Transformacija pojma prava na privatnost kao posljedica razvoja tehnologije i novih sigurnosnih izazova

Pavuna, Andro

Doctoral thesis / Disertacija

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, The Faculty of Political Science / Sveučilište u Zagrebu, Fakultet političkih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:114:962407

Sveučilište u Zagrebu

Fakultet političkih znanosti

Andro Pavuna

Transformacija pojma prava na privatnost kao posljedica razvoja tehnologije i novih sigurnosnih izazova

DOKTORSKI RAD

Zagreb, 2019.

Sveučilište u Zagrebu

Fakultet političkih znanosti

Andro Pavuna

Transformacija pojma prava na privatnost kao posljedica razvoja tehnologije i novih sigurnosnih izazova

DOKTORSKI RAD

Mentor:

prof. dr. sc. Enes Kulenović

Zagreb, 2019.

University of Zagreb

Faculty of Political Science

Andro Pavuna

The transformation of the concept of the right to privacy as a result of developments in technology and new security challenges

DOCTORAL THESIS

Supervisor:

prof. Enes Kulenović, Phd

Zagreb, 2019.

Informacije o mentoru

Enes Kulenović izvanredni je profesor na Odsjeku za političku i socijalnu teoriju na Fakultetu političkih znanosti Sveučilišta u Zagrebu.

Uz školovanje na Sveučilištu u Zagrebu, školovao se, te znanstveno usavršavao na Sveučilištu Duke u SAD-u, Sveučilištu Bern u Švicarskoj, Sveučilištu Otto-von-Guerick, Magdeburg u Njemačkoj, te Sveučilištu York u Velikoj Britaniji.

U svom znanstvenom radu surađivao je na više znanstvenih projekata, a od 2015. godine voditelj je znanstveno-istraživačkog projekta Govor mržnje u Hrvatskoj.

Autor je broja izvornih znanstvenih članak objavljenih u prestižnim znanstvenim časopisima (Journal of Politics, Ethica and Politica, Croatian Political Science Review, Philosophy and Public Issues), urednik i ko-autor zbornika Govor mržnje u Hrvatskoj (Biblioteka političke analize, 2016.), urednik i koautor sveučilišnog udžbenika Moderna politička teorija (Biblioteka politička misao, 2013.), te autor znanstvene knjige Sloboda, pluralizam i nacionalizam: politička teorija Isaiaha Berlina (Biblioteka politička misao, Zagreb, 2006.) za koju je dobio Državnu nagradu za znanost 2007. godine.

U razdoblju od 2013. do 2017. bio je glavni urednik znanstvenog časopisa Anali HPD-a, te član je Savjeta za ljudska prava Pučke pravobraniteljice RH.

Zahvale

Ova disertacija nikada ne bi ugledala svjetlo dana da nije bilo nesebične podrške i pomoći niza ljudi kojima ovim putem od srca zahvaljujem.

Najprije, zahvaljujem supruzi Kristini na tome što mi je godinama davala prostora za pisanje i razmišljanje, što mi je bila podrška u brojnim i intenzivnim autorskim krizama te ponajviše na tome što se cijelo vrijeme trajanja ovog projekta nadljudskim snagama trudila kompenzirati moje izbivanje iz života naše Lede. Ledi zahvaljujem na strpljenju i ljubavi koju mi je bezuvjetno davala svojim poljupcima i zagrljajima.

Svojem mentoru, prof. dr. sc. Enesu Kulenoviću zahvaljujem na trudu koji je uložio u ovaj projekt, a posebno na njegovom izuzetno stručnom vodstvu te na njegovu razumijevanju i riječima podrške u trenucima kada mi je bilo najteže. Na svakom komentaru, prijedlogu, upozorenju, kritici i podršci iskreno hvala.

Prijatelju i genijalcu doc. dr. sc. Kosti Bovanu, koji je još jednom pokazao koliko ima veliko srce i oštar um, zahvaljujem na bezuvjetnoj podršci i neizmjernoj pomoći.

Članovima komisije za ocjenu disertacije doc. dr. sc. Hrvoju Cvijanoviću, izv. prof. dr. sc. Nebojši Blanuši i red. prof. dr. sc. Darku Polšeku zahvaljujem na vremenu i trudu koji su uložili u čitanje i recenziranje ovog rada te što su mi dali brojne konstruktivne prijedloge za njezino poboljšanje kao i ideje za buduća istraživanja.

Za pomoć u obavljanju intervjua posebno zahvaljujem Marijani Samirić i njezinim mladim prijateljima. Jednako tako, zahvaljujem svim prijateljima i poznanicima koji su proslijedili veze na e-anketu. Nažalost, ili nasreću, popis osoba koje su mi u tome pomogle je prevelik za ovu zahvalu, ali znajte da sam svakome od srca zahvalan! Bez vas ovo istraživanje ne bi bilo moguće provesti. Od srca zahvaljujem svim sudionicima koji su ispunili anketu, a posebno sudionicima koji su sudjelovali u intervjuima.

Svojim roditeljima Damiru i Nataši, obitelji i prijateljima zahvaljujem na pomoći, podršci i razumijevanju. Hvala vam što ste me trpjeli i što me niste zaboravili u ovih sedam dugih godina.

Konačno, zahvaljujem svojim kolegama i prijateljima iz grupe Općenita stručnost, Bojani, Aleksandri, Ajli, Lani, Amaru, Josipu i Kosti na smijehu koji liječi.

Sažetak

Osnovni cilj ove disertacije bio je utvrditi je li zbog rapidnog razvoja tehnologije i novih sigurnosnih izazova došlo do transformacije pojma privatnosti, odnosno prava na privatnost u političkom smislu. Najprije je privatnost definirana kao mogućnost kontrole pristupa (podacima o) sebi. Definicijom privatnosti u terminima kontrole pojedinca se stavlja u središte njegova postojanja te se naglašava vrijednost privatnosti za autonomiju i uspostavu bliskih međuljudskih odnosa. Ugroze privatnosti su prema stupnju kontrole koju pojedinac nad njima ima ugrubo podijeljene na interne i eksterne ugroze privatnosti, odnosno na one ugroze u kojima kontrolu nad (podacima o) nama nekome dobrovoljno predajemo ili nam je netko oduzima bez našega znanja. Na primjeru masovnog nekritičkog nadzora koji provode pojedine strane obavještajne službe prikazane su opasnosti koje proizlaze iz eksternih ugroza privatnosti, dok je za eksterne korišten odnos najvećih svjetskih informacijskih tvrtki prema korisničkim podacima, a posebice činjenica kako ljudi olako prepuštaju svoje osobne podatke u zamjenu za digitalne usluge ili trgovačke pogodnosti. Kroz normativnu raspravu o intrinzičnoj i instrumentalnoj vrijednosti privatnosti obrazloženo je kako je privatnost temeljno ljudsko pravo koje istovremeno ima svoj značaj za pojedinca, društvo, političku zajednicu i demokraciju. Na taj način definirana privatnost suočena je s opsegom i razinom eksternih i internih ugroza privatnosti te je zaključeno kako je pojam privatnosti radikalno transformiran iz temeljnog ljudskog prava u robu kojom se trguje.

U drugom dijelu rada, provedeno je empirijsko istraživanje čiji je cilj bio utvrditi način na koji ljudi razumiju koncept privatnosti. Istraživanje se sastojalo od kvalitativnog predistraživanja korištenjem metode polustrukturiranog intervjua provedenog na 16 sudionika te kvantitativnog anketnog istraživanja provedenog na uzorku od 966 sudionika. Rezultati istraživanja pokazuju kako većina ljudi deklarativno visoko vrednuje važnost privatnosti. No, istovremeno su tek umjereno zabrinuti za privatnost te, ono značajnije, tek rijetko iskazuju ponašanja kojima štite vlastitu privatnost. Prema tome, zaključeno je kako je trenutni odnos pojedinaca prema vlastitoj privatnosti te odnos država prema privatnosti svojih građana nespojiv s temeljnim postavkama liberalne demokracije. Budući da se temeljno ljudsko pravo na privatnost unutar liberalno-demokratske paradigme ne može normativno redefinirati, potrebno je bez odgode početi na odgovarajući način osiguravati, štititi i vrednovati pravo na privatnost svakog čovjeka.

Ključne riječi: privatnost, pravo na privatnost, paradoks privatnosti, autonomija.

Summary

The main purpose of this dissertation was to determine whether the concept of privacy was transformed as a result of the rapid technological development and emerging security challenges in the last fifteen years. The thesis is based on two levels of analysis. At the level of a nation-state a thorough normative discussion was conducted and at the level of citizens an empirical research was conducted. At first, privacy was defined as the ability to control access to (information about) oneself. The definition of privacy in terms of control places the individual at the centre of her existence and emphasizes the value of privacy for autonomy and the establishment of close interpersonal relationships.

After defining the concept of privacy and determining its value, next task was to observe current threats to privacy. Threats to privacy were divided into two broad groups based on the degree of control that an individual has over them. Depending on the locus of control of (information about) us the, there were two groups of threats – external and internal. External being those in which control over (information about) us was seized without our knowledge and/or against our will, whereas internal being those in which control over (information about) us was voluntarily given. As an example of dangers arising from external threats to privacy mass-surveillance carried out by certain large intelligence services was used. On the other hand, to illustrate the dangers arising from internal threats, the relationship between the world's largest digital and advertising companies and user data was used, and in particular the fact that people are reluctantly giving their personal information in exchange for digital services or virtually irrelevant convenience.

Through a normative discussion on the intrinsic and instrumental value of privacy, privacy was carefully established as a fundamental human right, which at the same time has its significance for the individual, society, the political community and democracy. Privacy defined in this was faced with the extent and the level of external and internal threats to privacy we encounter today. It was concluded that the concept of privacy is radically transformed from basic human rights to a tradable commodity.

In the second part of the thesis, an empirical study was conducted in order to get insights on the way people today view privacy. Research has collected some very valuable information on how people understand privacy and threats to privacy. In the qualitative pre-study 16 people were interviewed using a semi-structured interview method. Results have shown that people are very

rarely thinking about privacy, but when they do, most of them find it very important and they value it. Findings from this study have been used it the following quantitative study that has been carried out on a much larger sample of 966 participants. Primary goal was to test the privacy paradox, which describes a phenomenon of disparity between the high importance of privacy and the ease with which they are willing to give it up. The results have confirmed the existence of a privacy paradox, that is, those participants who appreciated their privacy the most showed that they behave statistically significantly different from what could be expected of those who value their privacy highly.

Furthermore, in both qualitative and quantitative study, we've collected a number of empirical data that contributes to better understanding of how individuals perceive privacy. These findings are complementary to the conclusion of the normative discussion on the radical transformation of the concept of privacy. Research results show that most people still highly value the importance of privacy. But at the same time, they are only moderately concerned about privacy and, more importantly, they rarely express privacy protecting behaviour. Therefore, it was concluded that the current relationship of individuals towards their own privacy as well as the way modern states respect privacy of their citizens is incompatible with the fundamental settings of liberal democracy. Since it is not possible to normatively redefine the fundamental human right to privacy within the liberal democratic paradigm, it is necessary to begin adequately securing, protecting the right of every person's privacy.

However, due to the widespread voluntary waiving of their privacy in order to gain access to various services and benefits, states should be determined to securing the privacy rights of their citizens despite the wish of its citizens to renounce it. Although such paternalism may, to a certain extent, be justified within the liberal paradigm, it is unrealistic for it to happen. More so because the states themselves are motivated to stay aside in this matter because due to reduced sensitivity to internal threats at the same time citizens have become less sensitive to external threats to privacy. Today's consumer wants a free service, benefits and discounts, precise recommendations, tailored advertisements, and believes that sharing of personal information is a low price for that.

This thesis should be seen as an attempt of contributing to this hot topic, having in mind that is just a small part of the extensive debate on the role and importance of privacy to follow. Despite the fact that this work represents a certain contribution to the restoration of privacy to its

deserved normative framework, the results of the empirical research give little room to maintain optimism.

Keywords: privacy, right to privacy, privacy paradox, autonomy.

Sadržaj

Uvod

Kakav bi svijet bio bez privatnosti? Neki distopijski romani, poput Orwellova romana *1984* (Orwell, 2016), Huxleyeva romana *Vrli novi svijet* (Huxley, 2000) i Zamyatinova romana *Mi* (Zamyatin, 1972), opisuju svijet bez privatnosti ili sa značajno narušenom privatnosti pojedinca. Ovi genijalni autori svojom maštom i izuzetnim umjetničkim sposobnostima osim stvaranja fikcije zapravo doprinose i filozofskoj raspravi o privatnosti. Njihov doprinos katkada nije eksplicitno vidljiv zbog relativno strogih akademskih i znanstvenih pravila za korištenje literature u znanstvenome radu, ali njihove se ideje provlače kroz teorije i razmišljanja mnogih autora koji pišu o privatnosti. Na primjer, Gerstein tvrdi kako bi bez privatne sfere društvene norme potpuno upile pojedinca (Gerstein, 1978), Bloustein govori o tome kako biće koje je u potpunosti izloženo drugima zapravo nije osoba (Bloustein, 1984), Reiman i Rössler naglasak stavljaju na kritičku misao i utjecaj privatnosti na demokraciju, što su ideje nedvojbeno inspirirane navedenim romanima. Naime, spomenuti distopijski klasici koriste upravo nedostatak privatnosti kao jedan od osnovnih načina na koji ilustriraju totalitarističke elemente svjetova u kojima se odvija radnja njihovih romana. Time što su nepostojanje privatnosti koristili kao jednu od temeljnih odrednica totalitarističkih poredaka, dodatno su naglasili značaj privatnosti za demokraciju. Upravo su navedeni romani, ali i brojni drugi, bili inspiracija za ovaj rad i poticaj prema boljem razumijevanju privatnosti pa će stoga biti spomenuti kada god to bude prikladno. Činjenica da u današnjem svijetu postoji sličnost ugroza privatnosti s nekim od elemenata koji su korišteni u zastrašujućim distopijskim romanima iz prve polovice 20. stoljeća, bila jedna od motivacija za proučavanje ove izazovne teme.

Kao što i sam naslov disertacije sugerira, osnovni cilj jest utvrditi je li zbog rapidnog razvoja tehnologije i novih sigurnosnih izazova u posljednjih petnaestak godina došlo do transformacije pojma prava na privatnost. Problemu se pristupilo s dvije razine i to s razine nacionalne države i s razine građana. Prva razina, ona normativna, propituje koliko je koncept prava na privatnost, definiran u prvom poglavlju, održiv u današnjem kontekstu, opisanome u drugom i trećem poglavlju. Početna pretpostavka jest da legitimitet liberalnih demokracija počiva na zaštiti temeljnih ljudskih prava njihovih građana. Jedno od takvih prava jest i pravo na privatnost te iz toga proizlazi temeljno istraživačko pitanje.

- **P1: U kojoj je mjeri došlo do transformacije pojma prava na privatnost kao posljedice razvoja tehnologije i novih sigurnosnih izazova? Je li takav transformirani pojam prava na privatnost i dalje spojiv s razumijevanjem zaštite prava od strane nacionalne države kao jednog od temeljnih uvjeta njihove legitimnosti?**

Pravo na život, slobodu i osobnu sigurnost nedvojbeno jesu temeljna ljudska prava i od svake se nacionalne države očekuje da ih osigura. Međutim, u svojem nastojanju da spriječe ugrožavanje života, sigurnosti i slobode svojih građana, brojne su države u određenoj mjeri počele ograničavati pravo na privatnost. Zbog toga je na akademskoj, političkoj i građanskoj razini došlo do tenzija između pozicije prema kojoj postoji razina prava na privatnost koja se ne smije ugrožavati ni radi zaštite sigurnosti i pozicije prema kojoj je država dužna osigurati sigurnost čak i pod cijenu širokog ograničavanja prava na privatnost svojih građana. Istraživačko pitanje usmjereno je na utvrđivanje razmjera transformacije pojma prava na privatnost, odnosno, njegove normativne i konotativne redefinicije.

U prvom poglavlju bit će pružen temeljni povijesni i konceptualni pregled koncepta privatnosti. Prije početka analize koncepta, privatnost će biti definirana u terminima kontrole i to kao mogućnost kontrole pristupa (podacima o) sebi. U nastavku poglavlja, bit će izvedena osnovna vrijednost privatnosti i to kao ona za autonomiju i uspostavljanje i održavanje bliskih međuljudskih odnosa.

Drugo poglavlje posvećeno je ugrozama privatnosti. Temeljem definicije privatnosti u terminima kontrole, ugroze privatnosti bit će ugrubo podijeljene na interne i eksterne, odnosno one u kojima kontrolu nad (podacima o) sebi nekome sami dobrovoljno predajemo i one u kojima nam tu kontrolu netko oduzima bez našeg znanja i/ili volje. I eksterne i interne ugroze privatnosti istovremeno ugrožavaju autonomiju čime se u opasnost dovodi dostojanstvo i blagostanje pojedinaca, društva i demokracije. Kao glavni primjer eksternih ugroza bit će korišteni podaci o masovnom nekritičkom nadzoru pojedinih stranih obavještajnih službi, a za ilustriranje internih ugroza bit će korišten odnos suvremenog potrošača i najvećih internetskih i telekomunikacijskih tvrtki s naglaskom na davanje, prikupljanje i korištenje osobnih podataka.

Treće poglavlje rezervirano je za temeljitu normativnu raspravu o intrinzičnoj i instrumentalnoj vrijednosti privatnosti nakon što je se suoči s ugrozama privatnostima opisanima u drugom poglavlju. Naime, nakon što privatnost definiramo kao temeljno ljudsko pravo koje

istovremeno ima svoj značaj za pojedinca, društvo, političku zajednicu i demokraciju, suočit će ga se s opsegom i razinom ugroze prikazanom u drugom poglavlju. Nakon definiranja razine transformacije pojma prava na privatnost, postavlja se pitanje je li ono transformirano u mjeri u kojoj zapravo više ne podrazumijeva osiguravanje minimalne nužne razine privatnosti.

Osim odozgo, iz perspektive legitimiteta nacionalne države, problemu transformacije pojma prava na privatnost pristupit će se i odozdo, iz perspektive građana. Naime, u četvrtom će poglavlju biti prikazano empirijsko istraživanje, koje se sastojalo od kvalitativnog predistraživanja provedenog korištenjem metode intervjua te kvantitativnog anketnog istraživanja provedenog na znatno većem uzorku. Primarni cilj predistraživanja bio je prikupiti podatke o načinu na koji pojedinci vide privatnost i ugroze privatnosti. Temeljem dobivenih rezultata generiran je anketni upitnik koji je primijenjen na znano većem uzorku, a čiji je primarni cilj bio provjeriti postojanje paradoksa privatnosti, prema kojem ljudi deklarativno izrazito drže do svoje privatnosti, ali je se zapravo s lakoćom odriču. Iz toga proizlazi drugo istraživačko pitanje:

- **P2: Koji je značaj privatnosti za pojedinca u današnjem društvu? Radi li se o pravu koje građani smatraju temeljnim ljudskim pravom? Jesu li se i pod kojim uvjetima spremni odreći svoje privatnosti?**

Kako bi se odgovorilo na tu dilemu, u pokušaju odgovora na drugo istraživačko pitanje provjerit će se postoji li paradoks privatnosti, odnosno postoji li značajno odstupanje između deklarirane visoke važnosti privatnosti za pojedince i lakoće kojom su je se spremni odreći. Konačno, rezultati dobiveni kroz odgovor na pitanje stvarnog značaja privatnosti za pojedince te uvjeta pod kojima su je se spremni odreći, upotrijebit će se kao temelj za doprinos normativnoj raspravi o konceptu prava na privatnost i odgovornosti nacionalne države da ga osigura građanima.

U petom poglavlju normativna rasprava bit će nadopunjena spoznajama dobivenima u empirijskom istraživanju kako bi se stekao bolji uvid u razinu transformacije pojma privatnosti. Konačni je zaključak rada kako je postojeće, transformirano, razumijevanje prava na privatnost nespojivo je s idejom da nacionalna država u okviru liberalne demokracije i dalje štiti prava svojih građana. Prema tome, potrebno je ili redefinirati postojeće razumijevanje načina na koji liberalne demokracije osiguravaju ljudska prava svojim građanima ili redefinirati značaj i

važnost prava na privatnost kao temeljnog ljudskog prava koje bi suverena država trebala osigurati svojim građanima.

Ovim radom suočit će se teorijska raspravu o pravu na privatnost s podacima dobivenim empirijskim istraživanjem u pokušaju boljeg razumijevanja evidentne normativne i manifestne transformacije pojma privatnosti. Disertacija će predstavljati doprinos boljem razumijevanju važnosti privatnosti i prava na privatnost te pokušaj utvrđivanja razine internalizacije odricanja od privatnosti.

1. Ideja i koncept privatnosti

Razmišljanje o privatnosti te problematiziranje koncepta privatnosti javlja se još u antici i od tada do danas ono je neizostavan dio povijesti društvenog i političkog mišljenja. Za Platona privatnost je suprotstavljena nadzoru i transparentnosti, budući da su "dobri čuvari" države oni koji "bdiju" nad državljanima kao očevi "nad potomstvom" (Platon, 2009:163) i stoga Platon sugerira "neka potraže mjesto u državi, gdje bi bilo najljepše udariti tabor, odakle bi najlakše držali na uzdi državljane, ako se tko ne bi htio zakonima pokoravati" (Platon, 2009:163), no istovremeno ogoljujući i vlastitu privatnost budući da nitko od njih ne bi trebao imati "stana ni takve riznice u koje ne bi mogao ulaziti svatko tko će htjeti" (Platon, 2009:165). Dakle, Platonov zamišljaj države pretpostavlja potpunu transparentnost nasuprot privatnosti u svrhu ostvarivanja ideje pravednosti i dobra.

Alan Westin, jedan od pionira u borbi za isticanje značaja privatnosti i jedan od najutjecajnijih autora u području, napravio je detaljan pregled razvoja pojma privatnosti u zapadnoj političkoj misli te je zaključio kako je razvoj pojma obilježilo postojanje dvije suprotstavljene tradicije (Westin, 1967:22). Jedna tradicija vuče svoje korijene iz „antičke Grčke, preko engleskog protestantizma do tradicije općeg prava, američkog konstitucionalizma i koncepta privatnog vlasništva“, a obilježava je „trend ograničavanja ovlasti nadzora državnih, vjerskih i ekonomskih vlasti i elita radi zaštite interesa privatnosti pojedinaca, obitelji i određenih skupina u svakom društvu“ (Westin, 1967:22). Druga tradicija razvoja privatnosti u zapadnoj povijesti svoje korijene ima u nešto drugačijim društvima, a Westin njezin razvoj prati od „Sparte, preko Rimskog Carstva i srednjovjekovne crkve do kontinentalne nacionalne države“ (Westin, 1967:23). Nasuprot prvoj, ovu tradiciju obilježava „postojanje širokih ovlasti nadzora koje na raspolaganju imaju državne, vjerske i ekonomske vlasti i elite“ (Westin, 1967:23). Ove dvije suprotstavljene tradicije, koje su se veći dio povijesti paralelno razvijale, obilježio je sasvim različit pogled na privatnost građana kao i na ograničenje mogućnosti njihova nadzora i kontrole. Tako je i danas, no rezultati istraživanja u ovom radu ukazuju na to kako je došlo do velikog zaokreta te danas privatnost uživa veću pravnu zaštitu i viši status u zapadnoeuropskim društvima proizašlima iz one tradicije koju Westin opisuje kao drugu, u odnosu na anglosaksonska društva iz prve tradicije.

