo imeli dokazne vrednosti na sodišču.

[18] Digitalni dokazi so latentni prav v taki ali morda še v večji meri kot prstni odtis ali deoksiribonukleinska kislina (DNK). V primerjavi s klasično papirno dokumentacijo so digitalni dokazi morda težje uničljivi (če niso kratkega roka), a jih je lažje spremeniti, prirediti ali celo ponarediti, kar lahko vpliva na njihovo dokazno vrednost. Digitalni dokaz je po svoji naravi torej krhek in lahko tudi kratkotrajen. Posebej je treba opozoriti tudi na to, da je te dokaze mogoče spremeniti, poškodovati ali uničiti tudi z nepravilnim ravnanjem med preiskavo, zato morajo biti za dokumentiranje, zbiranje, shranjevanje in analizo teh podatkov izpolnjeni določeni pogoji in spoštovana določena pravila. Več o tem Selinšek, Malovrh, s. 57–78.

[19] Giordano (s. 162) pa navaja primer priročnika za digitalne forenzične preiskave, v katerem je pojasnjeno, da mora biti preiskava opravljena tako, da se zagotovi kar pet elementov, in sicer morajo biti pridobljeni digitalni dokazi:

1) dopustni (*admissible*) – pridobljeni skladno s pravnimi pravili;

2) avtentični (*authentic*) – obstajati mora vzročna zveza med dokazom in incidentom;

3) popolni (*complete*) – dokaz mora sporočati celotno zgodbo in ne zgolj posameznega dela;

4) zanesljivi (*reliable*) – način pridobitve dokaza in ravnanje z njim ne smeta v nobenem primeru zbujati dvoma o avtentičnosti in verodostojnosti dokaza; in

5) verjetni (*believable*) – dokaz mora biti brez težav verjeten in razumljiv za člane porote.

1) *avtentičnost*: vprašanje avtentičnosti (*authenticity*) digitalnega dokaza ima dva vidika. Prvi se nanaša na vzročno zvezo med dokazom na eni strani in osumljencem oziroma obdolžencem na drugi stani. Ta je lahko zelo problematična za ugotavljanje. Dejstvo, da je bilo določeno kaznivo dejanje izvršeno z osumljenčevim ali obdolženčevim računalnikom ali preko njega, namreč ne pomeni nujno, da je imetnik računalnika tudi storilec. Treba je preveriti, ali ni v času izvršitve dejanja z računalnikom upravljala druga oseba in ali ni dokaza na računalnik podtaknil kakšen od zlonamernih računalniških programov (na primer trojanski konj).[21] Drugi vidik avtentičnosti digitalnega dokaza pa se nanaša na ustrezno povezavo med dokazom in računalnikom oziroma računalniškim sistemom, se pravi na vprašanje, ali je določen dokaz res povezan z določenim računalnikom (*computer source test*);[22]

2) *neokrnjenost*: neokrnjenost (*integrity*) je zagotovljena, če je digitalni dokaz, predočen sodišču, enak kot v času storitve kaznivega dejanja. V pravnih redih, kjer poznajo t. i. *best evidence rule*, po katerem je sprejemljiv dokaz praviloma le dokaz v originalni obliki (na primer originalna listina), kopija pa je upoštevna samo, če originala ni in če ne obstajajo nobene okoliščine, ki bi kazale na spornost kopije, so digitalni dokazi odprli posebno vprašanje, saj se preiskave nosilcev digitalnih dokazov praviloma opravljajo na kopijah teh nosilcev. Avtorji večinoma zastopajo stališče, da je tak pristop ustrezen in da ne nasprotuje pravilu najboljšega dokaza, saj tehnologija omogoča povsem natančno kopiranje nosilcev digitalnih. Celo na papir natisnjeni dokumenti, ki so sicer v digitalni obliki, lahko štejejo za originalne dokaze, vendar le, če so vsi deli originala vidni v natisnjeni obliki,[23] in

3) *preverljivost*: preverljivost (*accountability*) elektronskih dokazov je pogojena z okoliščinami njihovega pridobivanja in ravnanja z njimi. Vsi, ki imajo na kakršenkoli način opravka z nosilci elektronskih dokazov, morajo nadvse skrbno paziti, da ne pride do sprememb podatkov na teh nosilcih, saj je s tem elektronski dokaz lahko uničen oziroma izgubi pravno veljavo. S tega vidika je zelo ustrezna že omenjena praksa, po kateri se preiskave nosilcev digitalnih dokazov opravljajo na kopijah teh nosilcev (pri čemer je treba zagotoviti popolno identičnost kopije z originalom). To po potrebi zagotavlja preverljivost dokazov, saj je originalni nosilec vedno na voljo (po možnosti skrbno shranjen in zapečaten).

---

[20] Podrobneje o tem Walden, s. 378–382.

[21] Trojanski konji so majhni programi, ki so najpogosteje skriti v drugih programih. Izvirne programe lahko storilci spremenijo, tako da vanje dodajo svoje programe, lahko pa tudi sami izdelajo na videz popolnoma legalne programe, vanje pa skrijejo dodatne funkcije, ki izvajajo neavotrizirane operacije. Namen trojanskih programov je predvsem v zbiranju raznih sistemskih informacij (na primer gesel) ali v uničevanju sistemov. Če je na računalniku domnevnega storilca trojanski konj, je treba nujno razjasniti, kako se je ta program znašel tam. Pri tem je lahko v pomoč sumljiva elektronska pošta, vendar je treba biti dalje pozoren na to, ali ni morda pošiljatelj trojanskega konja poslal nevede, se pravi, da je dejansko tudi sam »napaden« s strani tega programa itd..

[22] Podrobneje o tem tudi Giordano, s. 163–165.

[23] Prim. tudi Casey, s. 178.

Povzeti je torej mogoče, da je dokazna vrednost digitalnega dokaza lahko pravilno ocenjena le, če sodnik pozna temeljne postopke in pravila za pridobivanje teh dokazov. V nasprotnem primeru lahko vešča obramba zbudi dvom v dokaz četudi za to ni realne podlage, vešč tožilec pa sodišče prepriča o verodostojnosti sicer trhlega digitalnega dokaza. Oboje lahko bistveno vpliva na pravilnost končne sodbe, zato je potrebno na sistemski ravni storiti vse, da se temu izognemo. Ne prezreti pa gre niti opozoril v literaturi, da obsodba za (kibernetsko) kaznivo dejanje praviloma ne bi smela temeljiti izključno na enem samem digitalnem dokazu.[24]

[24] Prim. Chaikin, s. 256.

## Zaseg, zavarovanje podatkov in preiskava elektronskih naprav po ZKP-J

Kot razlog, da se je slovenski zakonodajalec odločil v ZKP vnesti določbe o zasegu in preiskavi elektronskih naprav, se v prvi vrsti navaja odločba Ustavnega sodišča RS Up-106/05 z dne 2.10.2008.[25] V tem primeru je Ustavno sodišče obravnavalo področje varstva komunikacijske zasebnosti in poudarilo, da to varstvo poleg vsebine komunikacije vključuje tudi vse podatke, povezane s to komunikacijo. Ustavno sodišče je ocenilo, da pridobitev podatkov o zadnjih opravljenih in zadnjih neodgovorjenih klicih ter vpogled v vsebino sporočila SMS pomenita vpogled v vsebino in okoliščine komunikacije ter s tem poseg v pravico iz prvega odstavka 37. člena Ustave,[26] ki zagotavlja varstvo posameznikovega interesa, da se brez njegove privolitve nihče ne seznani z okoliščinami in vsebino sporočila, ki ga posreduje prek kateregakoli sredstva, ki omogoča izmenjavo ali posredovanje informacij, kot tudi interesa posameznika, da svobodno odloča o tem, komu, v kakšnem obsegu, na kakšen način in pod kakšnimi pogoji bo posredoval določeno sporočilo. Sodišče je odločilo, da je pridobitev navedenih podatkov v predkazenskem postopku s strani policije brez sodne odločbe protiustavna, kar je zakonodajalec razumel kot posreden opomin, da je to področje treba konkretneje zakonsko urediti.[27]

Poudariti je treba, da nova 219.a in 223.a člena ZKP ne urejata le primerov pridobivanja digitalnih dokazov, pri katerem se posega v ustavno zavarovano pravico do komunikacijske zasebnosti (na te primere se nanaša omenjena odločba ustavnega sodišča), ampak se je zakonodajalec odločil za precej širši koncept in je z novima členoma zajel pridobivanje vseh podatkov v elektronski obliki, ne glede na njihovo naravo. Nova člena torej ne urejata le pridobivanja digitalnih dokazov, ki so povezani z vsebino komunikacije in prometnimi podatki v zvezi z njo, ampak se nanašata na pridobivanje vseh podatkov, ki so v elektronski obliki in so pomembni za kazenski postopek. V zvezi s tem člena precej kompleksno in medsebojno povezano, a vseeno tako, da jih je treba ustrezno ločevati, urejata tri procesna dejanja v zvezi z digitalnimi dokazi:

- *zaseg elektronske naprave* (določbe o zasegu elektronske naprave so specialne napram splošnim določbam ZKP o zasegu predmetov. Pri tem je treba opozoriti na široko opredelitev pojma elektronske naprave, in sicer ZKP ta izraz uporablja za elektronske in z njimi povezane naprave, pa tudi za nosilce elektronskih podatkov, pri čemer zgolj primeroma našteva telefon, telefaks, računalnik, disketo, optični mediji in spominske kartice.),

[25] Ur.l. RS, št. 100/08

[26] Poseg v svobodo komuniciranja pa je po drugem odstavku navedenega člena Ustave dopusten le, če so izpolnjeni naslednji pogoji: 1) da je poseg določen v zakonu, 2) da poseg s svojo odločbo dovoli sodišče, 3) da je določno omejen čas izvajanja posega in 4) da je poseg nujen za uvedbo ali potek kazenskega postopka ali za varnost države.

[27] Prim. Predlog zakona o spremembah in dopolnitvah Zakona o kazenskem postopku, EVA:2008-2011-0117, s. 2.

- *zavarovanje podatkov v elektronski obliki* (opravi se tako, da se elektronski podatki shranijo na drug ustrezen nosilec podatkov ali se izdela istovetna kopija celotnega nosilca podatkov) in
- *preiskavo elektronske naprave* (obsega pridobivanje podatkov iz elektronske naprave, se pravi pridobivanje digitalnih dokazov, ki jih vsebuje elektronska naprava).

Skladno s prvim odstavkom 219.a člena ZKP se preiskava elektronske naprave lahko opravi *zaradi pridobitve podatkov v elektronski obliki*, če so podani utemeljeni razlogi za sum, da je bilo storjeno kaznivo dejanje[28] in je podana verjetnost, da elektronska naprava vsebuje elektronske podatke:

- na podlagi katerih je mogoče osumljenca ali obdolženca identificirati, odkriti ali prijeti ali odkriti sledove kaznivega dejanja, ki so pomembni za kazenski postopek, ali
- ki jih je mogoče uporabiti kot dokaz v kazenskem postopku.

Preiskava, torej pridobivanje podatkov oziroma dokazov iz elektronske naprave, se primarno opravi na podlagi vnaprejšnje pisne privolitve imetnika ter policiji znanih in dosegljivih uporabnikov elektronske naprave, ki na njej utemeljeno pričakujejo zasebnost (uporabnik).[29] Če take privolitve ni, se preiskava lahko opravi le na podlagi obrazložene pisne odredbe sodišča, izdane na predlog državnega tožilca.[30] Predlog in odredba o preiskavi elektronske naprave[31] morata vsebovati:

- podatke, ki omogočajo identifikacijo elektronske naprave, ki se bo preiskala;
- utemeljitev razlogov za preiskavo;
- opredelitev vsebine podatkov, ki se iščejo;
- druge pomembne okoliščine, ki narekujejo uporabo tega preiskovalnega dejanja in določajo način njegove izvršitve.

Izjemoma, če pisne odredbe za preiskavo elektronske naprave ni mogoče pravočasno pridobiti, ter če obstaja neposredna in resna nevarnost za varnost ljudi ali premoženja,[32] lahko preiskovalni sodnik skladno s petim odstavkom 219.a člena ZKP na ustni predlog državnega tožilca odredi *preiskavo elektronske naprave* z ustno odredbo. O predlogu državnega tožilca in odredbi preiskovalni sodnik izdela uradni zaznamek.

---

[28] Zakon ne zahteva utemeljenih razlogov za sum, da je bilo storjeno *uradno pregonljivo* kaznivo dejanje, ampak le utemeljene razloge za sum, da je bilo storjeno kaznivo dejanje, iz česar bi bilo mogoče sklepati, da pravila iz 219.a in 223.a člena ZKP smiselno veljajo tudi za kazniva dejanja, ki se preganjajo na zasebno tožbo.

[29] Kot poudarja Kovačič (s. 2), bo ta možnost prišla v poštev predvsem tedaj, ko se bodo iskali elektronski dokazi na napravi v lasti žrtve kaznivega dejanja.

[30] Če se preiskava opravi na podlagi odredbe sodišča, se izvod te odredbe pred začetkom preiskave izroči imetniku oziroma uporabniku elektronske naprave, ki naj se preišče (prim. drugi odstavek 219.a člena ZKP).

[31] Če se preiskava elektronske naprave odredi v odredbi za hišno ali osebno preiskavo, za izdajo tega dela odredbe in njeno izvršitev veljajo pogoji in postopki iz tega člena. V tem primeru tudi predlog za hišno ali osebno preiskavo poda državni tožilec (prim. četrti odstavek 219.a člena ZKP).

