*Jošt BARTOL, Vasja VEHOVAR, Andraž PETROVČIČ**

SKRB ZA INFORMACIJSKO ZASEBNOST NA INTERNETU: KONCEPTUALNA IZHODIŠČA IN RAZISKOVALNI IZZIVI**[1]

Povzetek. *Informacijska zasebnost je z razvojem računalnikov in interneta postala eno izmed pomembnih družbenih vprašanj, saj nove tehnologije omogočajo neslutene možnosti zbiranja in analize podatkov. Ker ima to posledice tako za demokratične družbe kot za vedénje posameznikov, se tej temi posvečajo številni raziskovalci iz različnih znanstvenih disciplin. V članku se osredotočimo na posameznikovo informacijsko zasebnost v internetnem okolju iz socialno-psihološkega vidika in predstavimo enega izmed osrednjih pojmov na tem področju, in sicer skrb za informacijsko zasebnost. Opišemo njegov dosedanji razvoj, konceptualna izhodišča in raziskovalne izzive. Na koncu podamo usmeritve za načrtovanje študij na tem raziskovalnem področju.*

Ključni pojmi: *informacijska zasebnost, internet, raziskovalni izzivi, konceptualizacija, skrb za informacijsko zasebnost*

Uvod

Zasebnost je nekaj, kar ljudje iščejo v vseh družbah (Westin, 1967). Posamezniku namreč omogoča avtonomijo, razvoj lastne identitete in razvoj razmerij z drugimi (Masur, 2019; Nissenbaum, 2010; Westin, 1967). Pravzaprav je tako pomembna, da je v demokratičnih družbah uzakonjena in da jo lahko razumemo kar kot »areno demokratičnih politik« (Westin, 2003: 433). Z drugimi besedami, odločitve o tem, kaj je zasebno in kaj je

* *Jošt Bartol, asistent, Fakulteta za družbene vede, Univerza v Ljubljani, Slovenija; dr. Vasja Vehovar, redni profesor, Fakulteta za družbene vede, Univerza v Ljubljani, Slovenija; dr. Andraž Petrovčič, docent, Fakulteta za družbene vede, Univerza v Ljubljani, Slovenija.*

** *Pregledni znanstveni članek.*

DOI: 10.51936/tip.58.3.991-1008

[1] *Članek je nastal kot del doktorskega usposabljanja prvega avtorja, ki je vključen v program »Mladi raziskovalci« in raziskovalnih aktivnosti soavtorjev v okviru raziskovalnega programa Internetno raziskovanje (P5-0399) in projekta Posledice posredne uporabe interneta za internetne veščine starejših (J5-2558), ki so (so)financirani s strani Javne agencije za raziskovalno dejavnost Republike Slovenije (ARRS) iz državnega proračuna.*

javno, v demokratičnih družbah določajo pravice in svoboščine subjektov, tako fizičnih kot pravnih. Posameznik je na primer z zakonom zaščiten pred neutemeljenim vdorom policije in drugih oseb v njegov dom.

Zgodovinsko gledano, je osnovna delitev med zasebnim in javnim sicer obstajala že v antični Grčiji (Weintraub, 1997: 29), zakoni, ki so kaznovali prisluškovanje, pa so bili v Angliji v veljavi že od 14. stoletja (Holvast, 2007). Kljub temu pa se pojem zasebnosti, kot ga razumemo danes, v filozofskih in družboslovnih razpravah pojavi relativno pozno, in sicer z obdobjem liberalne filozofije in razsvetljenstva (Kovačič, 2006; Masur, 2019). V slovenščini se denimo izraz »zaseben« pojavi šele v 18. stoletju (Snoj, 2021).

Tako so tudi konkretni zakoni o zasebnosti nastali precej pozno (Shank, 1986). En izmed pomembnejših premikov v to smer se je zgodil proti koncu 19. stoletja, ko sta Warren in Brandeis (1890: 195) zasebnost opredelila kot posameznikovo »pravico, da ga/jo pustijo pri miru«.[2] Takšno opredelitev sta spodbudila takraten razvoj novih tehnologij, predvsem fotoaparata, in razmah poročanja novinarjev, ki so »vdrli v svete prostore zasebnega in domačega življenja« (Warren in Brandeis, 1890: 195). Podobno je nekaj desetletij kasneje razvoj računalnikov, še kasneje pa tudi interneta (Westin, 2003) in mobilnih telefonov (Dwyer, 2020), povzročil strah glede možnih zlorab posameznikovih zasebnih podatkov. V tem času se je uveljavil pojem *informacijske zasebnosti*, ki se pomembno razlikuje od *fizične zasebnosti*. Prva se nanaša na dostop do posameznikovih (osebnih) informacij, druga pa na fizični dostop do posameznika (npr. dostop v dom) (Smith et al., 2011: 990–991). Oba pojma lahko združimo pod terminom *splošna zasebnost*.[3]

Tehnologija pomembno vpliva na razprave o zasebnosti, saj na eni strani preizprašuje ustaljene družbene norme, povezane z njo, na drugi pa povzroča strah pred konsolidacijo moči v rokah že tako dominantnih akterjev (Nissenbaum, 2010). Posledično razvoj tehnologije že vsaj od konca 19. stoletja spodbuja razprave o tem, kaj zasebnost sploh je, kako tehnologije ogrožajo posameznikovo zasebnost, in s tem njegovo avtonomijo in svobodo, ter kako posameznika kot tudi demokracijo ščititi pred tovrstnimi grožnjami (Nissenbaum, 2010; Westin, 1967; Westin, 2003). Ker je zasebnost vsebinsko zelo širok pojem, se z zasebnostjo ukvarjajo številni raziskovalci z različnih področij (Smith et al., 2011). Ta vsebinska širina pa je hkrati razlog za enega izmed ključnih izzivov pri raziskovanju zasebnosti, in sicer da ni mogoče podati enotne opredelitve tega pojma (DeCew, 1997; Nissenbaum, 2010).

Pregledu pristopov k opredelitvam zasebnosti se bomo podrobneje posvetili v prvem poglavju, tu pa velja poudariti, da nas v tem članku zanima

[2] *V originalu se zapis glasi »the right to be let alone«.*

[3] *V nadaljevanju uporabljamo termin zasebnost za poimenovanje splošne zasebnosti, ostali dve vrsti pa poimenujemo dosledno s polnim imenom.*

posameznikova informacijska zasebnost v internetnem okolju predvsem s *socialno-psihološkega vidika* (Masur, 2019). Tako se bomo osredinili na subjektivne ocene posameznikov glede možne izgube lastne informacijske zasebnosti. Razumevanje tovrstnih pomislekov je izredno pomembno, saj lahko namreč posameznike odvrnejo od uporabe določenih spletnih storitev (Dinev in Hart, 2006), kar pa ima lahko v današnjem svetu vse večje digitalizacije tudi stvarne posledice. Denimo, posamezniki lahko ostanejo brez dostopa do e-zdravstvenih storitev (Anderson in Agarwal, 2011) ali izgubijo socialni kapital (Ellison et al., 2011; Page et al., 2018).

