1. kolokvij
MEDIJI V INFORMACIJSKI DRUŽBI

6. ETIČNI FORUM INFORMACIJSKE DRUŽBE

INFORMACIJSKA DRUŽBA PO SNOWDNU

Uredniki:

JÓZSEF GYÖRKÖS

MELITA ZAJC

SMILJANA GARTNER

Zbornik razprav in prispevkov v okviru 1. kolokvija Mediji v informacijski družbi

6. etični forum informacijske družbe: »Informacijska družba po Snowdnu«

Uredila:
dr. József GYÖRKÖS,
Marijana ZELENIK

Vrsta publikacije:
E-zbornik

Uredniški odbor:
dr. József GYÖRKÖS,
dr. Melita ZAJC,
dr. Smiljana GARTNER

Organizacijski odbor foruma:
Marijana ZELENIK,
Mojca VILIČNJAK,
Jan DOLAR,
Katarina MOHORIČ

Avtor fotografij:
Miha MATAVŽ

Oblikovanje:
Aljaž SAHORNIK,
Mojca VILIČNJAK

Izdajatelj:
Univerza v Mariboru,
Fakulteta za elektrotehniko računalništvo in informatiko,
2014

CIP - Kataložni zapis o publikaciji
Univerzitetna knjižnica Maribor

004:17

ETIČNI forum informacijske družbe (6 ; 2014)
Informacijska družba po Snowdnu (Elektronski vir) : (zbornik razprav in prispevkov v okviru 1. kolokvija Mediji v informacijski družbi) / 6. etični forum informacijske družbe (in) 1. kolokvij Mediji v informacijski družbi ; uredniki József Györkös, Melita Zajc, Smiljana Gartner. - El. zbornik. - Maribor : Fakulteta za elektrotehniko, računalništvo in informatiko, 2014

ISBN 978-961-248-452-1
1. Györkös, József 2. Kolokvij Mediji v informacijski družbi (1 ; 2014)
79315457

1. kolokvij
MEDIJI V INFORMACIJSKI DRUŽBI

6. ETIČNI FORUM INFORMACIJSKE DRUŽBE

INFORMACIJSKA DRUŽBA PO SNOWDNU

KAZALO

6. ETIČNI FORUM INFORMACIJSKE DRUŽBE

"INFORMACIJSKA DRUŽBA PO SNOWDNU"

MAG. FRANCI PIVEC

Filozof in sociolog, starosta informacijskih znanosti, zaposlen na IZUMu

DR. BORIS VEZJAK

Izredni profesor za zgodovino filozofije na Filozofski in Pedagoški fakulteti v Mariboru

DR. FRIDERIK KLAMPFER

Izredni profesor za filozofijo na Filozofski fakulteti v Mariboru

DR. MELITA ZAJC

Medijska raziskovalka, docentka na Inštitutu za medijske komunikacije

JASMINA MEŠIČ

Diplomantka programa Medijske komunikacije, zaposlena na ARNESu

DR. JÓZSEF GYÖRKÖS

Redni profesor na FERI, predsednik Svetovalnega odbora CONNECT pri Evropski komisiji

ŠTUDENTI MEDIJSKIH KOMUNIKACIJ

Študentska razprava po diskusiji in predstavitev najboljših prispevkov na temo informacijske družbe

UNIVERZA V MARIBORU
FAKULTETA ZA ELEKTROTEHNIKO, RAČUNALNIŠTVO IN INFORMATIKO
PREDAVALNICA G2-P01, 23.5.2014 OB 10:00

1. KOLOKVIJ MEDIJI V INFORMACIJSKI DRUŽBI

slovensko društvo informatika

Avtorji: Mojca VILIČNJAK, Katarina MOHORIČ, Zoran BENCAK

PROGRAM FORUMA

10.00 UVODNI POZDRAV

10.05 RAZPRAVA

Moderator: mag. Franci Pivec (IZUM)

Panelistke in panelisti:

dr. Melita ZAJC (UM FERI), dr. Boris VEZJAK (UM FF), dr. Frederik Klampfer (UM FF), Jasmina MEŠIČ (ARNES), dr. József GYÖRKÖS (UM FERI)

11.30 ŠTUDENTSKA REFLEKSIJA PANELA

Študenti poročevalci: Jan DOLAR, Aleksandra SELINŠEK, Mojca VILIČNJAK.

12.00 PREDSTAVITEV IZBRANIH ŠTUDENTSKIH PRISPEVKOV

Katarina Mohorič: SAMOPREDSTAVLJANJE ALI "SAMOUSTVARJANJE"?

Filip Gornik, Matjaž Koren, Jernej Primčič, Robert Ratajac: SAFETY@EMAIL.COM

Mitja Piko: SPLETNO VEDENJSKO OGLAŠEVANJE

Filip Vrečko: ZASEBNOST IN SPLETNA TRŽIŠČA

13.15 ZAKLJUČEK

UVODNIK

Namen izida zbornika s prispevki šestega etičnega foruma informacijske družbe je večplasten, saj poskuša povezati različne vede, kot so informatika, etika in medijske komunikacije ter hkrati zajema zelo različne avditorije, kot so študenti, predavatelji ter predstavniki širše javnosti.

Slovensko društvo informatika (SDI) v povezavi z drugimi ustanovami tradicionalno organizira etične forume informacijske družbe, skozi katere vsako leto naslavlja aktualne vsebine posledic razvoja informacijsko komunikacijskih tehnologij. V poglavju Etični forumi informacijske družbe skozi čas njihov organizator v okviru SDI Franci Pivec podrobneje razloži namen in dosedanji potek forumov.

Podnaslov letošnjega foruma je ob aktualnosti tudi delno provokativen. Kakšna bo informacijska družba »po Snowdnu«, namreč ni zgolj retorično vprašanje, temveč zahteva temeljni premislek o načinih uporabe interneta ter potrebi po redefiniciji nekaterih osnovnih konceptov onkraj tehnologije, kot so na primer zasebnost, zaupanje in etika nasploh. V poglavju Prispevki razpravljalcev se nahajajo iztočnice, ki so služile kot izhodišča razprave na dogodku dne 24. maja 2014. V razpravi, ki jo je moderiral Franci Pivec, smo nastopili Melita Zajc (UM FERI), Jasmina Mešić (Arnes), Friderik Klampfer in Boris Vezjak (oba UM FF) ter József Györkös (UM FERI). Središčni del dogodka je bila študentska refleksija razprave, ki je objavljena v posebnem poglavju in so jo pripravili študenti poročevalci Jan Dolar, Aleksandra Selinšek in Mojca Viličnjak.

V zadnjem delu zbornika so objavljeni referati, ki so jih študenti pripravili v okviru dejavnosti pri drugostopenjskem študijskem predmetu Koncepti in modeli medijev v informacijski družbi, ter prispevek skupine študentov pri predmetu Medijska etika prve stopnje študijskega programa Medijske komunikacije. Izbrani referati so bili predstavljeni tudi na samem dogodku v okviru foruma.

Zbornik je prvi v ciklu Kolokvijev o medijih v informacijski družbi. Tudi naslednji zborniki bodo izhajali v okviru študijskega predmeta Koncepti in modeli medijev v informacijski družbi na drugi stopnji študijskega programa Medijske komunikacije in bodo podobno, kot je bil letošnji vsebinsko povezan s predmetom Medijska etika, povezani z drugimi predmeti študijskih programov Medijske komunikacije ter Informatika in tehnologije komuniciranja.

dr. József Györkös, glavni urednik zbornika

KRATEK PREGLED PETIH ETIČNIH FORUMOV INFORMACIJSKE DRUŽBE

Organiziranja »etičnega foruma« smo se domislili v Sekciji za zgodovino in etiko računalništva pri Slovenskem društvu Informatika in sicer v povezavi s Svetovnim dnevom informacijske družbe, ki so ga v Generalni skupščini OZN leta 2006 določili za 17. maj. Za etični vidik smo se odločili, ker je ob očaranosti s tehniko očitno zapostavljen, enako problematično pa je, da se nanj najpogosteje sklicujejo tehnofobi, ki bi razvoj najraje prepovedali. Na tej podlagi je nastal koncept Etičnega foruma informacijske družbe (EFID).

Prvi EFID smo organizirali pod pokroviteljstvom predsednika Državnega zbora dr. Pavla Gantarja, ki je bil poprej naš prvi (in edini) minister za informacijsko družbo. Odvijal se je zgradbi parlamenta, v ponedeljek, 18. maja 2009. Zastavili smo si izjemno zahteven naslov »Zadostnost klasičnih etičnih teorij za razumevanje in moralno delovanje v informacijski družbi«. Čeprav smo zbrali zelo interdisciplinarno skupino razpravljavcev – dr. Pavel Gantar, dr. Jozsef Györkös, dr. Leo Šešerko, Niko Schlamberger, dr. Rafko Valenčič, dr. Danilo Pumpernik, mag. Franci Pivec, dr. Marjan Krisper – kar je izražalo našo namero navezave dialoga med tehniko, družboslovjem in humanistiko, se nismo dokopali do skupnih izhodišč. Vseeno je bil praktični rezultat dober, ker smo strokovno verificirali etični kodeks, ki ga SDI kasneje sprejelo kot svoj osnovni akt.

Drugi EFID je bil 17. maja 2010. na mariborskem Institutu informacijskih znanosti (IZUM), gostili pa smo znamenitega Dona Gottebarna, enega od očetov računalniške etike, ki je govoril o etiziranju v informacijski družbi kot tveganju zaradi pomanjkljive usposobljenosti informatikov. To je bil tudi uvod v mednarodno konferenco IFIP o temi »Converging Technologies: Body, Brain, and Being«, ki je tudi vključevala številne etične vidike informacijske tehnologije.

Tretji EFID je bil v Narodni in univerzitetni knjižnici (NUK), 17. maja in je bil posvečen temi »Etični vidiki uporabe IKT v visokem šolstvu«. Uvodna referata sta prispevala dr. Cvetka Toth o vrednotah svetovnega etosa, in mag. Franci Pivec o informacijski etiki v strateških dokumentih visokega šolstva in znanosti. Morda smo s tem prispevali, da o etiki prvič govorita obe veljavni strategiji visokega šolstva in znanosti.

Četrti EFID je bil 17. maja 2012. spet v IZUMU, posvečen pa je bil stoti obletnici rojstva očeta računalnika-univerzalnega stroja Alanu Turingu, ki ga je predstavil dr. Matjaž Gams.

Peti EFID je bil 17. maja 2013. spet v zgradbi parlamenta pod pokroviteljstvom predsednika Državnega sveta Mitje Bervarja. Tema je bila »Varovanje zasebnosti in nadzorovanje«, o čemer sta predavala dr. Aleš Završnik (Nadzorovanje vsakdanjega življenja) in mag Andrej Tomšič (nadzorovanje na delovnem mestu), kritično analizo pogostega pristajanja na kršitev zasebnosti z utemeljitvijo »nimam česa skrivati« pa je prispeval mag. Franci Pivec.

mag. Franci Pivec

ŽVIŽGAŠKA ETIKA IN MIMIKRIJA: MEDIJSKE REPREZENTACIJE IN NOVINARSKA ZLORABA

dr. Boris Vezjak, UM Filozofska fakulteta

Žvižgači so posamezniki, ki v nasprotju z interesi neke organizacije zunanjim javnostim razkrijejo nezakonita ali kako drugače nepravilna ravnanja organizacij, v katerih so zaposleni (Vernon-Wortzel, 1994).[1] Če je žvižgaštvo zaželena in hvalevredna etična praksa, če so njegovi akterji v družbi postali novodobni heroji, kot pravi Žižek (2013),[2] ponuja Slovenija dobre pravne pogoje za njihovo delo - leta 2010 sprejeti zakon o integriteti in preprečevanju korupcije regulira tudi to področje, Transparency International pa Slovenijo uvršča med štiri države v Evropski uniji glede na maksimalno pravno varnost posameznikov.[3]

Se je število prijaviteljev zaradi tega povečalo? Komisija za preprečevanje korupcije poroča o tem, da namesto enega do dveh primerov na leto zdaj prejmejo tri ali štiri opozorila. Čeprav protikorupcijska komisiji ščiti identiteto žvižgača, se prijave ne povečujejo bistveno, ker se potencialni žvižgači bojijo maščevanja in pritiskov, a so zaščiteni kot priče v sodnih procesih in prikrita je tudi njihova identiteta (Kečanović, 2013).[4] Na nemotiviranost vpliva dejstvo, da ob morebitni izgubi službe ne bodo deležni finančne podpre in da je geografska majhnost države tista, ki povečuje možnosti, da bodo v družbi hitro razgaljeni.

V slovenskih razmerah, ki bi morale biti ugodne, ima žvižgaštvo še dodaten problem: v prispevku želim opozoriti, da ne odpira le novih dilem etičnih presoj v navezavi z uporabo ali zlorabo informacijskih tehnologij, temveč tudi povsem nenavadno konceptualno zmedo v javnosti in samih novinarskih stanovskih združenjih, kdo natančno je žvižgač in kaj šteje za tovrstno prakso. Razkrivanje informacije, ki je v nasprotju z interesom organizacije, toda usklajeno z javnim interesom na način, da ponuja uvid v neko nezakonito in nepravilno delovanje ali zlorabo nekega predpisa ali zakona, korupcijo, grožnjo varnosti ali grožnjo zdravju, se velikokrat meša z institutom prikritega vira informacije – v novinarskih postopkih se tako dogaja, da je nek vir, ki nima etičnega cilja, označen za žvižgača in s tem apriorno opredeljen kot nekdo, ki je izvedel želeno dejanje, vendar njegova informacija bodisi nima narave javnega interesa, bodisi njegov cilj ni etičen, temveč npr. političen, prav tako pa je tudi reprezentacija »žvižgača« s strani novinarja postala instrumentalizirana za neke druge potrebe.

Etična dilema žvižgača je vedno tudi njegova osebna, saj bo z objavo podatka o nepravilnosti v organizaciji tvegal svojo službo, zaradi česar je največkrat podvržen fenomenu »čebeljega žela« (ko uporabi želo, je z njim konec, tj. konec je njegove karierne poti). Če je zasebno vedno razcepljen med lojalnostjo organizaciji, varnostjo službe in etičnim »acting out«, ki od njega terja žrtvovanje imenu informiranja javnosti in ustrezno prepoznanje v podobi »etičnega subjekta«, pa njegovo ravnanje ni imuno na novinarske zlorabe. Domači primer preiskave na domu obrambnega ministra je pokazal: če novinar s pomočjo žvižgača razkrije napovedano policijsko preiskavo na domu ministra, s tem pač ni razkril nobenega nezakonitega dejanja. Vpeljala žvižgaške hermenevtike v novinarsko zgodbo o tem je pokazala, da je nekdo narobe interpretiral kar tri pojme: pojem žvižgača, pojem javnega interesa in pojem anonimnega novinarskega vira, če je prišlo do takega sklicevanja. Tudi v slovenski novinarski praksi se potemtakem že dogaja, da pod plaščem zaščite žvižgača nekritično odpiramo prostor novinarskemu pisanju, kjer namesto sledenja javnemu interesu prihaja do zlorab za potrebe senzacionalističnega in tabloidnega pisanja, s čimer je novinarska argumentacija prešla v funkcijo mimikrije nekega drugega, bistveno manj etičnega diskurza.

Prav takšen je bil primer novinarke Damijane Žišt, ki se je na dan hišne preiskave 11. decembra 2013 skupaj s fotoreporterjem Večera znašla pred hišo obrambnega

1 Vernon-Wortzel, Heidi (1994): Business and Society, A Managerial Approach-Fitth Edition, Prentice-Hall, Richard D. Irwin, Inc., Illinois.

2 O evforičnih opisih žvižgačev primerjaj zapis Slavoja Žižka v Guardianu 3.9.2013: http://www.theguardian.com/commentisfree/2013/sep/03/snowden-manning-assange-new-heroes

3 Poročilo Transparency International je dostopno na tem naslovu: http://www.integriteta.si/images/WB/eu_report_final_web.pdf

4 Citirano po novinarskem prispevku: http://www.24ur.com/novice/slovenija/moras/biti/pripravljen/vracati/udarce.html?bl=0

ministra Romana Jakiča. Zato, ker je od svojega vira izvedela, da bo do preiskave prišlo in kdaj se bo to zgodilo – namreč zaradi domnevne zlorabe položaja v času, ko je bil še direktor Zavoda Tivoli. Skupaj s fotoreporterjem je prispela petnajst minut pred policisti. Ko se je Jakič kot minister vrnil iz tujine, se je odločil zaradi odtekanja informacij podati ovadbo zoper neznanega storilca. Ob tem je javno osumil nekoga iz vrst policije, tožilstva ali sodišča. Žištova se je odločila, da svojega vira, ki ji je zaupal preiskavo pri Jakiču, ne bo izdala. V javnih nastopih je napovedala, da novinarji svoje vire ščitijo. In ceh ji je pritrdil ter jo podprl, razpravo pa sprevrnil v moralno dejanje žvižgača, ki ga mora novinar zaščititi.

Ob tem se je novinarka sklicevala na osmi člen Novinarskega kodeksa, ki pravi: »Novinar se z virom informacij, ki ga sicer lahko identificira, lahko dogovori za zagotavljanje anonimnosti. Takšen vir lahko uporabi le, če informacij ni mogel pridobiti na drug način, objava pa je v javnem interesu. Novinar je dolžan spoštovati dogovor o anonimnosti vira.«[5]

Dilema tukaj sploh ni bila, ali bi novinarka morala ali ne ščititi svoj vir. Pravo vprašanje temu predhodi in je, ali je njegova uporaba bila utemeljena. Iskanje anonimnega novinarskega vira je po moje smiselno le, če so podatki, ki jih ta ponuja, v interesu javnosti in če je ta vir nujen za to, da omogoči informacijo, ki je v javnem interesu. Če nam vir ponuja že itak dostopen javni podatek, je iskanje anonimnega vira in kasneje sklicevanje nanj pod vprašajem. Novinarka je torej svoj vir uporabila, da ji je povedal nekaj, kar mora biti in je javno dostopno. Za nekaj, o čemer so potem tisti dan poročali vsi mediji in ona je najbrž dobro vedela, da bodo.

O tem govori tudi citirani osmi člen, ki zapoveduje, da »takšen vir lahko uporabi le, če informacij ni mogel pridobiti na drug način« – če je informacija o preiskavi v hiši politiki javni podatek, potem temu pogoju zelo evidentno ni zadoščeno. Da je tu javni interes izkazan, ni dvoma. Sklicevanje na vir je potemtakem bilo manipulacija. Seveda ne pravim, da bi svoj vir morala razkriti, trdim le, da je v danem primeru prišlo do njegove neupravičene uporabe in sumljivega sklicevanja nanj.

5 Ob tem se sklicujem predvsem na nastop novinarke v oddaji Odmevi, 6.1.2014. Oddaja je dostopna na naslovu: http://ava.rtvslo.si/predvajaj/odmevi/ava2.174255087/

Če je informacija, o kateri govorimo, javnega značaja in bi v vsakem primeru prišla v javnost, se resnično postavlja vprašanje smiselnosti sklicevanja na anonimni vir. Zaščita novinarskih virov je absolutno pomembna in nesporna, toda kaj se je zgodilo v slovenskem primeru? Iz nekega razloga je bil ta institut povsem napačno uporabljen ali zlorabljen.

1. Novinarka ni imela nobenega pametnega razloga za sklicevanje na skriti vir, ker podatek, ki ga je ta prinesel, ni bil v nikakršnem posebnem interesu javnosti. Podatek o policijski preiskavi na domu nekega ministra ne izpolni tega kriterija. Celo novinarka sama je priznala, da je odredba o preiskavi javen podatek, pravnik dr. Andraž Teršek je govoril o informaciji javnega značaja. Za kršenje zakona mora biti podan dober razlog in tu ga res ni bilo.
2. V skladu z definicijo žvižgača novinarkin vir ne izpolnjuje te kvalifikacije. Njegovo ravnanje ne moremo opisati kot ravnanje razkrivanja nezakonitosti in nepravilnosti v neki organizaciji. Sklicevanje na žvižgače je povsem neutemeljeno.

V polnem pomenu torej nismo imeli ne žvižgača, ne izkazanega javnega interesa in ne razloga po sklicevanju na anonimni vir. Nimamo dobrega razloga domnevati, da bi informacija o policijski preiskavi na domu ministra Jakiča v javnosti ostala brez »žvižgača« kakorkoli spregledana.

Pojem žvižgaštva je torej bil zlorabljen in vsaj napačno interpretiran – tako s strani novinarke, s strani novinarskih druženj, s strani strokovnjakov. Verjetno se je pod pretvezo zaščite novinarskih virov in sledenja javnemu interesu promoviralo senzacionalistično in tabloidno pisanje, ekskluzivno poročanje z mesta dogodka, s čimer bi se prehitelo medijsko konkurenco. V tem smislu smo imeli priložnost videti, kako je bila ena zelo redkih razprav o žvižgaštvu v slovenskem javnem prostoru interpretirana povsem napačno, kar bi nas, glede na standarde novinarske profesionalizma, moralo resno skrbeti.

ZAUPANJE JE SREBRO, NADZOR JE ZLATO

dr. Friderik Klampfer, FF UM

Eno leto mineva, kar sta britanski The Guardian in ameriški The Washington Post pričela z razkrivanjem gosto spletene mreže nadzora. Članki so temeljili na tajnih dokumentih, ki jih je novinarjem teh dveh časnikov v Hong Kongu izročil takrat 30-letni pogodbeni sodelavec Ameriškega urada za nacionalno varnost (NSA) Edward Snowden.

Kaj so odtujeni tajni dokumenti sploh razkrili? Ocene nihajo od zavajajoče pomirljivih »nič takega, česar ne bi že dolgo vedeli« do histeričnih »najgloblje, najbolj skrbno varovane skrivnosti o škodljivem (oz. koristnem, odvisno od politične perspektive) podtalnem delovanju vlade in vladnih ustanov«. Ed Snowden je tako za ene nevaren fantast, ki je v trenutku slabosti ali zaradi slabe presoje postavil na kocko obstoj svoje domovine, za druge narodni izdajalec (ali celo prikrit ruski ali kitajski agent), in za tretje osamljeni, idealistični junak, ki je bil pripravljen žrtvovati lastno dobrobit za skupno dobro.

Ali je po letu dni, potem ko so se ohladile pregrete strasti in so se iz megle oblastnih klevet in manipulacij prikazali grobi obrisi dejstev, morda že čas za moralno sodbo o Snowdnovem ravnanju? Za preliminarno gotovo, dokončna bi bila še preuranjena. Prvič, doslej je bil objavljen le majhen del obremenjujočih dokumentov in čeprav je podoba ravnanja in še bolj ambicij oblasti, ki jo ti slikajo, vse prej ko pomirjujoča, je težko oceniti, koliko eksplozivnega gradiva, še bolj pa za nacionalno varnost škodljivih informacij bi se utegnilo skrivati v še neobjavljenih dokumentih. Ker manjka tudi drugi del enačbe, kolikor toliko verodostojna in nepristranska ocena koristi od vsesplošnega nadzora, je nemogoče oceniti, ali je tako drastičen poseg v pravico ljudi do komunikacijske zasebnosti izpolnjeval običajna moralna merila – skratka, ali je bil neizogiben, učinkovit in sorazmeren. Še o tem, ali je brezciljni, sodno neodobren nadzor nad komunikacijami sploh zakonit, si strokovnjaki niso edini! Še najmanj neznank je, se zdi, v zvezi s Snowdnovimi motivi – vtis je, da ga je k odločitvi, da prelomi obljubo o varovanju zaupnih podatkov, napeljala iskrena skrb za vrednote in načela, utelešena v ameriški ustavi, in skoraj naivna vizija svobodnega, tj. nadzora in zakonodajnih spon osvobojenega spleta.

Veliko lažje je s časovne distance odgovoriti na nekatera druga, nič manj pereča vprašanja. Za katera dragocena spoznanja smo po Snowdnovi zaslugi bogatejši? Tu je samo nekaj najosnovnejših: (a) vladni nadzor nad elektronsko komunikacijo je v času od 11. septembra in pod pretvezo vojne proti terorizmu dobil orwellovske razsežnosti; (b) krivdo za to gre najprej iskati v ohlapnih zakonskih določilih, ki vladnim ustanovam omogočajo, da kar se da velikodušno tolmačijo pooblastila, ki jim jih daje pogosto (napol) tajna, kritični javnosti nedostopna zakonodaja; nato v izrazito pomanjkljivem sodnem in parlamentarnem nadzoru nad delovanjem tajnih služb, v prvi vrsti ameriške NSA in britanske GCHQ (ta, se zdi, je v končni fazi odvisen izključno od samonadzora in samoomejevanja političnih in uradniških elit); in končno v servilnosti zasebnih korporacij, ki smo jim uporabniki interneta na stežaj odprli vrata do naših preferenc, misli in navad, do radovedne oblasti; c) posegi v komunikacijsko zasebnost ljudi v imenu zaščite pred teroristično grožnjo so drastični in sistematični (tudi če bi verjeli oblastem, ko nam zagotavljajo, da o komuniciranju zbirajo in analizirajo le t.i. meta-podatke), hkrati pa jim manjka minimalna demokratična legitimnost; d) na prepletu vzporedne izvršne in sodne oblasti, podtalne, ustavno in z vidika človekovih pravic in svoboščin problematične zakonodaje, pomanjkljivega demokratičnega nadzora (»checks and balances«) in čedalje cenejše tehnologije nadzora nastaja demokratični deficit, ki počasi ogroža same temelje demokratičnega sistema in procesa.

Ali ni pozivanje na barikade v obrambo komunikacijske zasebnosti v svetu, kjer uporabniki spleta zasebnim podjetjem vsakodnevno in brez posebnih zadržkov predajamo gore osebnih podatkov v zameno za drobtinice komunikacijskega udobja, nekoliko naivno? Toda kot v svoji analizi v časniku The Guardian pravilno ugotavlja pisatelj John Lanchester, da dovoljujemo Googlu in Facebooku zbirati osebne podatke o nas za komercialne namene, še ne pomeni, da smo dovolili do teh

podatkov dostopati tudi vladam, kadar koli jih te potrebujejo pod pretvezo zaščite državljanov pred bolj ali manj namišljenimi grožnjami. Pravica do komunikacijske zasebnosti je elementarna in univerzalna, odpoved taki pravici pa ne more biti ne implicitna in ne vsesplošna, temveč v najboljšem primeru eksplicitna in individualna. Snowdnova kalvarija pred očmi svetovne javnosti pa je razkrila še nekaj, namreč moč in vpliv ZDA ter sramotno klečeplazenje evropskih držav – v prvi vrsti Italije, Francije in Španije, ki so letalu z bolivijskim predsednikom Moralesom na krovu na zahtevo ZDA prepovedale vstop v svoj zračni prostor, ter Avstrije, ki je po prisilnem pristanku na Dunaju letalo preiskala, pa tudi vseh tistih več kot dvajset držav, ki so Snowdnu s prozornimi formalnimi izgovori zavrnile prošnjo za politični azil.

Podobno kot ocene o prelomnosti Snowdnovih razkritij so protislovne tudi ocene o njihovih posledicah. Te segajo od paranoičnih svaril o povečanem tveganju za teroristične napade do ciničnih napovedi, da se iz glasnega zgražanja in javnega moraliziranja itak ne bo izcimilo nič konkretnega: »psi lajajo, karavana pa gre naprej«. A z vdajo cinizmu bi naredili medvedjo uslugo začeti javni razpravi o dopustnih mejah oblastnega vdiranja v življenja ljudi in še sprejemljivih moralnih tveganjih. In ta razprava se je v zadnjem letu dni dodobra razmahnila. 500 uglednih intelektualcev iz 81 držav sveta je v javnem pismu pozvalo ZN k sprejemu nove Deklaracije o človekovih pravicah in svoboščinah v digitalni dobi. Osem ameriških multinacionalk, od Applea, Googlea, Microsofta in Facebooka do Yahooja, LinkedIn-a, Twitterja in AOL-a, je predsednika Obamo in ameriški kongres pozvalo k nujni spremembi zakonodaje, ki dopušča vsesplošen, ne-selektiven nadzor svetovnih komunikacij, da bi na ta način ohranili vse bolj načeto zaupanje javnosti v svetovni splet. Kot ugotavlja Brad Smith iz Microsofta, enega od podpisnikov pisma: "Ljudje ne bodo uporabljali tehnologije, ki ji ne zaupajo. Vlade so to zaupanje spodkopale in zato je njihova naloga, da ga ponovno vzpostavijo." Ena od osrednjih zahtev se zato glasi: vlade naj omejijo komunikacijski nadzor na posamezne, točno določene uporabnike, za katere obstaja utemeljen sum, da kršijo zakone oz. ogrožajo javno varnost (ali pa to vsaj naklepajo), in se odrečejo vsesplošnemu, neselektivnemu zajemanju podatkov o spletni in drugi elektronski komunikaciji. Pritisk svetovne javnosti se, skratka, bliža vrelišču in težko si je predstavljati – še zlasti, ker je zdaj na tehtnici tudi 'ultimativna vrednota', namreč komercialni interesi ameriških internetnih gigantov – da bi javna razprava o dopustnosti vohunjenja oblasti za svojimi državljani dirigirano ali zaradi pomanjkanja zanimanja javnosti nenadoma zamrla.