[32] Gre torej za nujne primere.

Pisna odredba mora biti izdana najpozneje v dvanajstih urah po izdaji ustne odredbe, sicer mora policija, ki je odredbo izvršila, zapisniško uničiti ali izbrisati shranjene ali kopirane podatke in o tem v osmih dneh obvestiti preiskovalnega sodnika, državnega tožilca in imetnika oziroma uporabnika elektronske naprave, če je znan. Določba o uničenju podatkov je smiselno ponovljena v drugem odstavku 223.a člena ZKP, po katerem v primeru, če je bila elektronska naprava zasežena brez odredbe sodišča[33] in je bila zaradi zavarovanja podatkov izdelana njihova kopija,[34] vendar sodišče v dvanajstih urah ni izdalo odredbe za preiskavo oziroma ni bila pridobljena privolitev imetnika in znanih uporabnikov naprave, policija zapisniško trajno uniči izdelano kopijo in o tem v osmih dneh pisno obvesti preiskovalnega sodnika, državnega tožilca in imetnika oziroma uporabnika elektronske naprave, če je znan.

Imetnik oziroma uporabnik elektronske naprave mora omogočiti dostop do naprave, predložiti šifrirne ključe[35] oziroma šifrirna gesla in pojasnila o uporabi naprave, ki so potrebna, da se doseže namen preiskave.[36] Posameznika, ki tega noče, sme sodišče kaznovati z denarno kaznijo, ki lahko znaša najmanj eno petino zadnje uradno objavljene povprečne mesečne neto plače v Republiki Sloveniji na zaposleno osebo, in največ trikratni znesek te plače. Če posameznik še vedno ne sodeluje, pa se ga sme zapreti. Zapor lahko traja do takrat, da posameznik omogoči dostop do naprave oziroma predloži šifrirne ključe ali gesla oziroma da potrebna pojasnila, ali pa do konca kazenskega postopka, vendar v nobenem primeru ne več kot mesec dni. Pri tem je treba

---

[33] Pri tem je treba biti pozoren na to, da ZKP ne zahteva odredbe oziroma privolitve za zaseg elektronske naprave, ampak le za preiskavo, torej vsebinski vpogled v podatke, shranjene v elektronski napravi. Del drugega odstavka 223.a člena ZKP, ki govori o elektronski napravi, zaseženi brez odredbe sodišča, se torej ne nanaša na odredbo za zaseg elektronske naprave, ampak *na odredbo za preiskavo elektronske naprave*. Ta odredba lahko (ni pa to nujno) med drugimi pomembnimi okoliščinami, ki določajo način izvršitve odredbe, navaja tudi zaseg elektronske naprave.

[34] Opozoriti je treba, da se ta določba in s tem 12-urni rok nanaša le na nujne primere, ko je bila *poleg zasega elektronske naprave izdelana kopija podatkov v napravi* (zaradi zavarovanja). Če je prišlo zgolj do zasega naprave, zakon tudi za nujne primere ne določa roka, v katerem je treba pridobiti pisno odredbo za preiskavo oziroma je ta rok določen posredno v sedmem odstavku 223.a člena ZKP, ki ureja hrambo zasežene elektronske naprave.

[35] Kot pojasnjuje Kovačič, bodo zakonske določbe o obveznosti razkritja šifrirnih ključev v praksi na primer v primeru, ko posameznik uporablja tehniko verodostojnega zanikanja (*plausible deniability*), neuporabne. Ta tehnika namreč omogoča, da se znotraj šifrirnega kontejnerja ustvari še en (skrit) šifrirni kontejner, ki ga je mogoče odkleniti z drugim šifrirnim ključem. Če torej uporabnik osnovni šifrirni kontejner odpre z enim ključem, se pokažejo eni podatki, če ga odpre z drugim, se pokažejo drugi podatki. Uporabnik, ki bo torej prisiljen razkriti šifrirne ključe, bo v primeru uporabe verodostojnega zanikanja v program za dešifriranje podatkov vpisal geslo, ki bo razkrilo zanj razbremenilne podatke, zanj obremenilni podatki pa bodo še vedno varno skrit. Sistem je zasnovan tako, da ni mogoče ugotoviti, ali konkretni šifrirni kontejner vsebuje še skrit šifrirni kontejner. Podrobneje o tem Kovačič, s. 5.

[36] Kovačič ob tem opozarja, da obveznost imetnika elektronske naprave glede pojasnil o uporabi naprave ne sme biti nesorazmerna oziroma ga preiskovalci na primer zaradi svojega neznanja ne smejo nesorazmerno obremeniti in od njega zahtevati brezplačnega strokovnega sodelovanja. Kovačič, s. 4.

izrecno poudariti, da možnost kaznovanja ne velja za osumljenca oziroma obdolženca in za osebe, ki ne smejo biti zaslišane kot priče ali so se v skladu z zakonom odrekle pričevanju,[37] s čimer se zagotavlja spoštovanje ustavnega privilegija zoper samoobtožbo.[38]

Preiskava elektronske naprave se mora opraviti tako, da se ohrani integriteta izvirnih podatkov in možnost njihove uporabe v nadaljnjem postopku. Preiskava mora biti opravljena na način, s katerim se v najmanjši možni meri posega v pravice oseb, ki niso osumljenci ali obdolženci, in varuje tajnost oziroma zaupnost podatkov ter ne povzroča nesorazmerna škoda.[39]

Ko se zaseže elektronska naprava zaradi oprave preiskave, se podatki v elektronski obliki zavarujejo[40] tako, da se shranijo[41] na drug ustrezen nosilec podatkov na način, da se ohrani istovetnost in integriteta podatkov ter možnost njihove uporabe v nadaljnjem postopku ali se izdela istovetna kopija celotnega nosilca podatkov, pri čemer se zagotovi integriteta kopije teh podatkov.[42] Če to ni mogoče, se elektronska naprava zapečati (če je mogoče, se zapečati samo tisti del naprave, ki naj bi vseboval iskane podatke).[43] Imetnika naprave se povabi, naj bo sam, njegov zastopnik, odvetnik ali

---

[37] Enak sistem po 3. odstavku 223.a člena ZKP velja za imetnika, uporabnika, upravljavca ali skrbnika elektronske naprave oziroma tistega, ki ima do nje dostop, če na zahtevo organa, ki je napravo zasegel, takoj ne ukrene vsega, kar je potrebno in je v njegovi moči, da se onemogoči uničenje, spreminjanje ali prikrivanje podatkov.

[38] O dilemah v zvezi s privilegijem zoper samoobtožbo v informacijski dobi gl. Selinšek, Privilegij …, s. 11–13.

[39] Tako določa sedmi odstavek 219.a člena ZKP. Skladno z osmim odstavkom istega člena se o preiskavi napravi zapisnik, ki med drugim obsega identifikacijo elektronske naprave, ki je bila pregledana, datum ter uro začetka in konca preiskave, morebitne sodelujoče in navzoče osebe, številko odredbe in sodišče, ki jo je izdalo, način izvedbe preiskave, ugotovitve preiskave in druge pomembne okoliščine.

[40] Tudi zaseg in zavarovanje podatkov morata biti opravljena tako, da se v najmanjši možni meri posega v pravice oseb, ki niso osumljenci ali obdolženci, in varuje tajnost oziroma zaupnost podatkov ter se ne povzroča nesorazmerna škoda zaradi nezmožnosti uporabe elektronske naprave (šesti odstavek 223.a člena ZKP).

[41] Kopije zaseženih podatkov se na podlagi sedmega odstavka 223.a člena ZKP hranijo, dokler je to potrebno za postopek. Elektronska naprava pa se hrani, dokler podatki niso shranjeni na način, ki zagotovi istovetnost in integriteto zaseženih podatkov, vendar ne več kakor tri mesece od dneva pridobitve. Če izdelava takšne kopije podatkov ni mogoča, se elektronska naprava ali njen del, ki vsebuje iskane podatke, hrani, dokler je to potrebno za postopek, vendar ne več kakor šest mesecev od dneva pridobitve, razen če je bila zasežena elektronska naprava uporabljena za izvršitev kaznivega dejanja oziroma je sama elektronska naprava dokaz v kazenskem postopku. ZKP torej uveljavlja načelo, da se zasežena elektronska naprava čim prej vrne imetniku, saj za kazenski pregon ni bistven nosilec, pač pa vsebina podatkov (načelo ima seveda določene izjeme). Prim. tudi Kovačič, s. 8. Avtor opozarja tudi na nerešeno vprašanje, kaj storiti v primerih, ko zakonodaja zahteva odvzem spornih podatkov.

[42] Pri zavarovanju podatkov se v zapisnik zapiše tudi kontrolna vrednost, oziroma se na drug ustrezen način v zapisniku zagotovi možnost naknadnega preverjanja istovetnosti in integritete zavarovanih podatkov (peti odstavek 223.a člena ZKP).

[43] Prim. prvi odstavek 223.a člena ZKP.

strokovnjak navzoč pri zavarovanju podatkov (ne more pa biti navzoč pri preiskavi). Če se ne odzove vabilu, če je odsoten ali če ni znan, se zavarovanje podatkov in izdelava istovetne kopije skladno s 4. odstavkom 223.a člena ZKP lahko opravi v njegovi nenavzočnosti.

Na podlagi izrecne določbe prvega odstavka 8. člena 219.a člena ZKP preiskavo opravi strokovno usposobljena oseba (enako skladno s četrtim odstavkom 223.a člena velja za zavarovanje podatkov). Obstajajo mnenja, da je ta oseba lahko le kriminalist ali druga oseba znotraj policije,[44] vendar ZKP te omejitve ne postavlja, kar pomeni, da se lahko izvedba preiskave zaupa tudi osebi izven policije ali organizaciji, znotraj katere delujejo strokovno usposobljene osebe za opravljanje digitalnih forenzičnih preiskav. Seveda pa morata nad tako preiskavo praviloma bdeti policija ali državno tožilstvo. V zvezi z zakonskim standardom strokovno usposobljene osebe je kup odprtih vprašanj,[45] dejstvo pa je, da je zaradi odsotnosti sistemskega (in globalnega) pristopa k reševanju teh vprašanj[46] v končni fazi sodišče tisto, ki bo moralo presoditi, ali je v konkretnem primeru digitalno forenzično preiskavo opravila strokovno usposobljena oseba.[47]

[44] Tako Lang, s. 180.

[45] Prim. Bernard in ostali, s. 27–29.

[46] Čeprav se zdi, da ZDA znatno prednjačijo na tem področju, je študija, opravljena v letu 2007, razkrila, da imajo tudi tam precej težav z usposobljenostjo organov odkrivanja, pregona in sojenja za ravnanje z digitalnimi dokazi. Medtem ko preiskovalci iz večjih organizacij (na primer FBI), ki imajo več možnosti za izobraževanje in boljšo opremo, vse bolj vključujejo digitalne forenzične preiskave v rutinsko preiskovalno delo, je v manjših preiskovalnih organizacijah (in takih je 90%) uporaba digitalnih forenzičnih preiskav znatno manjša, kar se lahko odraža tudi v tem, da se spregledajo pomembni (obremenilni ali razbremenilni) dokazi. Več o študiji gl. Rogers in drugi, sl. 42–52.

[47] Najbližje standardu strokovno usposobljene osebe za opravljanje preiskav elektronskih naprav je verjetno profil digitalnega forenzika. Popis in predstavitev osnovnih znanj, ki bi jih moral imeti digitalni forenzik, podaja na primer Craiger, s. 11–22. Avtor opozarja na to, da je treba ločevati pojma izobraževanje (*education*) in urjenje (*training*), ter predstavlja obseg znanj, ki jih mora imeti posameznik, da lahko uspešno in pravilno izvede digitalno forenzično preiskavo ter predstavi relevantne rezultate.

## Nekaj izbranih vprašanj

### »Plain view« doktrina in digitalni dokazi

*Plain view* doktrina je izraz, s katerim se označuje pravilo, da je lahko obremenjujoči dokaz zasežen tudi brez odredbe sodišča oziroma sodnega naloga, če je v »čistem pogledu« (*plain view*) preiskovalca, ki izvaja zakonito preiskavo. Gre torej za zaseg dokazov brez naloga (*warrantless seizure*).[48]

Iz ameriške sodne prakse je mogoče razbrati dve vrsti situacij, v katerih lahko pride do zasega elektronske naprave ali elektronskega dokaza na podlagi *plain view* doktrine. Prva zajema primere, ko se digitalni dokaz razkrije na računalniškem ekranu, medtem ko policija opravlja (hišno) preiskavo in išče fizične dokaze. V primerih *City of Akron v. Patrick*[49] (1982) in *Oklahoma v. One Pioneer CD-ROM Changer*[50] (1994) je sodišče odločilo, da se lahko na podlagi teksta ali slikovnega gradiva, ki se pojavi na ekranu, izvede zaseg računalnika (čeprav ta ni zajet v nalogu za preiskavo) na podlagi *plain view* doktrine, če je prikaz na ekranu takoj mogoče prepoznati kot dokaz. V navedenih primerih je šlo za kaznivo dejanje tihotapstva, Moore pa navaja, da bi lahko bila tipičen primer tudi otroška pornografija. Če bi policist pri izvajanju naloga za preiskavo na primer kaznivega dejanja hude telesne poškodbe po vstopu v stanovanje osumljenega na računalniškem ekranu opazil otroški pornografski material, bi lahko zasegli računalnik na podlagi *plain view* doktrine.[51] Medtem ko so ti primeri razmeroma podobni primerom *plain view* doktrine, kakršne smo navajeni v fizičnem svetu, pa je druga situacija precej kompleksnejša. Na podlagi *plain view* doktrine je mogoče zaseči tudi podatke (dokumente, fotografije ipd.), ki so shranjeni v računalniku. V tem primeru se dokaz torej ne pojavi na ekranu računalnika, ampak preiskovalec praviloma slučajno naleti nanj med preiskavo podatkov, shranjenih v računalniku ali drugi elektronski napravi, ki jo opravlja na podlagi naloga za preiskovanje nekega drugega kaznivega dejanja. Zanimivo je, da sta bili v letu 1999 pred ameriškimi sodišči sprejeti dve različni odločitvi na to temo.

