Ko to tamo špega?

Aljaž Potočnik

Nova sezona ameriške animirane serije *South Park* se je pričela z zabavno tematizacijo shizofrenega odnosa sodobne družbe do varovanja osebnih podatkov. Kot glavni protagonist epizode se Cartman odloči za infiltracijo v ameriško varnostno agencijo NSA. Od tam namerava razkriti svetovnemu občestvu vse razsežnosti zvedavosti državnih oblasti in njihove brezsramne invazije v naša zasebna življenja, hkrati pa želi svoj načrt izpeljati z najnovejšim družbenim omrežjem, ki s pomočjo dveh anten/zvočnikov v živo in brez kakršnekoli cenzure oddaja vse uporabnikove misli.

Premisa, s katero ustvarjalci *South Parka* kritizirajo odnos sodobne družbe do varstva zasebnih podatkov, je precej razširjena pri tistih, ki želijo upravičevati programe oziroma storitve, ki sledijo našemu spletnemu obnašanju. Takšno retoriko smo v preteklost slišali predvsem pri vprašanju legitimnosti beleženja naših navad za komercialne namene ponudnikov spletnih storitev, zdaj pa jo zasledimo tudi pri problemu vohunjenja za osebnimi podatki. Zamenja se le korist, ki ni več udobno pridobivanje informacij, prikrojenih posameznemu potrošniku, temveč osebna varnost in zaščita pred nevarnim svetom.

Opravičila zbiranja zasebnih podatkov običajno slonijo na tezi, da tako ali tako ne cenimo svoje zasebnosti tako močno, kot trdimo ob izbruhih afer. Apologeti se prav tako sprašujejo, zakaj toliko ogorčenja nad zbiranjem metapodatkov, kot so lokacije in časovni okvir telefonskih klicev, pošiljanja elektronskih sporočil in podobnega početja, če pa svojo lokacijo neprestano in prostovoljno delimo, ko se prijavljamo v aplikacijo Foursquare ali objavljamo fotografije na facebooku? Dodali bi lahko tudi, da se ljudje pogosto pritožujejo nad zbiranjem podatkov o obiskih spletnih strani, ki podjetjem pomagajo pri ciljnemu oglaševanju, hkrati pa imajo denarnice polne kartic zvestobe, ki služijo povsem isti funkciji. Še več, številni uporabniki twitterja in podobnih spletnih družbenih omrežjih se dnevno sredi spletne javnosti zapletajo v najbolj osebne in sramotne spore, ki med drugim razkrivajo tudi osebna prepričanja. Čeprav bi bili ogorčeni, če bi izvedeli, da državne oblasti beležijo njihove volilne preference, te podatke na ves glas naznanjajo spletni javnosti. Če kaj, je očitno, da ljudje dandanes ne cenijo svoje zasebnosti ter da skoraj vse informacije delijo z drugimi, afere v zvezi z državnim prisluškovanjem pa jih motijo zgolj zato, da bi oponašali ogorčenje, ki jim ga sugerirajo mediji ali drugi manipulativni posamezniki. Zato proč z ogorčenjem, trdijo zagovorniki vohunjenja: poleg anonimnih neznancev, ki lahko prostodostopne spletne podatke zlorabijo na sto milijonov načinov, ima vpogled v vašo zasebnost pač še kakšen spoštljivi državni uslužbenec, ki bi vas rad zgolj obvaroval pred nevarnostmi grdega sveta.