Znotraj tega raziskovalnega polja je izredno pomemben teoretični pojem *skrb za informacijsko zasebnost* (SIZ) (Li, 2011; Smith et al., 2011). Četudi je v literaturi mogoče zaslediti več zelo različnih opredelitev tega pojma (Rohunen, 2019), lahko SIZ v splošnem razumemo kot poglede posameznikov (ali skupin) o morebitni izgubi informacijske zasebnosti ob posredovanju podatkov poznani ali nepoznani entiteti (Bartol et al., 2021: 1). Zanimivo je, da med študijami prihaja do nesoglasij oziroma razlik v rezultatih. Nekatere študije kažejo, da SIZ pomembno vpliva na vedénje oziroma vedenjsko namero, druge pa, da med obema ni povezanosti in da obstaja tako imenovani *paradoks zasebnosti*, pri čemer posamezniki izražajo zaskrbljenost glede zlorabe svojih podatkov, a jih kljub temu neobremenjeno posredujejo drugim (Norberg et al., 2007). Rohunen et al. (2020) so kot glavni razlog za razlike med študijami prepoznali uporabo različnih teorij in konceptualnih modelov, kjer so sicer enako poimenovani pojmi različno opredeljeni in merjeni. To lahko posledično vodi do nasprotujočih si ugotovitev. Tudi Gerber et al. (2018) ugotavljajo, da obstaja nejasna delitev med različnimi pojmi, ki so povezani z informacijsko zasebnostjo na internetu, kar se odraža tudi v ne dovolj jasnih in točnih opredelitvah pojma SIZ (Bartol et al., 2021; Li, 2011; Preibusch, 2013).

Z ozirom na predstavljeno ozadje je namen članka dvojen. Najprej predstavimo konceptualna izhodišča in izzive pri opredelitvi pojma zasebnosti in pokažemo, kako se izzivi prenesejo tudi na opredeljevanje in operacionalizacijo pojma SIZ. Nato na tej podlagi predstavimo izvirne usmeritve za načrtovanje študij o SIZ v internetnih okoljih. Izsledki članka tako predstavijo izredno konceptualno razdrobljenost pojma zasebnosti in posledično SIZ, bodočim raziskovalcem pa ponudijo jasne korake, ki ne bodo samo olajšali snovanja študij o SIZ, ampak tudi izboljšali njihovo metodološko kakovost in vsebinski doprinos.

Preden se posvetimo sami vsebini, želimo izpostaviti, da naš cilj ni poiskati »pravilne« konceptualizacije pojma SIZ, temveč predstaviti ključne vidike, ki jih je pri njegovi konceptualizaciji in operacionalizaciji smiselno upoštevati. Enotno razumevanje tako (informacijske) zasebnosti kot SIZ zelo verjetno sploh ni mogoče (Bernal, 2020; DeCew, 1997), saj je njun

pomen močno odvisen tako od značilnosti okolja,[4] v katerem se posameznik nahaja, kot tudi od predpostavk in pristopov raziskovalcev, ki se z njima ukvarjajo. Povedati velja tudi, da se v članku osredotočamo predvsem na razumevanje zasebnosti v liberalnih, demokratičnih družbah. V nasprotju s tem je lahko zasebnost v avtoritarnih družbah razumljena in vrednotena drugače. Čeprav so strukturni vidiki pomembni, pa jih zaradi pomanjkanja prostora tukaj ne naslavljamo.

Tako je preostanek članka razdeljen na tri dele. V prvem delu očrtamo različne pristope, ki so bili uporabljeni za razumevanje in opredelitev zasebnosti. Tu tudi predstavimo pomemben vidik zasebnosti, in sicer kontekstualno specifičnost le-te. Temu sledi predstavitev pojma SIZ, izzivov pri njegovi konceptualizaciji in vpliva teh izzivov pri njegovem empiričnem merjenju. Nato predstavimo usmeritve za snovanje empiričnih študij o SIZ v internetnih okoljih. Članek sklenemo s kratkim povzetkom izzivov in priporočil.

Temeljna izhodišča razumevanja zasebnosti

Mnogoterost opredelitev zasebnosti

Zasebnost in doseganje zasebnosti sta pomembna vidika vseh človeških družb (Westin, 1967: 7–22). Prve jasne delitve na zasebno in javno zasledimo že pri Aristotelu (Weintraub, 1997: 29), ki je ločil med politično skupnostjo in gospodinjstvom. Vendar pa je nujno omeniti, da so antični Grki zasebno (tj. gospodinjstvo) razumeli kot polje prisile, in ne kot polje svobode (Arendt, 1958/1995), zaradi česar je antično razumevanje omenjenih sfer povsem drugačno od razumevanja, ki se je začelo razvijati z razsvetljenstvom in ki ga imamo še danes (Arendt, 1958/1995; Kovačič, 2006).

Iz razsvetljenstva izhajajoče razumevanje se je primarno nanašalo na razdelitev javne in zasebne sfere in je vključevalo omejevanje moči oblasti pred neutemeljenim poseganjem v posameznikovo zasebno življenje (Kovačič, 2006; Masur, 2019). V tem okviru je pravica do zasebnosti odigrala tudi pomembno vlogo pri prehodu v modernost, saj je vse več odločitev (npr. o zaposlitvi, poroki, združevanju) predala v roke posameznika (Baghai, 2012). Kljub številnim razpravam pa še vedno umanjka jasno in enotno razumevanje pojma zasebnosti (DeCew, 1997), kar predstavlja izziv tudi v pravnih postopkih (Nissenbaum, 2010). Nissenbaum (2010: 91–102) predstavi tri delitve na zasebno in javno, in sicer kot delitev glede na vladne (tj. javne) in zasebne akterje, zasebne in javne prostore ter zasebne in javne informacije.

[4] *To vključuje neposredno okolje, kjer se dejanje vrši, in širše strukturne dejavnike, kot so kulturno, socialno, ekonomsko, politično in tehnološko okolje (Masur et al., 2021).*

Vsaka izmed delitev pa ima drugačno razumevanje, kaj je v posameznem primeru zasebno in kaj javno. Denimo, če se na javnem prostoru pogovarjamo o zasebnih zadevah, ali bo nekdo tretji imel pravico poslušati razpravo? Nedavni razvoj informacijskih in komunikacijskih tehnologij je tovrstne nejasnosti samo še poglobil (Nissenbaum, 2010).