V primeru *United States v. Carey*[52] je sodišče odločilo, da se lahko na podlagi *plain view* doktrine upravičeno zaseže le prva podoba otroške pornografije, ki jo ugleda preiskovalec, za zakonito pridobitev ostalega materiala pa je potreben ustrezen sodni nalog. Konkretneje je dejansko stanje primera Carey naslednje: ob aretaciji Careya je eden od policistov opazil, da so v hiši predmeti, ki kažejo na opravke z mamili. Policisti so vprašali za dovoljenje, ali lahko v stanovanju poiščejo morebitne dokaze v zvezi z mamili, na kar je osumljeni pristal. Na podlagi tega dovoljenja so policisti zasegli dva računalnika in pridobili sodni nalog za preiskavo trdih diskov. Nalog je zajemal iskanje

---

[48] Več o tem glej na primer Dressler, Michaels, s. 241–250.

[49] City of Akron v. Patrick, 1982 WL 5049 (1982).

[50] Oklahoma v. One Pioneer CD-ROM Changer, 891 P.2d 600 (1994).

[51] Moore, s. 64.

[52] United States v. Carey, 172 F.3d 1268, 1273-75 (10th Cir. 1999).

dokazov v obliki imen, telefonskih številk, računovodskih listin, naslovov ali drugih potencialnih dokazov, ki bi kazali na udeležbo pri trgovanju z mamili. Preiskovalec je pri preiskavi računalnika iskal te dokaze, naletel pa je tudi na datoteke, ki so mu bile neznane. Te datoteke je prekopiral na drug disk in jih pogledal na drugem računalniku ter ugotovil, da vsebujejo podobe otroške pornografije. Nato je prekopiral še okoli 200 datotek in pogledal njihovo vsebino v pričakovanju, da prav tako vsebujejo otroško pornografijo (in nekatere so jo), potem pa se je ponovno osredotočil na iskanje dokazov v zvezi s trgovino z mamili. Carey je na sojenju zahteval izločitev dokazov v zvezi z otroško pornografijo, češ da nalog ni zajemal dovoljenja za njihov zaseg. Sodišče je temu smiselno pritrdilo in odločilo, da je preiskovalec s tem, ko je odpiral slikovne datoteke, prekoračil pooblastilo iz naloga. Sodišče se je pri tem oprlo predvsem na pričanje preiskovalca, ki je povedal, da je pri odprtju prve slikovne datoteke pričakoval slike v zvezi z mamili. Sodišče je ocenilo, da je bilo odprtje te prve datoteke še upravičeno in skladno s *plain view* doktrino, medtem ko je v zvezi z nadaljnjimi datotekami preiskovalec po mnenju sodišča vedel, da išče otroško pornografsko gradivo in ne dokazov v zvezi s trgovino z mamili.

V drugem primeru, to je *United States v. Gray*,[53] pa je sodišče zavzelo stališče, da morajo preiskovalci pri pregledu računalnika skrbno pregledati vse potencialne vire dokazov. Ob upoštevanju dejstva, da je odprtje vsakega shranjenega dokumenta skladno z ustaljenimi postopki digitalne forenzične preiskave, je sodišče ocenilo, da preiskovalec vse do takrat, dokler izvaja oziroma ne opusti preiskave v smeri iskanja dokazov za kaznivo dejanje, zajeto z nalogom, ravna zakonito. Četudi pričakuje, da bo poleg tistih, ki jih išče, našel še druge dokaze, so slednji dopustni, saj jih pridobi skladno s *plain view* doktrino. V tem primeru je policija na podlagi naloga za iskanje dokazov za računalniške vdore zasegla štiri Grayeve računalnike. Vsebino trdih diskov so najprej kopirali na drug disk, nato pa jih je posebni agent CART FBI (*Federal Bureau of Investigation's Computer Analysis and Response Team*) pričel prenašati na zgoščenke zaradi možnosti tudi kasnejšega pregleda. Ker pa je bila nosilnost posamezne zgoščenke znatno manjša od kapacitete diskov, je agent pričel odpirati posamezne datoteke z namenom, da bi ugotovil, koliko datotek bo spravil na eno zgoščenko. Skladno s standardnim forenzičnim postopkom je pri tem pogledal tudi njihovo vsebino, pri čemer je odkril, da nekatere datoteke vsebujejo podobe z otroško pornografijo. Po nekaj takih datotekah je CART agent ustavil preiskavo in pridobil dodatni nalog za preiskavo podatkov na trdih diskih v smeri posedovanja otroškega pornografskega materiala. Gray je na sodišču trdil, da je bil prvotni dokaz v zvezi z otroško pornografijo pridobljen brez naloga in zato nezakonito, kasnejša izdaja naloga pa je bila po njegovem mnenju nepravilna. Sodišče je ocenilo, da so tudi prvi dokazi v zvezi z otroško pornografijo v tem primeru dovoljeni dokazi skladno s *plain view* doktrino. Gray se je sklicevал tudi na pravilo v primeru Carey, da je dovoljen dokaz le prvi dokument z otroško pornografijo, a je sodišče to ovrglo in sprejelo pričanje agenta CART o tem, da odpiranje vseh shranjenih dokumentov terjajo ustaljeni postopki digitalne forenzične preiskave. Kot odločilno je sodišče upoštevalo tudi dejstvo, da je agent CART vseskozi hkrati iskal tudi dokaze, ki bi kazali na računalniški vdor, za kar je imel veljaven sodni nalog.

[53] United States v. Gray, 78 F. Supp 2d 524 (E.D.VA 1999).

Moore z analizo obeh primerov ugotavlja, da je bila odločitev sodišča v konkretnem primeru odvisna od usposobljenosti preiskovalca. Če bi bil agent, ki je izvajal digitalno forenzično preiskavo v primeru Carey bolje usposobljen na področju računalniške forenzike in bi sodišču znal predstaviti temeljna pravila, po katerih poteka taka preiskava (kar je napravil CART agent v primeru Gray), bi bila lahko odločitev sodišča v primeru Carey tudi drugačna.[54] Kasnejši primeri večinoma potrjujejo stališče, ki ga je sodišče zavzelo v primeru Gray.[55]

Ob tem se na ravni teorije postavlja vprašanje, ali je v zvezi z digitalnimi dokazi sploh mogoče govoriti o *plain view* doktrini, glede na to, da je posamezne datoteke treba odpreti, da bi se videla vsebina dokaza. Dejstvo je, da odprtja datoteke preiskovalec ne more utemeljevati oziroma utemeljiti na podlagi *plain view* doktrine, ampak vstop v datoteko v konkretnem primeru lahko temelji le na zakoniti podlagi za preiskavo (torej praviloma na odredbi oziroma nalogu). Ko je datoteka enkrat odprta na podlagi zakonitega temelja za preiskavo, pa se lahko zaseg posameznega dokaza opraviči tudi s *plain view* doktrino.[56]

Skladno z ameriško teorijo in sodno prakso torej *plain view* zaseg digitalnih dokazov zahteva troje:[57]

1) vstop v vir dokaza mora biti zakonit,
2) dokaz mora na prvi pogled kazati na nelegalno dejavnost,
3) preiskovalec ne sme opustiti prvotne oziroma temeljne preiskave.

V domačem pravu je situacija v bistvu manj kompliciranа, saj vprašanje slučajne najdbe elektronskih dokazov ureja deveti odstavek 219.a. člena ZKP. Če se pri preiskavi elektronske naprave najdejo podatki, ki niso v zvezi s kaznivim dejanjem, zaradi katerega je bila preiskava odrejena, temveč kažejo na drugo kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti, se zasežejo tudi ti. To se navede v zapisnik in takoj sporoči državnemu tožilcu, da začne kazenski pregon. Če državni tožilec oceni, da ni razloga za kazenski pregon in tudi ne kakšnega drugega zakonskega razloga, da bi se morali podatki vzeti, je treba zasežene podatke takoj uničiti in o tem sestaviti zapisnik.

---

[54] Eden od sodnikov je v ločenem mnenju zapisal, da bi bili vsi dokazi v zvezi z otroško pornografijo v primeru Carey dopustni na sodišču, če bi preiskovalec enostavno nadaljeval z iskanjem dokazov v zvezi s trgovino z mamili. Ob tem najdeni dokazi so upravičljivi na podlagi *plain view* doktrine. Težava v primeru Carey je bila torej ta, da je policist za določen čas svojo digitalno forenzično preiskavo usmeril izključno na iskanje otroškega pornografskega gradiva.

[55] Glej na primer primere State v. Schroeder (613 N.W.2d 911, 2000), Commonwealth v. Hinds (768 N.E.2d 1067, 2002) in United States v. Slanina (286 F.3d 670, 2002). Več o tem tudi Moore, s. 68–69 in Schwerha, s. 137–138.

[56] Tako Moore, s. 70.

[57] *Ibidem*, s. 71

### Upravičeno pričakovanje zasebnosti na izbrisanih podatkih

Zanimivo pravno vprašanje je tudi, ali obnovitev izbrisanih podatkov s postopki digitalne forenzike posega v posameznikovo upravičeno pričakovanje zasebnosti (*reasonable expectation of privacy*) na teh podatkih. Na to temo ni obsežnejše sodne prakse niti v ZDA, eden bolj reprezentativnih primerov pa je *United States v. Angevine*.[58] E.N. Angevine je bil profesor arhitekture na Oklahoma State University. Kot vsi ostali učitelji je imel tudi on službeni računalnik, ki je bil povezan z drugimi univerzitetnimi računalniki in internetom. Angevine je s tem računalnikom iz svetovnega spleta snel več kot 3000 pornografskih podob mlajših fantov. Potem ko si je podobe ogledal in nekatere natisnil, jih je izbrisal. Policija je na podlagi naloga zasegla njegov službeni računalnik in ga predala policijskemu strokovnjaku za računalniško forenziko, ki je s posebnim forenzičnim orodjem obnovil izbrisane podatke, ki so še bili v računalniškem spominu, vključno z otroškim pornografskim materialom. Angevine je na sojenju zatrjeval, da je na izbrisanih podatkih upravičeno pričakoval zasebnost, zato so pridobljeni dokazi nezakoniti. Sodišče pa je zavzelo stališče, da izbris določenega dokumenta ni dovolj za to, da bi se vzpostavilo razumno pričakovanje zasebnosti, sploh ker so se dokumenti v konkretnem primeru prenašali preko nadzorovanega univerzitetnega omrežja. Nekaj pa je tudi primerov, v katerih so sodišča ocenila, da izdan nalog, ki pooblašča preiskovalca za iskanje in zaseg dokazov (na primer za posest otroške pornografije) dovoljuje preiskovalcem, da iščejo dokaze povsod, kjer bi se utegnili nahajati, se pravi tudi med izbrisanimi datotekami oziroma podatki (takšno stališče je bilo zavzeto na primer v primerih *United States v. Upham* in *Commonwealth v. Coperhafer*).[59]

Koncept razumnega pričakovanja zasebnosti poznamo tudi v domačem ustavnem (in) kazenskem procesnem pravu,[60] vendar se zaenkrat še ni pokazal kot aktualen v zvezi z digitalnimi dokazi.

### Digitalni dokazi, najdeni s strani zasebnih subjektov

Ker so metode digitalne forenzike uporabne tudi v zasebnem sektorju, se lahko razmeroma pogosto zgodi, da se v kazenskem postopku znajde digitalni dokaz, ki ni bil pridobljen, zavarovan, shranjen in analiziran s strani policije oziroma organov pregona in skladno z ZKP, ampak s strani posameznika ali zasebne forenzične institucije, in sicer na podlagi civilnopravnega razmerja. Primer: podjetje A najame forenzično podjetje B, da bi pregledalo aktivnosti na računalniku določenega zaposlenega, za katerega obstaja sum, da dela v škodo delodajalca. Če se pri taki preiskavi zasebnega značaja najdejo obremenilni digitalni dokazi, ki kažejo na kaznivo dejanje, je seveda vprašanje, ali jih je mogoče uporabiti kot dopustno dokazno sredstvo v kazenskem postopku zoper storilca. ZKP o tem nima določb, vendar je mogoče reči, da ta zakon v splošnem ne prepoveduje posameznikom zbiranja informacij, ki imajo dokazno

[58] United States v. Angevine, 10CIR 225 28 F.3d 1130, 2002.

[59] Podrobneje o tem Schwerha, s. 135–136.

[60] Gl. komentar 36. in 37. člena Ustave RS, Šturm in drugi, s. 386–408.

vrednost v kazenskem postopku,[61] dokler je to zbiranje skladno s pravnim redom kot celoto. V nobenem primeru se v dokazne namene ne morejo uporabiti digitalni dokazi, ki so bili pridobljeni s kaznivim dejanjem (na primer z napadom na informacijski sistem ali s katerim izmed kaznivih dejanj, ki pomenijo kršitev zasebnosti) ali so bili pridobljeni na podlagi takšnega nedovoljenega dokaza. Taki dokazi so skladno z ureditvijo v ZKP predmet izločitve (ekskluzije). Ostale, na zakonit način zasebno pridobljene digitalne dokaze oziroma informacije pa mora sodišče presojati skladno z načelom proste presoje dokazov ter pri tem upoštevati enake okoliščine kot pri ocenjevanju spoznavne vrednosti dokazov, pridobljenih shranjenih, zavarovanih in analiziranih s strani policije.

