Zbornik znanstvenih razprav
Letnik 74 (2014) / Volume 74 (2014)
Oktober / October 2014

Spletna stran Zbornika: / Journal website:
http://zbornik.pf.uni-lj.si
http://journal.pf.uni-lj.si

5

UDK 343.45:342.7:659.4(497.4)

*Dr. Aleš Završnik**
*Pia Levičnik***

Zasebnost po Snowdnu: novejša pojmovanja zasebnosti in odnos javnosti do le-te v Sloveniji

1. Uvod

Masovno vohunjenje, ki ga je odkril Edward Snowden junija 2013,[1] odpira kazenskopravne in kriminološke teme, povezane s pravno regulacijo organov v nadzorstveno-varnostni domeni. *Datagate* je razkril podrobnosti procesa izginjanja meja med tradicionalnimi akterji v tej domeni, ki smo mu priča po koncu hladne vojne in s pospešenim razvojem informacijske tehnologije:[2] policisti postajajo vojaki (npr. v obliki *squad teams*) in obveščevalci;[3] vojska na mirovnih misijah spremlja otroke v šolo in izvaja volitve namesto klasičnega bojevanja;[4] obveščevalne službe se usmerjajo v notranje zadeve in postajajo odgovorne za boj zoper organizirani kriminal in terorizem.[5] To izginjanje organizacijskih in

* Višji znanstveni sodelavec na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani in docent za kriminologijo pri Pravni fakulteti Univerze v Ljubljani; ales.zavrsnik@pf.uni-lj.si.
** Univerzitetna diplomirana pravnica; pia.levicnik@gmail.com

1 Greenwald, NSA collecting phone records of millions of Verizon customers daily, v: The Guardian, 6. 6. 2013.

2 Bigo, Les nouveaux enjeux de l'(in)sécurité en europe (2005); Loader, Policing, Securitization and Democratization in Europe, v: Criminal Justice, 2 (2002) 2, str. 125–153; Bayley, Shearing, The new structure of policing: description, conceptualisation and research agenda (2001).

3 V Sloveniji je pomen obveščevalno vodene policijske dejavnosti (angl. *intelligence-led policing*) povzdignjen med temeljne prioritete Resolucije o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2012–2016.

4 Den Boer, Janssens, Moelker, Vander Beken, Easton, Epilogue, v: Blurring military and police roles (2010), str. 224.

5 Andreas in Price trdita, da se je ameriška država »nacionalne varnosti« rapidno transformirala iz države, ki bije vojne, v državo, ki se bojuje proti kriminalu. Andreas, Price, From War Fighting to Crime Fighting, v: International Studies Review, 3 (2001) 3, str. 31–52.

funkcionalnih meja ima za posledico večjo pravno negotovost položaja posameznika pri poseganju v njegovo zasebno sfero. Kako torej ob teh spremembah meja, ki naj jasno razmejijo pravno regulacijo različnih akterjev z namenom, da bi njihova pooblastila lažje nadzorovali, razumeti sodobni nadzor v podatkovni družbi?

Danes ni več dileme o tem, kdo je potencialno »bolj nevaren« ali manj nadzorljiv – države ali »zasebna« internetna, telekomunikacijska podjetja. Model interneta je zasnovan na nadzoru nad podatki,[6] kar koristi vladam in korporacijam, ki ustvarjajo »nadzorstveno-industrijski kompleks«:[7] vlade dobijo v zameno za bolj ohlapno regulacijo teh podjetij zbrane podatke, podjetja pa kujejo dobičke iz zbranih podatkov. Sodobni nadzor je zato treba razumeti drugače, skozi prizmo dveh centrov moči:[8] tradicionalne in razpršene moči.

Tradicionalna moč je organizirana institucionalna moč vlad in korporacij in moč obeh je vse večja. Moč korporacij se povečuje z novimi oblikami storitev v poglabljanju digitalne ekonomije. Npr. z razvojem spletnih socialnih omrežij ali s storitvami »računalništva v oblaku« (*cloud computing*); pri zadnjem se podatki selijo na centralno mesto v »oblak«, kar omogoča lažji nadzor korporacij (obdelovanje itn.) nad podatki in njihovo premeščanje po svetu – glede na ceno električne energije in s tem ceno najema pomnilniške opreme. Moč korporacij se kaže tudi v razvojnem trendu (»dizajnu«) računalniške IT-opreme: vse bolj upravljamo naprave, ki jih na daljavo nadzorujejo proizvajalci; npr. v operacijskem sistemu iOS (Apple) aplikacije težko spreminjamo, v App Storu so vse aplikacije preverjene s strani podjetja Apple, kar omogoča uveljavljanje specifičnega »moralnega reda«.[9]

Drug akter tradicionalne moči so vlade, ki pridobivajo večjo moč s paktiranjem z industrijo, ki masovno kopiči prometne in lokacijske (»meta«) podatke in tudi vsebino.[10] To je v tehnološki družbi čedalje bolj učinkovito: naprave so po Moorovem zakonu vse bolj učinkovite, kopica podatkov pa že generira novo paradigmo vednosti »velikega podatkovja« (*big data*), ki premošča iskanje »zgolj«

6 Schneier, Liars and outliers: enabling the trust society needs to survive (2012), *passim*.

7 Ball, Snider, The surveillance-industrial complex: a political economy of surveillance (2013), *passim*.

8 V nadaljevanju povzemava po: Schenier, The Battle for Power on the Internet, URL: https://www.schneier.com/essays/archives/2013/10/the_battle_for_power.html.

9 O tem več Zittrain, The future of the internet – and how to stop it (2009).

10 NSA ne zbira samo »manj« pomembnih lokacijskih in prometnih podatkov v javnih telekomunikacijskih omrežjih, temveč tudi vsebino (telefonskih pogovorov). The Washington Post poroča, da program MYSTIC za zbiranje telefonskih podatkov ameriške NSA izvaja hrambo »metapodatkov« in »hrambo« glasu vseh telefonskih klicev. Po Schenier, MYSTIC: The NSA's Telephone Call Collection Program, URL: https://www.schneier.com/blog/archives/2014/03/mystic_the_nsas.html.

statističnih povezav med spremenljivkami in omogoča predvidevanje. Družbene dejavnosti so po drugi strani vedno bolj zabeležene v digitalni obliki, kar vodi v naraščanje digitalnih sledi. To vladam in podjetjem omogoča večjo cenzuro, notorično znan je veliki kitajski požarni zid (*Great Firewall of China*) – ki pa se ne razlikuje od demokratičnih (ameriških) posegov,[11] omogoča pa tudi večje proaktivne (propagandne) dejavnosti vlad.

Distribuirana (razpršena) moč je dvojna: pozitivna moč, kot je disidentska moč zoper korupcijo v določeni državi, in negativna, npr. moč kriminalnih skupin.[12] Če tradicionalno moč primerjamo z distribuirano močjo, vidimo, da so predvsem razpršeni centri moči najprej izkoristili moč nove informacijske tehnologije. Npr., ko so se pojavile e-trgovine, so moč informacijskih tehnologij za pridobivanje moči, torej za nadzor, katerega bistvo je moč, (zlo)rabili kriminalci. Ko so se pojavila spletna socialna omrežja, so to izkoristila disidentska gibanja, kot priča primer »arabskih pomladi«. Policije in obveščevalne službe (tradicionalna moč) so potrebovale desetletje, da so dohitele hitri razvoj informacijske družbe. Tradicionalna moč je sicer počasna, ampak je kljub zapoznelim učinkom močnejša od distribuiranih centrov moči, ki so sicer hitri, a šibkejši.

Kako naj torej navadni uporabniki preživimo spopade med korporacijami, vladami in distribuirano močjo kriminalnih združb? Po eni strani je rešitev v transparentnosti delovanja vlad in korporacij, kar je mogoče doseči tudi s pravno regulacijo: z nadzorom (*oversight*) in z uveljavljanjem politične odgovornosti (*accountability*). Zmanjševanje razlik v moči je mogoče doseči s poznavanjem mehanizmov za uveljavljanje pravic, ki so nam na voljo, npr. dostop do informacij javnega značaja, s postavljanjem višje cene našim osebnim podatkom, večjo samozaščito pri uporabi novih spletnih socialnih omrežij in drugih možnosti, o katerih smo v spletnem anketiranju, katerega rezultate predstavljamo v nadaljevanju, povpraševali anketirance. Zmanjševanje razlik v moči pa je mogoče tudi s spremembami pravne doktrine o pojmovanju zasebnosti in regulacije, tj. prava varstva osebnih podatkov.

Osrednji vprašanji prispevka sta zato: (1) kako osmisliti zasebnost glede na nove digitalne tehnologije, zlasti zaradi velike nadzorne kapacitete interneta, v katerega se povezuje vse več naprav (od pametnih »telefonov« do »interneta stvari«), in vznika skrbi za zasebnost, kjer je doslej nismo pričakovali (npr. zasebnost na javnem prostoru), in (2) kakšen je odnos slovenske javnosti do različnih oblik nadzora (npr. na internetu z nastavitvami »odprtosti« uporabniških profi-

[11] Gagnon, Cyberwars and Cybercrime, v: Technocrime: technology, crime and social control (2008), str. 52, 59.

[12] Schneier, The battle for power, URL: https://www.schneier.com/essays/archives/2013/10/ the_battle_for_power.html.

lov v spletnih socialnih omrežjih ali v domeni cestnega prometa) in varovalk ter mehanizmov, ki so na razpolago za omejevanje nadzora v skladu s temeljnimi načeli prava varstva osebnih podatkov, načelom sorazmernosti, učinkovitosti in primernosti (npr. ali javnost pozna osrednji državni organ za varstvo zasebnosti, ali je seznanjena s hrambo prometnih in lokacijskih podatkov v javnih telekomunikacijskih omrežjih).

2. Evolucija pojmovanja zasebnosti in javni prostor

Informacijska tehnologija je sprožila zanimiv teoretični razvoj v pojmovanju zasebnosti, pri katerem izstopata pojmovanje zasebnosti kot kontekstualne integritete osebnih podatkov avtorice Helen Nissenbaum[13] in pluralistično razumevanje zasebnosti Daniela Solova.[14] Oba sta zanimiva z vidika osmišljanja zasebnosti tam, kjer je doslej ne bi pričakovali – pri »drugorazrednih« podatkih (npr. lokacijskih podatkih v javnih telekomunikacijskih omrežjih) na eni strani in zasebnosti na javnem prostoru, ki je bila do razvoja novih tehnologij (npr. video nadzora) bolj ali manj *contradictio in adjecto*.

2.1. Kontekstualna integriteta osebnih podatkov

Teorija Nissenbaumove o kontekstualni integriteti toka osebnih podatkov izhaja iz predpostavke, da so naši osebni podatki (in njihovo razkrivanje) vedno povezani z določenim (konkretnim) družbenim kontekstom. Ne obstaja nobeno področje človekovega bivanja, ki ne bi bilo urejeno s kontekstualno specifičnimi normami toka osebnih podatkov. Konkretneje, v določenih družbenih situacijah (kontekstih) je primerno razkriti določene osebne podatke, medtem ko v drugih kontekstih teh istih podatkov ni primerno razkriti (npr. pri zdravniku je normalno, da razkrijemo svoje zdravstvene težave, pri bančnem okencu pa bi bilo razkrivanje takšnih podatkov neprimerno). Iz tega Nissenbaumova sklepa, da obstajajo norme primernosti razkrivanja osebnih podatkov za posamične družbene sitaucije.

Poleg norm primernosti kontekstualno integriteto osebnih podatkov zagotavljajo še norme distribucije podatkov, tj. kako lahko enkrat razkrite norme potujejo naprej.