Edwardu Snowdnu smo lahko hvaležni, da je s svojim junaškim dejanjem sprožil prepotreben javni razmislek o tem, kje smo in kam gremo. Sodobna tehnologija nadzora ponuja državnim organom (pa tudi, nikar ne pozabimo, zasebnim korporacijam) moč in oblast, kot ju ta v zgodovini človeštva še ni imela, zato je javna, demokratična razprava o mejah, ki jih ta v svoji, če smo dobronamerni, hvalevredni skrbi za nacionalno varnost ne bi smela prestopiti, več kot nujna. Vlade, nas opozarja Snowden, so že zdavnaj prenehale zaupati svojim državljanom. Skrajni čas je, da jim vrnemo z enako mero.

NOVE DILEME ZADRŽEVANJA PODATKOV O PROMETU

dr. József Györkös

PODATKI O NAŠIH KOMUNIKACIJA

Direktiva o zadrževanju podatkov o elektronskih komunikacijah narekuje hranjenje podatkov o prometu (npr. kdo je klical koga, kdaj in od kod), do katerih lahko na podlagi sodnih nalogov dostopajo organi pregona. Direktiva je v okviru Evropske komisije začela nastajati kmalu po zaostrenih nadzornih dejavnostih ZDA po enajstem septembru 2001, priprave pa so dodatno spodbudili takratni teroristični napadi na evropskih tleh (London, Madrid). Direktiva je sprva bila načrtovana za olajšanje naknadnega preiskovanja terorističnih dejanj, vendar je bila ta omejitev pri njeni kasnejši implementaciji leta 2006 razširjena na hujša kazniva dejanja nasploh, kar je tudi eden izmed ključnih razlogov, da je direktivo Sodišče Evropske unije leta 2014 razveljavilo oz. izničilo. Ne glede na to nacionalni zakon o elektronskih komunikacijah v delu, kjer implementira to direktivo, še vedno velja.

OZADJE

Direktiva o zadrževanju oz. hranjenju podatkov o elektronskih komunikacijah (t. i. Podatkov o prometu)[1] je stopila v veljavo leta 2006. S takratno spremembo Zakona o elektronskih komunikacijah (ZEKom) je bila prenešena v pravni prostor Republike Slovenije. Na začudenje širše javnosti je zakonodajalec sprejel najdaljši možni rok hranjenja podatkov o prometu, in sicer dve leti, čeprav direktiva v šestem členu navaja možnost hranjenja podatkov od šestih mesecev do dveh let in odločitev prepušča posameznim državam članicam. Leta 2009 je Državni zbor RS na predlog vlade oziroma takrat pristojnega Ministrstva za visoko šolstvo, znanost in tehnologijo skladno s programom vlade in tudi na podlagi civilnodružbenih pobud rok hrambe skrajšala, in sicer na 14 mesecev za podatke v zvezi s telefonskimi storitvami in 8 mesecev za druge (podatkovne storitve). V medresorskih usklajevanjih dodatnih skrajšanj ni bilo mogoče doseči, saj so organi pregona sklicevali na dolgotrajnost postopkov, v smislu zaznave potrebe po dostopu do teh podatkov.

1 Skrajšano ime direktive se glasi Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, številka 2006/24/EC

RAZVELJAVITEV

Na spornost direktive v smislu prekomernega poseganja v zasebnost je dalj časa opozarjalo kar nekaj držav članic EU, ki direktive niso želele implementirati v lastnem pravnem prostoru. Sodišče Evropske unije je dne 8. aprila 2014 direktivo o hrambi podatkov razglasilo za neveljavno[2], saj »pomeni širok in posebno hud poseg v temeljni pravici do spoštovanja zasebnega življenja in do varstva osebnih podatkov« in svojo odločitev razložilo v treh sklopih (prvič, direktiva preveč na splošno pokriva vse posameznike, sredstva in podatke brez razlikovanja, omejitve ali izjeme glede na cilj boja proti hudim kaznivim dejanjem; drugič, zagotovilo, da pristojni nacionalni organi dostopajo do podatkov in jih uporabljajo le za namene preprečevanja, odkrivanja in pregona kaznivih dejanj, je pomanjkljivo; tretjič, direktiva ne pojasnjuje objektivnih meril, na podlagi katerih je treba določiti obdobje hrambe, da bi bilo to omejeno na najnujnejše).

DILEMA

Pri razveljavitvi direktive nedvomno gre za velik dosežek in pritrditev zahtevam civilne družbe ter tudi naporom Informacijskega pooblaščenca v Republiki Sloveniji, ki je že pred tem na ustavno sodišče vložil zahtevo po presoji ustavnosti[3]. V po-snowdnovski razpravi pa si na etičnem forumu informacijske družbe lahko drznemo tudi naslednji razmislek: mar niso člani o hrambi podatkov zaradi jasne zakonske opredeljenosti glede načina hrambe in pravic dostopa ter parlamentarnega nadzora predstavljali varovalko pred posegi organov pregona, ki bi presegali mejo upravičenosti? Mar se bodo ob skorajšnji razveljavitvi članov pojavili novi in manj transparentni načini pridobivanja podatkov o prometu? Snowdnova razkritja govorijo o dejavnosti obveščevalnih služb, ki jim kot vir pridobivanja informacij služijo sredstva elektronskega komuniciranja, zakonodaja o elektronskih komunikacijah pa teh ne naslavlja. Ali to pomeni, da je bil fokus javnosti glede posegov v osebne podatke o elektronskih komunikacijah ves čas usmerjen v napačen cilj? In nenazadnje, ali je o po-snowdnovskem krasnemu novemu svetu sploh možno razmišljati zgolj na evropski ali celo nacionalni ravni?

2 Sporočilo za javnost Sodišča Evropske unije

3 Urad informacijskega pooblaščenca RS: zahteva za oceno ustavnosti in zakonitosti členov ZEKom-1, ki se nanašajo na hrambo podatkov

INFORMACIJSKA DRUŽBA PO SNOWDNU

Jasmina Mešić, Arnes

Nekaj dni po samorazkritju Edward Snowden, žvižgač, ni obžaloval svojega dejanja. Novinar Washington Posta ga je v intervjuju[1] vprašal (podvomil), če resnično verjame, da bo javno razkritje sistematičnega in množičnega prestrezanja elektronskih komunikacij s strani ameriške varnostne agencije NSA kaj spremenilo. Snowden je zatrdil: »Mislim, da so se stvari že spremenile. Sedaj vsi razumejo, kako resna je situacija – in o tem tudi govorijo. Sami (uporabniki, op. p.) imajo moč, da se odločijo, ali so družbi nadzora pripravljeni žrtvovati svojo zasebnost.« Nekoliko naivna izjava za računalniškega strokovnjaka, ki je dodobra spoznal drobovje sistema PRISM.

Če se po slabem letu od velikega poka ozremo nazaj, dlje od govorjenja nismo prišli. Od nas, spletnih uporabnikov, je odvisno bore malo, naša moč samoodločanja je zreducirana zgolj na to, pri katerem oblačnem velikanu, lociranem v ZDA, bomo na strežniku najeli digitalni fevd in posledično tudi žrtvovali del svoje zasebnosti. Pa ne le v kontekstu delovanja varnostno-obveščevalnih agencij, ki so se z absolutnim argumentom nacionalne varnosti vedno postavile nad pravico državljana do zasebnosti. Tovrstna razkritja še vedno dvignejo največ medijskega prahu. Na drugi strani pa neopazno in brez spremljajočega pompa sprejemamo splošne pogoje, s katerimi prikimamo avtomatiziranim sistemom, da analizirajo vsebino naše elektronske pošte in temu primerno prikazujejo relevantne oglase. Strinjamo se, da si družbeno omrežje lasti vse naše naložene fotografije, budilki na pametnem telefonu dovolimo dostop do celotnega imenika in shranjenih fotografij. Deloma smo uporabniki sami pristali na vlogo »targetirane javnosti«, v kateri globalna visokotehnološka podjetja vidijo le kup demografskih in geolokacijskih podatkov, ki so dobro unovčljiva. Ker je tako bolj udobno, zabavno, priročno, družabno, predvsem pa brezplačno. Proti brezplačnosti se je težko boriti, argument brezplačnosti je močan skoraj toliko kot argument nacionalne varnosti. Ampak, še vedno velja – če je na internetu nekaj zastonj, potem smo blago mi.

1 http://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html.

Uporabniki prevzamemo del krivde, da smo se odpovedali delu zasebnosti, vendar pa ne moremo spregledati dejstva, da smo na pravila nove informacijske ekonomije bili prisiljeni pristati, saj prave alternative ni. Med vzemi ali pusti izberemo vzemi, saj bi pusti pomenilo, da dobesedno zapustimo to informacijsko avtocesto, saj je skoraj nemogoče uporabljati informacijska orodja in hkrati v celoti živeti koncept zasebnosti. Digitalni priseljenci o tem še problematiziramo, danes odraščajoči digitalni domorodci se od svoje prve Facebook objave »prvi sprehod, prvič na kahlici« s tem verjetno ne bodo pretirano obremenjevali. Konec leta 2013 je Snowden v svoji alternativni božični poslanici napovedal, da otrok, ki se je rodil danes, ne bo poznal koncepta zasebnosti, kot pravi: »Nikdar ne bodo izvedeli, kako je videti trenutek zasebnosti – misel, ki ni posneta in analizirana.«

Izziv, kako vzpostaviti novo ravnotežje med našimi informacijskimi pravicami, kamor gotovo sodi pravica do zasebnosti, interesi globalnih IKT korporacij, ki so pogosto gibalo razvoja in vedno prisotno željo države po nadzoru, verjetno ni edini. Čakajo nas – informacijsko pismene 2.0 državljane, še druge, včasih nasprotujoče si dileme. Zakaj smo v nenehno povezani družbi sami (alone together)? Kam bomo umestili Internet stvari (IoT), kako bomo obvladali omrežen hladilnik, če še pametnih naprav nismo dobro osvojili?

Jasmina Mešić je zaposlena na Arnesu in je koordinatorka nacionalnega programa ozaveščanja javnosti o informacijski varnosti, ki poteka pod imenom Varni na internetu.

TRANSFORMACIJE INFORMACIJSKE DRUŽBE: POSAMEZNIKI IN ZGODOVINA

dr. Melita Zajc, UM FERI

TEZA

»Ko delamo z računalniki, je tako, kot da bi šli v kino, in bi morali gledati projektor namesto filma,« je leta 1996 dejala Brenda Laurel. Ta nekoč znameniti citat dobro pojasni trenutno situacijo. V tridesetih letih, ki so minila, so tehnični pogoji informacijske družbe za uporabnika postali nepomembni - podobno kot projektor v kinu.

Konstrukcija tehničnega sistema je dokončana, ko tega sistema ne opazimo več. Ko deluje kot črna škatla. Danes so računalniki – metaforično rečeno - povsod, vendar jih ni nikjer. Tehnološki pogoji informacijske družbe so zanikani, množijo se vsebine. Vsebina je edina važna (Content is King[1]), pravijo oglaševalci, uredniki, novinarji, in uporabniki, ki so veseli, ker se jim ni treba več ukvarjati s kabli in kodeki. Vendar, kot opozori Lev Manovich, je pri digitalnih medijih – ki so numerično reprezentirani in jih je mogoče algoritemsko spreminjati – torej, pri teh medijih je tehnološki del že tudi kulturni del. Dejstvo, da uporabniki ne kontroliramo več tehničnega dela, prinaša lahkotnost uporabe, a tudi izgubo nadzora nad uporabo. Bistvena značilnost informacijske družbe po Edwardu Snowdnu je, da se tega postopoma začenjamo znova zavedati.

DVA MEJNIKA

Kritičarka interneta Astra Taylor je spremembo, ki jo je s seboj prineslo razkritje Eda Snowdena o nadzoru spletnih komunikacij, opisala tako: »Internet se je čez noč spremenil iz politično osvabajajočega medija arabske pomladi v orjaško vohunsku napravo.« Njena teza je, da je pred tem v spletnih in mobilnih komunikacijah vladala svoboda, zdaj pa vlada nadzor.

1 Denis Oštir, novinar POP TV, na okrogli mizi v okviru 22. Slovenskega oglaševalskega festivala, 21.marca 2013.

Vendar je to odvisno od perspektive. Mnogi strokovnjaki opozarjajo, da je Snowdnovo odkritje predvsem simbolnega pomena – podobno, kot deček v zgodbi Cesarjeva nova oblačila, je glasno povedal – dokazal - kar smo vsi takoalitako vedeli. Izguba interenta kot prostora svobode je bistveno povezana z dvemi dogodki, ki sta se zgodila desetletje pred tem.

Prvi je napad na stolpa Svetovnega trgovinskega centra 11. Septembra 2001.
Drugi je – skoraj sočasno - razblinjenje tako imenovanega dot-com mehurčka. Torej, nasprotno od pričakovanj, da bodo delnice informacijskih podjetij prinesle orjaške dobičke, so druga za drugo izgubljale vrednost. Oba dogodka sta pomenila konec optimističnih pričakovanj v zvezi z internetom. Civilna družba se je nadejala več možnosti javne komunikacije, in splošno širitev državljanjskih pravic in svoboščin. Ekonomija si je nadejala izjemnih finančnih zaslužkov.

Posledice niso bile za vse enake. Grožnja terorizma je omogočila širitev vseh možnih strahov, posledično pa željo po varnosti – torej večjemu nadzoru in krčenju državljanjskih pravic in svoboščin. Obenem pa so, v okviru ekonomije, ti isti mehanizmi nadzora postali tudi glavni vir dobička.

Pesimistična ugotovitev, ki iz tega izhaja – da pravice in svoboščine, ki jih jamči demokracija, niso pogoj za ustvarjanje dobička – je najverjetneje tudi razlog, zakaj Snowdnovo odkritje ni prineslo večje spremembe. Poudarek razvoja rab računalnikov, se je že pred tem prestavil s svobode k nadzoru. Programiranje kot način ustvarjanja spletnih vsebin so nadomestile že izgotovljene predloge, družbeni mediji so bistveno olajšali komuniciranje – a možnosti so bile s tem jasno zamejene. Ob tem pa so se razvili tudi učinkoviti poslovni modeli.

PROJEKCIJA

Bali smo se elit, ki so uravnavale vsebine starih medijev, a dejansko bi se morali bati ekonomskih elit. Edward Snowden je pokazal, da so nevarne tudi politične elite. Vendar kaže biti previden. Tudi predstave o hudobnih ljudeh, ki stojijo v ozadju in vlečejo niti, so del kulture strahu, zaradi katere smo se pripravljeni odreči svobodi, v imenu varnosti.

Izgubljamo svobodo – ki pa smo se ji v prvi vrsti odrekli sami, ko smo se – rade volje – odrekli možnosti, da pri informacijsko komunikacijskih tehnologijah poznamo tudi tehnologije: projektor, ne samo filma.

BIBLIOGRAFIJA

Lovink, G. 2012. Networks Without a Cause: A Critique of Social Media, Cambridge and Malden: Polity.

Manovich, L. 2002. The Language of New Media. MIT Press.

Sigaut, F. 2002. Technology. V Companion Encyclopedia of Anthropology, ur. Tim Ingold. London in New York: Routledge.

Timberg, S. 2014. Astra Taylor's Radical Internet Critique: "I Don't Want to Give in to the Libertarian Logic of Our Time". Salon.com, 4. maj. Dostopno na http://www.alternet.org/visions/astra-taylors-radical-internet-critique-i-dont-want-give-libertarian-logic-our-time (obnovljeno 30.6.2014)

Zajc, M. 1996. Hitri avtomobili, trdi zvoki: medij v mediji ali neznosna bližina razdalje. V Medij v Mediju, ur. Vanesa Cvahte, Ljubljana: SCCA. Dostopno na http://www.ljudmila.org/scca/mvm/sf_mel.htm (obnovljeno 30.6.2014).

6. etični forum o informacijski družbi je zbral strokovnjake s področja medijev in odprl živahno debato o varnosti in zasebnosti posameznikov pri uporabi informacijskih tehnologij. Glavna polemika je bila, koliko lastne zasebnosti lahko ob uporabi spleta in ostalih informacijskih tehnologij zadržimo zase, oziroma, ali jo sploh še lahko.

Kadar želimo aktivno sodelovati v družbi informacijskih tehnologij, smo v izdajanje svojih osebnih podatkov praktično prisiljeni, je na forumu izpostavila Jasmina Mešić, koordinatorka nacionalnega programa o ozaveščanju javnosti o informacijski varnosti na ARNES-u. Absolutna zaščita zasebnosti bi namreč pomenila popolno izogibanje spletu – na primer družabnim omrežjem (Facebooku, Twitterju,…), uporabi spletne pošte, pametnim telefonom itd., kar pa dandanes najverjetneje niti ni več mogoče. Z dobro ozaveščenostjo pa lahko le delno zaščitimo svojo zasebnost.

Razmišljanje o zasebnosti in spletu nas je napeljalo k dvema tezama o prihodnosti: mlajše generacije sčasoma svojih podatkov, ki jih dandanes večinoma želimo zaščititi pred javnostjo, morda niti ne bodo več smatrale za zaupne in problem zasebnosti utegne morda celo zbledeti? Drugo skrajnost dane situacije pa bi lahko v prihodnosti predstavljala popolna odsotnost nadzora nad vdori v zasebnost, kar bi le-to naredilo še bolj problematično.

Trenutno se naša družba s temi dilemami spoprijema z ozaveščanjem javnosti. Mag. Franci Pivec, svetovalec direktorja IZUM, ter moderator 6. etičnega foruma o informacijski družbi, poudarja, da je le znanje tisto, ki nam - kot uporabnikom tehnologije - daje največjo moč, zato je najpomembneje, da tehnologije, ki jih uporabljamo, čim bolje poznamo in spremljamo spremembe na področju varovanja zasebnosti ter se o njih pravočasno in ustrezno informiramo.

Poleg ozaveščanja ima pomembno vlogo pri varovanju zasebnih podatkov zakonodaja. A ta je, kot smo se z dr. Józsefom Györkösom, profesorjem na Fakulteti za elektrotehniko, računalništvo in informatiko (UM FERI), pogovarjali že na njegovih predavanjih, vedno korak za tehnologijo. Menimo torej, da utegne zakonodaja, ki regulira področje zasebnosti uporabnikov informacijskih tehnologij, sčasoma najti optimalnejši način reševanja problematike od trenutnega, ki ga je prisotnim na forumu podrobneje pojasnil dr. Györkös. Trenutno je pri nas to precej občutljiva tema, saj smo aprila letos razveljavili Direktivo o zadrževanju podatkov o elektronskih komunikacijah zaradi kršenja zasebnosti. Neopredeljenost oziroma nenehne spremembe na tem področju morda kažejo na lastno labilnost in hkrati kličejo po boljšem naslavljanju problema zasebnosti.

Tudi dr. Melita Zajc, docentka na UM FERI, je kot enega izmed ključnih problemov izpostavila slabo poznavanje ali nepoznavanje tehnologij. Ljudje zelo radi uporabljamo vse sodobne naprave, kako le-te delujejo pa nas žal premalokrat zanima. Žvižgač Edward Snowden je po njenem mnenju opozoril točno na to - da smo nadzor nad uporabo tehnologij že izgubili - česar nikakor ni mogoče zanikati. Afera Snowden nas je opozorila, da imajo agencije, kot je NSA, omogočen dostopa do zasebnih podatkov posameznikov. Po besedah dr. Friderika Klampferja s Filozofske fakultete Univerze v Mariboru (UM FF), so se ob tem razkritju pojavila vprašanja o moralnosti delovanja žvižgačev, saj naj bi ti kot zaposleni v nekem podjetju morali delovati v korist podjetja in ne v njegovo škodo, četudi je delovna praksa podjetja moralno in/ali etično sporna. Medtem ko dr. Vezjak, prav tako profesor na UM FF, opozarja, da so zaradi t. i. »družbeno koristnega dela«, ki ga opravijo žvižgači, le -ti postali v javnosti in medijih precej priljubljeni. Posledično naj bi se pojem žvižgača izrabljalo oziroma namenoma nenatančno uporabljalo. Tako dr. Vezjak omenja primer slovenske novinarke, ki je za žvižgača neupravičeno označila svoj anonimni vir, ki ji je posredoval informacije, s katerimi je lahko pripravila tabloiden in senzacionalen novinarski prispevek. Ravno zaradi tovrstnih zlorab je nujno, da je javnost dobro seznanjena s pojmom žvižgača in tako lažje sama presodi, ali ga mediji sploh pravilno in upravičeno uporabljajo.

Ob tem se nam poraja še vprašanje, koliko je delo novinarjev sploh še etično, oziroma ali novinarska etika sploh še obstaja, ali je le nedosežen ideal, katerega so že zdavnaj premagali senzacionalizem, publicizem in ostala zmeda sodobnosti. Glede na besede strokovnjakov, ki so sodelovali na 6. Etičnem forumu informacijske družbe, lahko zaključimo, da je varnost uporabnikov informacijsko-komunikacijskih tehnologij in zaščita njihove zasebnosti v veliki meri tudi v njihovih rokah: v poznavanju

tehnologije, zakonodaje in čim boljši ozaveščenosti o tem, zakaj je pomembno, da naši zasebni podatki ne dobijo oznake ‘javno’. V nasprotnem primeru je lahko cena uporabe informacijskih tehnologij izguba zasebnosti, česar pa si nikakor ne želimo.

Aleksandra Selinšek, Jan Dolar, Mojca Viličnjak

SAMOPREDSTAVLJANJE ALI "SAMOUSTVARJANJE"?

Katarina Mohorič, Medijske komunikacije

KLJUČNE BESEDE

samopredstavitev, identiteta, splet, fotografija, selfie

»To je potemtakem tisto Realno, ki nas čaka ...
Virtualizacija ukinja distanco med sosedom in oddaljenim tujcem ...
sosedje, tujci, vsi so enake prikazni z zaslonov.«
(Žižek, 1996, 133)

V tokratno pisanje nas je spodbudil razmislek o resničnosti ustvarjenih identitet na spletnih družbenih omrežjih. Zanimalo nas je, kako posamezniki izkoristijo dostopna okolja za prikaz samega sebe in kako sami sebe vizualizirajo z objavljenimi fotografijami. Zato bomo v nadaljevanju uvodoma pojasnili pojem samopredstavljanja in teorijo identitete, hkrati pa razložili tudi koncept upravljanja z vtisi. Kasneje bomo izpostavljene koncepte umestili v spletno resničnost. Podrobneje se bomo usmerili tudi v konstruiranje s fotografijami ter se kritično opredelili do njihove avtentičnosti in manipulacije. Zaključili bomo z današnjim fenomenom selfijev kot narcisoidnih samoreprezentacij. S člankom želimo opozoriti na problem ustvarjanja pretirano pozitivnih, nerealno vizualiziranih in napihnjenih virtualnih identitet.

Marjana Nastran Ule, na področju socialne psihologije, samopredstavitev (ang. self-presentation) opredeli kot »*proces vplivanja na vtise, ki jih imajo drugi ljudje o nas. Po navadi si želimo pri ljudeh ustvariti čim boljši vtis o sebi, zato je veliko dejavnosti v komunikacijski situaciji posvečenih tovrstnim predstavitvam*« (Ule, 2005a, 282). Z drugimi besedami, pojem opiše kot način, ki ga posameznik uporabi, ko predstavlja samega sebe in ko hoče to podobo o sebi posredovati drugim udeležencem komunikacijske situacije. Pri tem pomembno poudarja, da ne gre nujno le za predstavitve, kjer subjekt cilja na priljubljenost in ohranjanje dobrega vtisa o sebi. Lahko gre tudi za negativne samopredstavitve, na primer tedaj, ko ta isti udeleženec hoče pri drugih vzbuditi usmiljenje ali ko hoče na vsak način uveljaviti svojo premoč, ipd (Ule, 2005a).

Naj omenimo še opredelitev koncepta samopredstavljanja po enem najuglednejših teoretikov identitete, Goffmanu (v Ule, 2005). Ta jo enači z načrtno strategijo in sredstvom za doseganje določenih ciljev, s katerim ljudje zavestno manipulirajo. Tako dajejo napačne in izpuščajo pomembne informacije o sebi, izkoriščajo pričakovanja in slabosti drugih ljudi, da predstavijo svojo podobo, ki jih kaže v najboljši luči. Nasprotno Leary (v Ule, 2005b, 2013) posameznikom pripisuje, da se kljub ustvarjanju pretirano pozitivne podobe, vseeno trudijo predstaviti sorazmerno resničen obraz samih sebe. Dokaj podobno področje opredeli tudi Praprotnik (2003, 63), ki prepozna identiteto kot produkt svobodno izbrane igre oziroma teatralne reprezentacije sebe. Posameznik se je sposoben predstaviti v različnih vlogah, podobah in aktivnostih.

Ljudje oblikujejo svojo samopredstavitev predvsem glede na soudeležene ljudi, občinstvo in okoliščine, v katerih nastopajo (Kuhar, 2005, 142). Podrejeno je temu, kako razumemo svoje odnose z drugimi osebami oziroma kako bi radi videli sami sebe v odnosu z drugimi ljudmi (Ule, 2005a). Samopredstavitev je zato neizogibna sestavina medsebojnega komuniciranja v vsakdanjih odnosih oziroma kot reče Goffman, da ljudje nenehno »*igramo same sebe*« (Goffman v Ule, 2005b, 212), saj smo pod neprestanem pritiskom ocenjevanja in vrednotenja drugih.

Izmenično se v tuji literaturi kot vzporednica samopredstavljanju uporablja pojem »*management vtisa*« (*ang. impression management*). Gre za nekoliko obsežnejši termin, ki ga nujno ne povezujemo zgolj z individualnim subjektom, ampak ga lahko dojemamo širše kot upravljanje z vtisi tudi drugih entitet. Gre za »*zavedni rezultat, ki ga posameznik naredi, da bi kontroliral selektivna obnašanja za predstavitev njihovega želenega Jaza specifični publiki*« (Wang in Stefanone, 2013, 3).

Samopredstavljanje na spletu se vsekakor razlikuje od samopredstavljanja v vsakdanjem življenju. Leary pravi (v Tribušon, 2008), da je on-line predstavljanje bolj sistematično in da ima posameznik večji nadzor nad tem, kako se samopredstavlja. V off-line življenju je to odvisno tudi od nezavednih znakov, ki jih v medsebojni komunikaciji spontano oddajamo naslovniku, medtem ko slednje v spletni resničnosti lahko priročno zakrijemo. Tako imajo posamezniki večji nadzor nad tem, kakšne informacije bodo posredovali, in lahko preprečijo določene komunikacijske konflikte. Prikazujejo kontrolirane podobe, ki kažejo točno takšen obraz, kot želijo, da je viden (Donalth v Papacharissi, 2009, 210).

»*Internet predstavlja nekakšno igrišče, na katerem se posamezniki in posameznice igrajo z vidiki svoje identitete ter osebnosti (...).*« (Ule, 2005a, 407) Oziroma kot pravi Jenny Sunden (v Kečanović, 2009) uporabniki morajo znati napisati same sebe. Tekst, fotografija in video predstavljajo pomembne načine, kako ustvariti in prikazati virtualno identiteto. Slednjo pa je najlažje oblikovati prav v nadzorovanem okolju spletnih družbenih omrežij, ko posameznik svojo persono zgradi z oblikovanjem profila.

Če se sedaj natančneje usmerimo v zgolj samopredstavitev s fotografijami, potem lahko uporabimo raziskavo Andraje Siibak (2009), v kateri je pozornost namenila navadam vizualnega samopredstavljanja v spletnem okolju. Ugotovila je, da so na primer uporabniki Facebooka še posebej pazljivi pri izbiri fotografije in običajno objavijo tisto, na kateri se sami sebi zdijo najbolj privlačni. Poleg tega so rezultati ankete pokazali, da so dekleta veliko bolj precizna pri svojih profilnih slikah. Veliko bolj kot fantje cenijo estetske (lepa okolica na sliki), čustvene (posnet nek pomemben trenutek), samorefleksijske (fotografija zrcali življenjski slog) in estetsko-simbolične (slikal je slaven fotograf) vidike fotografiranja, medtem ko so fantje pri kreaciji virtualne osebnosti pozorni le na svoj čeden videz (Siibak, 2009).