V ZDA pa so se sodišča v več primerih srečala, na primer z vprašanjem, ali se lahko zoper lastnika računalnika uporabi dokaz, ki ga je našel subjekt zasebnega prava med izvajanjem aktivnosti, za katere ga je pooblastil lastnik računalnika. Večinoma je šlo za primere, ko je lastnik prinesel računalnik na servis zaradi popravila ali v trgovino zaradi nadgradnje programske opreme, izvajalci pa so pri izvajanju teh nalog na računalniku našli otroško pornografijo in o tem obvestili pristojne organe. Sodišča so v takih primerih odločila, da ustava ZDA ne zagotavlja varstva pred dejanji zasebnih subjektov, zato dokazi, ki jih pridobijo taki subjekti niso pridobljeni protiustavno. Da bi dosegel izločitev takega dokaza, bi moral lastnik računalnika dokazati, da je serviser oziroma druga oseba v konkretnem primeru ob odkritju dokaza delovala kot agent države[62] ali da je država naknadno izvedla neupravičeno preiskavo, ki je presegla aktivnosti, izvedene s strani serviserja, pri čemer so se odkrili dodatni dokazi (ta stališča izhajajo na primer iz primerov *United States v. Hall*,[63] *United States v. Kennedy*,[64] *United States v. Grimes*[65] in *Untied States v. Barth*[66]).

[61] Zadeva je pravzaprav zelo podobna vprašanju pravne uporabnosti tehničnih posnetkov, narejenih zunaj kazenskega postopka – več o tem gl. Dežman, Erbežnik (2003), strani 602–604.

[62] To se presoja na podlagi dvodelnega testa: 1) ali je država vedela ali privolila v intruzivno dejanje in 2) ali je zasebni subjekt nameraval pomagati organom odkrivanja. Če posameznik zgolj opravlja delo, za katerega je dobil naročilo, država pa nima nič skupnega s tem delom, tak posameznik torej ni vladni agent in dokazi, ki jih odkrije, ne kršijo ustavnih pravic lastnika računalnika. To velja kljub temu, da posameznik po odkritju dokazov pokaže interes za sodelovanje z državo s tem, ko o najdenih dokazih obvesti policijo. Prim. Schwerha, s. 136.

[63] United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998).

[64] United States v. Kennedy, 81 F. Supp.2d 1103, 1112 (D. Kan. 2000).

[65] United States v. Grimes, 244 F.3d 375 (5th Cir. 2001).

[66] United States v. Barth, 26 F. Supp. 2d 929, 932 (W.D. Tex. 1998).

### Zaseg elektronske naprave in zavarovanje podatkov s strani drugih državnih organov in organizacij z javnimi pooblastili

V sorodnem, a ne povsem enakem kontekstu kot v primeru najdbe digitalnih dokazov s strani zasebnih subjektov se pojavljajo vprašanja, povezana z morebitnim zasegom elektronske naprave in/ali zavarovanjem podatkov s strani državnih organov, ki ne delujejo po ZKP (na primer carinska uprava, informacijski pooblaščenec, davčna uprava in večina drugih prekrškovnih organov). Analiza pristojnosti, nalog in pooblastil teh organov presega namen tega prispevka, dejstvo pa je, da ti organi pri svojem delu pogosto naletijo tudi na nepravilnosti, ki imajo znake kaznivih dejanj.

145. člen ZKP nalaga vsem državnim organom in organizacijam z javnimi pooblastili dolžnost naznaniti kazniva dejanja, za katera se storilec preganja po uradni dolžnosti, če so o njih obveščeni ali če kako drugače izvedo zanje. Obenem z ovadbo morajo ti organi in organizacije navesti dokaze, za katere vedo, in poskrbeti, da se ohranijo sledovi kaznivega dejanja in predmeti, na katerih ali s katerimi je bilo kaznivo dejanje storjeno, ter druga dokazila. ZKP torej ne le pooblašča, ampak državnim organom nalaga dolžnost, da med drugim poskrbijo, da se ohranijo sledovi kaznivega dejanja, na katere naletijo, kar lahko pomeni tudi začasen zaseg elektronske naprave in pod določenimi pogoji zavarovanje podatkov v njej.

To določbo ZKP je treba ustrezno povezati tudi z novima 219.a in 223.a členom ZKP. Tema členoma predvsem ne bi smeli pripisovati širšega dometa, kot ga dejansko imata. Kot je večkrat smiselno poudarilo Vrhovno sodišče,[67] so določbe ZKP sprejete zaradi posebnega položaja in pooblastil policije pri odkrivanju kaznivih dejanj in storilcev, zbiranju dokazov in izvrševanju prisilnih ukrepov zoper osumljence in druge osebe v predkazenskem postopku.[68] Kadar torej na elektronsko napravo in podatke v njej pri svojem delu naleti policija, mora zaseg, zavarovanje podatkov in preiskavo opraviti na podlagi določb 219.a in 223.a člena ZKP, pri čemer lahko po potrebi za zavarovanje podatkov in preiskavo najame strokovno usposobljeno osebo izven policije.

Če pa na elektronsko napravo in podatke v njej naleti drug državni organ pri opravljanju svojega dela in pri tem ugotovi, da je (oziroma bo) nastopila njegova dolžnost vložiti uradno kazensko ovadbo, sme začasno zaseči elektronsko napravo in *če ima ustrezno strokovno usposobljene osebe* tudi zavarovati podatke v oziroma na njej.[69] Tudi če državni organ za začasen zaseg elektronske naprave in zavarovanje podatkov nima pooblastila v matičnih predpisih, na podlagi katerih opravlja svoje redno delo,

---

[67] Prim. sodbi I Ips 72/2004 z dne 21.4.2005 in I Ips 4/2008 z dne 5.6.2008.

[68] V konkretnem primeru je Vrhovno sodišče sicer odločalo o vprašanju dopustnosti davčnega inšpekcijskega zapisnika kot dokaza v kazenskem postopku in odločilo, da zapisnika ni treba izločiti iz kazenskega spisa.

[69] Pri tem je treba izrecno poudariti, da zavarovanje podatkov v elektronski obliki po ZKP ne zajema vpogleda v vsebino podatkov, saj je temu namenjena faza preiskave elektronske naprave, za izvedbo katere morajo biti izpolnjeni drugačni standardi kot za zaseg naprave in zavarovanje podatkov v njej. Zavarovanje podatkov s hkratnim vpogledom v vsebino se lahko za potrebe kazenskega postopka izvede le na podlagi odredbe sodišča.

lahko to napravi na podlagi drugega odstavka 145. člena ZKP.[70] Niti za začasni[71] zaseg, niti za zavarovanje podatkov ZKP namreč ne zahteva privolitve oziroma sodne odredbe,[72] zato ni nevarnosti, da bi morala biti zasežena elektronska naprava oziroma zavarovani podatki izločeni kot vir digitalnih dokazov v kasnejšem kazenskem postopku. Ne sme pa drug državni organ samostojno in primarno za potrebe kazenskega postopka opraviti preiskave zasežene elektronske naprave oziroma pogledati vsebine zavarovanih podatkov, saj je to dovoljeno le pod pogoji iz ZKP. Če ima drug državni organ za preiskavo elektronskih naprav pravno podlago v matičnih predpisih in digitalne dokaze razkrije v prvi vrsti za potrebe svojega rednega dela (in pri tem ugotovi, da je naletel na znake kaznivega dejanja), pa je pravno dopustnost takih dokazov v kazenskih postopkih treba presojati po pravilih oziroma načelih, ki veljajo za dokaze, zbrane v nekazenskih postopkih.[73]

Prav tako je treba opozoriti na previdnost pri zavarovanju podatkov (na primer v obliki izdelave njihove kopije). Če državni organ nima ustrezno strokovno usposobljene osebe (lastne ali najete) za to opravilo, je bolje, da tega ne počne, ampak elektronsko napravo na primer zapečati in preda policiji. Sicer se bo v kasnejšem kazenskem postopku lahko izpostavilo vprašanje verodostojnosti dokazov zaradi spornega postopka njihovega zavarovanja, kar lahko ima znaten negativen vpliv na njihovo dokazno vrednost.

S strani drugega državnega organa zasežena elektronska naprava in, če je izpolnjen pogoj strokovnosti izvajalca, zavarovani elektronski podatki so pod zgoraj navedenimi pogoji torej pravno dopustna podlaga za izvedbo preiskave elektronske naprave po ZKP. Preiskava elektronske naprave, pri kateri se iščejo digitalni dokazi primarno za potrebe kazenskega postopka, pa mora obvezno temeljiti na privolitvi imetnika oziroma uporabnikov ali pa na odredbi sodišča, za kar lahko v kazenskem postopku pravnoveljavno poskrbita le policija oziroma državno tožilstvo.

Ob tem se lahko postavi vprašanje, ali je v primerih zasega elektronske naprave in zavarovanja podatkov v njej s strani drugih državnih organov treba upoštevati drugi odstavek 223.a člena ZKP. Kot pojasnjeno zgoraj, ta odstavek ureja primere zasega elektronske naprave in zavarovanja podatkov brez predhodne odredbe sodišča za preiskavo elektronske naprave in v zvezi s tem določa, da mora policija zapisniško trajno uničiti izdelano kopijo podatkov, če sodišče v dvanajstih urah ni izdalo odredbe za preiskavo oziroma imetnik ter uporabniki niso privolili v preiskavo (skladno s petim oziroma drugim odstavkom 219.a člena ZKP). Ta 12-urni rok v povezavi s petim

---

[70] Drugi odstavek 145. člena ZKP se glasi: »*Obenem z ovadbo morajo organi in organizacije iz prejšnjega odstavka navesti dokaze, za katere vedo, in poskrbeti, da se ohranijo sledovi kaznivega dejanja in predmeti, na katerih ali s katerimi je bilo kaznivo dejanje storjeno, ter druga dokazila*.« Organi »iz prejšnjega odstavka« so državni organi in organizacije z javnimi pooblastili.

[71] To je do predaje policiji oziroma državnemu tožilstvu skupaj z uradno kazensko ovadbo.

[72] Kot rečeno, ZKP zahteva odredbo sodišča (če ni privolitve imetnika ter uporabnikov) le za preiskavo elektronske naprave, ne pa tudi za zaseg in zavarovanje podatkov.

[73] Ta pravila pri nas na sistemski ravni zaenkrat niso dodelana, zato se v zvezi s tem v praksi utegnejo pojaviti težave. Več o tem gl. Selinšek, Pravna ..., s. 75–84.

odstavkom 219.a člena ZKP teče od izdaje ustne odredbe preiskovalnega sodnika za preiskavo elektronske naprave v nujnih primerih, ko obstaja neposredna in resna nevarnost za varnost ljudi ali premoženja. To pomeni, da je drugi odstavek 223.a člena ZKP dodatna varovalka, ki preprečuje zlorabe t. i. nujnih primerov,[74] zato tudi pride v poštev le v zvezi s takšnimi primeri, v katere se mora po naravi stvari takoj vključiti policija (delovanje drugih državnih organov na svojo roko brez takojšnjega angažiranja policije bi bilo v primeru, ko obstaja neposredna in resna nevarnost za varnost ljudi ali premoženja, najmanj neodgovorno).

Določba drugega odstavka 223.a člena ZKP torej v ničemer ne vpliva na predstavljeno stališče, da začasen zaseg elektronske naprave in pod določenimi pogoji (to je ustrezno strokovno usposobljen (so)delavec) tudi zavarovanje podatkov v njej lahko za potrebe (pred)kazenskega postopka poleg policije izvedejo tudi drugi državni organi, in sicer v zvezi z njihovo obveznostjo iz 145. člena ZKP.

## Sklep

Digitalni dokazi so v sodobni tehnološki družbi prisotni praktično povsod. Vendar gre za pojave, ki so drugačni od vsega tistega, kar je predstavljalo dokaze v dolgi in zanimivi zgodovini kazenskega pravosodja. Kot taki morajo biti pravosodju izziv! Digitalnim dokazom je vsekakor treba priznati mesto med pravno relevantnimi dokazi, saj bi odlašanje ali celo ignoriranje teh dokazov pomenilo znaten bonus za storilce kaznivih dejanj. Kaznivih dejanj namreč ne izvršujejo elektronske naprave, ampak ljudje (ob hitrem napredku tehnologije je upati, da bo tako tudi ostalo …). Standardi pravičnega sojenja zahtevajo, da se digitalni dokazi za potrebe kazenskega postopka pridobijo na pravno dopusten način, nato pa pravilno ovrednoti njihova dokazna vrednost.

Slovenija je oktobra 2009 dobila posebno zakonsko ureditev za zaseg in preiskavo elektronskih naprav ter zavarovanje podatkov v njih. Dva (obsežna) člena v ZKP pomenita skok na stopnico višje. S tem, ko smo se povzpeli na njo, pa se je odprl nov razgled – na cel gozd hipotetičnih, teoretičnih, pa tudi čisto praktičnih vprašanj, ki jih bo tako ali drugače treba obdelati in razrešiti na poti do končnega cilja. Ta bo dosežen, ko se o digitalnih dokazih ne bo govorilo kot o posebnem, eksotičnem in zapletenem sredstvu dokazovanja, ampak bodo v zavesti policistov in kriminalistov, predvsem pa državnih tožilcev in sodnikov te metode in dokazi nekaj čisto običajnega, pač z določenimi svojimi značilnostmi, ki bodo vsem vpletenim znane in obvladljive na podlagi jasno določenih pravil.