V drugi polovici 20. stoletja pa se je začel krepiti socialno-psihološki pristop k razumevanju zasebnosti (Masur, 2019: 47). Pomembna ločnica v tem času je bil razvoj računalnikov, ki je vplival na družbene razprave in razvoj pojma informacijske zasebnosti (Westin, 2003; Masur, 2019). Margulis (1977) za začetnika in utemeljitelja socialno-psihološkega pristopa k zasebnosti postavi Ervinga Goffmana (1959). Slednji sicer ni govoril neposredno o zasebnosti, a so njegove študije o »samopredstavitvi, vedénju na javnih prostorih in stigmatiziranih identitetah« pomembno vplivale na kasnejše pristope k zasebnosti (Masur, 2019: 50). Temu so sledile sistematične študije zasebnosti s socialno-psihološkega vidika in objavljeni sta bili dve še danes zelo pomembni teoriji o zasebnosti, in sicer Westinova (1967) in Altmanova (1975). Westin (1967) je zasebnost razumel kot nekaj, kar se lahko doseže s (prostovoljnim) odmikom od družbe. Denimo, odmik v samoto ali intimnost. Nasprotno pa je Altman (1975) razumel zasebnost kot obliko nadzora nad dostopom do posameznika. Pomembno nadgradnjo Altmanove teorije je nekaj desetletji kasneje predstavila Sandra Petronio (2002), ki je zasebnost eksplicitno povezala z razkrivanjem informacij.

Kot vidimo, ima zasebnost zelo dolgo in bogato zgodovino ter številne pristope k razumevanju. Tako so številni avtorji predstavili tipologijo opredelitev (npr. Allmer, 2011; Minkkinen, 2015; Tavani, 2007), med katerimi pa je najobširnejša kategorizacija Smitha et al. (2011: 994–995). Slednja namreč vključuje tako tako pravne, filozofske, sociološke, ekonomske kot socialno-psihološke pristope. Smith et al. (2011) razlikujejo dva osnovna pristopa k opredelitvam zasebnosti:

1. Prvi pristop razume zasebnost v smislu vrednot oziroma vrednosti. Ta se dalje členi na razumevanje zasebnosti kot *pravice* in na razumevanje informacijske zasebnosti kot *dobrine*. Ta razumevanja so bolj ali manj lastna filozofskim, pravnim, političnim in sociološkim razpravam o zasebnosti, saj razumejo zasebnost kot pravico, ali pa razumejo informacijsko zasebnost (oziroma osebne podatke) kot dobrino, ki ima na »trgu« določeno vrednost in jo lahko prosto menjamo za druge dobrine. To razumevanje se pogosto uporablja v okviru interneta, kjer se govori o tem, da uporabniki interneta ponudnikom spletnih storitev posredujejo svoje podatke kot plačilo za številne ugodnosti (Campbell in Carlson, 2002), s čimer se upraviči zbiranje podatkov. Tovrstno razumevanje se uporablja tudi pri analizi informacijske zasebnosti z vidika komodifikacije (npr. Sevignani, 2013).

2. Drugi pristop pa razume zasebnost v smislu subjektivnih ocen. Vsebuje opredelitve, ki razumejo zasebnost kot *stanje*, in opredelitve, ki razumejo zasebnost kot *nadzor*. Sem spada tudi socialno-psihološki pristop in omenjene teorije Westina (1967), Altmana (1975) in Petronie (2002). Opredelitve znotraj tega pristopa se osredotočajo na posameznikove zaznave, kognicije in mnenja o zasebnosti ter vplive teh zaznav na vedénje. A kljub temu da številni avtorji opredelijo zasebnost kot nadzor ali možnost nadzora nad lastnimi osebnimi podatki ter da je ta opredelitev pogosto uporabljena v empiričnih raziskavah (Smith et al., 2011), pa pravzaprav za ohranjanje zasebnosti nadzor ni ključen pogoj. Kot ugotavljata Laufer in Wolfe (1977), je lahko določena situacija razumljena kot zasebna, čeprav posameznik nad njo nima nadzora. Za ponazoritev vzemimo obisk zdravnika. Kot pacient nad okoljem praktično nimamo nadzora, a kljub temu pričakujemo, da bodo naše informacije ostale zaupne in da bo naša zasebnost ohranjena. Kljub pomislekom, ali je zasebnost oblika nadzora ali ne, pa je smiselno predpostaviti, da je nadzor nad osebnimi informacijami pomemben, čeprav ne ključen, element pri vprašanjih o zasebnosti (Masur, 2019).

Kljub precejšnji heterogenosti pristopov k opredelitvi zasebnosti lahko prepoznamo določene skupne točke. Kot ugotavlja Masur (2019: 67–68), je s socialno-psihološkega stališča razumevanje, kaj je zasebno in kaj ne, sicer družbeno pogojeno, a hkrati še vedno odvisno od vsakega posameznika: njegove osebnosti, znanja, razvojne faze (npr. otrok nasproti odraslemu) in konkretnega konteksta. V vsakem primeru pa gre pri zasebnosti za postavljanje meja oziroma omejevanje dostopa do sebe. Vse to nakazuje, da zasebnost ni statična kategorija in da posamezniki nimajo oziroma ne želijo enake stopnje zasebnosti v razmerju do vseh oseb ali v vseh situacijah oziroma kontekstih (Laufer in Wolfe, 1977).

Kontekstualna specifičnost zasebnosti

Za ponazoritev in utemeljitev pomena kontekstualne specifičnosti zasebnosti v nadaljevanju predstavimo dve teoriji. To sta teorija *upravljanja komuniciranja zasebnosti* (angl. communication privacy management theory), ki jo je razvila Sandra Petronio (2002), in teorija *kontekstualne integritete* (angl. theory of contextual integrity), ki jo je razvila Helen Nissenbaum (2010).

Teorija upravljanja komuniciranja govori o načinu, kako posamezniki upravljajo z razkrivanjem in prikrivanjem informacij o samih sebi. Teorija sloni na metafori *mej* (angl. boundaries), ki »označujejo lastniške črte za posameznikove zasebne podatke« (Petronio, 2002: 6). Tako je zasebnost (avtorica ne izpostavi, ali gre za splošno ali informacijsko zasebnost) v