---

[13] Po Nissenbaum, Protecting Privacy in an Information Age, v: Law and Philosophy, 17 (1998), str. 559–596; Nissenbaum, Privacy as Contextual Integrity, v: Washington Law Review, 79 (2004) 1, str. 119–157.

[14] Po Solove, »I've Got Nothing to Hide«, v: San Diego Law Review 44 (2007), str. 745.

Ko so norme primernosti in norme distribucije spoštovane, obstaja kontekstualna integriteta osebnih podatkov. Sodobne informacijske tehnologije pa te norme primernosti in norme distribucije osebnih podatkov pogosto kršijo. Npr., nadzor javnega prostora z nadzornimi kamerami in »pametne« tehnologije za komuniciranje osebnih vozil v prometu (z drugimi vozili ali s cestno infrastrukturo) kršijo kontekstualno integriteto osebnih podatkov. Običajno gre tovrstni nadzor pod radarji varuhov zasebnosti: ni vladnega nadzora, ker ne gre za občutljive osebne podatke, te dejavnosti se ne izvajajo v zasebnih prostorih in težko govorimo o tem, da v teh prostorih obstaja »upravičeno pričakovanje« zasebnosti.

Primer aplikacije te teorije je nova komunikacijska tehnologija za varnost vozil (VSC – *vehicle safety communications*).[15] Tehnologija omogoča komunikacijo vozila s prometno infrastrukturo tako, da je v vsakem trenutku mogoče ugotoviti, kje se določeno vozilo nahaja. To je občutno več, kot bi pričakovali po današnjih normah primernosti, ki zahtevajo, da so informacije naših vozil v sicer javnem prometu nespecifične in vizualne (nedigitalne). Če bi kdo želel nadzorovati vozila, bi lahko stal na nadvozu in vozila opazoval, več oseb bi lahko pridobilo več tovrstnih vizualnih podatkov, a za pravo sledenje bi potrebovali zelo veliko število ljudi, ki bi opazovali in pretvorili vizualne podatke v digitalno obliko (kar omogoča nadaljnje obdelave in povezave); potrebovali bi skratka veliko virov; pod predpostavko, da bi nadzorniki bili tudi zelo vešči in bi bili zmožni videti posamezne osebe v vozilih. Tehnologija VSC nasprotno omogoča kontinuiran nadzor nad vozili, kar krši norme primernosti, tj. tega, katere podatke danes štejemo za primerne ob opazovanju vozil. To so le vizualni in nespecifični podatki. Tehnologije VSC (lahko) nadalje kršijo norme distribucije osebnih podatkov: vozila, opremljena s tehnologijami VSC, konstantno oddajajo podatke o identiteti, lokaciji in statusu vozila, te podatke bodo lahko sprejemala druga vozila, prometna infrastruktura ali tretja oseba s primernim sprejemnikom.

Pričakovana zasebnost na javnih prostorih se je s tovrstnimi tehnologijami tako spremenila. Doslej se to ni zdelo pomembno, meni Nissenbaumova, ker: (1) je bila konceptualno ideja, da bi zasebnost v javnem prostoru lahko bila kršena, paradoksna; (2) so dejavniki tega normativne narave, zasebnost je bila pojmovana kot pravica, ki jo je treba uravnoteževati z drugimi med seboj tekmujočimi vrednotami; (3) empirično zasebnosti na javnem prostoru pred vznikom novih informacijskih tehnologij ni bilo mogoče intenzivno kršiti.

[15] Po Zimmer, Surveillance, Privacy and the Ethics, v: Ethics and Information Technology, 7 (2005) 4, str. 201–210.

Teorija o kontekstualni integriteti toka osebnih podatkov je podobna mozaični teoriji o zasebnosti,[16] ki zasebnost pojmuje kot sestavljeno iz informacij, ki same po sebi niso »pomembne«, a so na agregatni ravni ali v kombinaciji z drugimi javno znanimi dejstvi »pomembne«.[17] Vsota »javnih« informacij po tej teoriji ni nujno tudi javna informacija. Ali kot je odločilo Vrhovno sodišče ZDA v primeru *Kylo proti ZDA*[18] za nezakonite preiskave z uporabo tehnologije: četudi bi lahko policija nekatere informacije zbrala s »klasičnim« opazovanjem na javnem mestu, se uporaba posebnih tehnoloških sredstev, ki niso v splošni rabi, lahko kvalificira kot preiskava v smislu 4. amandmaja, ki zahteva odredbo sodišča. Še posebej to velja, če je učinek tehnologije takšen, da bi bil nadzor sicer mogoč, a tako delovno intenziven in drag, da bi bil brez tehnologije praktično neizvedljiv. Pričakovanje zasebnosti obstaja torej tudi glede kumulativnih podatkov, ki jih je mogoče zbrati s tehnologijo, čeprav bi jih lahko teoretično zbrali tudi brez tehnologije.

2.2. Mozaična teorija zasebnosti

Ker na agregatni ravni podatki, ki sami zase niso »pomembni«, v kombinaciji z drugimi podatki postanejo veliko bolj zgovorni o posamezniku, uživajo (ali bi morali uživati) višjo stopnjo pravnega varstva.

V primeru *Jones proti ZDA* (2012) je Vrhovno sodišče ZDA neposredno trčilo v dileme, ki jih odpira mozaična teorija zasebnosti. Policija je na osumljenčevo vozilo brez odredbe sodišča namestila oddajnik GPS in tako prišla do pomembnih inkriminirajočih dokazov. Sodišče je bilo tako pred dilemo, ali pridobivanje mozaičnih delcev – lokacijskih podatkov iz naprave GPS, pritrjene na avtomobil osumljenca – brez odredbe sodišča pomeni takšen poseg, da bi zanj policija potrebovala nalog sodišča (preiskava v smislu 4. amandmaja k ameriški ustavi). Vrhovno sodišče ZDA je odločilo v prid obdolžencu, ker bi sodišče potrebovalo odredbo sodišča. Morda presenetljivo pa svoje odločitve ni oprlo na mozaično teorijo, temveč na drugo argumentacijo. Neavtoriziran fizični vdor policije pri nameščanju naprave GPS na avtomobil je bil kritična točka policijskega dela. Policija bi za namestitev naprave GPS na avtomobil osumljenca morala pridobiti odredbo sodišča zaradi *posega v lastninsko pravico* osumljenca, je

[16] Sanchez, GPS Tracking, URL: http://www.cato.org/blog/gps-tracking-mosaic-theory-government-searches.

[17] Več o mozaični teoriji zasebnosti Kerr, The Mosaic Theory, v: Michigan Law Review, 111 (2012), str. 311–354.

[18] *Kyllo v. United States* (99-8508) 533 U.S. 27 (2001).

menilo sodišče in razveljavilo obsodilno sodbo zoper Jonesa, ker je bila ta oprta na nezakonito pridobljene dokaze.

Nadaljnji razvoj tehnologije, ki se že kaže vsaj v obrisih z razvojem »velikega podatkovja« (*big data*) in paradigmo napovednega policijskega dela (*predictive policing*), kaže, da takšno pojmovanje, kot ga vidimo v opisani sodbi, kmalu ne bo več zadostovalo. Bellovin *et al.* so npr. pokazali, kako je mozaike mogoče kvantificirati, in ugotovili, da za izdelavo celovite podobe posameznika, ki je tako detajlna, da bi o posegu moralo odločati sodišče (in ne sama policija), zadošča že en teden sledenja.[19] V zadevi *Jones* je policija »sledila« osumljencu z napravo GPS en mesec.

Iz drugega zornega kota je v tem smislu mogoče razumeti tudi odločbo sodišča Evropske unije v združenih primerih C-293/12 in C-594/12, z dne 8. 4. 2014, s katero je sodišče odločilo, da je direktiva o hrambi prometnih podatkov[20] neveljavna. Ta direktiva je od samega sprejema vzbujala številne kritike s strani nevladnikov,[21] evropskega nadzornika za varstvo podatkov, nacionalnih organov za varstvo osebnih podatkov (DPA) in Delovne skupine iz 29. člena,[22] a za sodno reakcijo je bilo potrebnih 8 let. Sodišče je tako le odločilo: (1) da je evropski zakonodajalec prekoračil pooblastila, v skladu z dolžnim spoštovanjem načela sorazmernosti; (2) da direktiva ni predvidevala učinkovitih zaščit zoper mogoče zlorabe in nezakonit dostop do osebnih podatkov in (3) da direktiva ni zagotovila uspešnega nadzora nad spoštovanjem vseh zahtev zaščite in varnosti s strani neodvisne institucije. Vsaj za prvi očitek nesorazmernosti velja, da sodi v arzenal mimobežnega naslavljanja problema agregiranih podatkov. Z drugimi besedami, tudi Sodišče Evropske unije ni neposredno naslovilo mozaikov, podobno kot pred njim tudi ne Vrhovno sodišče ZDA v primeru *Jones*.

---

19 Bellovin, Hutchins, Jebara in Zimmeck, When Enough is Enough, v: NYU Journal of Law & Liberty 8 (2014).

20 Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES.

21 Raziskava v poročilu European Digital Rights (17. 4. 2011) navaja, da je hramba imela učinek pri samo 0,002 odstotka kazenskih preiskav. European Digital Rights: »Shadow evaluation report on the Data Retention Directive (2006/24/EC) 17 April 2011«, URL: http://www.edri.org/files/shadow_drd_report_110417.pdf.

22 Delovna skupina za varstvo osebnih podatkov iz člena 29, ustanovljena na podlagi Direktive 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995, je poudarila, da »pomanjkanje razpoložljivih smiselnih statističnih podatkov otežuje oceno, ali je Direktiva dosegla zastavljene cilje«, in da »kvalitativni podatki, kot so npr. vrste kaznivih dejanj, pri katerih bi bilo s pomočjo ukrepov iz Direktive moč zavreči obtožbe, ne pomenijo statističnih dokazov v smislu 10. člena Direktive«. Sporočilo za javnost z dne 14. julija 2010.

2.3. Pluralistično razumevanje zasebnosti

Nov pogled na zasebnost, ki ga je sprožila informacijska tehnologija, predstavlja Solove,[23] ki trdi, da je tradicionalna metoda konceptualiziranja – tj. ko iščemo nujne in zadostne elemente pojavov – za razumevanje zasebnosti slepa ulica. Zelo hitro tako zdrsnemo v preozko pojmovanje zasebnosti kot intimnosti na eni strani ali pa smo – na drugi strani – pri pojmovanju zasebnosti preširoki in jo pojmujemo kot »pravico, da nas pustijo pri miru«. Solove trdi, da to, kar opisujemo s pojmi zasebnosti, pogosto nima skupnega imenovalca, ampak so problemi drug z drugim v razmerju na različne načine. Zato predlaga izdelavo zemljevida različnih tipov problemov in škode, ki skupaj konstituirajo problematiko zasebnosti.

Zasebnost je po Solovu niz zaščit zoper sorodne probleme. Problemi niso povezani na enak način, so si pa podobni. V taksonomiji različnih tipov problemov in škode, ki skupaj konstituirajo kršitve zasebnosti, se osredotoča na štiri kategorije problemov: (1) zbiranje podatkov in z njimi povezana škoda; (2) obdelovanje podatkov, kamor sodijo izzivi, povezani s shranjevanjem, analiziranjem in spreminjanjem podatkov, (3) razpečevanje podatkov in (4) invazijo kot npr. vmešavanje v odločanje. Solove prepričljivo ovrže Orwellovo metaforo sodobnega nadzora. Ta se nanaša samo na sklop zbiranja podatkov, izpušča pa preostale. Primernejši aparat ponuja Kafkova, saj se sodobni nadzor nanaša na skrivnostne obdelave, ki so ne le skrite pred očmi, temveč njihove posledice (npr. zavrnitev kredita, ker je naša boniteta v medbančnem sistemu slaba, ali pa zavrnitev vkrcanja na letalo, ker smo se znašli na t. i. seznamu *no-fly*) tudi neposredno učinkujejo na razmerju moči med ljudmi in med ljudmi ter institucijami v moderni državi.