[74] Tako tudi Kovačič, s. 7.

## Literatura


1. Bernard, J.; Selinšek, L.; Lesjak, B.; Šavnik, J. (2008). **Digitalna forenzika v kazenskih postopkih**. Ljubljana: GV založba.
2. Bianchi, R.P.; Pollitt, M. (2005). Digital Evidence V: A. Mozayani, C. Nozigila [ed], **The Forensic Laboratory Handbook**, Totowa: Humana Press Inc., s. 80–90.
3. Casey, E. (2004). **Digital Evidence and Computer Crime**. London: Elsevier Academic Press.
4. Chaikin, D. (2006). Network investigations of cyber attacks: the limits of digital evidence. **Crime, Law and Social Change**, št. 46, s. 239–256.
5. Dressler, J.; Michaels, A. S. (2006). **Understanding criminal procedure**, Volume 1, Investigation, Lexis Nexis.
6. Dežman, Z.; Erbežnik, A. (2003). **Kazensko procesno pravo Republike Slovenije**. Ljubljana: GV založba.
7. Giordano, S.M. (2004). Electronic Evidence and the Law. **Information Systems Frontiers**, let. 6, št. 2, s. 161–174.
8. Kovačič, M. (2009). **Komentar določb novele Zakona o kazenskem postopku (ZKP-J), ki opredeljujejo nekatere posege v komunikacijsko zasebnost**. Po URL: http://hr-cjpc.si/pravokator/index.php/2009/10/21/novela-zakona-o-kazenskem-postopku-posegi-v-komunikacijsko-zasebnost/, dostop 12.12.2009.
9. Lang, A. (2009). Preiskovanje komunikacijske in elektronske zasebnosti po ZKP-J. V: **Zbornik 2009, konferenca kazenskega prava in kriminologije**, Ljubljana: GV založba, s. 175–183.
10. Mason, S. [ed.] (2008). **International Electronic Evidence**. London: British Institute of International and Comparative Law.
11. McKemmish, R. (2008). When is Digital Evidence forensically sound? V: R. Indrajit, S. Shenoi [ed], **IFIP Advances in Information and Communication Technology, Vol. 285**, **Advances in Digital Forensics IV**, Boston: Sprigner, s. 3–15.
12. Moore, R. (2004). To view or not to view: Examining the Plain View Doctrine and Digital Evidence. **American Journal of Criminal Justice**, let. 29, št. 1, s. 57–73.
13. Rogers, M.; Scarborough, K.; Frakes, K.; San Martin, C. (2007). Survey of Law Enforcement Perceptions regarding Digital Evidence. V: P. Craiger, S. Shenoi, [ed], **IFIP Advances in Information and Communication Technology, Vol. 242**, **Advances in Digital Forensics III**, Boston: Springer, s. 41–52.
14. Scheetz, M. (2007). **Computer Forensics. An Essential Guide for Accountants, Lawyers, and Managers**. New Jersey: John Wiley & Sons.
15. Selinšek, L.; Malovrh, M. (2008). Digitalni dokaz – med pravom in tehniko. V: A. Dvoršek, L. Selinšek (ur.), **Nekateri praktični problemi dokazovanja v kazenskih postopkih**, Maribor: Pravna fakulteta in Fakulteta za varnostne vede UM.

16. Selinšek, L. (2009). Privilegij zoper samoobtožbo v informacijski dobi. **Pravna praksa**, let. 28, št. 2, s. 11–13.
17. Selinšek, L. (2009). Pravna dopustnost dokazov, zbranih v nekazenskih postopkih. V: **Zbornik / 2. konferenca kazenskega prava in kriminologije**. Ljubljana: GV založba, s. 75–84.
18. Schwerha, J.J. (2004). Cybercrime: Legal Standards Governing the Collection of Digital Evidence. **Information Systems Frontiers**, let. 6, št. 2, s. 133–151.
19. Šturm, L. in drugi (2002). **Komentar Ustave Republike Slovenije**. Ljubljana: Fakultete za podiplomske državne in evropske študije.
20. Walden, I. (2007). **Computer Crimes and Digital Evidences**. New York: Oxford University Press.

# 6 Forenzika mobilnih telefonov in vloga sodnega izvedenca za računalniško forenziko v kazenskih postopkih

**Janko Šavnik**

## Opredelitev računalniške forenzike

Računalniška forenzika je odgovor na zahteve varnostnih organov po podpori (Morgan, 2002: 1). Izraz računalniška forenzika različnim ljudem pomeni različno stvar. Že v osnovi je izraz računalniška forenzika nekoliko neroden, saj dobesedno pomeni izvajanje forenzike s pomočjo računalnika. Za bolj pravilno pojmovanje bi morali biti besedi obrnjeni – forenzika računalnikov. Tako formuliran izraz pomeni pravilno uporabo pridevnika in samostalnika, vendar tudi ta izraz ni najboljši, saj se preveč ozko omeji samo na računalnike in pozablja na ostale naprave, kjer se nahajajo podatki v digitalni obliki, kot so GSM telefoni, spominske kartice in podobno. Dosti bolj primerna bi bila izraza forenzika elektronskih (digitalnih) naprav ali forenzika elektronskih (digitalnih) podatkov. Izraza sta pravilno formulirana in hkrati obsegata forenziko vsega, kar je v digitalni obliki, od običajnih računalnikov, prenosnikov, vseh nosilcev podatkov, komunikacij in podobno. Pomembno je tudi ločevanje med pojmoma pregled in preiskava, saj je slednji bistveno bolj podroben in ob upoštevanju zakonskih določil dejansko pomeni forenziko.

Pogovorno se uporablja različno izrazoslovje, kot na primer iskanje elektronskih dokazov, digitalna preiskava, pregled podatkov, analiza računalnikov, preiskava računalnikov in podobno. Nekateri izrazi so bolj pravilni, drugi spet manj, vendar niti eden izmed njih ne ustreza povsem dejanskemu pomenu besedne zveze računalniška forenzika. Verjetno je še najboljše alternativno poimenovanje za računalniško forenziko forenzika digitalnih podatkov. Logično je namreč, da se računalniška forenzika nanaša na preiskovanje digitalnih podatkov za potrebe sodnih in tudi drugih postopkov in v tem je tudi njeno bistvo: iskanje dokazov med podatki v elektronski obliki, ki so zanesljivi in so uporabni na sodišču.

Ne glede na opisano se bo še naprej uporabljal izraz računalniška forenzika, saj se je med ljudmi že zelo prijel.

Kaj sploh je računalniška forenzika? Definicij je mnogo, med najboljšimi pa je zagotovo: »*Računalniška forenzika je proces identificiranja, zavarovanja, analiziranja in predstavljanja dokazov v elektronski obliki na način, ki je zakonsko sprejemljiv.*« (McKemmish, 1999: 1; Rathmell in Valeri, 2003: 33). Navedena definicija je najboljša iz več razlogov, saj v grobem vsebuje pomembnejše korake v postopku izvajanja forenzike (»proces identificiranja, zavarovanja…«), kot tudi zahtevo, da je postopek izveden na »zakonsko sprejemljiv način«. Prav slednje je tisto, kar loči forenziko digitalnih dokazov od pregleda digitalnih dokazov, saj je njen smisel in cilj zagotavljanje sodišču sprejemljivih dokazov v elektronski obliki.

Zavarovani dokazi v elektronski obliki so cilj vsakega preiskovalca spornega dogodka. Z njimi namreč potrdi svoje trditve in na ta način dejanje tudi dokaže. Pri preiskovanju klasičnih dogodkov v tako imenovanem materialnem svetu so dokazi materialni. Drugače je pri informacijski tehnologiji, kjer so vsi podatki shranjeni v

digitalni oziroma elektronski obliki in kot rečeno, se te dokaze pridobiva s pomočjo računalniške forenzike. Dokazi v elektronski obliki so torej vsaka predstavitev teksta, zvoka, slik, multimedije ali programov in ostalih možnih podatkov, ki na sodišču ali drugje služijo kot dokaz.

Da bi se sodišča in ostali dejansko lahko oprli na dokaze v elektronski obliki je nujno, da to obliko dokazov priznava tudi zakonodaja. V Republiki Sloveniji je to urejeno z Zakonom o elektronskem poslovanju in elektronskem podpisu, ki v 4. členu pravi: »*Podatkom v elektronski obliki se ne sme odreči veljavnosti ali dokazne vrednosti samo zato, ker so v elektronski obliki.*« V istem zakonu je v 1. točki I. odstavka 2. člena tudi opredeljena elektronska oblika podatkov, in sicer: »*Podatki v elektronski obliki so podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način.*«

## Načela računalniške forenzike

Računalniška forenzika se je v zadnjih letih razvijala vedno hitreje in odkrivala vedno nove podrobnosti o delovanju informacijskih sistemov, na podlagi katerih se nato dopolnjujejo in izdelujejo programska in strojna forenzična orodja. Poznavanje vseh forenzičnih skrivnosti in programskih ter strojnih orodij, s pomočjo katerih je mogoče izvajanje računalniške forenzike, pa žal ni dovolj, da bi bil postopek sam po sebi forenzično pravilen in dokazi sprejemljivi v katerem koli postopku. Tega se zavedajo mnogi guruji računalniške forenzike, ki so v ta namen zapisali načela računalniške forenzike. Načela dajo izvajalcem okvir za delo, ki se ga preprosto morajo držati in ne smejo delati drugače kot zapovedujejo načela, sicer so digitalni dokazi lahko celo neuporabni.

Načel digitalne forenzike bi lahko našteli cel kup, vendar je bolj smiselno našteti najpomembnejša:

1. *Revizijska sled*: vse aktivnosti v zvezi s forenzičnimi postopki glede digitalnih dokazov morajo biti natančno dokumentirane, hranjene in dostopne za pregled tako, da jih lahko ponovi tretja neodvisna stranka in doseže enak rezultat.
2. *Integriteta*: noben postopek ne sme spremeniti originalnega izvoda podatkov. Če namerava preiskovalec izvajati forenzično preiskavo podatkov, mora narediti delovno kopijo originala.
3. *Znanje preiskovalca*: preiskovalec ne sme preseči ravni svojega znanja, saj lahko pride do napačnih ugotovitev ali celo spremeni, poškoduje oziroma delno ali v celoti uniči digitalne dokaze.
4. *Skrbniška veriga*: digitalni dokazi morajo biti ustrezno varovani, zato je posameznik v času, ko jih ima pri sebi, odgovoren za vse aktivnosti v zvezi z njimi.
5. *Zakonodaja*: pri delu z digitalnimi dokazi je treba upoštevati splošna forenzična pravila in zakonske določbe za zavarovanje dokazov.

# Forenzika mobilnih telefonov

Časi, ko so bile digitalne naprave zgolj stacionarne, nameščene na pisalnih mizah pisarn in dnevnih sob so že davno mimo. Po zaslugi vedno zmogljivejših pomnilnikov in baterij ter energijsko vedno manj potratnih procesorjev, ki pa so hkrati postajali vedno bolj zmogljivi, ter brezžične komunikacije, ki se je razvijala skupaj z njimi, smo prišli v obdobje, ko so mobilne digitalne naprave preplavile svet.

Danes ima v razvitem svetu skorajda vsakdo svoj mobilni telefon, vsaka družina ima vsaj en digitalni fotoaparat ali videokamero, podobno pa je tudi z napravami GPS. Vse naštete naprave, pa tudi nekateri dlančniki – osebni organizatorji (angl. *PDA – Portable Digital/Data Assistant*), tiskalniki, telefaksi, optični čitalci oziroma kombinirane naprave, imajo vgrajene pomnilne enote v obliki trdih diskov ali bliskovnih pomnilnikov, na katerih se shranjujejo podatki. Seveda se ne sme pozabiti niti na tako imenovane pametne telefone (angl. *smartphone*), ki so kombinacija mobilnih telefonov in dlančnikov. Meja med običajnimi in pametnimi telefoni je večinoma že tako zabrisana, da jih uporabniki niti ne ločijo oziroma te razlike ne poudarjajo.

Mobilni telefoni, ki jih uporabljamo v Sloveniji, za vzpostavitev povezave z omrežjem potrebujejo kartico SIM, na kateri se prav tako shranjujejo podatki. Poleg tega lahko uporabniki podatke shranjujejo tudi na spominskih karticah, če to naprava omogoča. Kot je splošno znano, pa lahko danes na spominske kartice shranimo že izredno veliko količino digitalnih podatkov.

## Forenzika kartic SIM

Kartica SIM je udomačeno ime za pametno čipno kartico, na kateri je več računalniških aplikacij med katerimi je tudi modul – aplikacija SIM (angl. *Subscriber Identity Modul*), ki se uporablja za identificiranje uporabnika mobilnega telefona. Skladno s standardi je bila kartica na začetku enako velika kot plačilne kartice. Ker bi v današnje telefone tako veliko kartico težko vtaknili, so proizvajalci že pred leti omogočili, da se lahko čipni del pametne kartice odstrani in ločeno vstavi v mobilne telefone. Kartice SIM, če uporabljamo popularno poimenovanje, so lahko v uporabi v načinu »samo za branje« ali pa v načinu »za pisanje«. Prvi način je verjetno izjemno redek, a vendarle obstaja, saj uporabniku onemogoča zapisovanje kakršnega koli podatka na kartico (tudi na primer o zadnjih klicih), kar je nepraktično.