okviru te teorije razumljena kot »občutek, ki ga nekdo ima o pravici do posedovanja zasebnih informacij, tako individualno kot kolektivno« (Petronio, 2002: 6). Z individualnim posedovanjem je mišljeno, da določene informacije pozna samo ena oseba. Kolektivno posedovanje pa predpostavlja, da je poznavanje teh informacij deljeno, a ne nujno vzajemno. Družina na primer lahko kolektivno poseduje informacije o bolezni nekega člana. Taka družina nato vzpostavi pravila, ki določajo v kolikšni meri in na kakšen način lahko družinski člani, ki posedujejo omenjene informacije, te informacije delijo z drugimi, ki niso člani družine in ne posedujejo teh informacij. S postavljanjem »lastniških mej« nad informacijami in uporabo pravil o njihovem razkritju se družina izogne nevarnostim, ki bi jih njihovo morebitno razkritje neprimernim osebam lahko prineslo. A ker razkritje informacij prinese tudi določene koristi (npr. družina z razkritjem bolezenskega stanja zdravniku pridobi zdravila), jedro te teorije temelji na spoznanju, da je zasebnost neločljivo povezana z izražanjem oziroma posredovanjem informacij, saj želijo posamezniki enkrat prikriti, drugič pa razkriti informacije, ker v različnih situacijah pričakujejo različne posledice (enkrat pozitivne drugič negativne). Tako je namen teorije opisati »logiko, ki jo ljudje uporabljajo, pri odločanju o lastnih zasebnih informacijah« (Petronio, 2002: 33). En izmed ključnih vidikov te teorije so pravila, ki jih posamezniki uporabljajo za določanje in upravljaje z mejami. Pravila namreč določajo, kaj je lahko deljeno in kaj ne in pod katerimi pogoji. Vsekakor različni posamezniki razvijejo različna pravila. Petronio (2002: 38–71) predstavi pet ključnih meril, ki vplivajo na oblikovanje pravil. To so kulturni kriteriji (npr. kulturne norme o zasebnosti), kriteriji, povezani s spolom (predpostavlja se, da ženske in moški postavljajo drugačna pravila z ozirom na zasebnost), motivacija (nekateri posamezniki imajo večjo težnjo po deljenju informacij), kontekst situacije[5] (npr. ob katerih priložnostih je primerno govoriti o določeni stvari), prav tako pa je pri oblikovanju pravil pomembno razmerje med koristmi in tveganjem, ki sta povezana z (morebitnim) razkritjem določenih informacij. Na podlagi te teorije vidimo, da so posameznikove odločitve glede posredovanja svojih zasebnih informacij kompleksne in odvisne od številnih dejavnikov.

Podobno tudi teorija kontekstualne integritete (Nissenbaum, 2010) informacijsko zasebnost razume kot odvisno od okolja in v povezavi z drugimi osebami. Znotraj te teorije je informacijska zasebnost razumljena v okviru informacijskih tokov in je dosežena le v primeru, ko prenos informacij poteka na primeren način. Kaj je primeren način, določajo informacijske norme. Gre za pravila in pričakovanja o prenosu informacij (Nissenbaum, 2010: 141), ki so opredeljena s štirimi parametri: (i) s kontekstom, torej

[5] *Petronio (2002: 25) kontekst situacije razume kot kombinacijo fizičnega in družbenega okolja. Za podrobnejšo analizo o pomenu situacije pri vprašanjih o zasebnosti glej Masur (2019).*

okoljem z vnaprej določenimi vlogami, normami, aktivnostmi in cilji; (ii) z akterji, ki vključujejo pošiljatelja informacij, prejemnika informacij in podatkovnega subjekta (tj. subjekt, na katerega se informacije nanašajo); (iii) z vrsto informacij; (iv) s prenosnim principom, ki igra vlogo zaviralca prenosa informacij, saj izraža pogoje, pod katerimi se prenos lahko oziroma ne sme zgoditi (Nissenbaum, 2010: 145). Teorija trdi, da lahko sprememba enega samega parametra (npr. vrste informacij) povzroči kršitev ustaljenih informacijskih norm, kar lahko posledično ogrozi posameznikovo informacijsko zasebnost. To bomo v nadaljevanju ponazorili s primerom.

Denimo, da se posameznik z zdravnikom dogovori za srečanje v ambulanti. Tedaj so vloge jasne (zdravnik in pacient), jasen je tudi način obnašanja (formalen, spoštljiv), kakšne aktivnosti potekajo (npr. postavitev diagnoze) in kaj so cilji (pomoč pacientu). Opravka imamo tudi z le dvema akterjema: zdravnikom v vlogi prejemnika informacij in pacientom, ki je hkrati posredovalec informacij in podatkovni subjekt. Vrsta informacij je precej občutljiva, saj gre za informacije povezane z zdravjem, a pacienta to ne skrbi, ker verjame v zaupnost situacije (torej prenosni princip). Verjetno bi redki pomislili, da takšna situacija predstavlja kršitev ustaljenih informacijskih norm in posledično kršitev informacijske zasebnosti (kršitve so sicer teoretično možne, če bi zdravnik denimo prekršil pravilo zaupnosti). Sedaj si zamislimo enako srečanje prek spleta, le da se sedaj zbirajo še dodatni podatki o srečanju, kot so na primer trajanje, pacientova lokacija ali termin srečanja. Zbiranje dodatnih podatkov – in njihovo morebitno posredovanje tretjim osebam (ki bi bile dodatni prejemnik informacij) – pa krši ustaljene informacijske norme (Nissenbaum, 2010: 150), in s tem predstavlja vdor v informacijsko zasebnost pacienta. Tako vidimo pomen elementov okolja, v katerem se prenos informacij vrši, in njihov vpliv na razumevanje situacije kot zasebne.

Vsi ti vidiki močno otežijo tako teoretska razmišljanja in empirične raziskave o zasebnosti kot tudi primerjave med različnimi študijami. Prepredenost različnih dejavnikov, ki vplivajo na razumevanje zasebnosti pri posameznikih, se lahko odraža tudi v na videz nasprotujočih si ugotovitvah študij. Na internetu se pogosto obravnava omenjeni paradoks zasebnosti, ki pravi, da se posamezniki vedejo v nasprotju z izraženo SIZ (Gerber et al., 2018; Smith et al., 2011). A kot ugotavljajo nekatere študije, do paradoksa pride le v določenih kontekstih, kot so družbena omrežja, ne pa v komercialnih interakcijah, kot je spletno nakupovanje (Lutz in Strathoff, 2014).

Primerjava študij iz različnih kontekstov lahko zanemari in/ali zabriše značilnosti, ki so pomembne v razumevanju informacijske zasebnosti v posameznih kontekstih in njenih posledicah na vedénje (Rohunen et al., 2020). Ravno zaradi tega je potrebno biti v raziskovanju informacijske zasebnosti zelo previden in jasno opredeliti konceptualno podstat informacijske

zasebnosti, okolje, v katerem se zasebnost raziskuje, situacijo, znotraj katere se bo preverjalo hipoteze in podobno. Koristi natančnih opredelitev se ne izrazijo samo pri lažjem uokvirjanju in analizi problema, temveč omogočajo tudi lažjo primerjavo med študijami. S poznavanjem opisanih vidikov in izzivov tematizacije informacijske zasebnosti se v nadaljevanju osredotočimo na izzive raziskovanja SIZ.

Skrb za informacijsko zasebnost

Kljub velikemu pomenu in pogosti uporabi pojma SIZ ne bomo našli njegove enotne opredelitve. To je po svoje razumljivo glede na težave z opredelitvami same zasebnosti kot tudi njene kontekstualne specifičnosti. Tako Rohunen (2019: 66–67) identificira sedem vrst različnih opredelitev SIZ: (i) izguba zasebnosti, (ii) izguba nadzora nad zasebnostjo, (iii) negotovost glede uporabe osebnih podatkov, (iv) pomanjkanje zavedanja o uporabi podatkov, (v) oportunistično vedénje povezano s posredovanimi podatki, (vi) uporaba podatkov, (vii) pravično obdelovanje in uporaba podatkov. Tu bi lahko domnevali, da so razlike v opredelitvah SIZ posledica uporabljenih teorij pri konceptualni zasnovi različnih študij in značilnosti preučevanega konteksta. A Rohunen (2019) ugotavlja, da so različne opredelitve pogosto uporabljene s sklicevanjem na isto teorijo ali pa v istem kontekstu. Težava je v tem, da številne teorije, uporabljene v empiričnem raziskovanju SIZ, niso osredotočene neposredno na zasebnost (npr. teorija racionalnega delovanja [Fishbein in Ajzen, 1975]) ali pa mesto in pomen SIZ v teoriji nista natančno opredeljena (npr. v primeru teorije upravljanja komuniciranja zasebnosti). Podobno velja tudi za neupoštevanje kontekstov, pri čemer se pogosto natančno ne preuči vseh značilnosti določenega tehnološkega okolja (Nissenbaum, 2010: 150; Rohunen, 2019: 67).