Ne, ni tako preprosto

Zgodba v resnici ni tako preprosta. Trik je v tisti malenkosti, ki jo argument poskuša prekriti. Prek spleta ter družbenih omrežij s prijatelji in neznanci delimo skoraj vse. Kar nas v resnici moti, so podatki, ki jih zaradi takih ali drugačnih razlogov ne želimo deliti. Da med obojim obstaja velika razlika, hitro opazimo, če že na hitro pregledamo, kaj so najpogostejši podatki, ki smo jih pripravljeni posredovati prek spleta, nato pa lahko vsak zase opravi premislek, katere spletne dejavnosti v to kategorijo ne sodijo. Nobena skrivnost ni, da so najpogostejše vsebine, ki jih javno delimo prek spleta, zelo podobne tistim, ki smo jih z veseljem javno delili tudi pred razvojem sodobnih komunikacijskih tehnologij. Najpogosteje gre za fotografije počitnic oziroma izletov, obiskov prireditev ali okusnih jedi, ki smo jih pripravili. Gre za reči, na katere smo ponosni in za katere želimo, da jih vidi kar največje število ljudi. Če je poleg fotografij še gumb, ki meri količino pohval in zavisti, smo z deljenjem podatka še toliko bolj zadovoljni. Včasih so ljudje v društvih, gostilnah ali na domačih obiskih razkazovali diapozitive, danes sta tu facebook in instagram. Morda bi se lahko zdelo malce bolj kočljivo spletno objavljanje pogledov in stališč, a tudi to ni nič novega. Nihče ne pravi, da so pisma bralcev ali klici v radijske in televizijske oddaje primeri razsipnega deljenja osebnih podatkov. Naj opomnimo, da so v primeru radijskih in televizijskih oddaj ljudje z gosti pogosto delili tudi zdravstvene podatke. S priho-

Ilustracija: Emory Allen

dom družbenih omrežij se je pri našem odnosu do deljenja osebnih podatkov zares spremenila le potencialna odmevnost vsebin, ki jih želimo deliti. Čeprav včasih deljenje kakšnega podatka kasneje tudi obžalujemo, se ta občutek bistveno razlikuje od odkritja, da nekdo dostopa do podatkov, ki jih izrecno nismo želeli deliti.

Čeprav je na površju morda videti, kot da naše spletne aktivnosti nimajo filtrov in da z občestvom delimo vse naše misli in aktivnosti, podobno kot Cartman v *South Parku*, so naše dejavnosti prek spleta precej bolj premišljene. Lep primer je tudi razlika med uporabo javnih in zasebnih pogovorov prek družbenih omrežij. Za navidezno iskrenostjo statusov in komentarjev se najpogosteje skriva bistveno globlji nivo deljenja osebnih podatkov v zasebnih pogovorih, za katere uporabniki sklepajo, da so varni pred špegavčki takšnih in drugačnih vrst. Kako resno jemljemo to zasebnost, dobro razkriva folklora ugrabitev facebook profilov. Ko sodelavec na delovnem mestu ali prijatelj pozabi izklopiti svoj profil, pogosto sledi objavljanje neumnosti na zid, menjavanje fotografij, spreminjanje osebnih podatkov in številne druge oblike spletnega grafitiranja. Vse to je nedolžna zabava, ker vemo, da se na površju ne skriva nič bistvenega. Precej drugače pa bi bilo, če bi med grafitiranjem pričeli še prebirati privatne korespondence z drugimi osebami. Šale bi bilo verjetno konec že tedaj, ko bi samo pogledali na seznam oseb, s katerimi se pogovarja lastnik ugrabljenega profila. Če bi se izkazalo, da do teh informacij sistematično dostopa neka neznana oseba z neznanimi nameni, pa občutek izdaje zaupanja zamenja tesnoba, ogorčenje pa se še okrepi.