Na kartici SIM sta dva identifikacijska znaka, ki se uporabljata za identifikacijo uporabnika mobilnega telefona, hkrati pa sta tudi podlaga za obračunavanje uporabe mobilnega omrežja. Prvi znak je številka IMSI (angl. *International Mobile Subscriber Identity*), ki je običajno sestavljena iz 15 cifer, od katerih so prve tri cifre MCC (angl. *Mobile Country Code*) – šifra države, druge tri MNC (angl. *Mobile Network Code*) – šifra operaterja, preostale pa so MSIN (angl. *Mobile Station Identification Number*) – identifikacijska številka mobilnega telefona.[1] Navedena številka je edinstvena posamezni kartici SIM kjerkoli na svetu.

[1] Po Wikipedia URL: http://en.wikipedia.org/wiki/International_Mobile_Subscriber_Identity, dostop 2.6.2009.

Drugi identifikacijski znak pa je številka ICCID (angl. *Integrated Circuit Card Identity*), ki je dolga 19 ali 20 cifer in dejansko omogoča identificiranje pametne kartice. Številka je sestavljena iz oznake sistema (89 za GSM), MCC, MNC, MSIN in kontrolne številke, če ta obstaja. V primeru, ko kontrolna številka obstaja, je izračunana po Luhnovem algoritmu, podobno kot to velja pri številkah plačilnih kartic. Obe številki sta dodani na kartico SIM med personalizacijo in ju uporabnik kartice SIM kasneje ne more spremeniti.

Na kartici SIM je običajno natisnjena tudi številka SSN (angl. *SIM Serial Number*), ki predstavlja dejansko serijsko številko kartice.

Na kartici SIM je še mnogo drugih podatkov, od katerih so za potrebe računalniške forenzike najzanimivejši naslednji:

1. *International Mobile Subscriber Identity* (IMSI),
2. *Integrated Circuit Card Identifier* (ICCID),
3. *Mobile Subscriber International ISDN Number* (MSISDN) – telefonska številka, če je na kartici zapisana,
4. *Abbreviated Dialing Numbers* (ADN) – telefonski imenik v kartici SIM,
5. *Last Dialed Numbers* (LDN) – seznam nekaterih zadnjih odhodnih klicev,
6. *Short Message Service* (SMS) – seznam prejetih in poslanih kratkih sporočil SMS,
7. *Location Information* (LOCI) – podatki o zadnji bazni postaji, s katero je bila povezana kartica SIM,
8. *Service Provider Name* (SPN) – podatki o ponudniku oziroma izdajatelju kartice SIM,
9. nastavitve za posredovanje sporočil SMS in glasovno tajnico.

Pri tem je pomembno, da je s pomočjo forenzičnih orodij na SIM kartici možno identificirati in zavarovati tudi predhodno izbrisana kratka sporočila SMS, v kolikor še niso bila prepisana. S stališča preiskovalcev je lahko pomemben tudi podatek o zadnji bazni postaji, da na ta način poskušajo ugotoviti, če je bil telefon od takrat do najdbe morebiti premaknjen, kar je uporabno na primer pri preiskovanju umorov.

Kartice SIM imajo vgrajeno zaščito pred zlorabo z zahtevanim vnosom številke PIN, ki je na karticah privzeto praviloma vključena, vendar jo lahko uporabnik na lastno odgovornost izključi. Navedena zaščita je lahko s stališča forenzičnih preiskav vsebine kartic SIM zelo velika omejitev, saj mora biti za uspešno izvedbo številka PIN poznana. V primeru, da številka ni zaznana, se namreč kartica SIM po treh napačnih vnosih zaklene. Odklene se jo lahko z vnosom številke PUK (angl. *Pin Unlock Code*), ki jo uporabnik prejme hkrati s kartico SIM oziroma jo je možno pridobiti od operaterja mobilne telefonije. V kolikor tudi številka PUK ni znana, se kartica SIM po 10 neuspešnih poizkusih trajno zaklene.

Večina današnjih telefonov (razen pametnih) ne deluje brez kartice SIM oziroma brez kartice ni mogoč dostop do podatkov. To pomeni, da je potrebno pred vklopom v telefon vstaviti kartico SIM, saj sicer do podatkov ni možno dostopati. Glede na to, da je nekatere telefone možno nastaviti tako, da ne dovolijo vstavitve neke tretje kartice SIM, saj se v takem primeru podatki uničijo, je potrebno poskrbeti, da to tega ne pride. A to še ne pomeni, da se lahko telefon zažene z originalno kartico SIM, saj bi se lahko telefon povezal v mobilno omrežje in pričel s sinhroniziranjem podatkov in bi omogočal dohodne klice, kar bi posledično močno ogrozilo verodostojnost preiskave in integriteto

podatkov, saj bi lahko prišlo do sprememb nekaterih bistvenih podatkov (na primer neodgovorjeni klici). To je potrebno rešiti bodisi s Faradayevo kletko, vrečko ali pregrinjalom, ki ne prepuščajo signala mobilnega omrežja, ali pa z uporabo posebne forenzične kartice SIM, na katero se s pomočjo specializirane programske opreme vpiše IMSI in ICCID številki, na njej pa ni podatkov za povezavo v omrežje, zato do poškodovanja podatkov ne more priti.

### Forenzika mobilnih telefonov

Mobilni telefoni so poleg elektronske pošte in spleta gonilna sila novodobnih tehnologij, ki so neverjetno močno vplivali na naše življenje, saj smo postali dosegljivi skorajda povsod in v vsakem času. Pred pojavom mobilnih telefonov so bili dogovarjanje za sestanke ali zmenke, klici o zamudah, nujna sporočila in ostala komunikacija omejeni na trenutke, ko smo bili blizu svojega telefona. Danes je vse to popolnoma drugače, dosegljivost sogovornika pa je pogojena le s pokritostjo s signalom, polnostjo baterije in njegovo voljo za odziv na klice. Prednosti mobilne telefonije oziroma zmogljivosti naprav samih so se z leti neverjetno hitro povečale, vse do te mere, da je iz okornega (a še vedno enostavnega) telefonskega aparata za govorno in nato tudi SMS komunikacijo nastal pametni telefonski aparat, ki pozna koledar, alarme in budilko, ima vgrajen fotoaparat in videokamero, diktafon in radijski sprejemnik, omogoča delo z elektronsko pošto in pregledovanje spleta, igranje iger, delo z datotekami računalniških pisarniških paketov (na primer programov *Microsoft Word* in *Excel*) in še bi lahko naštevali.

Posledično je na telefonih shranjenih izredno veliko zasebnih in osebnih podatkov od uporabnikov, njihovih bližnjih in ostalih, s katerimi oseba komunicira. Pri tistih, ki uporabljajo telefone tudi v službene namene, pa so na njih tudi koledarji, opomniki, službena elektronska pošta s priponkami, službena kratka sporočila SMS in podobno. Hkrati s tem so na telefonih tudi uporabniška imena in pripadajoča gesla.

S stališča forenzike so med najzanimivejšimi naslednji podatki:

1. podatki o napravi (znamka, model, tip, številka IMEI, serijska številka, operacijski sistem, verzija, *firmware* in sistemska ura),
2. telefonski imenik/kontakti,
3. organizator (koledar, rojstni dnevi, opravila…),
4. telefonski klici (odhodni, prejeti, neodgovorjeni),
5. SMS/EMS/MMS (fotografije in video) in e-pošta,
6. dnevniki takojšnjega sporočanja (IM),
7. nastavitve za dostop do interneta, e-poštnih predalov,
8. WAP začasni pomnilnik/števec prenesenih podatkov GPRS,
9. zgodovina pregledovanja svetovnega spleta,
10. T9 slovarji,
11. galerija (fotografije, glasba, video, melodije za zvonjenje),
12. diktafonski posnetki,
13. varnostne kode, številke PIN, digitalni certifikati,
14. običajne datoteke poznane iz osebnih računalnikov,
15. aplikacije (na primer GPS, J2ME).

Vsi mobilni telefoni ne hranijo vseh naštetih vrst podatkov, temveč je to odvisno od vrste telefona (običajni/pametni) in seveda od znamke, tipa in programske opreme

telefona. Forenzika mobilnih telefonov je zaradi tega in pa iz razlogov opisanih v nadaljevanju bistveno bolj zahtevna, kot običajna računalniška forenzika trdih diskov in drugih nosilcev podatkov.

Med največjimi problemi forenzike mobilne telefonije je zagotavljanje integritete, ki je delno opisan pri forenziki kartice SIM. Poleg slednjega, je zagotavljanje integritete tudi sicer zelo velik problem, saj se takoj, ko forenzik zažene mobilni telefon, podatki na pomnilniku spreminjajo. Telefona namreč ni mogoče vklopiti in zagnati na forenzično ustrezen način. Edini način za zagotavljanje integritete podatkov na pomnilniku je razspajkanje pomnilniškega čipa in nato izdelava slike pomnilnika z ustreznimi napravami. To je postopek, ki lahko stane tudi 10.000 EUR in več, ki jih je za preiskavo enega pomnilnika resnično težko odobriti. Posledično mora mobilni telefon delovati in mora imeti polno baterijo oziroma potrebujemo napajalnik.

Na področju integritete je med najbolj spornimi postopki ta, ko je včasih potrebno narediti nekaj, kar si pri forenziki trdih diskov nikakor ne moremo predstavljati. V nasprotju z vsemi forenzičnimi načeli je potrebno na telefone včasih namestiti posebno aplikacijo, ki omogoča povezavo z napravo za prenos podatkov na nek zunanji pomnilnik, s tem pa se grobo krši forenzična načela, saj se spreminja integriteta podatkov na izvornem nosilcu, hkrati pa tudi prepisuje prazen prostor, kjer bi lahko bili pomembni podatki. Seveda to ni pravilno, a se v primeru, ko to preiskovalec argumentirano zapiše, tudi tolerira, saj drugače pač ne gre.

Naslednja težava je velika raznolikost naprav, saj na tržišču obstaja preko 2.000 različnih znamk in modelov mobilnih telefonov. Za forenzike to pomeni najmanj tri probleme:

- raznolikost napajalnikov,
- raznolikost načinov povezave (običajno vodnik, infrardeča povezava – *IrDA* in *Bluetooth*),
- raznolikost konektorjev za prenos podatkov iz telefona na forenzični nosilec podatkov v primeru uporabe vodnika.

Medtem ko je raznolikost napajalnikov dokaj enostavno rešljiva, pa je povsem drugače pri povezljivosti, saj mobilni telefoni v osnovi niso bili izdelani tako, da bi se povezovali na osebne računalnike ali druge naprave. Zato je predvsem pri starejših telefonih povezovanje s forenzičnimi napravami še toliko bolj zahtevno, v primeru uspešne povezave pa se s telefona praviloma ne prenesejo vsi živi (neizbrisani) podatki, temveč zgolj nekateri (na primer telefonski imenik). Ostale podatke je možno zavarovati forenzično ustrezno edino z uporabo specializiranih orodij za forenzično fotografiranje ekranov mobilnih telefonov.

Naslednji problem predstavlja dejstvo, da je na zgoraj opisane načine možen dostop le do tako imenovanih živih podatkov oziroma tistih, ki niso izbrisani. Forenzikom znano dejstvo je, da podatki po uporabnikovem izbrisu na telefonu še vedno obstajajo do prepisa, zato bi jih bilo s stališča kvalitetnega in objektivnega preiskovanja smiselno pregledati. Žal je dostop do teh podatkov zopet mogoč le s posebnimi forenzičnimi napravami (eno takih ima tudi Inštitut za forenziko informacijskih tehnologij iz Ljubljane) ali pa napol domačimi, v garažah izdelanimi napravami imenovanimi *flasher*-ji, s pomočjo katerih je možno prekopirati celotni bliskovni pomnilnik. Medtem ko v prvem primeru naprava oziroma pripadajoča programska oprema omogočata priklic in rekonstrukcijo izbrisanih podatkov, pa je to v primeru izdelave kopije s *flasher*-ji

težje. Vzrok za to so različni datotečni sistemi, ki jih uporabljajo izdelovalci mobilnih telefonov, katerih podrobnosti niso pripravljeni javno ali brezplačno razkriti. Zato je forenzična obdelava takih podatkov praviloma izredno zahtevna in pogosto nemogoča. Najpogosteje se začne z običajnimi forenzičnimi aplikacijami in iskanjem datotek glede na njihovo šestnajstiško vrednost zaglavja, nadaljuje pa se z ostalimi bistveno zahtevnejšimi pristopi.

Ne glede na to, pa je razveseljiv podatek, da je razvoj naprav za forenziko mobilnih telefonov zelo napredoval do te mere, da je zaseg celotnih pomnilnikov s specialnimi orodji dokaj enostavno možen za več kot 100 različnih mobilnih telefonov, na seznamu pa jih je iz dneva v dan več.

### Forenzika spominskih kartic

Spominske kartice so v mobilnih telefonih tretji potencialni vir digitalnih dokazov, ki pa s stališča zahtevnosti forenzičnega postopka na srečo niso nič posebnega. S pomočjo ustreznega (forenzičnega) bralnika in primerne programske opreme se namreč najprej izdela sliko celotnega nosilca, tudi izbrisanega. Nato se s pomočjo klasičnih forenzičnih aplikacij pregleda celotna vsebina in poskuša izločiti iskane digitalne dokaze. Postopek je torej povsem enak kot pri trdih diskih ali drugih vsakdanjih nosilcih podatkov.