Razlog za takšno stanje je verjetno v tem, da »je mamljivo privzeti, da so pogledi na zbiranje in uporabo informacij hitro razumljivi in izmerjeni z lahkoto, [vendar] pa so verjetno stališča in prepričanja kompleksni tako v opredelitvi kot merjenju« (Stewart in Segars, 2002: 36). To kompleksno naravo informacijske zasebnosti smo izpostavili že zgoraj, kjer smo pokazali, kako pomembno je pri razmišljanju o informacijski zasebnosti imeti v mislih tako lastnosti posameznika kot tudi fizične (oziroma tehnične) in socialne značilnosti okolja, v katerem se dejavnosti odvijajo. Jasne in točne opredelitve teoretskih pojmov so prav tako nujne, če želimo z njimi povezane pojave veljavno empirično raziskovati (Ferligoj et al., 1995). Dobra konceptualna opredelitev mora namreč vsebovati zapis konceptualne domene (ta vključuje opis narave teoretskega pojma [ali gre npr. za misel, občutek, percepcijo] in opis entitete [ali se pojem nanaša npr. na posameznika, organizacijo, razmerje ali odnos]), konceptualne teme (značilnosti, ki ga predstavniki

pojma vsebujejo), opis stabilnosti pojma skozi čas in v različnih situacijah, pa tudi jasno razločitev od drugih pojmov in predvidene povezave z njimi (Podsakoff et al., 2016).

Sistematičen pregled literature je pokazal, da pojem SIZ večinoma ni dovolj jasno opredeljen (Bartol et al., 2021). Opredelitvam namreč pogosto umanjka nedvoumna opredelitev konceptualne domene (kakšna je narava SIZ in na katere entitete se nanaša), kar posledično privede do nejasnega razločevanja od drugih (sicer povezanih) pojmov (Gerber et al., 2018), kot tudi v kakšnem razmerju je SIZ do njih (Li, 2011). To ima pomembne posledice za operacionalizacijo SIZ in interpretacijo rezultatov študij (Branch in Rocchi, 2015; Ferligoj et al., 1995; Podsakoff et al., 2016) ter lahko posledično privede do napačnih in/ali neskladnih ugotovitev (Bergman, 1998: 81).

Oglejmo si še posledice netočnih in nejasnih konceptualizacij SIZ na odgovarjajoče empirično raziskovanje. Nekateri avtorji ugotavljajo, da se težave v opredelitvah izražajo v nasprotujočih si rezultatih empiričnih študij (Dienlin in Trepte, 2015; Preibusch, 2013). Težave izhajajo iz dveh vidikov. Prvič, nesoglasja so lahko posledica kontekstualne specifičnosti SIZ. V nekaterih internetnih okoljih – na primer pri posredovanju finančnih (Dinev in Hart, 2006) ali zdravstvenih informacij (Anderson in Agarwal, 2011) – so lahko posamezniki veliko bolj občutljivi in pozorni na možnosti izgube informacijske zasebnosti kot denimo na družbenih omrežjih. Enako pomembne so entitete, med katerimi poteka izmenjava informacij. To nakazujejo tudi empirične raziskave, saj imajo posamezniki drugačno SIZ v odnosu do drugih uporabnikov kot pa v odnosu do ponudnikov storitev (npr. na družbenih omrežjih). Te različne »vrste« SIZ pa prav tako različno vplivajo na vedénje posameznikov (Krasnova et al., 2009).

Tako je SIZ smiselno deliti na vertikalne in horizontalne (Krasnova et al., 2009; Masur, 2019). Prve se nanašajo na SIZ v razmerju do organizacij, podjetij ali vlade. Druge pa so povezane s SIZ v razmerju do drugih posameznikov ali uporabnikov. Tako lahko merjenje SIZ v odnosu do dejanj organizacij in kasnejša analiza, ali SIZ vplivajo na vedenjsko namero deljenja informacij z drugimi uporabniki, privedejo do ugotovitev, da SIZ ni povezana z vedenjem posameznikov. To vsekakor ne drži; je pa smiselno pričakovati, da vertikalna SIZ ne bo pomembno vplivala na uporabnikovo namero deljenja informacij z drugimi uporabniki.

Hkrati obstaja težava z določitvijo narave SIZ. V literaturi namreč ni (še dovolj) jasno opredeljeno, na kaj se skrbi (angl. concerns) v besedni zvezi »skrb za informacijsko zasebnost« dejansko nanašajo. Vprašamo se lahko, ali gre za neke vrste predispozicij ali vrednot, ali gre za prepričanja, stališča, ali za kaj tretjega. Glavna težava v tem primeru je, da so različni pojmi, vezani na ta različna razumevanja, med seboj različno povezani. Če bi denimo sledili teoriji racionalnega delovanja (Fishbein in Ajzen, 1975), potem vemo,

da vrednote (torej vrsta dispozicij) vplivajo na prepričanja, ta posledično vplivajo na stališča in šele stališča vplivajo na vedenjsko namero, slednja pa na dejansko vedénje. Pomembno je izpostaviti, da so stališča v omenjeni teoriji vedno usmerjena na nek objekt in vključujejo čustveno komponento, nasprotno pa prepričanja predstavljajo kognitivno oceno nekega objekta.

Pri empiričnem raziskovanju SIZ navedena razlikovanja praviloma umanjkajo. Tako Smith et al. (2011: 997) pri enačenju percepcije, prepričanj in stališč ne vidijo težav, saj pravijo, da se lahko vse to združi pod enoten pojem SIZ. A natančna določitev narave pojma SIZ – in iz tega izhajajoče povezave z drugimi pojmi – je zelo pomembna. Ta vidik sta empirično prikazala Dienlin in Trepte (2015). Najprej sta poustvarila rezultate študij, ki kažejo, da SIZ v kontekstu družbenih omrežji nima neposrednega vpliva na posameznikovo vedénje. Nato pa sta, z natančnim slednjem teoriji racionalnega delovanja, SIZ opredelila kot prepričanja in pokazala, da ima SIZ nezanemarljiv posreden vpliv na vedenjsko namero in vedénje, in sicer prek stališč o informacijski zasebnosti. Menimo, da so netočne in nejasne opredelitve pojma SIZ glavni razlog za številne težave pri raziskovanju informacijske zasebnosti in SIZ v internetnih okoljih.