Ključen za Solova je premik v pojmovanju zasebnosti kot le individualne pravice (kot spoštovanja posameznikove osebnosti ali njegove avtonomije). Družbena vrednost zasebnosti je namreč večja in kot individualna pravica ni v nenehni napetosti z družbenimi interesi. Njegova teorija je zato v tem smislu »postmodernistična« in ciklična, saj predpostavlja, da je posameznik tisti, ki ga družba šele oblikuje, hkrati pa razume družbo tako, da ta obstaja le, če jo posamezniki performativno poustvarjajo. Družba zato varuje zasebnost, ker je ta koncept način varovanja specifične oblike skupnosti. Zasebnost ni le način, kako izvleči posameznika iz družbenega nadzora (»pravica, da te pustijo pri miru«), temveč je sama pravna regulacija zasebnosti oblika družbenega nadzora.

[23] Solove, »I've Got Nothing to Hide«, v: San Diego Law Review 44 (2007), str. 745.

Poglejmo v nadaljevanju, kako javnost, zlasti slovenska in mlajša javnost, dojema različne vidike zasebnosti.

3. Odnos slovenske javnosti do zasebnosti

3.1. Metoda

V letih 2012, 2013 in 2014 smo na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani v okviru projekta »Tehnično okrepljeno nadzorovanje in boj zoper kriminaliteto: etični, pravni in kriminološki vidiki porajajočih se detekcijskih in nadzornih tehnologij« izvedli spletno anketo o uporabi informacijske tehnologije, o kibernetski kriminaliteti in o viktimizacijah s pomočjo spletnega sistema Google docs. Anketa je vsebovala 31 zaprtih vprašanj (intervalna vprašanja, vprašanja z eno možno izbiro, tabelarična vprašanja z več možnimi odgovori, ocenjevalne tabele) in 4 demografska vprašanja. V analizo so vključeni odgovori prvega anketiranja v šolskem letu 2012/2013 (od oktobra do maja) in drugega anketiranja v šolskem letu 2013/2014 (od oktobra do februarja).

Anketa je obsegala štiri sklope:

1. kibernetske viktimizacije: med temi so za zasebnost relevantna vprašanja o odnosu do prestrezanja vsebine spletnih komunikacij, o tem, ali so anketiranci že bili žrtve osebnih podatkov na internetu, objave diskreditirajočih fotografij brez soglasja. Anketirance smo spraševali še o samozaščitnem vedenju (npr., ali uporabljajo različne vrste računalniške programske zaščite), njihovem razumevanju delovanja različnih spletnih groženj in njihovem obnašanju po viktimizacijah (tj. na koga bi se obrnili v primeru različnih viktimizacij);

2. kibernetske aktivnosti: med temi smo preverjali dejanja anketirancev, ki kršijo zasebnost tretjih oseb (samoprijavitvena študija). Vprašanja so se nanašala na grožnje zasebnosti, ki so jih anketiranci zadajali tretjim osebam na spletu, posebej na socialnih omrežjih;

3. varstvo osebnih podatkov: merili smo stopnjo zaskrbljenosti nad varnostjo osebnih podatkov v različnih domenah nadzora (poleg interneta še pri izdelavi osebnih dokumentov, pri videonadzoru javnega prostora, pri uporabi pametne kartice Urbana, v programih »zvestobe« trgovskih verig). Preverjali smo obstoj strahu pred različnimi izvajalci nadzora, pripravljenost anketirancev oddati svoje osebne podatke za različne ugodnosti, poznavanje in odnos do hrambe podatkov v javnih telekomunikacijskih omrežjih in poznavanje mehanizmov za varstvo pravic;

4. odnos do izbranih nadzornih tehnologij se je nanašal na nadzor v cestnem prometu (npr. koliko podpirajo različne tehnologije) in na spletu (npr. zanimala nas je percepcija lastnega nadzora respondentov nad osebnimi podatki, nastavitve zasebnosti v spletnih socialnih omrežjih).

Anketirance smo k sodelovanju povabili z objavo obvestil na internetu, po fakultetah in po elektronski pošti. Ciljna populacija so bili študentje (sodelovali so pretežno študentje Pravne fakultete in Fakultete za družbene vede Univerze v Ljubljani ter Fakultete za varnostne vede Univerze v Mariboru).

Analiza podatkov je bila opravljena s programom SPSS 15.[24] Izdelane so bile dvorazsežne frekvenčne (kontingenčne) tabele, za izračune povezav med spremenljivkami so bili uporabljeni Pearsonov hi-kvadrat, test χ^2, razmerje verjetij (*likelihood ratio*) in Cramerjev koeficient. Test χ^2 smo izvajali s stopnjo značilnosti $\alpha = 0{,}05$ (mejna vrednost verjetnosti, pod katero zavrnemo ničelno hipotezo). Ne glede na to, da je pri testiranju neodvisnosti spremenljivk na majhnih vzorcih bolj natančen test razmerja verjetij, pri velikih vzorcih, kot je bil naš, pa Pearsonov χ^2, sta bila vedno preverjena oba.[25] Če je bil χ^2 za Pearsona manjši od 0,05, za *likelihood ratio* pa večji, smo sprejeli sklep, da spremenljivki nista povezani. Za ugotavljanje srednjih vrednosti so bile izdelane tabele srednje vrednosti in 95-odstotni interval zaupanja. Za razlike med spoloma smo uporabili ordinalno logistično regresijo, kjer je neodvisna spremenljivka spol lahko zavzela vrednosti *moški, ženski*, odvisna spremenljivka pa je lahko zavzela vrednosti na intervalu [1–5].

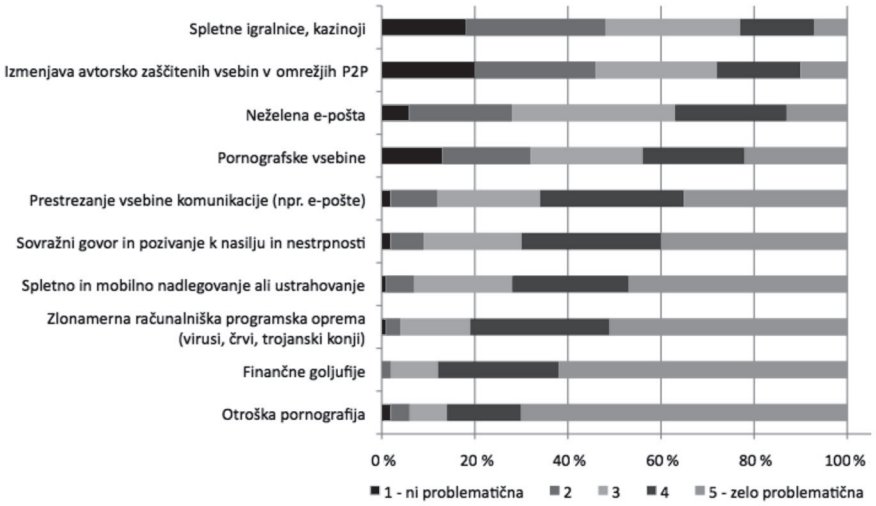
Prvi sklop anketiranja smo izvedli v šolskem letu 2012/2013, kjer s končnim vzorcem 539 (n_1). V omenjenem obdobju smo postopno dodali nekaj vprašanj in tako v istem časovnem obdobju za štiri vprašanja velja $n_2 = 481$. Drugi sklop anketiranja smo izvedli v šolskem letu 2013/2014, ko je bil vzorec anketirancev enak 266 (n_3).

3.2. Viktimizacije, povezane s posegi v zasebnost

Med različnimi *nevarnostmi pri uporabi interneta* 66 odstotkov anketiranih nevarnost prestrezanja vsebine komunikacij dojema kot bolj problematično (na lestvici med 1 – ni problematično in 5 – zelo problematično so dali oceno 4 ali 5). Kar 82 odstotkov pa jih zlonamerno računalniško opremo, ki je pogosto sredstvo za kršitve zasebnosti, dojema kot bolj problematično (ocena 4 ali 5); bolj problematične se jim zdijo le še otroška pornografija in finančne goljufije.

[24] Za pomoč pri statistični obdelavi podatkov se posebej zahvaljujeva spec. Bogomilu Brvarju.
[25] Brvar, Statistika (2007).

Slika 1: Nevarnosti pri uporabi interneta

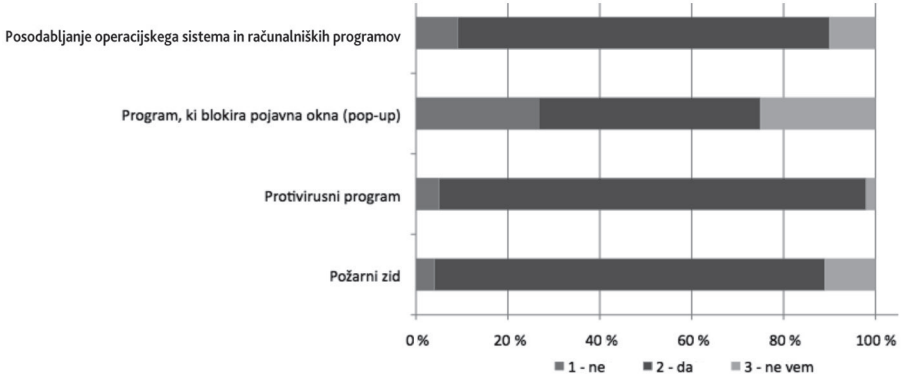


Na vprašanje, ali so bili anketirani že *žrtve* različnih viktimizacij, povezanih z internetom in z varstvom zasebnosti, jih je 9 odstotkov odgovorilo, da so že bili žrtev kraje osebnih podatkov na internetu (enkrat ali večkrat), 23 odstotkov anketiranih pa je bilo viktimiziranih v obliki objavljanja diskreditirajočih fotografij brez soglasja (npr. na Facebooku ali s pošiljanjem po e-pošti).

Na vprašanja o *poznavanju spletnih groženj* – spraševali smo jih o poznavanju računalniških virusov in črvov, spletnega ribarjenja (*phishing*), *botnet* mrež, *skimminga* bančnih kartic in vohunskih programov – so za neposredne grožnje zasebnosti uporabnikov, ki jih pomenijo vohunski programi, respondenti odgovorili, da vohunske programe »še kar« in »zelo dobro« (na lestvici od 1 – ne razumem do 5 – zelo dobro razumem) razume 35 odstotkov. To je sicer slabše od računalniških virusov in črvov, a še vedno občutno bolje od preostalih spletnih ogrožanj.

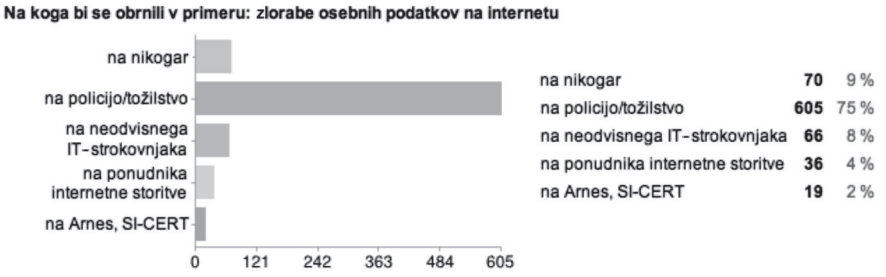
Samozaščitno preventivno vedenje respondentov je sestavni del celovitega varstva zasebnosti, zato smo respondente spraševali o tem, kako ščitijo svoje računalnike.

