UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Gregor Perič

# Kraja identitete v informacijski družbi

**Diplomsko delo**

Ljubljana, 2014

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Gregor Perič

Mentor: red. prof. dr. Marjan Brezovšek

# Kraja identitete v informacijski družbi

**Diplomsko delo**

Ljubljana, 2014

# ZAHVALA

*Noben človek ni tvoj prijatelj,*
*noben človek ni tvoj sovražnik,*
*vsak človek je tvoj učitelj.*

Težko bi drugače kot s to hindujsko mislijo bolje povzel, kar sem med študijem in še zlasti v času nastajanja svojega diplomskega dela imel priložnost spoznati. Moja iskrena zahvala gre zato vsem, ki so kakorkoli pripomogli k nastanku tega diplomskega dela.

Za vso podporo in neumorne spodbude sem globoko hvaležen staršema. Brez njune prizadevnosti in vsega, kar sta mi posredovala, to delo prav gotovo ne bi ugledalo luči sveta. Zahvaljujem se tudi vsem sorodnikom, ki so mi kakorkoli stali ob strani.

Zahvaljujem se svojemu mentorju prof. dr. Marjanu Brezovšku za nasvete, pomoč in prijazen odnos pri pisanju diplomskega dela. V veliko pomoč so mi bili tudi predlogi dr. Mateja Kovačiča, informacijske pooblaščenke Nataše Pirc Musar, ki me je tudi spodbudila k obravnavi zadevne tematike, in nekaterih njenih sodelavcev.

Navsezadnje gre zahvala tudi prijateljem; tako za koristne nasvete in predloge, zaradi katerih je bil zaključek tega dela še bližje koncu, pa tudi za obstranske zadeve, zaradi katerih se je oddaljeval, a mi obenem še drugače omogočil se učiti in zoreti.

Bili ste in ostajate izjemni učitelji.

**Kraja identitete v informacijski družbi**
Kraja identitete posplošeno pomeni prevzeti identiteto nekoga drugega z uporabo osebnih podatkov oz. idenitete žrtve za pridobitev določenih koristi. Pojem zlorabe identitete se uporablja tudi kot sopomenka za krajo identitete; temeljna razlika med pojmoma pa je v tem, da zloraba identitete zajema tudi uporabo lažne, namišljene identitete. Posledice kraje identitete najbolj občutijo v Avstraliji, Kanadi, Koreji, ZDA in Združenem Kraljestvu, najmanj pa v EU. Zaradi anonimnosti in brezprostorskosti kibernetskega okolja se konvencionalne patologije selijo tudi v ta prostor in predstavljajo tveganja zasebnosti. Spletna kraja identitete je po obsegu, učinkih in posledicah najmanj izenačena z nepovezano obliko kraje identitete; v praksi pa kršitelji kombinirajo prvine obeh. Zaradi različnih pravnih ureditev področja varovanja osebnih podatkov je različno tudi preprečevanje, preganjanje in sankcioniranje zlorab identitete, zlasti pa njihov obseg.
Kršitelji delujejo v majhnih, geografsko razpršenih skupinah znotraj omrežij brez jasne hierarhične linije odločanja. Zaradi razpršenosti storilcev, potencialnosti žrtev in spremenljivosti/prilagodljivosti oblik kriminala je večina današnjega kiberkriminala izven dosega organov pregona in regulatorjev; zato se preganjajo le prestopki zadostnega (največjega) obsega. Breme za zagotavljanje varnosti leži na iskanju tehnoloških rešitev in zakonitostih trga.

**KLJUČNE BESEDE:**
kraja identitete, kiberkriminal, informacijska družba.

**Identity theft in the information society**
Idenitity theft generalized means to take over someone else's identity using personal data or victims' identity to obtain certain benefits. The term ID Fraud is being used also as a synonym for ID Theft; the fundamental difference between the two terms is in that ID Fraud includes the use of a false notional identity as well. The most affected countries by the consequences of ID Theft include Australia, Canada, Corea, USA and UK, the less affected is the EU. Because of anonymity and spacelessness of cyber environment conventional pathology is moving in this area as well and poses risks to privacy. The scope, impact and consequences of online identity theft are not less than equated with offline identity theft; therefore in practice the offenders combine elements of both. Due to different legislative regulation of protection of personal data also prevention, prosecution, sanctioning and in particular the scale of identity theft are different.
The perpetrators act in small geographically dispersed groups within networks without clear hierarchical lines of decision-making. Considering that the offenders are dispersed, the potentiality of victims and the variability/adaptability of forms of crime the majority of today's cyber crime lies beyond the reach of prosecuting organs and legislators; therefore only the large-scale infringements are being prosecuted. The burden for provision of security lies in searching for technological solutions and in the laws of the market.

**KEY WORDS:**
Identity Theft, Cyber Crime, Information Society.

# KAZALO VSEBINE

# KAZALO PREGLEDNIC IN SLIK



*Questa a peccar con esso così venne,*
***falsificando sé in altrui forma,***
*come l'altro che là sen va, sostenne,*

*per guadagnar la donna de la torma,*
*falsificare in sé Buoso Donati,*
*testando e dando al testamento norma.*
(Alighieri 1994)

Da bi do greha z njim prišla, lisica,
**privzela si je tuj obraz**, kot tisti,
ki proč gre in ga je kobil kraljica

tako zamikala, da je obisti
in glas potvoril Buoseja Donati
in pravno stal je v oporočni listi.

*Do kraje identitete pride, kadar nam nekdo ukrade osebne podatke in jih uporabi brez našega privoljenja. Gre za resen zločin, ki lahko močno prizadane naše finance, kreditno zgodovino in ugled – za odpravo njenih posledic je pa potreben čas, denar in potrpljenje.*
(Federal Trade Commission 2013a)

# 1 UVOD

Skoraj ne mine dan, da ne bi bili soočeni s tem, kako zadnji dosežki s področja informacijsko komunikacijske tehnologije vplivajo na življenje, naravo in organizranost dela, preživljanje prostega časa, spreminjajo odnose med posamezniki, v skupinah in celo med državami. Če na eni strani dosežki tehnološkega razvoja predstavljajo nove in nove poslovne in druge priložnosti, so po drugi strani tudi izziv, saj pravtako omogočajo priložnosti za vsakovrstne zlorabe in vdor v našo zasebnost. Meja, do koder bomo drugim dopustili, da imajo vpogled v našo zasebnost, je seveda najprej odvisna od vsakega posameznika. Vendar odkar spletne dejavnosti posameznikov, zlasti pa spletna družbena omrežja, zaradi informacijsko komunikacijskih tehnologij konvergirajo v en »center«, je to dejstvo v marsičem zapolnilo *podobo* družbe tudi v tistih segmentih, ki so bili doslej veliki večini skriti in težko, če sploh, dostopni. Zaradi tega je postala naloga upravljati z mejo naše zasebnosti veliko zahtevnejša, težavna, težko obvladljiva in posejana z mnogimi (skritimi) pastmi.

## *1.1 Zastavitev teme*

Nekatera področja družbene realnosti se zaradi neslutenega razvoja spreminjajo in prilagajajo hitreje od ostalih; področje kriminala ni pri tem nobena izjema, zlasti ne kibernetskega. Kraja identitete ima kot eksces več tisočletno zgodovino, vendar je šele v zadnjem času pridobila poimenovanje, kakršno ga poznamo danes, čeprav je tudi slednje geografsko pogojeno; pojem kraja identitete je najtrdneje zasidran v anglo-saksonskem svetu, medtem ko se v Evropi pogosteje srečujemo s pojmom zloraba identitete ali kriminalom s področja identitete. Na osnovi prebranih gradiv lahko avtor zatrdi, da je v slovenskem jezikovnem področju bolje zastopan pojem kraje identitete, kar gre pripisati »amerikocentričnosti« tega pojava. Iz vrste razlogov, ki se jih bomo podrobneje dotaknili v nadaljevanju, ima kraja identitete v ZDA in Združenem Kraljestvu daljšo »tradicijo«, pa tudi domet.

Pri poglabljanju v problematiko kraje identitete hitro naletimo na sprva nerazumljivo pomanjkanje referenčnih raziskav, zlasti z območja Evrope, kar se nato izkaže kot

posledica drugačne tradicije pravnega urejanja področja varstva zasebnosti in manjše (ali večje) izpostavljenosti temu pojavu.

Za kaj pravzaprav gre pri kraji identitete? Najbolj poenostavljeno pomeni prevzemanje identitete nekoga drugega. Do nje pride, kadar kršitelj uporabi osebne podatke oz. ideniteto nekoga drugega (ime, datum rojstva, naslov bivanja, gesla za dostop do finančnih in drugih storitev) za pridobitev neke koristi, običajno ekonomske narave, ali inkriminacijo druge osebe (Fraud Prevention Expert Group; IP-RS 2012b, 5; United States Department of Justice 2013). Krajo identitete je moč izvesti na klasičen način, z vohljanjem za žrtvijo, odtujitvijo njenih dokumentov ali drugih predmetov, kar zahteva fizično prisotnost in močno poveča tveganje ob izpostavljanju. Nove oblike kraje identitete se pa zanašajo na prednosti, ki jih v te namene omogoča anonimnost in brezprostorskost kibernetskega okolja. Zaradi nenehnega razvoja na področju informacijsko komunikacijskih tehnologij so nekatere ugotovitve v pričujoči nalogi skoraj gotovo podvržene hitremu zastaranju, kljub temu pa ostaja osnova kraje identitete nespremenjena skozi čas. V nadaljevanju bomo opazili, da se nekatere klasifikacije in tipologije zlorab zasebnosti mestoma tudi ponavljajo ali podvajajo. Metodološko je sicer možno postaviti ločnico med krajo identitete, ki se odvija na »klasičen« način in tisto, ki jo omogoča kibernetski prostor, v praksi pa potekajo zlorabe kot najbolj optimalna kombinacija ene in druge.

## *1.2 Namen diplomskega dela in njegovi cilji*

Problem kraje identitete je za člane informacijske družbe, odvisne od uporabe informacijsko komunikacijskih tehnologij, realno tveganje. Namen te naloge je **ugotoviti, ali širše implikacije novih tehnologij resnično predstavljajo tolikšno tveganje za našo zasebnost ali pa po drugi strani ne gre pri tem bolj za tehnofobične vzgibe in zadržanost do novosti ter podvrženost vplivu skupin pritiska in medijskega »infotainmenta«.** Da bi avtor uresničil svoj namen, želi v tej nalogi s kritično obravnavo področja kibernetskega kriminala in upoštevanjem razlik med pravnimi ureditvami varstva osebnih podatkov presoditi o (različnih) stopnjah tveganja članov informacijske družbe za primere zlorab identitete.

Avtor si je v diplomskem delu zastavil tri izhodiščne cilje:

- predstaviti osnovne lastnosti kibernetskega kriminala in podati splošno oceno o njegovih bodočih razvojnih dinamikah;
- oceniti, ali ustroj interneta premore takšen red oz. strukturo, da jo je moč regulirati na način, ki omogoča uspešen boj zoper poskuse zlorab in;
- opredeliti koncept zlorabe identitete, njegove osnovne lastnosti, najpogostejše pojavne oblike in glavne dejavnike, ki ga omogočajo.

Na podlagi ugotovitev, vezanih nanje, se bo avtor poskusil karseda približati odgovoru na zastavljeno raziskovalno vprašanje. Avtor obenem ugotavlja, da če želi v svoji nalogi priti do ugotovitev, ki zaradi hitrega spreminjanja tehnik zlorab zasebnosti ne bodo izrazito podvržene zastaranju, mora pri obravnavi koncepta kraje identitete obvezno zajeti tudi makro pogled, torej splošnejše lastnosti, zakonitosti in trende kibernetskega kriminala.

## *1.3 Raziskovalno vprašanje, metode in tehnike*

Temeljno raziskovalno vprašanje, ki si ga v pričujočem diplomskem delu zastavljamo, je:

| ali je v pogojih informacijske družbe več možnosti (večja verjetnost) za zlorabe zasebnosti. |
|---|

Način, kakor je vprašanje zastavljeno, implicira primerjavo, pri čemer ne bo odveč opomba, da ta primerjava ne želi biti zgodovinska, tj. nanašajoča se na pretekla »predinformacijska« obdobja, marveč bolj »tehnološka«. S tem pa ne mislimo toliko na tehnološko podstat delovanja informacijsko komunikacijskih tehnologij, ampak na razlikovanje med spletno (online) in nepovezano (offline) krajo identitete.

Avtor namerava v diplomskem delu uporabiti kombinacijo deskriptivnih in empiričnih metod. Za opredelitev in podrobnejšo analizo na zlorabo identitete vezanih pojmov in konceptov, kot so informacijska družba, kibernetski prostor, kibernetski kriminal, bosta to analiza primarnih virov (področna zakonodaja) ter zlasti analiza in sinteza sekundarnih virov (znanstvene literature, člankov, poročanj množičnih medijev). Za oceno obsega in pogostosti pojavljanja oblik zlorabe identitete pa se bodo izsledki v diplomski nalogi opirali na dostopne empirične analize (raziskave z anglo-saksonskega področja in Evrope), v zelo omejenem obsegu pa tudi na medijska poročanja (intervjuji s strokovnjaki za informacijsko varnost).

Uporabljene raziskovalne metode v marsičem vplivajo na raziskovalne rezultate. Avtor je pri analizi zbrane literature in raziskav naletel na kar nekaj tehtnih opozoril, ki jih podrobneje obravnava v poglavju 1.5 Metodološke omejitve in zadržki.

## *1.4 Zgradba diplomskega dela*

Delo je sestavljeno iz treh komponent: prva komponenta zajema uvod z zastavitvijo teme, namenom in cilji, raziskovalno vprašanje, uporabljeno metodologijo in metodološke zadržke. V drugi komponenti avtor postavi strukturo diplomske naloge v treh členih. Po uvodni opredelitvi temeljnih pojmov je prvi člen strukture poglavje o nadzoru in zasebnosti, s posebnim poudarkom na konceptu anonimnosti znotraj kibernetskega okolja. V drugem členu sledi opredelitev kibernetskega v splošnem smislu in zlasti skozi prizmo kriminogenosti. Vsebina sklepnega, tretjega člena je osredotočena na zlorabe identitete in obravnava terminološke nedorečenosti, navezavo na ostale kategorije kaznivih dejanj, umestitev v mednarodno primerjalni kontekst, deloma pa se dotakne tudi odgovornosti in nekaterih prevladujočih tehnik zlorab. Zaključno komponento predstavlja sklep z odgovorom na zastavljeno raziskovalno vprašanje in poskusi nakazati možen trend razvoja koncepta kraje identitete.

## *1.5 Metodološke omejitve in zadržki*

Na prelomu tisočletja so se preučevalci kiberkriminala soočali s pomanjkanjem kakršne koli oblike uradno zabeleženih statistik. Iz tistega časa obstoji sicer precej ocen, ki so jih naredile komercialne organizacije na področju hekerstva in komercialnih dejavnosti, vendar so pomanjkljive v smislu standardiziranosti definicij različnih kriminalnih dejanj, kakor tudi metodološko (Wall 2001, 7–8). Desetletje zatem je sicer mogoče najti nekatere vladne longitudinalne analize (zlasti Zvezne komisije za trgovino Združenih držav Amerike; ki jo obravnava pričujoče delo) (Federal Trade Commission 2013c) glede uradno registriranih primerov oblik kraje identitete, k čemur je pripomogla postopna standardizacija postopkov za prijavo zlorab. Vendar je potrebno tovrstne analize jemati z nekaj zadržki, saj so pogojene s specifiko pravno-ekonomske ureditve (npr. podlaga za koriščenje nekaterih pravic v EU terja drugačne, kompleksnejše oblike osebne identifikacije kot v ZDA). K

nepopolnosti pogleda na realno stanje deloma pripomore tudi težnja žrtev, najsi bodo to posamezniki ali pa skupine, podjetja, k zamolčanju kršitev in zlorab. Za obravnavo področja posegov v identiteto posameznikov se je zato kot bolj zanesljiva izkazala kvalitativna metoda raziskovanja s pomočjo analize tekstov.

Kakor velja za vse vrste kvantitativnega raziskovanja kriminala belih ovratnikov, je tudi pri proučevanju kiberkriminala težava v nezmožnosti, da bi vnaprej predvideli dejanski obseg in verjetnost ravni tveganja. Razlogi tičijo v tem, da (se) žrtve:

- nihče ne vpraša o viktimizaciji;
- ne podajo odgovorov, kadar so o njem izprašane;
- ne razkrijejo svojih izkušenj, ali;
- ne zavedajo viktimiziranosti (Wall 2001, 50).

K dodatni previdnosti so v svojem poročilu posebne skupine Evropske Komisije *Fraud Prevention Expert Group* (FPEG) iz leta 2007 o zlorabah identitete v finančnem sektorju pozvali z ugotovitvijo, da »merjenje problema ni enostavno. Na eni strani je močno odvisno od tipa uporabljene definicije; na drugi strani pa, da so nekatere posledice pri žrtvah težko merljive« (Fraud Prevention Expert Group 2007b, 2).

Do podobnih ugotovitev prihajajo v raziskavi OECD, ki je morda ena najbolj poenotenih analiz stanja[1] s področja kraje identitete (s poudarkom na elektronskem poslovanju in e-bančništvu), kjer kot največji oviri za ugotavljanje obsega in primerjave med državami / ureditvami vidijo (OECD 2009, 9):

a) *Pomanjkanje enotne definicije*. Krajo identitete nekatere države definirajo kot specifično obliko kriminala, spet druge pa kot pripravljalni korak pri izvrševanju drugih oblik kriminala.
b) *Pomanjkanje primerjalnih podatkov*. Statistične analize so področje kraje identitete (tako tiste spletne kot nekibernetske) zaobšle. Večina dostopnih podatkov izhaja iz ZDA; podatki iz Evrope so pa, z izjemo Združenega Kraljestva, razpršeni. Kadar so podatki v evropskih državah o kraji identitete na voljo, običajno te oblike kriminala ne obravnavajo samostojno, temveč v povezavi z ostalimi oblikami. Ena redkih držav, ki krajo identitete obravnava

[1] Kljub vsemu zbir ugotovitev statističnih analiz v vzorcu ne zajema vseh držav članic OECD (2009, 33).

neodvisno od drugih oblik kriminala, so ZDA, zaradi česar je avtor v pričujoče delo tudi vključil izsledke ameriške Zvezne komisije za trgovino.

Potrebno je poudariti tudi, da različne države različno zbirajo statistične podatke o kraji identitete in tako otežujejo, če ne celo onemogočajo medsebojne primerjave. Pomembno zavedanje je, da prihaja do velikih odstopanj v ugotovitvah med zasebnimi in javnimi subjekti; nekateri opažajo padajoče trende pojavnosti kraje identitete in to pripisujejo povečanemu zaupanju potrošnikov, nasprotno pa drugi beležijo trend rasti (OECD 2009, 9). Dejstvo, da prihaja do razlik v ugotovitvah med statističnimi analizami, ki jih delajo državni organi v policy namene in tistih, ki jih izvajajo zasebna podjetja v poslovne namene ter zavedanje, da statistične analize ne merijo istih tipov zlorab in so zato neprimerljivi (ibid., 33), morajo služiti kot resen metodološki poziv k previdnosti pri izvajanju splošnejših sklepov in ugotovitev o dejanskem stanju.

Dodatni vidik kvalitativne dimenzije raziskovanja je pravtako pomemben. Pa ne le zato, ker lahko hekerji in drugi kršitelji zaradi lastnih interesov napihujejo svoje dosežke. V Wall (2001, 50) beremo, da je lahko isto tudi z oblastnimi odzivi, ko strokovnjaki za varnost v *uradnih* raziskavah namenoma ali paranojično napihujejo tveganje, s tem pa vplivajo na »namensko« (pre)razporejanje sredstev v državni in javni upravi za zagotavljanje primernih varnostnih ukrepov.

Kljub temu, da se na področju informacijskega okolja meritve izvajajo že desetletja, ohranja merjenje zlasti tistih družboslovnih pojavov, ki so zaradi bliskovitega tehnološkega (in socialnega) razvoja podvrženi hitremu spreminjanju svojevrsten metodološki izziv (prim. Vehovar v Babnik 2012, 18). Dodatno k temu prispeva splošno nerazumevanje osnovnih pojmov, vezanih na internet.

# 2 OPREDELITEV TEMELJNIH POJMOV

Za ustrezno razumevanje področja zlorab in kršitev s področja varstva osebnih podatkov v realnosti, kjer informacijsko komunikacijska tehnologija pomembno soustvarja družbeni zemljevid, je najprej potrebno definirati, kaj so podatki, informacije in kaj razumemo s konceptom informacijske družbe. To je zlasti pomembno, ker smo v vse večji meri odvisni od informacij, ki so, še z materiali in energijo, temeljni viri sveta, v katerem danes živimo (Babnik 2012, 9).

## *2.1 Podatki in informacije*

»Podatki so dejstva in številke« (Rosenfeld in Morville 2002, 5). Z *digitalnostjo* v informacijskem okolju poenostavljeno mislimo na to, da dosežemo redukcijo podatkov v tokove ničel in enic v dvojiškem številskem sistemu. Tako lahko praktično skoraj vsako informacijo prenašamo preko telekomunikacijskih omrežij, najsi bodo žična ali brezžična (Wall 2001, 29). Temeljna infrastruktura, ki komunikacijo omogoča, je informacijska tehnologija[2]. Informacijski sistemi z njeno pomočjo operirajo s podatki in jih pri obdelavi kakovostno oplemenitijo v informacije. Vse tisto vmes med podatki, relacijskimi bazami podatkov (ki dajejo konkretne odgovore na konkretna vprašanja) in znanjem so informacije (Rosenfeld in Morville 2002, 5). Bell (v Babnik 2012, 9) ravno tako informacijo pojmuje kot nadpomenko podatkov: zanj je informacija »novica, dejstvo, statistika, poročilo, predpis, davčna koda ...«, ki jo moramo razlikovati od znanja (znanje je torej »interpretacija v kontekstu, eksegeza, odnosnost in konceptualizacija, oblika argumentacije«). Pri reflektiranju informacije moramo biti pozorni na njeno vsebino, prav tako pa tudi na njene širše implikacije – informacija je tudi »zasebno in javno dobro, življenjsko pomemben resurs (in) sprožilni element znanja« (ibid., 9–10).

Definicije o informacijah lahko uvrstimo v 4 skupine; enim je lastna redukcija na podatkovne tokove in binarnost, ki v skrajni interpretaciji postavi enačaj med

[2] Informacijska tehnologija zajema katero koli opremo, ki jo uporabljamo za samodejno zajemanje, shranjevanje, upravljanje, organiziranje, razvoj, nadzor, prikazovanje, preklapljanje, izmenjavo, posredovanje ali sprejemanje podatkov ali informacij (Walz v Babnik 2012, 11). Pintarič (v Babnik 2012, 11) pa izpostavlja konvergenco predhodnih tehnologij za omogočanje komunikacijskih procesov.

kvaliteto in kvantiteto; drugim je lastna organiziranost in »sporočljivost«; tretjim širina (»informacije so vse, kar zmanjšuje negotovost« (Trček 2003,18)); četrtim je pa lastna vsebina lastnosti, ki jo pridobijo (fenomenološki pogled) ... V (tridelni) preglednici 2.1 so tri trditve Barlowa, zagovornika fenomenologije, o treh sklopih lastnosti informacij: v prvem sklopu izpostavlja pomen interakcij in informacijskih tokov, v drugem sklopu pomen spreminjanja in po/obnavljanja, v tretjem pa časovno komponento in menjavo. Posredno ta taksonomija predpostavlja ubikvitarnost informacij, torej njihovo *vseprisotnost*.

Preglednica 2.1: Taksonomična definicija informacij(e) po Barlowu

| **Informacija = dejavnost, delovanje** |
|---|
| • je glagol, ne samostalnik<br>• jo izkušamo, ne posedujemo<br>• mora biti v gibanju<br>• se razmnožuje, ne razdeljuje |

| **Informacija = življenjska forma** |
|---|
| • želi biti svobodna<br>• se replicira v nove možnosti<br>• se želi spreminjati<br>• je (po)kvarljiva |

| **Informacija = odnos, zveza** |
|---|
| • njen pomen in vrednost sta edinstveni za vsakega sprejemnika<br>• podobnost ima večjo vrednost kot različnost, redkost<br>• izključnost določa vrednost<br>• čas nadomešča prostor<br>• udejanjenje je najboljša zaščita<br>• avtorstvo, vir sporočila določa vrednost<br>• je sama po sebi lahko nagrada, zadoščenje |

Vir: Trček (2003, 19).

Tokovi informacij se gibljejo v okolju, ki je »globalno, v realnem času in nepretrgoma« (ibid., 20); kraj (v geografskem smislu) zanje več nima odločujoče vloge. Ubikvitarne informacije se (lahko) hkratno pojavljajo na več lokacijah istočasno.

Vendar pa moramo informacijo obravnavati z zadostno mero kritičnosti. Trček (2003, 21) opozarja na hekerski pregovor oziroma kratico GIGO – »Garbage In, Garbage Out«, ki postavlja poenostavitve, – kakršnih v obliki spodnje enačbe najdemo mnogo tako v jedru teoretskih osmišljanj pojma informacije, kot tudi v političnih in novinarskih diskurzih, – pod vprašaj:

| podatek = informacija = znanje = modrost = resnica = svoboda |
|---|

Ta logična poenostavitev ni le generator kvalitativne pestrosti informacij, temveč tudi nenadzorovanih in neobvladljivih količin podatkov.

Če na informacije pogledamo še skozi prizmo varnosti, so zanje značilni trije elementi oz. pogoji (Bagon in drugi 2006, 114):

- celovitost - točnost, popolnost in ažurnost sprememb;
- razpoložljivost in dostopnost - konstantna dostopnost, odsotnost (tehničnih idr.) motenj, dostopnost na podlagi pravic tipov uporabnikov; in
- zaupnost in tajnost - varovanje pred razkritji, nepooblaščenimi dostopi in zlorabami.

## *2.2 Informacijska družba, kibernetski prostor*

Koncept zgodovinskih razvojnih faz družbe je prešel od industrijske v storitveno in kasneje še v informacijsko družbo (Ježek 2004, 4). Informacijska družba se postavlja v okoliščinah postfordistične proizvodnje in globalizacije. Izgrajevanje tega koncepta sovpada z obdobjem v 60-ih in 70-ih letih, ko je prevladujočo industrijsko tehnologijo pričela zamenjevati informacijska tehnologija, okrepilo se je pa zlasti v 90-ih letih s popularizacijo interneta. Soroden pogled na informacijsko družbo ponuja ugotovitve, da so družboslovne razprave o kibernetskem okolju v začetkih raziskovanja termine prevzemale z novinarskega področja (t. i. trendovske skovanke oz. »buzz-words«), ki so danes postali »privzeta nedefinirana terminološka stalnica« (Trček 2003, 11):

»informacijska družba, omrežena družba, informacijska avtocesta, kiberpank, avatarji ...« K naštetim lahko dodamo še sledeče: post industrijska družba, storitvena družba, družba znanja in inovacijska družba (Ježek 2004, 4). Slednje priča, da je paradigmatska podstat ne v celoti dodelana in definirana. V klasičnih funkcionalističnih in marksističnih opredeljevanjih družbe kot sociološkega fenomena namreč še ne zasledimo izpostavljanja informacijske podstati (Babnik 2012, 13). Po mnenju teoretika strukturacije Giddensa (v Trček 2003, 17) se informacijske družbe izoblikujejo tedaj, ko se družbe organizirajo v nacionalne države. Slednje za svoje delovanje namreč potrebujejo razvejan in kompleksen aparat shranjevanja in procesiranja informacij o svojih državljanih. Korak dlje stori Webster (v Trček 2003, 107), ki meni, da je o modernih nacionalnih državah z vidika informatiziranosti bolje kot o »informacijskih družbah« smiselneje govoriti kot o »družbah nadzora« (ibid.). Informacijsko družbo opredeljuje vrsta dejavnikov, ki so medsebojno prepleteni: »(t)i dejavniki so predvsem izobraževanje in usposabljanje, raziskave, tehnološki razvoj in inoviranje ter uporaba informacijsko-komunikacijske tehnologije v vseh segmentih gospodarstva in družbe« (Ježek 2004, 4). Kot še nikoli doslej v zgodovini človeštva za informacijsko družbo velja, da je človeško mišljenje postalo avtonomna produkcijska sila (Pivec v Babnik 2012, 16). Za naše razumevanje pa je še najpomembnejša Castellsova (v Babnik 2012, 17) ugotovitev, da se »dominantne funkcije in procesi v informacijski dobi organizirajo okoli mreže.« Mrežno delovanje pa odločilno vpliva na delovanje in odnose v družbi.

Dotaknimo se še kibernetskega prostora. Navkljub temu, da je ta termin zelo pogosto uporabljen, ohranja nekatere nedorečenosti, predvsem v odnosu med virtualnim in realnim. Mnogo avtorjev izpostavlja odnos kibernetskega prostora do fizičnega in/ali geografskega prostora; ta naj bi bil afizičen in ageografski. Vendar pa z razvojem tehnologije, ki omogoča »taktilno percepcijo« (tj. prejemanje impulzov s pomočjo dotika), se ta meja vse bolj briše. Holmes (v Babnik 2012, 12) opredeljuje kibernetski prostor kot »realni in imaginarni prostor, v katerem se znotraj elektornsko posredovanega in simuliranega prostora srečujejo posamezniki.« Holmesova opredelitev je oprta na razlikovanje med kibernetskim in virtualnim na osnovi ne/obstoja komunikacije; kibernetski prostor je možen le s povezanostjo in izmenjavo. Trček (2003, 13) ga z minimalistično sintezo ostalih definicij opredeljuje kot »virtualno, omrežno, elektronsko posredovani interesni prostor, (ki služi kot)

prizorišče za zagotavljanje različnih formalnih in neformalnih interesnih nagnjenj (in) potreb[3] (...), ki poteka z interakcijo in transakcijo med akterji.«

Pri presoji, kakšen vpliv ima informacijsko komunikacijska tehnologija na družbo in kakšne so zaželjene oblike tega vpliva, so tako v ZDA kot v EU že na polovici 90-ih letih oblikovale razvojne strategije. Ob tem bomo iz njih povzeli 5 glavnih področij, ki so aktualna še danes in predstavljajo sečišča družbenega zanimanja: demokratična agenda za internet, civilne pravice v informacijski družbi, fleksibilnost, odprt javni sektor, ter digitalna trgovina in industrija (Babnik 2012, 21).