Usmeritve za snovanje empiričnih študij o SIZ

Upamo, da smo jasno prikazali konceptualno širino pojma (informacijske) zasebnosti in posledično tudi potrebo po natančnih konceptualnih opredelitvah pojma SIZ. Hkrati je izrednega pomena, da se konceptualna opredelitev ujema s kontekstom, znotraj katerega želimo preučevati SIZ, kot tudi z mestom v miselnem procesu posameznikov. Konceptualna natančnost ne bo pripomogla le k bolj veljavnim empiričnim rezultatom študij, temveč bo olajšala tudi primerjave med njimi.

V nadaljevanju predstavimo izvirne usmeritve, ki jih je smiselno upoštevati pri snovanju empiričnih študij na tem področju. Usmeritve strnemo v tri korake: *določitev spletnega konteksta in njegovih značilnosti, določitev opredelitve SIZ in izbor teorije* ter *izbor merskega inštrumenta za merjenje SIZ*.

Določitev spletnega konteksta in njegovih značilnosti je najpomembnejši korak, saj so kontekstualni dejavniki ključni pri razumevanju situacije kot zasebne ali ne. Če se vrnemo k primeru, ki smo ga podali pri razlagi teorije kontekstualne integritete, je jasno, kako močno lahko zbiranje le nekaj dodatnih informacij in vključitev dodatnega prejemnika informacij vpliva na razumevanje situacije kot zasebne. Zaradi tega smo določitev spletnega konteksta postavili na prvo mesto. Tako tudi predlagamo, da se pri snovanju študij o SIZ na internetu spletne kontekste razume kot sociotehnične sisteme oziroma soodvisne funkcionalne enote, kjer se prepletajo tako tehnični kot družbeni vidiki (Baxter in Sommerville, 2011; Petrič in Atanasova,

2013). S tem lahko prepoznamo osrednje tehnične značilnosti posameznega konteksta, osvetlimo način zbiranja in uporabe podatkov, kot tudi družbene značilnosti konteksta, torej ali prihaja do stika med uporabniki (npr. družbena omrežja, spletni forumi) ali pa tega stika ni (npr. spletno nakupovanje). Značilnosti tako tehničnega kot družbenega sistema namreč pomembno vplivajo na zaznave informacijske zasebnosti (Trepte, 2020).

Za oporo pri analizi konteksta tako ponudimo naslednja vprašanja, na katera bi moral raziskovalec odgovoriti, preden se loti opredelitve SIZ in izbora merskega inštrumenta SIZ:

1. Kdo je posameznik, čigar SIZ nas zanima?
2. Katera vrsta podatkov nas zanima?
3. Kdo zbira ali ima dostop do teh podatkov?
4. Na kakšen način se podatki zbirajo?
5. S kakšnim namenom posameznik deli te podatke?
6. Kakšne so norme[6] pri uporabi ali deljenju teh podatkov?

Ko bomo namreč odgovorili na ta vprašanja, bomo imeli dober pregled nad déležniki, ki sodelujejo pri izmenjavi podatkov, njihovem odnosu in pričakovanji glede ravnanja s podatki. To bo prineslo tudi dobro podlago za naslednji korak, in sicer *določitev opredelitve SIZ in izbor teorije*. Razumeti značilnosti konteksta pred opredelitvijo je pomembno, saj nam lahko šele to pove, kakšna vrsta SIZ nas zanima in kateri vidiki so pomembni. Denimo, če smo ugotovili, da so v kontekst, v katerem preučujemo SIZ, vključeni tako ponudniki storitev kot drugi uporabniki, je smiselno razmišljati o dveh vrstah SIZ, in sicer vertikalnih in horizontalnih.

Ker je konceptualna narava SIZ slabo opredeljena (tj. ni povsem jasno, kako točno razumeti »skrbi«), je smiselno zapisati, na kakšen način razumemo ta pojem (ali gre za prepričanja, občutke, vrednote) in v razmerju do koga ga razumemo. To bo pomagalo pri pojmovni jasnosti, ter hkrati olajšalo umestitev pojma v teoretski model.

Pomembno je razmisliti tudi, ali je v posameznem kontekstu smiselno SIZ razumeti kot večrazsežen pojem. V literaturi se denimo SIZ pojavlja kot pojem, ki lahko vključuje skrb glede zbiranja podatkov, skrb glede nadzora nad zbranimi podatki, skrb glede nedovoljenega dostopa do zbranih podatkov in podobno. Razumeti SIZ na tak način je načeloma zaželeno, saj imajo posamezne razsežnosti v določenih internetnih okoljih večji pomen kot druge (Mwesiumo et al., 2021), hkrati pa različne razsežnosti vodijo do drugačnih čustvenih odzivov in strategij spoprijemanja (Jung in Park, 2018).

Skupaj z opredelitvijo SIZ je smiselno razmišljati tudi o teoriji, ki nam bo najbolje pomagala razumeti in razložiti posameznikove zaznave in vedénje

[6] *Norme razumemo skladno z razumevanjem Nissenbaumove (2010: 137–140), in sicer kot pričakovanja ali predpise o sprejemljivem delovanju v določenem okolju.*

v danem okolju. Pri tem lahko ponovno upoštevamo značilnosti preučevanega konteksta. Če nas na primer zanima pripravljenost za posredovanje informacij v okviru spletnega nakupovanja, potem je morda primerna teorija racionalnega delovanja (Fishbein in Ajzen, 1975), v okviru družbenih omrežij pa je morebiti bolj primerna teorija upravljanja komuniciranja zasebnosti (Petronio, 2002), saj nam pojasni, kako posamezniki skupaj posedujejo določene informacije in kako postavljajo pravila, pod katerimi se informacije lahko ali ne sme deliti. Vsekakor se lahko za izhodišče vzame tudi druge teorije, ki so bile uporabljene v empiričnem raziskovanju SIZ na internetu – za pregled glej Li (2012).

Ko smo jasno opredelili kontekst in poiskali ustrezno opredelitev pojma SIZ, se lahko osredotočimo na tretji korak, in sicer *izbor merskega inštrumenta za merjenje SIZ*. Ker se za merjenje SIZ večinoma uporabljajo *anketni merski inštrumenti* (za preglede glej Bartol et al., 2021; Li, 2011; Preibusch, 2013), bomo naša priporočila osredotočili na ta način merjenja. Pri izbiri anketnega inštrumenta moramo upoštevati določeno opredelitev konstrukta SIZ in značilnosti preučevanega konteksta. Na podlagi tega nam bo namreč jasno, katero vrsto SIZ želimo meriti in katere razsežnosti SIZ so pomembne v posameznem spletnem kontekstu. Pomemben vidik je uporaba inštrumentov, ki merijo ali vertikalne ali horizontalne SIZ. Tu vsekakor predlagamo, da raziskovalci uporabijo inštrument, ki je primeren za njihov raziskovalni cilj. Zanimivo je sicer, da validiranih inštrumentov, ki bi merili horizontalne SIZ, praktično ni (Bartol et al., 2021). V nekaj študijah so bili takšni inštrumenti sicer razviti (Krasnova et al., 2009; Lutz in Ranzini, 2017; Masur, 2019), a večinoma za potrebe dotične študije in brez nadaljnjega testiranja. Poleg vrste SIZ je pomembno izbrati tudi inštrument, ki pokriva razsežnosti, pomembne za posamezen spletni kontekst. Hkrati je smiselno SIZ meriti na isti ravni kot druge konstrukte, vključene v študijo. Če nas zanima pripravljenost za posredovanje zdravstvenih informacij zdravnikom prek interneta, potem moramo meriti SIZ v primeru posredovanja zdravstvenih informacij zdravnikom, in ne nekih splošnih SIZ (Li, 2011). Večja specifičnost inštrumentov namreč omogoča bolj natančne napovedi vedenjskih namer v izbranih kontekstih (DeVellis, 1991/2016).