Pohlman također donosi povijesni pregled razvoja pojma privatnosti, no on ga ne razdvaja na dvije suprotstavljene tradicije već o razvoju ideje privatnosti piše kao o jedinstvenom razvoju.

Stavljanjem naglaska na dominaciju određene političke misli u određenom povijesnom trenutku Pohlman daje prednost pojedinoj tradiciji, u smislu u kojem ih Westin opisuje (Pohlman, 1993). Kao što je detaljnije opisano na primjeru Platona, koji u svom pogledu na privatnost nije bio usamljen, grčki mislioci privatnost nisu smatrali pozitivnom vrijednosti budući da je predstavljala svojevrsnu suprotnost transparentnosti političke sfere te javnom djelovanju u njoj, što je bio tadašnji ideal. Prema Polhmanu, Aristotelov stav kako je osobni kontemplativni stav barem jednako vrijedan kao i politička participacija jedan je od začetaka postepenog potkopavanja statusa politike u antičkoj Grčkoj (Pohlman, 1993:267). Povijesni razvoj u narednim stoljećima doveo je do postepenog gubitka značaja gradova-država, a time i do prostora za veće okretanje pojedinaca prema sebi, za veći razvoj značaj privatnosti. Međutim, malo koja škola misli to je i učinila (Pohlman, 1993). Značajniji preokret donijela je pojava kršćanstva. Pritom je privatnost u kršćanstvu imala dvojak značaj. S jedne strane, kroz osobni i privatni odnos Bogom, privatnost je dobila na značaju, dok je s druge strane sam temelj vjerovanja u sveznajućeg i svevidećeg Boga bio kontradiktoran privatnosti. Pohlman, slično kao i Westin, naglašava kako je zapravo tijekom Srednjeg vijeka dominirao negativistički pogled crkve, osobito katoličke, na privatnost, dok je jačanje privatnog i osobnog odnosa s Bogom dobilo na značaju tek se protestantskom reformacijom, koju Westin pripisuje tzv. prvoj tradiciji (Pohlman, 1993).

Protestanstka reformacija bila je posebno značajna za razvoj prosvjetiteljstva. Kroz kritiku katoličke crkve otvorio se velik prostora za redefiniciju postojećeg društvenog uređenja. U *Pismu o toleranciji*, John Locke uz pomoć zagovaranja religijske tolerancije, za njega „toliko bliske Kristovu evanđelju i istinskom umu čovječanstva“ (Locke, 2015:11–12), postulira znatno veću ideju. Za Lockea je država „zajednica ljudi konstituirana samo zbog postizanja, očuvanja i unapređenja njihovih vlastitih građanskih interesa“ koji su prema njemu „život, sloboda, zdravlje i odsustvo teških bolova, kao i posjedovanje izvanjskih stvari“, a „dužnost je građanskog vladara da nepristranim provođenjem jednakih zakona svim ljudima (…) osigura pravedno posjedovanje stvari koje pripadaju ovom životu“ (Locke, 2015:12-13). Ključan moment bio je pretvaranje filozofskog koncepta, objektivnog prava, u subjektivno pravo koje pripada svakom građaninu. Time je posijano sjeme liberalne misli. U nastavku njezina rasta, subjektivno pravo svakog građanina razvit će se u svojevrsnu sferu slobode oko njegova postojanja, u koje nitko drugi neće imati pravo nepozvan ulaziti. U 18. stoljeću liberalna je ideja poprimila jasnije konture definiranjem temeljnih prava s naglaskom na pravo privatnog

vlasništva, a Pohlman (1993) posebno izdvaja Četvrti amandman Povelje o pravima SAD-a kojim je 1791. godine građanima SAD-a zajamčena nepovredivost vlastite osobe, mjesta stanovanja, dokumenata i imovine od neosnovanih pretraga i zapljena. Krajem 19. stoljeća, razvoj moralnog ideala privatnosti bio je u većoj mjeri dovršen (Pohlman, 1993: 271–272) te je započeo razvoj *prava* na privatnost.

Unatoč tome što privatnost svoje korijene ima u filozofskim raspravama još od antike, privatnost kao pravni koncept postoji tek nešto više od stotinu godina. U tom je razdoblju privatnost iz dana u dan sve više dobivala na značaju te se danas o privatnosti govori znatno više nego prije nekoliko godina ili nekoliko desetaka godina. Kao i većina društvenih konstrukta, privatnost kao pojam, od svojeg je nastanka prošla težak put i brojne su vrlo uvjerljive kritike u konačnosti dovele do toga da danas možemo reći kako među autorima koji proučavaju pojam privatnosti postoji konsenzus oko toga da je privatnost značajna i vrijedna. Doduše, privatnost potencijalno ima i svoju tamnu stranu jer kroz zaštitu privatne sfere osigurava siguran poligon za nedjela kao i svojevrsnu sigurnu luku u koju se može sakriti od legitimnog progona. I dok se doista većina autora slaže oko značaja privatnosti, postoje značajne razlike u načinu na koji pojedini autori poimaju privatnost kao i u razlozima zbog kojih je smatraju značajnom i vrijednom.

Možemo reći kako je zaštita privatnosti započela krajem 19. stoljeća u SAD-u, kada je pokrenuta sveobuhvatna pravna rasprava o *pravu* na privatnost. Ta je rasprava u početku vrlo intenzivno, a kasnije nešto manje intenzivno trajala veći dio 20. stoljeća. Raspravu su obilježila neslaganja oko definicije pojma i različiti pogledi na razloge zbog kojih je privatnost vrijedna i zašto bi je trebalo zaštititi. Međutim, dominantna podjela među autorima bila je na one koji su na privatnost gledali kao na jedinstven i koherentan konstrukt koji obuhvaća niz međusobno povezanih pitanja i potreba te na one koji su smatrali da se privatnost može svesti na druga temeljna prava koja se može štititi bez „umjetnog“ stavljanja pod isti nazivnik privatnosti.

Upravo su ti skeptični pogledi, kritični prema davanju velikog značaja privatnosti i prema definiranju prava na privatnost, značajno doprinijeli razumijevanju pojma privatnosti. Osim redukcionističke kritike prema kojoj se privatnost može jednako dobro objasniti već postojećim temeljnim ljudskim pravima (Scanlon, 1975) ili deliktima (Prosser, 1960), postoji i skupina autora koji su na privatnost gledali kao na nešto negativno budući da su smatrali kako ljudi uz pomoć prikrivanja podataka o sebi manipuliraju drugima i zavaravaju ih (Posner, 1978;

Wasserstrom, 1984), čime ugrožavaju ekonomski i društveni rast i razvoj (Posner, 1978) ili su na privatnost gledali negativno stoga što za njih privatnost omogućuje stvaranje zida iza kojeg je olakšano zlostavljanje i zanemarivanje žena (MacKinnon, 1989). Kroz odgovore na ove i druge kritike privatnost je kao koncept dodatno izbrušena i ojačana.

Tako danas možemo reći kako većina autora ipak smatra da je privatnost vrijedan i važan koncept (DeCew, 2013), unatoč tome što među njima postoje različiti pogledi na definiciju ili značaj privatnosti za pojedinca ili društvo. Pa tako je za jedne privatnost *pravo biti ostavljen na miru* (Warren i Brandeis, 1890), ili imati *mogućnost ograničiti pristup sebi* (Gavison, 1980). Daljnji razvoj koncepta privatnosti uvažio je značaj *kontrole* pa je tako mogućnosti ograničavanja pristupa sebi dodana mogućnost kontrole pristupa sebi. Pri tome se za neke radilo o kontroli nad informacijama o sebi (Fried, 1968; Gerstein, 1970; Posner, 1978; Westin, 1967), kontroli nad sferom intimnosti (Iness, 1992), kontroli nad pristupom osobi (Rachels, 1975) ili kombinaciji nekih od navedenih aspekata (Moore, 2003). Prema tome, u ovom će radu ta sintagma biti korištena na način da se privatnost definira kao mogućnost kontrole pristupa (podacima o) sebi, kako bi osim samih podataka uključivala i širi oblik pristupa osobi, kako fizički tako i psihološki.

Kao i oko definicije, tako i oko vrijednosti i važnosti privatnosti postoje različite koncepcije, ali među njima su dominantne one koje privatnost smatraju značajnom zbog njezine povezanosti s ljudskim dostojanstvom, s temeljem iz kojeg proizlaze ljudska prava (Benn, 1971; Bloustein, 1984; Gavison, 1980; Reiman, 1976; Rössler, 2006), te one koje smatraju kako privatnost ima središnju ulogu u ostvarivanju i održavanju različitih međuljudskih odnosa (Fried, 1968; Gerstein, 1978; Rachels, 1975). Oba uvida vrlo su vrijedna i međusobno se ne isključuju. Naprotiv, zajedno pokazuju izuzetnu vrijednost privatnosti i upućuju na opću vrijednost privatnosti i za društvo te potvrđuju potrebu da se pravo na privatnost utemelji i štiti kao temeljno ljudsko pravo.

1.1. Kultura i ljudska priroda

Alan Westin, jedan od pionira u borbi za isticanje značaja privatnosti još je 1967. godine u knjizi *Privacy and Freedom* na temelju nekoliko vrlo opsežnih istraživanja životinjskog ponašanja i njihove društvene organizacije ustvrdio kako je čovjekova potreba za privatnosti duboko ukorijenjena u njegovu evolucijskome nasljeđu (Westin, 1967). Jedna od temeljnih

spoznaja proizašlih iz proučavanja ponašanja životinja jest ta da gotovo sve životinje traže razdoblja za izdvajanje iz grupe ili za intimnost unutar manje grupe, a takva se ponašanja uglavnom opisuju kao tendencija prema teritorijalnosti te se vjeruje da imaju vrlo važnu svrhu za opstanak vrste. Teritorijalnost jedinke ili manje grupe životinja osigurava opstanak vrste kroz ravnomjerniji pristup dostupnim resursima te ono omogućuje i potiče pojavu tzv. vrijednih mužjaka. Fizičko izdvajanje omogućuje životinjama prostorni okvir unutar kojeg mogu ostvariti grupne aktivnosti poput učenja, igre, skrivanja kao i međusobnog kontakta s članovima grupe. Zoološka istraživanja pokazuju kako životinje posjeduju potrebu za određenom minimalnom razinom privatnosti bez koje njihov opstanak može biti i ugrožen, a zabilježeni su mnogi primjeri u kojima nedostatak privatnog prostora kao posljedica prevelike napučenosti kod nekih životinja može izazvati nagon za ubijanjem ili pak za samoubojstvom (Westin, 1967).

Proučavajući nastanak i razvoj ljudi možemo zaključiti kako je rapidni razvoj sapiensa i značajniji skok u razvoju u odnosu na ostale životinje relativno nova pojava. Još do prije svega nekoliko desetaka tisuća godina ljudi su se, pa tako i rani sapiensi, vrlo malo razlikovali od ostalih životinja iz porodice velikih majmuna i po svemu sudeći nisu bili na vrhu hranidbenog lanca (Harari, 2014). Iz toga se razumnim čini pretpostaviti kako i ljudi dijele sličnu tendenciju prema izdvajanju iz grupe i intimnosti unutar manje grupe. Mnogi antropolozi pokušali su utvrditi je li potreba za privatnosti dio ljudske prirode ili je ona društveno nametnuti konstrukt ovisan o kulturi. Dakako, potreba za privatnosti ne postoji izvan socijalnog okruženja, kada su pojedinci sami (Moore, 2003), no to nipošto ne znači da potreba za *barem nekim oblikom* privatnosti nije dio ljudske prirode. Taj se dio ljudske prirode kao kulturalni fenomen u pojedinom društvu manifestira na način neodvojivo povezan s običajima i društvenim praksama pojedine kulture. Istraživanja poput onog opisanog u knjizi *Coming of Age in Samoa* Margaret Mead iz 1928. godine pokazuju na koji način različite kulture štite i vrednuju privatnost kroz prikrivanje, odlazak u osamu te ograničavanje pristupa tajnim ritualima (DeCew, 2013). Westin je na temelju pregleda nekoliko stotina različitih primitivnih zajednica među kojima je bilo nekoliko tisuća različitih kultura ustvrdio kako tek njih nekoliko nisu poznavale privatnost, a detaljnim kvalitativnim uvidom u opisane slučajeve zaključio je kako ti slučajevi ne mogu biti dokaz za nepostojanje univerzalne potrebe za privatnosti (Westin, 1967). Dakako, način na koji se u primitivnim zajednicama manifestira potreba za privatnosti malo podsjeća na način na koji se to čini u modernim zapadnim kulturama, ali Westin je izdvojio četiri opća aspekta privatnosti

prisutna u praktički svakoj zajednici koja je detaljno proučavana, a koji će nešto kasnije biti detaljnije opisani.

Antropolog Robert Murphy pod utjecajem pisanja o konstruktu *socijalne distance* njemačkog filozofa Georga Simmela, a dominantno na temelju istraživanja nad afričkim nomadskim plemenom Tuarega, poznatim po njihovu stalnom korištenju vela kojim prekrivaju lice, zaključio je kako je stvaranje i održavanje socijalne distance prisutno u svim društvenim odnosima uz opasku kako različiti odnosi ili različita društva različito određuju razine udaljenosti (Murphy, 1964). Govoreći o socijalnoj distanci, Murphy je iznio jedan vrlo pronicljiv zaključak, koji će kasnije prihvatiti drugi autori kada govore o privatnosti. Naime, Murphy je još od Simmela preuzeo intuitivno uvjerenje kako je socijalna distanca obrnuto proporcionalna količini informacija koje akteri imaju jedno o drugome, odnosno, što više dvoje ljudi zna jedno o drugome to je manja njihova socijalna distanca. Ovaj je zaključak na prvi pogled intuitivan i sam po sebi samorazumljiv, no ključan dio jest stavljanje naglaska na količinu informacija o nekome. Kao što ćemo kasnije vidjeti, upravo je upravljanje pristupom informacijama o sebi jedna od najprihvaćenijih definicija privatnosti. Murphy je kasnije došao i do zaključka kako je važnost postojanja socijalne distance među dvoje ljudi to veća što je njihov odnos kompleksniji i teži za održavanje, a iz bilo kojeg razloga ga je potrebno održati (Murphy, 1964). Dobar dio međuljudskih odnosa u našem životu možemo odabrati. Biramo svoje intimne partnere i biramo svoje prijatelje. No, istovremeno značajnu količinu vremena provodimo u odnosu s osobama koje nismo odabrali. Roditelje, djecu, nadređene osobe i kolege ne možemo birati, a istovremeno te je odnose društveno prihvatljivo zadržati i održati. Značaj socijalne distance, odnosno količine informacija o nama kojom te osobe raspolažu, posebno je važan za uspješno održavanje odnosa. Upravo nam privatnost omogućuje da upravljamo sadržajem i količinom informacija o nama kojima drugi raspolažu i time nam omogućuje stvaranje i održavanje međuljudskih odnosa. Kao što ćemo kasnije vidjeti, kada se radi o intimnim odnosima, onima s prijateljima i intimnim partnerima, značaj privatnosti još je i veći.

Socijalni psiholog Barry Schwartz pružio je važnu perspektivu značaja privatnosti za društvo. Naime, Schwartz tvrdi kako u svakom društvu uzorke ponašanja međusobne interakcije prate i suprotni uzorci ponašanja povlačenjem iz međusobne interakcije. Prema Schwartzu, postoji prag iznad kojeg društveni kontakti postaju iritirajući za pojedinca te stoga u ustroj svakog društva moraju biti ugrađeni mehanizmi koji omogućuju pojedincu da izađe iz interakcije s drugima (Schwartz, 1968). Ova spoznaja u potpunosti slijedi iz ranije spomenutih nalaza

dobivenih na životinjama te ukazuje na to kako ljudi istovremeno uz snažnu potrebu za socijalnim kontaktima i pripadanjem imaju i potrebu za povremenim izdvajanjem iz grupe ili odnosa. Slično kao Rachels (1975), Westin (1967), te osobito Nagel (2002), i Schwartz smatra kako je privatnost ključna za uspostavu i održavanje međuljudskih odnosa i grupa, ali i za održavanje socijalnog reda i statusa. Kroz mogućnost izlaska iz neugodnih i frustrirajućih situacija dolazi do smanjenja napetosti što rezultira manjom vjerojatnosti razvijanja društvenog nezadovoljstva te osobito socijalnih nemira. Iako je Schwartz opisivao fizičko izdvajanje iz neugodne i frustrirajuće situacije, isto se može primijeniti i na psihološko i emocionalno izdvajanje. Upravo je o tome govorio Murphy kada je opisivao značaj socijalne distance za održavanje kompleksnih i zahtjevnih odnosa. Održavanje socijalne distance, bilo povremenim fizičkim udaljavanjem ili kvalitativnim i kvantitativnim smanjenjem sadržaja međusobne komunikacije, katkada može učinkovito održati zahtjevne odnose, koje je iz bilo kojeg razloga potrebno održati.

Osim toga, privatnost je privilegij osoba s većim društvenim statusom pa je tako Schwartz primijetio kako vojnici spavaju u velikim spavaonicama, dijeleći ih s više desetaka kolega, dok su dočasnici smješteni u sobama sa svega nekoliko kolega, a časnici i generali osim ostalog luksuza uživaju i u luksuzu privatnosti. Slično je i u današnjim tvrtkama gdje se društveni status osobe može vrlo dobro procijeniti na temelju privatnosti koja joj je osigurana za vrijeme radnoga dana. (Ne)kvalificirani radnici rade u halama sa desecima kolega, komercijalisti u nabavi dijele sobu s nekoliko kolega, dok mnogi direktori uživaju privatnost u prostranom uredu s pogledom na grad, zaštićeni od uznemiravanja osobnom tajnicom i zaštitarima. Uostalom, nisu li upravo sva vrata, zavjese i ladice najbolji pokazatelj naše potrebe za privatnosti?[1]

Pojedine aspekte privatnosti može se pronaći u svakom društvu, a Westinovu tvrdnju da je ona kulturalno univerzalna podržavaju i antropolozi John Roberts i Thomas Gregor u članku

[1] Puno prije Schwartza, privilegij osoba s većim društvenim statusom uočio je i Karl Marx (1976). Industrijska revolucija značajno je utjecala na ekonomske i društvene procese. Zbog toga se u devetnaestom stoljeću u političkoj misli pojavila zasebna struja mišljenja koja se usredotočila na novonastale društvene nejednakosti. Za Marxa je cijeli koncept subjektivnog individualnog prava, kako ga se opisuje u liberalnoj tradiciji, po svojoj prirodi sebičan i egoističan (Tucker, 1978). Privatnost, kao i ostala individualna prava, potrebna su nam isključivo ukoliko smatramo da bismo nekome mogli biti prijetnja. A u kapitalistički uređenom društvu i ekonomiji, ljudi si međusobno jesu prijetnja jer se natječu za komad istog, ograničenog, kolača (K. Marx, 1976). Međusobno se nadmeću za profit. No, uspostavom besklasnog društva, privatnost će, kao i mnoga druga subjektivna prava, postati nepotrebna. Prema tome, na retoričko pitanje iz prethodnog odlomka odgovor je potvrdan čak i iz Marxove perspektive, ali uz važan dodatak: Da, vrata, zavjese i ladice pokazatelj su naše potrebe za privatnosti, ali *samo zato* što smo odlučili živjeti u kapitalističkom društvu gdje se njima moramo štititi od ostalih ljudi s kojima se nadmećemo. Umjesto toga, mogli bismo društvo urediti na način da se rad i profit drugačije raspoređuju pa stoga ne bi bilo potrebe za međusobnim nadmetanjem, a time ni za subjektivnim pravima.

Privacy: A Cultural View (vidi: Moore, 2003), a u antologiji o privatnosti slično je iz pregleda literature zaključio i Schoeman (1984). Dok možemo reći kako je privatnost, barem u svojem rudimentarnom obliku, zajednička svim društvima na svijetu, postoje značajne razlike u razumijevanju i konzumiranju privatnosti među kulturama. Granica između onoga što želimo zadržati za sebe i onoga što smo spremni podijeliti s drugima te osobito načina, vremena i mjesta na kojem ćemo to napraviti razlikuje se među različitim kulturama. Međutim, postoji gotovo univerzalna potreba pojedinaca za povremenim povlačenjem u osamu, a društva koja ne uspiju osigurati barem minimalnu razinu privatnosti svojim članovima propadaju (Moore, 2003).

Privatnost je kulturološki fenomen zavisan od društva, odnosno bez društva ne postoji privatnost. Dakako, bez drugih ljudi nemamo od koga štititi sebe i informacije o sebi. Međutim, ta nas tvrdnja može navesti na pogrešni zaključak kako privatnost nije dio ljudske prirode. Kao što je, na primjer, privrženost definirana u odnosu na druge, a poznato je kako se radi o urođenoj potrebi, tako je i privatnost definirana u odnosu na druge, a zapravo se u velikoj mjeri radi o urođenoj potrebi.

Privatnost je potreba čije je zadovoljenje kulturno uvjetovano. Svaki čovjek ima potrebu za privatnosti, ali ta će se potreba u različitim kulturama kod pojedinca manifestirati na veoma različite načine. Osim toga, značajno će se razlikovati i način na koji će pojedinci zadovoljavati svoju potrebu za privatnosti kao što će postojati i značajne razlike u društvenoj prihvaćenosti ili poticanju ponašanja kojima se osigurava privatnost u pojedinoj kulturi. No, ljudi načelno žude za određenom razinom privatnosti i za određenim oblikom njezina osiguravanja. Zaštita privatnosti prepoznata je kao nužnost za sva ljudska bića, te iz toga proizlazi ideja prava na privatnost kao temeljnog ljudskog prava.

1.2. Definiranje pojma privatnosti

Pojam privatnost danas je vrlo raširen i često se koristi, kako u javnosti, tako i u literaturi. Većina nas ima vlastite intuitivne koncepcije privatnosti i načelno nam je jasno što privatnost podrazumijeva i na što se to zaštita privatnosti odnosi. Međutim, kao što je slučaj i s mnogim drugim konceptima u društvenim znanostima, spuštanje s te načelne razine na konkretniju dovodi nas do uvida kako ne postoji univerzalni konsenzus oko definicije privatnosti. Pojedini autori pomalo rezignirano tvrde kako je literatura koja opisuje privatnost *konceptualna džungla i nered* (Solove, 2008: 196, 1), dok drugi jednostavno tvrde kako se „čini da nitko nema ikakvu

jasnu viziju o tome što je privatnost“ (Thomson, 1975: 295). Pojam privatnosti koristi se kako bi označavao različite stvari poput prava, stanja, situacije, oblika kontrole, vrijednosti i povezuje ga se s ljudskim dostojanstvom, autonomijom, slobodom, vlastitim identitetom, informacijama o sebi, fizičkim kontaktom i sigurnosti. Brojne pokušaje definiranja privatnosti autori su pokušali grupirati u pet (Rössler, 2004b) ili čak šest (Solove, 2002) kategorija. Nasuprot njima, u ovom će radu, uz velika međusobna podudaranja s ostalim kategorizacijama, ti pokušaji biti grupirani u četiri kategorije.