Siibak (2009) pripisuje mladim strateško ustvarjanje svoje vizualne predstavitve in skrbno izbiro fotografij(e), ki spremljajo njihove profile na omrežjih. Trudijo se, da bi z virtualno komunikacijo dosegli pozitiven odziv pri čim širšem občinstvu. Zato na svojih Facebook profilih objavljajo fotografije, ki prikazujejo pomembne trenutke v

življenju, njihovo osebnost, ali pa deluje kot pomemben dokaz prisotnosti drugega. Uporabniki se trudijo ustvariti svoj »*idealni jaz*«. Angela Thomas (v Siibak, 2009) ugotavlja, da se je v spletnih skupnostih ustvaril nov tip telesa.

Podobno ugotavlja tudi Strano (2008), ko poudari, da ženske večkrat zamenjajo videz svojega osebnega profila in s tem ustvarjajo bolj dinamično identiteto. Poleg tega fotografije ne vrednoti več z dokazom resničnosti, ampak ji vrednost pripisuje šele z izmenjavo. Zgodil se je premik od fotografiranja (*taking picture*) do delanja fotografije (*making picture*). Digitalna fotografija, dostopna programska oprema (Photoshop, Google Picasa, Fotor, Microsoft Office Picture Manager) in aplikacije (Instagram, Pinterest, Snapchat, We Heart It) omogočajo manipulacijo fotografije s ponujenimi filtri.

Objektivnost in avtentičnost fotografije se še posebej izgubi pri fotografiranju samega sebe, pri *selfijih*. Gre za žanr, ki obstaja že dlje časa, medtem ko je besedo Oxford Dictionaries definiral šele v letu 2013, in sicer kot »*fotografijo samega sebe, ki jo posameznik ustvari s pametnim telefonom ali spletno kamero in jo doda na socialni medijk*[1]. V zadnjem času pa je število selfijev bistveno naraslo, zato lahko govorimo o t.i. fenomenu. Lahko bi prav tako trdili, da je tovrstna fotografija še posebej popularna, ker dovoljuje nadzor nad ustvarjanjem slike. Selfie kot izdelana reprezentacija samega sebe.

Najbolj pomembno pa je pri *selfiju* izgledati dobro, zato komentatorji povezujejo *selfie* z narcizom. Tega avtorja Buffardi in Campbell (2008) vidita v veličastnemu in napihnjenemu izražanju osebnostnih lastnosti na fotografiji. Peggy Drexler (2013) *selfie* celo opiše kot odraz obsedenosti družbe z videzom. Po njenem mnenju je *selfie* kot neprestano gledanje v ogledalo in dopuščanje, da te pri tem gledajo tudi drugi. Sociolog Nathan Palmer (2014) pa opaža, da se posamezniki pri *selfijih* trudijo ujeti fotografski jaz na zanimivih lokacijah, pozitivno vizualizirati svoj izgled in pri tem predstaviti pomembne osebnostne lastnosti. *Selfiji* delujejo kot nekakšna fotografska samohvala.

1 V Sloveniji še nimamo ustreznega prevoda za selfie, kljub temu pa bi lahko pisali o avtoportretu, ki ga posameznik naredi s pametnim telefonom in pripomočki. Zaradi aktualnosti besede smo se odločili, da bomo tudi sami v nadaljevanju uporabili prav to angleško različico besede - selfie.

S pomočjo teoretičnega razumevanja samopredstavljanja smo želeli bralcu približati idejo o konstruiranju različnih identitet posameznika. Pri tem smo pomembno izpostavili dejstvo, da to ustvarjanje osebnostnih podob ne poteka le v resničnih življenjskih situacijah in v neposrednih pogovorih "face-to-face", ampak tudi na spletu. Eden lažjih načinov za konstruiranje virtualnega jaz-a je prav okolje družbenih omrežij, ki uporabniku ponuja sistematično predstavljanje s svojimi enostavnimi orodji. Predvsem pa smo želeli bralca soočiti s problemom tega nadzorovanega komuniciranja, kjer posameznik priročno prikrije svoje pomanjkljivosti in oblikuje nadvse pozitivno sliko samega sebe. Prepričani smo, da se posamezniki dovolj dobro zavedamo, da uporabniki družbenih omrežij z objavami predstavljajo sami sebe in s tem vplivajo tudi na to, kako jih bomo razumeli drugi. Istočasno pa zaznavamo, da smo prav uporabniki, ki se vsega zavedamo, premalo kritični do teh posredovanih podob, ki nemalokrat ustvarjajo neresnične vtise. Ne zavedamo se, da samopredstavljanje lahko pomeni tudi priložnost "*samoustvarjanja*".

BIBLIOGRAFIJA

Buffardi, L. In Cambell, K. (2008): Narcissism and Social Networking Web Sites. Society for Personal and Social Psychology 34 (10): 1303-1314.

Kečanović, S. (2009): Prijateljstvo in narcizem na spletnih socialnih omrežjih. Dostopno na: www.ris.org/editor/1258937362kecanovic-sabina.pdf (3.5.2014)

Kuhar, M. (2005): Teorije medosebnega komuniciranja, komunikativna kompetentnost in analiza sebstva. Doktorska disertacija. Ljubljana: FDV.

Palmer, N. (2014): The Presentation of #SELFIE. Dostopno na: http://www.sociologyinfocus.com/2014/04/16/the-presentation-of-selfie/#fnref:1 (3.5.2014)

Papacharissi, Z. (2009): The Virtual Geodraphies of Social Networks: A Comparative analysis of Facebook, LinkedIn and A small World. Dostopno na: http://tigger.uic.edu/~zizi/Site/Research_files/VirtualGeographiesFacebook.pdf (3.5.2014)

Drexler, P. (2013): Our Gender, Ourselves. Dostopno na: www.psychologytoday.com/blog/our-gender-ourselves/201309/what-your-selfies-say-about-you (3.5.2014)
Oxford Dictionaries: Selfie. Dostopno na: http://www.oxforddictionaries.com/definition/english/selfie (3.5.2014)
Praprotnik, T. (2003): Skupnost, identiteta in komunikacija v virtualnih skupnostih. Ljubljana: Fakulteta za podiplomski humanistični študij.

Siibak, A. (2009): Constructing the Self through the Photo selection – Visual Impression Maanagement on Social Networking Websites. Dostopno na: http://www.cyberpsychology.eu/view.php?cisloclanku=2009061501 (3.5.2014)

Strano, M.M. (2008): User Descriptions and Interpretations of Self-Presentation through Facebook Profil Images. Dostopno na: http://www.cyberpsychology.eu/view.php?cisloclanku=2008110402 (3.5.2014)

Tribušon, T. (2009): Identiteta v okolju spletnega socialnega omrežja. Dostopno na: http://dk.fdv.uni-lj.si/diplomska/pdfs/Tribuson-Tanja.pdf (3.5.2014)

Ule, M. (2005a): Psihologija komuniciranja. Ljubljana: FDV.

Ule, M. (2005b): Socialna psihologija. Ljubljana: FDV.

Wang, S. S. in Stefanone, M. A. (2013): Showing off? Human Mobility and the Interplay of Traits, Self-Disclosure, and Facebook Check-Ins. Social Science Computer Review 00 (0): 1-21.

Žižek, S. (1996): Kiberprostor ali neznosna zaprtost bivanja. Problemi XXXIV (7-8): 101 – 132.

POSKUSI NADZORA NAD INTERNETOM V IMENU VAROVANJA INTELEKTUALNE LASTNINE

Jan Dolar, Medijske komunikacije, 2. stopnja

KLJUČNE BESEDE

SOPA, PIPA, ACTA, TPP, zakonodaja, intelektualna lastnina

UVOD

V zadnjih nekaj letih smo bili priča nekaterim predlogom zakonov in mednarodnih sporazumov, ki naj bi v osnovi ščitili intelektualno lastnino, oziroma se borili proti trgovanju s ponaredki. Predlogi SOPA (Stop Online Piracy Act), PIPA (Protect IP Act), ACTA (Anti-Counterfeiting Trade Agreement) in TPP (Trans-Pacific Partnership Agreement) so bili deležni največ pozornosti, predvsem zaradi številnih kritik. S sprejetjem teh predlogov so kritiki opozarjali na možnost cenzure in ogrožanja varnosti na internetu. Poleg tega so obsojali pogajanja teh predlogov, ker so se odvijala tako rekoč na skrivaj. Sami predlogi pa naj bi bili nejasno napisani, zaradi česar bi se jih lahko različno interpretiralo in s tem, med drugim, resno ogrozilo svobodo na internetu. Prvi trije, SOPA, PIPA in ACTA, so bili že zavrnjeni ampak TPP je še vedno v fazi pogajanj in kritiki še vedno opozarjajo na podobne napake, kot so jih vsebovali prvi predlogi.

V tem članku bomo na kratko predstavili vsakega izmed teh predlogov, kot si sledijo v časovnem zaporedju, v katerem so postali širše znani v javnosti. Izpostavili bomo nekatere sporne točke predlogov in predstavili nekatere podobnosti med njimi. Pri vsem tem se bomo skušali osredotočili samo na točke, ki se dotikajo interneta.

(NE)UTEMELJENI RAZLOGI

Boj za zaščito intelektualne lastnine in preprečevanje piratstva ter trgovanja s ponarejenimi izdelki se velikokrat opravičuje in prikazuje kot nujnega ob statistki škode, ki naj bi jo takšna dejanja povzročala. A vendar je ravno ta statistika lahko orodje v rokah kritikov, saj za prikazane številke naj ne bi bilo dovolj dokazov. Medtem ko nekateri svarijo na precejšnje probleme s ponaredki blagovnih znamk in z nepooblaščenimi kopijami, je organizacija za gospodarsko sodelovanje in razvoj (OECD - Organisation for Economic Co-operation and Development) ocenila, da je temu problemu podvrženega manj kot 2% svetovnega trgovanja (Moir, 2011). V to oceno je seveda všteto trgovanje na spletu, torej morda tudi učinek spletnega piratstva ni tako močan, kot ga želijo prikazati. Podporniki predlogov SOPA in PIPA prikazujejo spletno piratstvo, kot eno glavnih groženj in povzročiteljev gospodarske škode v ZDA (Sanchez, 2012). Mednarodna zveza za intelektualno lastnino (IIPA - International Intellectual Property Alliance), ki je večinoma združenje agencij, ki združujejo filmske, glasbene in programske industrije, je pozvala k večji vladni zaščiti produktov, temelječih na avtorskih pravicah. Razlog vidijo v tem, da naj bi imel ta industrijski sektor visoko gospodarsko vrednost in bi ga bilo treba zaščititi pred grožnjo piratstva. Očitno je, da piratstvo te industrije ni resneje ogrozilo, če jo je sploh. V zadnji recesiji so jo namreč podjetja v tem sektorju odnesla veliko bolje od ostalih in celo prekosili so na splošno celotno ameriško gospodarstvo. Ob takšnem stanju bi lahko rekli, da je posebna zaščita pred piratstvom skoraj odveč. Tudi če bi spletno piratstvo popolnoma izničili, so nekatere raziskave pokazale, da na gospodarstvo to ne bi imelo posebnega učinka. Kljub vsemu nasprotniki piratstva zapravljajo milijone dolarjev in težijo k spremembi zakonodaje, ki bi nekaj pravne moči prenesla v zasebni sektor.

SOPA IN PIPA

Prva predstavljena predloga, proti piratska SOPA (Stop Online Piracy Act) in PIPA (Protect IP Act) sta se pojavila leta 2011 v ZDA. Zakona naj bi bila namenjena zmanjšanju spletnega piratstva in ponarejanja, še posebej s strani podjetij izven območja ZDA (Yoder, 2012). Kritiki so ju označili za neučinkovita, ker naj bi bila napisana preveč na splošno. Na primer, po teh zakonih spletna stran krši zakon o avtorskih pravicah že, če samo vsebuje iskalnik, ki lahko pripelje uporabnika do piratskih vsebin. To seveda zelo oteži delo stranem, kot so na primer Google, Youtube in Dropbox. Čeprav se to v SOPA in PIPA kaže malo drugače, v osnovi stran

krši zakon že samo s tem, ker jo je mogoče uporabiti za kršenje zakona (Carrier, 2013). Problem je tudi v tem, da po zakonu v prvi vrsti ni kaznovan uporabnik spletne strani oz. njene storitve, ampak sama spletna stran in njen lastnik. To se je izkazalo že v primeru strani Napster, ki je morala ustaviti svojo storitev prenašanja datotek, ker so njeni uporabniki kljub raznim filtrom prenašali avtorsko zaščitene datoteke. Takšna zakonodaja bi tudi dovolila ponudnikom internetnih storitev (internet service providers- ISPs), da spletne strani, ki domnevno kršijo zakon, izbrišejo iz sistema domenskih imen (domain name system - DNS) in s tem naredijo stran nedostopno povprečnemu uporabniku (Yoder, 2012). Podoben pristop uporablja Kitajska za upravljanje s svojim požarnim zidom, ki drži njihove državljane stran od neodobrenih vsebin. Na nek način s tem legalizirajo DNS napade, ki se jih poslužujejo tudi računalniški hekerji (Benkler, 2011). Z zakonom so dovoljeni tudi drugi prijemi, s katerimi bi lahko napadali spletne strani, kot so to storili s stranjo WikiLeaks leta 2010, ko so s sistemskim DDos (distributed denial-of-service) napadom skušali onemogočiti dostop do strani. Ob vseh teh kritikah in opozorilih, naj bi SOPA kršila tudi prvi amandma ameriške ustave, kar je v pismu kongresu zapisal Tribe (2011).

Kljub neomajni podpori predlogoma s strani ameriške filmske zveze (MPAA - Motion Picture Association of America) in združenja ameriških glasbenih založb (RIAA - Record Industry Association of America) sta bila zakona zavrnjena (Yoder, 2012). Pri zavrnitvi je ključno vlogo odigral internet. Informacije o predlogih so se razširile po celem svetu in povzročile številne proteste. Med najbolj znane sodijo nasprotovanja s strani Reddita, Wikipedije in Googla. Slednji je na svoji strani, povrh vsega, objavil povezavo do peticije proti predlogoma. V primeru sprejetja omenjenih zakonov, takšni spletni protesti in vključenost javnosti v njih, najverjetneje ne bi bili mogoči. Vsaj za nekaj časa je tako internet ostal relativno svoboden, dokler te svobode ni ogrozila ACTA.

ACTA

V februarju leta 2008 se je pojavil predlog proti-ponarejevalskega sporazuma ACTA (Anti-Counterfeiting Trade Agreement) (Shaw, 2008). Mednarodni sporazum je bil razvit izven svetovne trgovinske organizacije (WTO - World Trade Organization) in svetovne organizacije za intelektualno lastnino (WIPO - World Intellectual Property Organization), ki navadno urejata zakone o intelektualni lastnini (Kaminski, 2011). Pri sporazumu naj bi šlo za poskus predstavitve maksimalističnega standarda za intelektualno lastnino na mednarodnem področju. Države vključene v ta sporazum bi bile Avstralija, Kanada, Japonska, Mehika, Maroko, Nova Zelandija, Singapur, Švica, Južna Koreja in ZDA ter Evropska Unija. Kaminski je še zapisala, da gre prvotno za sporazum o avtorskih pravicah, ki je pod krinko sporazuma, ki naslavlja nevarna zdravila in pomanjkljiv uvoz.

Čeprav se je predlog sporazuma pojavil že leta 2008, v javnosti ni bil deležen večje pozornosti vsaj do leta 2011. Razlog za takšno časovno luknjo je dejstvo, da so sporazum razvijali in se pogajali v tajnosti (Carrier, 2013). To je bilo vidno že od samega začetka, saj že ob pojavu predloga leta 2008 praktično ni bilo mogoče zaslediti objav v medijih (Shaw, 2008). Skrivni razvoj ni edina sporna stran sporazuma. Tudi besedilo sporazuma je nejasno napisano, zaradi česar se lahko različno interpretira njegove ključne pojme (Moir, 2011). Interpretacija sporazuma bi bila v rokah Odbora ACTA, ki bi uvajal, razlagal in spreminjal sporazum brez javnega nadzora (Savič, Lesjak, & Ručigaj, 2011). Zasebna podjetja, kot so ponudniki internetnih storitev, bi po sporazumu ACTA lahko upravljali, nadzirali in regulirali spletne vsebine in s tem tudi samo svobodo govora, za kar ta podjetja seveda niso kvalificirana. S sporazumom bi bila ogrožena zasebnost uporabnikov spleta, ker bi bili ponudniki dostopa do interneta prisiljeni nadzirati lastna omrežja. Poleg tega bi morali ob morebitnih kršitvah posredovati osebne podatke domnevnih kršiteljev. ACTA bi poleg interneta imela širši negativni učinek tudi na drugih področjih. Do tega vendarle ni prišlo, saj je Evropski Parlament, julija 2012, sporazum ACTA zavrnil (Carrier, 2013). Tako je ACTA postala dober primer na kaj naj bi bilo treba paziti pri prihodnjih sporazumih, kot je, na primer, TPP (Trans-Pacific Partnership) (Kaminski, 2011).

TPP

Trans-pacifiško partnerstvo ali TPP (Trans-Pacific Partnership) je trgovski sporazum, ki ima svoje korenine v sporazumu iz leta 2005 (Lewis, 2011). Takrat je, še pod imenom

Trans-Pacific Strategic Economic Partneship Agreement ali P4, združeval Brunej, Čile, Novo Zelandijo in Singapur. Ime TPP je dobil šele s priključitvijo ZDA po letu 2008. Danes je v pogajanjih o sporazumu vključenih 12 držav (WikiLeaks, 2013). Poleg prej omenjenih sodelujejo še Japonska, Mehika, Kanada, Avstralija, Malezija, Peru in Vietnam.

Tako kot SOPA, PIPA in ACTA je tudi TPP nejasno zapisan in s tem dopušča različno interpretacijo (Carrier, 2013). Pogajanja o TPP se prav tako odvijajo v tajnosti, zaradi česar ima zelo majhno število ljudi dostop do celotnega besedila (WikiLeaks, 2013). Najbolj sporno naj bi bilo poglavje o intelektualni lastnini, ki ga je javnosti razkrila stran WikiLeaks. V njem naj bi se našlo kar nekaj ponovljenih določil iz sporazumov SOPA in ACTA. Nekateri opozarjajo, da bo TPP ustvaril "internetno past", ki bo ogrozila digitalno svobodo, kot jo poznamo danes (Kingsmith, 2013). V tej "pasti" bo TPP reguliral deljenje digitalnih vsebin na družbenih in iskalnih platformah s tem, ko bo prepovedal uporabo začasnih kopij, katere računalniki avtomatično prekopirajo v bralno-pisalni pomnilnik (RAM). Izničil bo varnostne ukrepe za zagotavljanje zasebnosti, s tem ko bodo ponudniki internetnih storitev primorani sistematično filtrirati, zbirati in predajati informacije o uporabnikih vladnim nadzornikom, če jih bodo ti zahtevali. Medijski konglomerati bodo lahko zaobšli državne pravne sisteme. Tako bodo lahko denarno kaznovali uporabnike, odstranjevali neželeno vsebino, izbrisali celotne spletne strani in celo onemogočali dostop do interneta.

Ta sporazum se nas še ne tiče, a vendar obstaja možnost o širitvi. Poleg tega je WikiLeaks opozoril še na en tajni sporazum med ZDA in EU (WikiLeaks, 2013). Sporazum TTIP (Transatlantic Trade and Investment Partnership) naj bi bil zelo podoben TPP, pogajanja pa so se začela že januarja 2013.

ZAKLJUČEK

Svobodni internet je vedno bolj ogrožen. Kot smo videli, obstajajo organizacije, ki pišejo in sprejemajo nejasno definirane zakone in sporazume, vse to v imenu varovanja intelektualne lastnine. S temi predlogi bi prenesli določeno pravno moč in nadzor nad internetom v zasebne roke, kar bi lahko privedlo do popolne cenzure.

Do sedaj je svobodni internet uspel preprečiti sprejetje predlogov SOPA, PIPA in ACTA, medtem ko je javnost lahko pridobila ter si izmenjevala dovolj informacij o njih in se proti njim tudi uprla. Sporazum TPP pa nastaja v takšni tajnosti, da obstaja možnost, da bo sprejet preden se bo širša javnost lahko uspešno borila proti njemu. Ob morebitnem sprejetju bo najverjetneje vsak upor na spletu izbrisan, avtorji uporniških vsebin pa vsaj denarno kaznovani, saj bo to omogočila interpretacija neke točke v sporazumu. Zaradi tega mislim, da je ključnega pomena informiranje širše javnosti o vsaki pomembni informaciji, ki pricurlja iz strogo tajnih pogajanj, da se lahko pravočasno upre.

BIBLIOGRAFIJA

Band, J. (2012). The SOPA-TPP Nexus. Program on Information Justice and Intellectual Property Research Paper no. 2012-06. Retrieved April 20, 2014, from http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1030&context=research

Benkler, Y. (2011). WikiLeaks and the PROTECT-IP Act: A New Public-Private Threat to the Internet Commons. Daedalus, the Journal of the American Academy of Arts & Sciences, 140(4), 154-164. Retrieved April 20, 2014, from http://www.mai68.org/spip/IMG/pdf/WikiLeaks_PROTECT-IP_Benkler.pdf

Carrier, M. A. (2013). SOPA, PIPA, ACTA, TPP: An Alphabeth Soup of Innovation-Stifling Copyright Legislation and Agreements. Northwestern Journal of Technology and Intellectual Propery, 11(2). Retrieved April 18, 2014, from http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss2/1

Kaminski, M. E. (2011). An Overview and the Evolution of the Anti-Counterfeiting Trade Agreement (ACTA). Program on Information Justice and Intellectual Property Research Paper no. 17. Retrieved April 18, 2014, from http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1019&context=research

Kingsmith, A. (2013, Junij 4). How The Trans-Pacific Partnership Will Kill Internet Freedom in Canada. www.DESMOGCANADA.ca. Canada. Retrieved April 22, 2014, from http://www.desmog.ca/2013/06/01/how-trans-pacific-partnership-will-kill-internet-freedom-canada

Lewis, M. K. (2011). THE TRANS-PACIFIC PARTNERSHIP: NEW PARADIGM OR WOLF IN SHEEP'S CLOTHING? Boston College International & Comparative Law Review, 34(27), 27-52. Retrieved April 20, 2014, from http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1264&context=iclr

Moir, H. (2011). Anti-Counterfeiting Trade Agreement. Submission to Joint Standing Committee on Treaties of the Australian Parliament. Australian parliament. Retrieved April 20, 2014, from http://hdl.handle.net/1885/9538

Sanchez, J. (2012, Januar 18). SOPA, Internet Regulation And the Economics od Piracy. Wired (online). Retrieved April 18, 2014, from http://object.cato.org/publications/commentary/sopa-internet-regulation-economics-piracy

Savič, D., Lesjak, B., & Ručigaj, S. (2011, November). Zakaj je sporazum ACTA problematičen (in zakaj bi se morali zanj zanimati evropski poslanci?). (www.e-demokracija.si, Trans.) Retrieved April 20, 2014, from http://www.edri.org/files/ACTA/booklet/ACTA_brosura_SLO.pdf

Shaw, A. (2008). The Problem with the Anti-Counterfeiting Trade Agreement (and what to do about it). KEStudies, 2. Retrieved April 19, 2014, from http://www.kestudies.org/sites/default/files/data/Shaw_34-200-3-PB.pdf

Tribe, L. H. (2011, December 6). THE "STOP ONLINE PIRACY ACT" (SOPA) VIOLATES THE FIRST AMENDMENT. Retrieved April 20, 2014, from http://www.serendipity.li/cda/tribe-legis-memo-on-SOPA-12-6-11-1.pdf

WikiLeaks. (2013, November 13). Secret Trans-Pacific Partnership Agreement (TPP) - IP Chapter. www.wikileaks.org. Retrieved April 4, 2014, from https://wikileaks.org/tpp/pressrelease.html

Yoder, C. (2012). A Post-SOPA (Stop Online Piracy Act) Shift in International Intellectual Property Norm Creation. The Journal of World Intellectual Property, 15(5-6), 379-388. Retrieved April 20, 2014, from http://onlinelibrary.wiley.com/doi/10.1111/j.1747-1796.2012.00443.x/pdf

ZASEBNOST IN NADZOR NA DELOVNEM MESTU

Mojca Viličnjak, Medijske komunikacije, 2. stopnja

KLJUČNE BESEDE

zasebnost, nadzor, delovno mesto, osebni podatki

Človek si želi in potrebuje zasebnost, saj ta omogoča zaščito njegove svobode. Pravica do zasebnosti bi morala veljati v vsakem prostoru in času ter zaščititi posameznika pred neupravičenim in nepooblaščenim nadzorovanjem. Vendar, kaj sploh je zasebnost in pravica do zasebnosti? Pri razlagi pojma zasebnosti lahko najdemo več definicij, vendar nobena ni univerzalna. Križaj meni, da je zasebnost nekaj, kar predstavlja svobodno osebno življenje, brez nezaželenega vmešavanja in nadziranja drugih (Križaj, 1989). Kovačič predstavi zasebnost kot večdimenzionalni pojem, kjer so vključene zasebnost v prostoru, zasebnost osebnosti in informacijska zasebnost (Kovačič, 2000, str. 1021). Skupno definicijam in bistvo zasebnosti je, da ščiti posameznika s tem, ko omogoča svobodno odločanje brez vmešavanja in prisile drugih. Glavne prvine so svoboda, avtonomija in samoodločanje (Gutwirth v Kovačič, 2006, str. 12). Gre torej za neko ločnico med javnostjo oziroma družbo in posameznikom, ki ni fiksna, ampak se lahko spreminja. Ti sferi, javnosti in zasebnosti, sta bili pred pojavom interneta veliko bolj ločeni, kot sta danes. Uporabniki interneta se namreč nahajajo v obeh sferah hkrati, s tem pa se oži zasebni prostor posameznika (Kovačič, 2006, str. 40).

V tem delu se ukvarjamo z vprašanjem zasebnosti na delovnem mestu. To vprašanje je prisotno že od nekdaj, vendar se je njegova pomembnost povečala z nastankom interneta in razvojem digitalnih tehnologij. Tehnološke spremembe prinašajo namreč nove oblike in načine posegov v zasebnost (Kovačič, 2006, str. 46). Pojavlja se vedno več delovnih mest v informacijskem sektorju, tam pa delodajalci in njihovi zaposleni pri delu vedno bolj uporabljajo digitalne naprave (mobilni telefoni, računalniki, tablični računalniki ipd.) in storitve na internetu (e-pošta, socialna omrežja, storitve v oblaku ipd.). S tem pa se ne razširi ali premesti le področje samega dela in aktivnosti delavcev, temveč se na nek način razširi tudi področje nadzorovanja. Ni več le fizičnega nadzorovanja delavcev, tega, kaj delavci delajo, nadzorovanje telesne aktivnosti delavca, kje se fizično nahaja, ter nadzorovanje rezultatov dela in podobno, ampak se začne tudi nadzorovanje nad informacijami. Gre za informacije, ki se izmenjujejo, pošiljajo in prejemajo oziroma obdelujejo, v našem primeru, na delovnem mestu ali med delovnim časom, lahko pa tudi v privatnem življenju delavcev. Tehnologije omogočajo številne nove možnosti nadzora.