Pravno izsiljevanje spletnih podjetij

Ravno to je razlog enormnega ogorčenja, ki je preplavilo svet, ko je Edward Snowden, pogodbeni podizvajalec ameriške državne varnostne agencije NSA, pred meseci razkril množična prisluškovanja, ki so poleg tujcev ujela tudi domače državljane, potekala pa so prek netransparentnega pravnega postopka. Razlika med tujimi in domačimi državljani se nam kot tujcem zdi nepomembna, a v resnici podobna prisluškovanja opravljamo tudi pri nas. Čeprav se pravica, da poseg v komunikacijsko sredstvo odredi neodvisni sodnik, v evropskem pravu šteje kot človekova pravica, čeprav imamo to zapisano tudi v 37. členu slovenske ustave, zakon o Sovi omogoča, da se lahko na mednarodnih zvezah prisluškovanje omogoči že z odredbo direktorja Sove. Tako se je leta 2004 med pogovori s hrvaškim kolegom Ivom Sanaderjem v prisluškovanje Sove ujel tudi takratni premier Janez Janša. Pogovori o spremembi dikcije zakona o Sovi naj bi se obnovili vsakih nekaj let, a pravih premikov za sprejem spremembe ni videti.

Snowdnovo razkritje samo po sebi zato ne bi smelo preveč presenetiti. *Washington Post* je že leta 2010 objavil poročilo, ki je razkrivalo, da NSA na dan prestreže 1,7 milijarde elektronskih pošt, telefonskih klicev in drugih oblik komunikacij. Prav tako je z argumentacijo boja proti terorizmu ameriško sodišče domačim agencijam dovolilo dostopati do podatkov, ki se nahajajo v podatkovnih centrih ameriških podjetij tudi izven ZDA. To pomeni, da so imele pravno podlago za poseg v podatkovne baze, ki se nahajajo na ozemlju pod tujo jurisdikcijo. Kakšen sod smodnika predstavlja to dejstvo, je bilo verjetno znano tudi podjetjem, ki ponujajo spletne storitve kot so shranjevanje v oblaku in podobno. Prav ta podtjetja pa so po Snowdnovemu razkritju tudi utrpela največjo blamažo.

Microsoft, Yahoo, Google, Facebook, Pal-

talk, AOL, Skype, Youtube in Apple so se po razkritju vpletenosti v prisluškovanje NSA odločno lotile kampanje za reševanje ugleda. Vsa so odločno zanikala sodelovanje z NSA, nekatera so se od takrat naprej odločila tudi za objavljanje letnih podatkov o uradnih zahtevkih za informacije uporabnikov. Seveda je bilo že od samega začetka jasno, da zagotovila o nevpletenosti niso povsem verodostojna, saj bi sodelovanje z NSA vsebovalo tudi klavzulo o tajnosti, še bolj pa bode v oči odločnost ameriških oblasti pri pridobivanju nadzora nad komunikacijami, ki je očitna zlasti iz dokumentov v zvezi s primerom spletnega ponudnika za elektronsko pošto Lavabit.

Podjetje, ki je nekoč obljubljalo varno pošiljanje elektronske pošte, je letos avgusta po desetih letih prenehalo delovati, že kmalu po zaprtju pa so se pojavili sumi, da je zgodba povezana z Edwardom Snowdnom, ki je storitev uporabljal. Dokumenti, ki so se za javnost odprli pred nekaj tedni, sedaj razkrivajo, da je FBI od podjetja zahteval orodja za realnočasovno nabiranje metapodatkov o uporabnikih: gesla, ključe za enkripcije in druge kode, ki bi jim omogočale vohunjenje za slehernim uporabnikom, ne zgolj za tistim, ki so ga v konkretnem primeru preganjali (šlo naj bi ravno za Snowdna). Lastnik podjetja je po neuspešnih pravnih bitkah FBI predal zahtevana orodja, a hkrati zaprl svoje podjetje. Verjetnost, da so se pritiskom lahko kaj bolje izmikala večja podjetja, ki nimajo tako preproste lastniške strukture, da bi se lahko čez noč zaprla, je zato precej majhna. Angleški časnik *The Guardian* na podlagi Snowdnovih dokumentov celo piše, da so pri Microsoftu pod prisilo zakona sodelovali s pripadniki NSA ter jim omogočali vstop skozi zadnja vrata sistemov, kot so poštni program Outlook, telefonija, skype ter Microsoftov oblak »skydrive«.