Slika 2: Samozaščitni ukrepi – preventiva



Samozaščitno kurativno vedenje smo preverjali tako, da smo povprašali, na koga bi se respondenti obrnili v različnih primerih spletnega ogrožanja, in sicer v primerih nepooblaščenega vdora v računalnik, sesutja informacijskega sistema iz neznanega razloga, neželene e-pošte, nadlegovanja po e-pošti, nadlegovanja v spletnem socialnem omrežju, nadlegovanja po mobilnem telefonu in zlorabe osebnih podatkov.

Slika 3: Samozaščitni ukrepi – kurativa v primeru zlorab osebnih podatkov na internetu



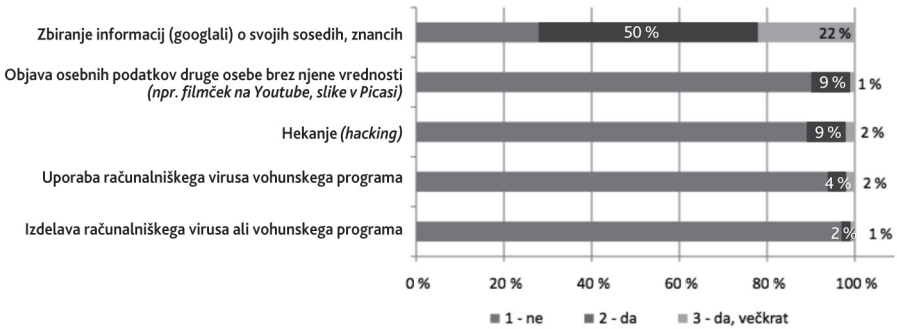
Pri zlorabi osebnih podatkov so respondenti pokazali relativno večje zaupanje do policije kot pri drugih oblikah ogrožanja in kršitev, zlasti pri nepooblaščenem vdoru v računalnik, kjer bi večina bolj zaupala neodvisnim strokovnjakom kot policiji.

Slika 4: Samozaščitni ukrepi – kurativa v primeru nepooblaščenega vdora v računalnik

3.3. Samoprijave groženj zasebnosti

Anketirance smo v samoprijavitveni študiji spraševali, ali so že kdaj storili dejanja, ki ogrožajo tretje osebe ali pomenijo obliko nadzora.

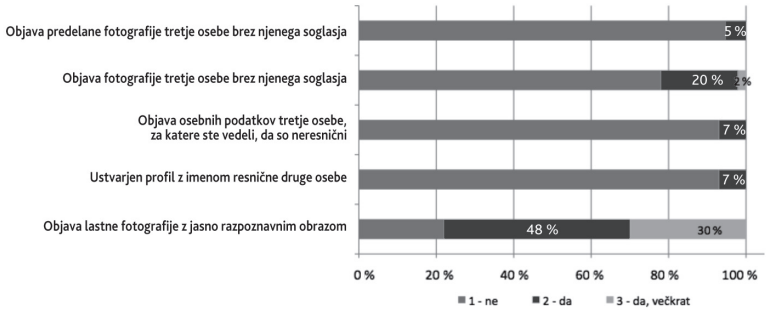
Slika 5: Samoprijave ogrožanja



Medtem ko je zbiranje informacij iz javno dostopnih zbirk večinsko opravilo, saj le 28 odstotkov anketirancev še nikoli ni »googlalo« za drugimi, so dejanja uporabe zlonamerne kode ali njene izdelave razmeroma redka.

Približno desetina anketirancev se v spletnih socialnih omrežjih obnaša odklonsko. Ko smo jih povprašali glede storitve več različnih dejanj, smo glede dejanj, ki pomenijo potencialne grožnje varstvu zasebnosti tretjih oseb, ugotovili to, kar kaže slika 6.

Slika 6: Samoprijave ogrožanja v spletnih socialnih omrežjih

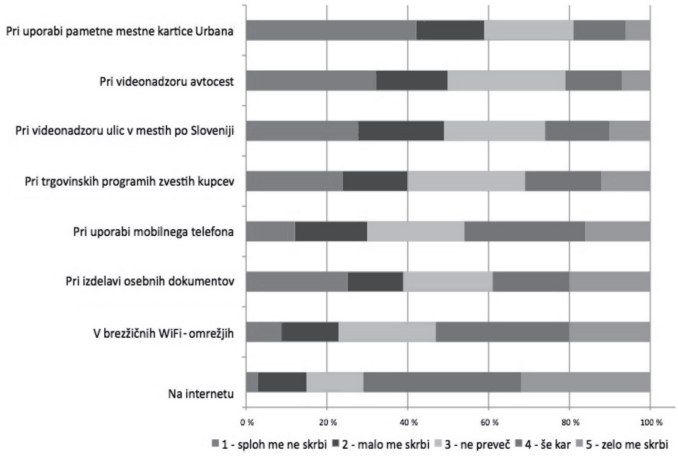


Pri napadu na zasebnost tretjih oseb prednjači objava fotografije tretje osebe brez njenega soglasja. Za dejanja, ki razkrivajo lastno zasebnost (objava lastne fotografije z jasno razpoznavnim obrazom), pa ugotovljamo visokih 78 odstotkov anketiranih, ki je objavilo (enkrat ali večkrat; 30 odstotkov večkrat) takšne lastne podobe; s primerjanjem prvega in drugega anketiranja ugotavljamo tudi, da podatek v času narašča.

3.4. Skrb za varnost osebnih podatkov

Anketirance smo spraševali, kako zelo jih skrbi varnost njihovih osebnih podatkov (vzorec = n_1).

Slika 7: Kako zelo vas skrbi varnost vaših osebnih podatkov



Pri tem vprašanju se največja zaskrbljenost kaže na področju interneta, saj »še kar« ali »zelo skrbi« kar 70 odstotkov anketirancev. Povečana zaskrbljenost se kaže tudi pri priklopu v brezžično omrežje (53 odstotkov) in pri uporabi mobilnega telefona (45 odstotkov).

Pri izračunu časovne primerjave med n_1 in n_3 ni statistično pomembnih razlik.

Tabela 1: Kako zelo vas skrbi varnost vaših osebnih podatkov – razlike med spoloma

Kako zelo vas skrbi varnost vaših podatkov	hi-kvadrat	s. p.	P (H0)	Cramerjev koeficient
na internetu	14,6	4	0,00	0,16
v brezžičnih WiFi-omrežjih	0	4	0,30	0,00
pri izdelavi osebnih dokumentov	0	4	0,82	0,00
pri trgovinskih programih »zvestih kupcev« (npr. pri zbiranju točk za občasne popuste)	0	4	0,50	0,00
pri videonadzoru avtocest	12,1	4	0,02	0,15
pri videonadzoru ulic v mestih po Sloveniji	9,7	4	0,05	0,13
pri uporabi pametne mestne kartice Urbana	0	4	0,08	0,00
pri uporabi mobilnega telefona	15,7	4	0,00	0,17

Spol nekoliko močneje vpliva le na skrb za varnost podatkov na internetu ($\chi^2 = 14{,}6$, $p = 0{,}006$), pri videonadzoru cest ($\chi^2 = 12{,}1$, $p = 0{,}016$) in predvsem pri uporabi mobilnega telefona ($\chi^2 = 15{,}7$, $p = 0{,}003$), zmerno povezanost (0,16, 0,15, 0,17, i. o.) potrjuje tudi Cramerjev koeficient. Pri vseh treh navedenih spremenljivkah so večjo skrb izrazile ženske.

3.4.1. Skrb za varnost osebnih podatkov na spletu

Zanimalo nas je tudi, kakšen je odnos vprašanih do zasebnosti pri udejstvovanju na svetovnem spletu. Statistično pomembnih razlik v času in med spoloma ni (vzorec = n_2).

Tabela 2: Zaznavanje nadzora nad podatki v spletnih socialnih omrežjih

ANKETA * 28. Koliko nadzora menite, da imate nad podatki, ki ste jih razkrili na spletnih socialnih omrežjih (Crosstabulation)

			28. Koliko nadzora menite, da imate nad podatki, ki ste jih razkrili na spletnih socialnih omrežjih?				Total
			1 - popolni nadzor	2 - delni nadzor	3 - nobenega nadzora	4 - ne vem	
ANKETA	Druga anketa	Count	41	281	124	35	481
		Expected Count	33,5	293,0	118,5	36,1	481,0
		% within ANKETA	8,5 %	58,4 %	25,8 %	7,3 %	100,0 %
	Tretja anketa	Count	11	174	60	21	266
		Expected Count	18,5	162,0	65,5	19,9	266,0
		% within ANKETA	4,1 %	65,4 %	22,6 %	7,9 %	100,0 %
Total		Count	52	455	184	56	747
		Expected Count	52,0	455,0	184,0	56,0	747,0
		% within ANKETA	7,0 %	60,9 %	24,6 %	7,5 %	100,0 %

Tabela 3: Zaznavanje nadzora nad podatki pri spletnem nakupovanju

ANKETA * 28. Koliko nadzora menite, da imate nad podatki, ki ste jih razkrili pri spletnem nakupovanju (Crosstabulation)

			28. Koliko nadzora menite, da imate nad podatki, ki ste jih razkrili pri spletnem nakupovanju?					Total
				1 - popolni nadzor	2 - delni nadzor	3 - nobenega nadzora	4 - ne vem	
ANKETA	Druga anketa	Count	58	46	247	101	87	539
		Expected Count	38,8	43,5	266,5	103,1	87,0	539,0
		% within ANKETA	10,8 %	8,5 %	45,8 %	18,7 %	16,1 %	100,0 %
		% within 28. Koliko nadzora menite, da imate nad podatki, ki ste jih razkrili pri spletnem nakupovanju	100,0 %	70,8 %	62,1 %	65,6 %	66,9 %	67,0 %
		% of Total	7,2 %	5,7 %	30,7 %	12,5 %	10,8 %	67,0 %
	Tretja anketa	Count	0	19	151	53	43	266
		Expected Count	19,2	21,5	131,5	50,9	43,0	266,0
		% within ANKETA	0 %	7,1 %	56,8 %	19,9 %	16,2 %	100,0 %
		% within 28. Koliko nadzora menite, da imate nad podatki, ki ste jih razkrili pri spletnem nakupovanju	0 %	29,2 %	37,9 %	34,4 %	33,1 %	33,0 %
		% of Total	0 %	2,4 %	18,8 %	6,6 %	5,3 %	33,0 %
Total		Count	58	65	398	154	130	805
		Expected Count	58,0	65,0	398,0	154,0	130,0	805,0
		% within ANKETA	7,2 %	8,1 %	49,4 %	19,1 %	16,1 %	100,0 %
		% within 28. Koliko nadzora menite, da imate nad podatki, ki ste jih razkrili pri spletnem nakupovanju	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %
		% of Total	7,2 %	8,1 %	49,4 %	19,1 %	16,1 %	100,0 %

Tabela 4: Nastavitve zasebnosti v spletnih socialnih omrežjih

ANKETA * 29. Kakšne nastavitve imate v spletnih socialnih omrežjih (Crosstabulation)

			29. Kakšne nastavitve imate v spletnih socialnih omrežjih					Total
			delno zasebno	javno	Ne uporabljam	ne vem	zasebno	
ANKETA	Druga anketa	Count	160	15	15	21	270	481
		Expected Count	152,0	16,1	16,7	21,2	274,9	481,0
		% within ANKETA	33,3 %	3,1 %	3,1 %	4,4 %	56,1 %	100,0 %
	Tretja anketa	Count	76	10	11	12	157	266
		Expected Count	84,0	8,9	9,3	11,8	152,1	266,0
		% within ANKETA	28,6 %	3,8 %	4,1 %	4,5 %	59,0 %	100,0 %
Total		Count	236	25	26	33	427	747
		Expected Count	236,0	25,0	26,0	33,0	427,0	747,0
		% within ANKETA	31,6 %	3,3 %	3,5 %	4,4 %	57,2 %	100,0 %