Nadzor na splošno pomeni spoznavanje delovanja posameznikov, s tem pa gospodovanje nad njimi. Nadzor se pojavlja v obliki zbiranja informacij ali kot usmerjanje delovanja ljudi. Nadzor ljudem omogoča življenje v družbi (Kovačič, 2006, str. 22), po drugi strani pa je lahko tudi negativen. Nadzor je koristen, kadar pripomore k boljšim rezultatom nekega dela in je nujen tudi pri učenju. Njegova slabost pa se pokaže, ko gre za neutemeljen nadzor in pri tem za poseganje v zasebnost brez utemeljenega razloga oziroma brez prevlade druge pravice. Tako, kot je nadzor potreben za življenje neke družbe, tako je potreben tudi v podjetjih, ustanovah, da se omogoča obstoj neke skupnosti, ki sodeluje pri delu in le tega uspešno opravlja. Gre torej za delovno mesto, ki je lahko dejanski ali virtualni prostor, kjer delavec dela za delodajalca, proizvaja dobrine oziroma opravlja storitve, pri tem pa dobi plačilo ali dobiček (Ransome v Šprah, 2009, str. 885). Odnos oziroma razmerje med delodajalcem in delavcem imenujemo delovno razmerje. Interes delodajalca je zaposlovati delavce, ki bodo čim bolj produktivni in ki bodo opravljali delo dobro in s tem prinašali dobiček podjetju. Pri tem se ne da izogniti temu, da se delodajalec seznani z nekaterimi delavčevimi podatki in nadzoruje delavca. Delodajalci so upravičeni do nadzora nad zaposlenimi, nadzor je povsem legalna in legitimna pravica delodajalca (Šprah, 2009, str. 887). Vendar pa mora biti hkrati v ospredju pravica delavca, da ohrani zasebnost tudi na delovnem mestu oziroma v delovnem razmerju (Peček, 2012, str. 78). Del definicije delovnega razmerja se nanaša na to, da delodajalec daje navodila in nadzoruje delavca, vendar morata pri tem oba upoštevati dogovorjene in predpisane pravice in obveznosti, ki so zapisani v Zakonu o delovnih razmerjih (ZDR-1, 2013; 4. člen). V današnji tako imenovani

informacijski družbi je velik poudarek na informacijski zasebnosti, ki je povezana z osebnimi podatki in informacijami o posamezniku (Šprah, 2009, str. 887). Ko se nekdo zaposli, je izmenjava nekih podatkov o posamezniku, zlasti o zaposlenem, nujna. Delodajalec sme od kandidata oziroma delavca zahtevati le določene podatke in ne katerekoli se njemu zdijo primerni in potrebni. Kaj delodajalec sme zahtevati in kaj je delavec oziroma kandidat dolžan odgovoriti, je zapisano v 28. in 29. členu ZDR. Katere podatke lahko zbira in obdeluje delodajalec, je določeno tudi z Zakonom o evidencah na področju dela in socialne varnosti (ZEPDSV). Tako na primer delodajalec od delavca po tem zakonu ne sme zahtevati njegove fotografije, razen, če je fotografija pomembna zaradi uresničevanja in obveznosti iz delovnega razmerja (Peček, 2012, str. 81). Izredno pomemben je 46. člen ZDR, ki delodajalcu predpisuje, da mora spoštovati delavčevo osebnost ter upoštevati in ščititi delavčevo zasebnost. Zasebnost vsakega človeka pa ščiti tudi 35. člen Ustave RS (Ustava Republike SLovenije). O ravnanju z osebnimi podatki delavca je zapisano v 48. členu ZDR. Varovanja osebnih podatkov se dotika tudi Zakon o varstvu osebnih podatkov (Ur. l. RS št. 86/2004, v nadaljevanju ZVOP-1). Osebni podatek je podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen (ZVOP-1, 2004). Osebni podatek je lahko tudi podatek o obisku spletnih strani na delovnem mestu, saj je to podatek o delavcu kot posamezniku (Hostnik & Valenti, 2011). Vendar se ta šteje kot takšen, če gre za zasebno uporabo spleta, e-pošte in podobno, na službeni opremi. Pri tem delavec namreč izkazuje svoje interese, počutja in osebna stanja, kar velja za osebne podatke in v tem primeru delodajalec nima pravice v vpogled teh podatkov, saj so podatki delavca varovani z ZVOP-1 (Hostnik & Valenti, 2011). Delodajalec tako nima dostopa do elektronske pošte zaposlenega, tudi v službeno pošto ne sme pogledati, če mu zaposleni tega ne dovoli (Pirc Musar, 2009). Vprašanje pa je, če je delavcu dovoljeno med delovnim časom, na službeni opremi, brskati po spletu zaradi zasebnih interesov. To bi naj bila stvar delodajalcev, če to dovolijo ali ne. Delavec lahko zaradi tega, ker med delovnim časom počne stvari, ki niso povezane z delom, ki bi ga moral opravljati, izgubi službo. Primer iz Anglije je, da je delodajalec odpustil delavko, ko je ugotovil, da je med delovnim časom na Facebooku objavila, da ji je dolgčas (Šoštarič & Lipovšek, 2009, str. 59). Delodajalec lahko v takih primerih s tehničnimi sredstvi na službeni opremi tudi onemogoči dostop do spletnih strani, za katere meni, da jih delavec ne bi smel obiskovati med delom. To ni sporno, saj ima delodajalec pravico nadzorovati, ali je njegova oprema dejansko uporabljena za to, kar je bil njen namen (Hostnik & Valenti, 2011). Podobno lahko rečemo tudi za mobilne telefone in druge naprave, ki so v lasti delodajalca. Osebni podatki se lahko obdelujejo le, če to določa zakon ali če je podana privolitev delavca. To določa 10. člen ZVOP-1. V nadaljevanju pa ta člen določa, da mora biti posameznik seznanjen z namenom obdelave osebnih podatkov, če v to privoli. V nasprotnem primeru se torej podatki o klicanih številkah, času klicev, dolžini pogovorov, smatrajo za zasebne podatke, ki jih delodajalec ne sme pridobiti oziroma obdelovati. Delodajalec pa lahko prenese stroške, ki so bili višji od dogovorjenih in o katerih je bil seznanjen zaposleni, na stroške zaposlenega (Pirc Musar, 2012a). Nekatera podjetja oziroma organizacije sprejmejo tudi pravilnike o uporabi službenih mobilnih telefonov, ki podrobneje določajo uporabo mobilnih telefonov. V njih je zapisano, ali lahko zaposleni službene naprave uporabljajo tudi v zasebne namene, kolikšen je znesek, ki ga krije podjetje in kakšne so sankcije v primeru prekoračitve zneska ter podobno (Pravilnik, 2012). Delodajalec pa je kot naročnik telefona upravičen do pridobitve razčlenjenega računana, ki ne vsebuje telefonskih številk, s katerimi je zaposleni komuniciral. Za pridobitev višje stopnje razčlenjenega računa je potrebna privolitev uporabnika telefona. Te pravice delodajalcu pripadajo na podlagi Zakona o elektronskih komunikacijah (ZEKom-1, 2012), in sicer 120. in 121. člena, ki omogoča tudi omejitev in blokiranje določenih številk izhodnih klicev. Pri omenjenih napravah je bistvena komunikacija, ki se nanaša na sredstva sporazumevanja, kot so telefon, elektronska pošta, računalniška omrežja, in pri tem je potrebna komunikacijska zasebnost, ki ščiti vsebine komunikacije in tudi podatke povezane s komunikacijo (prometni podatki). Iz tega izhaja, da imajo zaposleni pravico do svobode komuniciranja in ohranjanja tajnosti svojih sporočil (Šprah, 2009, str. 887). Pravica do komunikacijske zasebnosti je določena v Ustavi RS, v 37. členu. Primeri kršenja komunikacijske zasebnosti so se pojavljali že pred več kot desetletjem. Lynette Copland je bila uslužbenka, ki je bila žrtev pretiranega nadzora. Njen nadrejeni se je zanimal za njeno zasebno življenje, zato je nadziral njene telefonske pogovore, elektronsko pošto, obisk internetnih strani in podobno. Sodniki so kasneje razsodili, da je bil kršen 8. Člen Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin. Coplandova je bila namreč nadzorovana brez, da bi jo na to opozorili in brez utemeljenega razloga (Delo,

2012). Danes delodajalci velikokrat izkoristijo svoj nadrejeni položaj nad delavci in si dovolijo preveč. Zasledimo lahko anonimna pisma informacijski pooblaščenki, kjer zaposleni najpogosteje sprašujejo, kakšne so pravice delodajalca pri nadzorovanju ter kako daleč v zasebnost smejo posegati. Imamo primer, ko se je delodajalec dokopal do zasebnega maila delavca. To pomeni, da je zlorabil geslo, ali vdrl v računalnik, ali kako drugače prišel do gesla, vendar vsekakor nezakonito. Delavec ni vedel kakšne so njegove pravice in kaj lahko naredi glede tega. Gre za kaznivo dejanje (poseg v tajnost pisem in občil), ki ga lahko prijavi policiji (Pirc Musar, 2012b).

Poleg že omenjenih sredstev komunikacije so danes zelo razširjena socialna omrežja, kot so Facebook, MySpace in podobno. Veliko delodajalcev se poslužuje socialnih omrežij za nadzor nad zaposlenimi, ali ko zbirajo kandidate, ki bi jih sprejeli v službo. Pri tem od nekaterih kandidatov oziroma zaposlenih delodajalci zahtevajo celo uporabniška imena in gesla za vstop v profil socialnih omrežij, kar je vdor v zasebni profil. Tega pa delodajalec nima pravice zahtevati. Takšna dejanja se štejejo med hujše kršitve zasebnosti. Kerr meni, da ga lahko primerjamo s tem, da od nekoga zahtevamo ključe njegovega doma (Kerr v Delo, 2012). Kazen za takšne zahteve po geslih lahko segajo tudi čez 12.000 evrov (Finc, 2012). Justin Basset ima izkušnje s primerom, ko je potencialni delodajalec zahteval uporabniško ime in geslo Facebook profila. V njegovi situaciji se je to zgodilo na razgovoru za službo, vendar je zahtevo po geslu zavrnil, posledično pa ni imel možnosti sodelovanja s podjetjem (Delo, 2012). Tudi Robert Collins je doživel podobno izkušnjo. Delodajalec ga je prosil za prijavo v njegov profil, Collins je prošnji ugodil. Vložena je bila pritožba nad tem podjetjem, ki je kasneje spremenila izpraševanje kandidatov tako, da ni zahtevala gesla in uporabniškega imena, ampak so od kandidata zahtevali, da se sam prijavi v profil (Delo, 2012). Tudi zahteve delodajalca, da se delavec oz. kandidat prijavi v svoj profil in s tem pokaže zasebne podatke, so vdor v zasebnost. Delodajalec lahko ima vpogled le v profil delodajalca, ki je javno dostopen, oziroma se lahko pridruži prijateljstvu na socialnem omrežju, če delavec ve, da gre za delodajalca in sprejme njegovo prijateljstvo.

Nekateri delodajalci želijo ves čas nadzorovati svoje zaposlene, vendar je to nemogoče, ker ne morejo biti ves čas z njimi in jih opazovati. Način, kako nekoga opazovati cel čas, brez da smo tam prisotni, je snemanje oziroma videonadzor. Nadzorovanja s pomočjo video snemanja na delovnem mestu se dotika ZVOP-1 s 74. in 77. členom. Slednji se nanaša na videonadzor znotraj delovnih prostorov. Ta člen dovoljuje izvajanje takega videonadzora le v izjemnih primerih. To so primeri, kadar je nadzor nujno potreben za varnost ljudi, premoženja ali za varovanje tajnih podatkov in poslovnih skrivnosti, pa tega ni možno urediti z drugimi, milejšimi sredstvi. Če se videonadzor izvršuje, pa morajo bili zaposleni o tem nujno obveščeni. Izven delovnega mesta pa delodajalec nima nikakršne pravice videonadzora (Peček, 2012, str. 81, 82). Tu pa imamo še podobne vrste nadzora, kot je zvočno snemanje in fotografiranje, sledenje z napravami GPS, ki so z zakoni opredeljeni zelo podobno kot videonadzor.

Čeprav imamo jasno določena pravila, celo z zakonsko podlago, o nadzoru in poseganju v zasebnost na področju zasebnosti in nadzora na delovnem mestu, se vršijo številne kršitve. Najpogostejše kršitve v delovnih razmerjih se nanašajo na vpoglede v elektronsko pošto zaposlenih, nadzor nad uporabo interneta in mobilnih telefonov. Veliko je tudi kršitev o pridobivanju osebnih podatkov, neutemeljenega videonadzora, nadzora z GPS napravami in podobno (Informacijski pooblaščenec). Pri vseh teh kršitvah vidimo, da so delavci šibkejša stranka v povezavi z delodajalcem. Za izboljšanje odnosa med delavci in delodajalci bi se delodajalci morali zavedati obveznosti in pravic, ki so določeni z zakoni. Zagotoviti bi morali varne delovne razmere zaposlenim, spoštovati delavčevo osebnost in ščititi njihovo zasebnost (Šprah, 2009, str. 888). Pri tem pa je pomembno odločanje o količini in načinu nadzora. Tukaj gre za izbiro neke optimalne opcije med dvema skrajnostma, med popolnim nadzorom in brez nadzora, saj nobena od teh skrajnosti ni dobra in ne prinese željenih ciljev. Potrebno je najti sorazmernost. Poseganje v zasebnost je dovoljeno le v toliki meri, da se še ohrani dostojanstvo in pravica delavca. Nadzor pa naj bo izvajan le zato, da se ustvarijo pozitivni rezultati dela. Odnos med delodajalcem in zaposlenim pa bi se moral graditi na zaupanju, saj bi lahko tako zmanjšali nadzor, izboljšali odnose in dosegli uspešnost brez nevšečnosti in poseganja v zasebnost ali dostojanstvo ljudi.

BIBLIOGRAFIJA

Delo. (maj 2012). Prevzeto april 2014 iz Socialna omrežja – sovražniki iskalcev zaposlitve: http://www.delo.si/druzba/panorama/socialna-omrezja-ndash-sovrazniki-iskalcev-zaposlitve.html/

Finc, M. (marec 2012). Zasebnost na delovnem mestu: z uporabo tehnologij več kršitev . Prevzeto april 2014 iz Delo: http://www.delo.si/druzba/delova-borza-dela/zasebnost-na-delovnem-mestu-z-uporabo-tehnologij-vec-krsitev.html

Hostnik, E., & Valenti, I. (2011). Nadzor nad uporabo spletnih strani, službenih telefonov in e-poštnih naslovov. Prevzeto marec 2014 iz Konfederacija sindikatov 90 Slovenije: http://www.sindikat-ks90.si/index.php?option=com_content&view=article&id=285:nadzor-nad-uporabo-spletnih-stranim-slubenih-telefonov-in-e-potnih-naslovov&catid=3:novice

Informacijski pooblaščenec. Zlata pravila zasebnosti na delovnem mestu. Prevzeto april 2014 iz https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Zasebnost_na_delovnem_mestu.pdf

Kovačič, M. (2000). Zasebnost v informacijski družbi. Teorija in praksa.

Kovačič, M. (2006). Nadzor in zasebnost v informacijski družbi. Ljubljana: Fakulteta za družbene vede.

Križaj, F. (1989). Osebne svoboščine in zasebnost v" informacijski družbi". Gospodarski vestnik.

Peček, D. S. (2012). Varstvo zasebnosti v delovnem razmerju. Anali PAZU, 78-83.

Pirc Musar, N. (januar 2009). Delavec v zlati kletki zasebnosti ali delodajalec kot pravice ječar? Prevzeto april 2014 iz Razgledi: http://www.razgledi.net/2009/01/23/delavec-v-zlati-kletki-zasebnosti-ali-delodajalec-kot-pravice-jecar/

Pirc Musar, N. (oktober 2012a). Odločbe in mnenja - Varstvo osebnih podatkov. Prevzeto april 2014 iz Informacijski pooblaščenec: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1(showUid)=2254&cHash=98b824ea848eabc9ed43854be8c55c05

Pirc Musar, N. (januar 2012b). Turbulenca - Klepetalnica. Prevzeto maj 2014 iz RTV SLO: http://www.rtvslo.si/turbulenca/chat/archive/1638

Pravilnik o uporabi službenih mobilnih telefonov in mobilnih kartic za prenos podatkov. (junij 2012). Ljubljana. Pridobljeno iz http://www.fe.uni-lj.si/mma_bin.php/$fId/2012070511484273/$fName/Pravilnik+o+uporabi+sluzbenih-GSM-junij_2012.pdf

Šoštarič, A., & Lipovšek, I. (april 2009). S koliko zasebnosti v službo? Glas Gospodarstva.

Socialna omrežja – sovražniki iskalcev zaposlitve. (marec 2012). Prevzeto april 2014 iz Delo: http://www.delo.si/druzba/panorama/socialna-omrezja-ndash-sovrazniki-iskalcev-zaposlitve.html

Šprah, F. (2009). Kje so meje zasebnosti na delovnem mestu. Zbornik 6. študentske konference Fakultete za management Koper, 885-889.

Ustava Republike SLovenije. Prevzeto marec 2014 iz http://www.us-rs.si/media/ustava.republike.slovenije.pdf

Zakon o delovnih razmerjih (ZDR-1). (13. marec 2013). Prevzeto 19. marec 2014 iz Uradni list: http://www.uradni-list.si/1/content?id=112301

Zakon o elektronskih komunikacijah (ZEKom-1). (december 2012). Prevzeto april 2014 iz Uradni list: https://www.uradni-list.si/1/content?id=111442

Zakon o varstvu osebnih podatkov (ZVOP-1). (julij 2004). Prevzeto 2014 iz Uradni list: http://www.uradni-list.si/1/objava.jsp?urlid=200486&stevilka=3836

SPLETNO VEDENJSKO OGLAŠEVANJE

Mitja Piko, Medijske komunikacije, 2. stopnja

KLJUČNE BESEDE:

spletno vedenjsko oglaševanje, vedenjsko ciljanje

Oglaševanje je velik ter nepogrešljiv del kapitalistične družbe. Postaja vse bolj načrtovano in dodelano. Obdaja nas vsepovsod, bodisi v realnem bodisi na svetovnem spletu. In prav spletnemu oglaševanju se bomo podrobneje posvetili v tem delu. Namen dela je prikazati splošen pregled nad področjem spletnega vedenjskega oglaševanja.

Ko govorimo o trženju, lahko njegov cilj zelo strnjeno povzamemo. Na svetu je veliko neznancev, namen je te neznance spremeniti v kontakte in kontakte v stranke. Tržno komuniciranje je prešlo dolgo pot, od klasičnega oglaševanja od ust do ust do sodobnega množičnega naslavljanja potencialnih kupcev. Eden izmed trenutno najbolj aktualnih načinov, ki se razvija in dopolnjuje, je spletno vedenjsko oglaševanje. Vedenjsko oglaševanje, s svojim napredkom in posledično ogromnimi količinami podatkov, prinaša strokovni diskurz o varnosti osebnih podatkov. Postavlja se vprašanje, ali trenutna samoregulacija zadostuje, kako jo je potrebno dopolniti ter ali so potrebne dodatne zakonske omejitve. Trenutno stanje zasebnosti in transparentnosti pri mnogih vzbuja skrb (Lohr, 2010), saj brskalniki sami po sebi ne ponujajo dovolj možnosti. Zato postajajo vse bolj množično uporabljena orodja, kot so »Ghostery«, »Do Not Track« in druga, ki nam ponujajo dodaten nadzor. Pri vsem tem pa se vprašamo, ali so dobre strani oglaševanja večje od slabih in kakšen napredek prinaša spletno vedenjsko oglaševanje.

KAJ JE SPLETNO VEDENJSKO OGLAŠEVANJE

Spletno vedenjsko oglaševanja spada pod ciljno oglaševanje. S pomočjo piškotkov tretje strani se spremlja vedenje in gibanje uporabnika na spletu, glede na to pa se prikaže uporabniku (predvidoma) zanj primeren oglas. »Namen sistema vedenjskega ciljanja je avtomatsko določanje ustvarjalca, ki je najbolj primeren, da bi bil prikazan uporabniku spletne strani, osnovano na prej zaznanih spletnih vedenjih uporabnika.« (Jaworska & Sydow, 2008, str. 63). Na primer, če je posameznik zainteresiran za šport in pretežno obiskuje strani s športnimi tematikami, se mu bodo tudi na straneh nepovezanimi s športom prikazali oglasi povezani s športom, če stran (na kateri je trenutno) uporablja vedenjsko oglaševanje.

Na začetku spletnega oglaševanja sta obstajali dve zainteresirani stranki, na eni strani oglaševalec in na drugi lastnik spletne strani, ki je ponujal prostor za oglaševanje. Zaradi številčnosti spletnih strani je ostajalo mnogo neizkoriščenega oglaševalskega prostora. Zato se formirajo oglasna omrežja, ki delujejo kot posredniki ali prodajni zastopniki (Karpinski, 2010). Oglasna omrežja uporabijo tehnologijo ter publiko združijo v pakete, te pakete pa prodajajo kupcu, tako za oglaševalca poenostavijo naslavljanje želene ciljne publike.

Kadar se na tržišču množično pojavljajo oglasna omrežja, pride do nepreglednosti ter neučinkovitosti in možnosti prekrivanja že naslovljenih ciljnih skupin. Pojavijo se podjetja za izmenjavo oglasov, ki ponujajo možnost menjave ciljnega občinstva in ne vsebine. Spletne strani objavijo njihovo želeno občinstvo na izmenjavi oglasov, nato si oglaševalci izberejo primerno občinstvo in podajo ponudbo (Karpinski, 2010). Na strani kupcev so se v nekaterih podjetjih dodatno kreirale interne agencije za trgovanje ter za povpraševanje spletnih platform, ki so skrbele za učinkovitost in pospeševanje trgovanja (ANA, 2011). Uporabnikom je večinoma neznano, da so v oglaševanje vključena podjetja iz tretje strani, ki zbirajo njihove podatke in prirejajo njim primerne oglase. Le redki se pozanimajo, kaj se skriva za opozorilnim okencem o piškotkih na spletnih straneh. Podjetja kot Google zakonsko zahtevana opozorila o piškotkih oblikujejo tako: »Piškotki omogočajo, da vam ponudimo svoje storitve. Z uporabo teh storitev se strinjate z našo uporabo piškotkov.« (Google, 2014). Uporaba storitev neposredno pogojuje strinjanje uporabnika s piškotki. Ko si preberemo več o tem vidimo, da jih uporabljajo med drugim tudi za prikazovanje, kot pravijo, ustreznejših oglasov (Google, 2014).

OMEJITVE SPLETNEGA VEDENJSKEGA OGLAŠEVANJA V EVROPSKI UNIJI

V evropski zakonodaji se varstvo podatkov opira na nekaj dejavnikov. Evropska konvencija o človekovih pravicah (1953) ščiti pravico do zasebnega življenja. Pravica do zaščite podatkov je podana v listini o temeljnih pravicah Evropske unije (2009). Direktiva o zaščiti osebnih podatkov (1995) definira osebne podatke kot: »vsi podatki povezani z določeno ali določljivo fizično osebo, na katero se podatki nanašajo« (Borgesius, 2013, str. 82). Po direktivi iz leta 2009 morajo podjetja pridobiti soglasje, če želijo shraniti ali dostopati do piškotkov na računalniku. To uporabnik vidi v obliki pojavnega okenca, kjer se lahko strinja z uporabo piškotkov. To ne velja za piškotke, ki so nujni za delovanje strani ali piškotke, ki se uporabljajo interno na spletni strani. Evropska zakonodaja izvaja načela varstva podatkov, tako imenovana poštena načela informacij: načelo transparentnosti, kjer je vsako tajno zbiranje podatkov prepovedano; načelo varnosti, kjer mora biti zagotovljen primeren nivo varnosti za podatkovne baze; načelo namenske omejitve določa, da se osebni podatki, lahko zbirajo za določene, izrecne in zakonite namene in se ne smejo uporabljati za druge nezdružljive namene (Borgesius, 2013, str. 85). Podjetje lahko obdeluje podatke, če ljudje dajo svojo nedvoumno privolitev. Pogoji privolitve pa se pogosto skrivajo v pravilnikih o zasebnosti.

Na področju samoregulacije se je najbolj prijela ikona »AdChoices«, propagirana s strani European Interactive Digital Advertising Alliance (v nadaljevanju: EDAA), po tem ko so jo sprejela vsa večja oglaševalska podjetja. Ikona označuje vedenjsko oglaševanje in s tem uporabniku nudi večjo preglednost, hkrati pa označuje, da oglaševalec pripada združenju EDAA (Maier, 2011). EDAA se trudi to področje oglaševanja obdržati izven zakonodajnih omejitev in v samoregulaciji oglaševalskih podjetij in združenj oglaševalcev. Izvaja samoregulativni program za spletno vedenjsko oglaševanje, v okviru katerega pozivajo podjetja k sodelovanju in izvajanju dobre prakse. Obstaja še manj množičen TRUSTe certifikat, ki opozarja in izobražuje o spletnem vedenjskem oglaševanju (TRUSTe, 2013). Trenutno edina možnost kontrole za uporabnika so tako imenovane »opt-out« zasebnostne nastavitve. TRUSTe in AdChoices ponujata informacije, kako do »opt-out« nastavitev podjetij, ki uporabljajo vedenjsko oglaševanje. Glavni brskalniki ponujajo orodja za večjo kontrolo vedenjskega oglaševanja, ta orodja nam prikažejo imena podjetij, ki nam sledijo. Programi, ki se namestijo v brskalnik, so na primer Ghostery ali Do Not Track. Alternativa »do not track« programom so »opt-out« nastavitve. Ko nastavimo »opt-out«, to podjetju prepreči, da nam prikaže oglase glede na naše vedenje, to pa ne prepreči, da še vedno zbirajo naše podatke in nam sledijo. Oglasi, ki nam jih prikazujejo s ciljnim oglaševanjem, se prestavijo na klasično generično oglaševanje. Problem, ki se pojavlja pri »opt-out« nastavitvah, je, če nimamo nameščenih dodatnih programov, saj z izbrisom naših piškotkov, izbrišemo tudi »opt-out« nastavitve.

»Opt-out« omogoči prenehanje prikazovanja vedenjskih oglasov, še vedno pa obstaja še problem sledenja našega gibanja po spletu. »Do not track« standard je bil predlagan že leta 2009. Tudi trudi World Wide Web Consortiuma (W3C) za standardizacijo so do sedaj bili neuspešni (Mayer & Mitchell 2012, str. 424). Ker ne obstaja primerne zakonodaje, je od podjetij iz tretje strani odvisno ali bodo spoštovali naše želje, da nam ne sledijo. Tako lahko namestimo dodatek za brskalnik proti sledenju (npr. Do Not Track) in upamo, da podjetje iz tretje strani spoštuje naše želje. Obstajajo programi (npr. Adblock Plus), ki v celoti blokirajo vsebino tretjih strani, delujejo na principu seznama teh podjetij. Te nastavitve so precej učinkovite, ampak primernejše za naprednejše uporabnike (Mayer & Mitchell 2012, str. 423).

ZAGOVORNIKI IN NASPROTNIKI

Vedenjsko oglaševanje že skoraj dve desetletji vzbuja diskurz o zasebnosti in njegovih prednostih za uporabnika. Začetki so se začeli s ponudniki storitev za aplikacije, kot je bil takrat Double Click, ki je bil ustanovljen leta 1995. Glede na dolgo zgodovino je zanimiv vpogled v nekaj glavnih argumentov za in proti temu naprednemu načinu ciljno usmerjenega oglaševanja. Vedenjsko oglaševanje nam prinaša zelo specifične oglase, glede na to, kaj je trenutno naš interes. Tako nam lahko oglas ponudi nekaj, za kar še nismo vedeli, da potrebujemo. Oglaševalcem pripelje točno zaželeno publiko, tako lahko maksimirajo učinkovitost in povečajo število klikov oglasa. Študija izvedena s strani Microsofta leta 2009 je pokazala, da se kliki na oglase lahko povečajo za 670%, za ta rezultat so uporabili najbolj

temeljne algoritme za združevanje uporabnikov (Yan in drugi, 2009, str. 270). Zaradi tako specifično usmerjenega oglaševanja se tudi zmanjša cena, ker ni potrebe po tako množičnemu razpršitvi oglasov. Ponujajo se možnosti združevanja vedenjskega oglaševanja s GPS lokacijo posameznika. Tako bi uporabnik lahko v bližini njegove trenutne lokacije in glede na njegove predhodno zaznane interese, dobil ponudbo, ki ga mogoče zanima.

Na drugi strani pa so argumenti, ki preprečujejo razvoj takšnih tehnologij in oglaševanja. Kot prvo lahko omenimo preglednost. Za uporabnika je nemogoče prebrati vse pravilnike o zasebnosti, saj bi bilo za popolno preglednost potrebno prebirati dodatno še pravilnike podjetij iz tretjih strani. Pravilniki pa se nenehno spreminjajo in dopolnjujejo. Kot pravi McStay bi bilo naše podajanje informacij tedaj etično pravilno, če bi uporabniki popolnoma razumeli vrsto kupčije, kar pa je zaradi dolgih pravilnikov o zasebnosti, iznajdljivosti in kratkoročnih sprejemanj odločitev nemogoče (McStay, 2012, str. 600). Da bi javnost čim bolje razumela možnosti, ki jih ponuja vedenjsko oglaševanje, je potrebno izobraževanje in informiranje ljudi. Samo ljudje, ki vedo za vedenjsko oglaševanje imajo mnenje o njem in se odločajo za nadaljnje korake, kot so dodatni programi in nastavitve. Odkritost industrije do želje po izobraževanja potrošnikov je vprašljiva, saj prihaja iz potrebe po zakonitosti v očeh politikov ter potrošnikov (McStay, 2012, str. 600). Eno izmed glavnih vprašanj je, ali si v prid bolj udobnega in učinkovitega potrošništva želimo deliti vse osebne podatke. Zaradi neizobraženosti javnosti o spletnem vedenjskem oglaševanju in nevednosti, kakšne podatke zbira in obdeluje to oglaševanje, se pojavlja skrb, da se bodo ti zbrani podatki nekdaj vrnili na neprijeten način. Kakšen podatek je oseben podatek, ali je podatek o političnem prepričanju ali financah, čeprav ni vezan na ime, dovolj. Četudi Sodišče Evropske unije še ni odločilo o vedenjskem oglaševanju, obstaja podobna sodna praksa. Gre za razpravo o IP naslovih, kjer je sodišče leta 2011 odločilo, da so IP naslovi osebni podatki. Tako je sodišče potrdilo, da so lahko informacije brez imena osebni podatki in lahko izločijo posameznika znotraj skupine (Borgesius, 2013, str. 84). Izražene so skrbi glede zavajanja in ogrožanja zdravja uporabnikov. V večini gre tukaj za vedenjske oglase, ki bi ljudi lahko zavajali in jih ujeli v ponavljajoči krog. Kot pravi McStay, ni nič narobe, če se uporabljajo podatki ljudi v namen dobička, dokler se spoštujejo pravice ljudi.