Prva kategorija definicija obuhvaća one autore koji privatnost definiraju u terminima *mjesta* pa je tako privatno ono što je svojstveno domu. Ovakvoj definiciji skloniji su autori kojima privatnost nije primarni interes, a takva je jednostavna definicija svojstvena feminističkoj kritici privatnosti. Hannah Arendt je u knjizi *The Human Condition* govoreći o privatnoj i javnoj sferi, primijetila kako je, suprotno od današnjeg viđenja, u klasičnoj Grčkoj privatna sfera bila rezervirana za brigu o vlastitoj egzistenciji, privređivanje i ondje se vrijeme provodilo s robovima, dok su ljudska kreativnost, razmišljanje, individualnost i političnost mogli doći do izražaja tek u javnoj sferi (Arendt, 1958). U eseju *Gender and Privacy*, Beate Rössler iz feminističke perspektive uvjerljivo kritizira moderna liberalna društva zbog uparivanja dihotomije privatnog i javnog s onom spolnom, žene i muškarca, te donosi detaljan pregled literature kojom potkrepljuje svoju argumentaciju: „Srce i um, osjećaji i razum, žene i muškarci, privatni i javni život: paralele izvedene iz ovih parova suprotnosti, sa svim svojim konotacijama, tvore sastavni element u samorazumijevanju i samooblikovanju suvremenih liberalnih društava“ (Rössler, 2004a: 53). Međutim, unatoč uvjerljivoj feminističkoj kritici uparivanja žena s osjećajima, obitelji i domom, gdje je zaštićena od izloženosti javnom političkom životu, rezerviranom za muškarce, na definiranje privatnosti u terminima mjesta ne treba gledati isključivo negativno. Iris Marion Young vidi upravo mogućnost imanja vlastitoga doma, vlastitoga kutka za obitavanje, kao jedan od vrlo važnih aspekata vrijednosti privatnosti te naglašava prostorne i materijalne aspekte vrijednosti privatnosti (Young, 2005).

Druga kategorija odnosi se na definiciju koju su ponudila dva bostonska odvjetnika, Samuel Warren i Louis Brandeis, koji je kasnije imenovan sucem Vrhovnog suda SAD-a, u *eseju The Right to Privacy* (Warren i Brandeis, 1890) u kojem se prvi puta privatnost definira kao pravo, *pravo biti ostavljen na miru*. Iako je sama definicija nejasna i općenita, njihov je članak bio izuzetno utjecajan i započeo je veliku raspravu u desetljećima koja su uslijedila, a koja je rezultirala velikom produkcijom djela napisanih o privatnosti. Iako se definiciju privatnosti kao

prava biti ostavljen na miru može pronaći u popularnoj literaturi, ona se u tom obliku kasnije nije zadržala u znanstvenoj literaturi. Međutim, nedvojbeno je kako su Warren i Brandeis zadali jasan smjer razvoja koncepta te se njihov utjecaj može vidjeti u sljedećim kategorijama definicija, koje su dobrim dijelom pokušaji preciziranja njihove definicije.

Upravo jedan takav pokušaj predstavlja treća kategorija definicija u kojoj se privatnost definira u terminima *ograničenog pristupa osobi*. Ruth Gavison piše kako pojedinac uživa savršenu privatnost onda kada je u potpunosti nepristupačan drugima pri čemu to za nju podrazumijeva nepristupačnost informacijama o osobi, neobraćanje pažnje na osobu i izostanak fizičkog pristupa osobi (Gavison, 1980). Iz toga proizlazi kako pojedinac gubi privatnost kada netko spozna informacije o njemu, kada postane predmet nečije pažnje te, dakako, kada netko ostvari fizički pristup njemu. Vrlo slično privatnost definira i Anita Allen, za koju je privatnost *stanje nepristupačnosti osobe*, njezina ili njegova mentalnog stanja ili informacija o osobi osjetilima ili nadzoru drugih (Allen, 1988). Definiranje privatnosti u terminima ograničenog pristupa predstavlja vrijedan doprinos u preciziranju pojma, no i dalje se radi o vrlo širokoj i općenitoj definiciji.

Četvrtoj kategoriji valja posvetiti nešto više prostora budući da u nju spadaju brojni utjecajni autori. Pukoj, i općenitoj, (ne)mogućnosti pristupa osobi, dodana je mogućnost *kontrole* pristupa. Unatoč tome što je svim autorima u ovoj kategoriji zajedničko da njihova definicija uključuje kontrolu pristupa, postoje razlike između toga nad čime postoji kontrola pa se tako može raditi o kontroli nad informacijama o sebi (Fried, 1968; Gerstein, 1970; Posner, 1978; Westin, 1967), kontroli nad sferom intimnosti (Iness, 1992), kontroli nad pristupom osobi (Rachels, 1975) ili kombinaciji nekih od navedenih aspekata (Moore, 2003). Među autorima iz ove kategorije po utjecaju na razvoj pojma i utjecaju na ostale autore ističe se Alan Westin koji je privatnost opisao kao „mogućnost svakog pojedinca (…) da za sebe odredi na koji će način, kada, kome i do koje mjere biti prezentirani podaci o njemu“ (Westin, 1967: 5). Prema Westinu, svatko je uključen u stalni proces prilagodbe između želje za privatnosti i želje za razotkrivanjem podataka o sebi drugima, pritom uzimajući u obzir kontekst i socijalne norme društva u kojem živi. Osim na kontrolu, Westin je još veći naglasak stavio na *stalni proces prilagodbe* čime je uzeo u obzir kulturalne kao i situacijske razlike koje utječu na potrebu za privatnosti i manifestiranje ponašanja za njezinom zaštitom. Naime, to da je svatko uključen u stalni proces prilagodbe između želje za privatnosti i želje za razotkrivanjem već samo po sebi uključuje to kako će neki pojedinci biti skloniji većoj privatnosti dok će drugi biti skloniji

razotkrivanju podataka, budući da među ljudima postoje značajne razlike u osobinama ličnost i načinu doživljavanja svijeta oko sebe. Osim uzimanja u obzir dispozicijskih razlika među ljudima, stalni proces prilagodbe podrazumijeva i to da ne postoji konstantna sklonost privatnosti kod pojedine osobe, već se osoba prilagođava situacijama i okolnostima. Jednako tako, u nekim će kulturama privatnost biti više vrednovana nego u drugima pa će sukladno tome pripadnici tih kultura različito odrediti situacije u kojima će izraziti veću privatnost kao i načine na koji će to učiniti.

S druge strane, William Parent nudi strogo deskriptivnu definiciju prema kojoj je privatnost stanje u kojem drugi ne posjeduju privatne podatke o nama, odnosno ne posjeduju podatke koji već nisu na određeni način dokumentirani u javnim zapisima (Parent, 1983). Njegova je definicija problematična iz nekoliko aspekata. Naime, Parent smatra kako je do ugroze privatnosti došlo samo u slučaju kada osoba podatke o sebi nije željela otkriti nikome. Za primjer uzima djevojku koja se dobrovoljno povjerila svojoj prijateljici o određenim intimnim stvarima. Za razliku od Westina koji bi takav čin smatrao izrazom određene razine kontrole nad podacima o sebi budući da je sama odabrala kome će, kako i kada reći što o sebi, Parent smatra kako taj čin ni na koji način ne možemo smatrati očuvanjem privatnosti ili izrazom kontrole nad podacima o sebi nego upravo suprotno – razotkrivanjem svoje privatnosti. Parent ne dopušta kontrolirano otkrivanje informacija o sebi samo određenim osobama pod određenim uvjetima u određenim okolnostima, već to naziva odricanjem od privatnosti. Nadalje, prema Parentu, do ugroze privatnosti može doći samo u slučaju da se radi o nedokumentiranim podacima, odnosno o podacima koji nisu zabilježeni u javnim zapisima (Parent, 1983). Za Parenta, javni zapis podrazumijeva bilježenje podataka o osobama u tisku, ali i u različitim evidencijama i bazama podataka koje imaju elemente javne dostupnosti kao što su sudski spisi. Parent je veliki naglasak stavio na dokumentiranje podataka te je smatrao da podaci koji su jednom dokumentirani, odnosno koji su jednom postali dio javnog zapisa, više nisu privatni. Čak ni naknadno objavljivanje podataka koji su u bilo kojem trenutku u prošlosti postali dio javnog zapisa, prema Parentu, ne može se smatrati ugrozom privatnosti.

Brojni autori artikulirali su svoje poglede na privatnost upravo kroz napadanje Parenta. Moore kritiku Parenta dovodi do apsurda u primjeru osobe koja šeće parkom. Samim pokazivanjem u javnosti osoba daje na raspolaganje brojne podatke o sebi poput izgleda, približne visine i težine, boje očiju, dobi. Osim toga, u slučaju da osobi na travu javnog parka padne vlas kose, ona time javnosti nudi i podatke o svojem genetskom profilu (Moore, 2003). Dakako, ovo

cinično tumačenje pojednostavljuje Parenta, ali kritika je sasvim opravdana. Ne možemo smatrati da se osobe koje u krugu obitelji dijele intimne podatke odriču svoje privatnosti. Uostalom, Parentova definicija javne sfere u velikoj je mjeri ovisna o tehnologiji. Dramatični razvoj tehnologije za nadzor, nadziranje cijelih gradova videokamerama, prikupljanje metapodataka o svim telefonskim pozivima samo su neki od primjera povećanja dosega javne sfere u odnosu na privatnu. Sveobuhvatne baze podataka koje o svojim korisnicima vode moderne tvrtke kao i njihovo umrežavanje s bazama raznih državnih institucija, službi i agencija redefiniraju pojam javnog zapisa. Tako se čini da upravo zbog razvoja tehnologije Parentov uvid sve više dobiva na značaju. Naime, unatoč tome što Parent nije bio u pravu kada je tvrdio kako javno objavljivanje osobnih podataka koji su ranije evidentirani u pojedinoj bazi podataka ne predstavlja ugrozu privatnosti, morali bismo biti svjesni da, zbog načina na koji moderna digitalna tehnologija funkcionira, davanjem podataka u pojedinu bazu podataka te podatke zapravo činimo dostupnima velikom broju znatiželjnih očiju. Rjeđe onih bioloških, a znatno češće onih virtualnih. Iduće poglavlje posvećeno je detaljnom opisu ugroza privatnosti kao posljedici razvoja tehnologije te će u tom smislu biti prepoznat novi smisao Parentova uvida o tome kako je možda doista jednom dokumentiran podatak zauvijek prestao biti privatan.

Kao što je ranije navedeno, podjela definicija u četiri kategorije vrlo je gruba. Unatoč tome što se doista značajan dio definicija utjecajnih autora u području privatnosti može obuhvatiti jednom od ove četiri kategorije, ta je kategorizacija daleko od sveobuhvatne. Cilj kategoriziranja privatnosti na ovaj način je ilustrativne naravi i služi tome kako bi se čitatelju omogućio osnovni uvid u nastanak i razvoj koncepta te kako bi bio zadan jasan okvir unutar kojeg će se privatnost u ovom radu koristiti. Sveobuhvatan pregled pokušaja definiranja i opisivanja privatnosti seže izvan dosega ovog rada. Međutim, postojanje čitavog niza različitih definicija i pristupa privatnosti inspiriralo je dio autora, osobito onih suvremenih, na širi, integrativni pristup privatnosti koji vrijedi spomenuti. U tome se posebno ističu višedimenzionalni pogled na privatnost te kontekstualni pogled na privatnost.

Kada govorimo o višedimenzionalnom pogledu na privatnost, put drugim autorima utabao je Westin opisavši različita stanja privatnosti. On je u svojem radu razlučio četiri osnovna stanja: *samoću*, kao stanje u kojem je pojedinac izdvojen iz grupe i slobodan od opažanja drugih ljudi; *intimnost*, koja se odnosi na mogućnost pojedinca da se kao dio manje jedinice izdvoji kako bi ostvario bliske, opuštene i iskrene donose između dvije ili više osoba; *anonimnost*, kao mogućnost sudjelovanja u javnom prostoru i u javnim aktivnostima slobodan od identifikacije

i nadzora; te posljednje i najsuptilnije stanje *zadršku*, koja se odnosi na stvaranje svojevrsne psihološke brane od neželjene intruzije, a odnosi se na uskraćivanje određenih podataka o sebi koje može biti i u odnosu s bliskim i dragim ljudima (Westin, 1967:33–35). Westinov rad dalje je inspirirao niz ideja i različitih klasifikacija privatnosti, a na temelju njihova detaljnog pregleda Burgoon je ponudila svoju klasifikaciju u četiri dimenzije: *fizičku privatnost*, definiranu kao slobodu od nadzora i neželjenog pristupa nečijem osobnom prostoru i tijelu; *društvenu ili interakcijsku privatnost*, definiranu kao mogućnost odabira s kime će, kada, kako i što dijeliti; *psihološku privatnost*, definiranu kao zaštitu nečijih misli, osjećaja, stavova i vrijednosti, kao zaštitu od persuazije, neželjenog uvjeravanja, vrijeđanja i drugih spoznajnih manipulacija te konačno *informacijsku privatnost*, kao mogućnost kontrole tko, i pod kojim okolnostima, može prikupljati i širiti podatke o osobi (Burgoon, 1982; Burgoon et al., 1989:132–134). I sama Burgoon ustvrdila je kako između njezinih dimenzija postoji određeno teoretsko preklapanje, a provedenim empirijskim istraživanjem povreda privatnosti specificiranih u okviru zadanih dimenzija pokazala je kako je tek fizička privatnost značajnije različita od ostalih te kako su psihološka i informacijska privatnost blisko povezane (Burgoon et al., 1989). Za Moorea, privatnost je definirana kao mogućnost pristupa više domena. On je razgraničio tjelesnu i informacijsku privatnost te je zaključio kako je tjelesna privatnost, definirana kao pravo na kontrolu pristupa vlastitome tijelu, jedno od najuvaženijih prava uklesano u pravnu regulativu kao i u opći moral. Međutim, informacijska privatnost, definirana kao pravo na kontrolu pristupa informacijama o sebi, tek treba dostići taj uzvišeni status (Moore, 2003). Iako i Moore na privatnost gleda u terminima kontrole pristupa, značaj njegova pogleda je u diferenciranju između različitih dimenzija, različitih domena privatnosti.

Slično kao i Burgoon osamdesetih godina prošloga stoljeća, tridesetak godina kasnije pravni stručnjak za pitanja privatnosti Daniel Solove našao se zatečen različitim definicijama i načinima na koje ljudi doživljavaju privatnost. Prema njemu, upravo je nepostojanje jasne definicije koncepta privatnosti doprinijelo slabijoj pravnoj zaštiti privatnosti, ali i tome da su i sami pojedinci manje zabrinuti za ugroze vlastite privatnosti (Solove, 2008). Njegov pristup tom problemu bio je nešto drugačiji od dotadašnjih značajnijih pokušaja. Za razliku od traženja zajedničkog nazivnika za konceptualiziranje privatnosti na apstraktnoj razini, Solove se založio za pristup *odozdo-prema-gore* (Solove, 2002). Njegova namjera nije bila ponuditi sveobuhvatnu teoretsku definiciju privatnosti već je pragmatično želio podignuti uporabnu vrijednost koncepta privatnosti kako bi ga se lakše moglo pravno zaštititi te kako bi ljudima

bilo lakše prepoznati vrijednost privatnosti i prepoznati situacije u kojima je njihova privatnost ugrožena. Gradeći na temeljima utjecajne taksonomije delikata privatnosti Williama Prossera (Prosser, 1960), Solove je kroz kritiku njegove taksonomije (Richards i Solove, 2010) te proširivanje fokusa s delikata na znatno šire i kompleksnije polje pravnih tekstova i dokumenata ponudio vlastitu taksonomiju (Solove, 2006). Budući da Solove nije imao pretenzija definirati koncept privatnosti, niti je to u konačnici učinio, te da je bio primarno usredotočen na pravni aspekt (zaštite) privatnosti, njegova taksonomija bit će prikazana nešto kasnije. No, ključan doprinos njegova razumijevanja privatnosti jest odmak od višedimenzionalnog pogleda na privatnost ka kontekstualnom pogledu na privatnost.

Kontekstualni pogled na privatnost može se prepoznati već u Westinovoj definiciji privatnosti kao mogućnosti svakog pojedinca da za sebe odredi na koji će način, kada, kome i do koje mjere biti prezentirani podaci o njemu (Westin, 1967). Kao što definicije imaju nedostatak utoliko što su nerijetko apstraktne, tako konkretni prikazi imaju nedostatak utoliko što su nerijetko preuski te ih je stoga lako odbaciti kao neodgovarajuće. Solove je tome pokušao doskočiti na način da privatnost smatra kišobran-pojmom kako bi pod taj kišobran mogao staviti što više elemenata koji čine privatnost, a bez nužnog pronalaženja zajedničkog nazivnika više razine apstrakcije (Solove, 2006). Sasvim drugi pristup kontekstualnoj konceptualizaciji privatnosti predstavila je Nissenbaum. Ona je odbacila i ideju kako je privatnost pravo na kontrolu nad osobnim podacima i ideju kako je privatnost pravo ograničavanja pristupa osobnim podacima te je privatnost definirala kao *pravo da naša očekivanja o toku osobnih podataka u većoj mjeri budu uvažena* (Nissenbaum, 2010). *Kontekstualni integritet*, kako je to pravo nazvala Nissenbaum, postiže se kroz usklađivanje i prilagodbu društvenih i pravnih normi, osobnih i općih vrijednosti s ciljevima i načinima postizanja tih ciljeva. Njezina operacionalizacija kontekstualnog pogleda na privatnost predstavlja pronicljiv i vrijedan doprinos, a kontekstualni integritet osobitu vrijednost ima u mogućnosti prilagodbe konceptualizacije privatnosti sve brže rastućim novim tehnologijama koje predstavljaju izazov za zaštitu privatnosti. No, unatoč tome što koncept kontekstualnog integriteta predstavlja inspirativan pogled na privatnost te unatoč tome što ga je Nissenbaum vrlo dobro razradila te ga je kroz teoretsku raspravu suočila s mnogim kritikama, vrlo ga je teško primijeniti na svakodnevne situacije te će u tome smislu ostati na razini utopije sve dok se ne razviju konkretni modeli njegove primjene. Psiholog Tobias Dienlin doktorirao je 2017. godine postuliravši *model procesa privatnosti* kao jedan kontekstualni pogled na privatnost (Dienlin, 2017). Prema

tom modelu, postoje tri ključna segmenta: *kontekst privatnosti*, *percepcija privatnosti* i *ponašanje*. Prema modelu, svaka situacija u kojoj se pojedinac nalazi predstavlja *kontekst privatnosti* i ona dovodi do određenog osjećaja intimnosti i povjerljivosti, odnosno do *percepcije privatnosti*, ovisno o kojoj ljudi manifestiraju više ili manje otkrivajuće *ponašanje*. Za svaku percepciju privatnosti kao i za ponašanje, ljudi uspoređuju trenutnu razinu privatnosti s onom željenom te ukoliko među njima postoji diskrepancija pristupaju regulaciji privatnosti na način da ili utječu na promjenu konteksta, odnosno izlaze iz određene situacije, ili utječu na ponašanje, odnosno povećavaju ili smanjuju razinu otkrivanja (Dienlin, 2017). Dienlin je model testirao u nekoliko empirijskih istraživanja te je pronašao potvrdu za njegove temeljne postavke (Dienlin i Trepte, 2015; Trepte, Dienlin i Reinecke, 2014). Njegov model predstavlja jednu uspješnu operacionalizaciju temeljne Westinove ideje o kontekstualnom pogledu na privatnost.

U ovom odjeljku pružen je kratki teoretski i povijesni pregled konceptualizacija privatnosti. Iako svaka od navedenih kategorija definicija pruža vrijednu perspektivu razumijevanju koncepta privatnosti, najviše prostora posvećeno je konceptualizaciji privatnosti u terminima kontrole budući da to odražava njezinu prisutnost i značaj u literaturi o privatnosti, ali i zbog toga što je ona najbliža razumijevanju privatnosti u okvirima ovog rada. Prema tome, privatnost će u ovom radu biti definirana kao mogućnost kontrole pristupa (podacima o) sebi.

Upravo je kontrola ključan dio definicije privatnosti. To što netko posjeduje kontrolu istovremeno znači da posjeduje slobodu izbora, ali i mogućnost upravljanja onime nad čime ima kontrolu. Govoreći o kontroli u terminima pristupa sebi, informacijama o sebi ili vlastitoj intimi, stavljamo osobu u središte njezina autentičnog postojanja. Kontroliranje pristupa sebi dio je osobne autonomije, slobode odabira tko će, kada, koliko i kako pristupiti (podacima o) nama, a mogućnost odabira hoćemo li, kome i kada otkriti sebe, nužna je za uspostavljanje i održavanje intimnih veza. No, značaj privatnosti za osobnu autonomiju pojedinca i mogućnost uspostave i održavanje intimnih veza predstavlja tek jedan dio pogleda na vrijednost privatnosti. Sljedeći odjeljak pružit će pregled različitih tumačenja značaja i vrijednosti privatnosti te će ponad deskriptivne definicije biti razmotreni i normativni aspekti privatnosti.

1.3. Razvoj poimanja privatnosti i njegova društvenog vrednovanja

Jednom kada je privatnost definirana, odnosno kada je pružen dovoljno uzak okvir unutar kojega se privatnost u ovom radu razumijeva, postavlja se pitanje značaja i vrijednosti

privatnosti. S normativnog aspekta, pitanje je radi li se o pozitivnoj ili negativnoj pojavi te u čemu je sadržana vrijednost ili štetnost privatnosti? Kako bismo mogli pristupiti daljnjoj argumentaciji koja predstavlja temelj ove disertacije, najprije je potrebno dati jasan odgovor na pitanje vrijednosti privatnosti.

Inspirirano načelnom podjelom koju je ponudio Schoeman (1984), a u svrhu isticanja vlastita pogleda na značaj privatnosti, argumenti su ugrubo podijeljeni u tri kategorije. Jedna skupina autora među kojima se ističu Benn (1971), Bloustein (1984), Gavison (1980), Reiman (1976) i Rössler (2006), značaj privatnosti vidi u njezinoj povezanosti s ljudskim dostojanstvom, s temeljem iz kojeg proizlaze ljudska prava. Oni naglasak stavljaju na osobu, individuu koja ostvaruje svoja prava biti ostavljen na miru, realizirati se, slobodno djelovati. S druge strane, značajna je skupina autora koji smatraju kako privatnost ima središnju ulogu u ostvarivanju i održavanju različitih međuljudskih odnosa (Fried, 1968; Gerstein, 1978; Rachels, 1975). Ti su autori prvenstveno usmjereni na način na koji pojedinac razumije sebe kao društveno biće te razmišljaju o utjecaju privatnosti na društvo. Posljednja, no ne i zanemariva, skupina autora su oni koji na kritički način razmišljaju o privatnosti bilo na način da su tek skeptični prema većoj zaštiti privatnosti, bilo da ne vide moralna i vrijednosna opravdanja za zaštitu privatnosti (Allen, 2003; Etzioni, 2004; MacKinnon, 1989; Posner, 1978), ili pak da uopće ne smatraju kako je privatnost koherentan pojam kojeg se može koristiti u akademskim raspravama (Thomson, 1975).