Tabela 5: S kom komunicirate na spletu

ANKETA * 30. S kom komunicirate na spletu (Crosstabulation)

			30. S kom komunicirate na spletu				Total
			ne komuniciram po spletu	oboje	z osebami, ki jih poznam že od prej	z osebami, ki sem jih spoznal/a na spletu	
ANKETA	Druga anketa	Count	7	145	326	3	481
		Expected Count	9,7	140,4	329,0	1,9	481,0
		% within ANKETA	1,5 %	30,1 %	67,8 %	0,6 %	100,0%
	Tretja anketa	Count	8	73	185	0	266
		Expected Count	5,3	77,6	182,0	1,1	266,0
		% within ANKETA	3,0 %	27,4 %	69,5 %	0,0 %	100,0%
Total		Count	15	218	511	3	747
		Expected Count	15,0	218,0	511,0	3,0	747,0
		% within ANKETA	2,0 %	29,2 %	68,4 %	0,4 %	100,0%

Tabela 6: S kom delite gesla uporabniških računov spletnih socialnih omrežij

ANKETA * 31. Svoja gesla za dostop do spletnih socialnih omrežij (Crosstabulation)

			31. Svoja gesla za dostop do spletnih socialnih omrežij				Total
			delim izključno s svojim partnerjem/partnerko.	imam zapisana na listu papirja ob svojem računalniku.	ne delim z nikomer.	ne uporabljam spletnih socialnih omrežij.	
ANKETA	Druga anketa	Count	79	13	385	4	481
		Expected Count	75,3	10,3	390,9	4,5	481,0
		% within ANKETA	16,4 %	2,7 %	80,0 %	0,8 %	100,0 %
	Tretja anketa	Count	38	3	222	3	266
		Expected Count	41,7	5,7	216,1	2,5	266,0
		% within ANKETA	14,3 %	1,1 %	83,5 %	1,1 %	100,0 %
Total		Count	117	16	607	7	747
		Expected Count	117,0	16,0	607,0	7,0	747,0
		% within ANKETA	15,7 %	2,1 %	81,3 %	0,9 %	100,0 %

Kar četrtina anketirancev je prepričanih, da nad podatki, ki jih razkrijejo v spletnih socialnih omrežjih, nimajo nobenega nadzora, kljub temu, da skoraj dve tretjini vprašanih uporablja nastavitev »zasebno«, da jih več kot dve tretjini komunicira zgolj z osebami, ki jih poznajo od prej, ter da več kot 80 odstotkov anketirancev svojega gesla za dostop do spletnih socialnih omrežij ne deli z nikomer.

3.5. Zaznavanje ogroževalcev zasebnosti

Izmed ponujenih možnosti anketirancem največjo grožnjo zasebnosti pomenijo spletni velikani, in sicer se je za odgovor »še kar« ter »zelo« odločilo 56 odstotkov anketirancev, za njimi pa operaterji telekomunikacijskih storitev s 25 odstotki in trgovine s programi »zvestobe« s 23 odstotki (vzorec = n_1).

Slika 8: Kdo najbolj ogroža vašo zasebnost?

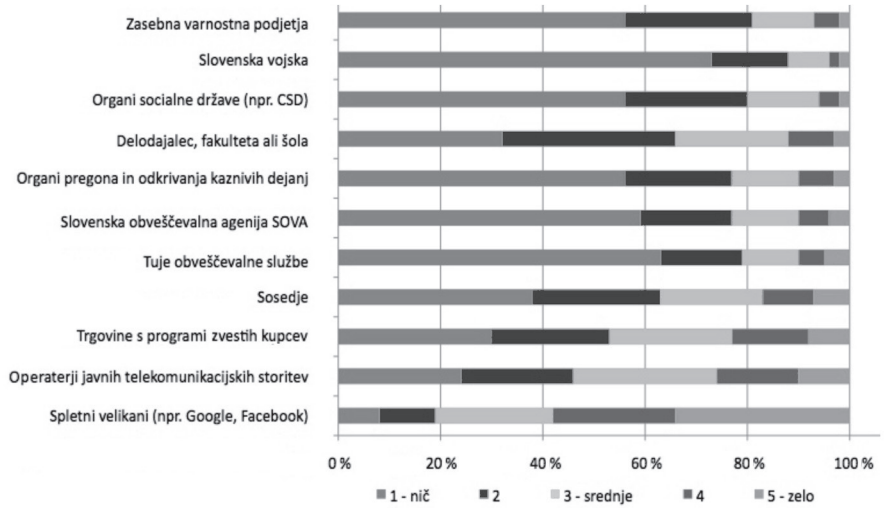


Tabela 7: Kdo najbolj ogroža vašo zasebnost – razlike med spoloma

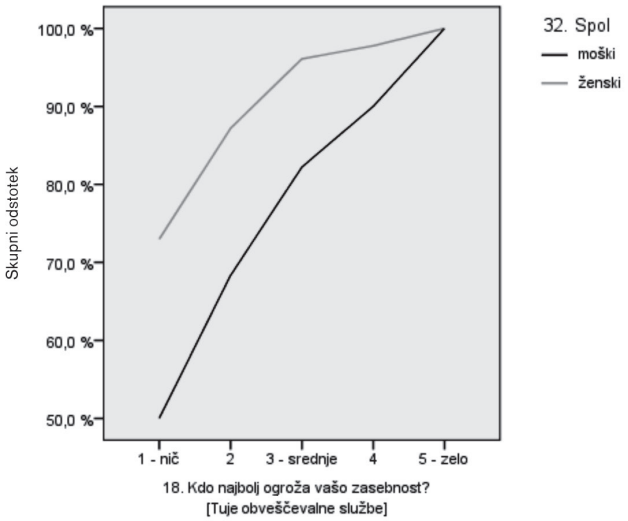
Kdo najbolj ogroža vašo zasebnost	Hi-kvadrat	s. p.	P (H0)	Cramerjev koeficient
Organi pregona in odkrivanja kaznivih dejanj	21,5	4	0,00	0,20
Organi socialne države (npr. centri za socialno delo)	3,8	4	0,43	0,08
Slovenska obveščevalna agencija SOVA	39,3	4	0,00	0,27

Slovenska vojska	18,8	4	0,00	0,19
Tuje obveščevalne službe	40,9	4	0,00	0,28
Spletni velikani (npr. Google, Facebook)	1,2	4	0,87	0,05
Trgovine s programi zvestih kupcev	7,4	4	0,12	0,12
Operaterji javnih telekomunikacijskih storitev	8,6	4	0,70	0,13
Sosedje	12,4	4	0,15	0,15
Zasebna varnostna podjetja	21,4	4	0,00	0,20
Delodajalec, fakulteta ali šola	3,6	4	0,46	0,08

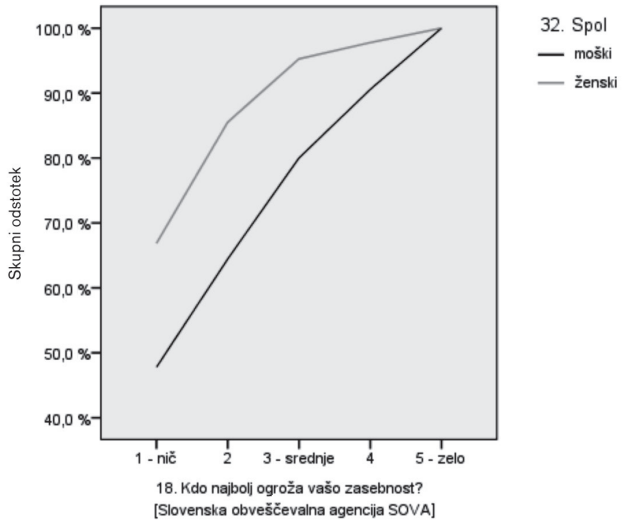
Povezanost med ogrožanjem zasebnosti in spolom je za vse spremenljivke v tej kategoriji šibka. Moški se nekoliko bolj počutijo ogrožene s strani tujih obveščevalnih služb (χ^2 = 40,9, p = 0,000) ter slovenske obveščevalne agencije (χ^2 = 39,3, p = 0,000). Cramerjev koeficient nakazuje zmerno povezanost (0,28 in 0,27, i. o.).

Pri izračunu s pomočjo ordinalne logistične regresije smo ugotovili, da moški anketiranci na to vprašanje 0,34-krat več odgovorijo z nižjimi ocenami (tuje obveščevalne službe) in 0,38-krat z nižjimi ocenami pri odgovoru »slovenska obveščevalna agencija SOVA«, kar lahko tudi grafično ponazorimo:

Slika 9: Tuje obveščevalne službe



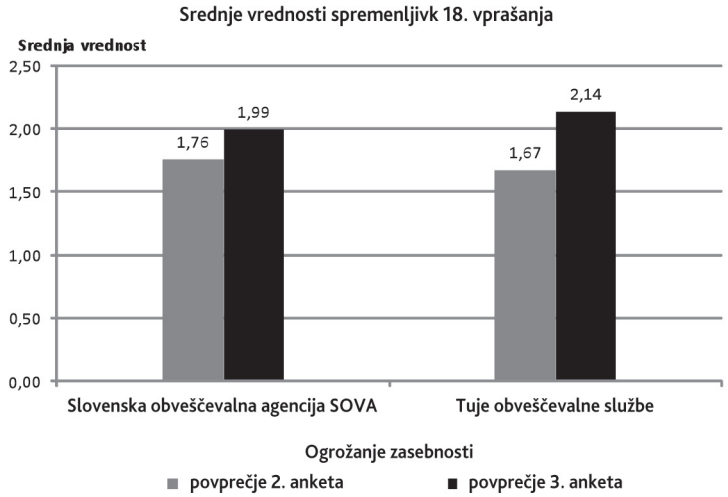
Slika 10: Slovenska obveščevalna agencija SOVA



Primerjali smo odgovore anketirancev glede ogrožanja zasebnosti s strani domačih in tujih obveščevalnih agencij pred afero Datagate (junij 2013) in po njej. Po pričakovanjih se je v obdobju anketiranja pred tem datumom (anketiranje 2012–2013) le malo ljudi počutilo ogroženih s strani tujih in domačih obveščevalnih agencij – kot stopnjo ogrožanja »nič« je izbralo, i. o., 65 odstotkov oz. 60 odstotkov, medtem ko je enak odgovor v poznejšem anketiranju (september 2013 – januar 2014) izbralo zgolj, i. o., 48 odstotkov oz. 44 odstotkov anketirancev.

To lahko prikažemo tudi s primerjalnim izračunom srednje vrednosti (aritmetične sredine) in standardnih odklonov: pri odgovoru »tuje obveščevalne službe« smo zaznali povečanje srednje vrednosti z 1,67 na 2,14. Srednja vrednost pri občutku ogrožanja s strani domače obveščevalne agencije pa se je povečala z 1,76 na 1,99. Standardni odkloni so podobni pri obeh anketah, so pa veliki, kar pomeni, da so vrednosti – ocene posameznih odgovorov – razpršene okoli srednje vrednosti.