# Vloga sodnega izvedenca za računalniško forenziko v kazenskih postopkih

Vsi postopki digitalne forenzike in drugi z njimi povezani postopki na splošno, ne samo za forenziko mobilnih telefonov, so za nestrokovnjake za področje informacijskih tehnologij večinoma zelo zahtevni in težje razumljivi. Gre namreč za področje, kjer so potrebna visoka tehnična znanja in izkušnje, prav tako pa tudi osnovno poznavanje prava, da bi tako zagotovili izvedbo forenzičnih postopkov skladno z načeli računalniške forenzike, zakonodajo in tehničnimi zahtevami ter omejitvami.

Šolski sistem v Sloveniji je že vrsto let tak, da študentje prava, ki so večinoma ciljna publika za izsledke postopkov računalniške forenzike, skozi šolanje ne pridobijo dovolj drugih znanj, razen pravnih. To velja tako za informatiko in računalništvo, kot tudi druga znanstvena področja. Dodatna znanja bi namreč pravnikom omogočala lažje razumevanje in odločanje v postopkih, ki sicer niso tipično pravni. Eden takih je seveda razumevanje in uporaba računalniške forenzike v civilnih in kazenskih postopkih, kjer imajo lahko nepoučeni pravniki precejšnje težave že pri osnovnih pojmih, kaj šele, ko primer zabrede globoko v tehnične področnosti.

Dokler se sistem ne bo spremenil, kar zagotovo ne bo prav kmalu, bodo pravniki v kazenskih postopkih prisiljeni za pomoč uporabiti sodnega izvedenca za računalniško forenziko. Seveda bi si lahko pomagali tudi z izvedencem za računalništvo ali informatiko, vendar ti običajno nimajo forenzičnih in pravnih znanj, da bi lahko suvereno trdili, da je bil nek forenzičen postopek izveden skladno z načeli računalniške forenzike, ki so omenjeni na začetku prispevka. Pri tem je mišljeno predvsem vprašanje ustreznosti zagotavljanja integritete podatkov, ustreznosti beleženja revizijske sledi in skrbniške verige, včasih pa tudi skladnosti postopkov z zakonodajo.

Pravnikom, torej sodnikom, tožilcem in odvetnikom, lahko edino sodni izvedenec za računalniško forenziko pomaga pri:

- razumevanju tehnične in forenzične terminologije, ko je potrebno razumeti določene termine, ki se uporabljajo v računalniški forenziki,
- razumevanju opravljenih forenzičnih in drugih postopkov v zvezi z digitalnimi podatki, ko pomaga razložiti, kaj se pri takih postopkih dogaja,
- razumevanju primera glede ustrezne klasifikacije kaznivega dejanja, ko pomaga razložiti načine uporabe informacijskih sredstev s stališča namena in naklepa ter zavestne, naključne ali posredne uporabe informacijskih sredstev, kakor tudi malomarne uporabe istih sredstev, če je to potrebno in smiselno,
- razumevanju pisne dokumentacije, ki se nanaša na forenzične postopke in je bila pridobljena v predkazenskem postopku (na primer zapisniki in uradni zaznamki policije), ko je potrebna razlaga postopkov ali ugotovitev opisanih v dokumentaciji,
- pregledu, razumevanju in vrednotenju zavarovanih digitalnih podatkov in dokazov, ko naročniki nimajo ustrezne strojne in programske opreme za uporabo ali prikaz določenih tipov datotek ali nosilcev podatkov oziroma ko je potrebno ugotoviti kaj posamezni digitalni dokazi sploh pomenijo v konkretni zadevi in ali so ti isti dokazi dejansko obremenilni in za koga (v smislu, kdo je dejanski uporabnik računalnika v kritičnem času),
- ugotavljanju strokovne ustreznosti forenzičnih postopkov, ko je potrebno ugotoviti, če so bili forenzični postopki opravljeni v skladu z načeli računalniške

forenzike in s primerno strojno in programsko opremo,

- ugotavljanju vsebinske pravilnosti rezultatov forenzičnih postopkov, ko je potrebno ugotoviti, če je oseba, ki je opravila forenzično preiskavo digitalnih podatkov pravilno interpretirala ugotovitve oziroma ali so izsledki pravilni ali napačni in bi bilo potrebno digitalne dokaze dopolniti ali pa jih celo zavreči,
- potrditvi istovetnosti digitalnih dokazov, ko obstaja kakršen koli sum, da izpostavljeni digitalni dokazi ne izvirajo iz preiskanega nosilca podatkov oziroma bi lahko bili ti digitalni dokazi celo spremenjeni, ponarejeni ali prilagojeni, da postanejo bolj obremenilni ali razbremenilni,
- ponovitvi že izvedenih forenzičnih postopkov, ko je potrebno ugotoviti, če je bil predhodni forenzični postopek dejansko opravljen tako, kot je razvidno iz dokumentacije oziroma revizijske sledi postopkov in je forenzik dejansko lahko prišel do predstavljenih ugotovitev,
- izvedbi še ne izvedenih forenzičnih postopkov, ko pri predhodnih forenzičnih preiskavah nosilci podatkov niso bili pregledani v celoti oziroma sploh niso bili in obstaja možnost, da se na njih najdejo še drugi digitalni podatki pomembni za konkretni postopek,
- predstavitvi primera, forenzičnih postopkov in digitalnih dokazov na razumljiv način, po potrebi tudi z grafično podporo, ko je tožilcem, sodnikom in odvetnikom v katerikoli fazi (pred)kazenskega postopka potrebno na enostaven, poljuden način razložiti tehnično zahtevno ozadje kaznivega dejanja, kompleksne forenzične postopke in pa tudi dokaze, saj si lahko s tem močno olajšajo razumevanje zadeve saj s pomočjo diagramov, skic, tabel in celo video posnetkov nekaterih postopkov lažje razumejo zapleteno tehnično situacijo.

Očitno je, da lahko sodni izvedenec za računalniško forenziko vsem strankam v vsaki fazi (pred)kazenskega postopka zelo pomaga vsem udeleženim, ki kakorkoli potrebujejo razlago, preverjanje ali dodatno forenzično preiskavo nosilcev digitalnih dokazov. Pri tem se ne sme zanemariti dejstva, da lahko pride sodni izvedenec do drugačnih ugotovitev, kot so prišli predhodni preiskovalci. V takih primerih je namesto imenovanja tretjega strokovnjaka smiselno soočiti vse dotedanje strokovnjake, ki bodo poenotili programska in strojna orodja oziroma celo metodologijo in na tak način prišli do enakih ugotovitev.

## Zaključek

Informacijska tehnologija se je v vsakdanje življenje vpletla do te mere, da je danes težko najti civilni ali kazenski postopek, kjer forenzika nosilcev digitalnih podatkov ni potrebna. To je še zlasti očitno sedaj, ko se digitalni dokazi nahajajo na mobilnih telefonih in drugih prenosnih napravah, ki jih ima praktično vsak posameznik. Prav za te naprave, ki jih je neprimerno več, kot računalnikov, pa so potrebna še dodatna posebna znanja in posebne naprave, da se zagotovi strokovnost forenzičnega postopka.

Posledično to pomeni veliko šolanja za organe pregona, tožilstvo, sodišča in odvetnike. Glede na količino dela, predznanje in opremljenost vseh naštetih, je lahko pomoč sodnega izvedenca zelo dobrodošla, saj se na tak način neprimerno hitreje pride do želenih ciljev, ob tem pa naštetim ni potrebno nobeno vlaganje v izobraževanje in nakup strojne ter programske opreme.

## Literatura


1. McKemmish, R. (1999). **What is Forensic Computing? Trends & Issues in Crime and Criminal Justice**. Australian Institute of Criminology, junij 1999. Po URL: http://www.aic.gov.au/publications/tandi/ti118.pdf, dostop 16.10.2005.
2. Morgan W. C. (2002). An Historical Perspective of Digital Evidence: A Forenisc Scientist's View. **International Journal of Digital Evidence**, let. 1 izdaja 1. Po URL: http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78 -1059-3432402909E27BB4.pdf, dostop 16.2.2006.
3. Rathmell, A.; Valeri, L. (2003). **Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries**. RAND Europe – študija za Evropsko komisijo, Generalni direktorat za informacijsko družbo. Po URL: http://europa.eu.int/information_society/eeurope/2005/doc/all_about/csirt_handbook_v1.pdf, dostop 5.9.2005.

# Povzetki poglavij

## Kriminaliteta in tehnologija: uvod

**Aleš Završnik**

Informacijska tehnologija (IT) omogoča učinkovita »zdravila« pri odkrivanju kaznivih dejanj in pregonu domnevnih storilcev (na primer s policijsko uporabo zbirk osebnih podatkov) in omogoča bolj učinkovito varstvo zasebnosti (na primer komunikacijske zasebnosti s programi za kriptiranje komunikacij). A vendarle IT pogosto učinkuje tudi kot Pandorina skrinjica, ker omogoča zlorabe ali preprosto zato, ker »v praksi« ne deluje: zbirke osebnih podatkov »puščajo«, intenziteta profiliranja in internetnega nadzora nesorazmerno posegata v temeljne človekove pravice in svoboščine, videonadzorni sistemi javnega prostora ne odvračajo storilcev kaznivih dejanj itn. Članek predstavi to dvojno »Janusovo« naravo IT in njeno soodvisnost od družbenega konteksta. Tehnični predmeti, uporabljeni pri sodobnem tehnično okrepljenem nadzoru in pri odkrivanju kaznivih dejanj in kazenskem pregonu storilcev, so, tako kot je kriminaliteta, sociološki proizvodi. To so objekti, ki jih ni lahko opazovati ali meriti. Poglavje predstavi, kako so ti tehnološki predmeti »politika z drugimi sredstvi« in kako pomagajo izgrajevati nov koncept »prevencijske pravičnosti« (angl. »*pre-crime justice*«), ki delovanje akterjev kazenskopravnega sistema in novih zasebnih varnostnih akterjev vedno bolj usmerja tudi na zgodnje označevalce (tveganja) za nastanek kazenskopravnega primera.

## 1 Nadzorstvene študije v kulturi bajtov: Kaj je »novo« nadzorovanje?

**Aleš Završnik**

Informacijska tehnologija (IT) spreminja kulturo, zato so družbeni podsistemi vključno z mnogovrstnimi oblikami družbenega nadzora in sistemom kazenskega pravosodja neizogibno deležni kulturnih transformativnih učinkov IT. Poglavje predstavi kulturne transformativne učinke IT, kot so povečan pomen (kult) informacij v sodobni družbi in vpliv računalniške »ontologije« na naše dojemanje sveta, ter analizira vpliv teh kulturnih sprememb na osmišljanje in boj zoper kriminaliteto. IT spreminja družbeno nadzorovanje tudi bolj neposredno, kar je privedlo do nove renesanse nadzorstvenih študij. Poglavje zato predstavi »novo« tehnično okrepljeno nadzorovanje (angl. *surveillance*), razlike med modernim in postmodernim nadzorom oziroma med »tradicionalnim« in »novim« nadzorom. Analizira značilnosti »novega« nadzora kot so tehnična okrepitev nadzora, usmerjenost nadzora na telo, vsakodnevnost nadzora, univerzalnost nadzora ter motive in subjekte »novega« nadzora. Na koncu prikaže slabosti teze o nadzorstveni družbi in možnosti upora in subvertiranja vseprisotnega nadzora.

## 2 Komunikacijska zasebnost na delovnem mestu

**Kovačič Matej**

Pri vprašanju zasebnosti na delovnem mestu gre za trk dveh interesov – interesa delodajalca po gospodarni izrabi delovnega časa in sredstev na eni ter pravice do zasebnosti zaposlenega na drugi strani. Različni pravni sistemi dajejo prednost enkrat enemu, drugič drugemu. V praksi sta se v zvezi s tem izoblikovala predvsem t. i. »ameriški« pristop, ki daje prednost delodajalcu, in t. i. »evropski« pristop, ki daje prednost zaposlenemu. V prispevku sta z analizo zakonodaje in odločitev sodišč predstavljena oba pristopa, nekoliko podrobneje pa še ureditev področja zasebnosti na delovnem mestu v slovenski zakonodaji. Za Slovenijo je pomembno zlasti dejstvo, da se je evropska pravna praksa postavila na stališče, da lastninska pravica ne prevlada samodejno nad pravico do zasebnosti, kar pomeni, da je pravico do zasebnosti do določene mere potrebno spoštovati tudi na delovnem mestu. Vprašanje, kakšne naj bodo torej omejitve zasebnosti, pa je tako povezano tudi z vprašanjem sorazmernosti.

## 3 Hekerstvo kot izziv in upor

**Rusjan Marko**

Prispevek obravnava pojav hekerstva kot posebne oblike delovanja v umetno ustvarjenem informacijskem okolju, imenovanem kiberprostor. Hekerji kot soustvarjalci tega prostora skušajo delovati po svojih pravilih, ki so velikokrat v navzkrižju s pravnim redom, ki ga skušajo uveljaviti državne oblasti. Opredeliti je tudi potrebno, kaj vse lahko smatramo za hekerstvo in kakšni so motivi za hekanje. Prikazane so tri različne hekerske prakse: socialni inženiring, hektivizem in izmenjava datotek po internetu. Vse tri prakse pomenijo v veliko primerih kršenje pravnih predpisov, velikokrat pa so tudi inkriminirane kot kazniva dejanja. Socialni inženiring je največkrat oblika protipravne pridobitne dejavnosti. Hektivizem je družbeni aktivizem z uporabo dovoljenih ali nedovoljenih sredstev. Izmenjavanje datotek pomeni velikokrat kršenje avtorskih pravic in načenja vprašanja nematerialne lastnine.