V preglednici 2.2 so povzete osnovne razlike med ZDA/Japonsko in Evropo na področju stopnje razvitosti in značilnosti informatične družbe[4] na prelomu tisočletja. Opazimo predvsem razlike, ki izvirajo iz homogenosti in konvergentnosti ameriškega/japonskega okolja in pluralnosti in divergentnosti evropskega okolja. Z okoljem je mišljen tako trg in njegova dinamika, pa tudi naravnanost vladnih politik.

Preglednica 2.2: Informatična družba – razlike med ZDA/Japonsko in Evropo

| | **ZDA/Japonska** | **Evropa** |
|---|---|---|
| **Vsebina** | Vsebina je nacionalno utemeljena.<br>Obstajajo velike, integrirane medijske skupine z ogromno investicijsko močjo za nove tehnologije.<br>Vsebine se večinoma prodajajo na enotnem velikem trgu. | Vsebine so nacionalne in multikulturne.<br>Majhni nacionalni producenti se morajo združevati, če želijo doseči velikost in finančno moč posameznega ameriškega producenta.<br>Vsebine se prodajajo na nacionalnih in vseevropskem trgu. |
| **Omrežja – infrastrukture** | Enotni niz standardov, ki se je razvijal v daljšem časovnem obdobju. Vseeno obstajajo problemi interoperabilnosti.<br>Večina tehnologij je domači produkt in razvoj je neposredni rezultat nacionalnih R&D | Veliki uspeh mobilne telefonije. Obstoj razl. standardov na številnih ravneh; številni zunanji dobavitelji in ponudniki so bolj povezljivi s standardi ZDA.<br>Pogosto obstajajo medsebojno tekmujoče tehnologije; razvoj je |

[3] Po Trčku so interesi so lahko racionalni, lahko pa tudi izključno emotivno ali performativno pogojeni.
[4] Trček (2003, 121) ugotavlja, da se informacijska (nacionalna) država/družba razvije v informatično družbo, sicer se pa »informatična družba« uporablja na področju sociologije, medtem ko je »informacijska družba« pojem splošnejše rabe.

| | | |
|---|---|---|
| | programov.<br>Dobra razporstranjenost osnovne infrastrukture (telefonija, kabelska TV, cenovno ugodna omrežja visokih hitrosti).<br>Navedene lastnosti veljajo v manjšem obsegu tudi za Japonsko. | posledica nacionalnih R&D iniciativ; razširjenost inovacij.<br>Razprostranjenost osnovnih infrastruktur z mednacionalnimi infrastrukturnimi in regulativnimi razlikami.<br>Razvita osnovna telefonija. |
| **Programska oprema** | V ZDA vladajo ogromni, agresivni oligopoli industrije programske opreme na kritičnih področjih osnovne programske opreme.<br>Na Japonskem je slabo razvita industrija programske opreme. | Obstoj specialističnih razvijalcev programske opreme in odličnih rešitev za specifične niše. |
| **»Človeški« dejavnik** | Uporabniki, posebno v poslovnem svetu in industriji, so tehnološko orientirani in informacijsko izobraženi, kar povečuje njihovo kompetitivnost.<br>Producenti informacij so seznanjeni in znajo uporabljati številne obstoječe tehnologije.<br>Zavedanje pomena informacijskih tehnologij in informacijske družbe postaja vseprisotno. | Zgodovinsko nižja stopnja informatizacije v poslovnem svetu, industriji, gospodinjstvih in v srednjih ter visokih šolah se hitro zmanjšuje.<br>Zamuda pri uvajanju novih informatičnih uslug je vzrok za nedoseganje primerljivih deležev z ZDA.<br>Naraščajoče zavedanje pomena informacijske družbe. |

Vir: Longhorn v Trček (2003, 103).

Nekateri (Bagon in drugi 2006, 113) razvoj informacijskih tehnologij zaradi intenzivnosti enačijo z industrijsko revolucijo. Vendar pa ta razvoj ob odsotnosti reguliranja (morda bi bil boljši izraz: usmerjanja) in civilno-družbenega nadzora vodi v smeri utrjevanja monopolističnih elit, najsi bodo to kapitalski interesi ali poskusi držav za maksimalizacijo nadzora (Trček 2003, 112).

Bežno se dotaknimo še prevladujočih družboslovnih razprav o vplivu tehnologije na družbo. Precej akademske pozornosti je bil deležen precep področij dela in tehnologije, zlasti o vplivu računalnikov na vzorce dela. **Tehnološki determinizem**

(Grint v Haralambos in Holborn 2001, 207) »meni, da se tehnologija razvija eksogeno in avtonomno, s čimer vsiljuje in določa družbene in gospodarske organizacije ter odnose.« Način organizacije dela naj bi tako bil določen s tehnologijo. Z **družbenim determinizmom** pa, nasprotno, zagovorniki pojasnjujejo razvitost in uporabo tehnologije na podlagi kulturnih in družbenih vidikov. V tem primeru pa naj bi bil način organizacije dela določen z načinom, kakor se ljudje odzivajo na določeno tehnologijo. Sodobne interpretacije računalniške tehnologije zagovarjajo teze, ki so nekje med tehnološkim in družbenim determinizmom.

Kling (v Haralambos in Holborn 2001, 213) ugotavlja, da »(v)časih računalniki spremenijo družbene odnose pri delu in v širši družbi, lahko pa tudi okrepijo obstoječe odnose ali pa imajo zanemarljiv učinek.« Še korak dlje v smeri družbenega determinizma pa storita Grint in Woolgar (v Haralambos in Holborn 2001, 214), ki trdita, da ima pri tehnoloških učinkih odločilno vlogo diskurz o tehnologiji. Pomembne so torej opredelitve in stališča ljudi, iz katerih je moč sklepati na družbeno razporeditev moči, kjer tehnologija nastopa kot orodje oz. eden od vzvodov moči. Pomen ali »zmožnosti« tehnologije so »različni in odvisni od občinstva, ki jo ocenjuje« (ibid., 215). Tako lahko neka tehnologija zadobi pozitivno ali negativno konotacijo.

Iz perspektive **družbenega konstruktivizma**[5] je izšla **kritična teorija o tehnologiji**, avtor katere je Andrew Feenberg. Teorija, ki se je kasneje razvila v pristop, poimenovan kar *kritični konstruktivizem*, naziva vprašanja o delovanju (agency), strukturi, neenakosti in dominaciji in širi jasno politično agendo – na kakšen način naj se tehnološki razvoj odraža v večji vključevalnosti (inkluzivnosti) in prepustnosti (ang. permeability) demokratičnih vrednot (Bakardijeva 2005, 15). Kritična teorija o tehnologiji sloni na predpostavki, da niti naravni zakoni niti tehnični principi ne določajo tehnologije kot take. Po Feenbergu je tehnologija eden od instrumentov, ki »omogočajo sistematsko dominacijo določenih družbenih skupin nad ostalimi« (ibid.). Na ta način tehnologija ne more biti nevtralna, saj vselej služi interesom nekaterih družbenih skupin. Vendar pa je tehnologija tudi *mikropolitična*, saj daje mesto in priložnost za politične proteste, ki jo imajo ob pomoči uporabnikov, strank in žrtev namen transformirati. V praksi navsezadnje ljudje ustvarjajo interpretacije

[5] Fokus družbenega konstruktivizma je znanje, ki ga v medsebojnih interakcijah člani izmenjujejo v okviru družbenih skupin (groups). Povedano drugače, družbene strukture in individualni akterji se sooblikujejo (Wendt, Onuf v Dolinar 2007).

tehnologije, ki se razlikujejo od sprva načrtovanih s strani njenih dizajnerjev (ibid., 19).

# 3 NADZOR IN ZASEBNOST

Pravica do zasebnosti je pravica posameznika pred posegi oblasti, gre za nekakšno (abstraktno) merilo svobode. V središču vprašanja o kršenju zasebnosti se skriva izpraševanje o bistvu moči in oblasti, ki je povezano z vsakokratno tehnologijo človeka. Tradicionalno pojmovanje moči[6] je temeljilo na informacijskem monopolu oblasti oz. nacionalne države (prim. Whittaker 2002, 124). Vendar pa država ni več edini uporabnik novih tehnik in tehnologij nadziranja. Njihova cenovna dostopnost in nizka delovna intenzivnost omogočajo splošno rabo (Whittaker 2002, 124; Hvala in Sedmak 2004, 93). Kovačič ugotavlja, da nadzor obstaja neodvisno od informacijske tehnologije, ravnotako pa velja, da je s pomočjo slednje postal učinkovitejši (Kovačič 2003, 26). »Ker (pa) je še vedno prevladujoča najvišja oblika v hierarhiji družbene regulacije nacionalno-teritorialna, je država s svojo administracijo tisti (monopolni) akter, ki vzpostavlja sisteme zbiranja, shranjevanja in obdelave informacij o svojih državljanih (in dogajanjih v drugih teritorialnih sistemih),« in tako potrjuje Giddensov pogled, da je težnja vsake države v maksimalizaciji nadzora (Trček 2003, 107). Za nadzor, ki ga omogočajo elektronske tehnologije (nadzora) je značilno, da so nevidne ali prikrite, nenamerne (niso vezane na natanko opredeljen cilj), so bolj kapitalsko kot delovno intenzivne, decentralizirane, posamezniki so pa obravnavani znotraj kategorij (Lyon v Kovačič 2003, 27). »Za tistega, ki opazuje, je značilna moč, tako kot je za tistega, ki je opazovan, značilna nemoč« (Mlinar 2006, 162).

V elektronskem prometu uporabnik tehnologije za seboj pušča »elektronske sledi« (Burnham v Kovačič 2003, 27), ki se običajno s pomočjo sistemov avtomatsko beležijo in shranjujejo. Zbiratelju informacij z uporabo informacijske tehnologije pa omogoča neprimerno hitrejšo obdelavo podatkov v primerjavi s preteklimi obdobji, predvsem pa njihovo povezovanje. V povezovanju podatkov je skrita tudi nevarnost, da pride do njihove zlorabe, ko jih imetniki uporabijo v namene, ki se razlikujejo od tistih, zaradi katerih so bili zbrani, ali pa da podatki preidejo v neprave roke.

Nadzor je imanenten vsaki družbi, trendi v smeri čedalje večjega obsega, nezaznavnosti, instrumentalizacije, neselektivnosti in preventivnosti pa prihajajo v nasprotje s človekovimi svoboščinami in pravicami. Ta moč mora v demokratičnih

[6] S tem se avtor nanaša na znani deli Georgea Orwella »1984« (iz l. 1949) in Aldousa Huxleya »Krasni novi svet« (iz l. 1958).

družbah biti podvržena učinkovitemu demokratičnemu nadzoru (Kovačič 2003, 30–31). Sodobnim nadzornim sistemom je lastno, da zaznavajo vse, kar odstopa, je odklonsko, neobičajno in nenormalno (Mlinar 2006, 161). Zato gre pričakovati, da bo prihodnost razvoja sistemov za nadzorovanje šla v smeri uporabe sistemov umetne inteligence, ki delujejo ob pomoči predvidevanja dogodkov oziroma ravnanj. Preventivna naravnanost umetne inteligence pa je v (očitnem) nasprotju z domnevo nedolžnosti in omogoča različne oblike diskriminacije na podlagi vnaprejšnjih ocen (Kovačič 2003, 28).

Potrošniki in državljani tako živimo v svetu, v katerem se moramo nujno odopovedati delu svoje zasebnosti na račun večje funkcionalnosti in obvladovanja kompleksnosti življenja v sodobni družbi (Kovačič 2003, 34). Ta sodobna družba se je po padcu realnega socializma na Slovenskem uveljavila »ne (kot) resnično svobodna družba, temveč liberalno demokratična družba z nekaterimi avtoritarnimi in neliberalnimi elementi« (Hvala in Sedmak 2004, 94).

Ob vse večjih težavah in problemih, ki so se pojavaljali ob nenadzorovanem vzponu informacijske tehnologije, je OZN, izhajajoč iz 12. člena[7] Splošne deklaracije človekovih pravic, v letu 1974 sprejela priporočilo, ki obsega tri načela: *načelo relevantnosti* (zbiranje le nujno potrebnih podatkov za dosego namena)*, načelo notifikacije* (predhodna seznanitev posameznikov, katerih podatki se uporabljajo) in *načelo privolitve* (zbiranje podatkov, za katere posamezniki dajo soglasje) (Kovačič 2003, 36). Glavna sestavina zaščite informacijske zasebnosti je torej *nadzor pretoka in posredovanja podatkov, ki se nanašajo na nekega posameznika* (Kovačič 2003, 37).

Pri poskusu iskanja odgovora na vprašanje, ali je kibernetski prostor nov prostor svobode ali nadzora in v kaktero smer naj se razvija, naletimo na dve konceptualni usmeritvi, ki sta si medsebojno nasprotujoči. Za nekatere avtorje (Boyle v Trček 2003, 121) je internet »tehnologija svobode«, ki mu zaradi hitrosti razvijanja in drugih dinamik (razpršenost uporabnikov, ateritorialnost, pluralnost vsebin ...) nacionalna država in kapitalski interesi težko postavljajo učinkovite regulativne okvire. Iz tega razloga se na strani starih centrov nadzora pojavlja imanentna težnja k ohranjanju »enake pozicije tudi v novem prostoru s pravno-formalno regulacijo in novimi pojavnimi oblikami nadzora« (Trček 2003, 121). K starim pojavnim oblikam, med katere sodijo vse dejavnosti in ukrepi za zagotavljanje varnosti oziroma, splošneje, uveljavljanja človekovih pravic, megakorporacije dodajajo nove pojavne oblike s

[7] Besedilo člena na 29. strani.

področja *avtorskih pravic*. Trček (2003, 122) sklene z ugotovitvijo, da tako internet kot kibernetski prostor nista ne »tehnologija svobode« ne novi panoptikum. Njuno družbeno vlogo pogojuje in določa (a)simetričnost razporeditve družbene moči. Tako so načrtovalci, uporabniki in lastnosti tehnologije tisti, ki določajo, ali bo posamična ali niz tehnoloških rešitev svobodo omogočal(a) ali jo preprečeval(a).

## *3.1 Težave pozitivnega nadzora*

Ko lahko po eni strani govorimo o potencialnih grožnjah, ki jih predstavlja možna i/legalna uporaba sistemov umetne inteligence v prihodnje, se po drugi strani lahko oblastni, *legalni* nadzor sooča s pojavom *dizintermediacije*. Wall (2001, 23) namreč ugotavlja, da na spletu funkcija posrednikov (zaposlovalne agencije, trgovine, finančna posredništva ...) med ljudmi in storitvami peša, zato slednji izginjajo. V pogojih spleta, kjer sta dimenziji časa in prostora v primerjavi z realnim povsem izvzeti, je uspešnost *pozitivnega* nadzora organov pregona kaj hitro lahko vprašljiva, možnosti kršiteljev pa neomejene.

Zoper ta nezaželjen pojav so se organizirali v različnih iniciativah (npr. britanski Internet Watch Fonudation in še nekatere druge) z namenom, da bi ob pomoči prijav internetnih uporabnikov omejevali ali onemogočili dostop do vsebin, ki so opredeljene kot nezakonite ali škodljive. Tovrstni *lokalni* poskusi pozitivnega nadzora so se ob odsotnosti globalne strategije za boj zoper sporne internetne vsebine izkazali za neučinkovite in v nekaterih sodnih postopkih tudi s škodljivimi posledicami za pravico do svobode govora (Wall 2001, 73–92).

Pozitivni nadzor pa je še dodatno omejen z dvema lastnostma. Vodenju policijskih preiskav in kazenskih pregonov je lastno, da potekata primarno na lokalni ravni in neodvisno. Poleg tega pa pri ukrepanju ne upoštevajo postopkov sprejemanja odločitev vseh oblastnih organov (Wall 2001, 25). Posledica prve lastnosti je, da je psihološki učinek na globalno delujoče kršitelje praktično minimalen; posledica druge, pa premalo narejenega bodisi v fazi preprečevanja kaznivih dejanj (npr. upoštevanja standardov in priporočil pri izdelavi izdelkov) ali njihovega preganjanja (npr. postopkovne zahteve zaradi razkritij kršitve odvračajo oškodovanca od prijave).

Morda največjo oviro pozitivnemu nadzoru predstavljata tajnost (podatkov; vsebine sporočil) in anonimnost (pošiljatelja). Z uporabo tehnologije kriptiranja podatkov in

tehnologij zakrivanja identitete, t. i. *spoofinga* (npr. alteracije URL naslova spletne strani, alteracije izpisa številke kličočega na stacionarne/GSM idr. telefone, alteracije e-poštnega naslova pošiljatelja ...) in hitrim prehajanjem med strežniki v različnih državah, ki so posledično podvrženi različnim pravnim ureditvam, je kršitelje izredno težko izslediti. Tehnično se zakrivanje identitete na spletu sliši kompleksno, a nam že obisk za to namenjenih spletnih strani (t. i. *re-mailerji*)[8] pokaže, kako malo truda je potrebno. Storilec za dostopanje do spletnih aplikacij preko običajnega internetnega brskalnika uporabi filter za anonimiziranje (omenjeni *re-mailer*) in njegov IP-naslov je praktično nemogoče izslediti, storilcu pa zagotovljenja popolna anonimnost. Taki pogoji gredo močno v prid krepitvi primerov ekonomsko motivirane kraje identitete (Wall 2001, 34–35).

Pozitivni nadzor pa izvajajo tudi državljani in druge civilno družbene organizacijske forme, kar pa s krepitvijo informatizacije in širjenjem nabora subjektov, ki operirajo z osebnimi podatki in drugimi občutljivimi informacijami od javnih, državnih organov na zasebne subjekte lahko predstavlja resne ovire in varnostna tveganja.

## *3.2 Anonimnost in nadzor*

Če je pozitivni nadzor v družbi zaželjen prav v namen zagotavljanja varnosti njenih članov, ima zanje po drugi strani omejujoče učinke, zlasti kadar je njegov obseg nesorazmeren glede na namen, ki ga ima. Protiutež takemu nesorazmernemu nadzoru predstavlja ustavno zagotovljena nedotakljivost človekove zasebnosti ter tajnost pisem in drugih občil[9], prav tako pa tudi svoboda govora. Anonimnost, ki jo zagotavlja nedotakljivost zasebnosti posameznika, slednjega ščiti pred možnimi negativnimi učinki družbene stigmatizacije in omogoča svobodno izražanje in polno uveljavljanje drugih (političnih) pravic.

Za boljše razumevanje je potrebno ločiti med pojmoma pravice do *zasebnosti*, ki zajema vse informacije, ki jih posameznik sme/more zadržati le zase (npr., zdravstveno stanje, spolna nagnjenja in verska prepričanja) in konceptom *anonimnosti*, ki je »pravica ne razkriti svoje identitete oblasti« v smislu svobode govora, anonimnega publiciranja, političnega ali civilnodružbenega udejstvovanja ... (Bailey 2004, 36).

[8] Recimo: www.anonymizer.com ali www.onlineanonymizer.com.
[9] Omenjeni pravici sta v slovenskem pravnem redu opredeljeni v 35. in 37. členu Ustave RS.

Svoj vsakdan si težko predstavljamo brez anonimnosti, hkrati pa je slednja »postala ena osrednjih šibkih točk odprte družbe« (ibid., 26). Anonimnost nosi v sebi pomemben družbeni potencial, saj opogumlja ljudi k družbeno koristnim ravnanjem (k prijavljanju kaznivih dejanj, darovanju biološkega materiala, objektivnosti znanstvenega raziskovanja, zaščiti virov v množičnih medijih ...). Obenem pa anonimnost omogoča tudi pogoje za varno okolje, v katerem se lahko posameznik sprosti (ibid., 28). V eni od sodb je Vrhovno sodišče ZDA pri obravnavi pravice do anonimnega govora odločilo, da slednji omogoča »izogibanje socialnemu ostrakizmu[10], preprečuje diskriminacijo, nadlegovanje in ščiti zasebnost«[11] (ibid., 29). V interpretaciji ustavnega reda so sodniki sklenili, da je pravica do anonimnih objav na internetu ali pa (političnih) objav pod nepravimi, izmišljenimi imeni nad pravico vedeti.

Anonimnost lahko hitro stopi v konflikt s ključno prvino družbenega reda – odgovornostjo. Anonimnost in odgovornost sta nekompatibilni, saj postane skušnjava za zlorabo anonimnosti nezadržna, v kolikor se lahko kršitelj izogne tveganju, da bi ga izsledili. Dober primer te nekompatibilnosti je ravno internet, kjer najdemo poleg pozitivnih vidikov anonimnosti (npr. anonimne prijave nepravilnosti) še celo vrsto negativnih: širjenje govoric, kriva obtoževanja, goljufivi zahtevki, neželena pošta (spam), širjenje sovraštva (sovražni govor), obrekovanje, kršitve avtorskih pravic, trgovanje z otroško pornografijo in nadlegovanje prek spleta (t. i. *stalking*) ... (ibid., 30–31).

Bailey (2004, 32–33) zato opredeljuje dva tipa anonimnosti, in sicer na podlagi sledljivosti oz. nesledljivosti. **Sledljiva anonimnost**, najobičajneje tedaj, ko se uporabniki poslužujejo psevdonimov, zagotavlja odgovornost. Na drugi strani pa kombinacija uporabe t. i. »remailerjev« v verigi in metod enkripcije pred sledljivost postavljajo kup tehničnih ovir, do izvornega pošiljatelja pa je zelo težko priti (t. i. **nesledljiva anonimnost**).

Nadzor države nad svojimi državljani v smislu zagotavljanja varnosti se je skozi zgodovino razvijal v odvisnosti od komunikacijskega medija; pomena nadzora nad državljani in prestrezanja komunikacij so se države hitro zavedale in zato tudi uvedle monopol nad sprva poštnimi, nato pa tudi telekomunikacijskimi službami. Vzporedno s tehnološkim napredkom so tudi apetiti države po nadzoru rasli, praviloma stran od

[10] Ostrakizem je bil postopek v atenski demokraciji, ko so državljani z ustrezno večino izgnali posameznika za dobo 10-ih let.
[11] Sodba Vrhovnega sodišča ZDA »ACLU of Georgia v. Miller« iz leta 1997.

oči javnosti in drugih mehanizmov demokratičnega civilnodružbenega nadzora. V tem oziru je zaradi ekscesov na relaciji med ZDA in Evropo (industrijsko vohunjenje Američanov na škodo evropskih podjetij, primer »Echelon«) prišlo (zgolj) do poskusov pravne ureditve razmerij (»International User Requirement« standard (IUR 1.0)). Podobno sta nadzor nad svojimi državljani uredili ZDA s programom »Carnivore« in Združeno Kraljestvo z »Regulation of Investigatory Powers Act« (t. i. RIP) (Whittaker 2002, 125). Kljub temu, da je z računalniško podprtim poslovanjem in delovanjem poenostavljen nadzor nad elektronskimi komunikacijami, to hkrati tudi pomeni, da je prav to na računalnike oprto delovanje istočasno resna ovira za totalni nadzor države (ibid., 127).

Z razvojem metod digitalne enkripcije je bila tudi ta, kot številne druge storitve, podvržena dezintermediaciji in izgubi državnega »monopola« nad tem področjem. Temu so sledili poskusi pravnega urejanja, ki so npr. v ZDA od dekriminalizacije (najprej so metode enkripcije prištevali med streliva) prešli k regulaciji (omejitev moči kodiranja ali pa uporaba t. i. metode »key escrow«[12], kjer vladne službe razpolagajo s kodirnim ključem). Pozornost ameriške izvršilne oblasti se je od poskusov prepovedi preusmerila k spremljanju spletnih strani, ki zagotavljajo programsko opremo za enkripcijo (Whittaker 2002, 127–8).

Sklenemo lahko, da kljub navidezni nasprotnosti v dihotomiji med anonimnostjo in identifikacijo, edinole slednja oblasti omogoča zagotavljanje varnosti svojim članom in je zato predpostavka vseh prednosti, ki jih omogoča prva. Brez identifikacije namreč ni mogoče obiskovati javne šole, koristiti državne podpore, dedovati, kandidirati in voliti (Bailey 2004, 37).

## *3.3 Mesto zasebnosti v okviru človekovih pravic in svoboščin*

Pravna ureditev področja zasebnosti posameznika sega na mednarodno področje (mednarodne konvencije in pogodbe), zlasti pa jo natančneje opredeljuje veljavni pravni red vsake države. Zato bomo najprej pogledali splošne delitve človekovih pravic in razmerja med posameznikom in državo, nato se pa dotaknili mednarodnih dokumentov in konkretne pravne ureditve v Republiki Sloveniji. Človekove pravice[13]

[12] Ameriški vladni organi so bili kasneje ta projekt primorani opustiti.

[13] Vsebovane so v Splošni deklaraciji o človekovih pravicah iz l. 1948 ter kasnejših dopolnitvah – Mednarodni pogodbi o državljanskih in političnih pravicah in pa Mednarodni pogodbi o gospodarskih,

opozarjajo na različne odnose med posamezniki in skupnostjo (državo) ter med posamezniki z vidika vrste in širine posameznikove svobode (Zajc 2005, 18). Zlasti od novoveške[14] politične misli dalje je posameznik temeljno oprijemališče pravic v družbi, zato je smiselno pogledati, kako se delijo človekove pravice v odnosu med posameznikom in državo. Cerar v Brezovšek in Črnčec (2007, 189) pri upoštevanju tega odnosa opredeljuje tri kategorije:

a) **pravice negativnega statusa**: ki zajemajo nabor pravic, v katere ne država ne kdo drug ne sme posegati, kot so naprimer svoboščine (svoboda vesti, veroizpovedi ...) in varstvo osebnih podatkov.

b) pravice pozitivnega statusa: pri katerih je država obvezana ravnati na način, da bo upoštevan posameznikov interes, npr. na področju osnovnega izobraževanja, zdravstvenega varstva.

c) pravice aktivnega statusa: ki omogočajo in zagotavljajo aktivno državljanstvo na področju javnega (upravljanje javnih zadev, volilna pravica ...).

Izhajajoč iz (mednarodnih) pravnih dokumentov, se lahko pravice delijo tudi na podlagi vsebine dobrin:

a) **osebne pravice in svoboščine**: ki zajemajo vse klasične človekove pravice, mednje pa sodi tudi pravica do zasebnosti;

b) politične pravice in svoboščine;

c) socialne in ekonomske pravice in svoboščine;

d) kulturne idr. pravice;

e) pravice narodnih oziroma etničnih skupin (Cerar v Brezovšek in Črnčec 2007, 189).

Brezovšek in Črnčec (2007, 190) v odnosu do državnega aparata človekove pravice delita na 4 kategorije:

a) ***individualne obrambne pravice***: zajemajo sfero svobode, kamor država ne sme posegati (varno življenje, svobodno ekonomsko, družbenopolitično delovanje, lastnina);

b) *individualne zahtevbene pravice – kombatibilne z obrambnimi*: so s področja materialne varnosti, politične enakosti in kulturnih možnosti (socialni

socialnih in kulturnih pravicah. Seveda pa posredno z odstopanji navzgor od »zajamčenih standardov« na način in obliko uveljavljanja in razvoj človekovih pravic vplivajo tudi posamezne države (npr. skandinavski model socialne države).

[14] V starem Rimu je bil *ius naturale* na zdravorazumskost vezan nabor pravic, oprt prav na posameznika.

transferi v primeru nezaposlenosti, pokojnine, brezplačno šolanje in zdravstvena zaščita);

c) *individualne zahtevbene pravice – nekompatibilne z obrambnimi*: so tiste, ki dajejo prednost kolektivu pred posameznikom (pravica do dela);

d) *kolektivne pravice*: določajo svobodo kolektiva in podrejenost posameznika in drugih kolektivov (pravica do samoodločbe).

Razvoj človekovih pravic je zgodovinsko potekal v treh fazah; v prvi so se konstituirale politične in civilne pravice, sledile so ekonomske in socialne pravice v drugi, da bi se lahko sklenile s tretjo fazo – informacijskimi in komunikacijskimi pravicami, ki so »neposredno povezane prav z vprašanji javnega dostopa do informacij in pravice do javnega komuniciranja, hkrati pa z rekonceptualizacijo zasebne sfere in pravice do zasebnosti« (Splichal v Brezovšek in Črnčec 2007, 193). Šinkovec (v Brezovšek in Črnčec 2007, 193) zatrjuje, da zato, ker velja, da je »človekovo dostojanstvo absolutna pravica, napad na to dobrino daje prizadetemu legitimacijo za obrambo proti vsakomur (državi, pravnim in naravnim osebam),« slednje dodatno priča o temeljnosti pravice varstva osebnosti. Brezovšek in Črnčec (2007, 209) izpostavljata tri pogoje, pod katerimi je možen poseg države v zasebnost posameznika: posameznikovo soglasje, zakonska podlaga in upoštevanje načela sorazmernosti. Nenazadnje pa je naloga države tudi, da posameznika ščiti pred nedovoljenimi posegi zasebnih subjektov z ustreznima nadzorom in pravno ureditvijo. K slednjemu jo obvezujejo tudi mednarodni pravni akti; **Splošna deklaracija človekovih pravic v 12. členu** določa takole: »Nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi« (Splošna deklaracija človekovih pravic 1948).

Zagotavljanje zasebnosti je v pogojih informacijske družbe postavljeno pred težke preizkušnje z uveljavljanjem »sodobnih sredstev prisluškovanja, (video)snemanja, navigacijskega sledenja in registriranja« (Brezovšek in Črnčec 2007, 194). Temu se danes v sferi javnega preprosto ne moremo izogniti, sodobna sredstva pa nezadržno pronicajo tudi v sfero zasebnega.