Slika 11: Ogrožanje zasebnosti s strani obveščevalnih služb v času – srednje vrednosti

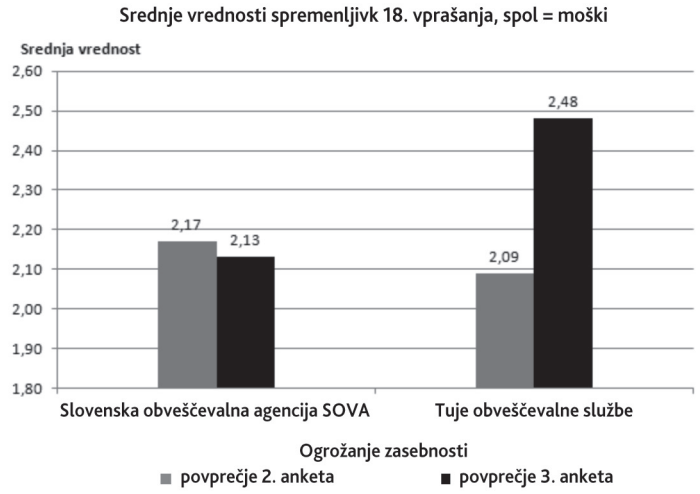


Standardni odkloni:

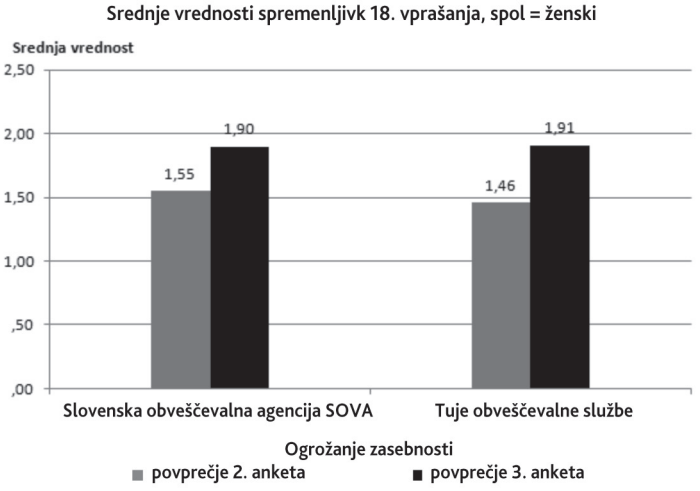
- slovenska obveščevalna agencija SOVA: $n_1 = 1{,}135$ $n_3 = 1{,}143$;
- tuje obveščevalne agencije: $n_1 = 1{,}112$, $n_3 = 1{,}224$.

Povečan občutek ogroženosti s strani teh dveh služb se kaže tako pri moških kot pri ženskah. Srednja vrednost pri moških se je tako povečala z 2,09 na 2,48 (tuje obveščevalne službe), medtem ko se je, zanimivo, pri odgovoru SOVA ta srednja vrednost malenkostno zmanjšala (z 2,17 na 2,13). Pri ženskah sta se obe vrednosti znatno povečali: z 1,46 na 1,91 (tuje obveščevalne službe) ter z 1,55 na 1,90 (SOVA).

Slika 12: Ogrožanje zasebnosti s strani obveščevalnih služb v času glede na spol (M) – srednje vrednosti



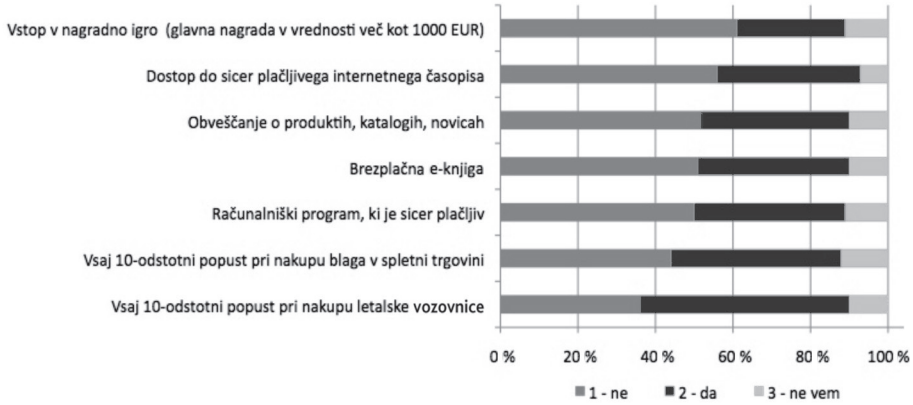
Slika 13: Ogrožanje zasebnosti s strani obveščevalnih služb v času glede na spol (Ž) – srednje vrednosti



3.6. (Samo)vrednotenje zasebnosti

Pri naslednjem vprašanju nas je zanimalo, kolikšnemu obsegu zasebnosti so se anketirani pripravljeni odpovedati v zameno za korist, ki jim jo oddaja osebnih podatkov prinese. Vprašanje se je glasilo: ali bi oddali svoje osebne podatke (npr. datum rojstva, spol in elektronski naslov) v zameno za ...« (vzorec = n_1).

Slika 14: Cena zasebnosti



Med danimi možnostmi se najmanj mamljiva zdi ponudba vstopa v nagradno igro, saj 62 odstotkov anketirancev ne bi oddalo osebnih podatkov v ta namen, medtem ko se je večina anketiranih pripravljena odpovedati delu zasebnosti za vsaj 10-odstotni popust pri nakupu letalske vozovnice (52 odstotkov) ali vsaj 10-odstotni popust pri nakupu v spletni trgovini (42 odstotkov).

Pri primerjavi med prvo anketo (n_1) in drugo anketo (n_3) se je statistično pomembna razlika pokazala le pri možnosti »računalniški program, ki je sicer plačljiv«, in sicer se je povečalo število anketirancev, ki ne bi oddali svojih osebnih podatkov za ta namen (n_1 = 51 odstotkov, n_3 = 61 odstotkov).

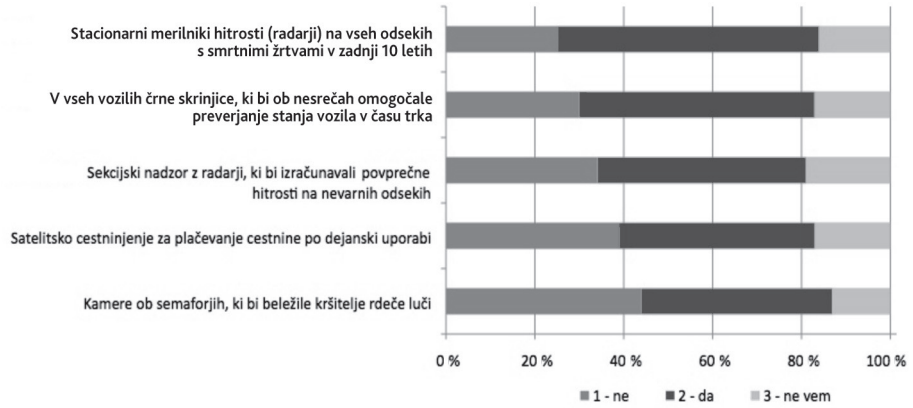
Tabela 8: Ali bi oddali svoje osebne podatke v zameno za ...
– razlike med spoloma

Ali bi oddali svoje osebne podatke (npr. datum rojstva, spol in elektronski naslov) v zameno za	hi-kvadrat	s. p.	P (H0)	Cramerjev koeficient
obveščanje o produktih, katalogih, novicah	28,2	2	0,00	0,23
dostop do sicer plačljivega internetnega časopisa	0,3	2	0,99	0,02
računalniški program, ki je sicer plačljiv	7,0	2	0,30	0,11
vsaj 10% popusta pri nakupu	0,3	2	0,99	0,02
vsaj 10% popusta pri nakupu letalske karte	1,7	2	0,42	0,06
brezplačno e-knjigo	13,7	2	0,00	0,16
vstop v nagradno igro (glavna nagrada v vrednosti več kot 100 EUR	1,9	2	0,38	0,06

Razlike med spoloma so statistično pomembne pri odgovorih »obveščanje o produktih, katalogih, novicah« (χ^2 = 28,2, sig. = 0,000) ter pri možnosti brezplačne e-knjige (χ^2 = 13,7, sig. = 0,001). Cramerjev koeficient nakazuje zmerno povezanost (0,23 in 0,16, i. o.). Pri obeh spremenljivkah so moški v primerjavi z ženskami bolj zadržani pri oddaji osebnih podatkov za ponujene ugodnosti.

Anketirance smo še vprašali, ali bi podprli namestitev različnih nadzornih tehnologij na slovenskih cestah.

Slika 15: Naklonjenost nadzoru na cestah



Največ se jih je odločilo za stacionarne merilnike hitrosti na vseh odsekih s smrtnimi žrtvami v zadnjih desetih letih, in sicer 58 odstotkov. Najmanj priljubljen ukrep so kamere ob semaforjih, ki bi beležile kršitelje rdeče luči, in sicer bi jih podprlo 43 odstotkov vprašanih. Razlike v času in med spoloma pri tem vprašanju ni.

3.7. Odnos do hrambe osebnih podatkov

Kar 53 odstotkov anketirancev (vzorec = n_1) ni vedelo, da Zakon o elektronskih komunikacijah (ZEKom-1)[26] določa, da morajo ponudniki telekomunikacijskih storitev hraniti vse prometne podatke telefonskih in internetnih komunikacij (npr. kdo je kdaj komu in koliko časa telefoniral, poslal elektronsko sporočilo, kdo je kdaj obiskal katero spletno mesto ter podatke o lokacijah mobilnih telefonov) 14 oz. 8 mesecev. Zanimalo nas je, ali zaradi tega manj uporabljajo telefonske in internetne komunikacije; velika večina, ki je tovrstno hrambo predhodno poznala, je odgovorila z »ne« (83 odstotkov). Podobnega mnenja so bili pri vprašanju, ali zaradi tovrstne hrambe menijo, da drugi manj komunicirajo z njimi; o tem jih je bilo prepričanih (»da«) zgolj 8 odstotkov. Statistično pomembne razlike med spoloma ni.

Nadalje nas je zanimalo, ali so kljub tovrstni hrambi podatkov pripravljeni uporabiti telefonsko ali internetno komunikacijo za bolj osebne zadeve (npr. pogovor s psihoterapevtom, odvetnikom ipd.); 48 odstotkov anketirancev bi uporabilo takšno komunikacijo.

Tabela 9: Hramba in uporaba telefonske ali internetne komunikacije za osebne zadeve – razlike med spoloma

	hi-kvadrat	s. p.	P (H0)	Cramerjev koeficient
Ali bi kljub tovrstni hrambi podatkov uporabili telefonsko ali internetno komunikacijo za bolj osebne zadeve (npr. pogovor s psihoterapevtom, odvetnikom ipd).	16,9	10	0,00	0,18

Vrednost hi-kvadrata in posledično Cramerjevega koeficienta kaže na šibko povezanost spremenljivk, vendar je statistično pomembna. Ženske manj tvegajo, ko gre za komuniciranje o osebnih zadevah (χ^2 = 19,9, sig. = ,000).

[26] Zakon o elektronskih komunikacijah (Uradni list RS, št. 109/12, 110/13 in 40/14 – ZIN-B).

3.8. Poznavanje organov varstva osebnih podatkov

V zadnjem sklopu (vzorec = n_1) smo anketirance ob navedbi različnih pristojnosti spraševali po poznavanju dela državnega organa za varstvo osebnih podatkov. Zgolj 39,5 odstotka anketirancev je vedelo, da se na Informacijskega pooblaščenca RS (IP) lahko obrnejo v zvezi s pravico do seznanitve z lastnimi osebnimi podatki, ki jih različni subjekti zbirajo o posameznikih, in 41,6 odstotka, da se nanj lahko obrnejo v primeru, ko fakulteta ali delodajalec posameznikov ne obvesti o videonadzoru prostorov. Kar 68,6 odstotka jih ni vedelo, da to lahko storijo tudi v primeru, ko potencialni delodajalec na razgovoru za službo zahteva podatke o otrocih.

Večja ozaveščenost se je pokazala pri možnosti, da se obrnejo na IP v primeru zlorabe osebnih podatkov za namene neposrednega trženja, ko jim pošiljajo neželena elektronska sporočila, kjer je to možnost poznala slaba polovica vprašanih (45,3 odstotka), ter pri možnosti »suma nezakonitega snemanja telefonskih pogovorov«, kjer je skoraj dve tretjini (59,7 odstotka) anketirancev odgovorilo pritrdilno.