1.3.1. Privatnost i dostojanstvo

Ljudsko dostojanstvo nepovrediv je temelj svake osobe te predstavlja osnovu iz koje proizlaze temeljna ljudska prava. Već u prvoj rečenici preambule Opće deklaracije o pravima čovjeka Ujedinjenih naroda stoji kako je „priznavanje urođenog dostojanstva i jednakih i neotuđivih prava svih članova ljudske obitelji temelj slobode, pravde i mira u svijetu“ (United Nations, 1948: 1).

Moderno poimanje privatnosti počelo je s pravnim tekstovima, još 1890. godine člankom Warrena i Brandeisa, a nešto kasnije posebno je utjecajan bio rad dekana pravnog fakulteta na Berkleyu William Prossera koji je kulminirao objavom njegove taksonomije delikta kršenja privatnosti 1960. godine. Dok su Warren i Brandeis u zaštiti privatnosti vidjeli nešto uzvišeno i povezano s *nepovredivom osobnosti* svakoga čovjeka (Warren i Brandeis, 1890), Prosser je zaštitu privatnosti sveo na nekoliko delikata kojima se ponajprije štitilo ugled, nematerijalno

vlasništvo te emocionalno i mentalno blagostanje (Prosser, 1960). Zbog njegova utjecaja kao dekana Berkleya, ali i stoga što je taksonomiju uspostavio upravo temeljem dotadašnje sudske prakse, Prosserova taksonomija delikata imala je velik odjek i brzo je prihvaćena među američkim sucima i pravnim stručnjacima (Solove i Richards, 2007). Prosserov je rad konceptu privatnosti dao upravo onu razinu pravne opipljivosti koja je bila potrebna kako bi je se u praksi počelo štititi, ali je istovremeno kontroverzan zbog toga što je u njegovom radu bio sadržan skeptični, redukcionistički pogled na privatnost koji je zaštitu privatnosti sveo na puki delikt, čime je bilo otežano i usporeno prepoznavanje privatnosti kao znatno šireg pravnog koncepta tj. temeljnog ljudskog prava. Međutim, upravo zbog te kontroverze, Prosserov je rad inspirirao pravne i druge stručnjake na kvalitetniju, dublju i sadržajniju obranu privatnosti kao temeljnog ljudskog prava. No, najbolje je krenuti od samoga početka.

Esej o privatnosti Warrena i Brandeisa jedan je od najcitiranijih znanstvenih članaka u pravnoj znanosti, a čini se da je sve započelo s osobnom pričom. Naime, tada mladi i relativno nepoznati odvjetnik Warren oženio je Mabel Bayard Warren, najstariju kćer vrlo utjecajne senatorice Delawarea. Njihovo vjenčanje u siječnju 1883. godine detaljno su popratile brojne novine u New Yorku i Washingtonu (Lane, 2009). Detaljni pregled šezdesetak članaka objavljenih o Warrenu i njegovoj obitelji, daju jasan uvid u moguće povode koji su mogli utjecati na njegovu motivaciju da napiše esej o potrebi za pravnom zaštitom privatnosti (Gajda, 2007). Po svemu sudeći, Warren se teško mirio s razmjerom kojim su novinari pratili život njegove obitelji, a pojava žutog tiska i trač rubrika koje su na senzacionalistički način pratile privatna druženja njegove supruge, predstavljali su točku preokreta te je tada Warren zajedno sa svojim prijateljem započeo pisati poznati esej. Osim toga, iz njihova eseja jasno se može iščitati i zabrinutost zbog pojave i širenja novih tehnologija, osobito pojave fotografske opreme, za koju su smatrali da bi mogla dodatno ugroziti privatnost (Warren i Brandeis, 1890).

U svojem eseju o privatnosti, Warren i Brandeis upozorili su kako tadašnje suvremene kompanije kao i novi izumi kroz narušavanje privatnosti mogu izložiti čovjeka psihološkoj boli znatno većoj nego što je proizvode tjelesne ozljede (Warren i Brandeis, 1890). Kritike njihova pogleda na privatnost dominantno su usmjerene prema tome da nigdje nisu definirali što točno za njih znači privatnost, čime su otvorili prostor za preširoko tumačenje povreda privatnosti (Kalven, 1966) te prema njihovoj kritici medijskih objava *točnih* podataka o (javnim) osobama (Richards, 2015), za koju Richards smatra kako je prešla granicu prihvatljivog utjecaja na slobodu tiska.

Njihov članak je prvenstveno pravni tekst u kojem daju svoj doprinos definiranju prava na privatnost kroz pravila i pravnu terminologiju. Warren i Brandeis praktički su započeli nezaustavljivu raspravu o pravu na privatnost i omogućili su stvaranje uvjeta za zaštitu toga prava. O privatnosti su govorili prvenstveno u terminima informacijske privatnosti, odnosno zadržavanja informacija o sebi privatnima. No, unatoč tome što u tekstu privatnost nigdje nisu eksplicitno definirali, ponudili su svoj pogled na privatnost te su, još važnije, značajan dio teksta posvetili obrazlaganju zašto smatraju da je ona vrijedna zaštite. Upravo je najveći doprinos njihova članka bio u tome što su istaknuli moralne razloge za zaštitu privatnosti, a koje su vidjeli u povezanosti privatnosti s takozvanom *nepovredivom osobnosti* (Warren i Brandeis, 1890), čime su sugerirali kako privatnost ima značaj za najdublje temelje ljudske psihe, za ono što nas čini onima koji jesmo. Iz toga onda razumljivo proizlazi i njihov poziv za zaštitom privatnosti.

Ako su Warren i Brandeis povredama privatnosti postavili temelje, onda možemo reći kako im je Prosser dao formu i kredibilitet (Richards i Solove, 2010). Naime, Prosser je više desetljeća proučavao delikte, među kojima je značajan dio karijere posvetio upravo deliktu kršenja privatnosti. Od 1940.-ih godina, kada je počeo proučavati delikte kršenja privatnosti, sljedećih tridesetak godina proveo je u pokušaju razumijevanja i kategoriziranja stotina sudskih slučajeva koji su predstavljali neki oblik povrede privatnosti (Richards, 2015). Na temelju više od tristo analiziranih slučajeva, Prosser je zaključio kako ne postoji jedinstveni oblik povrede privatnosti, kao što su opisali Warren i Brandeis, već je zaključio kako se radi o četiri različite negativne povrede, odnosno, delikta kršenja privatnosti: *intruzija, javno sramoćenje objavljivanjem osobnih podataka o oštećeniku, publicitet koji osobu u javnosti predstavlja u lažnom svjetlu* te *prisvajanje* (Prosser, 1960). Intruziju je Prosser opisao kao upad u nečije stanje izdvojenosti ili u njihova privatna pitanja, a mogla bi se ilustrirati na primjeru djevojke koja se presvlači u svlačionici, a nepoznati muškarac otvori vrata njezine svlačionice. Međutim, ovaj oblik ugroze privatnosti u širem smislu obuhvaća i postavljanje opreme za audio i/ili video snimanje nečijeg prostora i slično. Prema Prosseru, primarna namjera uspostave ovog delikta bila je zaštiti osobu od mentalnog uznemiravanja. Javno sramoćenje objavljivanjem osobnih činjenica može se ilustrirati primjerom objavljivanja fotografija preljuba lokalnog pekara s automehaničarevom kćeri. Prosser je istaknuo kako je nužno da objava mora biti javna, a ne dio privatnih tračeva ili ogovaranja te da objavljene činjenice moraju biti doista privatne naravi. Napravio je i distinkciju između javnih osoba, koje su ne samo prihvatile živjeti pod povećalom javnosti nego u pravilu i žive od te pažnje, i običnih građana koji žele zadržati svoju privatnost

za sebe. Ovim je deliktom želio zaštititi ugled i osigurati zaštitu od emocionalnog uznemiravanja. Publicitet koji osobu u javnosti predstavlja u lažnom svjetlu može se opisati primjerom objave fotografije policajca koji regulira promet uz novinsku vijest o tome kako su određeni policajci prekoračili svoje ovlasti prilikom postupanja te su pripadniku nacionalne manjine nanijeli teške tjelesne ozljede. Slično kao i s prethodnim deliktom, i ovim je deliktom prvenstveno želio zaštititi ugled i osigurati zaštitu od emocionalnog uznemiravanja. Četvrti delikt, prisvajanje, nešto je drugačiji od prethodna tri i odnosi se na korištenje imena ili lika osobe bez njezina pristanka radi ostvarivanja određene koristi. Prosser je pri opisivanju ovog oblika ugroze uglavnom koristio tadašnje primjere kada su fotografije poznatih osoba korištenje za reklamiranje određenih proizvoda bez njihova pristanka. Ovim se deliktom manje pretendiralo zaštititi mentalno blagostanje, već je primarni interes bio zaštititi vlasništvo osobe i njezina materijalna prava (Prosser, 1960).

Za razliku od Warrena i Brandeisa, koji su privatnosti pristupili na način da su željeli opisati situacije i slučajeve koje *bi* sudovi *trebali smatrati* povredama privatnosti, Prosser je imao potpuno suprotni pristup – on je svoju kategorizaciju utemeljio na situacijama i slučajevima koje sudovi *jesu smatrali* povredama privatnosti (vidi Schoeman, 1984). Stoga ne treba čuditi što su došli do različitih zaključaka o tome što je ugroženo povredama privatnosti. Dok su Warren i Brandeis u zaštiti privatnosti vidjeli nešto uzvišeno i povezano s *nepovredivom osobnosti* svakoga čovjeka, Prosser je zaštitu privatnosti sveo na nekoliko delikata kojima se ponajprije štitilo ugled, nematerijalno vlasništvo te emocionalno i mentalno blagostanje. Richards i Solove prepoznali su i priznali Prosserov značajan doprinos uspostavi i razvoju prava na privatnost, međutim istovremeno su istaknuli kako je on ujedno i jedan od najvećih krivaca za to što se pravo na privatnost toliko sporo razvija i ne uspijeva se uskladiti s modernim tehnologijama i izazovima (Richards i Solove, 2010). Zbog usmjerenosti na prošle slučajeve umjesto na vrijednosti koje je potrebno zaštiti, kao i njegove očigledne redukcionističke pozicije uspostavio je preusku kategorizaciju od svega četiri moguća oblika ugroze prava na privatnost bez ideje za budući razvoj koncepta zbog čega je u današnjem informacijskom dobu zaštita prava na privatnost praktički potpuno neučinkovita (Solove, 2004). U svojoj taksonomiji, Prosser je u potpunosti zanemario vrijednosni aspekt zaštite privatnosti, koji su Warren i Brandeis nedvojbeno jasno izrazili. Richards i Solove uvjereni su kako je Prosser to namjerno učinio znajući da će, zbog načina na koji pravosudni sustav i pravna znanost u SAD-u funkcioniraju, u konačnici njegova naizgled isključivo deskriptivna taksonomija zapravo

negativno utjecati na razvoj i prihvaćanje privatnosti kao temeljnog ljudskog prava (Solove i Richards, 2007).

Međutim, kontroverze koje je izazvao Prosserov rad imale su i pozitivan učinak budući da su se kroz kritiku njegova rada razvili kvalitetno razrađeni i vrijedni argumenti za zaštitu privatnosti. Jedan od prvih koji je reagirao na Prosserovu usku taksonomiju i redukcionistički pristup privatnosti bio je Edward Bloustein koji se već 1964. godine direktno referirao na njegov rad. Bloustein je opisao veliku pravosudnu i teorijsku pomutnju koja je nastala oko zaštite prava na privatnosti, citirajući jednoga američkoga federalnoga suca, kao „stog sijena u uraganu" te je odlučio ponuditi vlastitu opću teoriju individualne privatnosti kako bi „vratio slamke natrag u stog sijena" (Bloustein, 1984: 962). Prema njemu, sve je kulminiralo 1960. godine objavom rada dekana Prossera kojemu je, osim zbunjivanja sudova, zamjerio narušavanje osnovnog znanstvenog načela parsimonije jer nije preferirao jedno opće objašnjenje nad kombinacijom različitih pravila te činjenicu da Prosser nije ostavio odgovarajući prostor za prilagodbu privatnosti novim tehnoloških izazovima (Bloustein, 1984).

Detaljno je analizirao i secirao Prosserov rad te ga je uspoređivao s radom Warrena i Brandeisa. Posebno se usmjerio na kontekst i njihove motive za pisanje o privatnosti. Utvrdio je kako su Warren i Brandeis doista u više navrata govorili o uznemirenosti koju naklapanje i trač može izazvati u ljudi. Uostalom, i u ovom je radu izdvojeno njihovo upozorenje kako narušavanje privatnosti može izložiti čovjeka psihološkoj boli znatno većoj nego što je proizvode tjelesne ozljede (Warren i Brandeis, 1890). To naizgled ide u prilog Prosserovom stavljanju naglaska na zaštitu od emocionalne uznemirenosti u čak tri od četiri njegova delikta kršenja privatnosti. Međutim, Bloustein tvrdi kako je Prosser, svevši privatnost na puke povrijeđene osjećaje, pogrešno protumačio Warrena i Brandeisa te ističe kako su oni u pojašnjavanju onoga što vide povredom jasno i eksplicitno razdvojili povredu privatnosti kao „čin pogrešan u svojoj biti" od „mentalne patnje" kao posljedice te povrede (Bloustein, 1984: 966).

Kao osnovni princip kojim su to opravdali Bloustein je izdvojio upravo *nepovredivu osobnost.* Nju je vidio kao termin koji predstavlja samostalnost pojedinca, njegovo dostojanstvo i integritet te ga definira kao samoodređujuće biće. Smatrao je kako su Warren i Brandeis svoj rad napisali iz straha da bi obijesno medijsko hranjenje privatnim životom pojedinaca moglo uništiti njihovo dostojanstvo i integritet te osakatiti individualne slobode i nezavisnost (Bloustein, 1984: 969). Stoga je detaljno analizirao Prosserovu taksonomiju te je za svaki

pojedini delikt vrlo uvjerljivo na primjeru brojnih sudskih slučajeva pojasnio zašto smatra da je ugroženo ljudsko dostojanstvo, a ne tek ugled[2], povrijeđeno vlasništvo ili izazvana uznemirenost. Iz toga proizlazi kako se u slučajevima na temelju kojih je Prosser konstruirao svoju taksonomiju zapravo radi o jednom jedinom deliktu kršenja privatnosti u čijoj je podlozi povreda ljudskog dostojanstva (Bloustein, 1984). Značaj privatnosti za Blousteina možda je najbolje dočarati kroz njegov opis čovjeka koji je izgubio privatnost:

> Čovjek koji je primoran u svakom trenutku živjeti među drugima i čija je svaka potreba, misao, želja, fantazija ili zadovoljstvo predmet javnog nadzora, lišen je osobnosti i ljudskog dostojanstva. Takav pojedinac stapa se s masom. Nakon što su postala javna, njegova mišljenja gube tendenciju biti drugačijima. Nakon što su postale javne, njegove težnje imaju tendenciju uvijek biti one konvencionalno prihvaćene. Nakon što su postali otvoreno izloženi, njegovi osjećaji gube jedinstvenosti i osobnu toplinu i postaju osjećaji svakog čovjeka. Takvo biće, iako živo, potpuno je zamjenjivo; ono nije osoba (Bloustein, 1984: 188)

Kritike Blousteinova pogleda usmjerene su, očekivano, prema tome kako su koncepti poput ljudsko dostojanstvo, individualnost i samoodređenje široki i nejasni, slično kao *nepovrediva osobnost* i *pravo biti ostavljen na miru* u radu Warrena i Brandeisa (Gavison, 1980; Richards i Solove, 2010). Doduše, i sam se Bloustein djelomično ogradio od kritika upozorivši kako ne predstavlja svaka prijetnja privatnosti dovoljnu ugrozu da bi zahtijevala pravnu zaštitu te kako kao pripadnici društva moramo moći biti podvrgnuti određenoj razini javne prosudbe (Bloustein, 1984).

Stanley Benn vrijednost privatnosti vidio je u njezinoj povezanosti s osobnom autonomijom i slobodom (Benn, 1971). Pošao je od toga da su ljudi racionalne jedinke koje imaju mogućnost odabira i upravljanja svojom sudbinom te imaju osobnu perspektivu svijeta. Upravo zbog te dvije sposobnosti smatrao je da ljudi zavrjeđuju zaštitu privatnosti. Naime, kao liberal prepoznao je tri ideala vrijedna zaštite, a za koje je smatrao da je preduvjet postojanje privatnosti. Prvi ideal je uspostava međuljudskih odnosa za koju je smatrao da je privatnost važna jer omogućuje različite socijalne uloge nužne za ostvarivanje tih odnosa, no o tome će mnogo više riječi biti u sljedećem ulomku. Drugi je svojevrsni lockeovski ideal slobodnoga građanina koji je slobodan od uplitanja u njegov život čime mu je omogućeno da slobodno i neovisno donosi životne odabire. Konačno, kao treći ideal, Benn je istaknuo kantovski ideal

[2] Ugled predstavlja procjenu karaktera osobe temeljem procjene drugih ljudi, a u nešto širem smislu i razinu prepoznavanja koju osobi pridaju drugi ljudi. S druge strane, dostojanstvo predstavlja neotuđivo inherentno pravo svakog pojedinca da ga se vrednuje, uvažava i poštuje.

(moralno) autonomnog čovjeka. Zaštita od petljanja drugih u našu intimu nužna je za stvaranje uvjeta za nastanak nezavisne misli, kao i kasnije za njezin razvoj i opstanak.

U viđenju značaja privatnosti za autonomiju i slobodu pojedinaca, Benn nipošto nije usamljen. Vrlo slično, Reiman ističe kako pravo na privatnost omogućuje pojedincu da postane, bude i ostane osoba (Reiman, 1976). Za njega je privatnost ključni dio „kompleksne društvene prakse kojom se pojedincu daje do znanja kako je njegovo postojanje isključivo njegovo“ (Schoeman, 1984; 21), što je preduvjet osobnosti. U nešto novijem članku, Reiman je pružio izvrstan pogled na vrijednost privatnosti kroz opisivanje četiri rizika kojima se izlažemo u slučaju da naši životi postanu u potpunosti vidljivi drugima (Reiman, 1995). Pod *rizikom od ekstrinzičnog gubitka slobode* Reiman je prvenstveno smatrao utjecaj na pojedince preko društvenog pritiska. Osobama koje čine nepopularne ili neuobičajene stvari mogle bi biti uskraćene dobrobiti poput radnog mjesta, napredovanja ili članstva u formalnim i neformalnim grupama te bi stoga bile sklone korigirati svoje ponašanje. Dakako, značajnu ulogu u mogućnosti odupiranja društvenom pritisku igra ličnost osobe te će samopouzdanije osobe trebati manje privatnosti kako bi se ostvarile, ali Reiman dobro primjećuje kako je za stvaranje takve snažne, samopouzdane ličnosti bila potrebna privatnost (Reiman, 1995). Na tom su tragu i drugi autori poput Blousteina ili Gersteina, koji privatnu sferu vidi kao sredstvo koje im omogućuje formiranje nezavisnih prosudbi o društvenim normama koje ujedno i sprječavaju da ih te norme apsorbiraju (Gerstein, 1978). Drugi rizik Reiman je nazvao *rizikom od intrinzičnog gubitka slobode*, a za razliku od svjesne autocenzure koja je sadržana u prethodnom riziku, ovdje se radi o gubitku spontanosti kroz internalizaciju i nesvjesno konformiranje društvenim normama. Kao što je ranije navedeno, za Reimana privatnost je svojevrsni društveni ritual kojim se pojedincu daje na značaju kao jedinstvenoj osobi, vlasniku sebe, svojega tijela i svojih misli, a ti simboli omogućuju stvaranje i razvoj autonomnih pojedinaca. Život bez privatnosti ljude bi izložio takozvanim *simboličkim rizicima* jer bi im bilo sve teže pojmiti sebe kao isključive vlasnike sebe samih. To znači da bi pojam *posjedovanja* izgubio na značaju i vrijednosti, a u domeni misli i identiteta to može imati zastrašujuće posljedice. Ne radi se o tome da bismo time „izgubili nešto što trenutno uživamo, nego bismo postali netko drugačiji od onoga tko smo sada“ (Reiman, 1995: 40). Na tom je tragu i posljednji rizik koji Reiman naziva rizikom od *psihopolitičke metamorfoze* i ovaj je rizik najvažniji. Reiman polazi od ranije istaknutog Blousteinova zastrašujućeg citata o tome kakvim postaje čovjek lišen privatnosti te ga nadograđuje političkim elementima. Osim gubitka osobnosti i otupljivanja emocija, Reiman

tvrdi kako se bez privatnosti gubi *unutarnja osobna jezgra* koja je izvor kritičnosti prema konvencijama, izvor kreativnosti, pobune i obnove. „Kazati da će osobe lišene privatnosti biti lako ugnjetavati, malo je za reći“ (Reiman, 1995: 42). Benn je govorio o važnosti privatnosti za razvoj nezavisne misli i autonomnih pojedinaca, koji bi imali kapacitet kritičkog sagledavanja svijeta, umjesto slijepog upijanja misli, stavova, želja i osjećaja. Cijela liberalna paradigma zapravo se oslanja na postojanje autonomnih pojedinaca koji mogu nezavisno donositi svoje vlastite prosudbe. Na tom je tragu Ruth Gavison koja ističe kako je privatnost nužna za demokratsku vladavinu jer njeguje i potiče moralnu autonomiju građana te kako pojedinci mogu u potpunosti ostvariti svoju slobodu tek ako imaju pravo i mogućnost u privatnosti zadržati svoje političke preferencije i stavove (Gavison, 1980). Ne postoji bolji način za zaokružiti ovu cjelinu od citata Beate Rössler, koji u ovom kontekstu funkcionira i bez komentara:

> Ako je normativna povezanost između autonomije i privatnosti točna, onda je ravnodušnost prema privatnosti istovremeno i ravnodušnost prema autonomiji. A demokracija se oslanja na pojedince koji vrednuju svoju autonomiju, kako javno tako i privatno. Stoga su prijetnje privatnosti uvijek ujedno i prijetnje demokraciji. (Rössler, 2006: 709)

1.3.2. Privatnost i međuljudski odnosi

Poput autora spomenutih u prethodnom dijelu, i Charles Fried smatrao je kako je privatnost temeljna za moralni i društveni razvoj pojedinca, kao i za osobnu slobodu. No, on je prepoznao i drugu vrijednost privatnosti. Smatrao je kako je jednako temeljna i za sposobnost razvijanja intimnih veza utemeljenih na poštovanju, ljubavi, prijateljstvu i povjerenju (vidi Schoeman, 1984). Zapravo, njegova je teza bila da privatnost nije samo jedan od načina na koji se temelji međuljudskih odnosa mogu razvijati već je tvrdio kako su oni bez privatnosti jednostavno nezamislivi (Fried, 1968: 478). Dakako, Fried je u pravu. Bez privatnosti, bez mogućnosti reguliranja i upravljanja podacima o sebi, bez mogućnosti da neke misli, dojmove i uvjerenja zadržimo samo za sebe ili samo za uzak krug ljudi, jednostavno ne bismo mogli ostvarivati intimne odnose. Milan Kundera je nepodnošljivom lakoćom u svojem najpoznatijem romanu opisao upravo ono o čemu Fried govori:

> Kada se privatni razgovor uz bocu vina emitira na radiju, što to može značiti osim da se svijet pretvara u koncentracijski logor? (Kundera, 1987: 136)

Nešto kasnije, svoj argument detaljnije je pojasnio u eseju *Testaments Betrayed: An Essay in Nine Parts*:

> Pisao sam o tome u Nepodnošljivoj lakoći postojanja: Jan Prochazka, važna figura Praškog proljeća, došao pod teški nadzor nakon ruske invazije 1968. U to vrijeme, prepoznao je drugog pripadnika oporbe, profesora Vaclava Gernya, s kojim je volio piti i razgovarati. Svi njihovi razgovori bili su tajno snimljeni, a sumnjam kako su dvojica prijatelja za to znali i nije ih bilo briga. Međutim, jednoga dana 1970. ili 1971. godine, s namjerom da se Prochazku diskreditira, policija je počela emitirati njihove razgovore kao radijski serijal. Za policiju je to bio odvažan čin bez presedana u to vrijeme. I začudo, gotovo da je i uspio; Prochazka je trenutno bio diskreditiran; jer u privatnosti čovjek kaže svakakve stvari, ogovara prijatelje, psuje, djeluje glupo, zbija prljave šale, ponavlja se, nasmijava sugovornika šokirajući ga nečuvenim izjavama, nabacuje ideje i mišljenja koja nikada ne bi priznao u javnosti i tako dalje. Naravno, svi se ponašamo kao Prochazka, u privatnosti ogovaramo prijatelje i psujemo; djelovati drugačije u privatnosti nego u javnosti svakome je itekako poznato iskustvo, to je temelj života pojedinca; Zanimljivo, ova očita činjenica ostaje neosviještena, nepriznata, zauvijek skrivena lirskim snovima prozirnoj staklenoj kući, i rijetko se smatra vrijednosti koju valja braniti iznad svih ostalih. Ljudima je trebalo mnogo da shvate kako pravi skandal nije Prochazkin smion govor o životnom silovanju; Shvatili su (kao da su doživjeli strujni udar) da su privatno i javno dva bitno različita svijeta i da je poštivanje te razlike nužan uvjet, conditio sine que non, kako bi čovjek bio slobodan; shvatili su kako se zastorom koji razdvaja ta dva svijeta ne treba igrati, i da su trgači zavjesa kriminalci. (Kundera, 1996: 261)

Svatko od nas ima određene misli čije bi obznanjivanje bliskoj osobi moglo narušiti odnos. Nagel ide i korak dalje te tvrdi kako društvene konvencije o privatnosti imaju „vrijednu funkciju držanja nas od unošenja u lice jednih drugima“ (Nagel, 2002: 4). Prema njemu, skrivanje je preduvjet civilizacije. Znatno više toga odvija se unutar nas nego što smo spremni iskazati i civilizacija bi bila neostvariva kada bismo si međusobno mogli čitati misli (Nagel, 2002). Njemački filozof Goerg Simmel prije više od sto godina odlično je opisao važnost povlačenja za društvo o kojoj Nagel govori:

> Sve što drugome želimo riječima, ili pak na drugi način, poručiti, pa čak i one najsubjektivnije, najimpulzivnije, najintimnije stvari zapravo su pažljivo probrane iz naše sveobuhvatne psihološke stvarnosti, čiji bi potpuni sadržaj svakog čovjeka odveo u ludnicu. (Simmel, 1908: 341)

Dakako, kao što i sami imamo razne negativne misli, svjesni smo da ih imaju i drugi. Stoga je opravdano pitanje ukoliko smo svjesni svojih negativnih misli i činjenice da i drugi imaju slične negativne misli o nama koje bi nas mogle povrijediti, koja je razlika ako ih se izrekne budući da ionako postoji uzajamno razumijevanje prema tome da te misli postoje i da im se ne pripisuje značaj na način da ih se realizira. Za Frieda, odgovor leži u tome da postoji svojevrsni društveni konsenzus kako su takve misli benigne i sasvim prirodne, a tek ih njihovim verbalnim izražavanjem ili manifestiranjem na drugi način prihvaćamo i odabiremo ih kao dio sebe (Fried,

1968). I to ima smisla. Distinkcija između misli, izgovorene riječi i učinjenog djela postoji te je razlika između negativnih misli, riječi i djela nedvojbeno vrlo velika.

Osim ovog negativističkog pogleda na važnost privatnosti za odnose prikrivanjem od bliskih osoba, u svrhu razvijanja i održavanja odnosa s njima, Fried je vidio i pozitivni aspekt privatnosti kroz izgradnju povjerenja. Naime, odnosi su bazirani na povjerenju i grade se međusobnim povjeravanjem kroz otkrivanje intimnih detalja o sebi. A da bi ti detalji mogli biti otkriveni, najprije moraju biti skriveni (Fried, 1968). Upravljanje kvalitetom i kvantitetom intimnih podataka o sebi koje ćemo drugome otkriti omogućuje nam da upravljamo stupnjevima intimnosti i ostvarimo različite kategorije bliskih odnosa. James Rachels svoje viđenje značaja privatnosti izgradio je upravo oko ove Friedove koncepcije, ali ju je generalizirao na odnose s različitim ljudima, a ne samo s onima najbližima. Naime, on slično kao i Kundera, Westin i Fried, tvrdi kako je jedan od najvećih razloga zašto vrednujemo privatnost taj da „zbog naše mogućnosti kontrole toga tko ima pristup nama i toga tko što zna o nama, možemo održavati niz različitih društvenih veza i odnosa s drugim ljudima“ (Rachels, 1975: 329).

Ključna kritika ovakvog pogleda koji dijele Fried i, u nešto proširenom smislu Rachels, usmjerena je na značajno pojednostavljivanje kompleksnosti međuljudskih odnosa. Činjenicu da Fried smatra kako se upravljanjem iznošenja intimnih podataka o sebi mogu stvarati i održavati različiti odnosi, Reiman smatra *neukusnom* jer to za njega predstavlja *trgovački pogled na intimnost* (Reiman, 1976: 30). Stoga on predlaže uvođenje brižnosti u jednadžbu jer smatra kako je upravo brižnost ključna za intimnost. Iz toga proizlazi da različitim ulaganjem brige, a ne podataka o sebi, upravljamo kvalitetom i razinom međuljudskih odnosa (Reiman, 1995). Valja napomenuti kako Fried nikada nije eksplicitno isključio važnost brižnosti za uspostavu i održavanje odnosa već je samo govorio o nužnoj, ali ne i dovoljnoj, ulozi dijeljenja i upravljanja informacijama o sebi za uspostavu bliskih odnosa. I konačno, unatoč tome što upravljanje brižnosti zvuči romantičnije od upravljanja podacima, u oba se poimanja radi o upravljanju odnosima ulaganjem nečega, bilo to ulaganje brige ili ulaganje podataka o sebi, što i Reimanov prijedlog čini jednako *neukusnim trgovačkim pogledom na intimnost*[3], kako je on opisao Friedov.

[3] U socijalnoj psihologiji razlikuju se dva različita pristupa odnosima, temeljem pravičnosti i temeljem zajedništva. Na odnose s poznanicima i osobama koje površno poznajemo imamo tendenciju primjenjivati temelj pravičnosti te (pod)svjesno pratimo ulaganja u odnos, brzo uzvraćamo na usluge i osjećamo se iskorištenima ako nam drugi ne uzvrate uslugu. S druge strane, na dugoročne interakcije između bliskih prijatelja, članova obitelji i partnera

Nadalje, i Gerstein smatra kako intimne veze bez privatnosti ne bi mogle postojati te vrijednost vidi u ekskluzivnom dijeljenju podataka među partnerima (Gerstein, 1978). On razlikuje dvije osnovne uloge u odnosu, onu promatrača i sudionika uključenoga u odnos. Promatranje uključuje postojanje određenog odmaka i nezavisnosti od odnosa dok sudjelovanje u odnosu predstavlja potpunu uronjenost u odnos. Te se dvije pozicije međusobno isključuju. Ako netko naruši našu privatnost promatranjem nas dok smo uronjeni u neki intimni odnos, imamo dvije mogućnosti. Možemo promijeniti svoje ponašanje, čime bismo narušili spontanost koja je ključna za intimnost, a možemo se i pokušati oduprijeti iskušenju za promjenom ponašanja i nastaviti se ponašati na jednak način. Međutim, i u tom slučaju bili bismo prisilno izvučeni iz uloge sudionika u ulogu promatrača budući da bi sama svijest o tome kako smo promatrani značila da više ne možemo biti potpuno uronjeni u odnos. Gerstein tvrdi kako šteta nastala takvim narušavanjem intimnosti nadilazi puko uznemiravanje te može imati dugoročne posljedice na odnos te smatra kako svatko tko nepozvan narušava nečiju intimnost ujedno na vrlo ozbiljan način ugrožava njegovu autonomiju (Gerstein, 1978).

Značaj privatnosti za uspostavu i održavanje bliskih međuljudskih odnosa predstavlja njezinu dodatnu vrijednost. Uvjerljiv je argument kojeg nude Fried i Rachels, a prema kojem bez privatnosti, bez mogućnosti reguliranja i upravljanja podacima o sebi, bez mogućnosti da neke misli, dojmove i uvjerenja zadržimo samo za sebe ili samo za uzak krug ljudi, jednostavno ne bismo mogli ostvarivati intimne odnose. Kada razmišljamo o povjerenju, jednom od temeljnih blokova svakog bliskog odnosa, jasno je da ono ne bi moglo postojati kada bi postojala potpuna transparentnost. Jednako tako, da bismo s nekime mogli imati ekskluzivan odnos, da bismo s tom određenom osobom mogli dijeliti podatke koje ne dijelimo ni sa kim drugim, moramo imati mogućnost činiti upravo to – ne dijeliti te iste podatke ni sa kim drugim. A upravo nam je za to potrebna privatnost, mogućnost kontrole s kime ćemo, kada, kako i što dijeliti o sebi, tj. kome ćemo i pod kojim uvjetima omogućiti pristup (podacima o) sebi. Nadalje, osim upravljanja kvantitetom intimnih podataka o sebi, a time i blizinom različitih odnosa, kako sugerira Fried, privatnost nam omogućuje da upravljamo i kvalitetom, odnosno sadržajem podataka koje dijelimo s drugim ljudima zbog čega možemo uspostavljati međuljudske odnose sasvim različite vrste. Pojašnjenje ovog stava najbolje je prikazati citatom Rachelsa u kojem se referira na primjer osobe za koju je smatrao kako mu je blizak prijatelj, no nakon što je došao do

imamo tendenciju primjenjivati temelj zajedništva prema kojem ljudi jedni drugima pomažu prema njihovoj potrebi i u odgovoru na tuđu potrebu bez obzira na to hoće li im se vratiti (Clark & Mills, 1993)

saznanja kako ta osoba strahuje zbog gubitka posla te kako jako voli poeziju, o čemu također govorio s drugim ljudima, ali ne i s njime, Rachels na koncu mora zaključiti kako očito njih dvojica nisu tako bliski prijatelji kako mu se činilo:

> Jednako opće pravilo može se primijeniti i na različite druge vrste međuljudskih odnosa: poslodavca sa zaposlenikom, svećenika sa župljaninom, liječnika s pacijentom, muža sa ženom, roditelja s djetetom i tako dalje. U svakom od tih odnosa, oblik odnosa koji će ljudi imati uključuje zajedničko poimanje načina međusobnog ophođenja koji je za njih prihvatljiv te, još i važnije, zajedničko poimanje vrste i razine znanja jednoga o drugome koje je prihvatljivo da jedno o drugome imaju. (Rachels, 1975: 328)

1.4. Kritike pojma privatnosti

Osim normativno pozitivnih pogleda na privatnost te spomenutih autora koji su u privatnosti vidjeli nešto vrijedno, bilo za razvoj pojedinca u samostalnu i slobodnu osobu te njegovo samoostvarenje, bilo za uspostavu i održavanje različitih međuljudskih odnosa, ili oboje, raspravu o privatnosti obilježili su i skeptični pogledi na privatnost. Svojevremeno je vrlo aktualna bila tvz. redukcionistička kritika privatnosti prema kojoj privatnost nije mogla biti smatrana jedinstvenim konstruktom koji ima jasne konture već je se moglo jednako dobro obrazložiti drugim konstruktima. Pojedini autori izrazili su osobito skeptičan stav prema privatnosti te su smatrali da ona šteti razvoju društvenih i ekonomskih odnosa (Posner, 1978) ili da je neotkrivanje podataka o sebi jednako zavaravanju i manipuliranju drugima (Posner, 1978; Wasserstrom, 1984). Komunitarna kritika privatnosti dominantno sadržana u opsežnom radu profesora Etzionija priznaje privatnost kao vrijedan konstrukt koji zaslužuje zaštitu, ali se prema njemu ispred zaštite privatnosti u pravilu trebaju staviti opći interesi zajednice (Etzioni, 2015). Na sličan način na privatnost gleda i feministička kritika, koja je prepoznaje kao vrijednost, ali koja ima zadršku prema zaštiti liberalnih vrijednosti koje bi mogle doprinijeti jačanju nejednakosti, među koje ubrajaju autonomiju te s njome povezanu privatnost (Rössler, 2005). Nešto radikalniji feministički pogled na privatnost u njoj vidi prijetnju da će stvaranje privatnih sfera bez uplitanja drugih osigurati poligone na kojima će zlostavljanje ili zanemarivanje žena biti još lakše, a otkrivanje počinitelja bit će još teže (MacKinnon, 1989). U nastavku će biti pružen kratak pregled osnovnih predstavnika pojedinih skeptičnih pogleda na privatnost i njihovih argumenata. Budući da većina tih pogleda uključuju vrijedne uvide, rasprava o njima doprinijet će stvaranju integrativne kontekstualne definicije privatnosti koja će biti korištena u ovom radu.

1.4.1. Redukcionistička kritika pojma privatnosti

U uvodu je spomenuta rasprava o tome je li privatnost jedinstven konstrukt koji obuhvaća međusobno smisleno i moralno povezana pitanja ili se radi o nezavisnim problemima koji su tek površno povezani. Većina autora u literaturi eksplicitno se svrstava, ili ih se više ili manje nedvojbeno može svrstati, u jednu od dvije kategorije, a koje DeCew naziva *koherentistima* i *redukcionistima* (DeCew, 2013). S jedne strane nalazi se veći dio autora koji prepoznaju kako postoji nešto fundamentalno zajedničko i karakteristično za slučajeve povreda privatnosti (DeCew, 2013), a promišljanja o privatnosti ključnih predstavnika te skupine izložena su ranije u ovom poglavlju. Unatoč tome što različito pristupaju definiranju koncepta, ili na drugačiji način vide vrijednost privatnosti, slažu se kako je privatnost potrebno izdvojiti kao jedinstven i vrijedan koncept te ih se stoga u literaturi naziva *koherentistima*.

Za razliku od njih, postoji i druga skupina autora koji smatraju kako se slučajevi ugroze prava na privatnost pažljivim pristupom mogu na odgovarajući način i jednako dobro objasniti u terminima ugroza već postojećih prava. Oni definiranje i postuliranje prava na privatnost smatraju redundantnim jer u konceptu prava na privatnost ne vide ništa što se ne bi moglo pojasniti već postojećim temeljnim ljudskim pravima poput vlasničkih prava te prava na slobodu i osobnu sigurnost (Thomson, 1975). U literaturi se takve kritičare privatnosti naziva *redukcionistima* budući da smatraju kako se slučajeve povrede privatnosti može svesti na povrede nekih elementarnijih prava kao što su nanošenje emocionalne boli ili povrede vlasništva (DeCew, 2013).

U takve redukcionističke poglede na privatnost ubraja se i ranije spomenuta taksonomija delikata dekana Prossera. Međutim, dok je on vrlo suptilno izrazio svoj redukcionistički pogled na privatnost, Judith Jarvis Thomson eksplicitno je i bez okolišanja ustvrdila kako je pravo na privatnost skup međusobno nepovezanih prava te kako se bilo koje pravo koje osobi osigurava privatnost može u cijelosti osigurati nekim drugim pravom poput prava na osobno vlasništvo, pravom na slobodu ili/i osobnu sigurnost (Thomson, 1975: 313). Kako bi potkrijepila svoje tvrdnje, Thomson je koristila izmišljene priče kao misaone eksperimente. Poznat je njezin primjer čovjeka koji u svojem zidnom sefu ima pohranjenu pornografsku fotografiju, za koju ne želi da je itko vidi. Kao vlasnik te fotografije on na to ima pravo. Za Thomson pravo vlasništva uključuje set prava među kojima je i negativno pravo, pravo da nitko nema pristup našem vlasništvu. S druge strane, u tom misaonom eksperimentu, Thomson i čitatelj posjeduju rendgen kojim mogu vidjeti sadržaj čovjekova sefa. Thomson se slaže kako bi korištenje tog

rendgena za gledanje čovjekove pornografske fotografije u sefu predstavljalo povredu njegove privatnosti, ali samo stoga što je pornografska slika čovjekovo osobno vlasništvo pa mu je stoga povrijeđeno pravo vlasništva. U tom je smislu za Thomson nešto što se naziva pravom na privatnost redundantno jer se, u ovom primjeru, može objasniti povredom prava vlasništva. Bez takve povrede prava vlasništva, prema Thomson, ne bi bilo ni povrede privatnosti. Da se u zidnom sefu nalazila tuđa pornografska fotografija, ili karta podzemne željeznice koju je čovjek skinuo s javnog mjesta i odnio kući u sef, gledanjem u taj sef pomoću Thomsonina svemogućeg rendgena, čovjeku ne bi bila povrijeđena privatnost budući da on nije vlasnik tih objekata i time ne polaže negativno pravo koje drugima ograničava mogućnost gledanja tih objekata. Međutim, sam čin gledanja u nečiji sef već je sam po sebi povreda privatnosti. Budući da je zidni sef u vlasništvu tog čovjeka, i Thomson bi se trebala složiti kako je već samo gledanje u sadržaj njegova vlasništva povreda njegova prava bez obzira na to čije je vlasništvo u sefu. Međutim, u ovom se primjeru ne radi samo o povredi prava vlasništva. Recimo da ni sef nije u vlasništvu, pa ni u posjedu čovjeka. Svejedno se radi o povredi prava na privatnost tog čovjeka. Sam čin gledanja što netko radi, na koji način to radi, osobito bez njegova znanja i privole oblik je oduzimanja kontrole tom čovjeku da sam raspolaže podacima o sebi. Jedan od prvih kritičara Thomsonina pogleda na privatnost, Thomas Scanlon, između ostalog, koristi upravo spomenuti primjer kako bi argumentirao svoju poziciju. I njemu je samorazumljivo kako sam čin gledanja u sef bez čovjekova znanja i privole predstavlja povredu privatnosti bez obzira na to čiji je sadržaj sefa (Scanlon, 1975). Scanlon nadalje uvjerljivo argumentira kako je nebitno i to u čijem je vlasništvu sef. Svoj bismo sef mogli dati prijatelju na čuvanje. Pregledavanje sadržaja tog sefa narušilo bi privatnost našeg prijatelja bez obzira na to što sef nije njegov. Sama činjenica da netko spoznaje podatke o nama, pa makar to bili i podaci da nemamo svoj sef ili da nemamo svoje pornografske fotografije predstavljaju povrede naše privatnosti.

Da, Thomson je u pravu kada kaže da gledanjem ljudi posebnim rendgenom ne narušavamo njihovo pravo da budu *ostavljeni na miru*, kako su o privatnosti pisali Warren i Brandeis, ali itekako narušavamo njihovu sposobnost da autonomno, slobodno i suvereno upravljaju time tko će, kada i kako imati pristup podacima o njima. Uostalom, postavlja se i pitanje zašto bi uopće pravo vlasništva imalo prednost nad pravom na privatnost. Za Thomson je to samorazumljivo, ali to ne mora tako biti. Scanlon također na određeni način relativizira dominaciju prava vlasništva nad pravom na privatnost navodeći kako je od samog vlasništva znatno važnije pitanje konvencionalne granice. Kao primjer Scanlon koristi veliko polje na

kojem je svakome dodijeljen jednak djelić tog polja kako bi u njemu zakopao svoje dragocjenosti. Primjena Thomsonina rendgena na nečije zakopane dragocjenosti nedvojbeno ugrožava njegovo pravo na privatnost bez obzira na to čije je polje, tko ga može prodati, tko na njemu može graditi (Scanlon, 1975: 318). Argument je moguće i proširiti na dragocjenosti koje su zakopane. Naša je privatnost ugrožena ne samo bez obzira na to čije je polje nego i bez obzira na to čije su dragocjenosti koje smo zakopali. Možda nam je netko dao da zakopamo njegove dragocjenosti, možda smo nečije dragocjenosti zakopali bez njihova znanja, s dobrom ili lošom namjerom. Možda smo ukrali dragocjenosti i nemamo ih pravo zakopati, ali to ne znači da korištenje rendgena ne narušava našu privatnost. Dakako, pravo na privatnost nije neograničeno i postoje uvjeti i okolnosti u kojima ga se može i treba ograničiti, ali to ne znači da ono ne postoji ili da ono nije vrijedno.

Iako prvi, Scanlon nipošto nije jedini koji je uvjerljivo i opsežno kritizirao Thomsonin redukcionistički pogled na privatnost. Julie Iness u svojoj knjizi o privatnosti cijelo jedno poglavlje posvetila je samo raspravi o Thomsoninu pogledu, koju smatra reprezentativnim skeptikom za privatnost (Iness, 1992). U vrlo detaljnoj i opsežnoj argumentaciji Iness izdvaja dvije osnovne linije argumenta. Najprije, pretpostavimo li da je privatnost doista tek skup temeljnijih prava, ostaje pitanje što povezuje upravo ta temeljna prava. Uzmemo li da se svaki primjer koji je Thomson navela doista može svesti na neko drugo pravo, postoji li neka zajednička, latentna kategorija višeg reda koja objedinjuje baš te primjere i baš ta prava, a ne i sva ostala. Thomson je u više navrata ustvrdila kako je privatnost skup međusobno *nepovezanih* prava, no to ustvrditi jednostavno nije dovoljno. Bilo je potrebno značajno više argumentacije kako bi doista pokazala da ne postoji povezanost između različitih primjera i prava koje je navodila. A izvjesno je da u tome ne bi ni uspjela, kao što Iness sugerira (Iness, 1992). Drugi Inessin argument odnosi se na to kako značaj i „vrijednost koju pripisujemo privatnosti ne proizlazi nužno iz vrijednosti koju pripisujemo drugim pravima“ (Iness, 1992: 10), a Iness tu ponajviše misli na intimnost, koja je prema njoj središnja vrijednost privatnosti i ne može se u potpunosti objasniti drugim pravima. I konačno, kao što je ranije navedeno, da je Thomson i uspjela pokazati kako se sve povrede privatnosti mogu objasniti u terminima drugih prava i da te povrede korespondiraju u potpunosti, što nije, ne bismo mogli znati radi li se o tome da se privatnost može svesti na druga prava ili se druga prava mogu svesti na privatnost (Iness, 1992: 37).