Čebulj v analizi konceptov zasebnosti zaznava tri sestavine (Čebulj v Brezovšek in Črnčec 2007, 194):

- **zasebnost v prostoru**, kadar se posameznik lahko povsem oddalji od ostalih (npr. zasebnost na delovnem mestu);
- **zasebnost osebnosti**, ki omogoča »svobodo misli, opredelitve in izražanja«;
- **informacijska zasebnost** pa dejansko zajema varstvo osebnih podatkov.

Najpogostejše pojmovanje zasebnosti obsega prvi dve sestavini, tretjo pa pušča ob strani. Trček (2003, 107) ugotavlja, da je tretja dimenzija zasebnosti, informacijska zasebnost, podlaga, s pomočjo katere država zagotavlja red in ščiti svoje državljane pred njimi samimi. Samo z relativno visoko stopnjo informacijskega nadzora lahko moderne kompleksne družbe delujejo racionalno in omogočajo (pravno) predvidljivost. Zaokrožimo lahko z navedbo Čebuljevega (v Trček 2003, 106) citata o zasebnosti, ki ima vselej »različno vsebino v različnih političnih ureditvah, na njeno opredelitev pa vpliva tudi časovni horizont.«

V **Ustavi Republike Slovenije** so te tri sestavine zasebnosti (po Čebulju) opredeljene v štirih členih, njihov namen pa je omejevanje vdorov v zasebnost. **35. člen** zagotavlja **nedotakljivost** človekove celovitosti, **zasebnosti** in osebnostnih pravic. **36. člen** govori o **nedotakljivosti stanovanja** in drugih tujih prostorov. **37. člen** jamči **tajnost pisem** in drugih občil. V **38. členu** Ustava zagotavlja **varstvo osebnih podatkov** in prepoveduje njihovo uporabo v nasprotju z namenom njihovega zbiranja.

Brezovšek in Črnčec (2007, 195) zatrjujeta, da v razmerah, ko si sodobne družbe brez informacijske tehnologije ne moremo več predstavljati, velja rek »kdor ima informacijo, ima moč.« Moč, ki jo najpogosteje pojmujemo kot grožnjo, izhaja iz tveganja, da najsi bo posameznik, skupina (organizirani kriminal) ali država z dostopom in povezovanjem ogromnih podatkovnih baz »spremlja posameznika (...) brez nadzora in mimo njegove vednosti« (ibid., 196). Zlasti je tvegano, če bi do tovrstnih povezovanj in združevanj podatkov prihajalo avtomatsko. Zato je učinkovito varstvo osebnih podatkov tako zelo pomembna prvina demokratičnih in pravno urejenih demokracij.

Varstvo osebnih podatkov obsega »zbiranje, obdelovanje in prenos osebnih podatkov« (ibid., 196) in terja, da ima posameznik vseskozi nadzor nad prometom podatkov, ki se nanj nanašajo. Kovačič (2008, 10) opredeljuje razmerje med zaščito in varstvom podatkov s tem, da se »(v)arstvo podatkov (...) nanaša na varovanje pomembnih podatkov, medtem ko se zaščita podatkov nanaša na pravice posameznika in zaščito njegovih osebnih podatkov. Zaščita in varstvo podatkov sta tako med seboj nerazdružljivo povezana.« Podobna je sinteza, kjer varstvo osebnih podatkov zadeva

integriteto posameznika in njegovo zasebnost, zaščita pa tehnični in organizacijski vidik (Brezovšek in Črnčec 2007, 196). Informacijski pooblaščenec glede veljavnega Zakona o varstvu osebnih podatkov[15] razlaga, da je »varstvo osebnih podatkov namenjeno preprečevanju nezakonitih in neupravičenih posegov v informacijsko zasebnost posameznika,« zakon pa hkrati določa, »da je na ozemlju Republike Slovenije vsakemu posamezniku, ne glede na državljanstvo in prebivališče,« ta pravica zagotovljena. V ospredju ni varovanje posameznikovih podatkov, ampak zaščita njegovih pravic (IP-RS 2013c; prim. Kovačič 2008, 10). Slednje je še toliko bolj pomembno, ker v medčloveških interakcijah veljata t. i. *dva zakona dostopnosti*. Zajemata »protislovne težnje, ko vsakdo poskuša uveljavljati prost dostop do (informacij o) drugih in hkrati povsem obvladovati dostop drugih do sebe bodisi na individualni bodisi na kolektivni ravni« (Mlinar 2006, 155).

V slovenskem prostoru se je v obdobju procesa privatizacije utrdila zavest o lastništvu in vrednosti dobrin (denarna sredstva, nepremičnine in premičnine, infrastruktura ...). Na področju intelektualne lastnine je tega zavedanja manj. Na področju vrednosti in lastništva informacij ga pa še ni (Bagon in drugi 2006, 112).

## *3.4 Zasebnost na internetu*

Internetu je lastno, da si njegovi uporabniki morajo sami zagotoviti ustrezno raven zaščite svoje zasebnosti. Internet je »odprt javni sistem, ki deluje po tehnično znanih protokolih in katerega tehnična in programska konstrukcija sta primerno usmerjeni v izmenjavo informacij« (Brezovšek in Črnčec 2007, 202). Kot smo že omenili, internetni uporabniki pri tej izmenjavi informacij za seboj puščajo »elektronske sledi« (Burnham v Kovačič 2003, 27), to pa ustvarja pogoje za nezakonito sledenje uporabnikom in prikrito zbiranje njihovih osebnih podatkov (Brezovšek in Črnčec 2007, 203). Klemenčič (v Brezovšek in Črnčec 2007, 203) v ta namen med sredstva za izboljšanje osnovne zaščite zasebnosti na internetu uvršča požarni zid, anonimne pošiljatelje elektronske pošte, programsko opremo za filtriranje elektronske pošte (t. i. *anti-spam filter*), programsko opremo za uničevanje piškotkov, kriptiranje elektronske pošte, posamičnih datotek ali računalniškega diska, digitalni podpis in digitalni certifikat.

[15] ZVOP-1-UPB1, Ur. l. št. 94/07

Z odmevnejšimi terorističnimi napadi v zadnjem desetletju se je vprašanje razmerja med posameznikovo varnostjo in zaščito zasebnosti (anonimnostjo) dotaknilo tudi interneta in njegovih storitev. Legitimna težnja vlad in njihovih obveščevalno-varnostnih služb nadzorovati vsebino elektronskih komunikacij odpira vrsto pravnih, pa tudi etičnih vprašanj. Zlasti kadar poteka nadzor elektronskih komunikacij celovito in sistematično s pomočjo ustrezne »vladne« programske opreme[16], nameščene neposredno na računalniške strežnike elektronske pošte, smo avtomatsko vsi podvrženi latentni obliki sistematičnega nadzora. Tovrstna ureditev je vprašljiva, saj posega v posameznikovo zasebnost in erodira domnevo nedolžnosti[17]. Problematična pa je tudi, če ni časovno in vsebinsko omejena (prim. Brezovšek in Črnčec 2007, 205).

[16] Tak vladni program ameriške vlade se je imenoval **Carnivore** (prim. Brezovšek in Črnčec 2007, 204) in je bil nadgrajen in preimenovan v **NarusInsight**, http://www.narus.com/.

[17] Za sodobni mešani obtožno-preiskovalni postopek je značilno, da se začne po uradni dolžnosti na pobudo javnega tožilca na podlagi **ocene verjetnosti**, da je bilo storjeno kaznivo dejanje (prim. Trifunović 2009, 11, poudarek moj).

# 4 KRIMINOGENOST KIBERNETSKEGA

Da bi znotraj zastavljenega raziskovalnega namena karseda omejili realne ovire, ki jih predstavlja plastičnost terminov in konceptov na področju kibernetskega, bomo v tem poglavju najprej navedli osnovne predpostavke in lastnosti znotraj abstraktnejšega (konceptualnega) okvirja kibernetskega polja.

## *4.1 Razločitev kibernetskega*

V najširšem smislu zajema pojem kibernetsko (ang. *cyber*) področje, ki je na kakršen koli način vezano na internet. Pogosto se kot sopomenki uporabljata tudi pojma *virtualno* in *elektronsko* (zlasti pogosta je predpona *e-*). Virtualno želi izpostaviti navideznost ali simulacijo, npr. virtualne resničnosti. S pojmom elektronsko pa poudarjamo predvsem tehnični oz. tehnološki vidik. Grabosky in Smith namesto elektronsko uporabljata pojem *digitalno* (v Wall 2001, 29). Prav tako moramo biti pozorni in kibernetskega ne zamenjevati s kibernetiko, področjem znanosti, ki zajema raziskovanje strukture različnih (socialnih) sistemov.

Kibernetskemu je lastno, da nima zgodovine, ne pozna spomina, pa tudi prihodnosti ne. Je globalna kultura, pa ne zato, ker bi predstavljalo unitarno svetovno kulturo, ali na svetovno državo vezano kulturo, temveč zato, ker je vseobsegajoče in neenako; je vključevalno in hkrati izključevalno; ni razdeljeno na osnovi državnih meja, časa ali prostora in na navedenem vezani identiteti, ampak na osnovi številnih različnih in neprestano se spreminjajočih fragmentarnih ravneh (Featherstone, Barker v Brown 2003, 166). Med kibernetskim in realnostjo ne moremo postaviti enačaja, prej lahko govorimo o tem, da je kibernetsko popačena zrcalna podoba realnega.

Številni nastanek kibernetskega povezujejo z razvojem obrambnega sistema ZDA, obdobjem hladne vojne, razvojem satelitarne tehnologije, tehnologije izmenjave podatkov in omrežij, pa tudi hitro rastočih potencialov na področju trgovanja in obrambe (Brown 2003, 166). Prav v vezanosti na »vojsko in državne interese ameriške dominacije« (Loader v Brown 2003, 167) naj bi tičal tudi razlog, zakaj prihaja na področju kibernetskega vseskozi do trenj z diskurzi zasebnosti in demokracije.

Nasprotno pa nekateri raziskovalci temeljne predpogoje za nastanek in razvoj kibernetskega iščejo prav v odprtosti in demokratičnosti, v svobodnem trgu, človekovih pravicah, svobodni izmenjavi idej in informacij in predstavniških oblasteh. Prav odprtost in svoboda omogočajo zlorabe in različne oblike nasilja. Še več, anonimnost, pomembna vrednota in pravica v postindustrijski, informacijski družbi, se lahko hitro spremeni v nevarno orožje (Bailey 2004, 4–5).

## *4.2 Kriminogenost kibernetskega*

V fizičnem svetu je anonimnost bistveni dejavnik, ki omogoča kriminalne dejavnosti (Bailey 2004, 33). Bailey (ibid.) dalje navaja ugotovitve Davida Brina, pri čemer storilce kaznivih dejanj ne motivirajo nizke kazni, temveč zanje ugodno razmerje tveganja, da bi bili ujeti. Vsekakor pa v splošnem velja, da sta predpogoj za zagrešitev kaznivih dejanj in blažjih prestopkov *želja in priložnost*. Anonimnost v tem oziru zelo pripomore k priložnostim, zlasti kadar zagotavlja zelo majhne možnosti izsleditve in sankcioniranja.

Tako so tudi prostori in mesta kibernetskega kriminogeni, ampak ne na način, kot so mesta[18] in fizično družbeno, kakor tudi ne fizično telo (Brown 2003, 145). In glede na to, da je prostor izpostavljenosti v kibernetskem veliko večji, so tudi možnosti, da v metropolitanskih oazah najdemo varna območja, toliko manjše. Prav tako ne izhaja, da je »virtualna« viktimizacija v svojih učinkih manj destruktivna. Prizadane več ljudi hkrati; možnosti prepoznavanja so zelo zmanjšane in temu primerno tudi možnosti pravnega urejanja; potencialni dobički nekaterih kriminalnih dejanj (goljufija, vdor v računalniški sistem itn.) so ogromni; in navsezadnje je možnost onesposobitve (javne) infrastrukture, ki temelji na virtualnem, povsem mogoča.

Nekateri raziskovalci prihajajo do zaključkov, da je z okrepitvijo področja kibernetskega prišlo ne le do pojava »novih« kriminalnih dejanj, temveč da so se povečala tudi stara (sabotaža, zalezovanje, rop itd.) (Brown 2003, 146; prim. Wall 2001, 29, 44–58, ki opozarja pred *prehitrimi* sklepanji o učinkih in obsegu kiberkriminala). Gledano širše na to vprašanje so učinki interneta na človeške dejavnosti treh vrst. Deloval naj bi bodisi kot medij za poenostavitev že obstoječih oblik kriminala bodisi naj bi ustvarjal nove priložnosti bodisi omogočil pojav povsem

[18] Brownova mesto pojmuje v materialnem, infrastrukturnem smislu, kjer se odvija družbeno in gibljejo »realna«, fizična telesa.

novih oblik. Wall (2001, 26) ugotavlja, da se vse od preloma tisočletja, po tem, ko se je zgodila nekakšna *demistifikacija* (npr. predimenzionirani »milenijski hrošč«) odvija proces, ko postaja razumevanje fenomena kibernetskega prostora in njegovega vpliva precej bolj realistično.

Na percepcijo tveganja oz. ogroženosti pred negativnimi učinki kibernetskega kriminala vpliva definiranje *dnevnega reda* tako s strani množičnih medijev (pogosto s histerijo in prenapihovanjem deviantnosti), kakor vplivnih interesnih skupin in strokovnih/političnih teles. Kakor ugotavlja Levi (v Wall 2001, 46) »mediji tako ustvarjajo kakor tudi odsevajo koncepcijo tehtnosti konstrukcij (kibernetskega) kriminala. Različne skupine[19] zagovarjajo partikularne koncepcije, ki služijo njihovim materialnim in simbolnim interesom.«

Nekateri avtorji, kot npr. Taylor (v Wall 2001, 71), hekerjem pripisujejo precejšnjo vlogo v smeri družbenih sprememb. S svojim početjem, ki je nemalokrat tudi družbeno in politično angažirano (»hektivistično«), kar so v svojem bistvu pozivi po neomejenem dostopanju do informacij in uporabi moči računalništva, spreminjajo ne samo internetno tehnološko kodo, ampak tudi abstraktnejšo kodo kapitalizma. Slednje se kaže zlasti z ogroženostjo komunikacijskih sistemov in elektronskega poslovanja, pa tudi v obliki formalnih odzivov in strategij vladnih in medvladnih teles. Ena od rešitev, kako povečati stopnjo zaupanja uporabnikov interneta (predvsem na področju e-trgovanja), je vsekakor razvoj regulativnega okvira za uporabo zanesljivih tehnologij enkripcije (Wall 2001, 76).

Pojav modernih globalno delujočih terorističnih skupin je v zadnjem času močno zaznamoval svetovni varnostni zemljevid in prinesel marsikatero spremembo. V tem smislu sta analitika Arquilla in Ronfeldt[20] boj zoper moderne teroristične skupine opredelila s terminom *netwar* (Research And Development Corporation; Bailey 2004, 15). Z njim mislimo na konflikte, ki bazirajo na pretoku informacij med narodi in družbami. Netwar je poskus vplivanja na način, kako določena populacija percepira sebe ali svoje okolje ob pomoči vnašanja motenj. Tarče teh bojev so javno mnenje ali mnenje družbenih elit, vključujejo lahko diplomacijo, propagandne in psihološke kampanje, politične in kulturne prevrate, zavajanje ali motenje delovanja množičnih medijev, vdiranje v računalniška omrežja in baze podatkov in agitacijo prek socialnih

[19] Tu mislimo predvsem na interesna profesionalna združenja, ki skrbijo za računalniško oz. informacijsko varnost.

[20] Ustanovitelja ameriške korporacije RAND, globalnega policy think tanka (Research And Development Corporation).

(računalniških) omrežij. Netwar predstavlja nov pristop v spektru konfliktov, ki presega tradicionalne gospodarske, politične, socialne, pa tudi vojaške oblike »vojne«. V nasprotju z gospodarskimi vojnami, ki imajo za cilj vplivati na raven proizvodnje in distribucije blaga in političnimi vojnami, ki imajo za cilj spremeniti politična vodstva in vladne institucije, se netwar spopadi osredotočajo na informacije in komunikacijo (Arquilla in Ronfeldt 1995).

Novi izzivi tako prihajajo s strani majhnih, geografsko razpršenih skupin, organiziranih v omrežjih brez jasne (hierarhične) linije odločanja. Posamični deli omrežja lahko delujejo povsem neodvisno od njegovega jedra na različnih lokacijah, pri tem pa se poslužujejo informacijske tehnologije (Arquilla in Ronfeldt 1995).

Kako velikim tveganjem so lahko podvržene razne skupnosti zelo dobro oriše Bailey, s tem, ko izpostavlja varnostna vprašanja pri zaprtih sistemih. Z njihovo pomočjo namreč upravljajo kritično elektronsko nadzorovano infrastrukturo (mostovi, železnice, vodovodne črpalke, naftovodi, plinovodi, jezovi, zapornice, hladilni sistemi jedrskih reaktorjev) in za mnoge velja, da niso bili načrtovani, da bi bili povezani v svetovni splet. Slednje predstavlja resno grožnjo javni varnosti ob morebitnemu hekerskemu/terorističnemu vdoru (Bailey 2004, 44). V letnem poročilu za 2013. Europolovi analitiki ugotavljajo, da je v zadnjih letih do tovrstnih napadov na »kritično nacionalno infrastrukturo« že prišlo. Pri tem pa dejanska škoda ni bila povzročena zaradi nezmožnosti hekerjev, temveč zato, ker to ni bil njihov namen (Europol 2013, 28).

## *4.3 Kibernetski kriminal*

Kibernetski kriminal zajema pojav škodljivih ravnanj, ki so vezana na računalnik. Zakonodaja se nanj specifično ne nanaša, kot koncept pa so ga izumili mediji (Wall 2001, 2, 44–57). Wall pri preučevanju vpliva interneta na kriminal opredeljuje tri ravni vpliva (*komunikacijsko sredstvo; oblikovanje transnacionalnega okolja* in*; ločitev časa in prostora*). Pri presoji kibernetskega kriminala Brownova (2003, 166) opozarja na neproblematičnost uporabe konvencionalnih (sočasnih) zakonskih kategorij, ki urejajo običajni kriminal. Iz zapletenosti odnosa med kibernetskim in utelešenim svetom izhaja, da je potrebno ta diskurz, ki sloni na tradicionalnih predstavah o telesu, identiteti, lastništvu in avtorskih pravicah *na novo teoretizirati*.

Breztelesnost virtualnih identitet in (istočasna) mnogoidentitetnost spreminjajo predstavo o subjektu, njegovih zmožnostih, storilcu in žrtvi. Neželjene pojave na področju kibernetskega v nasprotju s številnimi (neuspelimi) poskusi ni mogoče regulirati s pomočjo realne zakonodaje in drugih pravil, ker kibernetsko samo postavlja svoja pravila. Ta pravila pa so, ob odsotnosti nekakšnega centra moči in avtoritete, konsenzualne narave.

Za primerno kriminološko analizo kibernetskega kriminala je potrebno zavedanje o različnih stopnjah vpliva posameznih oblik kriminalnih dejanj na žrtve. Težave pri tem lahko predstavljajo različne ravni *vidnosti*, stopnja zavedanja žrtev, pogostost medijskega izpostavljanja in fluidnost definicij (Wall 2001, 11). Večina današnjega digitalnega kriminala je izven dosega organov pregona in regulatorjev. Razlogi za to tičijo v razpršenosti storilcev, potencialnosti žrtev in spremenljivosti/prilagodljivosti oblik kriminala. Varnost v kibernetskem okolju je zato pogojena s sodelovanjem številnih institucij in sposobnostjo samo-pomoči prizadetih (ibid., 29, 41). Pregon kaznivih dejanj, tehnološke in tržne rešitve ter mednarodno sodelovanje so soodvisni in od uigranosti njihovega medsebojnega sodelovanja bo v prihodnje odvisna tudi uspešnost pregona (ibid., 29).

Hkrati ni odveč zavedanje o pojavu splošne narave, kjer pri pridobitvah družbenega razvoja, kar različne tehnologije nedvomno so, poteka neprestani boj med izumitelji, avtorji, idejnimi očeti na eni strani in uporabniki na drugi strani (prim. Babnik 2012, 31). Ravnotežje moči se vseskozi vzpostavlja na novo in določa, ali gre v nekem primeru za »uzurpacijo« tehnologije ali pa za tehnologijo, ki v sebi nosi močan razvojni in demokratični potencial. Ta stopnja demokratičnega potenciala pa v zadnjih letih vse bolj kaže svojo realnejšo plat, ki vključuje tudi varnostne dogodke, v katerih igrajo vlogo hektivistične pobude in interesi posameznih držav (zlasti ZDA na eni in Kitajske na drugi strani) (TV Slovenija 2014). Torej, nedvomno tehnologija nosi določene posledice za družbeni ustroj in prinaša napredek, vendar je družba tista, ki določa način njene uporabe.

Od druge polovice 90. let 20. stoletja dalje deluje področju preprečevanja kibernetskih zlorab in snovanja policy ukrepov omrežje, v katerem formalizirano sodelujejo države skupine G8, Evropska Unija, Svet Evrope in OZN. Rezultati teh skupnih aktivnostih se kažejo predvsem v nekaterih dokumentih (npr. G8 iz leta 1997: *Principles and Action Plan to Combat Hi-Tech Crim*e; EU, 3. steber iz leta 1998: *10 prniciples on high-tech crime*), zlasti pa v medpovezanosti političnih dogodkov, odločevalcev in

strokovnjakov iz različnih forumov, oblikovanjem dnevnega reda ter izmenjavo in razširjanjem primerov dobrih praks (Wall 2001, 184–193).

## *4.4 Življenjski potek oblik internetnih zlorab*

Za nezaželjene oblike vedenja na internetu je moč pričakovati več različnih razvojnih ciklov (Lessig v Wall 2001, 179):

1. **Prenehanje popularnosti** – običajno zaradi »tržnih« ukrepov za preprečevanje določenih oblik zlorab;
2. **»Netiquette«** – uporabniki sami skladno s socialnimi normami poiščejo način za zagotavljanje reda;
3. **Prilagajanje »arhitekture«** – preventivni ukrepi (večja komunikacijska varnost, enkripcija, požarni zidovi idr. tehnologija) odvračajo kršitelje od zlorab;
4. **Nova zakonodaja in predpisi** – z natančnejšimi opredelitvami prestopkov prispeva k učinkovitejšemu pregonu in prilagoditvam »arhitekture«, »trga«, socialnih norm.

Kriminalno področje je dinamično okolje in »pregovorno« vsaj korak pred regulativnimi ukrepi. »Inovacije spreminjajo kriminal« (Wall 2001, 18). Zato ima uspešno napovedovanje bodočega razvoja e-kriminala ob upoštevanju inovacij pomembno vlogo pri omejevanju njegovih negativnih posledic. V tem oziru lahko na podlagi britanske študije Foresight Crime Panel (kljub njenim metodološkim omejitvam[21]) za potrebe pričujočega dela izpostavimo nekaj napovedi. Po mnenju raziskovalcev naj bi nove tehnologije »opolnomočile« posameznike (Levi v Wall (2001, 44) govori o »demokratizaciji priložnosti za kriminalna dejanja«) in jim povečale možnosti za zagrešitev kriminalnih dejanj. Nadalje, pričakovati je nacionalno omejene in nepremišljene institucionalne odzive pristojnih. Ker kaže, da bo nadzor nad premičnim premoženjem zaradi tehnološkega napredka čedalje boljši, se bo žarišče krminala premaknilo na ljudi. Dokazovanje identitete mora zato postati splošnejše in bolje artikulirano, ker se bodo kraje identitete kot sredstvo za

[21] Zajema le področje Velike Britanije na srednji rok, osredotoča se na spremembe, namesto na konstantnost zlorab (Wall 2001, 21).

okoriščanje in kot »kloaka« za nasilje in kazniva dejanja zoper spolno integriteto okrepile (Wall 2001, 22).

## *4.5 Je internet mogoče regulirati?*

Kljub temu, da ima kibernetski prostor svojo lastno dinamiko, je brez središča in formalizirnaih pravil, zanj velja nekakšen nenapisan kodeks etike njegovih uporabnikov; mogoče pa je tudi doseči določen obseg regulacije. Z načinom, kako regulirati internet, se je ukvarjal Lessig (v Wall 2001, 170), ki je opredelil štiri »načine omejitve«:

- **Zakonodaja** (definira ne/zaželjene oblike obnašanja);
- **Arhitektura** (s kodami in protokoli omogoča tako nove oblike zlorab kot tehnični nadzor);
- **Socialne norme** (ki jih uporabniki prenesejo/prilagodijo virtualnemu okolju) in;
- **Trg** (ustvarja in preprečuje priložnosti).

Rešitev za učinkovito reguliranje naj bi tako prej tičala v reguliranju arhitekture interneta s pomočjo zakonodaje, kakor v poskusih uporabe zakonodaje neposredno za reguliranje vedenja uporabnikov. Po klasifikacijah avtorjev se policy ukrepi za reguliranje in zagotavljanje reda v kiberprostoru uveljavljajo na **petih ravneh** (internetni uporabniki, ponudniki internetnih storitev (ISP), organizacije korporativne varnosti, javno financirane ne-javne varnostne organizacije in javno financirane javne varnostne organizacije (za podrobnejšo razčlembo glej Wall 2001, 170–177)), vključujoč njihove transnacionalne različice. Te ravni lahko opredelimo tudi kot »mesto«, kjer organi oblasti izvršujejo nadzor nad delovanjem in postavljajo pogoje uporabe tehnologije, vezane na internet. Zlasti za zadnjo raven, policijo, gre pričakovati, da bo v primerih zlorab identitete služila kot prvi naslov, kamor se bodo oškodovanci najprej obrnili. Odgovornost za pregon tovrstnih zlorab je pa v praksi porazdeljena med policijo in zasebni sektor. V praksi se to kaže tako, da npr. banke večino manjših zlorab obravnavajo same v okviru svojih (varovanih) protokolov. Le v primeru zlorab večjega obsega se v reševanje vključi tudi policija. Vsekakor pa največji izziv na tem področju predstavlja struktura odgovornosti; porazdelitev

odgovornosti med petimi ravnmi marsikdaj ni ustrezno definirana, zato prihaja na nižjih ravneh pogosto do odstopanj in zmotnih presoj pri obravnavanju zlorab (prim. Wall 2001, 178). Zaokrožimo lahko s sklepom, da navkljub mnenju nekaterih, da je za področje interneta značilna brezpravnost in odsotnost učinkovitih zakonskih omejitev in določil, velja prej nasprotno: internet je možno regulirati, prav tako obstoji nekakšna večnivojska struktura »policy« upravljanja.

## *4.6 Zagotavljanje varnosti in preprečevanje zlorab*

»Varnost obsega varovanje in zaščito vseh podatkov, še posebej pa poslovno občutljive, tajne, osebne in druge občutljive podatke ter informacijsko telekomunikacijska sredstva oziroma sisteme, ki so namenjeni obdelavi (oblikovanju, shranjevanju, spreminjanju, analiziranju, itd.) teh podatkov« (Bagon in drugi 2006, 112). Ker je današnje elektronsko (poslovno) okolje vse bolj konkurenčno, je vzporedno s tem tudi vrednost informacij večja, te pa so zato bolj ogrožene. »Z vse pogostejšo uporabo novih tehnologij pri zbiranju, prenosu in shranjevanju informacij so se pojavile tudi nove grožnje in s tem nova tveganja za razkritje, izgubo ali uničenje (pomembnih) informacij« (ibid.). Zato je področje računalniške varnosti naravnano preprečevalno oziroma defenzivno zoper poskuse tovrstnih zlorab. Da bi bilo zlorab (identitete ali sistemskih) čim manj, je na voljo čedalje več tehnoloških rešitev, tako za enkripcijo podatkov (pri pošiljanju podatkov ob kartičnem poslovanju itd.), kakor za prepoznavanje identitete (gesla, osebne identifikacijske številke (PIN), biometrične naprave (prepoznavanje glasu, prstnih blazinic, roženice) ...) ali nevtralizacijo virusov in druge zlonamerne programske opreme (Wall 2001, 36). Firbas (2009, 6) ugotavlja, da se soočamo z okoliščinami dveh ekstremov; na eni strani je neomejena pretočnost informacij in številne nove komunikacijske možnosti, na drugi strani pa krepitev internetnega kriminala in posledične potrebe po informacijski varnosti.

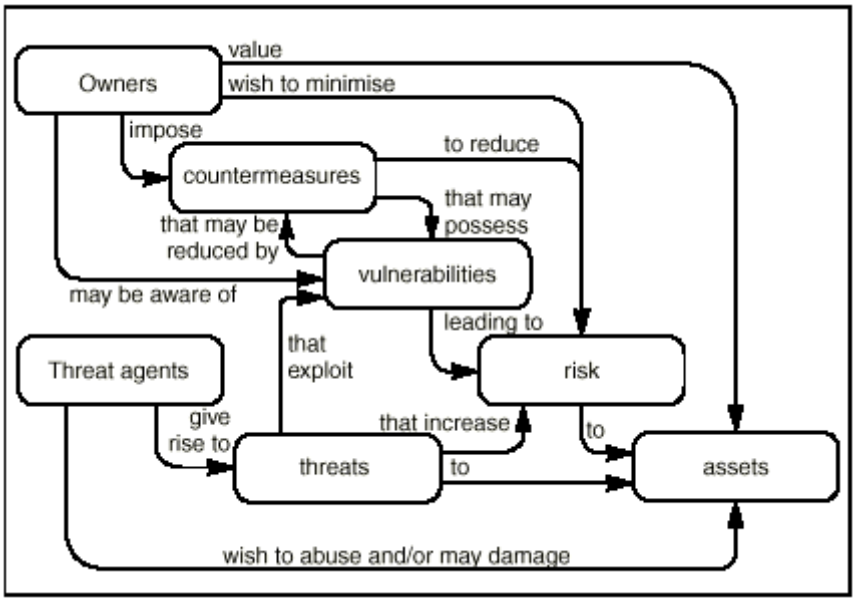
Nekateri pri tem (npr. Levi v Wall 2001, 44–45) kritično ugotavljajo, da so metode, ki se uporabljajo za preiskovanje elektronskih dejavnosti preprosto presajene iz vloge policije, kakršno je ta imela še v obdobju industrijske revolucije. Tipični interesi tako

policije kot akademikov ležijo izven dometa digitalnega kriminala, saj lahko policisti sklenejo svojo kariero, ne da bi o njem rabili vedeti kaj dosti[22].