Pred zavajanjem katere koli oblike je potrebno zavarovati ljudi za kakršno koli ceno, zato ni opravičila (McStay, 2012, str. 602). Tudi etičnost vedenjskega oglaševanja je vprašljiva, saj večina uporabnikov ne ve za podjetja iz tretje strani in taktih oglaševanja za njimi. Obstajajo problemi z varnim hranjenjem in obdelovanjem podatkov. Veliko je majhnih »startup« podjetij, ki ne morejo zagotoviti zadovoljive mere varnosti hranjenja podatkov in vprašljivo je, kako bodo majhna podjetja do tega zmožna, če imajo celo večje korporacije pogosto težave z varnostjo. Obstajajo tudi čisto banalne ovire za efektivno delovanje takšnega oglaševanja, ko računalnik uporablja več oseb ali če piškotke ovirajo dodatne nastavitve, tudi brisanje piškotkov povzroča nenatančno oglaševanje.

Ne smemo si zatiskati oči, večino programskih možnosti, ki jih uživamo na spletu zastonj, je prineslo prav oglaševanje. Torej bi lahko rekli, da so naši podatki plačilno sredstvo in vsak posameznik postavlja svoj nivo vrednosti. Vedenjsko oglaševanje prinaša uporabnikom ter oglaševalcem veliko novih možnosti. Potrebna bi bila poenotena zakonodaja, ki ne bi preveč omejila oglaševalce in vseeno ščitila osebne podatke posameznika. V kar pa dvomijo tudi podjetja, ki zadržano vlagajo v vedenjsko oglaševanje. Ostrejša samoregulacija oglaševalcev je za enkrat najboljša obstoječa rešitev. Če bo možno efektivno regulirati to področje, bo prav vedenjsko oglaševanje uspelo ponujati vsaki osebi prirejene zanimive oglase, ki nas ne bodo motili in bodo prispevali h kakovosti življenja.

BIBLIOGRAFIJA

Associacion of National Advertisers (2011, November 2). Agency Trading Dest. White Paper 2011. Povzeto z http://www.ana.net/miccontent/show/id/agency-trading-desks-whitepaper

Borgesius, F. Z. (2013). Behavioral Targeting, a European Legal Perspective. IEEE Security and Privacy, 11, 82-85.

Google (2014). Kako Google uporablja piškotke. Zasebnost in pogoji. Povzeto z http://www.google.com/intl/sl/policies/technologies/cookies/

Jaworska, J. & Sydow, M. (2008). Behavioural Targeting in On-Line Advertising: An Empirical Study. WISE 2008, 9, 62-76.

Karpinski, R. (2010, April 19). Ad Networks and Exchanges 101. Advertising Age. Povzeto z http://adage.com/article/special-report-ad-network-exchange-guide-2010/ad-networks-exchanges-101/143310/

Lohr, S. (2010, April 30). Privacy Concerns Limit Online Ads, Study Says. Bits. Povzeto z http://bits.blogs.nytimes.com/2010/04/30/privacy-concerns-limit-online-ads-study-says/?_php=true&_type=blogs&_r=0

Maier, F. (2011, December 19). The Evolution of Online Behavioral Advertising Self-Regulation. Direct Marketing News. Povzeto z http://www.dmnews.com/the-evolution-of-online-behavioral-advertising-self-regulation/article/220012/

Mayer, J. R. & Mitchell J. C. (2012). Third-Party Web Tracking: Policy and Technology. IEEE Symposium on Security and Privacy, 413-427.

McStay, A. (2013). I consent: An analysis of the Cookie Directive and its implications for UK behavioral advertising. New media & society, 15, 596-611.

TRUSTe (2014). What Control Do I Have? Povzeto z http://www.truste.com/consumer-privacy/about-oba/#&panel1-2

Yan, J., Liu, N., Wang, G., Zhang W., Jiang Y., & Chen Z. (2009). How much can Behavioral Targeting Help Online Advertising? 18th international conference on World Wide Web, 261-270.

ZASEBNOST IN SPLETNA TRŽIŠČA

Filip Vrečko, Medijske komunikacije, 2. stopnja

KLJUČNE BESEDE:

zasebnost, spyware, spletne trgovine, digitalni izdelki, zaščite avtorskih pravic

UVOD

V svetu elektronskih komunikacij se vsak obisk, dejanje ali poskus beleži. Sicer gre večinoma za zelo skopo obliko podatkov, a zbrani podatki lastnikom spletnih strani vseeno omogočajo predvideti, kolikšen obisk bo ob določeni uri, katere podstrani so največkrat zahtevane, ipd. Podatki se lahko uporabijo v prid obiskovalcem, oziroma v primeru spletnih trgovin, kupcem, lahko pa tudi za pospešitev prodaje. Uporabniki trgovin smo že navajeni, da z podajanjem informacij kupujemo po nižjih cenah, pa naj bo to v obliki indeksiranja nakupa (npr. kartice, prijave pred nakupom) ali sodelovanje v nagradni igri (prijava na novice podjetja). Cilji članka so predstaviti načine sledenja strankam, zakaj so ljudje pripravljeni dati svoje osebne podatke za majhen popust in raziskati vohunski potencial modernih digitalnih avtorskih zaščit. Najprej bomo preučili delovanje trgovin glede zasebnosti, nato pa se še dotaknili problematike digitalnih avtorskih zaščit.

ZASEBNOST IN UPORABA SPLETNIH TRGOVIN

Ljudje, predvsem starejši, še dandanes ne zaupajo spletnim trgovinam. Kot tudi v raziskavi ugotavlja Chellapa (2002), pri ljudeh obstajajo problemi z zaupanjem spletnim trgovinam izrecno zato, ker so spletne. Ugotavlja, da ljudje manj zaupajo spletni kot fizični trgovini iste verige. Nezaupanje izvira predvsem iz zgodnjega obdobja interneta, ko še ni bilo zakonodaje na tem področju. Leta 1995 so v ZDA s strani Federal Trade Commission uvedli popolno samo-regulacijo, a se ni obnesla, saj trgovci večinoma niso sledili njihovim predlogom. Pred letom 1998 namreč ni bilo na voljo niti izjave o zaupnosti na strani marsikatere spletne trgovine. Idejo o popolni samo-regulaciji so s sprejemom zakona opustili leta 2000. Ampak leto kasneje, s spremembo vodstva, se samo-regulacija ponovno pojavila, a je temeljila na sprejetem zakonu. (Hoofnagle, 2005, str. 4)

Da bi se zaupanje malce bolj utrdilo, so Smith et al. (1996) razvili pravila za ravnanje, zbiranje in obveščanje o informacijah v spletnih trgovinah. Ta so bila z leti nadgrajena in, kot jih predstavi Chelappa, so to dejanja opozorila, izbire, dostopa, integritete in izvajanja. Opozorilo je običajno v obliki pogojev poslovanja, kjer je predstavljeno kupcem, kako se bodo njihovi podatki zbirali. Izbira pomeni, da morajo imeti stranke izbiro, na kakšen način bodo njihove informacije uporabljene in kdo vse bo lahko do njih dostopal. Kupcem mora biti omogočen dostop do nadzora nad svojimi podatki. Integriteta pomeni, da obstajajo mehanizmi, ki preprečujejo nepooblaščeno uporabo podatkov. Izvajanje pa pomeni, da obstaja oblast, katera določi in izvršuje kazni za morebitne kršitve. (Chellappa, 2002, str. 11-12) Resda se ta pravila niso uporabila v zakonodaji, ampak so postale primer dobrih praks, tako da dandanes redko najdemo spletno trgovino brez vseh zgoraj navedenih elementov.

Vendar ljudje redko pomislijo na zaupnost vseh danih podatkov. Belanger et al. (2002) so raziskovali, kateri dejavniki so najpomembnejši, kadar ljudje nameravajo kaj kupiti in podati svoje podatke. Dejavniki so bili: odobritveni pečat o zaupnosti s strani tretje osebe, izjava o zaupnosti, odobritveni pečat o varnosti s strani tretje osebe in varnostne funkcije. Raziskava je pokazala, da so jim najpomembnejši dejavnik varnostne funkcije. Iz tega lahko sklepamo, da so ljudje precej zaupljivi do spletnih trgovin, ki imajo vse običajne zaščite pred vdorom tretjih oseb. Vendar, spletna trgovina lahko zbere gore podatkov o določenem uporabniku, še posebej, če je slednji ves čas prijavljen. Server lahko namreč sledi, katere podstrani so zahtevane, in nato personalizira oglase glede na dobljene informacije. Tudi če uporabnik ni prijavljen, se lahko seja shranjuje preko piškotkov, ter tako ohranja avtomatično prijavo, košarico, itd. (Oussayef, 2008, str. 109) Vendar se piškotki ne nameščajo le preko obiskov določenih spletnih strani, lahko gre le za element strani, zunanjega ponudnika, ki namesti piškotek brez izrazitega dovoljenja. T.i. piškotki tretjih oseb se uporabljajo predvsem za oglase in njihovo personifikacijo. Marsikatera spletna stran ima dogovor s zunanjim ponudnikom, v izjavi o zaupnosti pa so ti piškotki marsikdaj

označeni za uporabnikovo korist, saj naj bi »dostavili ciljane oglase, za katere verjamejo, da vas najbolj zanimajo.« (Hoofnagle, 2005, str. 6)

Piškotki niso edini način za sledenje uporabnikom. Poznamo še t.i. web bug, ki lahko preveri, če je bila neka stran videna. Običajno gre za nevidne slike ali sledljive piksle, ki so zmožni oddajati nazaj na izvirni server podatke, kot so čas obiska, IP naslov, ime strani, podatke o brskalniku, piškotkih, itd. Največji vohunski potencial, ki ga ta funkcija ima, je tvorba precej natančnih profilov brskanja z določene naprave, brez da bi obstajal kak jasen dokaz, kot v primeru piškotkov prisotnost oglasa, da se podatki zbirajo.

Najnevarnejše oglaševalsko orodje, ki ga lahko dobimo, sta t.i. spyware in adware. Prvi vohuni za uporabnikom na različne načine, drugi pa prikazuje oglase, oboje pa se lahko dogaja ločeno od spletnih brskalnikov. (Hoofnagle, 2005, str. 7) Marsikdaj so ti zlonamerni delci kode vključeni v programe, ki se jih prenese preko spleta. Najbolj znana oblika spyware-a je dodatna orodna vrstica (Symantec, 2005), katere se poslužujejo tudi veliki spletni trgovci (Amazon…). Primeri takšnega »toolbar« programa so WebSearch (spyware –' watchdog'), RX Toolbar (spyware - prenos podatkov o brskanju ob obisku herz.com) in Elitebar (adware-prikaz oglasov).
V številnih primerih uporabniki sami dajo informacije z namenom povečanja informativne ali zabavne vrednosti strani, kot so npr. ankete. Pri spletnih trgovinah je takšen najbolj pogost način ustvarjanje uporabnikovih »seznamov želja«, torej označitev izdelkov, ki bi jih rad v bližnji prihodnosti kupil. Marsikdaj pa se ne zavedajo, da se lahko njihove informacije predajo tretji osebi, ki jih nato zlorablja. (Oussayef, 2008, str. 110)

Zbrane informacije lahko kategoriziramo na več načinov, vendar je za naše potrebe dovolj, če ločimo med anonimne, nepovezane in osebne informacije. Pod anonimne spadajo npr. podatki o brskalniku in IP naslov, nepovezane informacije so predvsem podatki o starosti, spolu, interesih, itd., pod osebne informacije pa lahko štejemo osebno ime, e-poštni naslov, telefon, in seveda številko kreditne kartice. (Mekovec & Hutinski, 2012, str. 1884) Čeprav se večina zgoraj navedenih podatkov zbira na anonimen način (piškotki in web bug), prostovoljno pa običajno dajemo

nepovezane informacije (ankete), je še vedno prevelika uporaba in zahteva po osebnih informacijah (seznami želja, avtomatska prijava, itd.), se moramo vprašati, zakaj se nam ne zdi nenavadno, da trgovec želi toliko informacij. Odgovor bi se lahko skrival v vsakdanjosti dajanja informacij trgovcem v zameno za manjše ugodnosti – dober primer so kartice zvestobe (Worthington & Fear, 2009) – kadar kupujemo manjše, vsakdanje izdelke. (Hoofnagle, 2005 v Oussayef, 2008) Zato se nam ne zdi nič nenavadnega, ko spletna trgovina od nas zahteva registracijo in prijavo ter da moramo obvezno podati našo telefonsko številko, tudi če ne nameravamo prejemati spremembe statusa naše pošiljke. Ali pa, da lahko kupimo izdelek po nižji ceni, če smo prijavljeni, ali morda kar pošiljanje kode s popustom skupaj z novicami v e-poštni nabiralnik (Gambit trade d.o.o., 2014)? Ali pa, da se prijavimo na novice, v zameno pa dobimo bon za 5 € (Conrad, 2014)?

Ljudje, še posebej mladi, ki moramo paziti na vsak evro, vidimo takšno promocijo oz. zbiranje podatkov kot nenevarno in vredno tveganja. Da je to generacijski pogled sta dokazala Worthington & Fear (2009), ki sta z anketo v Avstraliji ugotovila, da je kar 63% uporabnikov med 18-24 leti pripravljeno podati zasebne informacije v zameno za popust. V starostni skupini 35-44 let je bilo takšnih uporabnikov 48%, med starejšimi od 65 let pa le 35%, iz česa sta avtorja sklepala, da z leti narašča pomembnost zasebnosti. Vendar tu bi še morali upoštevati višino finančnih zmožnosti, ki jih lahko določena generacija premore.

Obstaja torej veliko možnosti, kako spletne trgovine pridobijo podatke od kupcev, nekatere so etično sporne, druge ne. Ampak kar je še bolj pomembno, smo ljudje že navajeni podajati naše osebne podatke za manjše nakupe v fizičnih trgovinah, kaj šele v spletnih, kjer so cene še malenkost nižje. Resda marsikdo ne pomisli na zasebnost, ko daje podatke, a ko nato isti potrošnik prejme na svoje ime in naslov promocijsko pošto, ponudnika katere prej sploh ni poznal, začne spoznati težo podajanja informacij. Ali pa ne.

SISTEMI VAROVANJA DIGITALNIH PRAVIC (DRM) IN ZASEBNOST

Spletne trgovine med drugim prodajajo tudi digitalne izdelke, določene pa

omogočajo takojšnje koriščenje izdelka, le prenesti ga je treba. A v resnici ni tako preprosto. Takšne trgovine imajo celotne sisteme, ki preprečujejo uporabo prenesenih izdelkov ljudem, ki tega izdelka niso kupili. Seveda gre za dodatek v kodi izdelka, katerega je, ponekod lažje, drugje težje odstraniti. Vendar tukaj ne gre za piratizacijo izdelkov, temveč nevarnosti za uporabnike, ki so takšen izdelek kupili. Najbolj očiten primer izdelka te vrste so igre. Čim jo kupimo, moramo običajno pred namestitvijo same igre na računalnik namestiti še vmesnik (»Origin«, »Steam«, »SecureDisc«…), preko katerega se bodo shranjevali profili, pri starejših igrah pa še preverjala pristnost CD oz. DVD ploščka. Pri konzolah je to že večinoma vnaprej nameščeno. Pri starejših igrah je le šlo za preverjanje pristnosti, a s časoma so se razvile bolj intruzivne zaščite (npr. »StarForce«), ki so zahtevale precej živcev in volje kupcev. Ne le, da program ni vprašal za dovoljenje pred namestitvijo, kar je že precej sporno, temveč je lahko le-ta povzročili okvare strojne opreme; poleg tega popolna odstranitev ni bila možna (WikiDot, 2006). Kmalu so začeli vključevati preverjanje preko interneta oz. telefona za tiste, ki niso imeli stalne povezave. Nekatere igre tako ni bilo mogoče igrati brez internetne povezave (npr. Assassin's Creed 2), kar dviguje precej alarmov glede zasebnosti. Program je posredoval podatke o času uporabe in profile, ki so bili naloženi kot varnostna kopija. Hrani se unikatna koda stroja, na katerem je igra nameščena, ter omejitve števila namestitev. Z rednimi posodobitvami DRM programa je težko slediti izjavam o zasebnosti, tako da je mnogo iger lahko »poklicalo domov« (npr. Spore). Tako je tudi danes, v dobi socialnih DRM. Če vzamemo za primer Origin, od založnika Electronic Arts: za vsako kupljeno igro jo je treba aktivirati z lastnim računom (in podati osnovne osebne podatke ob registraciji – tudi datum rojstva), namestiti Origin, ki se običajno zažene kar z operacijskim sistemom, ter deluje v ozadju, ločeno od iger, nato še vzpostaviti internetno povezavo in po odigrani igri počakati, da naloži profil na oblak (varnostno kopijo). V igrah samih se zbirajo točke za dosežke (»Achievements«), na račun katerih igralec marsikdaj prejme nagrade – preko tega je možno ugotavljanje lokacije, tipa igralca, obnašanja, zgodovine igranja… (Schober, 2014). Meri se tudi čas, zapravljen v igri. Na ta način zbere EA različne podatke o trgu; na primer, v katerem delu sveta je katera igra popularna, kje se največ igra, kateri uporabnik kupi igro pred izidom (preko ekskluzivnega dodatka), za katero igro se splača izdati nove prenosljive dodatke – »DLC« (glede na čas, zapravljen v igri), in nenazadnje, kdaj je čas za novo igro v določeni franšizi (upad časa igranja). Origin deluje kot socialno omrežje (lastno in integracija s popularnimi), trgovina (seznami želja…), DRM in novičarski portal. (Schober, 2014) Vse informacije, ki jih podjetje želi imeti o uporabniku njihovih storitev in izdelka se nahajajo na enem mestu.

Alternativa Originu, vsaj kar se povečanja zasebnosti tiče, je na primer tržišče GOG.com (CD PROJEKT group, 2014), ki trži igre brez DRM zaščit. A kaj, ko to marsikdaj pomeni prihod iger šele po večjem upadu prodaje, torej nekaj let po uradnem izidu. Strah o kršenju avtorskih pravic je še vedno prevelik za marsikaterega razvijalca, da bi si upali razmišljati o zasebnosti uporabnikov.

ZAKLJUČEK

Zasebnosti je v današnjem svetu vedno manj, vendar jo imamo v spletnih trgovinah vseeno več kot v fizičnih, predvsem na račun zakonodaj, ki varujejo to področje. Da seveda ne omenjamo upada prometa pri trgovinah, ki bi prekomerno kršile zasebnost. Ampak povsem druga zgodba so digitalni izdelki, za uporabo katerih moramo pogosto razkriti osebno identiteto. Poleg tega ne govorimo le o igrah, tudi video in glasba na zahtevo od kateregakoli ponudnika imajo podoben koncept kot Origin. Pred devetimi leti je Hoofnagle (2005) izrazil skrb glede DRM sistemov, in sicer, »da bi lahko vodili do standardnih praks, kjer lastniki vsebin zahtevajo od vseh strank, da se identificirajo.« Precej lep povzetek pogojev poslovanja Origina ipd., kajne?

BIBLIOGRAFIJA

Gambit trade d.o.o. (2014). Prevzeto 2014 iz enaA.com: http://www.enaa.com/

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. Journal of Strategic Information Systems, vol. 11, str. 245-270.

CD PROJEKT group. (2014). Prevzeto 2014 iz GOG.com: http://www.gog.com/

Chellappa, R. K. (2002). Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security. Prevzeto 2014 iz Goizueta Business School, Emory University Atlanta: http://www.bus.emory.edu/ram/papers/sec-priv.pdf

Conrad. (2014). Prijava na novice in dnevne akcije. Prevzeto 2014 iz Conrad: http://postar.voipex.si/prijavise.php?b=conrad&idkat=11

EA Sports. (Oktober 2013). FIFA Soccer 14. FIFA 14 . Canada: Electronic Arts Inc.

Electronic Arts Inc. (2014). Prevzeto 2014 iz Origin: Powered by EA: https://www.origin.com/en-ie/store/

Feigenbaum, J., Freedman, M. J., Sander, T., & Shostack, A. (2012). Privacy Engineering for Digital Rights Management Systems. Prevzeto 2014 iz Computer Science - Yale University: http://cs-www.cs.yale.edu/homes/jf/FFSS.pdf

Hoofnagle, C. J. (4. Marec 2005). Merchants are starting to use tactics that are similar to online data collection. Prevzeto 2014 iz epic.org: http://epic.org/reports/decadedisappoint.pdf

Mekovec, R., & Hutinski, Ž. (2012). The role of perceived privacy and perceived security in online market . Prevzeto 2014 iz Hrvatska znanstvena bibliografija: http://bib.irb.hr/datoteka/583343.Rad.pdf

Oussayef, K. Z. (2008). SELECTIVE PRIVACY: FACILITATING MARKET-BASED SOLUTIONS TO DATA BREACHES BY STANDARDIZINGINTERNET PRIVACY POLICIES. Prevzeto 2014 iz Boston University - School of Law: http://128.197.26.3/law/central/jd/organizations/journals/scitech/volume141/documents/Oussayef.pdf

Schober, F. (2014). Gaming in Glass Safe - Games, DRM & Privacy. Prevzeto 2014 iz Defcon Communications Inc.: https://www.defcon.org/images/defcon-18/dc-18-presentations/Schober/DEFCON-18-Schober-Gaming-In-Glass-Safe.pdf

Smith, H., Milberg, J., & Burke, J. (Junij 1996). Information Privacy: Measuring Individuals' ConcernsAbout Organizational Practices. MIS Quarterly (20:2) , str. 167-196.

Symantec. (2005). Techniques of Adware and Spyware. Prevzeto 2014 iz Symantec: http://www.symantec.com/avcenter/reference/techniques.of.adware.and.spyware.pdf

WikiDot. (2006). Privacy Group - StarForce. Prevzeto 2014 iz WikiDot: http://privacygroup.wikidot.com/article:starforce

Worthington, S., & Fear, J. (December 2009). The hidden side of loyalty card programs. Prevzeto 2014 iz Monash University: http://www.buseco.monash.edu.au/centres/acrs/research/whitepapers/hidden-side-of-loyalty.pdf

GOOGLE STREET VIEW, KRŠITVE ZASEBNOSTI IN REŠEVANJE PROBLEMATIKE V EU

Aleksandra Selinšek, Medijske komunikacije, 2. stopnja

KLJUČNE BESEDE:

Google, Street View, zasebnost, zakonodaja

UVOD

Google poznamo vsi uporabniki interneta, saj nas velika večina dnevno posega po njegovih storitvah. Obsega vse, od najbolj razširjene elektronske pošte Gmail, aplikacij in operacijskih sistemov za mobilne telefone (Android in Google Play) do oblačnih storitev (Google Drive), in še mnogo drugih storitev. Google je ameriško podjetje, ki sta ga leta 1998 ustanovila (takrat še) dva študenta. Trenutno so njihovi glavni prostori locirani v slavni Silicijevi dolini v Kaliforniji, povsod po svetu pa imajo svoje pisarne (uradna spletna stran podjetja Google, 2014)).

Na Googlu trdijo, da je njihovo poslanstvo in vizija organiziranje svetovnih informacij:

»To organize the world's information and make it universally accessible and useful.«
(»Želimo organizirati svetovne informacije in omogočiti njihovo dostopnost ter uporabnost za vse.«) (uradna spletna stran podjetja Google, 2014).

Uporabniku spletnih vsebin zveni to zelo vabljivo in privlačno, a Google se je v letih svojega obstoja in razvoja soočal z mnogimi tožbami in kršitvami zakonodaje. V članku se bomo osredotočili na storitev Street View, nadgradnjo Google Zemljevida, ki je v preteklih letih s posegi v zasebnost oseb razburila mnogo držav. Pregledali bomo težave, ki so se pojavile vse od oznanitve aplikacije do danes, in tudi, kako uspešno se z njimi spopada Google.

Google Street View je uporabniku prijazna in enostavna oblika zemljevida, ki omogoča ogled panoramske podobe krajev v kombinaciji z iskanjem naslovov. Posnetki mest, ulic in krajev so začeli nastajati v letu 2007 (EPIC, 2014) in projekt nikakor še ni zaključen. Trenutno je posnetega večino »zahodnega sveta«, se pravi Severna Amerika, Evropa, Avstralija, del Vzhodne Azije in del Južne Amerike (EPIC, 2014). Pred kratkim so se lotili tudi možnosti časovnega (zgodovinskega) pregleda krajev (Uradni blog podjetja Google, 2014).

ZASEBNOST

Googlova širitev Google Zemljevidov, ki vključuje Street View, pa je odprla mnogo vprašanj, povezanih z zasebnostjo (Chen, L. Kraemerv in Sharma, 2009, str. 53).
Kot zanimivost lahko izpostavimo, da se je projekt Street View leta 2007 začel kot poskusni projekt, pri katerem so na strehe taksijev montirali kamere, ki so posnele panoramske slike metropolov Združenih držav (Chen, L. Kraemerv in Sharma, 2009, str. 59). Takrat si ni še nihče predstavljal, koliko vprašanj in skrbi bo projekt zbudil, niti razsežnosti, ki jo bo dosegel. Takoj je prišlo do ogorčenih reakcij uporabnikov v zvezi z njihovo zasebnostjo, saj je Google Maps Street View prikazoval slike oseb, domov in bližnje okolice brez kakršnegakoli dovoljenja (Chen, L. Kraemerv in Sharma, 2009, str. 59). Sledilo je ogromno tožb zaradi motenja posesti in kratenja zasebnosti.

Zajem fotografij krajev poteka s pomočjo za to posebej prirejenih vozil, ki posnamejo okolico, kasneje pa so vsi posnetki sestavljeni v skupen panoramski pregled kraja. O svoji pridobitvi na uradni spletni strani zapisujejo sledeče:

»Leta 2004 smo kupili podjetje za digitalno kartografijo Keyhole ter leta 2005 predstavili Google Zemljevide in Google Zemljo. Danes Google Zemljevidi vključujejo prometne informacije, navodila za pot z javnim prevozom in posnetke v načinu Pogled ulic (Street View), Google Zemlja pa vam omogoča raziskovanje morij in Lune.« (uradna spletna stran podjetja Google, 2014).

Uporabniki lahko s pomočjo storitve Street View pred potovanjem v tuje mesto, državo ali kontinent vidimo točen izgled kraja, kamor se odpravljamo, še preden smo

tam fizično prisotni. Lahko bi se reklo, da Street View omogoča virtualna potovanja, saj si lahko s pomočjo Googla zelo natančno ogledamo velik del svetovne oble iz udobja domače dnevne sobe. Google Street View se od Google Eartha razlikuje še v tem, da omogoča 360-stopinjski pogled horizontalno in 290-stopinjski pogled vertikalno po zemljevidu, medtem ko Earth omogoča le pogled iz ptičje perspektive (Van der Sloot in Z. Borgesius, 2009, str. 79).

Street View omogoča panoramski pogled posnetkov mnogih krajev, zajetih iz avtomobilov in drugih vozil, ki vsebujejo za ta namen posebej prilagojene digitalne fotoaparate in antene (S. Rubinstein in Good, 2013, str. 79). Google je od zagona projekta Street View (leta 2007) zbudil mnogo skrbi in dilem v zvezi z zasebnostjo, debate o orodju Street View pa so skoraj izključno osredotočene na zbiranje ter prikaz slik, pridobljenih s pomočjo Googlovih kamer (EPIC, 2014). Vprašanja zasebnosti posameznikov ob oznanitvi in pričetku projekta so s časom postajala vedno bolj očitna, odgovori nanje pa so v mnogih primerih prišli prepozno.

Od samega začetka projekta so se mnogi ugovori na račun storitve Street View nanašali na zajem in prikaz obrazov ljudi in avtomobilskih registrskih tablic, saj omogočajo identifikacijo posameznikov. Kadar se ljudje nahajajo pred določenimi stavbami ali na cesti, bi jih utegnili ti podatki povezati z neprijetnimi, sramotnimi ali kakorkoli drugače občutljivimi informacijami o njihovi zasebnosti (recimo golo sončenje ali pa odhod iz striptiz kluba) (S. Rubinstein in Good, 2013, str. 80). Google se je v ZDA glede tega najprej zagovarjal, da so ceste in ulice javni prostor, kjer je pričakovanje zasebnosti minimalno (S. Rubinstein in Good, 2013, str. 80). Sčasoma so bili vseeno primorani nadgraditi svoje postopke in prilagoditi stopnjo zasebnosti: dodali so t. i. tehnologijo »pikselizacije« (na primer zameglitev obrazov in registrskih tablic) povsod po svetu (S. Rubinstein in Good, 2013, str. 85).