Tabela 10: Poznavanje Informacijskega pooblaščenca RS – razlike med spoloma

	hi-kvadrat	d. f.	P (H0)	Cramerjev koeficient
Ali veste, da se lahko na Informacijskega pooblaščenca (državni organ za varstvo osebnih podatkov) obrnete... [s pritožbo v zvezi s pravico do seznanitve z lastnimi osebnimi podatki, ki jih npr. zavarovalnica ali trgovsko podjetje zbira o vas?]	9,9	1	0,00	0,14
Ali veste, da se lahko na Informacijskega pooblaščenca (državni organ za varstvo osebnih podatkov) obrnete... [v primeru, da vas fakulteta ali delodajalec ni obvestil o video nadzoru prostorov?]	6,9		0,01	0,11
Ali veste, da se lahko na Informacijskega pooblaščenca (državni organ za varstvo osebnih podatkov) obrnete... [v primeru zlorabe osebnih podatkov za namene neposrednega kršenja, ko vam pošiljajo neželena elektronska sporočila?	5,2	1	0,02	0,10

Ali veste, da se lahko na Informacijskega pooblaščenca (državni organ za varstvo osebnih podatkov) obrnete... [v primeru suma nezakonitega snemanja telefonskih razgovorov?]	0,7	1	0,41	0,04
Ali veste, da se lahko na Informacijskega pooblaščenca (državni organ za varstvo osebnih podatkov) obrnete... [če od vas na razgovoru za službo potencialni delodajalec zahteva podatke o otrokih?]	0,8	1	0,37	0,04

Med prvimi tremi spremenljivkami te kategorije in spolom je statistično značilna povezanost, vrednosti hi-kvadrata in Cramerjevega koeficienta so majhne. Ženske so manj kot moški seznanjene z možnostjo, da se lahko obrnejo na Informacijskega pooblaščenca.

4. Sklep

Rezultati spletne ankete se nanašajo na odnos do zasebnosti predvsem na področju uporabe spleta in telekomunikacij. Četudi smo anketirance soočili z drugimi morebitnimi obdelovalci in upravljavci osebnih podatkov, so tudi tu odgovori pokazali, da vprašani problem varstva osebnih podatkov zaznavajo predvsem v prej omenjenih domenah. Splet je postal sestavni del našega življenja in težko bi našli del človekovega vsakodnevnega udejstvovanja, ki se v takšni ali drugačni obliki ne manifestira tudi v digitalni obliki, povezani v splet. Prav zato tako velik delež anketirancev skrbi varnost osebnih podatkov »na internetu«, saj je ta področje, ki nam ne omogoča (tolikšne) varnosti kot nedigitalno okolje, kjer je naša možnost varovanja osebnih podatkov vsaj na videz večja (npr. pri plačevanju z gotovino imamo večji nadzor kot pri Bitcoinovi »digitalni denarnici«).

Zato ni presenetljiv cinizem anketirancev, ki v precej velikem deležu (ena četrtina) verjamejo, da nad podatki, ki jih razkrijejo v spletnih socialnih omrežjih, nimajo nobenega nadzora, čeprav so pri vprašanjih o samozaščiti izkazali dovolj visoko raven varovanja podatkov. Kot kaže, so prepričani, da so ukrepi, ki jih imajo na voljo (npr. uporaba nastavitev zasebnosti, ohranjanje zaupnosti gesla za dostop, previdna komunikacija zgolj z znanimi osebami), šibki in jih je mogoče obiti.

Podobno kontradiktoren (morda ciničen) odnos lahko prepoznamo v rezultatih, ki prikazujejo relativno visok delež ljudi, ki bi oddali svoje osebne podatke

v zameno za neko korist. Lakota trgovskih verig po osebnih podatkih deluje ne zgolj zaradi naivnosti potrošnikov – ti se pogosto zelo dobro zavedajo, da jih je mogoče profilirati, segmentirati ipd. –, temveč preprosto zaradi apatije in resignacije. Tako kot uporabniki spleta, ki ne verjamejo, da so njihovi podatki še kje dejansko varovani. Zato je v tem »podatkovnem divjem zahodu« (Steinhardt)[27] vseeno, če podatke ponudijo kar sami in morebiti s tem še kaj neposredno pridobijo.

Nezaupanje do dobičkonosnih gospodarskih organizacij je prav tako jasno razvidno pri vprašanju, kdo najbolj ogroža zasebnost. Dobra polovica vprašanih meni, da so to spletni velikani (Google, Facebook). V času krize je negativni odnos do internetnih podjetij, ki dobesedno »požirajo« uporabnike, močno narasel. Ni presenetljivo, da smo takšen odnos zaznali tudi v anketi, saj so naslednji potencialni kršitelji pravic zasebnosti operaterji telekomunikacijskih storitev in trgovine s programi zvestobe. Vprašani tako menijo tudi, da je poglavitni namen zbiranja in obdelovanja (ter posledično ogrožanja) osebnih podatkov kovanje dobička oz. koristi, ki niso njihove.

Zanimivo je tudi stališče vprašanih, ki so bili seznanjeni z retencijsko podatkovno zbirko, ki jo morajo hraniti operaterji javnih telekomunikacijskih storitev. Kar 83 odstotkov anketiranih zaradi tega ne znižuje količine uporabe telefonskih ali internetnih komunikacij in 92 odstotkov jih ne verjame, da drugi zaradi tovrstnega zbiranja v manjši količini komunicirajo z njimi. Tu se pojavi vprašanje, kaj bi sploh bilo potrebno, da bi ljudi v resnici odvrnilo od uporabe teh načinov komuniciranja.

Raziskovanje na tem področju bi bilo smiselno ponoviti, saj smo večino anketiranja izvedli pred razkritji Edwarda Snowdna in nedavno sodbo Sodišča EU (C-293/12 in C-594/12), ki je obsodila pavšalno in dolgotrajno hrambo prometnih in lokacijskih podatkov v javnih telekomunikacijskih omrežjih.

Vplive razkritij Edwarda Snowdna nam je uspelo preveriti pri vprašanju, kako javnost dojema grožnje s strani domačih in tujih obveščevalnih služb. Rezultati kažejo, da se je stopnja občutka ogroženosti, ki so jo navedli anketirani, prav zares dvignila po juniju 2013, in to lahko po našem mnenju precej zanesljivo pripišemo prav omenjenim razkritjem, ki so izrazito dvignila ozaveščenost in zavedanje ljudi, da so te službe v naših življenjih še kako prisotne, ter razkrila njihove dejavnosti, ki vzbujajo množična neprijetna občutja, jezo, strah in poglabljajo nezaupanje kot temeljni odnos našega časa do sveta.

[27] Nocera, The Wild West of Privacy, URL: http://www.nytimes.com/2014/02/25/opinion/nocera-the-wild-west-of-privacy.html?_r=0.

Navadni uporabniki smo torej »talci« tako tradicionalne kot distribuirane moči,[28] ki vse bolj pustošita tudi po digitalnem okolju. Nimamo niti znanja niti sredstev, da bi se izognili bodisi hitri bodisi veliki moči obeh centrov moči.[29] Težko se izognemo vohunjenju obveščevalnih služb, hkrati si v boju med korporacijami težko pridobimo nadzor nad podatki, ki jih te korporacije imajo o nas samih. Težko se tudi izognemo prevaram kriminalnih skupin, ki so hitro prilagodljive z uporabo informacijske tehnologije. Živimo torej v »internetnem fevdalizmu«:[30] fevdalci so googli, appli, amazoni itn., ki jih lahko svobodno izberemo, ponujajo nam neke ugodnosti in zaščito, mi pa jim plačujemo za varstvo neposredno ali (bolj pogosto) posredno s svojimi osebnimi podatki, ki so za fevdalca plačilna valuta.

»Zasebnost« je zato označevalec, ki, kot vidimo, s časom spreminja vsebino, pravo pa to vsebino bolj ali manj zapoznelo in trajno konceptualizira v pravne pojme, kot kaže še do pred kratkim nepredstavljiv primer »zasebnosti na javnem mestu«. Vsak dan vstopamo v družbene odnose, ki po definiciji pomenijo obliko nadzora. Ali kot je to misel izrazil profesor Lyon:[31] nadzor je relacijski koncept, ki vključuje dinamiko moči in ima Janusov obraz skrbi in nadzora. Podobno misel je izrazil že slovenski kriminolog Pečar, ki je nadzor razumel v podobnem dvojnem smislu in menil, da se nadzor pojavi povsod, kjer se srečata dva posameznika.[32]

Današnji posegi so takšni, da še sami v veliki večini nismo zmožni refleksije in temeljitega razmisleka o dejstvu, da svet poganja prav obdelovanje ogromnih količin osebnih podatkov. V prihodnosti bi bilo zanimivo raziskati, kolikšen je naš lastni prispevek k takšnemu razvoju dogodkov, koliko smo ga sposobni zaznati, kritično ovrednotiti in se pripravljeni kritično upreti lakoti po naših osebnih podatkih.

---

28 Schneier, The battle for power on the internet, URL: https://www.schneier.com/essays/archives/2013/10/the_battle_for_power.html

29 Prav tam.

30 O tem že pred izbruhom afere *Datagate*: Schneier, When It Comes to Security, We're Back to Feudalism, URL: https://www.schneier.com/essays/archives/2012/11/when_it_comes_to_sec.html. Pozneje bolj podrobno Schneier, Power in the Age of the Feudal Internet, URL: http://en.collaboratory.de/w/Power_in_the_Age_of_the_Feudal_Internet.

31 Lyon, Surveillance society: monitoring everyday life (2001).

32 Pečar, Neformalno nadzorstvo: kriminološki in sociološki pogledi (1991).

Literatura

Andreas, Peter; Price, Richard: From War Fighting to Crime Fighting: Transforming the American National Security State, v: International Studies Review, 3 (2001) 3, str. 31–52.

Ball, Kirstie; Snider, Laureen: The surveillance-industrial complex: a political economy of surveillance, Routledge, New York 2013.

Bayley, David; Shearing, Clifford: The new structure of policing: description, conceptualisation and research agenda, National Institute of Justice, Washington 2001.

Bellovin, Steven; Hutchins, Renee; Jebara, Tony; Zimmeck, Sebastian: When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning, v: NYU Journal of Law & Liberty, 8 (2014), str. 623.

Bigo, Didier: Les nouveaux enjeux de l'(in)sécurité en europe: terrorisme, guerrre, sécurité intérieure, sécurité extérieur, L'Harmattan, Pariz 2002.

Boer, Monica den; Janssens, Jelle; Vander Beken, Tom; Easton, Marleen; Moelker, René: Epilogue, Concluding Notes on the Convergence Between Military and Police Roles, v: Blurring military and police roles (ur. M. Easton, M. den Boer, J. Janssens, R. Moelker, T. Vander Beken), Eleven International Publishing, Haag 2010, str. 223–228.

Brvar, Bogomil: Statistika, Fakulteta za varnostne vede, Ljubljana 2007.

European Digital Rights: Shadow Evaluation Report on the Data Retention Directive (2006/24/EC), URL: http://www.edri.org/files/shadow_drd_report_110417.pdf (15. april 2014).

Greenwald, Glenn: NSA Collecting Phone Records of Millions of Verizon Customers Daily, v: The Guardian, 6. junij 2013.

Kerr, Orin: The Mosaic Theory of the Fourth Amendment, v: Michigan Law Review, 111 (2012), str. 311–354.

Gagnon, Benoît: Cyberwars and cybercrime, v: Technocrime: technology, crime and social control (ur. S. Leman-Langlois), Willan Publishing, Oregon 2008, str. 46–65.

Loader, Ian: Policing, Securitization and Democratization in Europe, v: Criminal Justice, 2 (2002) 2, str. 125–153.