Virtualno okolje, ki ga omogoča internet, je po mnenju nekaterih izredno urejeno, upoštevaje njegov velik obseg tako po številu vključenih posameznikov kot same gostote njihove vključenosti. Seveda pa najdemo tudi neurejena področja, zato v tej dihotomiji velja upoštevati, kdo ali kaj regulira vedenje uporabnikov interneta (glej Poglavje 4.5 Je internet mogoče regulirati).

Makro pogled na omrežje odnosov (glej Sliko 4.1) med »lastniki« (informacij) (*owners*) in »dejavniki tveganja« (*threats agents*) je koristen preventivni mehanizem tako za posameznika (če nekoliko karikiramo), kakor za organizacijo, ki pri svojem delu upravlja z bazami osebnih podatkov. S pomočjo evalvacije, ko se opredelijo najverjetnejša tveganja (*threats*) in določijo protiukrepi (*countermeasures*), je moč negativne učinke neželjenih posegov omejiti.

Slika 4.1: Dejavniki in odnosi v okolju zagotavljanja varnosti IT




Vir: Sanders (1999).

Vse več pa je tudi izzivov, s katerimi se v sodobni družbi soočajo organizacije (Bagon in drugi 2006, 113):

- Izguba in/ali zloraba informacij

[22] Tudi v okviru neformalnih razgovorov s pripadniki slovenske Policije se potrdi, da se s kibernetskim kriminalom ukvarjajo izključno specializirani oddelki.

- Nepooblaščeni dostopi do informacij
- Nerazpoložljivost/nedostopnost storitev in informacij
- Varno e-poslovanje in hranjenje dokumentov
- Usklajenost varnostnih politik med partnerji
- Zakonske obveze
- Motnje v poslovanju (izredni družbeni dogodki)
- Afere, tožbe, izguba dobrega imena, izguba zaupanja.

Varovanje podatkov delimo na organizacijski in tehnološki vidik, njun medsebojni preplet pa tvori sistem upravljanja varovanja informacij (ibid., 114–115). Med organizacijske ukrepe uvrščamo (ibid.):

- opredelitev in implementacijo načel varovanja v organizacijskih postopkih in pravilih;
- upravljanje sprememb v organizaciji;
- razmejitev odgovornosti in dolžnosti zadolženih za varovanje informacij;
- uvajanje nalog varovanja informacij v poslovne procese;
- krepitev varnostne kulture zaposlenih in;
- upravljanje z varnostnimi dogodki in incidenti.

Med tehnološke ukrepe pa uvrščamo (ibid.):

- požarne zidove;
- protivirusne zaščite;
- sisteme zaznavanja vdorov (IDS);
- sisteme za nadzor dostopa do sistemov in mrež;
- digitalna potrdila;
- uporabo varnostnih parametrov;
- varnostno kopiranje dokumentov (back-up);
- tehnično varovanje (alarmi, video nadzor, nadzor dostopanja, biometrija);
- tehnične rešitve za zagotavljanje razpoložljivosti sistemov (generatorji ob izpadu električne napetosti).

Za namene zagotavljanja varnega izvajanja nalog informacijskih sistemov, kar velja zlasti za hranjenje in posredovanje informacij, je OECD leta 2002 izdal dokument z

naslovom »Smernice za varnost informacijskih sistemov in omrežij: V smeri varnostne kulture.« »Med drugim je (dokument) poudaril, da zavedanje tveganj in razpoložljivih varnostnih orodij pomeni prvo obrambno črto za varnost informacijskih sistemov in omrežij. Priporočil je, naj vsi udeleženci redno preverjajo svojo varnostno politiko, navade, ukrepe in postopke ter ocenjujejo, ali so ustrezni glede na okolje, v katerem delujejo« (Sever 2012, 69). Pri taki izdelavi varnostne ocene pa bi morali upoštevati tako zunanje kot notranje dejavnike, med katerimi so tehnološke rešitve, človeški faktor, objektivne (fizične) okoliščine in sistem upravljanja varovanja informacij (t. i. varnostna politika) (ibid.).

Whittaker (2002, 122) povzema Powerjeve ugotovitve, da je premik iz tradicionalnih na spletne storitve imel za posledico poslabšanje varnosti, saj institucije in podjetja s težavo dohajajo razvoj informacijske tehnologije. Dodatno k temu prispevajo grožnje industrijskega vohunjenja, organiziranega kriminala in nezadovoljnih (nekdanjih) zaposlenih. K temu lahko dodamo tudi v zadnjem obdobju vse bolj perečo problematiko delovanja državnih varnostno obveščevalnih služb, ki je izvzeto demokratičnemu nadzoru.

## *4.7 Raziskave o obsegu kiberkriminala*

Na področju kiberkriminala opazimo, da je akademska pozornost in pozornost oblastnih organov glede tega vprašanja izrazito geografsko pogojena, saj prevladujoče raziskave, zlasti longitudinalne, povečini izhajajo iz ZDA. Kot bomo kasneje videli, naj bi po mnenju ameriških vladnih agencij razlog tičal v restriktivnejši zakonodajni ureditvi varstva osebnih podatkov, zato si ta problematika v Evropi ne zasluži tolikšne akademsko-raziskovalne pozornosti.

V poročilu generalnega državnega tožilca ZDA iz 1999. leta najdemo navedbe, da je naravo in obseg kiberzalezovanja težko kvantificirati, ugotavlja pa tudi, da ponudniki internetnih storitev (t. i. *ISP*) in organi pregona prejemajo več in več pritožb. Podobno je na prelomu tisočletja tudi Levi (v Wall 2001, 55) sklepal, da ni zanesljivih ocen o skupnih stroških posamičnih ali korporativnih žrtev. Za te ocene je bilo po njegovem sprva potrebno natančneje razdelati podtipe kibernetskega kriminala in ga šele nato analizirati kot širši del oziroma eno izmed oblik prevar. Nasprotno pa je britanski

NCIS[23] napovedal povečanje nadlegovanja preko e-pošte vzporedno s povečevanjem uporabe interneta (Wall 2001, 116).

Nadalje, Ameriški Computer Security Institute, profesionalna članska organizacija, ki v sodelovanju z ameriškim FBI letno izdaja poročila »Computer Crime and Security Survey« kot lahko zasledimo v Wall (2001) v študiji, narejeni 1998. leta ugotavlja, da se trditve strokovnjakov zasebnega sektorja o obsegu kiberkriminala bistveno razlikujejo od dejanskega stanja, tudi kar zadeva obseg stroškov. V kasnejši študiji iz leta 2000 so se povprečne letne izgube v raziskavo vključenih organizacij (velike korporacije, vladne agencije) po obsegu podvojile (Wall 2001, 53–54; Bailey 2004, 42). V raziskavi iz leta 2008 najdemo, da je bilo moč v daljšem obdobju zaznati konstantno upadanje izgub zaradi kiberkriminalnih dejanj, čemur je 2007. leta sledil znaten poskok, leta 2008 pa vnovični padec, kar je težko razložiti. Študija zaključuje z ugotovitvijo, da so napadi mnogo manj domiselni od zmožnosti, ki jih tehnologija ponuja (Richardson 2008, 1).

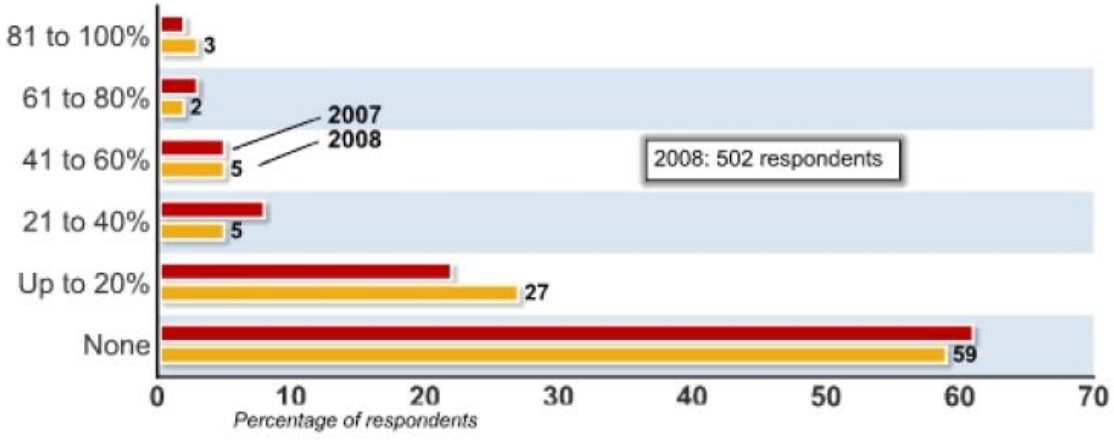
Europol v napovedovanju in policy priporočilih za leto 2013 (Europol 2013, 28) povzema ugotovitve raziskave Evropske Komisije, ki ugotovilja, da je 8% uporabnikov interneta v EU bilo žrtev kraje identitete, 12% pa žrtev drugih oblik spletnih zlorab. Obenem je pa z zlonamerno opremo (malware) prizadetih na milijone gospodinjstev, kakor tudi iz leta v leto raste obseg bančnih zlorab, vezanih na splet. Pomembna je tudi ugotovitev, da se v številnih članicah EU zabeleži le določen delež zlorab; po zatrjevanju nekaterih članic pa je zgolj 30% primerov (kraj identitete) prijavljenih organom kazenskega pregona.

Nezanemarljivo je tudi vprašanje, kako z obsežnimi bazami osebnih podatkov upravljajo organizacije iz zasebne in javne sfere, zlasti ker nekatere za to najemajo zunanje izvajalce. Zunanje izvajanje storitev informacijske varnosti v ZDA se v obdobju med leti 2006 in 2008 ohranja v približno enakih deležih (okoli 40 %), kar je ponazorjeno na Sliki 4.2. Podatek je pomemben zato, ker ima *obojestranske* implikacije. Na eni strani so organizacije, ki razpolagajo z večjim obsegom vsakovrstnih osebnih podatkov in same skrbijo za zagotavljanje njihovega varstva odvisne predvsem od ne/ustreznega obsega sredstev in ne/znanja svojih zaposlenih. Po drugi strani pa so podjetja, ki to storitev izvajajo profesionalno bolj specializirana, a hkrati tudi dovzetnejša za morebitne zlorabe s strani lastnih zaposlenih, s katerimi

[23] National Criminal Intelligence Service (Državna kriminalistično obveščevalna služba)

pride do konfliktov. Sklenili bi lahko, da odstotki (slabi dve tretjini) gredo v prid ohranjanju nadzora nad ukrepi zaščite v okviru lastnih organizacij.

Slika 4.2: Odstotek zunanjega izvajanja (»avtsorsanih«) storitev računalniške varnosti v ZDA




Vir: Richardson (2008, 12).

*Z Operacijo Aurora* označujemo več mesecev trajajoče hekerske napade leta 2009 na visokotehnološka podjetja iz ZDA. Napade, ki so izhajali iz Kitajske in za katerim naj bi stale tamkajšnje oblasti, so prvi javno priznali v Googlu v začetku 2010. Razlog zanje pa naj bi bil v tem, da Google ni želel uvesti zahtevane cenzure na svojih spletnih storitvah. Žrtve napadov so bila podjetja, kot npr. Adobe Systems, Yahoo, Symantec, Morgan Stanley ... »Cilji napadov naj bi bile shrambe programske kode podjetij, elektronska sporočila kitajskih oporečnikov in druge občutljive vrste informacij« (Sever 2012, 69). Še veliko hujši je bil razplet leta 2011 v primeru nizozemskega podjetja DigiNotar, ki je izdajalo varnostna potrdila. Posledica napada so bile zlorabe izdajanja varnostnih potrdil, ki so verižno rezultirale v težavah varnostnih potrdil ponudnikov spletnih storitev. Napadi, ki so predstavljali neposredno tveganje za uporabnike (v obliki pharminga, prestrezanja komunikacij), so bili v letu 2010 usmerjeni tudi nad VeriSign Inc, ki je izdajatelj varnostnih potrdil več kot 50% svetovnih spletnih strani, a je bila javnost o njih seznanjena šele 2 leti zatem. Tovrstni napadi, ki naj bi jih bilo po mnenju direktorja ameriške Nacionalne varnostne agencije (NSA) »nemogoče napovedati in se pred njimi zaščititi« (ibid.), naj bi

predstavljali neposredno grožnjo temeljem tehnologije, ki danes omogoča varnost komunikacije v spletu.

## *4.8 Oblike kibernetskega kriminala*

Wall je pri preučevanju vpliva interneta na kriminal izluščil štiri tipe ravnanj: (1.) »kiber**prestopke**« ali hekanje/krekanje; (2.) kibernetsko zavajanje/**kraje**; (3.) **opolzkosti**; in (4.) **nasilje** (Wall in drugi 2001, 2). Spekter prestopkov, vezanih na poseg v posameznikovo zasebnost je ne glede na motiv, zelo širok. V nadaljevanju bomo povzeli nekatere delitve pomembnejših oblik digitalnega kriminala.

Ena od delitev, kakor sta jo naredila Grabosky in Smith (v Wall 2001, 30–34), oblike digitalnega kriminala člení, kakor sledi:

- **Kraja telekomunikacijskih storitev**; namen katerih so brezplačne storitve (pogovori, prenos podatkov ...), izvajanje nezakonitih poslov, v zadnjem času pa tudi plačevanje različnih storitev s pomočjo mobilnikov.
- **Komunikacija kot podpora kaznivim dejavnostim**; so z novimi tehnologijami in metodami enkripcije še otežile delo organom pregona.
- **Informacijsko piratstvo/ponarejanje**; tiskovin, grafičnih podob, zvoka in večpredstavnostnih kombinacij se pojavlja bodisi za lastno rabo bodisi za prodajo po nižji ceni ali zastonjsko razdeljevanje.
- **Širjenje žaljivih vsebin**; zajema seksualno eksplicitne materiale, rasistično propagando in druge oblike sovražnega govora, kakor tudi navodila za izdelavo nevarnih naprav (t. i. *bomb-talk*). V to skupino uvrščata tudi nadlegovanje, grožnje in vsiljive komunikacije (t. i. s*talking*).
- **Digitalno izsiljevanje**; ki ga izvajajo posamezniki ali dobro organizirane skupine, se lahko pojavlja tako, da je internet medij za izvajanje nasilja ali razkritje občutljivih informacij ali pa tako, da postane tehnologija »žrtev« (vdiranje v strežnike, onemogočanje delovanja spletnih strani ...). Lahko pa internetna komunikacija (npr. ob e-plačilu) služi zaščiti izsiljevalca pred fizičnim soočenjem. Navsezdnje, informacije o posamezniku, ki jih izsiljevalec poišče ob pomoči iskalnikov in programske opreme, služijo kot dodatna pomoč pri zlorabah (prim. Deflem in Hudak 2008).

- **Elektronsko pranje denarja in davčne utaje**; s prenašanjem denarja med različnimi računi v različnih jurisdikcijah zelo otežuje nadzor centralnih bank in davčnih uradov. V ta namen so se tudi izoblikovali struktura neformalnih bančnih institucij in vzporedni bančni sistemi, zlasti na področju Azije.
- **Elektronski vandalizem in terorizem**; ki bi prizadel komunikacijske sisteme v informacijski dobi, lahko povzroči množično škodo. Uradne spletne strani držav in mednarodnih organizacij so pogosta tarča hekerskih napadov, veliko večje tveganje pa predstavlja informacijsko vojevanje, v okviru katerega lahko hekerji onesposobijo informacijsko tehnologijo, ki služi infrastrukturi obrambnih sistemov.
- **Elektronske zlorabe prodaje in naložb**; se dogajajo tako, da kršitelji z dezinformacijami in zavajanjem prepričujejo ljudi k vlaganju denarja v goljufive investicijske sheme, v navidez dobrodelne namene, za goljufivo prodajo.
- **Nezakonito prestrezanje digitalnih informacij**; je ob pomoči iznajdljivosti in tehnologije relativno enostavno (npr. z beleženjem GSM številk se klonira SIM kartice mobilnih telefonov in z njimi opravlja klice, plačuje storitve).
- **Nezakoniti elektronski prenos sredstev**; je možen v primeru prestrezanja podatkov in preusmeritve transakcij sredstev neznano kam. Pravtako so možne različne zlorabe pametnih kartic (*smart cards*), super pametnih kartic (*super smart cards*), optičnih spominskih kartic in zaobhajanje sistemov varnega dostopa.

Za pričujoče delo je funkcionalna tudi delitev kiberkriminala na 5 ravni, kakršno je uporabila Brownova (2003, 147–169).

**1. Spam**: Stivale (v Brown 2003, 146) neželena (ang. *spam*) sporočila opredeljuje kot nepotreben pretok podatkov, ki ga nekdo ustvari zato, da polni vrstice prejemnikovega zaslona ali pa posreduje agresivna sporočila. Pošiljanje neželenih sporočil zato zajema pošiljanje praznih besed posamezniku ali masovno, razumemo ga pa kot spletno nadlegovanje. Odvija se lahko posredno, denimo preko elektronske pošte, ali neposredno, v spletnih klepetalnicah. Po nekaterih ocenah obsegajo neželena sporočila skoraj 40 % vsega elektronskega poštnega prometa (Bailey 2004, 44). Neželena sporočila ne predstavljajo zgolj nadlegovanje internetnih uporabnikov,

temveč po nepotrebnem obremenjujejo strežnike oziroma pretočnost omrežij, hkrati so pa tudi medij, s pomočjo katerega prihaja do (poskusov) prevar.

Posebno vprašanje postavlja pojav mnogoterih virtualnih identitet, kjer v okviru MUD[24] aplikacij komunikacija poteka na povsem drugačnih ravneh. Ne le, da lahko uporabniki prosto zavzamejo katero koli identiteto, tudi v tehničnem smislu so pod vprašajem sama *dejanja*. V kibernetskem jeziku imajo pojmi, kot so »reči«, tj. govoriti neposredno, »izraziti čutenje«, tj. ob pomoči tekstovnih znakov, ali »šepetati«, tj. zasebno komunicirati s prejemnikom povsem drugačen pomen kot sicer. Zato je tudi veliko težje govoriti o nadlegovanju, kadar sta tako nadlegovalec in nadlegovani zgolj virtualna.

Predvsem pa ga je težko opredeliti; kdo je žrtev, kakšna je resnost samih dejanj in kakšen naj bo način reguliranja kibernetskega vedenja. Ito (v Brown 2003, 148) prihaja do sklepa, da je virtualna identiteta uporabnika MUD aplikacije nekakšen podaljšek njegove realne identitete, zato bi moral imeti tudi (virtualni) umor[25] drugega uporabnika drugačne posledice kot denimo pokončanje nasprotnika v spletnih igrah.

Sankcioniranje kršitelja je možno samo tako, da se mu onemogoči uporabo aplikacij; kar pa je zaradi možnosti ustvarjanja novih likov in številnih poti dostopanja do aplikacij nemogoče doseči. Onemogočeni uporabnik bo enostavno z uporabo drugačnega IP naslova dalje dostopal do spletnih mest oz. aplikacij. Prav ločenost virtualnega subjekta od njegovega fizičnega telesa dovoljuje širjenje zlorab (Brown 2003, 149). Na tak način nadlegovalci z uporabo breztelesnih identitet vršijo dominacijo in nasilje na simbolni ravni.

V zadnjih nekaj letih se trend neželenih sporočil iz pretežno nežaljivega oglaševanja premaknil v potencialno škodljiva sporočila, ki lahko prejemnika zavedejo in vodijo v zlorabo identitete. Sodoben spam širi zlonamerno programsko opremo ali uporabnike preusmerja na okužene spletne strani, na katerih se na uporabnikov računalnik namestijo škodljivi programi (OECD 2009, 26).

**2. Zalezovanje/*(S)talking***: O zalezovanju (ang. *stalking*) govorimo, ko posameznik iz določenega razloga (npr. razhajanja v mnenjih, konflikta, zavrnitve ...) svoji žrtvi pošilja neželjena sporočila, grožnje, ali privzame njeno identiteto in, denimo na internetnem forumu, pod njenim imenom objavlja besedila, fotografije, ali tudi kontaktne in druge osebne podatke. Pa tudi če do objave ali posredovanja osebnih

[24] MUD oz. (ang.) Multi-user dungeon so večuporabniške spletne strani, kjer udeleženci komunicirajo ob uporabi specifičnega jezika (Brown 2003, 147).

[25] Ang. »*P'king*«, onesposobitev uporabnika.

podatkov ne pride, je žrtev kljub vsemu deležna psiholoških posledic. Kršitelj s svojim čustvenim in simbolnim nasiljem žrtvi prizadeja povsem iste občutke, kakršnih so deležne tudi »nevirtualne« žrtve zalezovanja: strah, tesnoba, sram, jeza, ponižanje ... (Wall 2001, 6; Brown 2003, 150). Če je zalezovanje kršitev zoper posameznika, predstavlja virtualni sovražni govor kršitev zoper družbene ali etnične skupine (Wall 2001, 7).

**3. Kibernetsko zavajanje/kraje**: Ta segment zlorab zajema različne tipe goljufivih pridobitev na področju kibernetskega, ki gredo od tradicionalnejših oblik kraje, kot je zloraba kreditnih kartic in predplačniških dobroimetij, do racij spletnih bančnih računov.

**4.** Četrta izmed ravni je **(kibernetsko) piratstvo**, s čimer je mišljeno prilaščanje novih oblik intelektualne lastnine (podobe, glasba, blagovne znamke ...). To lahko poteka bodisi v obliki *ponarejanja*, kar velja predvsem za materialne proizvode, bodisi kot kiber-piratstvo/kraje. Največja bojazen lastnika tako predstavlja razvodenitev nadzora nad njegovo intelektualno lastnino.

**5. Hekerstvo**: Brownova ga opredeljuje kot mnogoslojno: sabotaža, vdor, vrinjenje, kraja, goljufija. Če se hekerstvo danes pojmuje v okvirih kontrakultur (Ross v Brown 2003, 158), je imelo v začetnih fazah razvoja interneta tudi legitimne obrise (prim. Wall 2001, 3, 59–62). Brownova dodaja, da je hekerstvo moč pojmovati še veliko širše; kot vsakršno početje, ki tehnologijo uporablja za namene, za katere sprva ni bila načrtovana. Predvsem pa hekerstvo zajema več funkcij, med katerimi so poleg že omenjene subverzivne, performativne in etične, še ekspresivna ter estetska, ki skupaj sestavljajo nekakšno kulturno politiko hekerstva. Podobno navaja tudi Taylorja, ki pravtako med osrednje motive hekerstva izpostavlja občutke odvisnosti, radovednost in pa užitek moči (2003, 158–160). Taylor (v Brown, 2003, 169) pa ugotavlja, da je najmanjši skupni imenovalec hekerstva intelektualni podvig. Ta pa za razliko od dejanskega vdora posegov v osebni fizični prostor ne zajema.

### 4.8.1 Podrobneje o hekerstvu

Za našo obravnavo je pojav hekerstva pomemben zato, ker je del in/ali sopomenka splošnejšega razumevanja računalniškega oz. kibernetskega okolja. Hekanje obsega širok nabor aktivnosti. Pojem »shekan« (ang. hacked) so prvi uporabili na kembriškem Massachusetts Institute of Technology (MIT) in izhaja s področja vlakov,

kjer so entuziasti na njih in na železniški infrastrukturi uvajali take modifikacije, da so omogočale hitrejše potovanje. Kmalu zatem se je hekanje asociiralo s »phreakingom«, tj. vdorom in nepooblaščeno uporabo telefonskih omrežij (Whittaker 2002, 120). V 80. letih 20. stoletja se je ta dejavnost preselila na računalnike.

Hekerji so po Levyu (v Whittaker 2002, 121) »tehnični strokovnjaki, ki želijo razumeti sisteme in programsko opremo karseda poglobljeno.« Zato lahko ločimo dve vrsti hekanja, legalno in potencialno ilegalno. Pogosteje in v splošnejšem smislu se hekanje opredeljuje kot sposobnost vstopiti (vdreti) in uporabiti kateri koli sistem. Wall (2001, 4; prim. ibid., 35) kibernetske prestopnike deli na načelne prestopnike (hekerje) in prestopnike brez načel (krekerje).

Zato poleg hekerjev, ločimo tudi:

- **krekerje (»crackers«)**, ki svoje spretnosti in znanja uporabljajo za dekodiranje šifer za enkripcijo;
- **»script kiddies«**, ki za dostop do računalniških omrežij uporabljajo že obstoječe pripomočke in skripte. Slednji so izmed vseh najpogostejši in najnevarnejši;
- **»warez pirates«**, ki trgujejo z nelgalnimi izvodi avtorsko zaščitenih proizvodov (Whittaker 2002, 121; Kovačič 2003, 40).

Po ugotovitvah Jordana in Taylorja (v Wall, 2001, 59) je hekerstvo podvrženo splošni in uspešni medijski demonizaciji (prim. McIntosh 2002). Navkljub obstoju **hekerske etike** in **hektivizma** (glej Wall 2001, 60; Whittaker 2002, 121), prevladuje negativno moralno vrednotenje, ki ga spodbujajo nekatere družbene skupine, zlasti industrija za zagotavljanje računalniške varnosti. Eno od razumevanj pojma hekerske etike je težnja po pridobivanju strokovnega tehničnega znanja in izkušenj. Nekoliko širše razumevanje zajema tudi pojmovanja, da so oz. morajo biti vse informacije brezplačne in splošno dostopne. So pa tudi razumevanja hekerske etike, ki upoštevajo, da ima hekanje pomembno vlogo pri odkrivanju varnostnih tveganj in tudi uvajanju inovacij. Hektivizem pa po drugi strani uporablja tehnološke spretnosti in znanja za doseganje družbenih in političnih sprememb (Wall 2001, 60), kar se je pokazalo zlasti v letu 2011 s skupino Anonymus (TV Slovenija 2014). Žgoče politične in strokovne polemike o aktualnem dogajanju v zvezi z razkrivanjem delovanja varnostno obveščevalnih služb nekaterih držav (zlasti ZDA, Velike Britanije, Kanade, Avstralije, Nove Zelandije, Nemčije in nenazadnje Kitajske) in forenzične

informatične preiskave nakazujejo na obstoj razvite mreže tajnih služb »krekerjev«, ki v imenu države vojujejo nekakšno kibernetsko hladno vojno; ta bi se naj zlasti odvijala med ZDA in Kitajsko (prim. TV Slovenija 2014).

### 4.8.2 Kibernetske grožnje

Ena od klasifikacij (Dokl 2006, 25–54) naravo groženj v kibernetskem okolju deli na tri tipe na osnovi kriterija namenskosti:

- Namerne grožnje
- Nenamerne grožnje
- Fizične grožnje

Za zadnji dve obliki velja, da negativne posledice, ki nastanejo zaradi groženj, niso namenske, vnaprej načrtovane ali nelegalne. Nenamerne grožnje predstavljajo varnostne luknje v programski opremi (npr. operacijskih sistemov idr. aplikacij) ali mehanske napake na strojni opremi (odpoved delovanja spominskih enot). Poleg motenj v delovanju pa lahko tudi uporabnik sam, bodisi zaradi nepoučenosti bodisi malomarnosti, s ponesrečeno kombinacijo programskih nastavitev omogoči različne oblike zlorab (izključitev požarnega zidu, nedelujoči protivirusni program, šibka kakovost varnosti gesel, nenameščanje varnostnih posodobitev programske opreme, nalaganje tvegane programske opreme ...). Tretja oblika – fizične grožnje, zajema pojave, kot so motnje in izpadi v delovanju električnega omrežja in pa vpliv naravnih pojavov (poplave, požari ipd.).

Pri naši obravnavi so najzanimivejše namerne grožnje, ki so tudi po obsegu in oblikah najbolj bogate. Dokl (2006, 25–57) jih je kakovostno in poglobljeno povzel v več podtipov:

- Zlonamerna programska oprema (trojanski konji; virusi[26]; črvi; logične-časovne bombe; zajci; bakterije; vohunski programi; oglaševalski programi) (glej & prim. Slika 4.3)

[26] Virusi, škodljive datoteke s funkcijo samomnoženja, so pozornost javnosti prvič pritegnili leta 1988, ko je študent univerze Cornell iz ZDA sprogramiral in »spustil« v omrežje črva, ki je v kratkem času okužil nekaj tisoč računalnikov. Kot zanimivost lahko omenimo, da je bil ta študent Robert T. Morris ml. sin glavnega strokovnjaka za varnost na ameriški National Security Agency (Whittaker 2002, 123).

Slika 4.3: Zlonamerna programska oprema po tipih v letu 2012

| Malware Infections by Type | % of malware samples |
|---|---|
| Trojans | 77.93% |
| Viruses | 7.48% |
| Worms | 5.89% |
| Rogueware | 3.98% |
| Other | 4.72% |

Vir: Anti-Phishing Working Group (2013, 8).

Na več milijonskem vzorcu napadov je več kot tri četrt vseh okužb programske opreme v obliki trojanskih konjev, ki jih žrtev naloži na okuženi spletni strani, zlasti zaradi ranljivosti Jave in Adobea (Anti-Phishing Working Group 2013, 8).