Street View je ostal predmet in problem zakonodaj v mnogih državah, saj zakoni o zasebnosti prepovedujejo objavo fotografij oseb brez njihovega soglasja, ali pa (so in še) lokalne oblasti smatrajo bivalne ulice kot del zasebnega prostora posameznikov (S. Rubinstein in Good, 2013, str. 91). Mnogi preiskovalci zasebnosti so vzeli Street View pod drobnogled in zahtevali, da Google ne zajema fotografij,

dokler problemi zasebnosti niso ustrezno naslovljeni. Google je večino teh problemov tekom delovanja že razrešil ali jih še rešuje (S. Rubinstein in Good, 2013, str. 80).

ZBIRANJE BREZŽIČNIH PODATKOV

Za izredno problematično se je leta 2010 izkazala ugotovitev, da je Google s pomočjo brezžičnih sprejemnikov, nameščenih v vozilih za zajem fotografij, prikrito zbiral širok spekter Wi-Fi informacij (S. Rubinstein in Good, 2013,). Google je to dejavnost kasneje, po opravljenih preiskavah, tudi priznal: šlo je za zbiranje MAC-naslovov (to je edinstven ID brezžičnega omrežja) in SSID-jev (ID omrežja, dodeljen uporabniku) v povezavi z lokacijami zasebnih brezžičnih omrežij. Priznali pa so tudi zbiranje in shranjevanje podatkov o brezžičnih prenosih, vključno z gesli in vsebino elektronskih sporočil (Cheung, 2014, str. 44).

V nasprotju s prvotnimi poskusi prepričevanja javnosti iz strani Googla, da je do zbiranja Wi-Fi podatkov prišlo po pomoti in je bilo le tehnični lapsus, je sodišče ugotovilo, da so leta 2006 Googlovi inženirji namerno vzpostavili sistem za zbiranje teh podatkov, ki je lahko zbral, dekodiral in analiziral vse vrste podatkov, prenesenih preko brezžičnih omrežij (Cheung, 2014, str. 44). Poleg tega je bilo ugotovljeno tudi, da je Google dovolil vključitev navedenega sistema, znanega kot tehnologija za brezžično »vohunjenje«, v svoja Street View vozila in postopek tudi patentiral (Cheung, 2014, str. 45).

Sledile so mnoge javne cenzure in tožbe. Google je bil primoran povečati trud za naslovitev novih (kakor tudi starih) problemov, a rezultati so bili mešani (S. Rubinstein in Good, 2013, str.51). Federal Communication Commision (v nadaljevanju FCC) je Google oglobila, ker so ovirali preiskavo in poizvedbe v zvezi z zbiranjem brezžičnih podatkov o plačilih (S. Rubinstein in Good, 2013, 51). Glede na najnovejše podatke, ki jih je FCC izdala ob objavi zadnjega poročila, zbiranje »ni bilo niti napaka niti delo površnega inženirja«, kakor je podjetje dolgo zatrjevalo, temveč je šlo za program, s katerem je nadzor bil seznanjen (S. Rubinstein in Good, 2013, str. 51). Posledično so mnoge države začele razmišljati o ponovnih preiskavah primera Google Street View (S. Rubinstein in Good, 2013, str. 50).

Lani (leta 2013) je Google zaradi nedovoljenega zbiranja brezžičnih podatkov plačal odškodnine v vrednosti 7 milijonov USD v 38 deželah (Cheung, 2014, str. 45). Po preiskavah in tožbah povsod po svetu je bil Google prisiljen opustiti nezakonito zbiranje podatkov o brezžičnih prenosih (EPIC, 2014).

GEO-LOKACIJSKE STORITVE V POVEZAVI S STREET VIEWOM

Problematika kršenja zakona v mnogih državah je tudi po reševanju prvega problema ostala. Tako je do leta 2012 Google v zvezi s storitvijo Street View preiskovalo najmanj 12 držav, najmanj 9 pa jih je obtožilo kršenja državnih zakonov (EPIC, 2014).

Eden resnejših problemov v zvezi s kršenjem zasebnosti v primeru storitve Street View je geo-lokacija dokumentov, naloženih na splet. Gre za postopek, pri katerem določene aplikacije (recimo Flickr, YouTube ali Twitter) avtomatično dodajo lokacijo, iz katere so bili dokumenti (fotografije, videi in podobno) prenešeni (Cheung, 2014, str. 46). Kot sta opozorila Friedland in Sommer (Cheung, 2014, str. 46), pa se uporabniki, ko nalagajo svoje dokumente na splet, pogosto tega niti ne zavedajo. Situacija utegne postati še posebej problematična, saj lahko v kombinaciji s tehnologijo Street View vsakdo najde točen naslov, od koder je bil dokument poslan, kar bi posledično utegnilo voditi v resnične (fizične) napade na zasebnost posameznikov (Cheung, 2014, str. 46).

Friedland in Sommer (Cheung, 2014, str. 46) sta na primer s pomočjo takšnih geo-lokacijsko označenih fotografij v kombinaciji s storitvijo Street View uspela odkriti točne naslove uporabnikov. Zlahka sta s pomočjo Twitterja in tam objavljenih fotografij izsledila tudi lokacije nekaterih zvezdnikov (Cheung, 2014, str. 46).

To pomeni, da lahko posameznik, brez da bi se tega zavedal, nehote skupaj s fotografijo, ki jo pošlje v splet, objavi tudi podatke o tem, kje se trenutno nahaja. To nikakor ni zanemarljiva informacija, saj si zlahka predstavljamo scenarij, v katerem posameznik recimo objavi, da se odpravlja na dopust, med njegovo odsotnostjo pa mu vlomilci vlomijo v hišo, saj so ga s pomočjo kombiniranja teh tehnologij zmožni zelo natančno locirati.

EVROPSKA ZAKONODAJA

Temeljne svoboščine državljanov članic EU varuje Konvencija o človekovih pravicah in temeljnih svoboščinah, ki v 8. členu Pravica do spoštovanja zasebnega in družinskega življenja navaja:

> 1. Vsakdo ima pravico do spoštovanja njegovega zasebnega in družinskega življenja, doma in dopisovanja.
> 2. Javna oblast se ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato da se prepreči nered ali kaznivo dejanje, da se zavaruje zdravje ali morala, ali da se zavarujejo pravice in svoboščine drugih ljudi (Evropska konvencija o varstvu človekovih pravic).

V tem poglavju bomo preverili, katerim načelom Direktive EU o varovanju zasebnosti podatkov Street View ne sledi in kaj bi morda lahko izboljšal.

Direktiva o varovanju podatkov je bila kot pravni akt v Evropi prvič sprejeta leta 1995, od takrat pa je dobila v skladu z napredkom tehnologij tudi mnogo dodatkov. Zadnji akt o spremembi je kot uredba stopil v veljavo leta 2003 (Direktiva Evropskega parlamenta in Sveta 95/46/ES, 2014).

Van der Sloot in Z. Borgesius (Van der Sloot in Z. Borgesius, 2009, str. 81) sta preverila, v kolikšni meri se Google drži omenjene zakonodaje.

Veljavnost Direktive iščemo, ko govorimo o »obdelovanju« »osebnih podatkov« in nadzoru le-teh (Van der Sloot in Z. Borgesius, 2009, str. 81 in 82). Oba pojma sta širše definirana v Direktivi. Osebni podatki so vsi podatki, ki jih lahko povežemo z osebo, ki jo je možno identificirati, neposredno ali posredno, zato v skladu s tem lahko trdimo, da Google absolutno obdeluje osebne podatke (Van der Sloot in Z. Borgesius, 2009, str. 85). Tako tudi fotografije oseb z zamegljenim obrazom na Street Viewu sestavljajo osebni podatki (Van der Sloot in Z. Borgesius, 2009, str. 85), saj jih

ljudje, ki jih poznajo, kljub pikselizaciji zlahka prepoznajo. Poleg tega Google Street View razpolaga tudi z zelo občutljivimi informacijami, kot so na primer rasni izvor, politična opredeljenost, versko prepričanje, podatki o zdravju in spolnem življenju. Google upravlja s temi podatki, saj določa namen in pomen podatkov, zato lahko trdimo, da te podatke tudi nadzira (Van der Sloot in Z. Borgesius, 2009, str. 86).

Van der Sloot in Z. Borgesius (Van der Sloot in Z. Borgesius, 2009, str. 91) sta opredelila tri zahteve, za katere sta ugotavljala, v kolikšni meri jih Google upošteva. Principi so bili sledeči:

- kakovost podatkov,
- zakonska podlaga za obdelavo podatkov in
- transparentnost v povezavi z upoštevanjem pravic nosilcev obdelanih podatkov (Van der Sloot in Z. Borgesius, 2009, str. 91, 97 in 102).

Ugotovila sta, da je Street View v glavnem skladen z zahtevami kar se tiče kakovosti podatkov, saj so osebni podatki obdelani z določenim in zelo specifičnim namenom (Van der Sloot in Z. Borgesius, 2009, str. 92).

Pri zakonski podlagi je situacija zelo kompleksna, saj ni pogodbene ali zakonske podlage, ki bi določala, da je obdelava podatkov potrebna, in Google s svojimi storitvami tudi ne služi življenjskim interesom oseb, nosilcev obdelanih podatkov ali javnemu interesu (Van der Sloot in Z. Borgesius, 2009, str. 98). Tako obstajata samo dve osnovi za uzakonjanje Googlove obdelave podatkov:

1. nedvoumno soglasje posameznikov ali
2. tako imenovana ravnotežna določba (Van der Sloot in Z. Borgesius, 2009, str. 98).

Direktiva prepoveduje obdelavo občutljivih podatkov, če niso zadovoljeni določeni pogoji. V primeru Street Viewa je najbolj izstopajoč problem vnaprejšnja pridobitev soglasja posameznika, ki ga določa Direktiva, saj ga Google ne pridobi (Van der Sloot in Z. Borgesius, 2009, str. 98). Možnost kasnejšega odstopa od storitve pa ne zadostuje kot nadomestilo za izrecno ali nedvomno soglasje (Van der Sloot in Z. Borgesius, 2009, str. 98). To nam pušča le drugo možnost, gre za tako imenovano ravnotežno določbo, ki dovoljuje obdelavo podatkov, kadar je to nujno potrebno za legitimne potrebe nadzornika podatkov, razen v primerih, ko prevladajo interesi varovanja zasebnosti obdelanih oseb (Van der Sloot in Z. Borgesius, 2009, str. 99). Googlov interes je nedvomno prisoten, a protiutež so temeljne pravice oseb, vključenih v proces. Postopek izdaje ravnotežne določbe je tako v primeru Street Viewa zelo zapleten, saj nekatere oblasti dovoljujejo upravljanje osebnih podatkov le v primerih, ko je zasebnost oseb dodatno zaščitena s pomočjo dodatnih ukrepov s strani Googla (Van der Sloot in Z. Borgesius, 2009, str. 99).

V primeru transparentnosti pa je potrebno upoštevati, da je Google v skladu z Direktivo dolžan zadostno in pravočasno obvestiti osebe, da bodo njihovi podatki v obdelavi. Poleg tega imajo osebe, katerih podatki so obdelani, pravico, ne le, da so obveščeni, temveč tudi, da zahtevajo popravke in ugovarjajo obdelavi podatkov v določenih okoliščinah (Van der Sloot in Z. Borgesius, 2009, str. 107). Vprašanje, v kolikšni meri je to načelo upoštevano v primeru Street Viewa, se nanaša predvsem na količino shranjenih podatkov, kako dolgo so ti podatki zadržani in kako so uporabljeni. Google upošteva pravice oseb predvsem z možnostjo naknadne zahteve, da so njihova vozila ter domovi zamegljeni (Van der Sloot in Z. Borgesius, 2009, str. 108) (uradna spletna stran podjetja Google, 2014). Seveda pa bi bilo transparentnost zagotovo možno še povečati.

ZAKLJUČEK

Google je izredno močna korporacija, njegova moč pa z leti le še raste. So zelo inovativni in prodorni. Njihove storitve vedno znova burijo duhove javnosti in zakonodajalcev. S časom in večanjem podjetja se njihova moč le še veča in ta trenutek si najverjetneje težko predstavljamo, kam nas bo njihovo zbiranje podatkov pripeljalo v prihodnosti. Seveda so se zakonodaji primorani prilagoditi, a kakor smo videli na danem primeru, so jo vsaj poskusili obiti, kršitve zasebnosti pa so bile številne. Zaradi velikosti in moči podjetja smatramo, da si tovrstne »nenamerne« spodrsljaje zlahka privoščijo, glede na vrednost podjetja pa jih tudi globe ne ovirajo pretirano.

Zaključili bi, da je Google skozi čas svoj Street View servis, kar se tiče preglednosti in varovanja zasebnosti, sicer že izboljšal, a zagotovo bodo popravki v prihodnjih letih še sledili. Utegne se tudi zgoditi, da bo prišlo do novih razkritij o varovanju in nevarovanju ter pridobitvi podatkov, pa naj gre za Google ali kakšno drugo svetovno korporacijo, saj je gonilna sila sveta, ki nas obkroža, podatek.

BIBLIOGRAFIJA

Chen, Rex, L. Kraemer, Kenneth, Sharma, Prakul. »Google: The World's First Information Utility?« Business & Information Systems Engineering 1 (2009): 53–61. DOI 10.1007/s12599-008-0011-6 URL: http://pcic.merage.uci.edu/papers/2009/Google.pdf (25. 4. 2014).

Direktiva Evropskega parlamenta in Sveta 95/46/ES URL: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_sl.htm (6. 5. 2014).

EPIC – Electronic Privacy Information Center: »Investigations of Google Street View« URL: http://epic.org/privacy/streetview/ (6. 5. 2014).

Evropska konvencija o varstvu človekovih pravic URL: http://www.varuh-rs.si/fileadmin/user_upload/word/Temeljni_dokumenti_VCP/Konvencijo_o_clovekovih_pravicah_in_temeljnih_svoboscinah.pdf (6. 5. 2014).

S. Rubinstein, Ira, Good, Nathaniel. »Privacy by design: A counterfactual analysis of google and facebook privacy incidents.« Berkeley Technology Law Journal Vol. 28 (2013): 1335–1412 URL: http://btlj.org/data/articles/28_2/1333-1414_Rubinstein&Good_11262013_Web.pdf (24. 4. 2014).

S.Y. Cheung, Anne. »Location privacy: The challenges of mobile service devices.« Computer law & security review 30 (2014) 41–54 URL: http://www.sciencedirect.com/science/article/pii/S026736491300201X (25. 4. 2014).
Uradna stran podjetja Google URL: http://www.google.com/about/company/ (6. 5. 2014).

Uradni blog podjetja Google URL: http://googleblog.blogspot.com/2014/04/go-back-in-time-with-street-view.html (6. 5. 2014)

Van der Sloot, Bart, Zuiderveen Borgesius, Frederik. »Google and Personal Data Protection.« Google and the Law, Information Technology and Law 22 (2012): 75–111. Dostopano

Kossinets, Gueorgi, and Duncan J. Watts. "Origins of Homophily in an Evolving Social Network." American Journal of Sociology 115 (2009): 405–50. DOI:10.1086/599247. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2146968 (25. 4. 2014).

RAČUNALNIŠKA/INFORMACIJSKA PISMENOST MLADIH V SLOVENIJI

Veronika Senekovič, Medijske komunikacije, 2. stopnja

»Tako kot vsaka pismenost je tudi informacijska pismenost opredeljena z okoljem in časom. Opredeljuje jo informacijska družba, v kateri je informacija neskončen proizvod, naše potrebe po informacijah pa eksistenčne. Oblikuje jo tehnologija, ki spreminja način oblikovanja, hranjenja, dostopnosti in uporabe informacij, ki je razširila ne samo količino ampak tudi obliko sporočil.« (Novljan, 2002; 8)

Informacijska doba je doba, v kateri živimo, in kot informacijska družba, katere skupek smo, od nas zahteva ustrezno raven *računalniške* in *internetne pismenosti*[1]. Doba informacijske družbe traja že več kot desetletje, vendar še vedno rezultati pismenosti, tako računalniške kot internetne, niso zadovoljivi. Pomanjkljivo digitalno pismeni posamezniki so izključeni iz informacijske družbe in gospodarstva, vedno več pa je delodajalcev, ki zahtevajo od kandidatov za delo poznavanje programske opreme in interneta.

Vsepovsod po svetu obstajajo statistično značilne razlike v računalniški in informacijski pismenosti glede na spol, ter glede na izobrazbo in regijo. Kljub njeni majhnosti tudi v Sloveniji prihaja do digitalnega razkoraka med regijami, mestnimi središči in vasmi. Številne študije in raziskave, med drugim raziskava European Social Survey (ESS), so pokazale, da je lahko širjenje informacijskih komunikacijskih tehnologij porazdeljeno neenakomerno, tako med državami kot tudi znotraj držav, med različnimi družbenimi skupinami. Pojavi se, že prej omenjen digitalni razkorak, ki se nanaša na razlike med posamezniki, gospodinjstvi, podjetji in geografskimi območji glede možnosti dostopa do informacijskih komunikacijskih tehnologij ter njihove uporabe. Do te ločnice pride zaradi zgodovinskih, socialno-ekonomskih,

[1] »V praksi se bolj kot ne uporablja pojem digitalna pismenost, vendar pa lahko ta pojem nadomestimo z računalniško in internetno pismenostjo oz. e- spretnostjo. E-spretnosti (angl. e-skills) so ena izmed najpomembnejših prioritet informacijske družbe. Največkrat e-spretnosti ugotavljajo z naborom nalog (opravil), ki jih je mogoče opraviti z računalnikom ali prek interneta.« (Sulčič, 2011; 147-148).

geografskih, izobraževalnih, vedenjskih, generacijskih dejavnikov ali pa zaradi fizične nezmožnosti posameznikov za uporabo informacijskih komunikacijskih tehnologij. Ponekod po državi se že pojavljajo razlike med revnim in bogatim prebivalstvom, prav te razlike pa bi lahko prinesle posledice, kot so zamere in morebitno nasilje med tema dvema ekonomskima razredoma, opozarjajo strokovnjaki.[2]

V statistiko o uporabi računalnika iz leta 2013 je bilo zajetih 1.677.006 posameznikov starih od deset do štiriinsedemdeset let. Tema članka je pismenost mladih, zato smo se osredotočili predvsem na uporabnike stare med šestnajstim in štiriindvajsetim letom. Glede na omenjeno statistiko imajo mladi v teh letih veliko več »e-spretnosti« kot ostala populacija v Sloveniji, prav tako so nad povprečjem Evropske unije.

»Če slovenski uporabniki računalnika in interneta zaostajajo za povprečjem evropskih držav, pa je slovenska mladina med šestnajstim in štiriindvajsetim letom pred vrstniki držav Evropske Unije.« (Sulčič, 2011; 149)

Statistični podatki o uporabi računalnika za preteklo leto kažejo, da je bilo v Statističnem uradu Republike Slovenija (SURS) zabeleženih 196.579 mladih, torej 11,7 odstotkov, od skupno vseh 1.677.006 v starostni skupini od šestnajst do štiriindvajset let. V Sloveniji je v vseh starostnih skupinah skupno 59,9 odstotkov rednih uporabnikov računalnika, od tega jih samo 0,8 odstotkov ne uporablja interneta. Od vseh rednih uporabnikov računalnika (59,9%) predstavlja starostno skupino od šestnajst do štiriindvajset let 17,9 % anketirancev, od česar pa jih 97,7 % redno uporablja tudi internet. Redni uporabniki interneta uporabljajo internet za različne namene. Med najbolj razširjenimi storitvami je prav gotovo elektronska pošta, ki se je znašla tudi v samem vrhu najbolj razširjenih storitev, tako med slovenskimi uporabniki kot tudi med preučevano skupino med šestnajstim in štiriindvajsetim letom. Na internetu najdemo tudi pomembne informacije povezane s šolanjem ali pa z iskanjem zaposlitve preko raznih študentskih servisov. Mladi se na internet

[2] Eden izmed člankov, ki se dotakne globalnega digitalnega razkoraka, ter njenih posledic je članek 15 Thesis about the Digital Future od Janne Anderson in Lee Rainie, kjer se pod poglavjem Less-hopeful theses avtorici članka dotakneta prav te teme. Poleg nevarnih razlik med bogatimi in revnimi- kar prinaša digitalni razkorak, sta zapisali, da je nevarna stran digitalne prihodnosti tudi to, da se bodo večale zlorabe na internetu, še posebej »samo-zloraba«, zloraba pred samim sabo.

pogosto povezujejo tudi zaradi sodelovanja v spletnih družbenih omrežjih, branje spletnih časopisov, novic, revij, iskanje informacij povezanih z zdravjem, izobrazbo, tečaji,… (Sulčič, 2011; 156)

Mladi uporabljajo internet tudi za ustvarjanje lastnih blog-ov in komentiranjem v spletnih časopisih, ter povezovanje med mladimi iz celega sveta, s katerimi izmenjujejo izkušnje, doživetja.

Slovenija je bila glede e- vključenosti leta 2010 v povprečju držav Evropske Unije, pa čeprav je še leto pred tem zaostajala za njimi. Slovenska mladina v starostni skupini od šestnajstega do štiriindvajsetega leta pozitivno vpliva na statistične podatke o rabi računalnika in interneta v Sloveniji, saj so med mladimi redki posamezniki, ki še niso uporabljali računalnika in interneta. Mladi uporabniki bi se morali bolj zavedati pomena računalniške pismenosti, saj je nujno potrebna za lažjo zaposljivost v času »brezposelnosti« kot tudi širjenje lastnega obzorja. Poznavanje programske opreme bi moralo biti v osnovni šoli eden izmed obveznih predmetov, in ne zgolj izbirni. V računalniški in informacijski pismenosti tako obstaja svetla prihodnost mladih v Sloveniji.

BIBLIOGRAFIJA

Anderson, J., Rainie, L. 15 Thesis about the Digital Future.2014. Dostopno preko: http://www.pewinternet.org/2014/03/11/15-theses-about-the-digital-future/ (zadnji dostop 1.7.2014)

Novljan, S. Informacijska pismenost. 2002. Dostopno preko: http://revija-knjiznica.zbds-zveza.si/Izvodi/K0204/novljan.pdf (zadnji dostop 8.5.2014).

Sulčič, V. Računalniška in internetna pismenost slovenske mladine. 2011. Dostopno preko: http://www.dlib.si/details/URN:NBN:SI:DOC-VD78BXQF/ (zadnji dostop 8.5.2014).

Statistični urad Republike Slovenija. Dostopno preko: http://www.stat.si/tema_ekonomsko_infdruzba_informacijsko.asp (zadnji dostop 8.5.2014).

SEM VAREN NA SPLETU?

Zoran Bencak, Medijske komunikacije, 2. stopnja

KLJUČNE BESEDE:

kraja identitete, vdori, spletne prevare

Kraja identitete je kriminalno dejanje, ki se ne ozira na starost, spol, veroizpoved ali etnično pripadnost. Žrtev je lahko vsak, ki ima bančni račun, kreditno kartico, računalnik, vozniško dovoljenje ali kakršenkoli drugi dokument. Internet je postal najbolj priljubljeno komunikacijsko orodje današnjega časa, saj ga uporablja več kot 2.5 milijarde ljudi po celem svetu (United Nations Office on Drugs and Crime, 2013, str. 18).

Ker pa uporabniki po vsaki aktivnosti na spletu pustimo svojo digitalno sled, spletni kriminalci nenehno prežijo za novimi žrtvami. Že z izpolnjevanjem najbolj osnovnih spletnih obrazcev, registracijo na forumih ali spletnim nakupovanjem lahko le-ti pridobijo dovolj podatkov za ugotavljanje prebivališča, telefonskih številk ali številke bančnih kartic. Namen tega članka je uporabnike spleta spoznati z nevarnostmi, s katerimi se srečujemo pri uporabi spleta, kako se zaščititi pred tovrstnimi nevarnostmi ter na koga se lahko obrnemo v primeru, če smo žrtve spletne prevare.

Nepridipravi se do osebnih podatkov lahko dokopljejo na različne načine. Nekateri ustvarjajo lažne spletne strani, ki so skoraj identične izvirnim, boljši programerji pa ustvarijo programsko opremo, preko katere dostopajo do žrtvinega računalnika. Torej lahko kibernetsko kriminaliteto opišemo kot kriminaliteto, kjer se informacijska tehnologija – računalnik, pametni telefon, tablica uporablja kot predmet napada (Završnik, 2005). Gre za kakršnokoli protipravno dejavnost, ki zajema vdor, vmešavanje, kopiranje, odstranitev ali drugo manipulacijo z računalniškimi sistemi, podatki ali programi.

Informacijski pooblaščenec krajo identitete definira kot uporabo osebnih podatkov oz. identitete nekoga drugega za pridobitev neke koristi ali inkriminacijo druge osebe. To pomeni posebno vrsto hudega in nepovratnega posega v varstvo osebnih podatkov. Kraja identitete se ne nanaša na premoženjski vidik, temveč posega v osebnost žrtve. Tako so lahko posledice tega kriminalnega dejanja primerljive z posledicami ostalih nasilnih kaznivih dejanj. Vendar pa kraja identitete ni samo zloraba osebnih podatkov, saj je povezana z namenom, pridobivanja koristi (Informacijski pooblaščenec, stran 5).

Pri kraji identitete gre za več vrst napadov – glede na osebo, ki izvaja napad (pooblaščena ali nepooblaščena), glede na to, ali so podatki ukradeni iz podatkovne zbirke ali med pretokom po omrežju, glede na motiv (finančna kraja, kriminalna kraja in prevzem identitete v vsakdanjem življenju) ter glede na izbrano metodo (tehnična ali ne-tehnična) (Informacijski pooblaščenec, stran 6).

Obstaja več metod kraje identitete. Med najbolj prepoznavne metode spada vdor (ang. hacking). Pri tej metodi napadalec izkorišča ranljivost ter slabost informacijskega sistema. Če uspe vdreti v računalnik, ima takoj dostop do vseh podatkov, ki jih ima žrtev na računalniku (SI-Cert, Vdori). Med razširjene metode spadajo tudi virusi. To so majhni programi, ki lahko negativno vplivajo na zdravje našega računalnika. Virusi lahko ustvarjajo nove datoteke, jih brišejo ali premikajo ter krepko povečajo porabo pomnilnika, kar povzroči moteno delovanje računalnika. Lahko se podvajajo, se pripnejo k drugim datotekam in potujejo po omrežju. Odprtje okuženega emaila je najpogostejši način okužbe računalnika (Techterm). Ribarjenje (ang. phishing) je izraz za krajo podatkov, ki storilcu omogočijo dostop do spletnih storitev v našem imenu in v skrajnem primeru tudi krajo našega denarja. Pri tej metodi nas storilec skuša z elektronskim sporočilom zvabiti na lažno spletno stran banke, pod pretvezo, da se moramo zaradi preverjanja podatkov prijaviti in »preveriti podatke«. Če na tej lažni strani vpišemo uporabniško ime in geslo za vstop, se le-to posreduje storilcu (Si-Cert, Phishing). Med škodljivo programsko opremo in kodo spadajo tudi vohunska programska oprema (spyware), adware in trojanski konji. Spyware se najpogosteje pretihotapi v naš računalnik med običajnim brskanjem po internetu, pri čemer izrabljajo varnostne pomanjkljivosti brskalnikov ali pa z nameščanjem različnih dodatkov in programov. Spyware brez naše vednosti lahko beleži gesla in druge podatke preko katerih se povezujemo v

internet. Adware je škodljiva koda, ki deluje podobno kot virusi in črvi – uporabnike zasipa z različnimi oglasi in nezaželeno elektronsko pošto. Razlikuje se le v tem, da se ni sposobna širiti na iz enega na druge računalniške sisteme. Trojanski konji pa pridejo v naš računalnik v preobleki legitimnega programa – ob namestitvi legitimnega programa se namesti tudi trojanski konj, ki napadalcem omogoči prevzem nadzora nad računalnikom (Informacijski pooblaščenec, str.8).