Lyon, David: Surveillance society: monitoring everyday life, Open University Press, Philadelphia 2001.

Nissenbaum, Helen: Privacy as Contextual Integrity, v: Washington Law Review, 79 (2004) 1, str. 119-158.

Nissenbaum, Helen: Protecting Privacy in an Information Age: The Problem with Privacy in Public, v: Law and Philosophy, 17 (1998), str. 559-596.

Nocera, Joe: The Wild West of Privacy, URL: http://www.nytimes.com/2014/02/25/opinion/nocera-the-wild-west-of-privacy.html_r=0 (16. maj 2014).

Pečar, Janez: Neformalno nadzorstvo: kriminološki in sociološki pogledi, Didakta, Radovljica 1991.

Sanchez, Julian: GPS Tracking and a 'Mosaic Theory' of Government Searches, URL: http://www.cato.org/blog/gps-tracking-mosaic-theory-government-searches (14. marec 2014).

Schenier, Bruce: MYSTIC: The NSA's Telephone Call Collection Program, URL: https://www.schneier.com/blog/archives/2014/03/mystic_the_nsas.html (20. marec 2014).

Schenier, Bruce: The Battle for Power on the Internet, URL: https://www.schneier.com/essays/archives/2013/10/the_battle_for_power.html (5. januar 2014).

Schneier, Bruce: Liars and outliers: enabling the trust society needs to survive, John Wiley & Sons, Indianapolis 2012.

Schneier, Bruce: Power in the Age of the Feudal Internet, URL: http://en.collaboratory.de/w/Power_in_the_Age_of_the_Feudal_Internet (20. april 2014).

Schneier, Bruce: When It Comes to Security, We're Back to Feudalism, URL: https://www.schneier.com/essays/archives/2012/11/when_it_comes_to_sec.html (24. marec 2014).

Solove, Daniel: »I've Got Nothing to Hide« and Other Misunderstandings of Privacy, v: San Diego Law Review, 44 (2007), str. 745.

Zimmer, Michael: Surveillance, Privacy and the Ethics of Vehicle Safety Communication Technologies, v: Ethics and Information Technology, 7 (2005) 4, str. 201–210.

Zittrain, Jonathan: The future of the internet – and how to stop it, Yale University Press, New Haven 2008.

Privacy After Snowden: Theoretical Developments and Public Opinion Perceptions of Privacy in Slovenia

Summary

Edward Snowden's revelations of massive espionage of intelligences services from June 2013 exposed new dimensions of contemporary surveillance. The deepening of the digital economy created a vast amount of personal data. Additionally, the existing internet model is built on surveillance. States thus want to access personal data for law enforcement and intelligence purposes, while internet and telecommunications companies that generate data want to maximize their profits with data processing and analysis according to the new slogan "Data is a new fuel". The debate about which entity is a greater threat to fundamental liberties, particularly the right to privacy, became obsolete. The real danger lies in governments and private companies that are forming new alliances, thereby creating the "surveillance-industrial complex".

Contemporary surveillance in digital societies is best understood by distinguishing centres of power that are using new technologies. According to Schneier (2013), governments and corporations are traditional powers, while distributed power occurs in two forms: either in the "negative" power of criminal groups, or the "positive" power of, for instance, dissident groups. Today, the traditional power of governments and corporations is growing exponentially. The development of online social networks, cloud computing services, and the design of devices controlled remotely by manufacturers, along with the general deepening of the digital economy, all strengthen the power of companies. Furthermore, governments want to access data collected by these companies. They want to strengthen their models of governance with data analytics and algorithms (e.g. Big Data) and use new stockpiles of data in various domains such as policing, where predictive policing aims to determine the location of future crime based on existing crime records.

Distributed power is the power of groups that operate rapidly but are weaker than traditional powers. So, while traditional powers, i.e. governments and corporations, are slow to adapt, they are stronger when they catch up. For instance, the police needed time to adapt to online crime, but became rather strong over time with digital forensic tools and other digital means to combat crime (e.g. with IMSI-catchers).

We, the ordinary users, find ourselves caught between these centres of power. We have neither the knowledge nor means to resist the rapid force of distributive powers, nor to withstand the immense power of governments and corpora-

tions. We have some mechanisms at our disposal such as data protection law and access to public information legislation, and we can stress the importance of transparency in the functioning of governments and corporations, exercising vigilance while disposing of our personal information. The following article attempts to contribute to these ends by (1) analyzing theoretical developments of conceptions of privacy in the digital age, and by (2) presenting the results of an online survey assessing the Slovenian public's view of various aspects of privacy.

The theoretical part of the article deals with recent theories of privacy that give meaning to the concept of privacy in places where reasonable expectations of privacy would not have existed prior to the development of new technologies: Helen Nissenbaum's theory on the contextual integrity of privacy (1998, 2004), and the theory of pluralistic understanding of privacy by Daniel Solove (2007).

The theory of the contextual integrity of privacy is based on the assumption that personal data is always linked to a certain social context, and that in any such context there are specific norms of that determine the appropriateness of the disclosure of personal data and the norms of personal data flow. New technologies such as Vehicle-Safety Technology (VSC) and video surveillance of public spaces disrupt the contextual integrity of personal data, either because they violate the norms of appropriateness, or the norms of distribution. For example, VSC technology (Zimmer, 2005) that allows vehicles to communicate with each other and with transportation infrastructure enables vehicle tracking, which creates digital databases on one's whereabouts, paths, and time spent at specific destinations. This clearly exceeds the notion of reasonable expectations of privacy in public space as the technology collects more than visual and non-specific information about our travel.

The theory of the pluralistic understanding of privacy defines privacy as an umbrella term for problems that are similar. For a better understanding of privacy, Solove claims, it is necessary to depart from the settled methodology, which seeks a common element for all problems related to privacy. Privacy should be understood as a set of family resemblances. Some concepts do not have "one thing in common" but "are related to one another in many different ways" (Solove, *ibidem*). Instead, the manifold types of problems and harms, which constitute privacy violations in contexts such as data collection and processing, must be mapped out. Solove convincingly claims that privacy is a set of protections against a related set of problems. Privacy is itself a form of social control.

The empirical component of the article presents the results of an online survey conducted in 2012, 2013 and 2014. The online survey consisted of 31 closed questions (interval questions, questions with one possible choice, tabular questions with multiple choice options, grading tables) and consisted of four parts:

(1) cyber victimization, (2) self-reported study on violations of the privacy of third parties, (3) protection of personal data, and (4) perspectives on certain surveillance technologies in road transport and on the internet. Data analysis was performed using SPSS 15. The results are shown in two-dimensional frequency (contingency) tables; for the calculation of links between the variables Pearson's chi-square test, likelihood ratio, Cramer's coefficient and ordinal logistic regression were used.

In the chapter on victimization-related privacy violations, we observed that among the various risks associated with the use of the internet, 66 percent of those surveyed perceived the risk of interception of their communications content as problematic. When asked whether the respondents were subjects of different privacy victimizations in the past, 9 percent responded that they have been victims of theft of personal data on the internet and 23 percent of respondents were victimized by a third party's publishing of discrediting photographs. When asked about their familiarity with various web-based threats, spyware programs were well known by 35 percent of respondents. The respondents' self-protective preventive behaviour is an integral part of a comprehensive privacy protection, so we asked respondents about the ways they protect their computers. The vast majority regularly update their operating systems and computer programs and use anti-virus programs.

Furthermore, we were curious about post-violation self-protective behaviour, and asked respondents to whom they would turn in various scenarios of online threats and violations. In the case of personal data abuse, the respondents expressed greater confidence in the public police than in other instances of misconduct. In the chapter on self-reported privacy violations, we asked the respondents whether they have ever acted in a way that threatened the privacy of third parties or attempted to execute surveillance of others. Collecting information about others from publicly available databases is a common task and only 28 per cent of respondents have never "Googled" other people. On the contrary, the use or manufacture of malicious code is very rare. About one tenth of respondents performed delinquent actions in online social networks. The leading violation of third party's privacy is publishing photographs of others without their consent.

In the chapter on concern over personal data safety the respondents were asked to what extent they worry about the security of their personal data. We used Cramer's coefficient and chi-square methods to compare results between genders. Women are slightly more concerned when it comes to personal data safety, especially while using mobile phones or the internet. Additional time was spent assessing the level of concern about privacy on the internet: what is the

perception of personal data control while being part of social networks, online shopping, what are the common privacy settings of users in social networks, with whom do they communicate online, and with whom they share their social network account passwords.

In the chapter on the perception of primary subjects of surveillance, 56 percent of respondents chose internet corporations as the greatest threat to their privacy, followed by telecommunications companies (25 percent), and shops with loyalty programs (23 percent). According to chi-square and Cramer's coefficient calculations, gender correlation is weak. Men feel slightly more threatened by foreign intelligence services and the Slovene Intelligence and Security Agency (SOVA). By using ordinal logistic regression, we found that male respondents answered this question 0.34 times more often with lower grades (foreign intelligence service) and 0.38 times more often with lower grades when answering "Slovene Intelligence and Security Agency".

By comparing responses before and after the Datagate affair, we noted that prior to this date, only a handful of people felt threatened by foreign or domestic intelligence agencies. This is illustrated by a comparative calculation of the mean (arithmetic mean) and standard deviations. An increased feeling of threat after this date is evident in men as well as women.

In the chapter about evaluating privacy we wished to learn to what extent the participants are willing to relinquish their privacy in exchange for certain benefits. Most of the respondents are ready to forego privacy for at least a 10 percent discount when purchasing airline tickets (52 percent) or the same discount when shopping online (42 percent). The gender difference calculations using Cramer's coefficient and chi-square indicate statistical significance in answers "Information about products, news" and the option to acquire free e-books. Evaluation of privacy and surveillance in road traffic shows that 58 percent of respondents opted for fixed speed cameras on all sections of the road that are proven to be deadly in the last ten years. The least popular method proved to be traffic light cameras, which record red light violators.

In the chapter on the attitude towards data retention in public telecommunication networks, we found out that 53 percent of respondents did not know the obligation of telecommunications service providers to retain all traffic and location data of telephone and internet communications under the Electronic Communications Act (ZEKom-1). We were quite surprised by the response of those who were familiar with this obligation. Despite these provisions, they would not decrease their use of the Internet and telephone communications (83 percent). According to chi-square and Cramer's coefficient calculations, gender

correlation is weak, but statistically significant: women tend to risk less when it comes to communicating personal matters.

In the chapter on knowledge of data protection authorities, we found that only 39.5 percent of respondents knew that the Information Commissioner of RS is the proper address for protecting the right to be notified of the collection of one's personal data. Less than half of the participants, 41.6 percent, knew that the Information Commissioner of RS is able to intervene if their faculty or employer would not inform the public about video surveillance of its premises. Awareness of the Information Commissioner of RS's competence only increased when respondents were presented with the option of a possible abuse of personal data for direct marketing purposes and possible illegal recording of telephone conversations. Cramer's coefficient and chi-square calculations about gender differences indicated that women are less familiar with these rights than men.

To conclude, privacy is a notion that changes over time, while the law conceptualizes its content and translates it in a more or less rigid legal concept. Due to the extreme proliferation of new information technologies, the current notion of privacy needs new understanding as Nissenbaum and Solove have shown and suggested. An empirical study on the view of the Slovenian public about privacy reveals various perspectives and awareness of privacy and behaviours related to its violation and protection in various forms. In general, the public opinion survey shows that the knowledge of particular dilemmas associated with privacy is relatively common (e.g. acquaintance with the Information Commissioner of RS seems low at first sight, but promising when compared to other EU Member States). However, the behaviour of the respondents remains relatively unchanged and apathetic or even fatalistic (e.g. respondents, while being aware of the telecommunications companies' obligation to retain traffic and location data, do not want to change their behaviour).