## 4 Nigerijska prevarantska pisma

**Modic David**

Izraz nigerijska prevarantska pisma oziroma pisma 419 morda ni takoj prepoznaven. Vendar, če jih definiramo opisno – tista elektronska sporočila, kjer vas nekdo v polomljeni angleščini obvesti, da vam je bogati stric (čigar obstoj je bil do sedaj za vas popolna neznanka) zapustil milijone dolarjev v obliki zlatih palic in vse, kar stoji na poti med vami in užitkarskim življenjem, je plačilo majhne akontacije – naenkrat vemo mnogo več. Poglavje se najprej posveti demografskim podatkom in orisu finančnih izgub, ki doletijo posameznike ob nasedanju na spletne prevare, potem pa se osredotoči na nigerijska prevarantska pisma in njihovo etiologijo. Sledi natančnejši opis mehanike prevar 419 in njihovega poteka s posebnim poudarkom na psiholoških vzvodih, ki jih storilci uporabljajo, da bi povečali svojo uspešnost. Na koncu prispevka avtor poda nekaj smernic za nadaljnje raziskave in nekatere bolj odmevne poskuse omilitve posledic nigerijskih prevarantskih pisem.

## 5 Digitalni dokazi v kazenskem postopku: pogledi na aktualna vprašanja

**Selinšek Liljana**

Avtorica v prispevku najprej kratko predstavi pojem digitalnega dokaza, nato pa se osredotoči na analizo nove zakonske ureditve zasega in preiskave elektronskih naprav ter zavarovanja podatkov v njih. Z uveljavitvijo Zakona o spremembah in dopolnitvah Zakona o kazenskem postopku (ZKP-J) oktobra 2009 se je Slovenija pridružila državam, ki v kazenskem procesnem postopkovniku urejajo tudi ta vprašanja, in sicer zaenkrat v dveh razmeroma obsežnih členih (219.a in 223.a člen ZKP), ki sta v prispevku predstavljena na strnjen in zaokrožen način. V nadaljevanju poglavja avtorica s pomočjo tuje (predvsem ameriške) sodne prakse izpostavi in obdela še nekatera izbrana vprašanja, povezana z digitalnimi dokazi (*plain view* doktrino, vprašanje pridobivanja teh dokazov s strani zasebnih subjektov, razumno pričakovanje zasebnosti na izbrisanih podatkih ter vprašanje zasega elektronske naprave s strani državnih organov, ki ne delujejo po pravilih ZKP).

## 6 Forenzika mobilnih telefonov in vloga sodnega izvedenca za računalniško forenziko v kazenskih postopkih

**Šavnik Janko**

Razvoj sodobne družbe je na področju informacijske tehnologije v zadnjih nekaj letih zelo izrazit, saj so skoraj dnevno objavljeni novi preseženi mejniki. Informacijska tehnologija se je v tem času močno tako vpletla v vsakdanje življenje, da si ga brez nje praktično ne moremo več zamisliti. Naprave, kot so osebni in prenosni računalniki, mobilni telefoni, bankomati, terminali POS, ter storitvi, kot sta elektronska pošta in splet, so spremenile svet, skupaj z njimi pa tudi storilce kaznivih dejanj, ki vse to tudi uporabljajo. Posledično so vsi našteti možni viri digitalnih dokazov, ki jih je potrebno v postopkih pred sodiščem pregledati. Na tak način zavarovane dokaze pa morajo policisti, tožilci, sodniki in odvetniki tudi razumeti in jih znati uporabiti oziroma jim oporekati. Poglavje zato prikaže načela računalniške forenzike, analizira forenziko mobilnih telefonov (posebej forenziko kartic SIM in forenziko spominskih kartic) in prikaže, kakšno vlogo ima sodni izvedenec za računalniško forenziko v kazenskih postopkih.

# Summaries of Chapters

## Crime and technology: introduction

**Aleš Završnik**

Information technology (IT) has proven to be an efficient 'panacea' for crime control (e.g. databases containing detailed personal data help police track down offenders) and the protection of privacy (e.g. electronic communication privacy can be substantively enhanced by using encryption programmes). However, IT can also have an opposite effect on crime control and privacy: it can severely threaten civil liberties or may just be unable to meet its own performance standards. For instance, we have repeatedly witnessed the leaking of databases containing sensitive personal information, disproportionate internet profiling and on-line surveillance that infringe civil liberties, and video monitoring of everyday life that has no effect on deterrence. The chapter introduces the illustrated Janus-faced nature of IT and its dependence on the social context. Technical surveillance objects that are able to intensify and enhance contemporary forms of surveillance are, much like acts labelled as crimes, merely sociological objects. It is difficult to monitor and measure them as they can cause diverse social, cultural and other psycho-social effects (for instance, it is not possible to claim that CCTV cameras only enhance or only diminish the fear of crime; the effect depends on the cultural perception of technology in a specific time and space). The chapter explores the thesis that (information) technology is »politics with other means«. It situates surveillance enhancing IT equipment in the process of constructing what has been termed a "pre-crime justice". The notion helps to refocus criminal justice systems together with private crime control actors into early detection of sings and risks of potential crimes.

## 1 Surveillance studies in the byte culture: What is the "new surveillance"?

**Aleš Završnik**

Information technology (IT) changes our culture and all social systems, including the criminal justice system and other forms of crime control inevitably feel its cultural transformative effects. The chapter analyses several such cultural transformative effects, for instance, the augmented dependence of our modern societies on information ("the cult of information") or the influence that "computer ontology" has on our perceptions of reality, ourselves, others and society as such. The cultural transformative effects of IT are also very relevant in the criminological context as they mediate the way we think about crime and respond to it. In addition to exploring the indirect cultural influences of IT on crime control, the chapter also considers the more direct changes it has in the field. IT is deeply rooted in the contemporary surveillance processes and has consequently triggered a renaissance of surveillance studies. The chapter analyses the contemporary characteristics of this "new surveillance". It considers the difference between "modern" and "post-modern" forms of surveillance and holds that the latter is

characterised by technical means that focus on the body, by "everydayness" and the universality of monitoring. It further discusses the motives for the intensification of surveillance and the new subjects of surveillance. It concludes by presenting the critiques of the notion of "surveillance society" and shows the possibilities of resistance to the ubiquitous and constant monitoring of our daily lives.

## 2 Communication privacy in the workplace

**Kovačič Matej**

In dealing with the issue of privacy in the workplace, we are confronted with a clash between two interests: on the one hand, the interest of the employer to use as rationally as possible the company's work time and means of work, and on the other hand, the employee's right to privacy. Although different legal systems sometimes give priority to the employer and at other times to the employee, there are basically two approaches which have developed in practice: the so-called "American" approach, more favourable to the employer, and the »European« approach, giving priority to the employee. Through the analysis of legislation and court decisions the paper presents both approaches and highlights the regulation of workplace privacy in Slovene legislation. It is particularly significant for Slovenia that the European case law adopted the standpoint according to which a right to property does not automatically prevail over the right to privacy; consequently, a right to privacy has to be respected to a certain extent also at workplace. The question about what should actually constitute the limits of privacy is therefore also related to the issue of proportionality.

## 3 Hacking as a challenge and rebellion

**Rusjan Marko**

The chapter deals with the phenomenon of hacking as a special form of operation in an artificially created information environment, called cyberspace. Hackers as co-creators of this space, try to act according to their proper rules which are often in opposition to the legal order imposed by state authorities. First we need to define what is actually considered as hacking and to establish motives for it. This chapter describes three different hacking practices: social engineering, "hacktivism" and internet data files exchange. Although all three practices in many cases represent merely a violation of legal regulations, they are often also defined as criminal offences. Social engineering appears in most cases as a form of illegal gainful activity. Hacktivism is a kind of social activism practised by the use of licit and illicit means. Data files exchange often constitutes a violation of authors' rights and addresses the issue of non-material property.

## 4 Nigerian letter fraud

**Modic David**

The term “Nigerian letter fraud”, also called “Fraud 419”, may not be recognizable at first glance. Yet, if it is described as an electronic letter in which you were informed in broken English that your rich uncle (of whose existence you have been completely ignorant so far) left you some millions of dollars in the form of gold bars and that the only obstacle you have to surmount in order to reach an enjoyable life is to pay a small amount of advance fee – then we are certainly immediately more familiar with the notion. The chapter first provides some demographic data and describes financial losses inflicting those individuals who succumbed to these internet frauds. Next, it focuses on Nigerian letter frauds and their aetiology. A mechanism of frauds 914 is described more precisely as well as their course, by giving special stress on the psychological levers used by perpetrators in order to increase their efficiency. Finally, the author gives some suggestions for further research and provides examples of some well known attempts undertaken in order to alleviate the consequences of Nigerian letter frauds.

## 5 Digital evidence in criminal procedure: Views on current issues

**Selinšek Liljana**

The author first briefly describes the notion of digital evidence, and then focuses on analysing the new Slovenian regulation of investigation and seizure of electronic devices and the protection of data stored in them. With the implementation of the Act Amending the Criminal Procedure Act in October 2009, Slovenia joined the countries in which these issues are regulated in their procedural codes. This area is now regulated by two relatively extensive articles (Article 219.a and 223.a of the Criminal Procedure Act), which are concisely presented in the chapter. Following this analysis, the author highlights some specific issues related to digital evidence (e.g. the plain view doctrine, the question of obtaining digital evidence from private subjects, reasonable expectation of privacy regarding deleted data and the question of seizure of electronic device by those state agencies which do not operate according to the Code of Criminal Procedure), mainly drawing from foreign (especially American) case law.

## 6 Mobile phones forensics and the role of forensic experts for computer forensics in criminal trials

**Šavnik Janko**

The development of contemporary society in the area of information technology has been very extensive in recent years, which can also be noticed by a nearly daily publication of news concerning recent advances in IT. Information technology has become so much entangled with our everyday life that it has become practically impossible to imagine life without it. Devices such as personal computers and laptops, mobile phones, cash dispensers, POS terminals and services like electronic mail and internet have not only transformed the world, but have also transformed criminals who all take advantage of this new information technology. The chapter discusses possible sources of digital evidence which have to be examined in court trials. It is important for police officers, prosecutors, judges and lawyers to understand the evidence protected in this way and also to know how and when to use it or to refute it. The contribution therefore highlights basic principles of computer forensics, analyses the forensics of mobile phones (with special attention being given to the forensics of SIM cards and memory cards) and displays the role of forensic expert for computer forensics in criminal trials.

# Stvarno in imensko kazalo

## *Č*



## *D*

## *E*



## *F*



## *G*

## *H*



## *I*



## *J*



## *K*

## *L*



## *M*

## *N*



## *O*

## *P*



## *R*

## *S*

## *Š*



## *T*



## *U*



## *V*

## *W*



## *Y*



## *Z*



## *Ž*

**Novejše monografije Inštituta za kriminologijo pri Pravni fakulteti v Ljubljani**

- 1996 Bojan Dekleva (ur.): Nove vrste vzgojnih ukrepov za mladoletnike.
- 1996 Alenka Šelih: Otrokove pravice, šolska pravila in nasilje v šoli.
- 1997 Zoran Pavlovič in dr.: Slabo ravnanje z otroki v Sloveniji – opažanje in obravnavanje.
- 1998 Katja Filipčič: Obravnavanje mladoletnih delinkventov primerjalnopravni vidik.
- 1998 Zoran Kanduč, Damjan Korošec in Marko Bošnjak: Spolnost, nasilje in pravo.
- 1998 Bojan Dekleva: Droge med srednješolsko mladino v Ljubljani.
- 1999 Zoran Kanduč: Kriminologija – (stran)poti vede o (stran)poteh.
- 2002 Bojan Dekleva, Špela Razpotnik: Čefurji so bili rojeni tu – življenje mladih priseljencev druge generacije v Ljubljani.
- 2002 Zoran Kanduč: Žrtve, viktimizacije in viktimološke perspektive.
- 2004 Gorazd Meško (ur.): Preprečevanje kriminalitete – teorija, praksa in dileme.
- 2005 Zoran Kanduč: Kriminaliteta, družbeno nadzorstvo in postmodernizacijski procesi.
- 2005 Katja Šugman (ur.): Poligraf v kazenskem postopku.
- 2006 Zoran Kanduč (ur.): Droge, zapori, ženske – postmoderna družba in njene zasvojenosti.
- 2006 Katja Šugman (ur.): Izhodišča za nov model kazenskega postopka.
- 2006 Katja Filipčič (ur.): Uvajanje vzgojnih ukrepov dela v korist skupnosti in socialnih treningov.
- 2007 Matjaž Ambrož: Kaznivo dejanje in njegove vrednostne prvine.
- 2007 Zoran Kanduč: Kriminologija – (stran)poti vede o (stran)poteh. 2.izd.
- 2007 Primož Gorkič, Matjaž Jager in Katja Šugman (ur.): Policija, državni tožilci in uspešnost preiskovanja kaznivih dejanj – izbrani pravni in sistemski vidiki.
- 2007 Alenka Šelih (ur.): Sodobne usmeritve kazenskega materialnega prava.
- 2007 Zoran Kanduč: Subjekti in objekti (ne)formalne socialne kontrole v kontekstu postmodernih tranzicij.
- 2009 Aleš Završnik: Homo criminalis – upodobitve zločinskega subjekta v
- visokotehnološki družbi tveganja.
- 2009 Ivanka Sket (ur.): Pregled raziskovalnega dela – 1954-2009.