Unatoč tome što se Thomson smatra reprezentantom pa i najpoznatijom (DeCew, 2013) za redukcionističku kritiku privatnosti, ona u njoj nije usamljena. Vrijedi spomenuti i skeptični pogled Richarda Posnera koji je postavio ekonomsku teoriju privatnosti (Posner, 1978). Osim redukcionističkog pogleda, on na zaštitu privatnosti u značajnoj mjeri gleda kao na negativnu vrijednost. Bez ulaženja u definiciju privatnosti, Posner je ustvrdio kako je zadržavanje ili prikrivanje podataka jedan od sastavnih dijelova privatnosti i bavio se isključivo tih aspektom privatnosti. Smatrao je kako zadržavanje podataka za sebe šteti ekonomskim odnosima i produktivnosti te je stoga postulirao svoju ekonomsku teoriju privatnosti u kojoj bi se pravo na privatnost, odnosno pravo na zadržavanje ili prikrivanje podataka, primjenjivalo samo na one slučajeve u kojima bi obznanjivanje tih podataka ili u potpunosti eliminiralo komunikaciju ili bi umanjilo njezinu vrijednost uključivanjem nevrijednih ili zavaravajućih podataka. Kao što je prikazano u tablici 1, njegova se teorija sastoji u tome da je osobne podatke podijelio na diskreditirajuće i nediskreditirajuće, a unutar svake kategorije dodatno na točne i na netočne. Na taj je način dobio dvije nezavisne dimenzije, odnosno četiri kategorije podataka.

Tablica 1. – prikaz Posnerove ekonomske teorije

Podaci	*Diskreditirajuće*	*Nediskreditirajuće*
Točni	Postoji društveni interes da se ovakvi podaci otkriju kako bi drugi znali kako se postaviti prema osobi. Otkrivanje takvih podataka je poput otkrivanja prevare te će pozitivno utjecati na informiranost ostalih potrošača, odnosno, korisnika društvenih odnosa.	Budući da nediskreditirajući podaci uglavnom nemaju značaj za ljudsku interakciju, njihovo iznošenje nema društvenu vrijednost.
Netočni	Netočni podaci štetni su za racionalno donošenje odluka te ih nije korisno dijeliti.	

Posner je netočne i nediskreditirajuće osobne podatke smatrao bezvrijednim za društvenu korist. Naime, netočne informacije svakako je smatrao štetnima za donošenje racionalnih ekonomskih odluka, bez obzira na to radi li se o diskreditirajućim ili nediskreditirajućim podacima te je smatrao kako ih ne treba dijeliti. Za nediksreditirajuće podatke smatrao je kako nemaju ekonomski značaj te ih je smatrao irelevantnima bez obzira na to jesu li točno ili netočno. No, temeljna poanta njegove teorije jest u tome što je on smatrao kako osoba nema pravo zadržati za sebe diskretitirajuće, a točne informacije o sebi.

Za Posnera postoji stalna dinamika između prava da prikrijemo podatke i prava da saznamo tuđe podatke pa tako jedni ljudi ulažu resurse u prikrivanje informacija koje posjeduju dok drugi ulažu resurse u pokušaje otkrivanja tih informacija. Posnerov ciničan pogled na ljudske odnose, između ostaloga, očituje se u njegovu mišljenju kako „Malo ljudi želi biti ostavljeno na miru. Oni žele manipulirati svijetom oko sebe selektivno otkrivajući podatke o sebi“ (Posner, 1978; 22). Na grub se način izrazio, ali njegova tvrdnja nije daleko od istine. Ljudi doista žele selektivno otkrivati podatke o sebi. U ovom je poglavlju privatnost definirana upravo u terminima kontrole nad podacima o sebi, a kao jedan od temeljnih značaja privatnosti jest upravo mogućnost uspostave smislenih odnosa. U tom smislu, već je odgovoreno na Posnerovu kritiku. Jednostavno, mnogi međuljudski odnosi ne bi bili mogući kada ljudi ne bi imali pravo neke stvari prikriti od drugih. No, Posner ne smatra da bi svi podaci trebali biti otkriveni već samo oni čije prikrivanje smanjuje društvenu produktivnost, odnosno podaci koji su nekome vrijedni ili drugi ljudi imaju interes za njihovim otkrivanjem (Posner, 1978). U svom je članku dao nekoliko primjera poput supruga koji supruzi prikriva svoju neplodnost, prodavatelja koji kupcu kuće prikriva određene nedostatke na kući ili radnika koji od poslodavca prikriva bolest koja doprinosi njegovu radnom učinku. U tim je primjerima pokušao ekonomskom logikom, stavljajući u relaciju resurse koji bi bili uloženi u nastavak odnosa s vrijednosti podataka, obrazložiti opravdanost prikrivanja. Međutim, Posner nije na dovoljno jasan način obrazložio koji su to točni i diskreditirajući podaci koje bi osoba imala pravo zadržati za sebe, a koje bi točno podatke trebala obznaniti drugima. Za Posnera „neobznanjivanje podataka u jednom trenutku prerasta u prevaru“ (Posner, 1978: 21), ali nije dovoljno dobro pojasnio koji je to točno trenutak. Nadalje, Posner je propustio jasno definirati što točno za njega znače diskreditirajući podaci.

Posnerova teorija ekonomije privatnosti u mnogočemu je zasnovana na pogrešnim premisama te istovremeno selektivno zanemaruje cijeli niz relevantnih podataka. Hladnoekonomski pogled na međuljudske odnose propušta uvažiti cijeli nematerijalni i iracionalni aspekt ljudskih odnosa, od doživljaja prošlih iskustava do emocija, koji na naše ponašanje utječe znatno više od bilance ulaganja resursa u neki odnos. Nadalje, njegov pogled na ljude kao na manipulatore koji druge zavaravaju i time oštećuju ekonomski i društveni napredak vrlo je ciničan. Sličan pogled ima i Richard Wasserstrom koji smatra kako je neotkrivanje informacija o sebi moralno izjednačeno sa zavaravanjem (Wasserstrom, 1984). Takav pogled na druge ljude podsjeća na Molièreova Mizantropa koji prezire licemjerno prenemaganje aristokracije, njihovu dvoličnost

i međusobno prikrivanje. Iako grub i ciničan, taj pogled nije nužno pogrešan. Stvar je u tome što ljudi imaju pravo biti takvi. Ljudi imaju pravo prikazivati se u svjetlu u kojem žele, imaju pravo na drugu priliku, imaju pravo reći o sebi samo ono što žele i samo onome kome žele. To što time određeni odnos čine manje produktivnim možemo smatrati lošim, ali to nipošto ne može biti razlog za ukidanje njihova prava na privatnost.

Na općenitoj razini postoje uvjerljivi argumenti protiv redukcionističkog pristupa privatnosti, odnosno mogućnosti jednostavnog svođenja povreda privatnosti na takozvana temeljna pitanja. Moore ističe dvojakost povrede privatnosti kroz razlikovanje objekta i koncepta (Moore, 2003). Naime, redukcionisti na povredu privatnosti gledaju tako da za njih svaka informacija (koncept) ima svoju materijalnu manifestaciju (objekt), koji bi onda netko mogao neovlašteno posjedovati što bi predstavljalo povredu vlasništva. Međutim, jasno je kako neizmjerna količina informacija, misli, uvjerenja i ideja nema svoju materijalnu manifestaciju, a mogu biti u neovlaštenom posjedu čime je osobi narušena privatnost. Nadalje, Ruth Gavison istaknula je određenu cirkularnost u odnosu na redukcionističku poziciju. Ona je prepoznala kako su, osobito tijekom prve polovice 20. stoljeća, mnogi redukcionisti svoja tumačenja privatnosti donosili na temelju pravnih slučajeva u kojima su gledali što su sudovi smatrali povredom privatnosti. Jedan od primjera takvog pristupa jest upravo taksonomija delikata privatnosti dekana Prossera. Gavison je prepoznala kako je problem u njegovu i sličnim pristupima bio u tome što u to vrijeme privatnost nije bila prepoznata kao zaseban pravni konstrukt pa su sudovi rijetko štitili privatnost ako u povredu nije bilo uključeno i neko drugo pravo zbog čega se stekao dojam da privatnost nije zasebno vrijedna i ne predstavlja zaseban konstrukt (Gavison, 1980).

Sve u svemu, redukcionistička kritika privatnosti imala je više ili manje eksplicitne te više ili manje dobro utemeljene pokušaje argumentiranja, no danas možemo reći kako je u raspravi o privatnosti prevladala koherentistička struja i pogled koji na privatnost gleda kao na jedinstven i vrijedan konstrukt. No, to ne znači da ne postoje ozbiljne kritike usmjerene prema konceptu privatnosti, prava na privatnost i njihovom značaju u društvu, ali oni se više odnose na kritike liberalnog individualizma u širem smislu, a time i na konceptualizaciju prava na privatnost kao temeljnog ljudskog prava. Nije više pitanje je li privatnost vrijedna i dostojna zaštite, već je više pitanje značaja privatnosti u odnosu na druga ljudska prava ili općeg dobra zajednice.

1.4.2. Komunitarna kritika pojma privatnosti

Teoretičari koji stavljaju interes društva iznad interesa pojedinca u svojem napadu na individualna prava zahvatili su i privatnost. Za sociologa Amitaia Etzionea, jednog od utemeljitelja liberalnog komunitarizma, koji je mnogo pisao o privatnosti, ona predstavlja društveno dopuštenje za to da se određena djelovanja, misli i osjećaji izuzmu iz društvena, javnog i vladina nadzora (Etzioni, 2005). Za njega, privatnost nipošto ne predstavlja apsolutnu vrijednost i u svojim knjigama ukazuje na to kako upravo privatnost često usporava ili onemogućuje razvoj brojnih društvenih interesa u usporedbi s kojima bi u većini slučajeva balans trebao biti na strani općeg dobra (Etzioni, 2004, 2005, 2007; Etzioni i Marsh, 2003). Etzioni nedvojbeno prepoznaje vrijednost privatnosti, ali je smatra suprotstavljenom općem dobru. Prema njemu, „liberalni komunitaristi drže kako sva društva moraju brinuti o dvije temeljne vrijednosti: dostojanstvu pojedinca, koje je temelj svih individualnih prava i važnosti općeg dobra“ (Etzioni, 2015: xi). Komunitarna ideja je pokušati zadržati ravnotežu između te dvije temeljne vrijednosti. Međutim, u tome je sadržan ključni problem. Ne postoji konsenzus oko toga što točno ta ravnoteža predstavlja. Iz Etzionijevih radova očigledno je kako je za njega ravnoteža vrlo često na strani općeg dobra, a kada u tom kontekstu preciznije govori o općem dobru najčešće spominje javno zdravlje i nacionalnu sigurnost (Etzioni, 2015). Postoji minimalna razina ljudskih prava, ponajprije dostojanstva, slobode i tjelesnog integriteta osobe, za čije narušavanje ne postoji opravdanje općeg dobra. Međutim, privatnost nije neograničeno ljudsko pravo te je se u određenim uvjetima i pod određenim okolnostima može, pa i mora, ograničiti i o tome će mnogo riječi biti u nastavku ovog rada. Oko određivanja uvjeta i okolnostima u kojima će se i na koji način pojedincima ograničiti privatnost radi općeg dobra već dugo postoji vrlo žustra rasprava. Ta je rasprava ponajprije vrijednosnog sadržaja i vrlo će teško biti pronaći konsenzus između komunitarne i liberalne ideje. Budući da u svojem opsegu i sadržaju izlazi izvan okvira ove disertacije, ta će vrijednosna rasprava biti stavljena sa strane.

Temeljna komunitarna ideja jest kako neka individualna prava, a u ovom slučaju radi se o privatnosti, u određenim okolnostima mogu biti u sukobu s idejom općeg dobra. No, to ne mora biti tako. Do sada su u ovom poglavlju prikazani brojni uvjerljivi argumenti prema kojima je privatnost povezana s autonomijom, dostojanstvom i slobodom pojedinaca čime direktno doprinosi demokraciji i općem dobru. U društvu u kojem se vrednuje privatnost lakše je imati samoostvarene građane, privatnost je jedan od preduvjeta autonomije koja je nužna za razvoj slobodne misli, kreativnost, kritiku i razvoj. U tom smislu, Etzioni uvelike podcjenjuje doprinos

privatnosti općemu dobru (Allen, 2004; Bernal, 2014; Solove, 2011). S druge strane, Rössler ističe kako feminističke teorije privatnosti upravo inzistiraju na tome kako je katkada, kao u slučaju prava žena, potrebno njihova individualna prava staviti ispred općeg dobra jer im u protivnom nije moguće jamčiti jednaku slobodu odlučivanja o svojem životu i tijelu (Rössler, 2006: 700).

Slično komunitarnoj kritici privatnosti, iz filozofije Habermasa i Arendt te osobito Marxa i Engelsa razvila se socijalistička kritika privatnosti prema kojoj privatnost „ideološki mehanizam koji pomaže stvarati i produbljivati nejednakost“ (Fuchs, 2011:231) i doprinosi većem potlačivanju radničke klase. Na temelju izvornih tekstova Marxa i Engelsa, Fuchs je izveo ključne elemente socijalističke kritike privatnosti koji se svode na kritike prevelikog naglašavanja individualizma koji je „egoističan“ i „škodi općem dobru“ (Fuchs, 2011:227) te predstavlja temelj za suvremeno (nepravedno) klasno uređenje. Fuchs ističe kako je „privatnost u kapitalizmu osigurana samo za bogate i za tvrtke“ (Fuchs, 2011:231) dok tvrtke radi maksimiziranja profita žele znati što više o svojim radnicima i potrošačima. Prema tome, Fuchs ne misli da je privatnost isključivo loša niti da ju je potrebno ukinuti, već predlaže kontekstualiziranje privatnosti na način da se uračuna njezina povezanost s kapitalizmom kako bi služila zaštiti radnika, a ne korporacija i buržoazije. „Privatnost je nepoželjna u onim slučajevima u kojima štiti bogate i kapital od javne odgovornosti, ali je poželjna u onim slučajevima u kojima pokušava zaštititi građane od korporativnog nadzora“ (Fuchs, 2011:231).

Značajan dio socijalističke kritike privatnosti zapravo se odnosi na socijalističku kritiku kapitalizma i liberalizma. Etzioni je u pravu u kritici onih koji smatraju da privatnost treba imati prednost nad općim dobrom, ali je u krivu u tome da privatnost, barem na prvi pogled, nije sasvim uskladiva s općim dobrom. Sukladno do sada iznesenim argumentima, privatnost predstavlja temeljno ljudsko pravo koje ima vrijednost za ljudsko dostojanstvo, autonomiju i slobodu pojedinaca te za mogućnost ljudi da uspostavljaju i održavaju smislene međuljudske odnose. No, još važnije, upravo zbog tih vrijednosti, privatnost ima značaj za društvo, za opće dobro i na taj se način privatnost razumije u okviru ovoga rada.

1.4.3. Feministička kritika pojma privatnosti

Slično kao komunitarna kritika, i feministička kritika privatnosti zapravo je dio šire feminističke kritike liberalnog individualizma. Feministička kritika privatnosti vrlo je heterogena, ali dvije ključne ideje koje je obilježavaju. S jedne strane radi se o kritici moderne

liberalne misli koja na autonomiju gleda kao na mušku vrijednost. „Suština feminističke kritike jest u tome što zaštita privatnosti i autonomije često znači i zaštitu patrijarhata i konzervativizma, a uobičajene koncepcije autonomije općenito su odraz muških vrijednosti“ (Bernal, 2014: 47). A s druge strane mnogi su feministi zabrinuti za *tamnu stranu* privatnosti, odnosno korištenje privatnosti kako bi se prikrila degradacija, dominacija i zlostavljanje žena, ali i ostalih (DeCew, 2013: 1).

Poput lijevo-progresivne kritike, i feministi izražavaju opću kritičnost prema distinkciji javnoga i privatnoga (Allen, 2004). Odličan kontekst za razumijevanje tog prvog aspekta feminističke kritike daje Beate Rössler. Ona razgraničuje stari i novi pogled na podjelu javne i privatne sfere pri čemu je stari pogled podjelu smatrao prirodno zadanom, dok je novi smatra rezultatom konvencija (Rössler, 2006). Prema starom pogledu, u domenu privatnoga pripadali su *osjećaji, dom* i *ognjište*, *emocionalna briga za muškarce* kao i *briga za djecu* te je poistovjećivana sa ženom, dok je u domenu javnoga pripadao *razum*, *profesija* i *politika* te je poistovjećivana s muškarcem. Takva dvojaka podjela sfera rezultirala je dvojakim značajem za privatnost u modernom društvu. Naime, s jedne strane privatna sfera, dom i obitelj štićeni su od zahtjeva neprijateljskoga vanjskoga svijeta kao mjesto ljubavi i brižnosti dok je s druge strane poistovjećivanje inferiorne žene s privatnom sferom podredilo privatnu sferu javnoj (Rössler, 2005, 2006: 59). Unatoč tome što se ovaj pogled prvenstveno odnosi na općenitu kritiku moderne liberalne misli, kritika je opravdana. Privatnost i autonomija potpuno su jednako vrijedne i značajne i za muškarce kao i za žene. Definiranje privatnosti u terminima mjesta u ovom je radu spomenuto tek kao dio povijesnog konteksta razvoja definicije pojma. Suvremeno tumačenje privatnosti, osobito ono koje uvažava tehnološki razvoj u digitalnog dobu, uključuje definiranje privatne sfere ne u terminima mjesta nego u terminima kvantitete i kvalitete sadržaja podataka koji se o nekome prikupljaju. Etzioni to opisuje na način da ljudi svoju „privatnu sferu nose sa sobom kamo god se kreću, uključujući i u javni prostor“ (Etzioni, 2015: 73). Na taj način izbjegnute su bilo koje konotacije koje bi privatnu sferu povezale sa ženom dok se istovremeno jačanjem privatnosti ženama daje kontrola nad podacima i njime čime ih se čini suverenima i autonomnima djelovati na način na koji žele i ostvarivati one međuljudske odnose na onaj način na koji to žele.

Drugi aspekt feminističke kritike dio je radikalnijeg feminističkog pristupa u kojem je najdalje otišla Catharine MacKinnon. Ona u svojoj radikalnoj egalitarističkoj feminističkoj kritici izjednačuje zaštitu privatnosti s jačanjem ograda koje onemogućuju žensku autonomiju, izlazak

iz tradicionalne uloge pa čak i bijeg od nasilja smatrajući kako privatnost predstavlja svojevrsni plašt koji omogućuje zlostavljanje i podređivanje žena (MacKinnon, 1989). Allen daje za pravo ovoj feminističkoj kritici zbog svega što su žene u prošlosti prošle, no smatra kako nema dvojbe da se žene sve više emancipiraju te da su već emancipirane žene započele uživati blagodati koju im omogućuje pojačano poštovanje prema mnogim oblicima privatnosti (Allen, 2004). I ovakav radikalniji pogled na privatnost je vrijedan jer je njime ukazano na to kako liberalna predanost privatnoj sferi nije uvijek bila i ne mora uvijek biti u skladu s liberalnim idealom jednakosti budući da se pod plaštem nepovredivosti doma omogućavao nastavak podređivanja žena. I ne samo žena. Kao što je već jasno izneseno, zaštita privatnosti u određenim je slučajevima u sukobu s drugim pravima. Zavjese štite ljude dok razigrano i sramotno plešu na lošu glazbu, ali zavjese mogu štititi i zlostavljanje žena, djece i muškaraca. Zavjese mogu štititi i teroriste koji se spremaju za izvođenje razornog napada, ali i prestrašenog novinara ili zviždača koji je razotkrio teški kriminal u političkim strukturama. Bez obzira na to, ljudsko je pravo koristiti zavjese. A te zavjese u određenim okolnostima i pod određenim uvjetima mogu biti razgrnute. O tim uvjetima i okolnostima bit će riječi u idućim poglavljima.

1.5. Zaključak

U ovom poglavlju pružen je temeljni povijesni i konceptualni pregled koncepta privatnosti. Nažalost, unatoč tome što o privatnosti kao konceptu filozofi raspravljaju još od Antike te tome što se čak već stotinu godina vodi intenzivna akademska rasprava o privatnosti u kojoj je mnogo napisano, Solove je u pravu kada tvrdi kako je literatura koja opisuje privatnost „konceptualna džungla“ (Solove, 2008: 196), a sam je „koncept u neredu“ (Solove, 2008: 1). Međutim, većina doprinosa raspravi o privatnosti vrlo su korisni i konstruktivni, a postoje i brojni svijetli primjeri koji su pokušali uvesti određenu organizaciju i red u razumijevanje privatnosti. Ovo poglavlje imalo je upravo taj cilj.

Osim toga, prije nego što se u radu pristupi daljnjoj argumentaciji, bilo je potrebno konceptu privatnosti dati jasan konceptualni okvir i definirati njegovu normativnu vrijednost. Najveći značaj dan je razumijevanju privatnosti u terminima kontrole pristupa (podacima o) sebi. Dijelom stoga što je to razumijevanje najznačajnije zastupljeno u relevantnoj literaturi o privatnosti, ali još i više stoga što odgovara načinu na koji privatnosti pristupa autor ove disertacije. Pri tome vrijedi naglasiti kako je autor koji je najbolje opisao način na koji se u ovom radu gleda na privatnost Alan Westin koji je u obzir uzeo i kulturalne i situacijske faktore

koji utječu na privatnost te je tvrdio kako je svatko uključen u stalni proces prilagodbe između želje za privatnosti i želje za razotkrivanjem podataka o sebi (Westin, 1967), pritom uzimajući u obzir kontekst i socijalne norme društva u kojem živi. Osim toga, konceptualizacija privatnosti u terminima kontrole omogućuje lakše razumijevanje klasifikacije ugroza privatnosti na eksterne i interne, koje čine sastavni dio idućeg poglavlja i ondje će biti detaljno opisane. Kao svojevrsnu nadgradnju definiranju u terminima kontrole, prikazani su i višedimenzionalni pogledi na privatnost kao i suvremeni kontekstualni pristup konceptualiziranju privatnosti. Oba su pristupa vrlo vrijedna, a poseban značaj imat će u empirijskom istraživanju koje je sastavni dio ove disertacije. Naime, slično kao što je Solove primijenio pristup odozdo-prema-gore kako bi na temelju pravnih dokumenata dokučio na što se privatnost odnosi, u ovom je radu u sklopu empirijskog istraživanja provedeno kvalitativno istraživanje koje je korištenjem metode polustrukturiranog intervjua imalo za cilj utvrditi na koji način pojedinci gledaju na privatnost. Jednako tako, u kasnijoj operacionalizaciji kvantitativnog dijela empirijskog istraživanja, u obzir su uzeti ranije opisani značajni uvidi i konceptualizacije Westina, Burgoon i Dienlina.

Upravo je kontrola ključan dio definicije privatnosti. S jedne strane sama potreba za zaštitom intime i sebstva omogućuje pojedincima razvoj autonomije. Istovremeno, mogućnost odabira hoćemo li, kome i kada otkriti sebe, nužna je za uspostavljanje i održavanje intimnih veza. To nas dovodi do značenja privatnosti i njezine vrijednosti koja je najbolje reprezentirana u načinu na koji je vide i autori kojima je dano najviše prostora poput Benna, Reimana, Blousteina, Gersteina, Gavison i Rössler. Kroz viđenje vrijednosti svih tih autora provlači se važnost privatnosti za razvoj nezavisne misli do svojevrsnog zaključka Beate Rössler koja uvjerljivo izvodi argument o tome kako su „zbog normativne povezanosti autonomije i privatnosti, te činjenice da se demokracija oslanja na autonomne pojedince, prijetnje privatnosti uvijek prijetnje demokraciji“ (Rössler, 2006: 709). Bez autonomnih pojedinaca, slobodnih kritički misliti nemoguće je zamisliti demokraciju. Nužnost privatnosti za razvoj i održavanje autonomne, slobodne i kritičke misli gotovo je samorazumljiva. Strah od javne osude u korijenu bi zatirao bilo koji oblik nepoželjne i drugačije misli ili djelovanja. Naš bi svijet i svakodnevica bili znatno uniformiraniji i siviji.