Januarja 2012 je v svetovnem merilu po spletu krožilo 0.33% zlonamerne e-pošte, ali eno zlonamerno na 295 sporočil, ki so bila okužena z virusom ali pa so predstavljala nevarnost okužbe za računalnik. Tu prednjači predvsem Nizozemska (1 na 61,4 sporočil), sledijo pa ji Velika Britanija (1 na 169,1) in Luksemburg (1 na 205,4). V tem obdobju je Symantec zaznal povprečno 2102 novih zlonamernih spletnih strani na dan – od tega 26 strani, ki so vsebovale vohunske programe in kar 2067 spletnih strani, ki so vsebovale viruse. (Symantec, 2012)

Kraja identitete je v Sloveniji z novim Kazenskim zakonikom Republike Slovenije definirana kot kaznivo dejanje, pri katerem storilec pridobi določene ključne osebne podatke, kot so na primer številke osebnih dokumentov, skupaj z enoznačnimi identifikatorji (v slovenskem pravnem redu sem uvrščamo EMŠO in davčno številko), za pridobivanje tako osebne, kot premoženjske koristi. Kaznivo dejanje zlorabe osebnih podatkov je določeno v 143. členu Kazenskega zakonika (KZ-1, 2012).

Slovenski nacionalni center za posredovanje pri omrežnih incidentih (SI-CERT) je v letu 2011 zabeležil 261 prijav spletnih goljufij in kraje identitete, kar je 92% več kot v letu 2010. V ZDA je vsako leto več kot 10 milijonov primerov kraje identitet (Računalniške novice).

V Novi Zelandiji se je 18. letni Owen Thor pridružil mednarodni kibernetsko kriminalni skupini, ki je vdrla v več kot milijon računalnikov in jih uporabila za krajo skoraj 20 milijonov ameriških dolarjev (Fraud-magazine.com).

Michael Dolan je izpeljal phishing prevaro, ki je imela za tarčo naročnike ponudnika interneta America Online (AOL). V štirih letih si je s skupino svojih hekerjev prilastil 400.000 ameriških dolarjev, kasneje je bil obsojen na 7 let zapora (Tomsguide.com). Posebna vrsta kraje identitete, ki je predvsem mobilne operaterje opozorila na pomen preverjanja identitete, je bil primer, ko so neznanci prepričali brezdomca, da je sklenil naročniško razmerje pri enem od pooblaščenih agencij za sklepanje naročniških razmerij. Zaradi pehanja po večjem številu naročnikov so novo naročniško razmerje sklenili brez večjih težav oz. preverjanja novega naročnika, neznanci pa so s pomočjo tako pridobljenega telefona opravili za več tisoč evrov neplačanih klicev v tujino (Informacijski pooblaščenec, stran 14).

Podam lahko tudi lasten primer ter primere znancev, ki so izkusili poskus zlorabe profila v socialnem omrežju Facebook. Napadalec je najprej spremenil geslo Facebook računa, zaradi česar je posledično zlorabil tudi elektronsko pošto. V vsakem našem poskusu spreminjanja gesla je le-tega vnovič spremenil, dokler račun ni bil zaščiten. Ugotovljeno je bilo, da so bili med prijatelje dodani neznani ljudje z različnih kontinentov, prebrana sporočila, komuniciranje z drugimi ter tudi pošiljanje slik s profila različnim dodanim osebam. Gesla smo vsi nemudoma po napadu spremenili, znanka pa je podala prijavo tudi na policijo zaradi nedovoljenega pošiljanja osebnih fotografij in lažnega predstavljanja drugim osebam pod njenim imenom. Računi so bili dodatno zaščiteni, gesla pa spremenjena, nihče, razen znanke ni utrpel hujše zlorabe.

Tehnologija se razvija zelo hitro, z njo pa tudi kibernetski storilci, zaradi česar posledično kriminal narašča. Zavedati se moramo problema zlorabe identitete in biti informirani o načinih njenega preprečevanja. Z malo tehničnega znanja ter pravilnega razmišljanja, jo lahko vsak posameznik pravočasno prepreči. Ker večina tovrstnih kriminalcev želi na lahek in hiter način priti do informacij, bodo hitreje obupali, ko jim bomo pridobitev teh informacij otežili. V ta namen je priporočljivo uporabljati varnostno programsko opremo. Sem spadata protivirusna programska oprema in požarni zid, ki ju je potrebno sproti posodabljati. Strokovnjaki navajajo še nekaj drugih nasvetov: uporaba filtrov, ki ločujejo vsiljeno od prave elektronske pošte, uporaba dodatkov v spletnih brskalnikih, ki nam onemogočajo prikazovanje oglasov na spletnih straneh, ki jih obiskujemo (Microsoft). Oglasi so namreč lahko zlonamerni in nas vodijo na lažne spletne strani ali pa se s klikom nanje na naše

računalnike namestijo trojanski konji. Hkrati je pomembna je tudi uporaba močnih gesel, katera bi po nasvetu strokovnjakov morali menjati vsaj nekajkrat na leto. Pri izbiranju gesel moramo biti pozorni na to, da si izberemo takšno, ki ga je težko uganiti – ne sme vsebovati imen, rojstnih datumov, kraja rojstva, itn. Vsebovati mora male in velike črke, številke in simbole ter biti dolgo vsaj 7 znakov. Prav tako moramo spremljati »zdravje« računalnika. V primeru počasnega ter neustaljenega delovanja računalnika, velikega števila nezaželjenih oglasov, itn., obstaja možnost, da je le-ta bil okužen, zato ga je potrebno očistiti.

Kljub nenehnim nevarnostim, s katerimi se soočamo uporabniki svetovnega spleta, obstaja kar nekaj metod za preprečevanje kraje identitete. Na najlažji način se jim lahko izognemo z upoštevanjem varnostnih navodil pri uporabi spleta, vsekakor pa je priporočljivo tudi spremljanje in seznanjanje z novostmi obravnavanega področja, saj je konec koncev vsak posameznik sam odgovoren za svoja dejanja ter varovanje svojih osebnih in finančnih podatkov.

BIBLIOGRAFIJA

Fraud-magazine.com, Identity Theft. Dostopno na: http://www.fraud-magazine.com/article.aspx?id=412

Informacijski pooblaščenec. Smernice za preprečevanje kraje identitete (n.d). Dostopno na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Smernice_kraja_identitete.pdf

Kazenski zakonik. Zloraba osebnih podatkov. 2012. Uradni list Republike Slovenije, 143.člen (14.6.2012). Dostopno na: http://www.uradni-list.si/1/objava.jsp?urlid=201250&stevilka=2065

Microsoft, Safety. Dostopno na: http://www.microsoft.com/security/pc-security/default.aspx

Oblike varnostnih groženj, SI-Cert. Vdori (n.d.). Dostopno na: https://www.cert.si/si/varnostne-groznje/vdor/

Računalniške novice, Varni na spletu. Dostopno na: http://www.racunalniske-novice.com/novice/splet/spletni-portali/varni-na-spletu--najvec-lahko-storimo-sami.html?RSS6ce5ea0b5f54b7dff15608c8cea90e67

Rustemagić, E. Kraja identitete v kibernetskem prostoru : diplomsko delo univerzitetnega študija Varstvoslovje. 2012. Ljubljana. (PDF). Dostopno na: http://dkum.uni-mb.si/IzpisGradiva.php?id=38529

Si-Cert, Phishing. Dostopno na: https://www.cert.si/si/varnostne-groznje/phishing/

Symantec. (2012). Symantec Intelligence Report: January 2012. Dostopno na: http://www.ris.org/uploadi/editor/1330375306b-intelligence_report_01_2012.en-us.pdf

Techterms, Virus. Dostopno na: http://www.techterms.com/definition/virus

Tomsguide, AOL Spammer Michael Dolan Sentenced to 7 years. Dostopno na: http://www.tomsguide.com/us/Michael-Dolan-AOL-Spammer,news-2355.html

United Nations Office on Drugs and Crime. (2013). Comprehensive study on Cybercrime. Dostopno na: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Završnik, A (2005). Kibernetična kriminaliteta – (kiber) kriminološke in (kiber)viktimološke posebnosti "informacijske avtoceste". Revija za kriminalistiko in kriminologijo, 56(3), 248-260

SAFETY@EMAIL.COM

Gornik Filip, Koren Matjaž, Primčič Jernej, Ratajc Robert,
Medijske komunikacije, 1. stopnja

POVZETEK

Spletna tehnologija je v informacijski družbi najpomembnejši vir komunikacije. Seveda pa tehnologija, ki ima do današnjega dne že skoraj 3 milijarde uporabnikov s seboj prinaša določena tveganja. Predvsem pa se odpira vprašanje, ali so vrednote in načela kot so resnicoljubnost, zasebnost, poštenost, pravičnost in zaupanja še vedno temeljne vrednote v množičnih medijih oziroma v informacijski in demokratični družbi. V naši raziskavi smo se osredotočili predvsem na elektronsko pošto, saj dnevno v velikih količinah kroži po spletu, tako poslovno kot privatno. V članku so predstavljene nevarnosti e-pošte, najpogostejše vrste napadov, ter kako se pred njimi zaščititi, kakšen vpliv ima ranljivost e-pošte na uporabnike, ter ponazorjen nadzor elektronske pošte s strani »nadzornikov«. V sklopu tega smo primerjali naše rezultate (pridobljene z anketnim vprašalnikom) z s že obstoječimi podatki, pri čemer lahko zatrdimo, da se, glede na našo raziskavo, ljudje ne zavedajo dovolj, da sta načelo zaupanja in zasebnost kot vrednota v množičnih medijih in v informacijski dobi veliko bolj izpostavljena nevarnostim. Glede na izveden eksperiment, s katerim smo poskušali preveriti obveščenost uporabnikov o nevarnostih, ki jih s seboj prinaša e-pošta, pa lahko potrdimo, da so nekatere vrednote in načela ob vdoru v posameznikovo elektronsko pošto poteptane ter da lahko s tem škodujemo njemu in drugim vpletenim. S svojimi izsledki smo dokazali tudi, da za napad na posameznikovo e-pošto ne potrebujemo večjega znanja s področja IT, oziroma računalništva, pač pa ga lahko izvede vsak posameznik, ki ima dostop do sistema povezanega s svetovnim spletom.

KLJUČNE BESEDE

napad, obramba, e-pošta, socialni inženiring, zasebnost, zaupanje, nadzor

Uvod

Življenje posameznika v informacijski družbi je tesno povezano z uporabo komunikacijskih sredstev, ki omogočajo hitro, kvalitetno in zanesljivo komuniciranje z drugimi. Elektronska pošta predstavlja eno izmed glavnih sredstev komuniciranja preko interneta vse od njegovega nastanka. Ponudniki storitev elektronske pošte pa ne ponujajo zgolj pošiljanja in sprejemanja informacij, temveč uporabniku ponujajo celovito uporabo njihovih storitev, ki zajema nastavitev elektronskega naslova, gesla, arhiviranje elektronske pošte in tako naprej. Zaradi njihove ponudbe uporabnik čuti, da ima popoln nadzor nad informacijami, ki jih pošilja preko elektronske pošte. Občutek nadzora daje uporabniku občutek zasebnosti in zaupanja, vendarle pa je lahko vsak tarča napadov, kraje informacij ali identitete ter prisluškovanja. V prvem delu članka vam bomo odgovorili na naslednja vprašanja: Ali je elektronska pošta res zasebna? Ima uporabnik nad elektronsko pošto res celovit nadzor in lahko storitvam zaupa? Kdo vse ima vpogled v elektronsko pošto posameznika? Kakšni napadi so možni? Ali se lahko obranimo in kako? Predstavili vam bomo teoretično ozadje, ki leži znotraj elektronske pošte, uprli se bomo na (i) (Ne)Varnost elektronske pošte, ter ali (ii) Zaupanje elektronski pošti predstavlja navidezen nadzor. Prav tako ne smemo pozabiti na zlorabe s strani ponudnikov storitev elektronske pošte, avtoritativnih institucij ter posameznikov v družbi, ki se ukvarjajo s krajo informacij ter z neposrednim vdiranjem v uporabnikovo zasebnost rušijo njegovo percepcijo nadzora nad elektronsko pošto. Z namenom da vse skupaj podkrepimo, smo opravili (iii) eksperiment, ki smo ga opisali v drugem delu članka. Z njim nazorno predstavljamo problem elektronske pošte, da je lahko vsak tarča napada, ter da lahko z zelo malo porabljenega časa ukrademo e-poštni naslov posameznika in s tem vplivamo na veliko skupino ljudi. Eksperiment je tudi pokazal, da so ljudje premalo osveščeni o sami elektronski pošti in verjamejo, da je velika večina sporočil, ki jih prejmejo, legitimnih. Na samem koncu članka (iv) pa bomo predstavili podatke pridobljene z anketo, ki prikazujejo nekatera zaskrbljujoča statistična dejstva o sami uporabi elektronske pošte.[1]

ELEKTRONSKA POŠTA IN NJENA (NE)VARNOST

Da lahko razumemo karkoli o e-pošti (ang. e-mailu), moramo najprej vedeti, kaj le-ta sploh je. Je sistem za tekstovno komuniciranje med dvema ali več uporabniki preko spleta. Prva elektronska pošta je bila uspešno poslana leta 1971, poslal pa jo je Ray

[1] Ob tem bi se radi zahvalili naši mentorici doc. dr. Smiljani Gartner za spodbudo, konstruktivno usmerjanje in vodenje projekta ter profesorju dr. Frideriku Klampferju za dano priložnost.

Tomlinson. (Završnik, 2010). Po podatkih statističnega urada republike Slovenije iz leta 2013, je kar štiriinšestdeset odstotkov uporabnikov internet uporabljalo za pošiljanje elektronske pošte. Čedalje več uporabnikov je tudi starejših (65-74 let), leta 2008 jih je bilo zgolj štiri odstotke, v prvem četrtletju 2013 pa jih je bilo kar petindvajset odstotkov (SURS, 2013). Zraven tega je analiza podatkov Statističnega urada republike Slovenije pokazala, da osemdeset odstotkov uporabnikov za izvajanje poslovnih komunikacij raje uporablja e-pošto, kot telefonske storitve (META, 2003). Splet je tako pritegnil že skoraj 3 milijarde uporabnikov (Internet Live Stats, brez datuma), ter s tem veliko potencialnih žrtev. Zaradi tega je varnost postala vroča tema diskusije v informacijski tehnologiji, saj se vdori v račune uporabnikov vedno znova pojavljajo na naslovnicah.

Med prebivalci ZDA, v povprečju ni najstrašnejša stvar več teroristični napad, pač pa kraje identitete, ki se v večini primerov pričnejo prav z vdorom v elektronsko pošto (C. White, 2012; Rogers, 2013; Reaves, 2002). Tudi Slovenija ni osamljena oaza, vendar je pri nas ta strah bistveno manjši, saj je tudi teh primerov bistveno manj (10 milijonov primerov v ZDA – 56 v Sloveniji). Hkrati s t. i. individualnimi spletnimi napadi se pojavljajo tudi množični spletni napadi. Žrtev takšnega napada leta 2011 je bil Sony-jev Playstation Network[2] (Staff Writers of "OnlineCollegeCourses", 2013). Če je torej lahko prizadeta cela množica naenkrat, kako preprosta mora biti izvedba napada na e-pošto posameznika? Vprašanje, na katerega bomo odgovorili v nadaljevanju članka.

Iz letnega poročila Nacionalnega odzivnega centra za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (SI-CERT) je razvidno, da je bilo v letu 2013 na območju Slovenije prijavljenih 525 kršitev, in sicer: 56 kraj identitete, 210 primerov goljufij, 50 primerov nezaželene elektronske pošte (ang. SPAM) in kar 209 primerov Elektronskega ribarjenja (ang. phishing). Kaj natančno to pomeni? Slednje pomeni »(…) kraja podatkov, ki storilcu omogočajo dostop do spletnih storitev v vašem imenu in v skrajnem primeru tudi krajo vašega denarja.« (SI-CERT S. c.) ter same sprožitve virusov, morajo biti ti preneseni po nekem mediju. Najpogosteje se za prenos uporabljajo vsiljeno pošto, (ang. spam, junk mail, third-class mail ipd.)

[2] Leta 2011 je bilo okoli 70 milijon Sony Playstation Network računov žrtev spletnega napada s strani neznanih hekerjev. Tako je nekdo pridobil 70 milijonov zasebnih podatkov (imena, naslove, datume rojstva, kot tudi podatke bančnih kartic). (Technology, 2011)

katero lahko definiramo kot :»(…) nezaželena sporočila, ki so v identičnih izvodih poslana na tisoče ali celo milijone elektronskih naslovov ne da bi si prejemniki to želeli oziroma v to privolili.« (Upelj, 2006) Za pošiljanje teh se napadalci poslužujejo dveh korakov. V prvem koraku uporabijo večje število predhodno okuženih sistemov (ang. botnet), s katerih pošiljajo svoja sporočila, ki vsebujejo okuženo datoteko (ang. virus) ali povezavo na okuženo spletno stran (Ramneek, 2014). Po definiciji je virus »(…) sestavljen iz dveh ključnih korakov, in sicer iz dostave ter proženja oziroma implantacije in zagotovitve čim daljše življenjske dobe implementirane škodljive programske kode.« (Dimc & Dobovšek, 2012). Drugi korak pa je, da na novo okužen sistem postane eden izmed tistih, ki so mu prvotno poslali vsiljeno pošto, ter posreduje sporočilo novim žrtvam.

Bolj kot za prenos elektronskih virusov se vsiljena pošta uporablja za tako imenovano ribarjenje. Tako kot virus se širi s pomočjo vsiljene pošte, saj tako najhitreje pride direktno do uporabnika oz. uporabnikov. Primeri ribarjenja se dogajajo po celem svetu, tudi na področju Slovenije. Primer tovrstnih napadov, je napad na uporabnike SiOL-ove elektronsko poštne storitve, ki je od uporabnika zahtevala, da zaradi »nadgradnje« SiOL potrebuje njihov e-poštni naslov, geslo, datum rojstva, itd. (SI-CERT S. c., brez datuma). Z ribarjenjem lahko napadalec torej dobi dostop do naših osebnih podatkov in posledično dostop do naših bančnih računov ter se tako okoristi. Ribarjenje deluje na principu izdajanja napadalca za zaupanja vredno osebo/organizacijo. Vse, kar napadalec potrebuje, je e-poštni naslov organizacije, e-poštni naslov žrtve, ter spletno stran, ki deluje legitimno (npr. spletno banko). Ker se zlonamerna sporočila skoraj ne razlikujejo od pravih, jih programska zaščitna oprema težko izloči, ter opozori uporabnika, zato je najučinkovitejša in najzanesljivejša metoda obrambe pred ribarjenjem izobraževanje na področju informacijske tehnologije (ang. IT), ki pa je pogosto pomanjkljivo (Kumaraguru, 2007).

V primeru, da ima napadalec dostop do posameznikovega e-poštnega naslova, lahko mnogokrat dostopa do večine storitev, ki jih ta posameznik uporablja, saj večina le-teh zahteva e-poštno potrditev ob registraciji. Tako lahko pride do kraje uporabnikove identitete, s katero napadalec razpolaga po želji. Da pa

lahko razumemo kaj kraja identitete sploh je, moramo najprej definirati, kaj to sploh je: »(…) prevladujoče definicije identitete bi lahko razvrstili na dimenziji, ki bi se raztezala med znotraj in zunaj. Prva skupina definicij je osredotočena okrog notranjih procesov v posamezniku kot izvoru istosti in identičnosti v času. Na drugi strani kontinuuma se koncepti identitete osredotočajo na kulturne in družbene strukture in konvencije, ki vplivajo na to, kakšni smo za druge in sebe.« (Ule, 2000). Torej je identiteta nekaj, kar nas dela drugačne, unikatne ter nekaj, s čim smo prepoznavni drugim kot individuum. Kraja identitete je postala oz. postaja vedno bolj popularna na področju spletnega napadalstva. Dnevno napadalci vdrejo v več kot šeststo tisoč uporabniških računov na Facebooku, kar predstavlja sedem uporabniških računov na sekundo (Staff Writers of "OnlineCollegeCourses", 2013).

Ko pride do varnosti elektronske pošte, pa je potrebno izpostaviti, da veliko ljudi uporablja pogosta, generična gesla, ki jih je lažje ugotoviti. Podjetje SplashData je leta 2013 naredilo raziskavo, s katero so ugotovili, da je najpogostejše geslo "123456", takoj za njim pa je "password" (Doel, brez datuma). Seveda pa se da pridobiti dostop do uporabniškega računa tudi s preizkušanjem vseh hipotetičnih kombinacij znakov. To je tako-imenovan "brute force" napad, kjer napadalec lahko uporabi besede iz slovarjev, sezname pogostih gesel, ali pa preprosto preizkusi vse možne kombinacije, dokler ne najde prave. Ta napad je izjemno počasen, saj imajo moderni računalniki omejeno hitrost procesiranja , ter lahko tako trajajo dneve oziroma mesece (Spector, 2014)Uporabnik se lahko pred tem zaščiti s kompleksnejšimi gesli, ki vsebujejo številke, znake, ter črke, velike in male začetnice, ter so večmestna. Ponudniki elektronsko poštnih storitev pa lahko preprečijo vdore v uporabniške račune tako, da omejijo število poskusov vpisa v določenem časovnem intervalu, ali pa z uporabo URL-jev, ki so specifični za uporabnika (Sullivan, 2007).

Zgoraj navedene vrste napadov na e-poštne sisteme pa so efektivne le zaradi socialnega inženiringa. Socialni inženiring pomeni: »(..) hekerjevo manipulacijo naravne človeške nagnjenosti k zaupanju s ciljem pridobiti informacije, ki bi omogočile neavtoriziran dostop do sistema informacij.« (Dimc & Dobovšek, 2012). Popoln sistem, ki je odporen na vse vrste napadov ne obstaja, razen če bi bil odporen tudi na napake uporabnika. Ravno tukaj se kaže problematika boja proti socialnemu inženiringu, to je posameznik sam, kajti »vsak sistem je le toliko močan, kot je močan njegov najšibkejši člen« (Dimc & Dobovšek, 2012). Kar pomeni, da je izobraževanje uporabnikov bolj pomembno, kot ustvarjanje ustrezne zaščitne opreme. Poglaviten oz. bistven aspekt je torej zaupanje, kajti :»Zaupanje je namreč neko osnovno vodilo vseh nas in prav na to primarno vodilo se osredotoči storilec, ki z uporabo psiholoških in socialnih tehnik zlorabi zaupanje žrtve z namenom pridobitve želenih informacij.« (Dimc & Dobovšek, 2012). Zaupanje je eno izmed temeljnih vrednot, ki ima velik pomen pri e-pošti. Več o zaupanju v naslednjem poglavju.

ZAUPANJE ELEKTRONSKI POŠTI PREDSTAVLJA NAVIDEZEN NADZOR

Temeljna vrednota znotraj osebnih relacij je spoštovanje (tudi spoštovanje zasebnosti) in zaupanje. Slednje daje posamezniku občutek kontrole informacij, občutek zaupanja med posamezniki v družbi itd. Načelo zaupanja je tudi relacija, ki jo prepoznamo v vsakodnevnih odnosih med posameznikom in drugimi osebami, s katerimi je posameznik povezan preko osebnega stika. V informacijski tehnologiji posameznik ni deležen osebnega stika ter ne zaupa ljudem, ki stojijo za storitvijo, ampak zaupa storitvi sami. »Zaupanje leži znotraj osebnih razmerij, ki so se razvila čez čas, in omogoča interakcijo, ki priskrbi osnovo za mrežno organizirane aktivnosti. Grajenje zaupanja je zahtevno in potrebuje čas ter posamezne vloge ljudi v organizacijah ali mrežah. Zaupanje v informacijski tehnologiji je pomembno, saj zaradi virtualnega okolja klasične osebne interakcije za razvoj in gradnjo zaupanja niso možne.« (Widén-Wulff, 2007) Zaupanje uporabnikov v ponudbo elektronske pošte tako ponudnikom storitev predstavlja uspešnost privabljanja novih uporabnikov in hkrati velik problem. Ponudniki elektronske pošte problem zasebnosti in zaupanja spretno rešujejo z eno izmed storitev celotne ponudbe. Vsakemu posamezniku omogočijo uporabo gesla za njegov uporabniški račun, ki si ga uporabnik priredi, kakor želi, kar pri posamezniku vzbudi občutek varnosti in zasebnosti. Zaupanje tako predstavlja osnovo za deljenje informacij preko elektronske pošte, kljub temu da vemo, da elektronska pošta ni ne varna in ne zasebna. Varnost in zasebnost sta veliki pomanjkljivosti elektronske pošte kajti, ni le uporabnik tisti, ki ima nadzor nad svojimi informacijami, ampak so tu tukaj ponudniki storitev, ki imajo celovit vpogled v uporabnikov poštni predal.

[3] Ti napadi se večinoma izvajajo s pomočjo grafičnih enot.

»Neformalne oblike družbenega nadzora spreminja informacijska tehnologija na več načinov. Tehnični pripomočki nadzora so dostopni tudi državljanom, ki danes lahko vohunijo drug za drugim in z lastnim zalezovanjem tudi kršijo človekove pravice drugih, a tudi tako, da vohunijo za državo in ji gledajo pod prste.« (Završnik, Kriminaliteta in tehnologija : kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon?, 2010). Tako razvoj tehnične opreme ne prinaša zgolj uporabnih vrednosti nove opreme, ampak tudi možnost nadzorovanja drugih ljudi in institucij. Nova tehnična oprema in novi virtualni prostori v vsakem trenutku uporabnikom omogočajo nadzorovanje drugih. Bistvo nadzorovanja drugih je v tem, da nadzorniki gledajo in pri tem niso vidni, s čimer se lahko izognejo odgovornosti za svoje početje, kar je glede posameznikove zasebnosti nesprejemljivo in sporno. Elektronska pošta je pod nadzorom posameznika, ki jo uporablja, ter pod nadzorom »nadzornikov«. Nadzorniki so ljudje, ki preverjajo in kradejo informacije s tujih elektronskih naslovov, jih v zlovešče namene uporabijo ali pa celo prevzamejo posameznikov elektronski naslov in s tem ukradejo posameznikovo identiteto. »Znan primer nadzora elektronske pošte s strani »nadzornikov« je Microsoftova afera s francoskim blogerjem, ki je leta 2012 v svojem blogu izdal zaupne informacije o takrat še neizdanem operacijskem sistemu Windows 8. Bloger je kot ponudnika svoje elektronske pošte uporabljal Hotmail, ki je v lasti Microsofta. Microsoft je to prednost izrabil in pregledal celotni uporabniški račun, da bi zaposleni izvedeli, od kod blogerju zaupne informacije.« (Hill, 2014) Sliši se sporno, vendar se je Microsoft branil s svojimi pogoji uporabe, v katerih piše, da lahko Microsoft pridobiva in razkrije informacije o posamezniku, da zaščiti svoje avtorske pravice in lastnino. Zanimivo je tudi to, da si ponudniki elektronske pošte, kot so Google, Yahoo in Apple, delijo enake pogoje uporabe kot Microsoft. Ponudniki storitev elektronske pošte, ki jim uporabniki zaupamo, si torej pridržujejo pravico branja in razkrivanja posameznikove elektronske pošte, če je v pošti uporabnika omenjena lastnina ponudnika. »Pomembno je vedeti, da so vse naše informacije shranjene na njihovih strežnikih, po spletu potujejo preko njihovih protokolov in oni so tisti, ki imajo ključe do enkripcije naših podatkov.« (Brandom, 2014) To pomeni, da če želijo ponudniki elektronske pošte priti do za njih pomembnih ali uporabnih informacij, morajo preveriti celoten poštni predal uporabnika. Zasebnost posameznika je najbolj zaskrbljujoča stvar celotnega sistema elektronske pošte, saj ne obstaja niti ena pravna ali tehnična rešitev, ki bi zavarovala uporabnikove podatke. Celoten sistem elektronske pošte deluje, ker nam ponudniki elektronske pošte ponujajo pomembne storitve, plačujejo stroške hranjenja podatkov na strežnikih in predvsem zato, ker jim zaupamo, da ne bodo preverjali naše pošte.

V prvem delu članka smo opisali, ter obrazložili vrsto pojmov povezanih z elektronsko pošto, ter potencialne ranljivosti in nevarnosti povezane z le-to. Dotaknili smo se napadov tako na organizacije, kot tudi na posameznike, opisali možne načine obrambe pred grožnjami povezanimi z elektronsko pošto in predstavili problem zaupanja ter nadzora nad storitvami.

Da bi podkrepili navedene podatke, pa smo drugi del članka namenili eksperimentu, s katerim smo želeli z empirično pridobljenimi dokazi podkrepiti teoretično ozadje iz prvega dela. Sestavili smo tudi anketni vprašalnik, s katero smo pridobili rezultate, ki smo jih primerjali z rezultati predhodno opravljenih raziskav iz istega področja.

EKSPERIMENT ZAUPANJA V LEGITIMNOST E-POŠTE

Glede na to, da so nekatere izmed temeljnih vrednot in načel zasebnost, poštenost in pravičnost, resnicoljubnost ter zaupanje, se zastavi vprašanje, ali so to vrednote in načela, ki se v informacijski družbi zlahka prekršijo ali ne in če se, ali jih prepoznamo. V okviru naše raziskave smo želeli preizkusiti predvsem, kako težko je zlorabiti elektronsko pošto, kakšne posledice lahko takšna zloraba prinese, ter kako ranljivi so uporabniki.