- Prevare in sleparije (kraja identitete; poneverba elektronske pošte, poneverba internetnih strani)
- Lovljenje gesel
- Elektronsko vohljanje
- Zasipanje z neželeno pošto
- Nepooblaščene spremembe in vdori

Posameznik kot družbeno bitje od vedno teži k temu, da drugim karseda omeji dostop do svojih osebnih in drugih občutljivih podatkov, istočasno pa si zagotovi dostop do čim širšega obsega informacij o drugih (t. i. dva zakona dostopnosti). V kibernetskem okolju je ta dihotomija med šifriranjem in dešifriranjem podatkov zaradi povsem drugačnega pojmovanja časovno-prostorske komponente toliko bolj izrazita. Za pričujoče delo je iz omenjene dihotomije zlasti pomemben vidik dešifriranja osebnih podatkov, pri čemer kot uporabniki oziroma člani kibernetskega okolja nosimo tveganje, da nam napadalci osebne podatke ali protipravno pridobijo ali nam jih poskusijo uničiti (prim. Firbas 2009, 23).
Firbas (2009, 23–29) ločuje med osnovnimi in naprednimi tehnikami za pridobivanje osebnih podatkov. Razlika med skupinama tehnik je v ne/avtomatiziranosti; osnovne tehnike delujejo povsem samodejno in samostojno, medtem ko je pri naprednih tehnikah, ki so tudi kompleksnejše, potrebna napadalčeva intervencija. Natančneje delitev tehnik zlorab obravnavamo v poglavju 5.11 Tehnike zlorab.

Namen delovanja opisanih oblik in ravni digitalnega kriminala ter navedenih podtipov namernih groženj je seveda več. Pomembno mesto imajo seveda finančne koristi posameznikov oziroma skupin organiziranega kriminala, ki pri izvajanju raznih oblik zlorab izkoriščajo prednosti anonimnosti in virtualnega okolja, kjer so pogoji identifikacije drugačni. V tehničnem smislu je namen groženj, zlasti zlonamerne programske opreme, se širiti in množiti ter pri tem z oddaljenim pristopom upravljati, ovirati ali povsem onemogočiti delovanje računalnikov in strežnikov, tako da spreminjajo ali uničujejo datoteke, prilagajajo parametre delovanja strojne opreme (kar ima za posledico tudi okvaro) ipd. Z beleženjem uporabniških navad lahko neželena oprema pošilja podatke, ki prejemniku bodisi služijo za nezakonito ciljno oglaševanje, ali pa prestreza osebna gesla, številke bančnih kartic in druge občutljive osebne informacije z namenom njihove zlorabe. Lahko pa gre tudi samo za sicer sporen, a neškodljiv hekerjev intelektualni izziv (prim. Dokl 2006, 27).

# 5 KRAJA IDENTITETE

Kako problematičen in težak prestopek je prevara, je že v srednjem veku prikazal Dante Alighieri (glej odlomek v uvodu), ko je v Božanski komediji prevarante[27] uvrstil na dno predzadnjega, IX. kroga pekla.

Kraja in zloraba identitete v najširšem smislu pomenita nedovoljeno prevzemanje identitete nekoga drugega. Kraja identitete je definirana kot uporaba osebnih podatkov oz. idenitete nekoga drugega (imena, datuma rojstva, obstoječega in nekdanjih naslovov) za pridobitev neke koristi, običajno ekonomske narave, ali inkriminacijo druge osebe (Fraud Prevention Expert Group; IP-RS 2012b, 5; United States Department of Justice 2013). »Škodljive posledice tega kaznivega dejanja namreč ne obsegajo zgolj pridobitve premoženjske koristi, ampak tudi druge koristi (na primer vstop v določene prostore)« (IP-RS 2007b, 4). Zloraba identitete se uporablja tudi kot sopomenka za krajo identitete; temeljna razlika med pojmoma pa je v tem, da zloraba identitete zajema tudi uporabo lažne, namišljene identitete (Fraud Prevention Expert Group).

> *Kraja identitete torej ni samo zloraba določenega osebnega podatka, saj je vedno povezana vsaj z* ***namenom****, da storilec pridobi določeno korist. Posebej pomembno je, da pri tem ne gre samo za izgubo denarja in premoženja, ker se posledice tega dejanja kažejo tudi kot* ***poseg v druge osebnostne pravice****. Prav tako ne gre le za pravico do varstva osebnih podatkov, ampak tudi za druge pravice zasebnosti, denimo varstvo tajnosti pisem in drugih občil – 37. čl. Ustave RS* (IP-RS 2007b, 4, poudarki moji).

OECD krajo identitete opredeljuje kot medsektorski pojav, za katerega je značilno, da ima širok vpliv in krši tako predpise o varstvu potrošnikov kot varnost, zasebnost in pravila glede neželene pošte (2009, 3). Standardne opredelitve kraje identitete na mednarodni ravni ni, naj bo to zloraba »identitete v spletu« (t. i. online identity) ali

[27] Epski junak Gianni Schicchi, zviti florentinski duhovitež, na prigovarjanje svojcev pravkar umrlega zelo premožnega aristokrata Buosa Donatija, ki želijo preprečiti, da bi vse premoženje šlo samostanskim bratom, »ponaredi sebe v podobo drugega« (v dobesednem prevodu), tako da prevzame identiteto umrlega in pod pretvezo, da je še živ, pred ostalimi dediči spremeni oporoko. Pri tem pa pretenta tudi svojce in kot dediča določi sebe.

»nepovezane identitete« (t. i. offline identity). Posledica različnih ureditev tega pravnega področja je različno preprečevanje, preganjanje in sankcioniranje (ibid., 15). Kraja identitete kot pojav ni enkratno dejanje, temveč se odvija oziroma razvija kot zaporedje dejanj. To je tudi razlog, zaradi katerega se uporabljajo različne pravne opredelitve kraje identitete, ki so lahko obravnavane kot specifična oblika kriminala, civilnopravni prestopek ali pripravljalno dejanje za druge oblike kriminalnih dejanj (glej poglavje 5.1 Kraja identitete, zloraba identitete in kriminal s področja identitete) (ibid., 16).

Povzamimo poskus OECD-jeve (ibid., 16) »globalne« oziroma **splošne** definicije kraje identitete s poudarkom na potrošniku, ki pravi, da »(d)o kraje idenitete pride, kadar stranka pridobi, posreduje, poseduje ali uporablja osebne podatke fizične ali pravne osebe na nepooblaščen način, z namenom storitve ali v povezavi s prevaro (fraud) ali drugimi kriminalnimi dejanji.«

Obenem pa OECD deli krajo identitete na **konvencionalno** in **moderno**. Pri prvi obliki so prevladujoče tehnike zlorab »brskanje po smeteh«, odtujitev plačilnih kartic, »zavajanje«[28], oprezanje[29], skimming[30] ali kraja osebnega računalnika. Pri moderni kraji identitete je v ospredju nameščanje zlonamerne programske opreme in phishing.

Do zlorab identitete je seveda prihajalo tudi preden je sodobna družba sploh postala informacijska. Tehnološki napredek in postopne spremembe družbenih institucij so sčasoma zagotovile zadostne pogoje, da so se pojavile različne oblike (»novega«) digitalnega kriminala, s pomočjo katerih je objektivnih (z)možnosti in priložnosti za zlorabe identitete več. Tovrstne digitalne zlorabe so moderen fenomen, ki se je najprej pojavil na območju ZDA in Kanade (Fraud Prevention Expert Group) in se razširil. Bailey zatrjuje, da je kombinacija anonimnosti in zlorabe identitete kršitve s področja kiberkriminala poenostavila (2004, 42). Podobno beremo v poročilu OECD, v katerem ugotavljajo, da se s pojavom interneta in elektronskega poslovanja kraja identitete kaže na »povsem novi ravni« (OECD 2009, 7), hkrati pa izražajo zaskrbljenost, ali med državami raznolike pravne ureditve vprašanja kraje identitete

[28] Zavajanje ali *pretexting/ pretext calling* zajema pridobivanje osebnih podatkov o drugih s posredovanjem zavajajočih navedb, zlasti po telefonu.

[29] Oprezanje ali tudi *shoulder surfing*, do katerega najpogosteje prihaja na javnih mestih z velikimi množicami ljudi, zlasti na javnem prevozu.

[30] S *skimming* tehniko se najpogosteje srečujemo pri poslovanju z bankomati, kamor zlikovci nelegalno namestijo dodaten čitalec na režo, kamor vstavimo kartico in kamero oz. dodatno tipkovnico, ki se prilega originalni, vse pridobljene podatke (magnetni zapis in PIN/CSC kodo) pa posnamejo s kamero ali brezžično posredujejo in z njihovo pomočjo naredijo dvojnik plačilne kartice (prim. OECD 2009, 31).

omogočajo implementacijo zadostnih ukrepov (ibid., 47). Do zaključka, da ukradene identitete omogočajo široko paleto organiziranih prevar, tako tistih *spletnih* kot tistih *nepovezanih*, prihajajo prav tako tudi v Europolu (Europol 2013, 17). Hkrati pa izpostavljajo, da so sodobni dokumenti za identifikacijo čedalje **bolje zaščiteni** (npr. biometrični potni listi) pred spreminjanjem in ponarejanjem, zato je zaznati vse več povpraševanja po specializiranih storitvah ponarejanja.

Vsekakor pa je na fenomen kraje identitete potrebno primarno gledati kot na poseg v posameznikovo *varnost*. V veliki večini primerov je namreč vdor v zasebnost posameznika zgolj stranski učinek kaznivega dejanja. »Cilj tatov identitete ni, da bi zlorabili zasebnost kogarkoli,« temveč le, da z uporabo posameznikove identitete dostopajo do njegovega denarja in se izognejo odgovornosti za svoja dejanja (Bailey 2004, 49–50).

Poudariti je potrebno, da so danes storilci s področja zlorabe identitete v veliki meri profesionalci, ki delujejo v okviru organiziranih kriminalnih združb. Njihovi napadi so vnaprej načrtovani, narejeni po meri[31], sufisticirani, ciljno usmerjeni in zato bolj nevarni. Na spletu je moč (proti plačilu) dobiti tudi programske komplete za spletno ribarjenje, ki omogočajo tudi manj veščim posameznikom, da se poskusijo in izurijo v spletnih zlorabah (OECD 2009, 27–28).

## *5.1 Kraja identitete, zloraba identitete in kriminal s področja identitete*

Na področju kraje identitete je v uporabi več različnih pojmov. Uporabljana terminologija je pogojena zlasti geografsko, kulturno, pravno in/ali jezikovno. Znotraj EU se kot sinonima najpogosteje uporabljata pojma zloraba identitete in kriminal s področja identitete; nasprotno pa v ZDA, ZK, Kanadi in Koreji prevladuje pojem kraja identitete (OECD 2009, 49).

Skladno s pojmovanjem Europola kakor tudi Organizacije združenih narodov sta kraja identitete in zloraba identitete obliki kriminala s področja identitete (»ID crime«), hkrati pa je kraja identitete oblika zlorab identitete. »Zloraba identitete je širša od kraje identete, ker se nanaša na zlorabo katere koli identite, naj bo realne ali

[31] Denimo s »spear-phishing« tehniko (podrobneje glej poglavje o socialnem inženiringu) se storilec pretvarja za sodelavca izbrane žrtve in pod pretvezo pridobi osebne ali druge občutljive poslovne podatke.

izmišljene; pri čemer je pa kraja identitete omejena s krajo identitete resnične osebe« (Europol 2006, 18; prim. OECD 2009, 49).

Za večino ljudi povsem učinkovitega načina zaščite preprosto ni, zatrjuje Bailey (2004, 40). Na drugi strani je pa mehanizmov zlorabe namreč kar veliko: od nepooblaščene uporabe številke socialnega zavarovanja (velja za ZDA; *Social security number*), bančnega ali drugih finančnih računov (investicije v sklade, delnice, druge vrednostne papirje ipd.), številke kreditne kartice, GSM telefona oz. pametne kartice telefona do drugih podatkov, s katerimi se je mogoče identificirati (United States Department of Justice 2013). Z ukradeno identiteto zlikovci zagrešijo tudi različne oblike drugih kriminalnih dejanj. Posledice prizadeti posamezniki zato odpravljajo še dolgo zatem, ko so vnovič pridobili nadzor nad uporabo svojih osebnih podatkov. Nanje ne pade zgolj breme finančne izgube zaradi nepooblaščenega dostopa do bančnega računa ali podobnih malverzacij, temveč tudi nezanemarljivi finančni stroški za popravo svojega ugleda in izbris napačnih informacij iz svoje »kartoteke« o kreditni sposobnosti (United States Department of Justice 2013). Ameriški potrošnik, žrtev zlorabe, sproži postopek pri Zvezni komisiji za trgovino (FTC), kjer oblikujejo poročilo, ki se ga lahko razširi v opozorilo (*fraud alert*) državnim organom in organom finančnih institucij. Prav tako je priporočljivo, da (ameriški) potrošnik sproži postopek pri eni od treh agencij za poročanje o kreditnih sposobnostih (t. i. *Credit Reporting Agencies*: Experian, Equitax in TransUnion) in uvede 90-dnevno »začetno opozorilo pred zlorabami« (t. i. *initial fraud alert*), ki se ga v primeru dejanske zlorabe nadgradi v 7-letno opozorilo pred zlorabami. Pri tem morajo finančne institucije za odprtje vsakega novega računa ali kakršno koli drugo obliko poslovanja preveriti identiteto njenega imetnika. Dodatno lahko potrošniki brezplačno zahtevajo poročilo o kreditni sposobnosti (*credit report free copy*), kjer preverijo vso svoje poslovanje in transakcije (OECD 2009, 40). Ocenjujejo, da žrtve zlorabe iz Združenega Kraljestva za povrnitev svojega ugleda v povprečju porabijo med 3 in 48 urami, vsekakor manj kot žrtve iz ZDA (Fraud Prevention Expert Group 2007b, 9–10), ki po nekaterih podatkih v povprečju potrebujejo kar 178 ur (Bailey 2004, 41).

Virov za vršenje zlorab (baz) osebnih podatkov je mnogo; krivci so lahko zaposleni na poštnih vložiščih, letališčih, v prenočitvenih kapacitetah, kadrovskih službah, finančnih družbah ali vladnih službah. Najdemo jih lahko med tistimi, ki so v poslovnem odnosu ali neformalno sodelujejo s podjetji, ki proizvajajo/prodajajo

opremo za kodiranje pri kartičnem poslovanju. Včasih pa tatovi identitet namenoma iščejo delovna mesta, ki jim zagotavlja dostop do finančnih podatkov, ali pa podkupijo tam zaposlene, da jim jih zagotovijo (U.S. Postal inspection service 2013).
Razvoj tehnik zlorab in odzivanje okolja nanje ima za posledico, da je za današnje napade značilno, da medsebojno kombinirajo različne tehnike (npr. socialni inženiring in neželeno programsko opremo) in niso več množični, temveč ciljno usmerjeni (OECD 2009, 21–22). Kljub temu, da države uveljavljajo različne ukrepe z namenom omejiti negativne vplive kraje identitete (kampanje za ozaveščanje potrošnikov in uporabnikov spleta, novi zakonski okviri, javno-zasebna partnerstva, pobude pod vodstvom industrije na področju ukrepov tehničnega varovanja ...), so namen, obseg in učinki kraje identitete različni od države do države (OECD 2009, 7).

## *5.2 »Online« ali »offline«?*

Spričo dejstva, da reprezentativne[32] statistične analize povečini ne razlikujejo med spletno (online) in nepovezano (offline) krajo identitete, je težko izvesti veljaven zaključek, katera od oblik je prevladujoča in/ali ima za žrtev hujše posledice (OECD 2009, 39).
V ameriški longitudinalni raziskavi Javelin Strategy and Research ID theft[33] iz leta 2006 (ibid., 39–40) so prišli do sklepa, da je »online« zlorab identitete zgolj 10%, preostalih 90% se odvija po konvencionalnih nekibernetskih poteh. Po njihovih ugotovitvah, četudi je poskusov zlorab na internetu sicer več, je devet od desetih poskusov obsojenih na neuspeh.
V povzetku poročila Javelin Strategy and Research Report iz leta 2012 lahko izpostavimo štiri poudarke (Business Wire 2013):

- V primerjavi z letom poprej se je absolutno število zlorab povečalo, prav tako tudi višina odtujenih stredstev;
- Pri avtomatsko generiranih opozorilih o zlorabah podatkov se v enem primeru od štirih razvije v zlorabo identitete, zlasti kadar je med podatki tudi SSN;

[32] O metodoloških in drugih omejitvah posameznih raziskav je v tem delu govora na več mestih.
[33] Javelin Strategy and Research ID theft raziskavo so oz. še financirajo podjetja, kot so FISERV (globalni ponudnik finančnih storitev za banke), INTERSECTIONS INC. (vodilno severnoameriško podjetje za storitve kriznega menedžmenta s področja identitete), WELLS FARGO (po velikosti 4. največja ameriška banka), VISA (ameriška multinacionalka s področja finančnih storitev), zato je s temu primerno distanco potrebno interpretirati ugotovitve. Letna poročila o stanju in trendih so na voljo le proti plačilu 3.000 $.

- Zaznati je trend skrajševanja trajanja zlorab, od 95 dni l. 2010, 55 dni l. 2011 na 48 dni l. 2012, k čemur naj bi prispevali izboljšani odzivi na strani potrošnikov in ponudnikov. Več kot polovica žrtev zlorabe identitete je koristila za to namenjene mehanizme za odpravo posledic.
- Žrtve zlorab spremenijo svoje potrošniške navade in se izogibajo zlasti manjših trgovcev na drobno.

Dodatno varnostno tveganje predstavljajo spletna družbena omrežja (Facebook, Twitter, Linkedin ...) iz treh potencialnih razlogov; kot prvi je vprašljivo zagotavljanje zadostnih ukrepov za zagotavljanje varnosti uporabnikov, kot drugi je to nepremišljenost uporabnikov pri objavljanju občutljivih, ažurnih in točnih poslovnih ali intimnih informacij in kot tretji je realna priložnost za (nedovoljeno) zbiranje osebnih podatkov za profiliranje uporabnikov. Četudi je varnostna politika spletnih družbenih omrežij ustrezna, lahko vtičniki neodvisnih izdelovalcev (t. i. »third party plug-in«) v dobro izdelani infrastrukturi omogočajo stranska vrata, skozi katera je moč izvajati kršitve. Zato vsakršna varnostna pomanjkljivost v sistemih spletnih družbenih omrežij in drugih spletnih zbirkah osebnih podatkov predstavlja resno grožnjo za odtujitev in posledično krajo identitete (prim. Firbas 2009, 33–34). K temu moramo prišteti še konvergenco informacijsko komunikacijskih tehnologij, ki rezultira v centralizaciji in močno olajša tako nadzor kot zlorabe zasebnosti (ibid., 39). Iz teh izsledkov ne moremo nedvoumno sklepati o razmerju med spletno in nepovezano krajo identitete, vendar ob upoštevanju vse pogostejšega koriščenja vsakovrstnih storitev preko spleta v globalnem smislu in porastu števila zlorab, je zaključek (stališče), da imajo spletne zlorabe blažje posledice od nepovezanih, vprašljiv. Zlasti ne izvemo dovolj podrobnosti o argumentih zanj. Tej skepsi in nelogičnosti pritrjujejo v številnih drugih raziskavah (prim. OECD 2009, 40), pri čemer ima resnost problemov neposreden inhibitoren učinek na spletno elektronsko poslovanje. Brez težav lahko sklenemo, da je spletna kraja identitete po učinkih in posledicah najmanj izenačena z nepovezano obliko kraje identitete. Navsezadnje se nabor možnosti za zlorabe z vse hitrejšim kreiranjem novih proizvodov in storitev, novimi pristopi k poslovanju ter tržnimi in naložbenimi priložnostmi (prim. Bučar v Babnik 2012, 33) le še povečuje.

## *5.3 Pravni vidiki digitalnih zlorab s poudarkom na kraji identitete*

Ena od posledic globalizacije in obstoja informacijske družbe je globalni domet kibernetskega kriminala, pri obravnavi katerega sta ključni točki, *kje* se je zgodil (zakonodaja katere države se uporablja za njegov pregon) in pa *pridobivanje dokaznih sredstev z lociranjem* kršitelja. Prvo pomembno oviro v postopku predstavljajo zakonodajna pravila, ki so teritorialno osnovana in tudi omejena; njihova kakovost in uspešnost ima omejen domet že v primeru, ko obravnava »domače« kršitve. Kadar pa so se kršitve zgodile v pravnih redih večih držav in so v postopek reševanja vključeni različni organi pregona, stroški (v času, kadrovskih, finančnih in drugih virih) pregona zlorab zelo narastejo in imajo za posledico to, da se preganjajo le prestopki zadostnega (največjega) obsega. Ker (med državami) v mednarodni skupnosti ne obstoji dovolj soglasja o vzpostavitvi eksteritorialne pristojnosti za pregon digitalnih zlorab, večjih pozitivnih premikov tudi v prihodnje ni pričakovati. Podobno so tudi izročitve oseb zaradi pregona obratno sorazmerne s kulturnimi in ideološkimi razlikami med strankami (državami) v postopku (Wall 2001, 38).

Učinkovitejše in koordinirano spopadanje s področjem zlorabe identitete na med- in naddržavni ravni ostaja problematično zlasti zaradi razlik v načinu pravnega urejanja tega področja v posamičnih državah (OECD 2009, 47). Zaradi tega je tudi odzivanje držav in gospodarstva na ta globalni fenomen temu primerno parcialno in omejeno.

Mednarodno primerjalno gledano države na tri različne načine pravno obravnavajo pojav kraje identitete:

a) kot samostojno kaznivo dejanje (Slovenija, ZDA, Kanada);
b) kot sestavni del drugih družbenih prestopkov, ki jih urejajo razna pravna področja (nepooblaščeno dostopanje do podatkov, goljufije, ponaredbe, pravice intelektualne lastnine ...) (ZK);
c) kot olajševalni dejavnik za hujše kategorije kaznivih dejanj (ibid.).

Prehajanje tradicionalnih oblik kraje identitete v okolje virtualnega (in zlasti na področje elektronskega poslovanja) obstoječe načine pravnega urejanja postavljajo pod vprašaj (ibid.), predvsem pa je vprašljivo, ali ti pravni okviri zadoščajo. Še več, »(v) poplavi novih zakonov, standardov in priporočil na področju informacijske industrije, varnosti podatkov, zaščite intelektualne pravice, upravljanja z IT dejavnostjo in kakovostjo poslovanja, je že spremljanje objav slednjih, kaj šele implementacija, prava umetnost« (Bagon in drugi 2006, 119).

V slovenskem pravnem redu področje informacijske varnosti ureja kar nekaj predpisov, zato bomo navedli tiste ali pretežni del tistih, ki vsebujejo določbe s področja varnosti; ti so (prim. Bagon in drugi 2006, 118):

- Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP)
- Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje
- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA)
- Zakon o varstvu osebnih podatkov (ZVOP-1)
- Zakon o splošnem upravnem postopku (ZUP)
- Uredba o upravnem poslovanju
- Zakon o davčnem postopku (ZDavP-2)
- Zakon o elektronskih komunikacijah (ZEKom-1)
- Zakon o varovanju tajnih podatkov (ZTP)
- Uredba o varovanju tajnih podatkov
- Slovenski računovodski standardi (SRS)
- Kazenski zakonik RS itd.

## *5.5 Kategorije kaznivih dejanj, povezane s krajo identitete*

Morda prvo zapisano krajo identitete v zgodovini najdemo v svetopisemski Stari zavezi, kjer drugorojenec Jakob po materinem prigovarjanju od svojega umirajočega očeta Izaka z zvijačo doseže blagoslov za vodenje judovskega ljudstva, do katerega je sicer bil upravičen njegov starejši brat Ezav (Sv. Pismo 2013):

> *(11) Jakob je rekel materi Rebeki: »Glej, moj brat Ezav je kosmat človek, jaz pa sem gladek. (12) Morda me oče potipa (...).« (15) Nato je Rebeka vzela najboljšo obleko svojega starejšega sina Ezava, ki jo je imela pri sebi v hiši, in jo nadela svojemu mlajšemu sinu Jakobu. (16) Koži kozličkov pa mu je ovila okoli rok in okoli gladkega vratu. (17) In dala je okusno jed in kruh, ki ga je pripravila, v roke svojemu sinu Jakobu.*

V slovenskem pravnem redu področje kraje identitete inkriminira **četrti odstavek 143. člena Kazenskega zakonika RS**, ki pravi: »kdor prevzame identiteto druge osebe ali z obdelavo njenih osebnih podatkov izkorišča njene pravice, si na njen račun pridobiva premoženjsko ali nepremoženjsko korist ali prizadene njeno osebno

dostojanstvo, se kaznuje z zaporom od treh mesecev do treh let« (Kazenski zakonik (KZ-1-UPB2)). Pred tem je slovenska zakonodaja za nedovoljeno smatrala kot »zgolj tisto uporabo osebnih podatkov, ki je v nasprotju z zakonom oziroma osebno privolitvijo posameznika, zato je usklajena z določbo 16. čl. Zakona o varstvu osebnih podatkov (...), po kateri se osebni podatki lahko zbirajo le za določene in zakonite namene (...). Iz določbe prvega odstavka izhaja, da gre za nezakonito uporabo osebnih podatkov, ki izhajajo iz zbirke osebnih podatkov« (IP-RS 2007b, 3). Povsem enaka sankcija[34] kot za nedovoljeno zbiranje osebnih podatkov (prvi odstavek 143. člena KZ), doleti namreč tudi osebo, ki bi na podlagi drugega odstavka istega člena vdrla v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobila kakšen osebni podatek.

Ugotovimo lahko, da je v slovenskem pravnem redu kraja ali zloraba identitete posameznika (zapor od treh mesecev do treh let) v primerjavi z nezakonito uporabo osebnih podatkov (denarna kazen ali zapor do enega leta) opredeljena kot večji prestopek in zato tudi huje sankcionirana.

Za našo obravnavo bomo v nadaljevanju pogledali različne kategorije kriminalnih dejanj, ki se v negativnem smislu dopolnjujejo z zlorabo ali krajo identitete, kakor jih je razdelal Amitai Etzioni (v Bailey 2004, 41–42):

- **Kriminalci na begu** – ki se ne glede na naravo storjenih prestopkov poslužujejo lažne identifikacije;
- **Nasilje nad otroki in kazniva dejanja zoper spolno nedotakljivost** – izvajajo ga ljudje, ki se zaradi preteklih prestopkov s pomočjo lažne identifikacije vnovič vključujejo v vzgojno-izobraževalne in podobne institucije;
- **Utaje davka na dohodek** – do njih prihaja, kadar si s pomočjo zlorabe osebnih podatkov nekdo v tujem imenu prilasti vračila in druge finančne ugodnosti pri davčnem organu;
- **Neplačevanje preživnin** – da bi se izognili tej obveznosti, starši zamenjajo službo, se preselijo in spremenijo/zabrišejo svojo pravo identiteto;
- **Nelegalna prodaja orožja** – ljudje z obremenilno kazensko kartoteko ob uporabi oz. zlorabi tuje idenitete zaobidejo zakonske pogoje in »legalno« pridobijo orožje;

[34] Kdor prekrši določbe prvega ali drugega odstavka 143. člena KZ, se kaznuje z denarno kaznijo ali z zaporom do enega leta.

- **Nezakonito priseljevanje** – obseg stroškov za storitve, ki jih koristijo nezakoniti priseljenci (in priseljenci z neurejenimi socialnimi zavarovanji) s pomočjo zlorab identitete, je vse prej kot zanemarljiv;
- **Zloraba socialnih pravic** – ko denimo starši ob prijavi fiktivnega otroka koristijo različne socialne transfere.

Ta seznam konvencionalnih kategorij kriminalnih dejanj lahko dopolnimo še s trgovino z mamili, pranjem denarja, krajami vozil in ilegalnim priseljevanjem (McAfee v OECD 2009, 27), seveda pa tudi s kibernetskim kriminalom (glej Poglavje 4.3 Kibernetski kriminal in 4.8 Oblike kibernetskega kriminala). Vsekakor pa lahko kriminalci s področja kraje identitete ukradene identitete zgolj preprodajajo naprej drugim organiziranim kriminalnim združbam (OECD 2009, 17).

## *5.6 Identifikacija*

Če privzamemo, da so mogoče različne *resnice* ali njihovi odtenki in so odstopanja od monolitnih pojmovanj pri primerjavi med posameznikovo identiteto in njegovim telesom na področju družbenega precej toga (denimo, pri njegovem družbenem spolu, rasi, narodnosti, telesnih značilnostih ...), okolje virtualnega na drugi strani siceršnjih fizičnih omejitev praktično ne pozna. »V naravi interneta je, da osebnih (*face-to-face)* odnosov med subjekti ni« (OECD 2009, 15). Ko razmišljamo o identiteti v okolju kibernetskega, praviloma umanjka zavedanje, *soglasje* glede raznoterosti identitete ene ali obeh (večih) v interakcijo vpletenih oseb. V tem primeru govorimo o prevari. Prevara pa je možna predvsem zato, ker, kot ugotavlja Reid (v Wall 2001, 117), se ob odsotnosti socialnega konteksta zameglijo meje med sicer ločenimi dovoljenimi in nedovoljenimi oblikami družbenega obnašanja. Od tod pa je pot do prevare zelo kratka (prim. OECD 2009, 15).

Dokazovanje identitete mora postati splošnejše in bolje artikulirano, ker se bodo kraje identitete kot sredstvo za okoriščanje in kot »kloaka« za nasilje in kazniva dejanja zoper spolno integriteto okrepile (Wall 2001, 22). Kot že omenjeno, obstoječi pogoji informacijske družbe od njenih članov vse bolj zahtevajo prehod iz identifikacije na osnovi instituta imena v institut osebne identifikacije. Sestavine instituta osebne identifikacije so preverljive lastnosti, med katere uvrščamo kombinacijo

posameznikovega spola, imena in priimka, kraja in datuma rojstva, imena staršev, uradnih osebnih identifikatorjev in različnih kod (PIN, uporabniških imen in gesel, IP naslovov, bančnih računov ...) (OECD 2009, 17). Pa vendar je v osnovi policijskega preiskovanja še vedno institut *imena*; oddvojitev slednjega od instituta osebne identifikacije odpre povsem nove dimenzije preiskovanja. V primeru, da osebna identifikacija sloni na identifikatorjih, kot so prstni odtisi ali DNK, je v postopku preiskave ob uspešnih povezavah in ujemanjih sledi z različnih mest zločina in istega DNK ali skupine DNK-jev (npr. barva las, zobovje) potem enostavno priti tudi do imen (Wall 2001, 23). Smiselno isti je tudi način obratnega dokazovanja posameznikove identitete, kadar gre za zaščito ali uveljavljane njegovih pravic.