Tako se lahko zgodi, da zaradi velike specifičnosti pojma SIZ, ki ga morebiti želimo v študiji obravnavati, ne bomo našli inštrumenta, ki bi bil razvit posebno za naš namen. V takih primerih lahko sicer spremenimo enega izmed obstoječih inštrumentov, a pri tem velja biti izjemno previden, saj se lahko hitro spremeni pomen merjenega konstrukta in z njim veljavnost merjenja (Preibusch, 2013). Tedaj je vsekakor smiselno upoštevati splošna priporočila za razvoj anketnih merskih inštrumentov (npr. DeVellis, 1991/2016; MacKenzie et al., 2011), pa tudi priporočila, ki jih Bartol et al. (2021) ponudijo konkretno za SIZ. Vsekakor pa pri razvoju novega ali

prilagoditvi obstoječega inštrumenta predlagamo izvedbo kvalitativnih študij. Tako se lahko preveri, kako ciljna skupina razume vprašalnik, od česa je to razumevanje odvisno in kdaj se morda razlikuje od vnaprej predvidenih načinov razumevanja (DeVellis, 1991/2016). Ta vidik posebej poudarjamo, saj je bil pri razvoju anketnih lestvic SIZ v preteklosti pogosto zapostavljen ali celo izpuščen (Bartol et al., 2021).

Sklep

V članku smo očrtali konceptualna izhodišča zasebnosti in njihove posledice za raziskovanje SIZ v internetnih okoljih s socialno-psihološkega vidika. Najprej smo se osredotočili na predstavitev pristopov k opredelitvam zasebnosti in predstavili njeno kontekstualno specifičnost. Nato smo se osredotočili na pojem SIZ. Ta ima osrednjo vlogo pri raziskovanju informacijske zasebnosti med internetnimi uporabniki. Hkrati smo predstavili, kako se konceptualne in kontekstualne težave, prisotne že pri zasebnosti, prenesejo na razumevanje in opredelitve pojma SIZ in njegovo empirično merjenje. Temu je sledil zapis usmeritev, kako raziskovati SIZ na internetu vsem konceptualnim težavam navkljub.

Avtorji upamo, da smo s pričujočim člankom motivirali slovenske (družboslovne) raziskovalce, da vključijo proučevanje SIZ v svoje raziskovalne projekte. Poudariti velja, da je natančnost pri razumevanju pojma SIZ nadvse pomembna tudi za širši poslovni in družbeni kontekst, saj tehnološki razvoj neprenehoma preizprašuje obstoječe družbene norme o informacijski zasebnosti. Posebej pomembno je razumevanje različnih vidikov informacijske zasebnosti v okviru nastajajočih internetnih rab, kot je uporaba aplikacij za sledenje stikov (vključno z aplikacijo covid-19), e-uprava, delo od doma ali uporaba podpornih tehnologij za samostojno življenje doma, pa tudi tehnologij, kot so pametni zvočniki, internet stvari, samovozeči avtomobili in podobno. Ustrezno razumevanje SIZ predstavlja izzive tudi za uveljavljanje Splošne uredbe o varstvu podatkov (GDPR), posebej v pogledu uporabe podatkov družabnih omrežij, rabe piškotkov ter procesiranja anketnih podatkov in masovnih podatkov. Le z natančnim razumevanjem SIZ lahko raziskovalci in tudi odločevalci pridejo do prepričljivih in utemeljenih spoznanj, na podlagi katerih bo mogoče oblikovati kakovostne politike za ohranjanje informacijske zasebnosti posameznikov in demokratičnosti digitalnih družb.

LITERATURA

Allmer, Thomas (2011): A Critical Contribution to Theoretical Foundations of Privacy Studies. Journal of Information, Communication & Ethics in Society 9 (2): 83–101.

Altman, Irwin (1975): The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding. Monterey: Brooks/Cole.

Anderson, Catherine L. in Ritu Agarwal (2011): The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. Information Systems Research 22 (3): 469–490.

Arendt, Hannah (1958, 1995): Vita Activa. Ljubljana: Krtina.

Baghai, Katayoun (2012): Privacy as a Human Right: A Sociological Theory. Sociology 46 (5): 951–965.

Bartol, Jošt, Vasja Vehovar in Andraž Petrovčič (2021): Should We Be Concerned about How Information Privacy Concerns Are Measured in Online Contexts? A Systematic Review of Survey Scale Development Studies. Informatics 8 (2): 1–22.

Baxter, Gordon in Ian Sommerville (2011): Socio-Technical Systems: From Design Methods to Systems Engineering. Interacting with Computers 23 (1): 4–17.

Bergman, Manfred M. (1998): A Theoretical Note on the Differences Between Attitudes, Opinions, and Values. Swiss Political Science Review 4 (2): 81–93.

Bernal, Paul (2020): What Do We Know and What Should We Do About Internet Privacy? Thousand Oaks, CA: SAGE Publications.

Branch, John in Francesco Rocchi (2015): Concept Development: A Primer. Philosophy of Management 14 (2): 111–133.

Campbell, John E. in Matt Carlson (2002): Panopticon.com: Online Surveillance and the Commodification of Privacy. Journal of Broadcasting & Electronic Media 46 (4): 586–606.

DeCew, Judith W. (1997): In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Ithaca, NY: Cornell University Press.

DeVellis, Robert F. (1991, 2016): Scale Development: Theory and Applications. Četrta izdaja 2016. Thousand Oaks, CA: SAGE Publications.

Dienlin, Tobias in Sabine Trepte (2015): Is the Privacy Paradox a Relic of the Past? An In-Depth Analysis of Privacy Attitudes and Privacy Behaviors. European Journal of Social Psychology 45 (3): 285–297.

Dinev, Tamara in Paul Hart (2006): Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use. e-Service Journal 4 (3): 25–60.

Dwyer, Tim (2020): Privacy From Your Mobile Devices? V: Rich Ling (ur.), Leopoldina Fortunati (ur.), Gerard Goggin (ur.), Sun S. Lim (ur.) in Yuling Li (ur.), The Oxford Handbook of Mobile Communication and Society, 546–62. New York, NY: Oxford University Press.