Nadalje, osim značaja za autonomiju pojedinca, te time posredno i za demokraciju, značaj privatnosti očigledan je i u njenom značaju za uspostavu i održavanje značajnih i bliskih međuljudskih odnosa. Jasno da ovdje nije namjera svesti kompleksnost intimnih odnosa na

puko dijeljenje i upravljanje informacijama o sebi, no upravo je ta mogućnost dijeljenja određenih podataka o sebi, osjećaja, misli, trenutaka jedan od ključnih načina na koji diferenciramo različite razine odnosa koje imamo s ljudima s kojima dolazimo u kontakt. Odnosi se grade međusobnim povjeravanjem i stvaranjem povjerenja kroz otkrivanje intimnih detalja koji najprije moraju biti skriveni da bi ih se uopće moglo otkriti. Dakako, ne može se zanemariti vrijeme i pažnja koju nekome posvećujemo, ali i za to nam je potrebna privatnost, sposobnost određivanja tko će, kada i pod kojim uvjetima imati pristup nama i podacima o nama. Gerstein poantu odlično sažima u napomeni kako potpuna transparentnost ubija spontanost, koja je sastavni dio intimnosti (Gerstein, 1978: 79). I konačno, s obzirom na utemeljene argumente feminističke i komunitarne kritike privatnosti kao i suvremene višedimenzionalne i kontekstualne konceptualizacije privatnosti, definiciji privatnosti u terminima kontrole pristupa (podacima o) sebi u ovom radu dan je osobito snažan integrativni i kontekstualni naglasak kroz višekratno isticanje dispozicijskih, situacijskih i kulturalnih razlika u doživljavanju i manifestiranju potreba za privatnosti. Jednako tako u razmišljanju o privatnosti kao temeljnom ljudskom pravu i njezinoj vrijednosti osobito je naglašen značaj privatnosti za društvo u cjelini. Drugo poglavlje će biti posebno posvećeno upravo raspravi o važnosti privatnosti za društvo i njezinoj ulozi kao temeljnog ljudskog prava u današnje digitalno doba.

2. Biti ili nemati privatnost: ugroze privatnosti

O privatnosti, a osobito o privatnosti u elektronskom okruženju, danas se mnogo govori. Gotovo svaka elektronska usluga dolazi s glomaznom i nejasnom politikom privatnosti, a pružatelji usluga ne propuštaju naglasiti kako im je privatnost korisnika izuzetno važna. Istovremeno, ugroze privatnosti gotovo su na svakom koraku, a u elektronskoj sferi gotovo na svakom pritisku tipke. Ne samo da je zaštita svoje privatnosti danas postala izuzetno teška, nego je i pitanje možemo li uopće u doba pametnih telefona, kolačića, društvenih mreža, elektronskih kartica, velikih podataka (eng. *Big data*) i povezanih uređaja (eng. *Internet of Things*) govoriti o privatnosti. Poput pravoga vizionara, Alan Westin još je 1967. godine, govoreći o tome kako svako slobodno društvo treba vlastima ograničiti kapacitete nadzora, predvidio izazove s kojima se danas susrećemo:

> U tom smislu, američko društvo će se u 1970-im godinama suočiti sa zadatkom zadržavanja te tradicije, kada se očekuje da će tehnološki razvoj javnim i privatnim tijelima omogućiti da čine ono što im je do tada bilo onemogućeno zbog kombinacije fizičkih i socio-pravnih zapreka. (Westin, 1967: 23)

Ulaskom u 21. stoljeće u telekomunikacijskom smislu dogodila su se dva značajna iskoraka, oba značajno povezana s mogućnosti nadzora i narušavanja privatnosti: u široku primjenu naglo su ušli mobilni (pametni) telefoni i došlo je do široke upotrebe interneta. Svatko od nas uz sebe gotovo dvadeset i četiri sata dnevno nosi mobilni telefon pomoću kojeg komunicira mnogo, često, sa svima i o svemu. Osim toga, web 2.0, kao posljedica masovne dostupnosti i sve veće brzine internetskog pristupa, doveo je do pojave društvenih mreža i seljenja mnogih javnih servisa i usluga na internet, što olakšava pristup informacijama i onima kojima su one namijenjene i onima kojima nisu. U takvom digitalnom i umreženom svijetu sve je teže kontrolirati tko ima pristup našim podacima i podacima o nama. Sve je teže očuvati privatnosti.

Po svemu sudeći, za većinu korisnika narušavanje privatnosti od strane internetskih oglašivača ili stranih obavještajnih službi i dalje je previše apstraktno. Uostalom, danas se sve češće može čuti takozvani ništa-za-sakriti argument (eng. *nothing-to-hide argument*) koji govori o tome kako ne moramo brinuti (o privatnosti) ako nemamo ništa za sakriti. A ako pak radimo nešto pogrešno, nemamo pravo to zadržati za sebe. Taj argument posebice promoviraju dužnosnici iz sigurnosnog sustava i veliki internetski oglašivači koji vrlo dobro žive od toga što se ljudi odriču svoje privatnosti, a najpoznatiji je citat predsjednika uprave Googlea Erica Schmidta iz intervjua za CNBC 2009. godine u kojem je rekao „ako postoji nešto za što ne želiš da drugi

znaju, možda to onda nisi trebao ni napraviti“ (“Google CEO On Privacy (VIDEO): ‘If You Have Something You Don’t Want Anyone To Know, Maybe You Shouldn’t Be Doing It’,” 2010). I čini se da se sve više korisnika slaže s takvom argumentacijom. Međutim, ona je pogrešna iz više razloga. Solove je napisao cijelu knjigu u kojoj kroz brojne primjere i argumente objašnjava zašto ništa-za-sakriti argument ne stoji, ali i zašto je opasan za društvo (Solove, 2011). Najprije, svatko ima nešto za sakriti. Ljudi u domu koriste zavjese i ladice, kupuju sefove i koriste enkripciju, šapuću i biraju o čemu će s kime razgovarati. Solove upozorava kako je ključna pogreška u tome što se kod privatnosti zapravo ne radi o *skrivanju* i sasvim je pogrešno poistovjetiti privatnost s mogućnosti skrivanja nečega pogrešnoga (Solove, 2011). Privatnost je mogućnost upravljanja pristupom (podacima o) sebi. Naša težina, dob, broj seksualnih partnera, neugledni ožiljak na potkoljenici, iznos mjesečne plaće ili naše mišljenje o kolegi ne predstavljaju ništa pogrešno. Međutim, to su podaci za koje moramo moći sami odrediti hoćemo li ih podijeliti, s kime, kako i kada. Ne radi se o skrivanju, već o dijeljenju. Ali pod našim uvjetima. I upravo u tom kontroliranom dijeljenju očuvano je naše dostojanstvo, sadržana je naša puna autonomija kako bismo kroz međusobno dijeljenje mogli produbljivati odnose s drugima. Reg Whitaker citirao je kolumnista New York Timesa Russela Bakera koji je u kolumni o tehnologiji nadzora 1998. godine naveo „Čujem kako se ljudi koji nemaju ništa za sakriti ne boje ove tehnologije nadzora koja nas guši. A gdje su to ti ljudi koji nemaju ništa za sakriti?“ (Whitaker, 1999: 158).

2.1. Podjela ugroza

U prošlom poglavlju opisano je nekoliko podjela ugroza privatnosti, poput taksonomije delikata dekana Prossera (1960) ili klasifikacije aktivnosti kojima se ugrožava privatnost Daniela Solovea (2002). Dok je Prosser svoju klasifikaciju temeljio isključivo na analizi sudskih slučajeva u kojima se radilo o povredi privatnosti, Solove je na ugroze privatnosti gledao odozdo-prema-gore te je uzeo u obzir i teoretske, društvene, povijesne te kulturalne aspekte kako bi ustanovio sveobuhvatnu klasifikaciju. Primarni cilj oba pristupa bio je pomoći pravnom sustavu da se uhvati u koštac s kompleksnim konceptom privatnosti (Solove, 2006). Ne ulazeći u način na koji pravnici i sudska praksa gledaju na povrede i ugroze privatnosti, možemo reći kako su oblici i načini povreda privatnosti brojni i mogu biti sasvim različiti. Držimo li se definicije privatnosti u terminima kontrole, pri ugrožavanju nečije privatnosti možemo razlikovati tko je taj koji nam oduzima kontrolu, nad kojim podacima, u kojem kontekstu, na

koji način, uz koje opravdanje te čini li to uz naše znanje ili čak i naše odobrenje. Ostanemo li bez kontrole pristupa (podacima o) sebi, ostajemo i bez privatnosti. Stoga ugroze privatnosti u najširem smislu možemo podijeliti na one kojima nam se oduzima kontrola i na one kojima kontrolu sami dobrovoljno predajemo. Dakako, samo se u prvom slučaju radi o neposrednim ugrozama privatnosti, dok je u slučaju dobrovoljne predaje kontrole primjerenije govoriti o *odricanju od privatnosti*. No, kako ćemo vidjeti u nastavku ovog poglavlja, upravo svojevoljno odricanje od privatnosti nerijetko dovodi do vrlo ozbiljnih i neželjenih ugroza privatnosti. Posebno je pitanje, ukoliko pravo na privatnost smatramo temeljnim ljudskim pravom zbog njegovog značaja za autonomiju, demokraciju i društvo, mogu li ga se građani doista tako olako odreći i trebaju li ga nacionalne države osigurati svojim građanima bez obzira na to što se oni žele odreći svoje privatnosti u zamjenu za bodove vjernosti ili pristup besplatnim mobilnim igricama. Iduće poglavlje primarno će se baviti upravo ovim pitanjima.

Dakle, budući da je upravo kontrola ključna za privatnost, ugroze privatnosti podijeljene su prema *lokusu kontrole* u dvije grube skupine koje su nazvane *eksterne* i *interne* ugroze privatnosti. Eksterne ugroze obuhvaćaju one ugroze privatnosti koje imaju intruzivne elemente, odnosno kojima se protiv volje pojedinaca, i bez njihova znanja, oduzima kontrola nad podacima o njima, odnosno podaci o njima se prikupljaju, obrađuju, dijele i pohranjuju. S druge strane, interne ugroze predstavljaju ugrožavanja privatnosti koja su posljedica svjesnih i često željenih ponašanja, odnosno radi se o svjesnom predavanju kontrole nad podacima o sebi nekome. Na primjer, eksternom ugrozom privatnosti možemo smatrati upad računalnih hakera u nečiju pohranu u oblaku u kojoj drži privatne fotografije, primjenu raznih mjera tajnog prikupljanja podataka od strane policije i slično. Osim elektronskih i komunikacijskih ugroza, u ovu skupinu spadaju i voajersko ponašanje, prisluškivanje razgovora koji se odvija u susjednoj sobi kao i bilo koji oblik prikupljanja podataka o pojedincu bez njegova znanja i privole. U svim ovim slučajevima radi se o gubitku kontrole nad podacima o sebi bez našeg znanja i pristanka. S druge strane, primjer interne ugroze može biti korištenje bankovnih kartica za plaćanje u trgovini, učlanjenje u razne programe vjernosti trgovaca, objavljivanje osobnih fotografija i podataka na društvenim mrežama, slanje svoje fizičke lokacije na poslužitelje radi primanja reklama skrojenih baš za vas i slična ponašanja. U ovim se primjerima radi o aktivnostima u kojima su pojedinci svjesni kako svoje podatke, odnosno kontrolu nad njima, predaju trećoj strani i to čine potpuno voljno, a nerijetko i vrlo rado.

Dakako, radi se o gruboj podjeli i ponekad je teško razgraničiti između te dvije kategorije. U slučaju video-nadzora na javnim površinama, koji je u svijetu, a sve više i u Hrvatskoj, postao standard u javnom prostoru, nije jednostavno reći radi li se o eksternoj ili internoj ugrozi. S jedne strane u tom je slučaju prikupljanje podataka pasivno, kamere moraju biti vidljive, a obavijesti o snimanju jasno istaknute. Međutim, reći da smo dali pristanak da nas se snima, i da se brojni i vrlo intimni antropometrijski podaci o nama spremaju i obrađuju, samo zato što smo prošetali nekim trgom ili ušli u neku trgovinu je u najmanju ruku cinično. Uostalom, argument pristanka i svjesnosti mogli bismo rastegnuti na način da sve zakonite ugroze privatnosti koje provode razne državne službe i agencije također smatramo internim ugrozama, jer smo kroz predstavničko zakonodavno tijelo sami odabrali i željeli upravo takve ugroze, no tako karikiran taj je argument barem jednako ciničan. Svrha ove podjele nije uspostava sveobuhvatne i precizne kategorizacije ugroza privatnosti, nego ona služi za ilustraciju dvaju različitih psiho-socijalnih procesa koji su u pozadini tih ugroza. Pri tome će eksterne ugroze biti predstavljene kroz paradigmu *države nadzora*, a interne ugroze kroz paradigmu *društva izlaganja*.

S jedne strane, kada govorimo o državi nadzora, u njezinoj je pozadini legitimna težnja nacionalnih država za osiguravanjem svoje opstojnosti, suvereniteta, sigurnosti te promoviranja nacionalnih interesa, za što im je prikupljanje podataka o drugima bez njihova znanja vrlo korisno, a katkada i nužno. S druge strane, kada govorimo o društvu izlaganja, u njegovoj su pozadini ljudske potrebe za povezivanjem i sviđanjem zbog čega ljudi mnogo i olako dijele velike količine osobnih i intimnih podataka s drugima, a objavljivanjem tih podataka na internetu i s nepoznatom trećom stranom. Unatoč tome što su u pozadini eksternih i internih ugroza sasvim različiti psihološki i društveni procesi, radi se o dvije izuzetno aktualne paradigme kojima se na značajan način ugrožava privatnost, a time se ugrožava i autonomija pojedinaca te se derogira pravo na privatnost, što predstavlja prijetnju demokraciji, društvu u cjelini i temeljima na kojima su sazdane moderne liberalne nacionalne države.

2.2. Država nadzora

Jedan od glavnih izvora eksternih ugroza privatnosti svakako su moderne obavještajne službe, osobito one ustrojene radi nadzora telekomunikacija. Nije tajna da države žele znati što misle i smjeraju druge države kao i da žele znati što misle i rade pojedinci i institucije koji bi mogli ugroziti njihove nacionalne interese ili sigurnost. To je nužno radi samog opstanka države, ali i radi njezina napretka. Osim vlastita opstanka i osiguravanja nacionalnih interesa, jedna od

osnovnih zadaća moderne države je uspostava vladavine prava i osiguranje sigurnosti svojim građanima. Kako bi država mogla na vrijeme znati tko njoj ili njezinim građanima želi zlo, koristila je usluge obavještajnog sustava.

Špijunažu, prikupljanje tajnih podataka o nekome bez njegova znanja, smatra se jednim od najstarijih poznatih ljudskih poslova, ako ne i najstarijim. Ljudi su još od najranijih zajednica željeli znati što netko drugi misli i koji su mu planovi. Postoje naznake da je upravo pojava trača bila jedna od prvih odskočnih dasaka naglog kognitivnog razvoja kojim se naša vrsta strelovito razvila, a trač je prvim sapiensima omogućio stvaranje bolje povezanih zajednica (Harari, 2014). Još se u Starom zavjetu eksplicitno spominje Božja uputa Mojsiju neka pošalje ljude kako bi istražili kanaansku zemlju koju je namijenio Izraelcima, od njih traži da je razgledaju, utvrde kvalitetu zemlje, ratnu sposobnost naroda i to na koji su način osigurani gradovi (Biblija, 1983: Knjiga Brojeva 13:1-2, 18-21), *de facto* daje im uputu za špijuniranje[4]. Sve od vremena Sun Tzua pa do nedavnog značajnijeg razvoja tehnologije krajem dvadesetog stoljeća, špijunaža se svodila na prikupljanje informacija o nekome neposrednim promatranjem ili posredno preko suradnika. Whitaker dvadeseto stoljeće naziva stoljećem špijuniranja budući da je, kako navodi, „tek tada obavještajno djelovanje postalo organizirana birokratska aktivnost sa svojom vlastitom specijaliziranom institucionalnom strukturom, svojim tehnologijama, svojim bazama podataka i svojom poluatuonomnom ulogom u globalnim politikama“ (Whitaker, 1999: 5). Tek je s razvojem elektronike i telekomunikacija započela nova era špijuniranja koja je omogućila znatno olakšani pristup informacijama o ljudima te osobito pristup informacijama na daljinu. Čini se da države to nisu gledale prekriženih ruku.

Nakon II. svjetskog rata, te osobito u vrijeme Hladnoga rata, došlo je do značajnih promjena u obavještajnom djelovanju. Dok je istočni blok ustrajao na vrlo zahtjevnom, skupom i kompliciranom prikupljanju podataka posredstvom ljudskih izvora tvz. HUMINT, SAD se sve više okretao automatiziranom prikupljanju podataka tzv. TECHINT, među kojima je dominiralo prikupljanje podataka iz signala tzv. SIGINT. Poznat je slučaj sovjetskog rušenja američkog špijunskog zrakoplova Lockhead U2 u svibnju 1960. godine koji je razotkrio dio američkog SIGINT programa (Pedlow i Welzenbach, 1998). Nadalje, doslovno desecima godina raspravljalo se o tome postoji li doista američki sustav za nadzor komunikacija ECHELON. Put od prvih teoretičara zavjera do konačne potvrde trajao je gotovo pola stoljeća.

[4] Za vrlo detaljan povijesni pregled razvoja kriptografije od 1900. g.p.n.e. pa do listopada 2000. godine vidi (Solomon, 2003)

Čak ni nakon što je 2001. godine Europski parlament objavio izvješće dvogodišnjeg privremenog odbora EP-a o ECHELON-u, prema kojem „nije bilo sumnje da se pod tzv. UKUSA sporazumom provodi globalni sustav za nadzor komunikacija“ (Gerhard Schmid, 2001), SAD nisu službeno priznale postojanje takvog programa. Znakovito je da to službeno izvješće Europskoga parlamenta počinje citatom rimskog pjesnika Juvenala „*Sed quis custodiet ipsos custodes?*“ (Juvenal, n.d.: ll. 347–348), što u prijevodu s latinskoga znači *Tko će čuvati čuvare?*, a kontekstu Juvenalove pjesme može se razumjeti i kao *tko će nadzirati nadzornike*, *tko će motriti motritelje?*

I doista, tko će čuvati čuvare, tko će nadzirati nadzornike? Danas se za opisivanje sveobuhvatnog i nekritičkog nadzora koristi termin *država nadzora* (eng. Surveillance state) i možemo reći kako je u svega nekoliko godina postao uvriježen. Među prvima nacionalnu državu nadzora opisao je pravnik Jack Balkin kao „posebnu vrstu informacijske države – države koja pokušava identificirati i riješiti probleme upravljanja pomoću prikupljanja, analiziranja i stvaranja informacija.“ (Balkin, 2008: 3). Kao pravnik, Balkin demistificira državu nadzora te rezignirano tvrdi kako „nije pitanje hoćemo li imati državu nadzora, nego je pitanje kakvu ćemo državu nadzora imati“ (Balkin, 2008: 3–4). Hoćemo li dopustiti neograničeni i nekritički nadzor ili ćemo nadzirati nadzornike? Kada govorimo o državi nadzora, važno je najprije pojasniti koncept panoptikona i posebice panopticizma kao metafore za društvo nadzora utemeljeno na disciplini.

2.2.1. Panoptikon

Gotovo je nemoguće pronaći rad iz područja studija nadzora (eng. surveillance studies) koji se ne referira na panoptikon, poseban oblik građevine koji je prvi opisao Jeremy Bentham 1787. godine. Naime, Bentham je inspiriran idejom koju mu je dao brat Samuel, 1787. godine iz Kričeva u Bijeloj Rusiji, nepoznatom prijatelju u Englesku poslao nekoliko pisama i arhitektonske nacrte koji su prikazivali panoptikon, prstenastu građevinu sastavljenu od prostorija koje su orijentirane prema središtu u kojem se nalazi toranj iz kojega se kroz velike prozore moglo jasno vidjeti u svaku prostoriju (Bentham, 1787). Pri tome je ključno bilo osigurati da promatrač iz tornja jasno može u svakom trenutku vidjeti bilo koji kutak građevine, dok se njega ne može vidjeti ni iz kojeg dijela građevine. Bentham je panoptikon primarno zamislio kao novi oblik kaznionice u Irskoj, no smatrao je da se panoptikon može koristiti i za dizajniranje različitih građevina kao što su ubožnice, tvornice, bolnice i škole. Glavne prednosti

svojeg novog dizajna vidio je u tome što bi *stvarnu prisutnost* stražara mogla zamijeniti *očigledna sveprisutnost*, pod čime je Bentham podrazumijevao stalnu neizvjesnost mogućeg nadzora koju bi svaki korisnik građevina osjećao (Bentham, 1787). Bentham je smatrao da se ljudi ljepše ponašaju kada vjeruju da su promatrani pa je zbog toga za održavanje reda u kaznionici dizajniranoj po uzoru na panoptikon bilo potrebno znatno manje stražara i bila je znatno manja mogućnost širenja zaraza (Bentham, 1787). Držao je da njegov dizajn doprinosi slobodi, ekonomičnosti upravljanja i bio je izuzetno ponosan na svoj dizajn. Možda najviše stoga što je smatrao da je ujedno doskočio i *jednom od najintrigantnijih političkih pitanja*, kako je nazvao upravo ono ranije spomenuto Juvenalovo pitanje *Tko će nadzirati nadzornike?*, time što je tvrdio da će zbog specifičnog dizajna panoptikona i stražari koji su u neposrednom kontaktu sa zatvorenicima prema njima biti korektniji, i sami svjesni da u svakom trenutku mogu biti promatrani od nadzornika kaznionice (Bentham, 1787). Bentham je kaznionicu dizajniranu kao panoptikon smatrao humanom te ogromnim unaprjeđenjem postupanja prema zatvorenicima za to vrijeme (Schofield, 2009). Bio bi izuzetno nezadovoljan kada bi saznao da je njegov dizajn panoptikona, ponajviše zahvaljujući Foucaultu, postao glavna metafora za društvo nadzora i represije.