Obstaja več možnih načinov zlorabe dokumentov za izkazovanje identitete. Ti so lahko spremenjeni (prilagojeni resnični dokumenti), ponarejeni (lažni dokumenti) ali pridobljeni z goljufijo (resnični dokumenti, pridobljeni na osnovi neresničnih dokumentov ali korupcije) (Europol 2013, 17). Osebni identifikatorji, ki nam jih dodelijo upravni organi, bodisi ob rojstvu bodisi ob izdaji dokumentov, dovoljenj in podobnega, imajo dve funkciji – funkcijo *imena*, ki se uporablja vzporedno z nazivom (imenom in priimkom) ali ga nadomešča (npr. številka osebnega dokumenta, davčna številka, EMŠO); in funkcijo *kode*, kot komplement posameznikovega naziva. Zlasti slednja, funkcija kode, služi kot dodatni varnostni prag pri preverjanju identitete posameznika, hkrati pa ima tudi negativno plat, saj ukradenih uradnih osebnih identifikatorjev ni moč spreminjati. V Koreji so leta 2006 prav iz tega razloga nadomestili 13-številčno registrsko številko državljanov z »i-PIN« številko, ki ne vsebuje osebnih podatkov in jo je mogoče kadarkoli nadomestiti z novo (OECD 2009, 17).

Prizadevanja za uveljavljanje in prehod v institut osebne identifikacije izhajajo tako iz preventivnih ukrepov potencialnih žrtev in iz zasebnega sektorja, ne le s strani organov pregona. Žrtve organe pregona aktivirajo šele tedaj, ko odpovedo mehanizmi preprečevanja kriminala (tehnično in fizično varovanje), ki se po obsegu, kakovosti in stroških zagotavljajo zasebno. Neredko pa je spodbuda k večji varnosti rezultat delovanja tržnih sil; ko se denimo ponudnik spletnih storitev zavaruje pred odgovornostjo, ki bi nastala ob zlorabi, zavarovalnica pa od ponudnika terja ustrezno strokovno-tehnično usposobljenost in uporabo varnostnih mehanizmov v podjetju (Wall 2001, 37). Pravtako se neredko izkaže, da nekritično zaupanje v podjetja, ki pri

svojem delu zbirajo pomembne osebne podatke, vendar ne spoštujejo varnostnih standardov[35], lahko vodi do zlorab.

Pomanjkljivi varnostni mehanizmi, mehanizmi identificiranja in nezadostna poučenost državljanov o pomenu varovanja osebnih podatkov močno olajšata delo kršiteljem. V ZDA se je zavedanje o problematiki kraje identitete okrepilo šele po terorističnih napadih 9. septembra 2001. V eni od raziskav[36] so predlagali uveljavitev nekaterih ukrepov, s katerimi bi zlorabe anonimnosti naredili manj dostopne organiziranim kriminalnim združbam in tudi teroristom. Ugotovili so, da je ponarejanje dokumentov (vozniških dovoljenj, potnih listov) preenostavno, da so potrebna dopolnila na področju zakonodaje s področja kraje identitete in veliko bolj usklajeno delovanje različnih (ravni) organov pregona. Po ugotovitvah sektorja za finančni kriminal ameriškega FBI, organizirani kriminal izkorišča nezahtevne postopke lažne identifikacije oz. kraje identitete za odpiranje bančnih računov in pretakanje finančnih sredstev v nezakonite namene (Bailey 2004, 35).

## *5.7 Odločilnost ureditve varstva osebnih podatkov: ZDA vs. Evropa*

Pri primerjavi področja, oblik, pogostosti in drugih značilnosti kraje identitete med ZDA in evropskim prostorom je potrebno upoštevanje nekaterih temeljnih razlik v pravni ureditvi področja varstva osebnih podatkov. Kovačič piše, da je v ZDA že zgodovinsko (bilo) razumevanje zasebnosti osnovano oz. izvedeno iz lastninske pravice in na tej podlagi lahko lastnik osebnega podatka tega z *licenco* odda/proda in tako zaupa tretji strani v upravljanje. »Ko posameznik odda svoje osebne podatke, tako v ZDA načeloma nima več praktično nikakršnega nadzora nad njimi« (Kovačič 2006, 50–52). Podatki postanejo last tistega, ki z njimi razpolaga, slednji pa jih lahko proda dalje ali javno razkrije, če za to ni zakonskih omejitev.

Zakonodaja na področju EU pa, nasprotno, uveljavlja vrsto restriktivnejših določil glede namena zbiranja in uporabe podatkov, posameznik tako mora imeti vselej na izbiro, ali dovoljuje, da se njegovi podatki razkrivajo tretjim osebam in/ali uporabljajo

[35] Pretok osebnih podatkov, urejenih v zbirkah osebnih podatkov reguliran z veljavnim zakonom o varstvu osebnih podatkov in drugimi mednarodnimi pravnimi akti (npr. Sveta Evrope). Eden od razlogov je preprečitev, da bi upravljavci tovrstnih zbirk osebnih podatkov pri njihovi obdelavi zaradi ekonomskih interesov »iznašali« zbirke na območja, kjer pravni red opredeljuje nižje standarde varstva podatkov (IP-RS 2012a, 30–32).

[36] Raziskavo je opravil eden izmed najvplivnejših ameriških think tankov s področja zunanje politike »Council on Foreign Rleations« (www.cfr.org). Izsledki so povzeti iz Bailey (2004, 35).

v namene, drugačne od tistih, zaradi katerih so bili zbrani (IP-RS Safe Harbor, prim. IP-RS 2007a glede iznosa podatkov posameznikov v letalskem in prometu finančnih transakcij). V ameriški Zvezni komisiji za trgovino ugotavljajo, da je »v Evropi težko opredeliti stopnjo oz. obseg zlorab kraje identitete, razlog pa tiči v tem, da problem ni pereč do te mere, da bi si zaslužil izdelavo celovite študije« (Federal Trade Commission 2013č; prim. OECD 2009, 33). Pri tem navajajo primerjalne podatke med Združenim Kraljestvom[37] in ZDA, kjer je bilo v ZK prizadetih 100.000 ljudi oz. 0,17 % populacije, v ZDA pa 10 milijonov oz. 3,39 % populacije[38]. Vseeno pa bi se nekateri avtorji nadejali striktnejše zakonodaje, ki obravnava krajo identitete, tudi v Evropi (Kovačič 2008, 17).

OECD ravno tako ugotavlja, da posledice kraje identitete najmočneje občutijo v Avstraliji, Kanadi, Koreji, v ZDA in Združenem Kraljestvu, slednje pa ne velja oz. ni značilno za EU (2009, 33).

Obstoj enotnega nacionalnega identifikatorja, ki je povezljiv in uporaben na več področjih, kakršna je ameriška koda socialnega zavarovanja (*Social Security Number*[39]), olajša delovanje državni upravi, bančnim/kreditnim institucijam in drugim branžam storitvenega sektorja, seveda pa tudi kršiteljem. Pogosteje se tak identifikator uporablja in pojavlja v dokumentih, odločbah, pri sklepanjih pogodb z javnim ali zasebnim sektorjem, večja je verjetnost, da pride do njegove zlorabe. K manj kršitvam v Evropi prispeva striktnejša ureditev glede hranjenja in nadaljnje uporabe osebnih podatkov (prim. IP-RS 2007a). Če je mogoče nek osebni podatek (nekdanje) stranke zasebnega podjetja v ZDA povezovati (npr. naslov/i, kontaktni podatki, starost, nakupovalne navade/kupna moč) in prodajati tretjim osebam, tega zakonodaja v EU ne dopušča. Tudi banke, zavarovalnice in ostale finančne institucije, ki se medsebojno povežejo, da bi lažje obvladovale kreditna tveganja pri ocenjevanju bodočih poslov, lahko preverjajo le komitente znotraj svojih mrež. Tuja institucija do tovrstnih informacij ni upravičena (Zvezna komisja za trgovino 5). Prav ta restriktivnost in

[37] ZK je v evropskem prostoru izjema, saj pri identifikacijskih dokumentih uporablja podobne prvine povezljivosti kot jih ZDA s sistemom SSN (glej drugo zapovrstno opombo).

[38] Iz razpoložljivih podatkov ni mogoče z gotovostjo opredeliti, na katero leto se nanašajo podatki. Iz izračunov s pomočjo deleža prizadetih in rasti populacije, je to morda l. 2000.

[39] SSN je devetmestna koda, s pomočjo katere ima njen naslovnik oz. lastnik dostop do različnih pravic iz naslova zdravstva, izobraževanja, financ, kreditne sposobnosti (**povezljivost**) in njihovih pripadajočih evidenc. SSN je dodeljen vsakemu posamezniku, ki je državljan ZDA, ima tam urejeno stalno bivanje oz. je na začasnem delu (U.S. Postal inspection service 2013). Temeljna »težava« pri zlorabah SSN je tudi v nerestriktivni zakonski ureditvi s področja varstva osebnih podatkov, pri čemer se smatra, da je **lastnik podatka njegov imetnik**; torej poleg naslovnika SSN tudi denimo zasebno podjetje, ki je ta podatek pridobilo.

zaprtost finančne institucije v Evropi sili k mnogo večji previdnosti in dodatnemu preverjanju pri odpiranju novih finančnih računov, kreditiranju in drugih oblikah zadolževanja (prim. ibid.). Posledično je tudi obseg zlorab identitete občutno bolj omejen (neobstoj longitudinalne študije za področje Evrope/EU, ugasnitev delovanja ekspertne skupine Evropske Komisije *EU Fraud prevention expert group*).

Kraja identitete je v ZDA postala (zvezno) kaznivo dejanje leta 1998 ob sprejetju zakona (*Identity Theft and Assumption Deterrence Act*), kar pa ni zaustavilo naraščajočega števila kršitev (Bailey 2004, 40). Pravna ureditev pred uvedbo tega zakona je bila zgolj parcialna, oblasti pa so lahko kršitelje preganjale zgolj za nekatere prestopke, npr. odpiranje bančnega računa na tuje ime, ne pa tudi za zlorabo pravic iz socialnega zavarovanja. Šele po uvedbi zakona so kršitve, kot so uporaba ukradenih uradnih dokumentov, najemanje kreditov na tuje ime, zloraba gesel za dostop do bančnih in drugih finančnih računov postale kaznivo dejanje. Prišlo pa je tudi do poenostavitve pregona kršiteljev, ki običajno delujejo iz drugih držav/pravnih ureditev, zaradi česar je pred tem prihajalo do številnih zapletov pri sledenju, sankcioniranju, izročanju ... Da je do tega prišlo, je bilo potrebno pristojnost pregona dodeliti Zveznemu preiskovalnemu uradu (FBI) in drugim pristojnim agencijam[40]. Zakon je Zvezni komisiji za trgovino (*Federal Trade Commission)*, ameriški neodvisni agenciji za zaščito potrošnikov, dodelil pristojnost za svetovanje in vodenje postopkov pri prijavah primerov kraje identitete (Federal Trade Commission). Vseeno pa je pozornost obravnavanega zakonskega akta osredišèena na klasičnih zlorabah identitete, slabše pa naslavlja oz. ureja področje kibernetskega kriminala.

Omenjena šibkost ameriškega zakona gotovo ima določen vpliv na dejstvo, da so kraje identitete po statističnih analizah (Preglednica 5.1) Zvezne komisije za trgovino[41] v letu 2012 že 13. leto zapored na prvem mestu med vsemi kategorijami pritožb potrošnikov s področja zlorab (Federal Trade Commission 2013b). Iz Preglednice 5.1 izhaja tudi, da relativni delež v kategoriji kraj identitete sicer upada, česar ne smemo interpretirati kot zmanjševanje števila kraj identitete, ampak gre ta

[40] Poleg Zveznega preiskovalnega urada (FBI) so to še Tajna služba ZDA (*United States Secret Service*), Urad za finančno zaščito potrošnikov (*Consumer Financial Protection Bureau*), Poštna nadzorna služba ZDA (*U.S. Postal Inspection Service*).

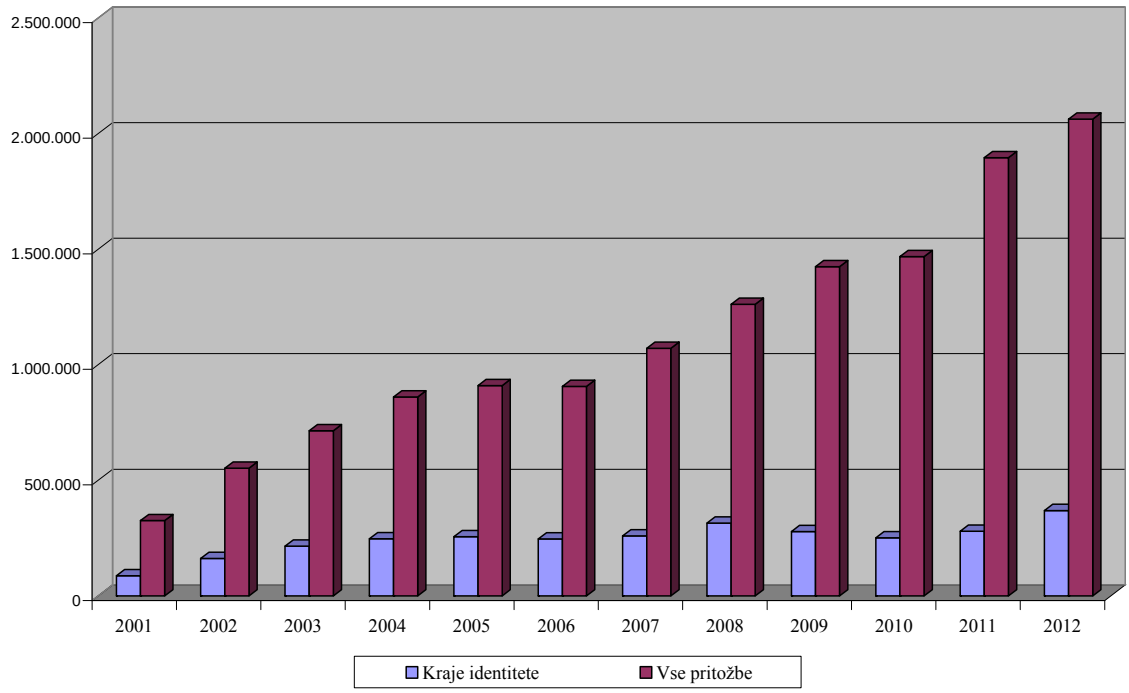
[41] Letne raziskave *Consumer Sentinel Network* je spletno omrežje ZDA, ki svojim članom (organi kazenskega pregona, kot npr. generalni državni pravobranilci) zagotavlja ustrezne podatke in analize o pritožbah s področja varstva pravic potrošnikov, ki jih žrtve zlorab vlagajo pri pristojni Zvezni komisiji za trgovino in drugih organih.

pojav pripisati vse boljši potrošniški ozaveščenosti po ostalih kategorijah,. Kraje v absolutnem smislu še vedno naraščajo. V letu 2012 je pripad pritožb Zvezni komisiji za trgovino zaradi kraj identitete v primerjavi z ostalimi znašal skoraj petino vseh zadev (18%), kar ponazarjajo podatki v Preglednici 5.2.

Preglednica 5.1: Delež kategorije »kraja identitete« izmed pripada vseh pritožb s področja zlorab pri Zvezni komisiji za trgovino med leti 2001 in 2012

| Leto | Kraje identitete | Skupno | Delež (%) |
|---|---|---|---|
| 2001 | 86.250 | 325.519 | 26 |
| 2002 | 161.977 | 551.622 | 29 |
| 2003 | 215.240 | 713.657 | 30 |
| 2004 | 246.909 | 860.383 | 29 |
| 2005 | 255.687 | 909.314 | 28 |
| 2006 | 246.214 | 906.129 | 27 |
| 2007 | 259.314 | 1.070.447 | 24 |
| 2008 | 314.587 | 1.261.124 | 25 |
| 2009 | 278.371 | 1.424.066 | 20 |
| 2010 | 251.089 | 1.467.255 | 17 |
| 2011 | 279.226 | 1.895.012 | 15 |
| 2012 | 369.132 | 2.061.495 | 18 |

Vir: Federal Trade Commission (2013c).




Vir: Federal Trade Commission (2013c).

Preglednica 5.2: Kategorije pritožb, vloženih pri Zvezni komisiji za trgovino za leto 2012. Iz Nacionalnega poročila o pritožbah potrošnikov 2012

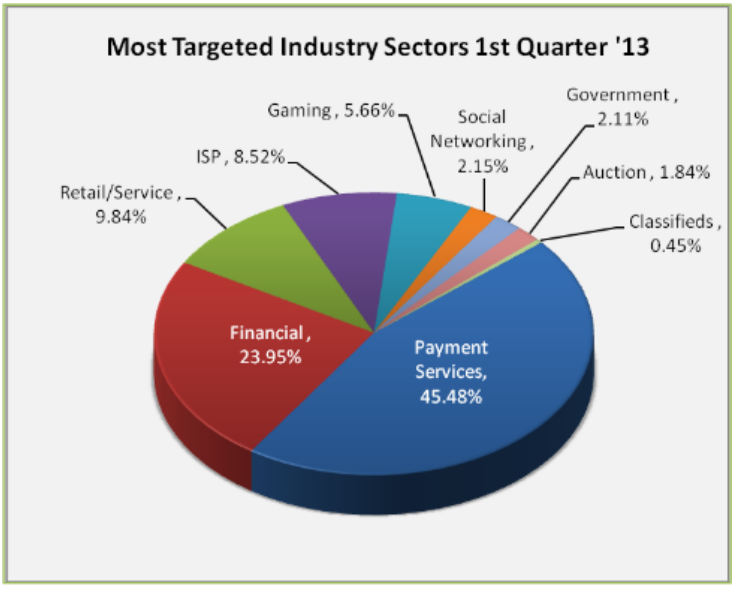
| **Rang** | **Kategorija** | **Število pritožb** | **Delež (%)** |
|---|---|---|---|
| 1. | Kraja identitete | 369.132 | 18 |
| 2. | Izterjava dolgov | 199.721 | 10 |
| 3. | Banke in posojilodajalci | 132.340 | 6 |
| 4. | Nakupovanje od doma in iz katalogov | 115.184 | 6 |
| 5. | Nagrade, nagradne igre in loterije | 98.479 | 5 |
| 6. | Goljufije | 82.896 | 4 |
| 7. | Internetne storitve | 81.438 | 4 |
| 8. | Pritožbe s področja avtomobilov | 78.062 | 4 |
| 9. | Telefonske in mobilne storitve | 76.783 | 4 |
| 10. | Kreditne kartice | 51.550 | 3 |

Vir: Federal Trade Commission (2013b); Federal Trade Commission (2013c, 6).

Tudi evropski Europol v analizi trendov s področja kriminala zaznava krepitev primerov spletnih zlorab v EU; zlasti je v letih 2011 in 2012 bil v porastu phishing. Pozornosti kriminalcev niso deležni zgolj posameznikovi osebni podatki, temveč vse obsežnejše podatkovne baze ponudnikov spletnih storitev (Europol 2013, 28). Po

podatkih delovne skupine Anti-Phishing Working Group[42] za izbrani 1. kvartal leta 2013 (glej Sliko 5.1) so v smislu zlorab najbolj na udaru industrijski sektorji s področja plačilnih storitev (45%), sledi področje financ (24%), prodaja na drobno (10%), ponudniki internetnih storitev (8%), preostala področja skupaj pa manj kot 15%. Gledano v širšem razdobju prihaja do nihanj oz. izmenjevanja pri vrhu tipov zlorab med sektorjem plačilnih storitev in financami (prim. starejših APWG poročil).

Slika 5.1: Najbolj ciljani industrijski sektorji 1. kvartala v letu 2013




Vir: Anti-Phishing Working Group (2013, 7).

Če na podlagi podatkov iz Preglednice 5.3., ki so na voljo v raziskavi Consumer Sentinel Network (Federal Trade Commission 2013c), sklepamo o starostni razporeditvi žrtev kraje identitete, opazimo, da je bila med leti 2010 in 2012 populacija relativno mlada, večinsko stara do 39 let (skupno 53% leta 2010; 51% leta 2011; in 46% v letu 2012). Največje število žrtev, med četrtino in petino vseh, je bilo v starostnem razredu od 20 do 29 let (24%; 23%; in 21%) in pada. Najmanjši delež žrtev je med mlajšimi od 19 let in pri starejših od 70 let, kar gre pripisati nižji stopnji družbene aktivnosti (pogostosti sklepanja raznih pravnih poslov, finančnih transakcij in podobnega), deloma pa tudi manjši vključenosti v (elektronske) komunikacijske tokove (starejši).

[42] Anti-Phishing Working Group (APWG) je globalno združenje, v katerem globalna industrija, organi kazenskega pregona in vlade delujejo usklajeno v boju zoper kiberkriminal. Oblikujejo podatkovne vire, standarde in modele sistemov odzivanja ter protokole za zasebni in privatni sektor (Anti-Phishing Working Group).

Preglednica 5.3: Starost žrtev kraje identitete po skupinah (v obdobju 2010–2012)[43]

| Consumer Age | CY - 2010 | | CY - 2011 | | CY - 2012 | |
|---|---|---|---|---|---|---|
| | Complaints | Percentages[1] | Complaints | Percentages[1] | Complaints | Percentages[1] |
| 19 and Under | 18,334 | 8% | 19,623 | 8% | 16,133 | 6% |
| 20-29 | 56,635 | 24% | 56,721 | 23% | 57,491 | 21% |
| 30-39 | 49,375 | 21% | 49,869 | 20% | 52,704 | 19% |
| 40-49 | 43,877 | 19% | 45,132 | 18% | 49,403 | 18% |
| 50-59 | 35,314 | 15% | 38,051 | 15% | 45,483 | 17% |
| 60-69 | 19,923 | 8% | 23,112 | 9% | 30,583 | 11% |
| 70 and Over | 12,984 | 5% | 15,819 | 6% | 22,027 | 8% |
| Total Reporting Age | 236,442 | | 248,327 | | 273,824 | |

Vir: Federal Trade Commission (2013c, 14).

Podatki iz Preglednice 5.4 kažejo, da je večina pritožb kraje identitete s področja zlorabe uradnih dokumentov in socialnih pravic (primeri davčnih goljufij in tistih, vezanih na plače so absolutno najštevilčnejši; primeri zlorab dokumentov pa zelo redki) in še naraščajo — njihov delež se je v letu 2012 v primerjavi z letom 2010 več kot podvojil in obsega skoraj polovico vseh oblik kraje identitete. Opaziti je trend padanja zlorab na ostalih področjih[44] (kreditne kartice, javne gospodarske storitve, bančne zlorabe ...).

Nasprotno so v raziskavi OECD o spletni kraji identitete iz l. 2009 napovedovali sklep, da bi se lahko vsled rastočemu številu uporabnikov elektronskega plačevanja tovrstna oblika kriminala dodatno okrepila. Vsekakor pa v raziskavah (Cyber Security Industry Alliance (2005); Business Software Alliance and Harris Interactive (2007); Europol (2013)) povzemajo, da zlorabe identitete omejujejo in zavirajo elektronsko trgovanje. »Kraja identitete za mnoge velja kot največje tveganje, ki so mu uporabniki in potrošniki izpostavljeni v današnjem digitalnem okolju« (OECD 2009, 17–18).

[43] Delež potrošnikov, ki so vložili prijavo na Zvezno komisijo za trgovino in je podatek o njihovi starosti znan, znaša 74% v letu 2012, 89% v letu 2011 in 94% v letu 2010. Opomba tudi v tabeli.

[44] Ameriški Identity Theft Resource Center je v raziskavi iz l. 2004 kot prevladujoče oblike kraje identitete zaznal finančne zlorabe (66%), finančne in kriminalne (9%) in finančne, kriminalne in kloniranje (6%) (OECD 2009, 17).

Preglednica 5.4: Delež pritožb glede na namen zlorabe osebnih podatkov

| Vrsta kraje identitete | 2010 | 2011 | 2012 |
|---|---|---|---|
| Zloraba uradnih dokumentov in pravic | 19,2 % | 27,4 % | 46,4 % |
| Zloraba kreditnih kartic | 15,8 % | 14,3 % | 13,4 % |
| Telekomunikacije & javne gosp. službe | 15,1% | 13,4 % | 9,7 % |
| Bančne zlorabe | 10,8% | 8,7 % | 6,4 % |
| Zlorabe, povezane z zaposlitvijo | 11,2% | 8,4 % | 5,4 % |
| Zlorabe s posojili | 3,7% | 3,1 % | 2,4 % |
| Druge oblike kraje identitete | 22,5% | 23,7 % | 18,5 % |
| Poskusi kraje identitete | 7,0% | 6,8 % | 6,6 % |

Vir: Federal Trade Commission (2013c, 12).

Zvezna komisija za trgovino (v OECD 2009, 29) deli žrtve kraje identite v tri kategorije:

- Novi računi (novo odprti bančni računi, kreditne kartice, posojila; javne socialne storitve),
- Zloraba obstoječih ne-kartičnih računov,
- Zloraba obstoječih kreditnih kartic.

Čeprav je (prva) kategorija žrtev, kadar storilci v njihovem imenu odpirajo nove račune, manj pogosta, ima lahko neprimerno večje finančne posledice, obenem pa terja več časa, da jo žrtev odkrije in negativne posledice tudi odpravi (ibid., 29). V splošnem s pojmom žrtev mislimo najpogosteje na posameznika, žrtve so pa tudi vlade, mednarodne organizacije, podjetja ali gospodarstvo kot celota (ibid., 33).

Kar vsak četrti slovenski potrošnik je po ugotovitvah raziskave Trženjski monitor Društva za marketing Slovenije iz pomladi 2012 skeptičen do načina plačevanja oziroma zlorab na spletu (Društvo za marketing Slovenije 2012). Po ugotovitvah Evropske Komisije v okviru sprejemanju ukrepov za podvojitev deleža elektronske trgovine do leta 2015, pa je takih potrošnikov v Evropi kar 35% (Evropska Komisija 2012). Po podatkih International Telecommunication Union online survey iz l. 2006 pa celo 40% (OECD 2009, 40). Da je zadržanost slovenskih potrošnikov do elektronskega kartičnega plačevanja izrazito, potrjuje tudi Aljoša Domijan, solastnik slovenske spletne trgovine Enaa.com, ki ugotavlja, da je plačevanje s kreditnimi

karticami zanemarljivo v primerjavi s plačilom po povzetju poštarju, osebnim prevzemom in plačilom prek banke (Kalan 2012, 22). Nadalje Domijan ugotavlja, da je zlorab kreditnih kartic tudi v svetu zelo malo. »Dogajajo se kvečjemu tako, da hekerska skupina vdre v neko banko in dobi veliko število podatkov o karticah. Posameznih kupcev na spletu se preprosto ne izplača loviti« (ibid., 23). Podobno velja tudi za zahteve po varstvu osebnih podatkov kupcev podjetja, pri čemer je dosežena najvišja raven ravno s plačilom s karticami, saj je pri tem potrebnih najmanj ali nič osebnih podatkov (le naslov za dostavo).

Ker je sistem varstva osebnih podatkov v ZDA drugačen od evropskega, je trend kraj identitete usmerjen navzgor; temu primerno so se v ZDA tudi strateško odzvali s poudarkom na preventivnih aktivnostih, dopolnjuje se seznam kaznivih dejanj, vezanih na krajo identitete in zaostrujejo kazniva dejanja, do katerih pride »sinergično« s krajo identitete (npr. neupravičeno koriščenje socialnih pravic s krajo identitete, zloraba kreditne kartice s pomočjo oziroma preko kraje identitete). Informacijski pooblaščenec je leta 2007 izrazil pričakovanje, da je v prihodnje pričakovati porast kaznivih dejanj te vrste in zato predlagal in dosegel razširitev kazenskega zakonika s krajo identitete (prim. IP-RS 2007b). Tudi v Europolu na podlagi obsežnosti oblik kibernetskega kriminala napovedujejo njegovo rast. Zlasti naj bi v prihodnje bila na udaru področja mobilne telefonije in računalništva v oblaku. Skupaj še s prepletanjem uporabe službene in osebne računalniške opreme v službene namene, kjer bodo na nosilcih spomina občutljivi osebni in poslovni podatki podvrženi različno kakovostni in učinkoviti zaščiti, bo to predstavljalo resen izziv razvijalcem, skrbnikom in lastnikom (osebnih) podatkov (Europol 2013, 28).

### 5.7.1 Zloraba plačilnih kartic

Do zlorabe plačilnih kartice pride na način, da storilec bodisi fizično pridobi kartico bodisi si zagotovi številke, vezane na račun bodisi podatke z magnetnega polja na hrbtni strani kartice. Ker je plačevanje možno preko interneta in »brez posedovanja kartice« (t. i. card-not-present poslovanje), slednje storilcem močno olajša zlorabe (OECD 2009, 29). Tudi potem, ko so bili pri pristojnih organih sproženi ustrezni postopki, preklicane bančne in kreditne kartice ipd., lahko kršitelj nadaljuje z zlorabami drugod, saj še vedno razpolaga s potrebnimi podatki (U.S. Postal inspection service 2013).

Za zlorabe plačilnih kartic sta značilna nizko tveganje in visoki dobički. V Europolu (Europol 2013, 29) ocenjujejo, da se letno v EU organizirane kriminalne združbe okoristijo za približno 1,5 milijarde eurov. V letu 2011 je bilo kar 60% zlorab pri kartičnem poslovanju izvedenih »brez posedovanja kartic« v skupni vrednosti 900 milijonov eurov. Obseg škode naj bi v nekaterih državah članicah EU že presegal tistega, ki ga kriminalci povzročijo s skimming tehnikami na bankomatih. S povečevanjem obsega plačevanja preko spleta je pričakovati tudi povečanje obsega zlorab brez posredovanja kartic. Ker bo v prihodnje vse več plačil izvedenih ob pomoči mobilne in NFC[45] tehnologije, bodo čedalje podjetnejše združbe organiziranega kriminala investirale v nadaljnji razvoj tehnik zlorab omenjenih tehnologij.