Ellison, Nicole B., Jessica Vitak, Charles Steinfield, Rebecca Gray in Cliff Lampe (2011): Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment. V: Sabine Trepte (ur.) in Leonard Reinecke (ur.), Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web, 19–32. Berlin, Heidelberg: Springer.

Ferligoj, Anuška, Karmen Leskovšek in Tina Kogovšek (1995): Zanesljivnost in veljavnost. Metodološki zvezki 11. Ljubljana: FDV.

Fishbein, Martin in Icek Ajzen (1975): Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley.
Gerber, Nina, Paul Gerber in Melanie Volkamer (2018): Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. Computers & Security 77: 226–261.
Goffman, Erving (1959): The Presentation of Self in Everyday Life. New York, NJ: Doubleday Anchor Books.
Holvast, Jan (2007): History of Privacy. V: Karl de Leeuw (ur.) in Jan Bergstra (ur.), The History of Information Security: A Comprehensive Handbook, 737–769. Elsevier.
Jung, Yoonhyuk in Jonghwa Park (2018): An Investigation Of Relationships Among Privacy Concerns, Affective Responses, And Coping Behaviors In Location-Based Services. International Journal of Information Management 43: 15–24.
Kovačič, Matej (2006): Nadzor in zasebnost v informacijski družbi. Ljubljana: FDV.
Krasnova, Hanna, Oliver Günther, Sarah Spiekermann in Ksenia Koroleva (2009): Privacy Concerns and Identity in Online Social Networks. Identity in the Information Society 2: 39–63.
Laufer, Robert S. in Maxine Wolfe (1977): Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues 33 (3): 22–42.
Li, Yuan (2011): Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. Communications of the Association for Information Systems 28: 453–96.
Li, Yuan (2012): Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework. Decision Support Systems 54: 471–481.
Lutz, Christoph, in Pepe Strathoff (2014): Privacy Concerns and Online Behavior Not so Paradoxical after All? Viewing the Privacy Paradox Through Different Theoretical Lenses. SSRN Electronic Journal. Dostopno prek https://doi.org/10.2139/ssrn.2425132, 23. 6. 2021.
Lutz, Christoph, in Giulia Ranzini (2017): Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder. Social Media + Society Januar–Marec: 1–12.
MacKenzie, Scott B., Phillip M. Podsakoff in Nathan P. Podsakoff (2011): Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques. MIS Quarterly 35 (2): 293–334.
Margulis, Stephen T. (1977): Conceptions of Privacy: Current Status and Next Steps. Journal of Social Issues 33 (3): 5–21.
Masur, Philipp K. (2019): Situational Privacy and Self-Disclosure: Communication Processes in Online Environments. Cham, Switzerland: Springer International Publishing.
Masur, Philipp K., Dmitry Epstein, Kelly Quinn, Carsten Wilhelm, Lemi Baruh in Christoph Lutz (2021): Comparative Privacy Research Framework. Predstavljeno na 71st Annual ICA Conference »Engaging the essential work of care: communication, connectedness, and social justice« (virtualna konferenca), 27.–31. maj 2021.
Minkkinen, Matti (2015): Futures of Privacy Protection: A Framework for Creating Scenarios of Institutional Change. Futures 73: 48–60.

Mwesiumo, Deodat, Nigel Halpern, Thomas Budd, Pere Suau-Sanchez in Svein Bråthen (2021): An Exploratory And Confirmatory Composite Analysis Of A Scale For Measuring Privacy Concerns. Journal of Business Research 136: 63–75.

Nissenbaum, Helen (2010): Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press.

Norberg, Patricia A., Daniel R. Horne in David A. Horne (2007): The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs 41 (1): 100–26.

Page, Xinru, Pamela Wisniewski, Bart P. Knijnenburg in Moses Namara (2018): Social Media's Have-Nots: An Era of Social Disenfranchisement. Internet Research 28 (5): 1253–74.

Petrič, Gregor in Sara Atanasova (2013): Social Informatics: Developmental Convergences and Research Achievements [Družboslovna informatika: Razvojne konvergence in raziskovalni dosežki]. Teorija in praksa 50 (2): 347–75.

Petronio, Sandra (2002): Boundaries of Privacy: Dialectics of Disclosure. Albany, NY: State University of New York Press.

Podsakoff, Philip M., Scott B. MacKenzie in Nathan P. Podsakoff (2016): Recommendations for Creating Better Concept Definitions in the Organizational, Behavioral, and Social Sciences. Organizational Research Methods 19 (2): 159–203.

Preibusch, Sören (2013): Guide to Measuring Privacy Concern: Review of Survey and Oservational Instruments. International Journal of Human-Computer Studies 71 (12): 1133–1143.

Rohunen, Anna (2019): Advancing Information Privacy Concerns Evaluation in Personal Data Intensive Services (doktorska disertacija). University of Oulu, Oulu, Finska, 14. december 2019.

Rohunen, Anna, Jouni Markkula, Marikka Heikkilä in Markku Oivo (2020): Explaining Diversity and Conflicts in Privacy Behavior Models. Journal of Computer Information Systems 60 (4): 378–393.

Sevignani, Sebastian (2013): The Commodification Of Privacy On The Internet. Science and Public Policy 40: 733–739.

Shank, Russell (1986): Privacy: History, Legal, Social, and Ethical Aspects. Library Trends 35 (1): 7–18.

Smith, Jeff H., Tamara Dinev in Heng Xu (2011): Information Privacy Research: An Interdisciplinary Review. MIS Quarterly 35 (4): 989–1015.

Stewart, Kathy A. in Albert H. Segars (2002): An Empirical Examination of the Concern for Information Privacy Instrument. Information Systems Research 13 (1): 36–49.

Tavani, Herman T. (2007): Philosophical Theories Of Privacy: Implications For an Adequate Online Privacy Policy. Metaphilosophy 38 (1): 1–22.

Trepte, Sabine (2020): The Social Media Privacy Model: Privacy and Communication in the Light of Social Media Affordances. Communication Theory. Predobjava na spletu 7. maj 2020.

Warren, Samuel D. in Louis D. Brandeis (1890): The Right to Privacy. Harvard Law Review 4 (5): 193–220.

Weintraub, Jeff (1997): The Theory and Politics of the Public/Private Distinction. V: Jeff Weintraub (ur.) in Krishan Kumar (ur.), Public and Private in Tohught and Practice: Perspectives on a Grand Dichotomoy, 1–42. Chichago in London: The University of Chichago Press.

Westin, Alan F. (1967): Privacy and Freedom. New York, NY: Atheneum.

Westin, Alan F. (2003): Social and Political Dimensions of Privacy. Journal of Social Issues 59 (2): 431–453.

VIRI

Snoj, Marko (2021): Fran/Etimološki slovar. Dostopno prek https://fran.si/193/marko-snoj-slovenski-etimoloski-slovar, 23. 9. 2021.