Sistematično uničevanje spletne zasebnosti

Dokumenti, ki jih je *Guardianu*, *New York Timesu* in *ProPublici* posredoval Snowden, namreč razkrivajo obsežne napore NSA, da bi ustvarili zadnja vrata v številne sisteme. Pri NSA so zadnja vrata v vse enkripcije želeli vstaviti že v devetdesetih, a takrat v javni razpravi niso dobili zelene luči, ko pa so od leta 2000 naprej vse boljše enkripcije skoraj že zatemnile spletno komunikacijo, je NSA investiral več milijard dolarjev za prikrite kampanje, ki bi jim spet omogočile vpogled v spletno komunikacijo.

Slika po Snowdnovem razkritju vliva precej manjše zaupanje predvsem v varnost storitev v oblaku, ki so bile naslednji veliki izdelek spletnih korporacij. Kljub povečani skepsi pa ljudje zaenkrat zatrjujejo, da niso občutili prevelikih negativnih sprememb, vendar je treba dodati, da je to predvsem zato, ker so mnogi med ponudniki šele zares pričeli nagovarjati večje uporabnike, zlasti podjetja, da bi svoje poslovanje prestavili iz zasebnih strežnikov v oblak. Mnoga podjetja so na prehod že od vsega začetka gledala skeptično, še zlasti tista, ki so že bila izpostavljena korporativnemu vohunjenju. Težko je verjeti, da se je situacija medtem izboljšala. O nezaupanju do oblaka pove precej izid novega iPhona, ob katerem je Apple veliko truda posvetil pojasnjevanju, da se prstni odtisi, ki jih lahko sedaj shranite z vgrajenim čitalcem, nikakor ne bodo shranjevali v oblak. Pri čemer je treba upoštevati dejstvo, da ima FBI že tako ali tako prstne odtise imetnikov ameriških vozniških dovoljenj in oseb, ki so v ZDA potovale z vizo.

Da je naša spletna varnost v veliki meri odvisna od našega nadzora nad infrastrukturo spletnega komuniciranja, postaja z aktualnimi razkritji vse bolj jasno. Če je obdobje pred Snowdnovim razkritjem razprave o kibervarnosti zaznamoval strah pred kitajskimi proizvajalci čipov in komunikacijskih naprav, ki naj bi v naprave in programsko opremo vgrajevali zadnja vrata za lažji vstop kitajske kiberarmade (opozarjalo se je predvsem na podjetje Huawei), se danes očitki kot bumerang vračajo v ZDA. Poleg boja proti enkripciji razkrivajo Snowdnovi dokumenti tudi obsežno kolaboracijo s proizvajalci čipov. Po poročanju *ProPublice* najdemo med letošnjimi uspehi NSA tudi namestitev zadnjih vrat v enkripcijske čipe, ki jih uporabljajo podjetja in vlade. To naj bi jim uspelo s pomočjo sodelovanja s proizvajalci čipov, torej ravno s tem, kar so ZDA pred tem očitali Huaweiju.

Preobsežno, da bi ostalo tajno

Če se vrnemo k uvodu in razliki med podatki, ki smo jih brez težav pripravljeni deliti, in podatki, ki jih zaupamo samo najbolj zaupnim bližnjim – včasih še celo njim ne – se s prosojnostjo spleta izrisujejo dokaj resne nevarnosti. Seveda v prvi vrsti tu ne gre za naša osebna življenja, čeprav pri NSA priznavajo, da njihovi delavci in podizvajalci včasih orodja zlorabijo za nedovoljeno vohunjenje za zasebne interese. Teh primerov naj bi bilo razmeroma malo. Govorijo o enem na leto. Malce večji problem nastane, ko gre za velika podjetja, ki se bojijo kraj poslovnih skrivnosti in patentov. Slednja so bila tudi najpogostejše ameriške žrtve spletnega vohunjenja, ki ga pripisujejo Kitajski. Vohunjenje za političnimi vodi-