## *5.8 Varnostne niše v verigi identificiranja*

Okolje, ki bi bilo povsem imuno na zlorabe identitete, ne obstaja. Za njihovo uspešno preprečevanje in preventivno naravnanost pa je pomembno, da je odgovornost v verigi identificiranja na vseh njenih členih: ustrezno harmonizirani zakonodaji za lažji pregon zlorab (univerzalnost); zanesljivosti dokumentov in verifikacijskih postopkov (legalnost); vključenosti strank oz. žrtev in (transparentnost) in; varnem hranjenju podatkovnih baz (varnost). Z vidika finančnega poslovanja poročilo posebne skupine Evropske Komisije (*Fraud Prevention Expert Group*) kot najšibkejše točke v verigi izpostavlja najprej uporabnikov osebni računalnik, bodisi zaradi nezadostnih varnostno-tehničnih ukrepov bodisi zaradi nepoučenosti (*phishing* in *pharming*); nato ponudnike internetnih storitev (ISP); in pa ponudnike storitev shranjevanja podatkov kot tretje osebe oz. uradni registri zbirk podatkov (Fraud Prevention Expert Group 2007b, 2–4).

Da so uporabniki v mnogih državah podvrženi tveganju, zatrjujejo v raziskavi OECD, kjer izpostavljajo, dejstvo, da na vprašanje zlorab identitete marsikje niso odgovorili z zadostno mero skrbnosti (2009, 18–19).

Poseben primer so ZDA, kjer pomanjkljiva raven standardiziranosti in centraliziranosti uradnih registrov pušča zlorabam na stežaj odprta vrata. »Mesta, okrožja in države vsaka zase uporabljajo svoje sisteme evidentiranja,« (Bailey 2004,

[45] Tehnologija NFC (Near Field Communication) je brezžična tehnologija kratkega dosega, ki temelji na spoju že uveljavljenih brez kontaktnih in povezovalnih tehnologij.

47) ki so zastareli, zato lahko kršitelji relativno enostavno pridobijo oz. zaprosijo za sicer veljavne identifikacijske dokumente, a osnovane na izmišljenih dejstvih. Med najbolj zaželjenimi so rojstni list ali vozniško dovoljenje, ki so potem podlaga za izdajo preostalih dokumentov (potni list, ameriško socialno zavarovanje SSN), odpiranje bančnih računov, najemanje hiš in stanovanj, kupovanje avtomobilov, vršenje kaznivih dejanj in drugih kršitev v tujem imenu (ibid., 48). Tudi teroristična dejanja, ki so jim bile priča ZDA v letu 2001, so bila izvedena ob pomoči zlorabe identitete – s pridobitvijo ponarejenega vozniškega dovoljenja so si teroristi zagotovili osnove za mobilnost in koriščenje ostalih storitev (najemanje stanovanj, pretakanje finančnih sredstev z računa na račun, obiskovanje tečaja za letalskega pilota ...) (ibid., 48–49).

Vsekakor je koristneje na vprašanje zlorab identitete gledati z vidika varnosti posameznikovih podatkov v celotni dolžini identifikacijske verige in manj kot problem vdora v zasebnost (ibid., 50).

## *5.9 Odgovornost pri kraji identitete*

Na to, kdo nosi odgovornost v primerih kraje identitete, vpliva način, na katerega pride do zlorab. Je posledica malomarnosti, ki jo lahko pripišemo tako državi, podjetju ali posamezniku. Od tega je tudi odvisno, kdo nosi odgovornost; le njen del, večino ali v celoti. Odgovornost se kaže v prevzemanju bremen, tako v obliki neposrednih stroškov kakor tistih, ki nastanejo posredno.

Neposredne stroške kraje identitete statistično najpogosteje najdemo zabeležene kot oceno višine bremena, ki ga mora gospodarstvo neke države pokriti pri odpravljanju posledic zlorab. Izražamo ga lahko tudi kot povprečno izgubo sredstev pri posamezni zlorabi identitete. Po podatkih, ki jih iz različnih virov povzema OECD (2009, 37) so ocenjene vrednosti za:

- VB v letu 2002 1,2 mrd GBP, v letu 2003 pa 1,7 mrd GBP;
- ZDA v letu 2007 49,3 mrd USD ali povprečno 1.408 USD leta 2006 in 3.257 USD leta 2007;
- Avstralijo v letu 2007 med 1 in 3 mrd USD;

pri čemer je dejavnikov, ki vplivajo na metodološko vprašljivost in ne/realen odraz[46] izsledkov raziskav toliko, da se slednje odraža na veljavnosti rezultatov, ki so si često nasprotujoči in kažejo na diametralno nasprotne trende.

Posredni stroški kraje identitete se kažejo na vrsto različnih načinov, v primerjavi z neposrednimi pa jih obravnavajo le redke statistične analize. V praksi mednje prištevamo težave posameznika pri izdajanju (novih) plačilnih kartic, zavračanje drugih nedenarnih plačilnih instrumentov (npr. čekov), »čiščenje« in ponovno vzpostavljanje kreditne sposobnosti, izgubo zaposlitvenih možnosti, aretacije za kazniva dejanja drugih oseb, stroški pravnih postopkov in pravne pomoči, kakor tudi psihološke posledice.

Področje odgovornosti v primerih zlorab ureja tako zakonodaja kot prostovoljne poslovne prakse (ibid., 38), vsem pa je skupno, da večidel ali celotno breme zlorabe prevzamejo družbe ali ponudniki storitev, posamezniki pa le v primeru, kadar jim je moč dokazati malomarno ravnanje. V številnih državah je v veljavi zgornja meja odgovornosti, tj. maksimalni znesek, ki ga mora plačati posameznik, žrtev finančnih zlorab (v ZDA je to do 50 USD, v EU do 150 EUR) (ibid., 39). Mnoga podjetja z namenom krepitve zaupanja potrošnikov slednjim zagotavljajo storitve z »nič odgovornosti« (t. i. *zero liability*).

## *5.10 Mimikretične taktike*

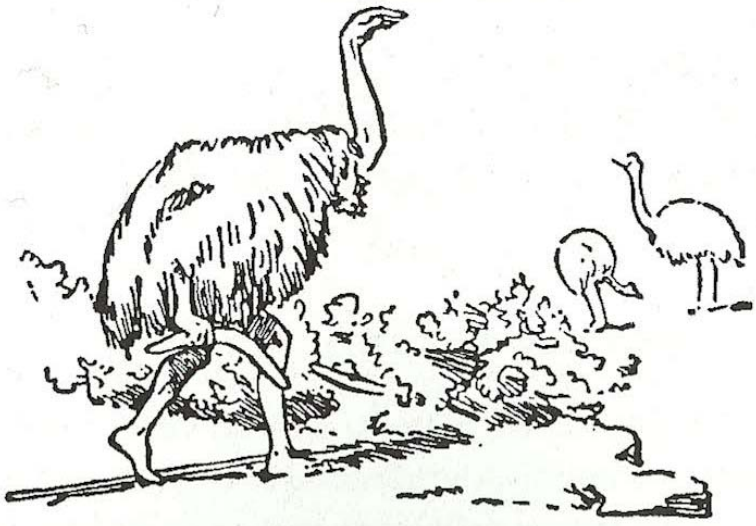
S splošnim pojmom mimikrija, ki je izvorno s področja botanike/zoologije, označujemo »obliko biološke podobnosti, v kateri nenevaren in užiten organizem (mimik) oponaša (za operatorja/plenilca) neužiten, škodljiv, oziroma nevaren organizem (model)« (Maksuti 2008, 236; prim. Smrke 2007, 16). Zelo nazoren primer iz živalskega sveta so denimo paličnjaki in živi listi[47]. Smrke ta koncept z biološkega področja aplicira na področje družbenega in družbeno (človeško) mimikrijo definira kot »pridobivanje osebe/skupine A (mimika) pojavu/osebi skupini B (modelu), kar osebo/skupino C (ali B) (operatorja) zavede oziroma naj bi zavedlo v napačno prepoznavo osebe/skupine A, s tem oseba oziroma skupina A (mimik) doseže (ali naj bi dosegla) določen cilj« (2007, 27). Na področju filozofije Lacan ta isti pristop

[46] Za natančnejšo obravnavo o vzrokih glej poglavje o Metodologiji.

[47] Kot zanimivost lahko navedemo, da je znanstveno ime reda teh žuželk Phasmatodea, kar v grščini pomeni »posnemalci« (Landcare Research 2013).

obravnava kot kamuflažo (Maksuti 2008, 237); Gambetta (2005, 223) pa o kamuflaži govori bolj kot o negativni mimikriji, tj. prikrivanju nezaželjene lastnosti (prim. Sliko 5.2).

Slika 5.2: Uporaba *mimikretične* taktike pri zalezovanju/lovu na živali



*Avstralski domorodec zalezuje emuje, pokrit z emujevo kožo. V roki nosi bumerang, med prsti na nogah pa sulico.*

Vir: Baden-Powell (2011, 175).

Za našo obravnavo pa je najzanimivejše področje kibernetske mimikrije; za to obliko zavajanja najpogosteje zasledimo angleški izraz *deception*. »Pri prevari v računalništvu se neka oseba ali program zamaskira kot nekdo drug s ponarejanjem podatkov in tako dobi neko (...) korist. Kibernetsko mimikrijo lahko razdelimo na več področij. Najbolj pomembno področje je poneverba spletnih strani, iz tega izhaja kraja identitete posameznika in na koncu še poneverba elektronske pošte« (Dokl v Poljšak 2009, 8). Prevare so povezane predvsem z novo tehnologijo, vključno z internetom v kibernetskem prostoru (Mintz v Poljšak 2009, 8).

Poljšak (2009, 9) lepo sintetizira kibernetsko mimikrijo na primeru spletnih strani in ugotavlja, da je

> *glavni medij kibernetske mimikrije (...) splet ali internet, na katerem so spletne strani, ki jih lahko poimenujemo tudi* ***model****, saj predstavljajo okolje,*

*ki ga mimik posnema. Internet omogoča vsakemu uporabniku, da ustvari lastne strani, ki se tičejo katerekoli vsebine. Omogoča različne možnosti skrivanja identitete izvora (dez)informacij. V vlogi* ***operatorja*** *oziroma sprejemnika je predvsem običajen, razmeroma nevešč in naiven uporabnik spleta, medtem ko* ***mimikretično akcijo*** *vodi tehnološko bolj vešča oseba, ki jo na področju kibernetske mimikrije lahko imenujemo* ***mimik****, saj je tisai, ki izvaja mimikrijo* (poudarki moji).

Najpogostejši način, da uporabnik zaide na kompromitirane spletne strani, je preko neželenih sporočil in zlonamerne programske opreme.

## *5.11 Tehnike zlorab*

V poglavju 4.8.1 Podrobneje o hekerstvu smo se že dotaknili tehnik, ki se jih napadalci poslužujejo za dešifriranje osebnih in drugih občutljivih podatkov svojih žrtev. V tem poglavju bomo uporabili Firbasovo (2009, 23–29) razlikovanje na osnovne in napredne tehnike zlorab za pridobivanje osebnih podatkov; distinkcija temelji na tem, ali je tehnika samostojna in deluje samodejno ali pa je za njen uspeh potrebna intervencija napadalca. To razlikovanje tehniko »poceni« ali »podraži«, saj, kot bomo videli v nadaljevanju, je moč nekatere tehnike uporabljati masovno, medtem ko je za uspeh drugih potreben napadalčev trud, ki je specifičen za vsak primer posebej.

### 5.11.1 Osnovne tehnike

- Računalniški virusi

Širijo se brez natančno določenega cilja. Včasih s pojmom virusi poljudno označujemo vse programe ali programske kode, namenjene povzročanju škode ali obremenjevanju računalniških sistemov, ki so se hkrati sposobni sami širiti (Kovačič 2003, 57). Medij za njihovo širjenje in eksponentno razmnoževanje so programi ali druge izvršilne datoteke, kar ima v primeru okužbe celotnega računalniškega sistema za posledico izgubo podatkov in vrsto sistemskih napak (prim. Firbas 2009, 23).

- Računalniški črvi

Črvi so v primerjavi z virusi samostojnejši, saj za svoje širjenje ne potrebujejo medija, temveč izkoriščajo varnostne pomanjkljivosti operacijskih sistemov in drugih v omrežje povezanih programov.

- Trojanski konj

Za razliko od virusov in črvov potrebujejo trojanski konji za svoje delovanje uporabnikovo intervencijo. Ne širijo se samodejno, kakor tudi ne morejo okuževati drugih datotek v računalniku. Običajno se »pretvarjajo«, da so povsem običajni programi, njihove skrite funkcije pa so najpogosteje namenjene odpiranju t. i. stranskih vrat na žrtvinem računalniku, kraji gesel ali povzročanju druge škode (Kovačič 2003, 56).

- »Dictionary attack« oziroma »brute force attack« (napad z grobo silo)

Z omenjenima izrazoma mislimo na tehniko za razbijanje šifriranih podatkov in dostop do gesel. Ugibanje gesla za dostop do računalnikov, omrežij, strežnikov s pomočjo ustrezne programske opreme je možno zlasti tedaj, ko sta kakovost in varnost gesla nizki (geslo je sestavljeno iz enostavnih kratkih besed, brez kombinacije malih in velikih črk ter posebnih znakov), varnostni sistem pa nima časovne blokade pri ponavljanjih ob napačnem vnosu. Napadalec s pomočjo programa poskuša vse možne kombinacije (malih tiskanih, velikih tiskanih črk, številk, znakov ...). Razvozlano geslo napadalcu odpre vrata za pridobivanje osebnih podatkov, spreminjanje varnostnih in drugih sistemsko-programskih nastavitev ter izvajanje vrste drugih kršitev in zlorab. Bolj kot je geslo kompleksno, dlje traja dešifriranje in manjši pomen imajo šifrirane informacije. Namreč, teoretično je možno dešifrirati čisto vsako geslo, vendar v primeru varnih gesel, ki so dovolj dolga in kompleksna, postopek zaradi dolgotrajnosti izgubi smisel (prim. Firbas 2009, 25).

### 5.11.2 Napredne tehnike

- »Tempest« napad

Tehnika »tempest« napadov se uporablja za prisluškovanje elektronskim signalom, ki jih oddajajo elektronske naprave. Temelji na prestrezanju elektromagnetnih signalov s pomočjo anten in širokopasovnih sprejemnikov na klasičnih katodnih zaslonih (Firbas 2009, 27). S pomočjo posebnih tehnologij pa je mogoče zajemati tudi vsebine z računalniških zaslonov (npr. LCD), za kar zadošča že odsev od predmetov, ki jih

običajno najdemo ob zaslonih (kozarci, vaze, lončki, plastenke, očala ali celo uporabnikova očesa) v razdaljah do 30 metrov (Backes in drugi 2008).

Prisluškovati pa je mogoče tudi klasičnim računalniškim tipkovnicam na vsaj dva načina. Prvi je s pomočjo infrardečega laserja, usmerjenega na odsevno površino prenosnega računalnika na razdalji med 15 in 30 metri, ki na podlagi kombinacije zaznavanja vibracij in tehnike »dynamic time warping« ugiba podobnost vzorcev ponavljanja signalov in tako sklepa na vnešene znake (Mills 2009). Drugi način je pa prestrezanje »prometa« s tipkovnic, ki so na računalnik priključene preko PS/2 konektorjev, tako da se z uporabo digitalnega osciloskopa in analogno-digitalnega pretvornika električne pulze iz električnega omrežja pretvori v črke in besede. Omenjena tehnologija ne deluje na prenosnikih in tipkovnicah, ki so v računalnike priključene preko USB konektorjev (Mills 2009).

TEMPEST je sicer kratica obsežnega projekta ameriške Agencije za nacionalno varnost (NSA), ki obsega metode prisluškovanja signalom, ki jih oddaja računalniška tehnologija in je le v manjšem delu dostopen javnosti (zgolj v delu, ki določa standarde o zaščiti) (TEMPEST 2014).

- »Cold boot« napad

Namen »cold boot« napada je zagotoviti si dostop do podatkov in gesel na delovnem pomnilniku računalnika. Podatke delovni pomnilnik hrani še kratek čas po tem, ko je bil računalnik ugasnjen. Pogoj za izvršitev[48] takega napada je, da ima napadalec fizični dostop do še prižganega računalnika (Firbas 2009, 28).

- Socialni inženiring

»Zlorabe zasebnosti niso povzročene samo s tehničnimi sredstvi, pač pa tudi z različnimi goljufijami, ko skušajo napadalci žrtev prepričati oziroma pretentati, da jim posreduje dostop do sistema ali posreduje želene podatke oziroma informacije, ali pa se do želenih podatkov dokopljejo s tajnim opazovanjem (»social engineering«)« (Kovačič 2003, 41). Tehnika socialnega inženiringa je »postopek in praksa pridobivanja zaupnih informacij s pomočjo manipulacije in zvijače od legitimnih uporabnikov določenih storitev« (Dokl 2006, 31), ko npr. heker kontaktira zaposlenega v podjetju in se pretvarja, da je nekdo drug in si na ta način zagotovi dostop do računalniškega sistema in podatkov. Napadalec izkorišča psihološko nagnjenost ljudi (zlasti naivnost in nevednost), da postavijo prijaznost in željo pomagati pred varnostnimi protokoli; kar predstavlja eno od možnih varnostnih niš v

[48] Za natančnejši opis postopka »cold boot« napada glej Firbas 2009, 28–29.

sistemu (Bailey 2004, 43). Pomembna sestavina socialnega inženiringa je »opazovanje in proučevanje navad žrtev« (Tulloch v Firbas 2009, 26). Ta tehnika se potem kombinira z nameščanjem zlonamerne programske opreme (OECD 2009, 21), npr. trojanskih konjev ali računalniških virusov.

- »Pretext calling«

»Pretext calling« oziroma klicanje z lažnim identificiranjem je oblika socialnega inženiringa, ki jo kršitelji uporabljajo zato, da pod pretvezo poskusijo pridobiti žrtvine podatke, tako da se pri ciljni ustanovi preko telefona lažno identificirajo, bodisi v škodo ustanove bodisi njenih strank.

- Brskanje po smeteh (»dumpster diving«)

Brskanje po smeteh terja od tatu, za razliko od ostalih tehnik, da je fizično blizu svoji žrtvi in ima dostop do njegove pošte, gospodinjskih odpadkov in drugih zanj zanimivih in uporabnih virov informacij. Ta tehnika je močno ciljno naravnana in tudi bolj tvegana od ostalih, ki jih ščiti anonimnost in breztelesnost virtualnega okolja.

- »Spoofing« oziroma prevare

»Spoofing« tehnika oz. prevare so lahko enostavnejše; denimo, da hekerji uporabijo programsko opremo, s pomočjo katere »ponaredijo« pošiljateljev elektronski naslov; do kompleksnejših, ko vdrejo v poštni strežnik in od tam pošiljajo elektronsko pošto. Spoofing tehnika ima namen bodisi pridobiti občutljive osebne podatke bodisi v javnost lansirati dez/informacije. Ena od tehnik je »IP spoofing«, kjer se nam v brskalniku prikazuje lažni IP naslov.

- Spletno ribarjenje (»phishing«)

Navkljub neobstoju splošne in univerzalne definicije phishinga[49], naj bi se za ta pojem štelo, da predstavlja glavno metodo, ki omogoča krajo identitete (OECD 2009, 22). »Phishing« (iz ang. *fishing* + *phreaking*[50] – spletno ali internetno ribarjenje (tudi: lažno predstavljanje) in telekomunikacijske zlorabe) je ena od tehnik socialnega inženiringa. Termin so 1996. skovali ameriški hekerji, ki so vdirali v uporabniške račune ameriškega portala AOL (ibid. 22). V splošnem gre pri phishingu za postopek zavajanja, ko želi nekdo s pomočjo lažnega predstavljanja pridobiti osebne podatke, najpogosteje uporabniška imena in gesla, številke bančnih kartic in PIN ter digitalna

[49] Ponekod je phishing sinonim za krajo identitete.
[50] Semantičnih razlag hekerskih pojmov je zaradi socio-kulturoloških razlogov pri obravnavi sub- in kontrakultur, razumljivo, več. Ena od razlag razčlenjuje *phishing* na »password« + »fishing«, tj. ribarjenje gesel (IP-RS 2013b). Pojem *phreaking* pa naj bi bil skovanka iz 70. let *ph(one)* + *hacking*, torej vdiranja v telefonske sisteme (OECD 2009, 22).

potrdila. Poskusi se najpogosteje pojavijo kot neželena e-sporočila (spam), v kateri žrtev kontaktira domnevni uradni administrator uporabniku poznane spletne strani in z različnimi izgovori želi iz**vabi**ti osebne podatke, na primer tako, da uporabnika pozove k prijavi na spletno mesto. Vendar pa administratorjeva povezava vodi na ponarejeno spletno stran (*Mirror-website*; mimikretični model), ki je na videz enaka izvirni. Da prevara izgleda čim bolj resnično, napadalec URL naslov[51] spletne strani prilagodi tako, da izgleda karseda podoben izvirnemu (Firbas 2009, 26). Na tak način zavedeni uporabnik vnese zahtevane podatke (najpogosteje sta to uporabniško ime in geslo), spletna stran pa javi napako in ga preusmeri na uradno spletno stran, kjer uporabnik, misleč, da je storil tipkarsko napako, tokrat uspešno opravi postopek prijave in se dejansko ne zaveda, da ni več edini, ki razpolaga s svojim uporabniškim profilom (Dokl 2006, 44; OECD 2009, 23–24). Tehnika ribarjenja se lahko izvaja tudi s pomočjo neželenih pojavnih oken pri uporabi internetnih brskalnikov. Dodatno jo je mogoče kombinirati s *spoofing* tehniko in neželenim nameščanjem »keylogging« programov, katerih naloga je beleženje zaporedij pritiskov tipkovnice in njihovo sporočanje kršitelju.

V poročilu ameriškega Identity Theft Technology Council o Spletni kraji identitete iz leta 2005 (ITTC v OECD 2009, 26) raziskovalci zaključujejo, da so »razlikovanja med tipi napadov (spletnega ribarjenja) porozna, saj so mnogi izmed njih **hibridni** in uporabljajo več tehnologij« (poudarek moj).

Povzeli bomo še nekatere druge podzvrsti spletnega ribarjenja, za katere je značilna avtomatiziranost:

- »Pharming«

»Pharming« (iz ang. *farming* + *phishing/pharmacy*[52] – »kmetovanje« in spletno ribarjenje in/ali tehnika genskega inženiringa) je tehnika napada, ki ima namen dostop(ajoče) na določeno spletno stran preusmeriti k lažni in na ta način nepooblaščeno dostopati do vnešenih osebnih podatkov in/ali gesel, s končnim namenom razpolagati s tujimi finančnimi sredstvi. Napad je usmerjen bodisi na računalniški strežnik internetnega ponudnika bodisi »na določeno datoteko, ki se nahaja na računalniku uporabnika (gre za t. i. datoteko o gostiteljih oz. *host file*, kjer se nahajajo podatki o URL-jih in domenah)« (IP-RS 2013b). Pharming je naprednejša

[51] Uvedba mednarodnih domen (IDN – International Domain Names) je uporabnikom prinesla dodatno varnostno tveganje, saj lahko napadalec registrira domeno, ki ima v naslovu namesto črk latinice skoraj identične posamične črke iz cirilice, česar žrtev ne opazi (Bratuša v Firbas 2009, 26).

[52] Za razlago glej pripombo št. 49.

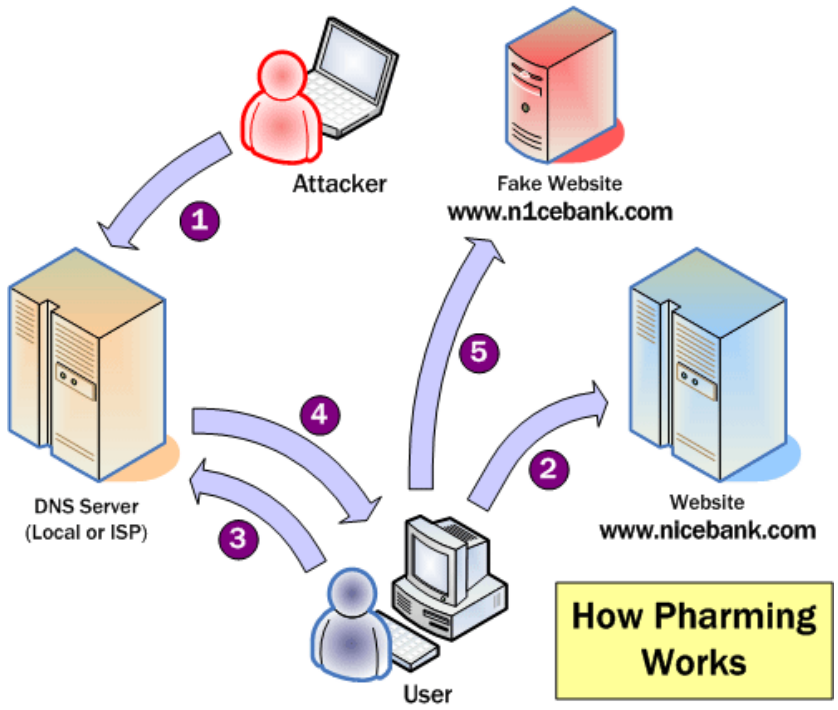
in manj opazna tehnika od spletnega ribarjenja, saj za svojo širitev ne potrebuje nalaganja zlonamernih programov, neželenih oken in e-pošte (»vabe«). Na ta način sta tudi domet napada in nabor njegovih žrtev (sama »žetev«) mnogo bolj gotova in neprimerno večja. Protivirusni in podobni programi zato žrtve pred pharmingom ne morejo zaščititi.

Dodatno k širjenju prevar (*spoof* spletnih strani) prispeva avtomatiziranost, ki je vgrajena v zlonamerno programsko opremo in tako z okuženih spletnih strežnikov učinkuje epidemično dalje na spletne strani (OECD 2009, 28).

Natančneje v kombinaciji s shematičnim prikazom (glej Sliko 5.3) poglejmo, kako v petih korakih tehnično poteka DNS pharming napad (Chaudhari 2006):

1. Napadalec kot cilj svojega napada izbere DNS strežnik spletne strani, do katere bo dostopala žrtev. Strežnik se lahko nahaja bodisi v zaprtem, LAN omrežju ali na javno dostopnem ISP strežniku. S pomočjo različnih tehnik napadalec preusmeri IP naslov izvorne spletne strani na ponarejeno spletno stran, ki je kopija izvorne.
2. Uporabnik želi dostopiti do uradne spletne strani in njen naslov vtipka v brskalnik.
3. Uporabnikov računalnik pošlje ukaz za dostop do uradne spletne strani.
4. Okuženi DNS strežnik uporabnikovemu računalniku vrne kompromitirani IP naslov in ga preusmeri na ponarejeno spletno stran.
5. Uporabnikov računalnik ne zazna, da ni na zahtevani spletni strani, uporabnik pa obišče ponarejeno spletno stran, s katero upravlja pharming napadalec.

Slika 5.3: Shematični prikaz poteka *pharming* napada




Vir: Chaudhari (2006).

- »Man-in-the-middle« napad

»Man-in-the-middle« napad je ena od konvencionalnejših podzvrsti spletnega ribarjenja. Zanj je značilno, da storilec prestreže in/ali spremeni podatke v interakciji med uporabnikoma. Kadar je napad uspešen, se uporabnika ne zavedata tretje osebe, hkrati pa oba mislita, da gre za drugo osebo oz. uporabnika.

- »SMiShing«

Podzvrsti spletnega ribarjenja segajo tudi na zunanje naprave, kakršni so mobilni telefoni (OECD 2009, 25). SMiShing je pojav, ko žrtev na sporno spletno stran zvabi s pomočjo poziva v obliki SMS sporočila. V pozivu prejemnika obvestijo, da se je včlanil v plačljiv klub, v izogib stroškom se pa lahko odjavi (ali npr. naj namesti »ustrezen« protivirusni program) preko vsebovane povezave na spletno stran, ki je kompromitirana in služi kraji osebnih podatkov.

- »Vishing«

Vishing tehnika za krajo osebnih podatkov izkorišča telefone. V kombinaciji s spoofing tehniko žrtev prejme denimo e-pošto, za katero se zdi, da so jo odposlali iz prave ustanove in v kateri je pozvan h klicu na vsebovano telefonsko številko zaradi preverjanja. Klic nato preusmerijo na avtomatski odzivnik, ki od žrtve zahteva osebne

idr. idenitifikacijske podatke. Druga možnost je tudi, da storilci žrtev neposredno pokličejo na stacionarno ali mobilno številko (prim. ibid., 25–26).

# 6 SKLEP

Namen pričujoče naloge je bil ugotoviti, ali tehnološke implikacije predstavljajo resno tveganje za našo zasebnost ali pa po drugi strani ne gre pri tem za tehnofobične vzgibe in zadržanost do novosti ter podvrženost medijskim poročanjem in skupinam pritiska. V treh odstavkih, ki sledijo spodaj, avtor poskuša poiskati odgovore na zastavljene cilje diplomske naloge.