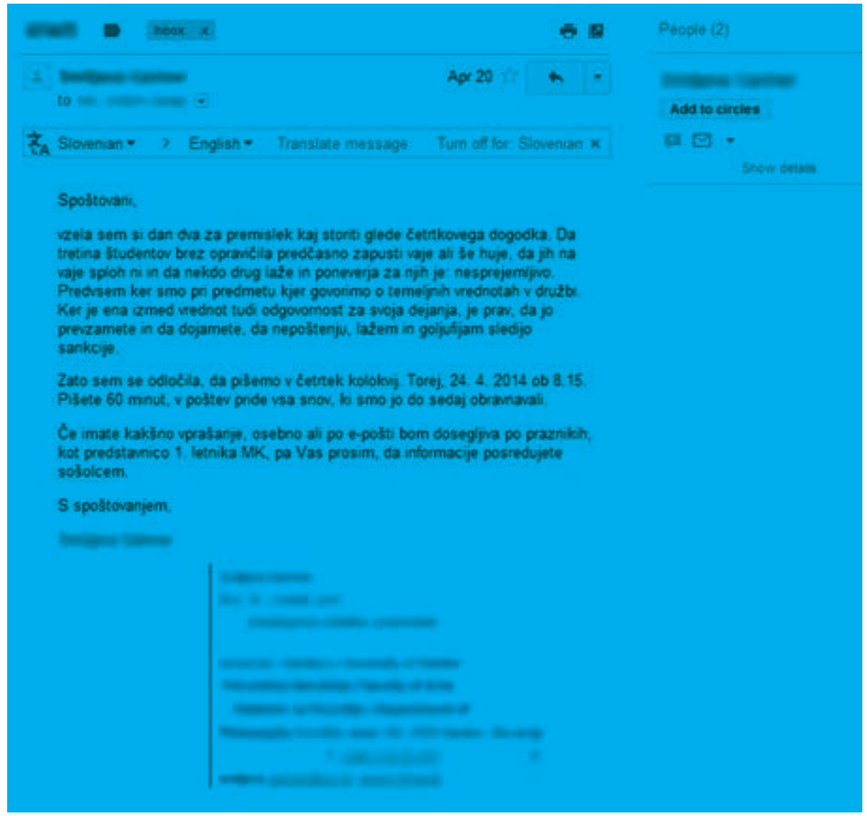
Pred začetkom eksperimenta, smo si postavili tri hipoteze:

Hipoteza 1: Brez večjega poznavanja računalniških sistemov in IT, lahko zlorabimo elektronsko pošto.

Hipoteza 2: Z vdorom v posameznikovo elektronsko pošto, lahko škodujemo njemu in ljudem, do katerih goji avtoriteto, oziroma ima na njih nek vpliv, ter posledično škodujemo njegovemu ugledu.

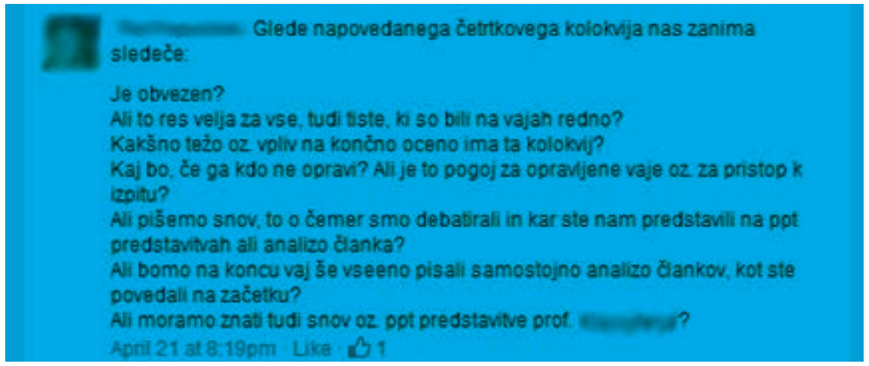
Hipoteza 3: Žrtve o nevarnostih informacijskih tehnologij niso dovolj obveščene, ter se posledično ne znajo zavarovati, ter ločiti zlonamernih sporočil od legitimnih.

Za preizkus le-teh smo uporabili skupinski eksperiment, v katerem smo se postavili v vlogo napadalca. Eksperiment je trajal od 20.4.2014 do 24.4.2014.



Reprezentativnost vzorca smo dosegli s tem, da smo testirali večjo skupino, ki so jo sestavljali študentje prvega letnika enega izmed študijskih smeri na FERI, vsebovala pa je približno šestdeset posameznikov. S pomočjo maskiranja pošiljateljevega naslova smo znotraj SMTP-ja (Simple Mail Transfer Protocol) preko telnet-a poslali sporočilo v imenu profesorice, ki je bila predhodno obveščena z naše strani. 20. 4. 2014 smo predstavnici testne skupine poslali sledeče sporočilo, ki je bilo videti legitimno, vendar smo ga napisali mi. Tako smo z enim samim dejanjem prekršili vse temeljne vrednote, kot so zaupanje skupine, zasebnost profesorice in našo poštenost v očeh drugih. S tem smo potrdili tudi eno izmed naših prvotnih hipotez, ki trdi, da lahko e-pošto zlorabimo brez večjega poznavanja računalništva in informacijske tehnologije. Po tem, ko smo sporočilo poslali, smo na socialnem

omrežju (Facebook) opazovali odziv študentov, ki je bil precej buren. Tako smo torej z enkratno krajo elektronskega naslova vplivali na večje število ljudi, ki so med seboj povezani. Problem, ki ga je prikazal naš eksperiment je, da lahko skoraj vsaka oseba z dostopom do računalnika povezanega s svetovnim spletom kadarkoli uporabi elektronski naslov druge osebe.



Slika 1: Objava predhodno napisanih vprašanj, ki so bila posredovana profesorici

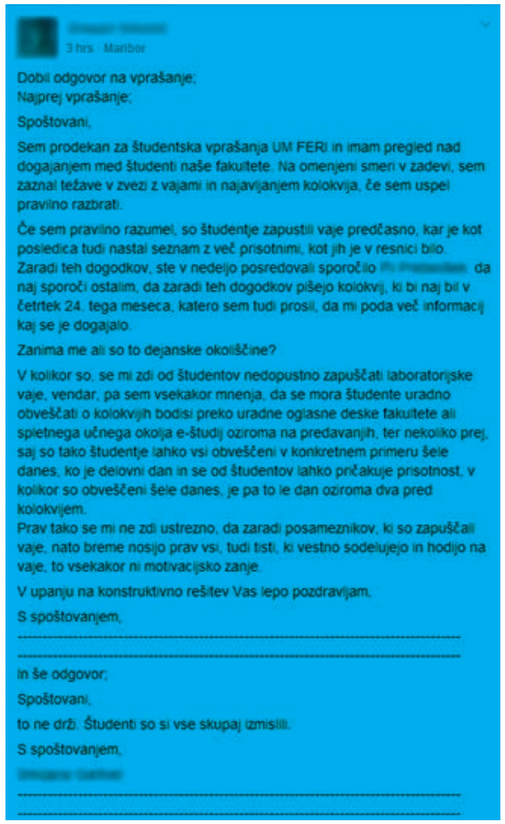
Študentje so aktivno pristopili k nastalemu problemu, saj so v iskanju rešitve v kratkem časovnem intervalu napisali kar 46 komentarjev. Nihče iz ciljne skupine ni podvomil v legitimnost prejetega, pač pa je večina želela več informacij v zvezi s prvotno poslanim sporočilom od nas. S tem potrjujemo našo tretjo hipotezo, v kateri trdimo, da: "žrtve o nevarnostih informacijskih tehnologij niso dovolj obveščene, ter se posledično ne znajo zavarovati, ter ločiti zlonamernih sporočil od legitimnih.".[4]

21. 4. 2014 so se študentje odločili za aktivni pristop. Začeli so zbirati vprašanja posameznikov, katera bi nato formulirali v eno sporočilo, ki so ga poslali profesorici. Tukaj je potrebno omeniti, da je ta odgovor bil poslan na naslov, ki je bil prikazan kot tisti od pošiljatelja v prvotnem poročilu. Tako je ta vprašanja prejela profesorica in ne mi. odgovor so študentje prejeli 22. 4. 2014, v njem pa je profesorica zanikala kakršnokoli seznanjenost s situacijo. Celotna situacija je po objavi odgovora eskalirala, do te mere da so študentje začeli dvomiti v profesoričino profesionalnost, še vedno pa ni nihče podvomil v samo legitimnost e-poštnega sporočila. To potrjuje našo drugo hipotezo, s katero smo želeli dokazati, da z vdorom v posameznikovo

[4] Tukaj je potrebno omeniti tudi to, da je naša ciljna skupina bila predhodno obveščena o nevarnostih, ki jih s seboj prinaša splet, saj je bila to tema njihovih predavanj.

elektronsko pošto, lahko škodujemo njemu in ljudem, do katerih goji avtoriteto, oziroma ima na njih nek vpliv, ter posledično škodujemo njegovemu ugledu. Tukaj je potrebno posebej izpostaviti dejstvo, da študentje po dobljenem odgovoru niso ukrepali, temveč so bili pasivni do te mere, da se je v reševanje problema bil primoran vključiti predstavnik študentov FERI, ki je slučajno opazil pogovor o tej temi. Tudi on je profesorici poslal sporočilo, v katerem jo je obvestil, da je seznanjen s problemom, ter da je pripravljen sodelovati pri iskanju "konstruktivne rešitve". Profesorica je tudi njemu odgovorila na enak način kot študentom in sicer s sklicevanjem na neobveščenost o situaciji. Zaradi nastale situacije se je predstavnik študentov odločil, da se udeleži naslednjega predavanja, kjer bi se s profesorico lahko pogovoril v živo, ter rešil nastalo situacijo.

Nato je situacija obstala vse do 24.4.2014, ko naj bi se odvijal dogodek, ki smo si ga izmislili v prvotnem sporočilu. Ob tej priložnosti smo ciljni skupini razkrili naša dejanja. S tem eksperimentom smo na enostaven način prikazali nevarnosti in pomanjkljivosti, ki jih s seboj nosijo moderni načini komunikacije. Posledično smo z eksperimentom študente soočili s tem, kako hitro se lahko porušijo družbena načela zaupanja in poštenosti.


[redacted] 3 hrs · Maribor

Dobil odgovor na vprašanje:
Najprej vprašanje:

Spoštovani,

Sem prodekan za študentska vprašanja UM FERI in imam pregled nad dogajanjem med študenti naše fakultete. Na omenjeni smeri v zadevi, sem zaznal težave v zvezi z vajami in najavljanjem kolokvija, če sem uspel pravilno razbrati.

Če sem pravilno razumel, so študentje zapustili vaje predčasno, kar je kot posledica tudi nastal seznam z več prisotnimi, kot jih je v resnici bilo.
Zaradi teh dogodkov, ste v nedeljo posredovali sporočilo [redacted] da naj sporoči ostalim, da zaradi teh dogodkov pišejo kolokvij, ki bi naj bil v četrtek 24. tega meseca, katero sem tudi prosil, da mi poda več informacij kaj se je dogajalo.

Zanima me ali so to dejanske okoliščine?

V kolikor so, se mi zdi od študentov nedopustno zapuščati laboratorijske vaje, vendar, pa sem vsekakor mnenja, da se mora študente uradno obveščati o kolokvijih bodisi preko uradne oglasne deske fakultete ali spletnega učnega okolja e-študij oziroma na predavanjih, ter nekoliko prej, saj so tako študentje lahko vsi obveščeni v konkretnem primeru šele danes, ko je delovni dan in se od študentov lahko pričakuje prisotnost, v kolikor so obveščeni šele danes, je pa to le dan oziroma dva pred kolokvijem.
Prav tako se mi ne zdi ustrezno, da zaradi posameznikov, ki so zapuščali vaje, nato breme nosijo prav vsi, tudi tisti, ki vestno sodelujejo in hodijo na vaje, to vsekakor ni motivacijsko zanje.

V upanju na konstruktivno rešitev Vas lepo pozdravljam,

S spoštovanjem,

In še odgovor;

Spoštovani,

to ne drži. Študenti so si vse skupaj izmislili.

S spoštovanjem,

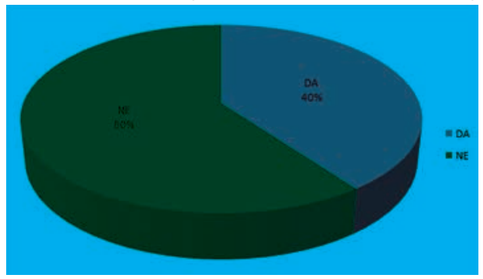
[redacted]

Slika 2: Vprašanje predstavnika študentov ter profesoričin odgovor nanj

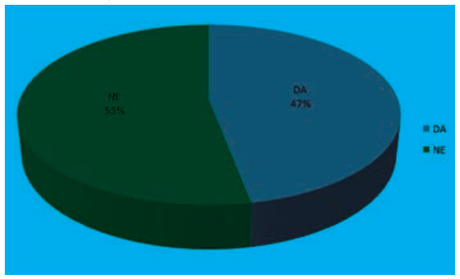
V KOLIKŠNI MERI SE UPORABNIKI ZAŠČITIJO

Čeprav je vsak dan odkrita kakšna nova pomanjkljivost v varnostnih mehanizmih, pa lahko za našo varnost na svetovnem spletu največ postorimo prav sami. Zaskrbljujoče je, da se večina uporabnikov začne zavedati tega dejstva šele, ko se jim zgodi kaj neprijetnega (vdor, kraja identitete, itd.). Na njihovo nesrečo pa je v večini primerov takrat že prepozno, saj je škoda že storjena.

V okviru raziskave smo ustvarili spletno anketo, v kateri smo zastavili vprašanja, z odgovori na le-te smo poskušali pridobiti podatke, ki bi jih lahko primerjali s tistimi od ostalih raziskav. Z anketo smo pridobili podatke o zaščiti in dinamičnosti uporabnikov e-pošte, s katerimi smo podkrepili problematiko varnosti, nadzora in zaščite e-pošte. V anketi je sodelovalo 150 naključnih oseb, med katerimi jih je 107 oseb bilo ženskega , 43 oseb moškega spola. Starostni razpon je bil med 14 in 65 let, s povprečno starostjo 30.8 let. Kot je iz rezultatov ankete razvidno, anketiranci pri določenih stvareh poskrbijo za ustrezno varnost, kljub temu pa je še vedno prostor za napredek, kar lahko razberemo iz prvega grafa.
Še vedno namreč kar 40% uporabnikov uporablja ista gesla za dostop do elektronske pošte, kakor tudi za dostop do različnih aplikacij, socialnih omrežij in



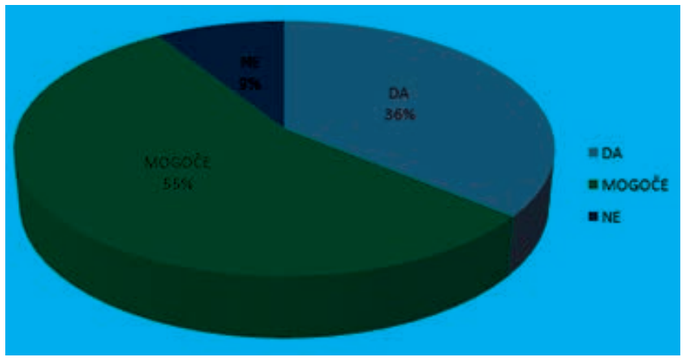
Graf 1:Rezultati vprašanja "Ali uporabljate ista gesla za dostop do različnih aplikacij/e-pošte/ spletnega bančništva?"



Graf 2: Rezultati vprašanja "Ali menjate svoja gesla?"

celo spletnega bančništva. Le 47% uporabnikov redno menja svoja gesla, kljub temu, da je priporočljivo gesla menjavati po določenem časovnem intervalu, medtem ko 53% uporabnikov tega ne počne.

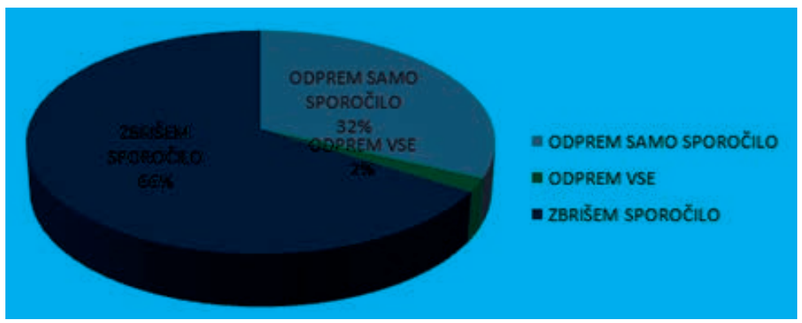
So pa uporabniki pokazali določen napredek v varnosti, glede na podobne raziskave iz preteklih let (Norton), saj so se počasi začeli zavedati, da elektronska



Graf 3: Rezultati vprašanja "Ali se bojite, da bi vam kdo vdrl v elektronsko pošto?"

pošta le ni tako varna in zasebna kot morda izgleda na prvi pogled. To lahko opazimo pri odgovoru na vprašanje, ali se uporabniki bojijo, da bi jim kdo vdrl v elektronsko pošto. Analiza je namreč pokazala, da se 36% uporabnikov boji, 55% je neopredeljenih, samo 9% pa je takšnih, ki se vdorov ne bojijo. Iz tega lahko izpeljemo oziroma potrdimo, da so ljudje iz leta v leto bolj seznanjeni z nevarnostmi in grožnjami, ki pretijo znotraj elektronske pošte. Omenjeno lahko potrdimo tudi z rezultati, ki smo jih pridobili pri vprašanju Kaj storite z elektronsko pošto, ki pride iz strani neznanega pošiljatelja.

Uporabniki so namreč izpolnili vprašanje o tem, ali ločijo zlonamerno pošto od pristne, oziroma, kako pogosto odpirajo pošto, pri kateri ne poznajo pošiljatelja.



Graf 4: Rezultati vprašanje "Kaj storite z elektronsko pošto, ki pride iz strani neznanega pošiljatelja?"

Le 2% je takšnih, ki odprejo pošto ki pride iz strani neznanega pošiljatelja, hkrati pa odprejo tudi povezave in datoteke znotraj sporočila, večina, kar 66% pa je jih sporočilo nemudoma izbriše. Neznane pošiljatelje namreč dojemajo kot tujce, jim ne zaupajo, zato jih tudi ne želijo spustiti v zasebnost, četudi so že v zasebnosti, saj so na osebnem računu.

Izsledke naše ankete smo primerjali z letnimi poročili enega izmed največjih proizvajalcev protivirusne opreme, Nortona. Uporabili smo letno poročilo iz leta 2012/2013, ki smo ga primerjali z rezultati naše ankete, nato pa še letno poročilo iz leta 2011. Poskušali smo ugotoviti, ali so se rezultati v tem obdobju spremenili in ali so uporabniki s časom postali varnejši. Iz letnega poročila 2013 je razvidno, da je vsako uro več kot milijon uporabnikov žrtev različnih vdorov v njihove sisteme. Preračunano je torej vsako sekundo prizadetih kar 18 uporabnikov svetovnega spleta. V poročilu iz leta 2013 je tudi zapisano, da je le 16% uporabnikov takšnih, ki se ne boji vdorov, kar 75% uporabnikov pa takoj izbriše sporočilo, ki pride iz strani neznanega pošiljatelja. Po drugi strani, pa je kar 45% takšnih , ki uporablja enaka gesla, oziroma 47% takšnih, ki svojih gesel ne menjavajo, oziroma uporabljajo generična gesla, ki jih je lahko uganiti. Kot lahko vidimo, so izsledki Nortona primerljivi z rezultati naše ankete. Če pa te rezultate primerjamo z letnim poročilom iz leta 2011 pa je razvidno, da obstaja določen trend, namreč uporabniki so vsako leto postali bolj ozaveščeni o nevarnostih vdorov, in so tudi bolje poskrbeli za svojo varnost. Razlog za to, pa morda tiči tudi v Edwardu Snowdnu in aferi NSA, ki je v informacijski družbi sprožila ogromno polemiko glede nadzora s strani vladajočih organov nad svetovnim prebivalstvom. Po Nortonovih podatkih, se je namreč število uporabnikov, ki jih ne skrbi, da bi bili lahko tarča vdorov, zmanjšalo za kar 30%! (2012 – 46%; 2013 – 16%). Prav tako se je povečalo število tistih, ki brišejo elektronsko pošto neznanih pošiljateljev, oziroma ne odpirajo sumljivih povezav in datotek znotraj elektronske pošte. Takšnih uporabnikov je bilo v letu 2013 že kar 75%, medtem, ko jih je bilo v letu 2011 le okoli 52% (Symantec, Cyber Crime Report, 2013) (Symantec, Cyber Crime Report, 2011).

ZAKLJUČEK

Kljub znanstvenemu in tehnološkemu napredku, trditev, ki jo je leta 1990 podal E. Marc Peetersen, v kateri trdi, da »E-pošto trenutno ne moramo označiti kot 100% zanesljivo storitev.« (Peeters, 1990), velja še danes. Napovedovati prihodnost e-pošte je nemogoče. Ali bo njena popularnost naraščala? Bo kdaj postala zanesljiva? Bo zašla v pozabo, kot pisma in jo bo nasledila naslednja komunikacijska tehnologija? Špekulirati o tem je nesmiselno, vendar pa je dejstvo, da je trenuten vpliv spletnih tehnologij, med katere spada tudi e-pošta, tako velik, da veliko ljudi enači pomembnost svoje spletne identitete s svojim življenjem. Mnogi se ne zavedajo, da informacije, ki jih dnevno pošiljamo prek spleta niso dostopne le nam in da je zasebnost v informacijski družbi postala redkost. Klub temu, da kršitve naše zasebnosti niso zmeraj zlonamerne, saj mnogi vladni organi nadzorujejo pretok informacij z namenom, da bi širšo družbo obvarovali pred škodo, pa se tukaj poraja vprašanje etičnosti njihovih dejanj in kršitve pravic državljanov, saj poseganje v človekovo zasebnost ni sprejemljivo ne glede na okoliščine. Kot je rekel Benjamin Franklin: "kdor se je pripravljen odreči pravicam, ki jih prinaša svoboda, za kanček varnosti, si ne zasluži ne enega, ne drugega".

BIBLIOGRAFIJA

Brandom, R. (2014). Microsoft just exposed email's ugliest secret: Email is more broken than you think. The Verge.

C. White, M. (20. 11 2012). Study: 10,000 Identity Theft Rings in U.S. Pridobljeno (24.4.2014) iz TIME : http://business.time.com/2012/11/20/study-10000-identity-theft-rings-in-u-s/

Dimc, M., & Dobovšek, B. (2012). Kriminaliteta v informacijski družbi . Ljubljana: Fakulteta za varnostne vede.

Doel, K. (brez datuma). "Password" unseated by "123456" on SplashData's annual "Worst Passwords" list. Pridobljeno (3.4.2014) iz SplashData News: http://splashdata.com/press/worstpasswords2013.htm

Hill, K. (2014). Microsoft Decides It's Actually A Bad Idea To Snoop Through Users' Emails. Forbes.

Internet Live Stats. (brez datuma). Internet Users. Pridobljeno (5.5.2014) iz Internet Live Stat: http://www.internetlivestats.com/internet-users/

Kumaraguru, P. (2007). Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer (2007). Institute for Software. Pensilvanjia, ZDA: Institute for Software Research .

Mandalia, R. (22. 9 2011). 48% of Companies Faced Social Engineering Attacks Claims Survey. Pridobljeno (26.5.2014) iz ITProPortal: http://www.itproportal.com/2011/09/22/48-companies-faced-social-engineering-attacks-claims-survey/

META, G. (2003). Spam, Viruses and Content Compliance: An Opportunity to Strategically Respond to Immediate Tactical Concerns.". Stamford: META Group Inc.

Mitnick, K. D. (2002). The art of deception: contorolling the human element of security. Indianapolis: Wiley.

Mozilla. (14. November 2006). Firefox 2 Phishing Protection Effectiveness Testing. Pridobljeno (10.4.2014) iz Mozilla: http://www.mozilla.org/security/phishing-test.html

Peeters, E. (1990). Electronic Mail Reliability. Rotterdam: Erasmus University of Rotterdam.

Pingdom. (10. 5 2014). Internet 2012 in numbers. Pridobljeno iz (18.4.2014) Royal Pingdom: http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/

Ramneek, P. (10. 5 2014). SANS Institue. Bots &; Botnet: An Overview, 3-10. Pridobljeno (22.4.2014) iz http://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299

Reaves, J. (23. 1 2002). Identity Theft: Could it Happne to You? Pridobljeno (1.5.2014) iz TIME: http://content.time.com/time/nation/article/0,8599,196857,00.html

Rogers, K. (20. 2 2013). One New Identity Theft Victim Every 3 Seconds in 2012. Pridobljeno (9.4.2014) iz FOX Business: http://www.foxbusiness.com/personal-finance/2013/02/20/one-new-identity-theft-victim-every-3-seconds-in-2012/

SI-CERT, S. c. (brez datuma). Phishing Napad Na Uporabnike Spletne Banke Abanet. Pridobljeno (22.4.2014) iz Varni na Internetu: https://www.varninainternetu.si/2010/phishing-napad-na-uporabnike-spletne-banke-abanet/

SI-CERT, S. c. (brez datuma). Phising Kraja Podatkov. Pridobljeno (11.4.2014) iz Varni Na Internetu: https://www.varninainternetu.si/article/phishing-kraja-podatkov/

SI-CERT, S. c. (brez datuma). Uporabniki SiOL Pošte Zopet Tarča Phishing Napada. Pridobljeno (3.5.2014) iz Varni Na Internetu : https://www.varninainternetu.si/2012/uporabniki-siol-poste-zopet-tarca-phishing-napada-3/

Spector, L. (17. 2 2014). Can a hacker use a brute-force attack to steal an online password? Pridobljeno (8.5.2014) iz PCWorld: http://www.pcworld.com/article/2095500/can-a-hacker-use-a-brute-force-attack-to-steal-an-online-password.html

Staff Writers of "OnlineCollegeCourses", S. (28. 1 2013). Online College Courses. Pridobljeno (2.4.2014) iz Hacked: http://www.onlinecollegecourses.com/hacked/

Sullivan, B. (11. 1 2007). Preventing a Brute Force or Dictionary Attack: How to Keep the Brutes Away from Your Loot. Pridobljeno (17.4.2014) iz CODE Project: http://www.codeproject.com/Articles/17111/Preventing-a-Brute-Force-or-Dictionary-Attack-How

SURS. (3. 12 2013). Uporaba računalnikov in interneta pri starejših, podrobni podatki, Slovenija, 2013 - končni podatki. Pridobljeno (26.4.2014) iz Statistični Urad Republike Slovenije: http://www.stat.si/novica_prikazi.aspx?id=5923

Symantec, C. (2011). Cyber Crime Report. Pridobljeno (3.4.2014) iz Norton: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/assets/downloads/en-us/NCR-DataSheet.pdf
Symantec, C. (2013). Cyber Crime Report. Pridobljeno (4.4.2014) iz Norton: http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/

Technology, B. N. (3. 6 2011). Sony Investigating Another Hack . Pridobljeno (1.5.2014) iz BBC NEWS Technology: http://www.bbc.co.uk/news/business-13636704

Ule, M. (2000). Sodobne identitete: v vrtincu diskurzov. Ljubljana: Znanstveno in publicistično središče.

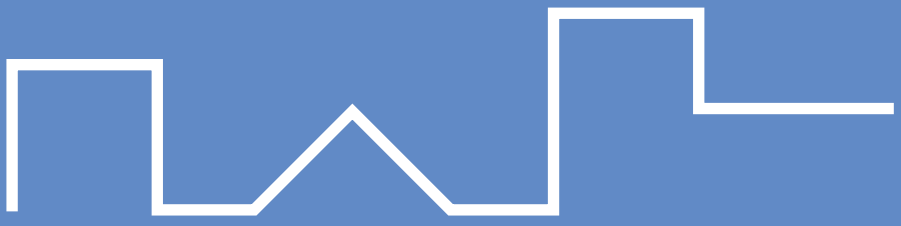
Upelj, B. (11. december 2006). Kaj je spam in kako se ga (vsaj nekoliko) ubranimo? Pridobljeno (19.4.2014) iz Dnevnik: http://www.dnevnik.si/magazin/znanost-in-tehnologija/216588

Widén-Wulff, G. (2007). The Challenges of Knowledge Sharing in Practice: A Social Approach. Oxford: Chados Publishing Limited.

Završnik, A. (2010). Kriminaliteta in tehnologija : kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon? Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

FOTO-UTRINEK FORUMA

FOTO-UTRINEK FORUMA



Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko

slovensko
društvo
informatika