telji tujih držav, tudi zavezniških, je malce bolj nerodno in s seboj prinaša tudi diplomatske in ekonomske protiukrepe. V resnici pa največji problem načrtnega rahljanja spletne zasebnosti in varnosti ni nujno koncept zvedavosti NSA, temveč nevarnost širjenja podatkov zlonamernim hekerjem, ki bi ustvarjene slabosti lahko izkoristili tudi sebi v prid. Poleg tega ogromno število zbranih podatkov predstavlja veliko grožnjo za varnost in uspešno delovanje same agencije, ki jih obdeluje. Zaradi strašanske obsežnosti zaseženih podatkov ima do njih dostop ogromno število notranjih in zunanjih pogodbenih sodelavcev. Kar 70 % ameriškega proračuna za obveščevalne dejavnosti gre v roke zasebnim podizvajalskim podjetjem, za enega med njimi je delal tudi Snowden. Vojak Manning in podizvajalec Snowden sta zato dobra pokazatelja dejstva, da je nadzor nad 4,2 milijona osebami, ki imajo dostop do tajnih podatkov ZDA, od tega več kot milijon do najbolj strogo zaupnih skrivnosti, praktično nemogoč. Ameriški politični vrh in tudi javnost sta pobesnela, ko sta Manning in Snowden ameriške državne skrivnosti namenila javni objavi. Bolj bi nas moralo skrbeti tiho prodajanje informacij ter orodij za prisluškovanje in dekripcijo sporočil kupcem z zlonamernimi načrti.

Kako nerodna je invazija v komunikacijo, ki je ne želimo deliti z drugimi, pa so konec oktobra dobro občutili tudi državni voditelji. Kar petintrideset je bilo takih, med njimi tudi nemška kanclerka Angela Merkel in brazilska predsednica Dilma Rousseff. Razkritje je poleg jezne retorike dalo nov zagon predlogu, ki sta ga kmalu po prvih Snowdnowih razkritjih pričeli razvijati Nemčija in Brazilija. Gre za novo resolucijo Združenih narodov o večji spletni zasebnosti, ki bi lahko bila na dnevnem redu že na zasedanju generalne skupščine konec novembra. Nemčija medtem igra dvojno igro. Poleg pozivov po večji varnosti osebnih podatkov hkrati skupaj s Francijo zahteva od ZDA ponovno okrepitev zaupanja med zaveznicami, kar izhaja iz stare želje obeh držav, da bi se pridružili elitni »skupini petih oči«. Skupina je bila po drugi svetovni vojni ustanovljena z namenom deljenja podatkov, pridobljenih prek signalskega vohunjenja, države članice pa bi se naj vzdržale tudi medsebojnega špeganja. Sestavljajo jo ZDA, Kanada, Velika Britanija, Nova Zelandija in Avstralija, vsaka pa je odgovorna za vohunjenje v svoji regiji.

Za velika spletna podjetja je medtem verjetno najbolj pomemben zaplet nov predlog evropskega parlamenta, ki ga je najglasneje zahteval Jan-Philipp Albrecht, nemški poslanec zelenih. Predlog predvideva, da bi za dovoljenje posredovanja podatkov, elektronske pošte in zgodovine spletnih aktivnosti evropskih državljanov morali spletni velikani najprej zaprositi odgovorno evropsko institucijo. Kazni bi v primeru kršitev dosegle tudi 100 milijonov evrov ali 5 % letnega priliva podjetja, če bi bila kazen v tem primeru višja. Podjetja bi se poleg tega znašla v navzkrižju ameriške in evropske zakonodaje.

Epilog zgodbe o javni agenciji, ki v javnosti ni dobila privoljenja za popolno prerešetanje spletne zasebnosti, a je to vseeno storila, kljub temu še ni povsem jasen, vsake toliko časa pa dobimo nove podatke, ki zgodbo še poglobijo.