V pomembnem delu diplomske naloge smo se ukvarjali s poljem kibernetskega kriminala. Pri reflektiranju tega polja družbenega veljajo določene specifike, saj denimo ločenost virtualnega subjekta od njegovega fizičnega telesa dovoljuje širjenje zlorab (Brown 2003, 149). Če k tej ločenosti dodamo še nesledljivo anonimnost, ki pomeni sila ugodno razmerje tveganja in praktično neomejene priložnosti, potrebujejo storilci kaznivih dejanj samo željo po hitrem zaslužku ter seveda ekspertna znanja s področja informacijsko komunikacijskih tehnologij. Zato je povsem umestno pričakovati, da se konvencionalne družbene patologije selijo tudi v ta relativno nov prostor družbenega delovanja (Trček 2003, 112).
Spoznali smo tudi, da izmed ugotovljenih tipov hekerjev so (v nasprotju s splošnim mišljenjem) najnevarnejši »script kiddiesi«. Slednji svoje znanje in veščine, ki so v primerjavi s hekerji in krekerji omejene, instrumentalizirajo v zlorabe iz koristoljubja; ne pa v željo po razumevanju programskih kod ali iz patološko motiviranih vzgibov za krajo identitete. Splošneje gledano gre za nov tip grožnje, osredotočen na informacije in komunikacijo, ki sta ga analitika Arquilla in Ronfeldt poimenovala *netwar*. Kršitelji so organizirani v majhne, geografsko razpršene skupine, dejavne v omrežjih brez jasne (hierarhične) linije odločanja, pri svojem delu pa se poslužujejo informacijske tehnologije (Arquilla in Ronfeldt 1995). Nekatere študije napovedujejo, da bodo z novimi tehnologijami »opolnomočeni« posamezniki žarišče krminala premaknili s premičnega premoženja na ljudi. Pričakovati pa je tudi nacionalno omejene in nepremišljene institucionalne odzive pristojnih. Zaradi razpršenosti storilcev, potencialnosti žrtev in spremenljivosti/prilagodljivosti oblik kriminala je večina današnjega digitalnega kriminala izven dosega organov pregona in regulatorjev; zato se preganjajo le prestopki zadostnega (največjega) obsega. Vendar v

pogojih spleta, kjer sta dimenziji časa in prostora v primerjavi z realnim povsem izvzeti, je utemeljeno pričakovanje, da so organi pregona stežka uspešni, možnosti kršiteljev pa neomejene. Pregon kaznivih dejanj, tehnološke in tržne rešitve ter mednarodno sodelovanje so soodvisni in od uigranosti njihovega medsebojnega součinkovanja bo v prihodnje odvisna tudi uspešnost pregona (Wall 2001, 29). Ker pa v mednarodni skupnosti še ni zadostnega soglasja, je breme za zagotavljanje varnosti preloženo na iskanje ustreznih tehnoloških rešitev in na zakonitosti trga.

Če hočemo priti do veljavnih zaključkov, ali je ustroj interneta takšne narave, da zagotavlja varnost ali, povedano drugače, da varnostna tveganja ne učinkujejo zaviralno na njegov razvoj, moramo razumeti njegovo strukturo, zlasti tiste njene gradnike, s katerimi je moč negativne pojave regulirati. Lessig je (v Wall 2001, 170) opredelil štiri »načine omejitve«: **zakonodajo**, ki definira ne/dovoljene oblike obnašanja; **arhitekturo**, ki s kodami in protokoli omogoča tehnični nadzor in nove oblike zlorab; **socialne norme**, ki jih uporabniki »uvozijo« v kibernetsko okolje; in **trg**, ki ustvarja in zavira priložnosti. Odgovornost za reguliranje in zagotavljanje reda v kiberprostoru je porazdeljena na **pet ravni** (internetni uporabniki, ponudniki internetnih storitev (ISP), organizacije korporativne varnosti, javno financirane ne-javne varnostne organizacije in javno financirane javne varnostne organizacije) (ibid.). Ugotovili smo, da učinkovito reguliranje ni v zakonodajnem reguliranju vedenja uporabnikov, temveč v reguliranju arhitekture interneta s pomočjo zakonodaje. Pogoji, kot so »(p)omanjkanje tehničnega (...) znanja, nezadostna osveščenost, pomanjkljiva programska oprema postavljajo posameznika v podrejen položaj nasproti velikim podjetjem, državi ali osebam z znanjem in motivom po pridobivanju osebnih podatkov« (Brezovšek in Črnčec 2007, 203) in tako odpirajo prostor raznovrstnim oblikam zlorab. Whittaker (2002, 122) povzema Powerjeve ugotovitve, da je premik iz tradicionalnih na spletne storitve imel za posledico poslabšanje varnosti, saj institucije in podjetja s težavo dohajajo razvoj informacijske tehnologije (prim. Bagon 2006). Zato je nižjim ravnem potrebno okrepiti podporo, višje ravni pa morajo imeti izdelano strategijo za delo v kibernetskem prostoru in varnostno politiko.

Politološka analiza pa ne more brez izpraševanja o temeljnem razmerju moči v kibernetskem, ki se kaže skozi odgovor na vprašanji *koliko* in *kakšna* anonimnost. Če nas družba sili v nujno odopovedovanje delu svoje zasebnosti na račun večje

funkcionalnosti in obvladovanja kompleksnosti življenja v sodobni družbi (Kovačič 2003, 34), se lahko anonimnost hipoma spremeni v nevarno orožje (Bailey 2004, 4–5). Boj za vojaško, ekonomsko, kulturno in politično hegemonijo se vse od konca hladne vojne seli v polje kibernetskega. Danes kot še nikoli doslej so očitne težnje po nadzoru nad tokovi informacij v želji oblikovati »strukturo informatičnega globalnega gospostva«, ki mu načelujejo le informacijsko najnaprednejše nacije z ustreznimi finančnimi sredstvi, dovršenimi tehnološkimi rešitvami in zasebno pobudo (prim. Trček 2003, 122). Vseeno pa dobivajo akademske in civilno družbene presoje, da se hekerje in krekerje zaradi njihovih sposobnosti in prepričanj smatra za najresnejšo nevarnost okolju kibernetskega, vse bolj realno podlago, ki na drugi strani ne pozabijo pojasnjevati, da je tako tolmačenje v interesu ravno tistih, ki si prizadevajo za vršenje monopolnega nadzora nad kibernetskim: konkretno sta to trgovina[53] in država (Wall 2001, 4).

Iskanje občutljivega ravnotežja o koliko in kakšni anonimnosti je prepredeno ne samo s pastmi, ampak tudi s paradoksi; kakršno je npr. razmerje med pravico do zasebnosti in varnosti, pri čemer sta pravici medsebojno povezani, soodvisni, a hkrati tudi v obratnem sorazmerju (Brezovšek in Črnčec 2007, 210). Prizadevanja države za zagotavljanje sledljive anonimnosti kot ključne prvine za zagotovitev varnosti ne le da potekajo daleč stran od civilno družbenega nadzora, ampak pogosto tudi državo samo postavijo nevarno blizu tistim, zoper katere naj bi se bojevala. Civilna družba pa, pogosto brez sodelovanja trga, nasprotno, vselej poišče način, da z novimi tehnološkimi rešitvami omogoča nesledljivo anonimnost.

Pred desetletjem je Bailey (2004, 45) razmišljal o tem, da bi se v elektronskem poštnem prometu s tehnologijo digitalnih potrdil moglo preseči slabosti anonimnosti in povečalo možnosti za izsledite neželjenih ravnanj (zlasti neželjenih sporočil). Danes je uporaba digitalnih potrdil za elektronsko poslovanje (SIGEN-CA) namenjena uporabnikom za identificiranje pri e-poslovanju z organi slovenske javne uprave. Ugotovimo lahko, da identificiranje s pomočjo potrdil ni postalo varnostni pogoj pri uporabi (povečini brezplačnih) elektronskih poštnih računov (omogoča pa njihovo nadgradnjo z elektronskim podpisom). Je pa vse pogostejša praksa izkazovanja identitete križanje uporabniških računov družbenih omrežij (npr. medsebojne kombinacije Google/Gmail, YouTube, Twitter, Facebook profilov ali z različnimi družbenimi aplikacijami).

[53] Wall omenja nadzor nad trgom (2001, 11).

Več uporabe interneta pomeni večji trg in več priložnosti, s tem pa tudi možnosti za zlorabe (Wall 2001, 116). V pogojih te poenostavitve oz. redukcije kompleksnosti so po mnenju Dokla (2006, 59) najbolj izpostavljeni tisti, ki se ne zavedajo dovolj, kakšnim grožnjam so v kibernetskem okolju izpostavljeni in kako se jim ubraniti. »Taki uporabniki so podvrženi veliki verjetnosti, da bo njihov računalnik postal tarča zlonamernih programov, nezaželene pošte, elektronskega vohljanja itd. Sami pa bodo prve tarče sleparij in prevar, ki jih spretni avtorji izdelujejo prav za take uporabnike – nepoučene« (ibid.). V teh primerih ima nepoučenost lahko zelo visoko ceno, tudi zato, ker veliko uporabnikov prevaro zazna šele tedaj, ko se sooči z negativnimi posledicami.

Zaokrožimo lahko z dvema sklepoma. Najprej, navkljub mnenju nekaterih, da je za področje interneta značilna brezpravnost in odsotnost učinkovitih zakonskih omejitev in določil, velja prej nasprotno: internet je možno regulirati, prav tako obstoji nekakšna večnivojska struktura »policy« upravljanja. In še, za posameznikovo varnost na internetu ne veljajo nič drugačna pravila kot so v veljavi za preprečevanje oz. omejevanje ostalih »nekibernetskih« oblik kriminalnih dejavnosti; tj. zavedanje stopnje tveganja in zagotavljanje zadostnih preventivnih ukrepov.

Kraja in zloraba identitete v najširšem smislu pomenita nedovoljeno prevzemanje identitete nekoga drugega. Kraja identitete je definirana kot uporaba osebnih podatkov oz. idenitete nekoga drugega (imena, datuma rojstva, obstoječega in nekdanjih naslovov) za pridobitev neke koristi, običajno ekonomske narave, ali inkriminacijo druge osebe (Fraud Prevention Expert Group 2007a; IP-RS 2012b, 5; United States Department of Justice 2013). Zloraba identitete se uporablja tudi kot sopomenka za krajo identitete; temeljna razlika med pojmoma pa je v tem, da zloraba identitete zajema tudi uporabo lažne, namišljene identitete (Fraud Prevention Expert Group 2007a). Namen kraje identitete je z zlorabo osebnih podatkov pridobiti si določeno premoženjsko korist, hkrati pa ima za posledico tudi poseg v druge osebnostne pravice (IP-RS 2007b, 4). OECD krajo identitete opredeljuje kot medsektorski pojav, za katerega je značilno, da ima širok vpliv in krši tako predpise o varstvu potrošnikov kot varnost, zasebnost in pravila glede neželene pošte (2009, 3). Standardne opredelitve kraje identitete na mednarodni ravni ni, naj bo to zloraba »identitete v spletu« (t. i. online identity) ali »nepovezane identitete« (t. i. offline identity).

Posledica različnih ureditev tega pravnega področja je različno preprečevanje, preganjanje in sankcioniranje (ibid., 15).

OECD je leta 2009 napovedoval sklep, da bi se lahko vsled rastočemu številu uporabnikov elektronskega plačevanja spletna kraja identitete dodatno okrepila. Europol v napovedovanju in policy priporočilih za leto 2013 (Europol 2013, 28) povzema ugotovitve raziskave Evropske Komisije, ki ugotovilja, da je 8% uporabnikov interneta v EU bilo žrtev kraje identitete, 12% pa žrtev drugih oblik spletnih zlorab. Obenem je pa z zlonamerno opremo (malware) prizadetih na milijone gospodinjstev, kakor tudi iz leta v leto raste obseg bančnih zlorab, vezanih na splet. Pomembna je tudi ugotovitev, da se v številnih članicah EU zabeleži le določen delež zlorab; po zatrjevanju nekaterih članic pa je zgolj 30% primerov (kraj identitete) prijavljenih organom kazenskega pregona.

Ameriške vladne ustanove pomenljivo ugotavljajo, da je »v Evropi težko opredeliti stopnjo oz. obseg zlorab kraje identitete, razlog pa tiči v tem, da problem ni pereč do te mere, da bi si zaslužil izdelavo celovite študije« (Federal Trade Commission 2013č; prim. OECD 2009, 33). Pri tem navajajo primerjalne podatke med Združenim Kraljestvom in ZDA, kjer je bilo v ZK prizadetih 100.000 ljudi oz. 0,17 % populacije, v ZDA pa 10 milijonov oz. 3,39 % populacije. OECD prihaja do istih ugotovitev: da posledice kraje identitete najmočneje občutijo v Avstraliji, Kanadi, Koreji, v ZDA in Združenem Kraljestvu, slednje pa ne velja oz. ni značilno za EU (2009, 33).

V ZDA so bile kraje identitete po statističnih analizah Zvezne komisije za trgovino v letu 2012 že 13. leto zapored na prvem mestu med vsemi kategorijami pritožb potrošnikov s področja zlorab (Federal Trade Commission 2013b). Populacija ameriških žrtev je relativno mlada, prevladuje starostni razred med 20 in 29 leti, sicer jih je pa več kot polovica starih do 39 let. Prednjačijo zlorabe uradnih dokumentov in socialnih pravic in še naraščajo – njihov delež obsega skoraj polovico vseh oblik kraj identitete. Opaziti pa je trend padanja zlorab na ostalih področjih (kreditne kartice, javnih gospodarskih storitev, bančnih zlorab ...).

Spričo dejstva, da analize povečini ne razlikujejo med spletno (online) in nepovezano (offline) krajo identitete, je težko izvesti veljaven zaključek, katera od oblik je prevladujoča in/ali ima za žrtev hujše posledice (OECD 2009, 39). Vseeno so v ameriški longitudinalni raziskavi Javelin Strategy and Research ID theft iz leta 2006 (ibid., 39–40) prišli do sklepa, da je »online« zlorab identitete zgolj 10%, preostalih 90% se odvija po konvencionalnih nekibernetskih poteh. Po njihovih ugotovitvah,

četudi je poskusov zlorab na internetu sicer več, je devet od desetih poskusov obsojenih na neuspeh.

Če poskusimo poiskati vzroke za razlike v obsegu zlorab identitete med ZDA in Evropo, leži del v tradiciji zagotavljanja socialnih storitev (v EU so načela države blaginje mnogo bolje uveljavljena in zato je potreb po izigravanju socialnih pravic posledično manj), nezanemarljiv del pa ima tradicija pravnega urejanja področja varstva osebnih podatkov. Posledica različnih ureditev tega pravnega področja je različno preprečevanje, preganjanje in sankcioniranje tudi na ožji ravni zlorab identitete (OECD 2009, 15). Restriktivnost in zaprtost finančne institucije v Evropi sili k mnogo večji previdnosti in dodatnim preverjanjem pri poslovanju s komitenti in s tem omejuje obseg zlorab.

Pomanjkljivi varnostni mehanizmi, mehanizmi identificiranja in nezadostna poučenost državljanov o pomenu varovanja osebnih podatkov močno olajšata delo kršiteljem. Vendar kljub temu, da države uveljavljajo različne ukrepe z namenom omejiti negativne vplive kraje identitete (kampanje za ozaveščanje potrošnikov in uporabnikov spleta, dopolnjevanje zakonskih okvirov, javno-zasebna partnerstva, pobude pod vodstvom industrije na področju ukrepov tehničnega varovanja ...), so namen, obseg in učinki kraje identitete različni od države do države (OECD 2009, 7).

Bailey zatrjuje, da je kombinacija anonimnosti in zlorabe identitete kršitve s področja kiberkriminala poenostavila (2004, 42). Podobno beremo v poročilu OECD, v katerem ugotavljajo, da se s pojavom interneta in elektronskega poslovanja kraja identitete kaže na »povsem novi ravni« (OECD 2009, 7), hkrati pa izražajo zaskrbljenost, ali med državami raznolike pravne ureditve vprašanja kraje identitete omogočajo implementacijo zadostnih ukrepov (ibid., 47). Do zaključka, da ukradene identitete omogočajo široko paleto organiziranih prevar, tako tistih *spletnih* kot tistih *nepovezanih*, prihajajo tudi v Europolu (Europol 2013, 17). Na podlagi izsledkov v tej nalogi ne moremo nedvoumno sklepati o razmerju med spletno in nepovezano krajo identitete, vendar ob upoštevanju krepitve na splet vezanih storitev, je zaključek (stališče), da imajo spletne zlorabe blažje posledice od nepovezanih, vprašljiv. Zlasti ne izvemo dovolj podrobnosti o argumentih zanj. Sklenemo lahko, da je spletna kraja identitete po obsegu, učinkih in posledicah najmanj izenačena z nepovezano obliko kraje identitete.

Na podlagi vseh upoštevanih vidikov lahko potrdimo uvodoma zastavljeno raziskovalno vprašanje in zaključimo, da je v pogojih informacijske družbe možnosti za zlorabe zasebnosti nedvomno več.

Najti ustrezno ravnotežje v družbi med anonimnostjo in identifikacijo (ali v nekaterih ozirih »sledljivo anonimnostjo«) je s pojavljanjem novih in novih tehnologij, spletnih aplikacij in spreminjanjem družbenih praks vse prej kot enostavna naloga, pred katero je postavljena vrsta strokovnjakov, od politologov, sociologov, kriminologov, komunikologov, pravnikov, družbenih aktivistov, navsezadnje pa tudi zakonodajalcev in običajnih državljanov. Pretirano nagibanje na stran nesledljive anonimnosti kaj hitro ustvari ustrezne pogoje in razmere, ko država pri zagotavljanju varnosti in reda postane kaotična in nemočna. Nagibanje na stran pretirano odprte in transparentne družbe pa duši človekovo ustvarjalnost in s spogledovanjem s policijsko državo presežno posega v sfero posameznikove intime. Vsekakor pa velja, da »tveganja anonimne družbe močno presegajo tveganja odprte družbe« (Bailey 2004, 38).

# 7 LITERATURA


1. Alighieri, Dante. 1994. *Božanska komedija*. Ljubljana: Mihelač.

2. *Anti-Phishing Working Group* (APWG). Dostopno prek: http://www.apwg.org/ (30. oktober 2013).

3. --- 2013. *Anti-Phishing Working Group poročilo 1. kvartala 2013.* Dostopno prek: http://docs.apwg.org/reports/apwg_trends_report_q1_2013.pdf (30. oktober 2013).

4. Arquilla, John J. in David F. Ronfeldt. 1995. *Cyberwar and Netwar: New Modes, Old Concepts, of Conflict.* Dostopno prek: http://www.rand.org/publications/randreview/issues/RRR-fall95-cyber/cyberwar.html (6. avgust 2012).

5. Babnik, Blaž. 2012. *Vpliv informacijske tehnologije na družbo.* Diplomsko delo. Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://dk.fdv.uni-lj.si/diplomska_dela_1/pdfs/mb11_babnik-blaz.pdf (20. december 2013).

6. Backes, Michael, Markus Dürmuth in Dominique Unruh. 2008. *Compromising Reflections or How to Read LCD Monitors Around the Corner.* Dostopno prek: http://www.cs.ut.ee/~unruh/publications/reflections.pdf (20. januar 2014).

7. Baden-Powell, Robert. 2011. *Skavtstvo za fante: priročnik za odgovorno državljanstvo.* Ljubljana: ZSKSS.

8. Bagon, Judita, Andreja Cirman, Tatjana Hajtnik, Anita Ivačič, Helena Kamnar, Maša Kociper, Dušan Kričej, Sašo Matas, Gorazd Perenič, Nataša Pirc Musar, Jože Šturm, Marjeta T. Vesel, Zdenka Ulaga, Dejan Verčič, Gregor Virant, Franci Zavrl, Urša Zore Tavčar in Karmen Uglešić, ur. 2006. *Priročnik za javne menedžerje.* Ljubljana: Portis.

9. Bakardijeva, Maria. 2005. *Internet society: the internet in everyday life.* London: Sage.

10. Brezovšek, Marjan in Damir Črnčec. 2007. *Demokratična uprava in tajnost podatkov*. Ljubljana: FDV.

11. Brown, Sheila. 2003. *Crime and law in media culture.* Buckingham; Philadelphia: Open University Press.

12. Business Wire. 2013. *Javelin Strategy and Research Report 2012*. Dostopno prek: http://www.businesswire.com/news/home/20130220005223/en/12-Million-Identity-Fraud-Victims-2012-Latest (2. november 2013).

13. Chaudhari, Nilesh. 2006. *Pharming on The Net*. Dostopno prek: http://palizine.plynt.com/issues/2006Mar/pharming/ (6. maj 2013).

14. Deflem, Mathieu in Brian Hudak. 2008. Internet Extortion and Information Security. V *Organized Crime: From Trafficking to Terrorism*, ur. Frank G. Shanty, 289–292. Santa Barbara, CA: ABC-CLIO. Dostopno prek: http://www.cas.sc.edu/socy/faculty/deflem/zinternetextort.pdf (14. maj 2011).

15. Dokl, Jure. 2006. *Internet in koncept človekove varnosti.* Diplomsko delo. Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://uploadi.www.ris.org/editor/1176446958dokl-jure.pdf (24. april 2013).

16. Dolinar, Maja. 2007. *Uporabnost konstruktivistične analize etničnega konflikta in oblikovanja identitete na primeru Makedonije*. Diplomsko delo. Ljubljana: Fakulteta za družbene vede.

17. Evropska Komisija. 2012. *Načrt ukrepov za podvojitev volumna elektronske trgovine v Evropi do leta 2015.* Dostopno prek: http://europa.eu/rapid/press-release_IP-12-10_sl.htm?locale=fr (17. avgust 2012).

18. Europol. 2006. *EU Organised Crime Threat Assessment* (OCTA). Dostopno prek: https://www.europol.europa.eu/sites/default/files/publications/octa2006_0.pdf (10. oktober 2013).

19. --- 2013. *EU Serious and Organised Crime Threat Assessment* (SOCTA). Dostopno prek: https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf (10. oktober 2013).

20. Firbas, Gregor. 2009. *Varovanje zasebnosti nekoč in danes.* Diplomsko delo. Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://dk.fdv.uni-lj.si/diplomska_dela_1/pdfs/mb11_firbas-gregor.pdf (15. januar 2014).

21. Fraud Prevention Expert Group (FPEG). 2007a. *Preventing payment fraud in Europe.* Dostopno prek: http://ec.europa.eu/internal_market/fpeg/identity-theft_en.htm (17. april 2013).

22. --- 2007b. *Report on Identity Theft/Fraud.* Dostopno prek: http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf (17. april 2013).

23. Gambetta, Diego. 2005. Deceptive Mimicry in Humans. V *Imitation, Human Development, and Culture,* ur. Susan Hurley in Nick Chater, 221–241. Cambridge: MIT Press. Dostopno prek: http://www.nuffield.ox.ac.uk/People/sites/Gambetta/Publication%20Files/Deceptive%20mimicry%20in%20humans.pdf (27. april 2013).

24. Haralambos, Michael in Martin Holborn. 2001. *Sociologija: teme in pogledi.* Ljubljana: DZS.

25. Hvala, Ivan in Marjan Sedmak, ur. 2004. *Politea. Civilne rarzsežnosti politike.* Ljubljana: Fakulteta za družbene vede in Društvo Občanski forum.

26. IP-RS. 2007a. *EU-ZDA: Nova omejevanja varstva osebnih podatkov v okviru boja proti terorizmu.* Dostopno prek: https://www.ip-rs.si/novice/detajl/eu-zda-nova-omejevanja-varstva-osebnih-podatkov-v-okviru-boja-proti-terorizmu/ (16. april 2013).

27. --- 2007b. *Pripombe na predloge predpisov.* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pripombe_na_predloge_predpisov__Pdf_in_doc_/Pripombe_na_KZ.doc (5. maj 2013).

28. --- 2012a. *Letno poročilo Informacijskega pooblaščenca za leto 2011.* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2011.pdf (7. avgust 2012).

29. --- 2012b. *Smernice za preprečevanje kraje identitete.* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Smernice_kraja_identitete.pdf (7. avgust 2012).

30. --- 2013a. *Safe Harbor – Varni pristan.* Dostopno prek: https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/iznos-osebnih-podatkov-v-tretje-drzave/safe-harbor/ (16. april 2013).

31. --- 2013b. *Varstvo osebnih podatkov na internetu.* Dostopno prek: https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/ (4. maj 2013).

32. --- 2013c. *Varstvo osebnih podatkov posameznika.* Dostopno prek: https://www.ip-rs.si/varstvo-osebnih-podatkov/pravice-posameznika/ (4. maj 2013).

33. Ježek, Maruša. 2004. *Slovenija na prehodu v družbo znanja.* Diplomsko delo. Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://dk.fdv.uni-lj.si/dela/Jezek-Marusa.PDF (21. december 2013).

34. Kalan, Maja. 2012. Intervju tedna: V slovenskih trgovinah pogrešam svetovne cene. *Žurnal24*, 22–23 (14. november).

35. Kovačič, Matej. 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut, Inštitut za sodobne družbene in politične študije.

36. --- 2006. *Nadzor in zasebnost v informacijski družbi.* Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://dk.fdv.uni-lj.si/eknjige/EK_Kovacic_2006_Nadzor.pdf (6. marec 2011).

37. --- 2007. Nadzoru ni mogoče uiti. *Mladina* (28): 34–35.

38. --- 2008. *Deskanje po varnih vodah*. Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://www.safe.si/uploadi/editor/1213086334Deskanje_po_varnih_vodah.pdf (4. marec 2011).

39. *Kazenski zakonik* (KZ-1-UPB2). Ur. l. RS 50/2012. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=201250&stevilka=2065 (10. november 2013).

40. Maksuti, Alem. 2008. Družbena mimikrija. *Časopis za kritiko znanosti* 36 (233): 236–242.

41. McIntosh, Neil. 2002. *Tangled web of e-commerce.* Dostopno prek: http://www.guardian.co.uk/uk/2002/sep/21/privacy4 (4. april 2011).

42. Mills, Elinor. 2009. *Sniffing keystrokes via laser and keyboard power*. Dostopno prek: http://archive.is/oAFeR (20. januar 2014).

43. Mlinar, Zdravko. 2006. Videonadzor in varnost v mestnih prostorih: kritična ocena dosedanjih izkušenj. *Uporabna informatika* XIV (3):154–163.

44. Organizacija za gospodarsko sodelovanje in razvoj (OECD). 2009. *Online identity theft.* Pariz: Committe on Consumer Policy, OECD.

45. Landcare Research. 2013. *Stick Insects (Phasmatodea)*. Dostopno prek: http://www.landcareresearch.co.nz/science/plants-animals-fungi/animals/invertebrates/systematics/phasmatodea (25. april 2013).

46. Poljšak, Borut. 2009. *Kibernetska mimikrija spletnih strani*. Diplomsko delo. Ljubljana: Fakulteta za družbene vede.

47. *Research And Development Corporation* (RAND). Dostopno prek: http://www.rand.org/about.html (6. avgust 2012).

48. Richardson, Robert. 2008. *CSI Computer Crime & Security Survey*. Dostopno prek: http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf (12. marec 2011).

49. Rosenfeld, Louis in Peter Morville. 2002. *Information architecture for the World Wide Web*. Sebastopol (Kalifornija): O'Reilly.

50. Sanders, H. John. 1999. *Analiza tveganja*. Univerza v Marylandu. Dostopno prek: http://polaris.umuc.edu/~jsaunder/admn641/641les10.htm (14. april 2011).

51. *Splošna deklaracija človekovih pravic* (SDČP). 1948. Dostopno prek: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/slv.pdf (20. december 2013).

52. Sever, Vital. 2012. Je varno še varno? *Življenje in tehnika* LXIII: 69–74.

53. Smrke, Marjan. 2007. *Družbena mimikrija*. Ljubljana: Fakulteta za družbene vede.

54. Sv. Pismo. 2013. *Jakobova zvijača in Izakov blagoslov,* 1 Mojzes 27: 11–12, 15–17. Dostopno prek: http://www.biblija.net/biblija.cgi?m=1+Mz+27%2C1-40&id13=1&pos=0&set=2&l=sl (19. april 2013).

55. Tekavec, Pavel. 2011. *Zlonamerna koda kot grožnja informacijski varnosti posameznika*. Diplomsko delo. Maribor: Fakulteta za varnostne vede. Dostopno prek: http://dkum.uni-mb.si/IzpisGradiva.php?id=20425 (23. april 2012).

56. TEMPEST. 2014. *Tempest (codename).* Dostopno prek: http://en.wikipedia.org/wiki/TEMPEST (24. januar 2014).

57. Trček, Franc. 2003. *Problem informacijske (ne)dostopnosti*. Ljubljana: Center za prostorsko sociologijo, Fakulteta za družbene vede.

58. Trifunović, Leona. 2009. *Domneva nedolžnosti v kazenskem postopku Republike Slovenije.* Diplomsko delo. Maribor: Fakulteta za varnostne vede. Dostopno prek: http://dkum.uni-mb.si/IzpisGradiva.php?id=11767 (9. maj 2013).

59. Društvo za marketing Slovenije (DMS). 2012. *Trženjski monitor DMS, pomlad 2012*. Dostopno prek: http://www.slideshare.net/fullscreen/marketingslo/ trenjski-monitor-dms-april-2012-poroilo/22 (12. avgust 2012).

60. TV Slovenija. 2014. *Na tretjem ... »Intervju z vodjem Varnostnega centra SI-CERT Gorazdom Božičem«.* Ljubljana. 1. februar. Dostopno prek: http://ava.rtvslo.si/predvajaj/intervju-z-vodjem-varnostnega-centra-si-cert/ava2. 174259178/ (3. februar 2014).

61. United States Department of Justice. 2013. *Identity Theft and Identity Fraud.* Dostopno prek: http://www.justice.gov/criminal/fraud/websites/idtheft.html (13. april 2013).

62. U.S. Postal Inspection Service. 2013. *Identity Theft: Stealing Your Name and Your Money.* Dostopno prek: https://postalinspectors.uspis.gov/investigations/ MailFraud/fraudschemes/mailtheft/IDProtectName.aspx (15. april 2013).

63. Wall, S. David, ur. 2001. *Crime and the Internet.* London; New York: Routledge.

64. Whittaker, Jason. 2002. *The Internet: the basics.* London; New York: Routledge.

65. *Federal Trade Commission*. Dostopno prek: http://www.ftc.gov/bcp/index.shtml (13. april 2013).

66. --- 2013a. *Identity theft*. Dostopno prek: http://www.consumer.ftc.gov/features/ feature-0014-identity-theft (13. april 2013).

67. --- 2013b. *FTC Releases Top 10 Complaint Categories for 2012*. Dostopno prek: http://ftc.gov/opa/2013/02/sentineltop.shtm (13. april 2013).

68. --- 2013c. *Nacionalno poročilo o pritožbah potrošnikov 2012*. Dostopno prek: http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf (13. april 2013).

69. --- 2013č. *Identity Theft – What Europe can teach us.* Dostopno prek: http://www.ftc.gov/os/comments/IDMngmntworkshop/527026-00017.pdf (15. april 2013).