Naime, u svojem djelu *Nadzor i kazna: rađanje zatvora*, Foucault koristi Benthamov panoptikon kao metaforu za sveprisutni nadzor u modernoj državi. Za Foucaulta panoptikon nije (samo) arhitektonsko ili tehničko rješenje, već *politička tehnologija* koja predstavlja osnovu cijelog novog društva, *disciplinatornog društva*, koje koristi *sveprisutni nadzor* kao metodu discipline kako bi osnažilo vlasti, osujetilo otpor, izazvalo pokornost (Foucault, 1995). Za Foucaulta je glavni disciplinatorni učinak panoptikona bio „izazvati u zatvoreniku stanje svjesne i stalne vidljivosti koja osigurava automatsko djelovanje moći“ (Foucault, 1995: 201), što je nadogradnja Benthamove *očigledne sveprisutnosti*. U podlozi automatskog djelovanja moći jest Benthamova ideja da će ljudi koji vjeruju da su promatrani internalizirati pravila, prihvatiti ih kao svoja, te će stoga kažnjavanje postati suvišno. U tom trenutku više neće biti važno ima li nekoga u tornju, promatra li uopće netko zatvorenike i tada će biti uspostavljeno automatsko djelovanje moći. Za uspostavu socijalnog reda puka izloženost pogledu postaje značajnija od činjenice gleda li uopće netko. Kao što je navedeno u prethodnom poglavlju, izlaganje prema drugima, oduzima nam autonomiju. A to osobito vrijedi za ono izlaganje, za ono oduzimanje kontrole nad (podacima o) nama, koje je protiv naše volje. Društvene norme, formalne i neformalne, izazivaju autocenzuru i udovoljavanje stereotipu, što pojedince

ukalupljuje i disciplinira. Bentham i Foucault prepoznali su kako za taj proces čak nije ni nužno nekoga doista izložiti pogledu, već je dovoljna sama činjenica da je čovjek uvjeren kako bi u bilo kojem trenutku mogao biti izložen pogledu kako bi se korigirao, prilagodio, suspregnuo, disciplinirao. Da bi došlo do automatskog djelovanja moći.

Opisujući sâm dizajn panoptikona, Foucault je primijetio inverziju u odnosu na klasični princip tamnice. Dok je tamnica imala funkciju deprivirati od svjetla i izolirati, panoptikon je uređen na način da je u svakoj ćeliji prisutno mnogo svjetla kako bi nadzornik imao slobodan pogled na svaki kutak ćelije. Za Foucaulta tama na određeni način štiti i čuva zatvorenika, dok je upravo izloženost svjetlu i pogledu problematična. „Vidljivost je zamka“ navodi Foucault (Foucault, 1995: 200), i ona to doista jest, kao što će biti prikazano u nastavku ovog poglavlja.

Najveći iskorak Foucaulta u odnosu na Benthama bio je u tome što je panoptikon kao dizajn građevine ekstrapolirao na razinu uređenja cijeloga društva koje se zasniva na discipliniranju, a koristi istu mehaniku discipliniranja – iluziju stalne nadziranosti. U tu je svrhu skovao i pojam *panopticizma*, koji je za njega bio „glavni princip nove političke anatomije čija svrha i cilj nisu utemeljeni na suverenitetu nego na disciplini“ (Foucault, 1995: 208). Njime je želio objasniti logiku koja se može vidjeti u dizajnu poslovnog okruženja, javnog prostora, ključnih društvenih, zdravstvenih, obrazovnih i psiholoških ustanova (Elmer, 2012). I doista, dok sam arhitektonski dizajn panoptikona nije zaživio i danas ne postoji mnogo zatvora, bolnica, škola i tvornica koje su izgrađene kao panoptikoni, razvoj tehnologije veći dio modernoga svijeta pretvorio je u panoptikon. U modernim gradovima teško je pronaći kutak javnoga prostora koji nije pokriven nadzornim kamerama, a kamerama su pokrivene brojne škole, bolnice, tvornice, privatne zgrade i stanovi. Uđete li danas u trgovački centar ili zgradu zračne luke, koje ni po čemu ne izgledaju kao Benthamov panoptikon, negdje u nekoj nadzornoj sobi nalazi se zaštitar koji ima mogućnost vidjeti svaki kutak te zgrade. Foucault je bio u pravu kada je tvrdio da je panoptikon nadišao arhitektonski dizajn i da je postao sinonim za uređenje društva utemeljenog na potpunoj izloženosti.

Iako se Foucault propustio referirati na Benthamovu očiglednu namjeru za podizanjem humanog postupanja prema zatvorenicima te unatoč tome što postoje autori koji opsežno kritiziraju njegovo razumijevanje discipliniranja u modernoj državi (Haggerty, 2006; Lyon, 1993; Mathiesen, 1997; Murakami Wood, 2007), Foucaultove su ideje inspirativne i ne čudi utjecaj koji je Foucault imao na teoretičare studija nadzora. Predstavljajući javnosti spoznaje

do kojih je došao intervjuirajući mladog tehničara i zviždača Edwarda Snowdena, novinar Glenn Greenwald prepoznao je Foucaultov panopticizam upravo u *modusu operandi* i razmjerima sveobuhvatnog nadzora komunikacija koje provode NSA i partnerske agencije (Greenwald, 2014).

Kao što je ranije spomenuto, nije tajna da države iz različitih razloga žele znati što njezini neprijatelji rade, što rade druge države i što rade osobe koje mogu ugrožavati sigurnost države i/ili njezinih građana. Represivni i obavještajni aparat raspolažu vrlo sofisticiranim sustavima i metodama prikupljanja podataka. Međutim, postoji značajna razlika u načinu postupanja represivnog aparata, odnosno policije i državnog odvjetništva, i načinu postupanja obavještajnog sustava. Represivni aparat u pravilu se aktivira *nakon* što se dogodio prekršaj ili kazneno djelo i na temelju saznanja o događaju pokušava identificirati počinitelja i prikupiti dokaze kako bi mogao biti osuđen u pravednom postupku pred sudom. S druge strane, za obavještajni aparat možemo reći kako koristi potpuno suprotni način djelovanja. Obavještajni aparat s određenom dozom vjerojatnosti pretpostavlja *tko* bi mogao napraviti *nešto*, no to *nešto* je toliko veliko i ozbiljno da se ne smije dogoditi. Ovo je, dakako, vrlo pojednostavljeni prikaz i postoje značajna preklapanja u određenim metodama i područjima rada. Lako je prihvatiti činjenicu da nakon počinjenog zločina, policija na temelju osnovnih prikupljenih dokaza s mjesta događaja usmjeri istragu prema određenim sumnjivim osobama te da prema nekome od njih, nakon što je temeljem obrazloženog zahtjeva dobila odobrenje nadležnoga suda, započne primjenu mjera tajnog prikupljanja podataka i ostalih posebnih dokaznih radnji. S druge strane, sastavljanje obrazloženog zahtjeva za primjenu takvih intruzivnih mjera za osobu koja dosad nije učinila ništa protuzakonito, a za koju postoji tek pretpostavka da bi svojim djelovanjem mogla na značajan način ugroziti javnu sigurnost građana ili nacionalnu sigurnost jedne države, vrlo je teško i nezahvalno. No, katkada je nužno. Jedno je pronaći otiske na oružju pronađenom na mjestu zločina te na temelju toga prema osobi čiji su ti otisci primijeniti postupanja kojima joj se ograničavaju temeljne slobode, a drugo je ograničiti temeljne slobode nekome na temelju podataka da simpatizira neku radikalnu skupinu, da se sastaje s nepoželjnim osobama, ima radikalne stavove ili jednostavno da se nalazi na krivom mjestu u krivo vrijeme. Istovremeno, propuštanje praćenja takvih pojedinaca, njihovih aktivnosti i osoba s kojima stupaju u kontakte potencijalno bi moglo ugroziti ljude ili državu na način znatno gori od bilo kojeg pojedinačnog krvnog delikta. Svjedoci smo terorističkih napada diljem svijeta koje čine pojedinci nerijetko

bez kriminalne povijesti i za čije je identificiranje potreban upravo pristup kakav koriste moderne obavještajne službe.

Većina zapadnih demokracija takvom problemu doskočila je na način da je obavještajnim službama dala vrlo široke ovlasti, ali je usporedo s time ustrojila temeljit i nezavisan nadzor nad njihovim postupanjem. Međutim, nedavna otkrića zviždača iz obavještajnih struktura koja će biti prikazana u nastavku, ukazuju na to kako ustrojavanje nezavisnog nadzora nije bilo dovoljno te da su određene države i/ili njihove obavještajne službe svoje ovlasti, ingerenciju i razmjere zatiranja temeljnih sloboda na svoju ruku odlučile značajno proširiti.

2.2.2. Nemaš se kamo sakriti: država nadzora kao paradigma eksternih ugroza privatnosti

Za ilustriranje države nadzora kao paradigme eksterne ugroze privatnosti bit će korišteni aktualni podaci o kapacitetima i mogućnostima nadzora komunikacija te o nekritičkom nadzoru pojedinih obavještajnih službi koje je 2013. godine razotkrio mladi tehničar Edward Snowden te dio dokumenata objavljenih 2017. godine iz *Vault 7* serije objava WikiLeaksa o aktivnostima i sposobnostima CIA-e, Središnje obavještajne agencije SAD-a.

Jedno od najvećih otkrića prekoračenja ovlasti i razotkrivanje razmjera nadzora svakako je ono mladog tehničara Edwarda Snowdena u lipnju 2013. godine. Svega nekoliko dana nakon što je troje istraživačkih novinara koji su se dokazali u borbi za ljudska prava Glenn Greenwald, Laura Poitras i Ewen MacAskill započelo s dnevnim objavama tekstova o tajnim dokumentima koje im je Snowden ustupio, on se osobno obratio javnosti iz hotelske sobe u Hong Kongu[5] (Greenwald, MacAskill i Poitras, 2013). Snowden je u to vrijeme bio dvadesetdevetogodišnji analitičar u tvrtki *Booz Allen Hamilton*, koja je obavljala određene tehničke poslove za *National*

[5] Zapravo, iz Oskarom nagrađenog dokumentarnog filma Laure Poitras Citizenfour (Poitras, 2014), kojim su zabilježeni ključni trenuci vrlo dramatična zajednička boravka troje novinara i Snowdena u hotelu Mira početkom lipnja 2013. godine, pa i njihova rasprava o tome treba li Snowden javno istupiti, može se vidjeti kako je to učinio upravo kako bi skrenuo pozornost sa sebe te kako bi se javnost mogla umjesto *lova na vještice* posvetiti razumijevanju razmjera nadzora koji su novinari u to vrijeme počeli razotkrivati temeljem dokumenata koje im je predao. Danas, pet godina kasnije, Snowden je visokokontroverzna osoba. Za borce za slobodu interneta i ljudska prava, Snowden predstavlja gotovo avatarsko uobličenje njihove borbe dok ga s druge strane političkoga spektra mnogi, mahom konzervativni realisti, smatraju izdajicom koja je ugrozila nacionalnu sigurnost, gospodarstvo i živote mnogih Amerikanaca te bi ga rado vidjeli zatvorenoga. Unatoč činjenici da je Snowdenov status i dalje neizvjestan te da se u ovom trenutku nalazi negdje u okolici Moskve gdje uživa privremenu međunarodnu zaštitu Ruske Federacije, njegova su otkrića dovela do značajnih promjena. U SAD-u je pokrenuta ozbiljna rasprava o ovlastima sigurnosnih službi, a čelnici država diljem svijeta, od Njemačke do Brazila, ujedinili su se u kritici nekontroliranog nadzora što je rezultiralo i revizijom uredbi EP te uspostavom posebnog izvjestitelja za privatnost UN-a. Uostalom, i ovaj je rad, kao i značajan dio literature na kojoj se temelji, nastao upravo zahvaljujući otkrićima Edwarda Snowdena.

Security Agency, američku obavještajnu službu za nadzor komunikacija. Prethodno je bio radio i za američku vanjsku obavještajnu službu CIA-u kao i u nekoliko privatnih tehnoloških tvrtki koje su bile podizvođači različitih službi američkog obavještajnog sustava. Detaljniji prikaz Snowdenove biografije s posebnim naglaskom na motive zbog kojih je odlučio postati zviždač, napisao je Glenn Greenwald u knjizi *No Place to Hide* (Greenwald, 2014). Snowden se još kao dvadesetogodišnji mladić prijavio u vojsku s namjerom odlaska u Irak, no vrlo ga je brzo odbila činjenica kako je za vrijeme osnovne obuke većina trenera bila znatno više motivirana ubijanjem Arapa nego pomaganjem ljudima (Greenwald, MacAskill i Poitras, 2013). Tijekom zaposlenja u CIA-i, vrlo je brzo napredovao te je zbog svojih sposobnosti upućen u ispostavu u Genevu. Ondje je imao pristup znatno većem rasponu klasificiranih dokumenata među kojima je vidio „vrlo loše stvari" i zaključio je kako je „ono što njegova vlada radi u svijetu znatno drugačije od onoga kako su ga učili" (Greenwald, 2014: 47). Na njegovu frustraciju utjecala je i suradnja s operativcima CIA-e na način da su ga neke, iz njegove perspektive, moralno i legalno dvojbene operacije regrutacije agenata natjerale da dodatno preispita svoju ulogu u sigurnosnom sustavu. Već je tada razmišljao o izlasku iz sigurnosnog sustava, no vjera u promjenu koju je donio početak prvog mandata predsjednika SAD-a Baracka Obame zadržala ga je u sustavu. No, trebalo je vrlo kratko kako bi shvatio da se ništa nije promijenilo, a u mnogim slučajevima zloupotrebe sustava dodatno su proširene (Greenwald, 2014). Tijekom narednih godina radio je uglavnom za kooperante NSA-e te je u tom razdoblju prikupio brojne podatke o nekritičkom i sveobuhvatnom nadzoru te „o namjeri NSA-e da bude upoznata sa *svakim razgovorom i svakim oblikom ponašanja na svijetu*" (Greenwald, MacAskill i Poitras, 2013: 1). Smatrao je da ono što NSA čini predstavlja egzistencijalnu prijetnju demokraciji te je bio uvjeren kako se radi o narušavanju temeljnih sloboda i kršenju američkoga ustava koje američka javnost nikada ne bi odobrila samo kada bi uopće znala da se ona odvija u njihovo ime (TED, 2014).

Snowden je tako odabrao dvoje istraživačkih novinara koji su se u svojem radu dokazali kao istaknuti borci za ljudska prava, a i sami su na svojoj koži osjetili metode američkoga obavještajnoga sustava, Greenwalda i Poitras. U zadnji čas prije susreta sa Snowdenom u Hong Kongu pridružio im se i Guardianov istraživački novinar Ewen MacAskill. Snowden im je ustupio enormnu količinu izvornih dokumenata, prezentacija, sudskih naloga, rješenja, izvještaja različitih američkih institucija vezanih uz obavještajni sustav te partnerskih obavještajnih agencija, a poglavito britanske agencije za nadzor signala GCHQ. Točan broj

dokumenata koje je Snowden preuzeo iz sustava nikada nije objavljen, a prema izjavi američkog kongresmena Mikea Rogersa, u izvještaju Pentagona stoji kako se radi o 1,7 milijuna dokumenata (Strohm i Wilber, 2014). Nije poznato ni koliko je dokumenata doista predao novinarima, ali vjeruje se kako se radi o otprilike 200 000 dokumenata (Ignatius, 2014). Većina dokumenata bila je aktualna i klasificirana najvišim stupnjem tajnosti, a najosjetljiviji su povrh toga bili ograničeni za dijeljenje isključivo unutar *Five Eyes* obavještajnog savezništva između SAD-a, Velike Britanije, Kanade, Australije i Novog Zelanda (Greenwald, 2014: 92). Dokumente najbolje opisuje upravo jedan od novinara kojemu su ustupljeni: „Čak i meni kao nekome tko je proveo godine pišući o opasnostima tajnog nadzora SAD-a, sama rasprostranjenost špijunskih sustava bila je istinski šokantna. Tim više što je očigledno cijeli sustav implementiran bez odgovornosti, transparentnosti i bez granica.“ naveo je Greenwald (Greenwald, 2014: 92). Nakon početka objave priča o dokumentima, američka i svjetska javnost trenutno je bila zgrožena. I doista, programi i aktivnosti NSA i određenih partnerskih agencija koji su razotkriveni u Snowdenovoj objavi[6] daju razloga za zabrinutost.

Dakako, sigurnosne službe nadziru građane. Upravo je to jedan od osnovnih razloga njihova postojanja, a represivni i sigurnosni sustav sastavni su dio države. Sigurnosne službe imaju ovlasti, ali i dužnost, uz opravdani razlog ograničavati određena ljudska prava određenim osobama na ograničeno vrijeme. Pri čemu sva četiri uvjeta moraju u svakom trenutku biti zadovoljena – opravdani razlog, samo neka ljudska prava, samo nekim osobama za koje postoji opravdani razlog te na ograničeno vrijeme. Bilo što drugo predstavljalo bi prekoračenje ovlasti sigurnosnog sustava, a u eventualnom slučaju da je takvo postupanje utemeljeno na zakonu neke države, ono naprosto ne bi bilo i ne može biti u skladu s temeljnim postavkama liberalne demokracije.

Iz Snowdenove objave čini se da su obavještajne službe udružene u Five Eyes savezništvo, a osobito američke i britanske, po više točaka bile prekoračile svoje ovlasti. Količina izvornih

[6] Snowden zapravo sam nije objavio niti jedan dokument. Unatoč tome što je svojim činom i sam narušio privatnost, a dijelom i sigurnost svojih kolega, ali i osoba koje ni na koji način nisu odgovorne, svjestan činjenice da je velik dio dokumenata iz opravdanih razloga klasificiran i označen određenim stupnjem tajnosti budući da bi nekritičko objavljivanje dokumenata moglo ozbiljno naštetiti operativcima na terenu i njihovim agentima te da bi moglo ugroziti mnoge vrlo ozbiljne i opravdane sigurnosne operacije, Snowden je dokumente ustupio istraživačkim novinarima. Nadalje, smatrao se pristranim i nije se osjećao dovoljno kompetentnim za najbolji način komuniciranja prema javnosti. Stoga je način, tempo i sadržaj objava, a dijelom i svoju sudbinu, u potpunosti prepustio novinarima od kojih je tražio da pronađu najbolji način kako bi upoznali javnost s razmjerima kršenja američkoga ustava i ljudskih prava, a da istovremeno maksimalno zaštite ljude na terenu i nacionalnu sigurnost. Stoga će u ovom radu za otkrića novinara temeljem dokumenata koje im je ustupio Snowden biti korišten termin *Snowdenove objave*.

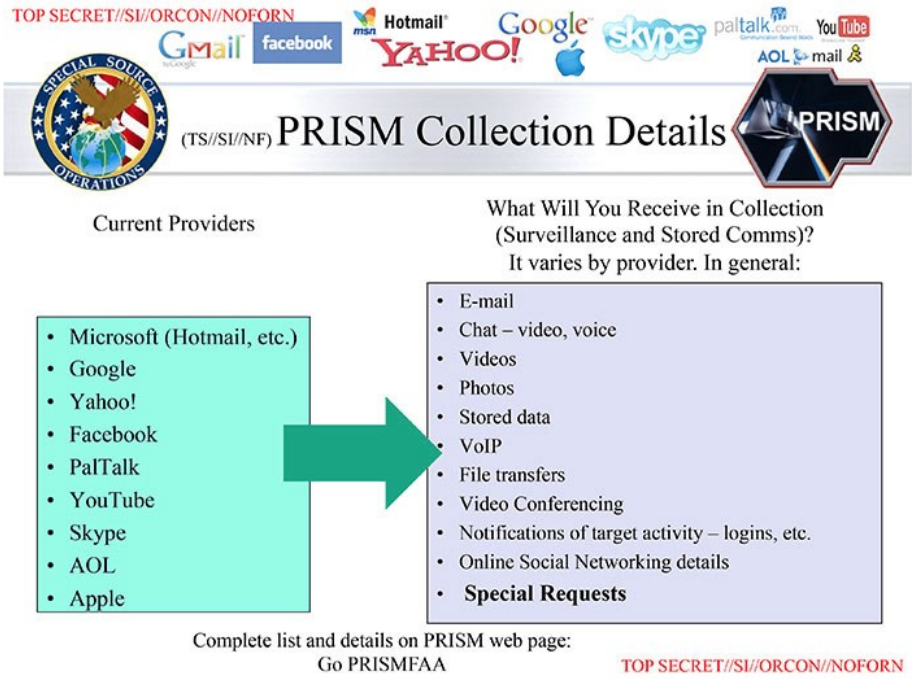
dokumenata iz Snowdenove objave koji je do danas objavljen broji se u tisućama, a samo broj tajnih programa i njihovih kodnih imena prelazi stotinu[7]. Ovdje će biti pružen uvid u ključne programe i načine djelovanja kojima su na najteži način kršene međunarodne konvencije i ugrožavana je privatnost ljudi diljem svijeta. Među svim razotkrivenim načinima na koje su NSA i GCHQ djelovali i kako su sve prikupljali podatke, izdvajaju se dva posebno sporna: nekritičko prikupljanje podataka i potkopavanje sigurnosti informacijskih sustava i elektroničkih uređaja. Nekritičkim prikupljanjem podataka prekršena su dva od četiri uvjeta pod kojima bi se privatnost mogla ograničiti, prikupljano je znatno više podataka nego što je nužno, i prikupljani su podaci o osobama za koje nije postojao opravdani razlog. Naime, putem programa kao što su PRISM, MUSCULAR, TEMPORA, UPSTREAM i brojni drugi, službe iz savezništva Five Eyes prikupljale su enormnu količinu podataka o izuzetno velikom broju korisnika, među kojima velika većina nije, i nikada neće biti, predmet njihova interesa niti je bilo utemeljenog razloga za prikupljanje podataka o njima. I drugi posebno sporan način jest potkopavanje enkripcije. Naime, NSA i GCHQ namjerno su potkopavali enkripciju i oslabljivali su sigurnost popularnog hardvera i softvera kako bi prema potrebi lakše pristupali podacima o osobama od interesa, čime su napravili nemjerljivu štetu milijunima drugih korisnika koji nikada neće biti predmet njihova interesa.

2.2.3. Nekritičko prikupljanje podataka

Za nekritičko prikupljanje podataka dominantno je zadužen NSA-in Odjel za operacije posebnih izvora (eng. *Specal Source Operations division*). Njihov program koji je vjerojatno izazvao najveću buru u javnosti jest NSA-in PRISM. Radi se o programu koji je NSA-i omogućio direktan pristup poslužiteljima i informacijskim sustavima velikih američkih internetskih tvrtki kao što su Google, Microsoft, Apple, Facebook, YouTube, Skype kako bi preuzimao brojne podatke iz širokog spektra podataka o njihovim korisnicima (Greenwald i MacAskill, 2013a). Mnoge tvrtke poricale su sudjelovanje u programu PRISM (Greenwald i MacAskill, 2013a; Rushe, 2013), a Odbor za nadzor nad privatnosti i građanskim slobodama SAD-a u svojem je izvješću prikazao značajno ograničen doseg programa, prema kojem podaci nisu prikupljani nekritički već ciljano i to isključivo temeljem zadanih selektora (Medine, Brand, Cook, Dempsey i Wald, 2014). Međutim, izvorni slajdovi iz internih prezentacija NSA-

[7] Za prikaz svih do sada objavljenih dokumenata iz Snowdenove objave vidi https://search.edwardsnowden.com/. Radi se o redaktiranim dokumentima koji su obrađeni i odabrani na način da njihova objava ne bi trebala ugrožavati ljudske živote te nacionalnu i gospodarsku sigurnost. Pregled svih obrađenih tema s popisom članaka i izvornih dokumenata nalazi se na vezi https://edwardsnowden.com/revelations/

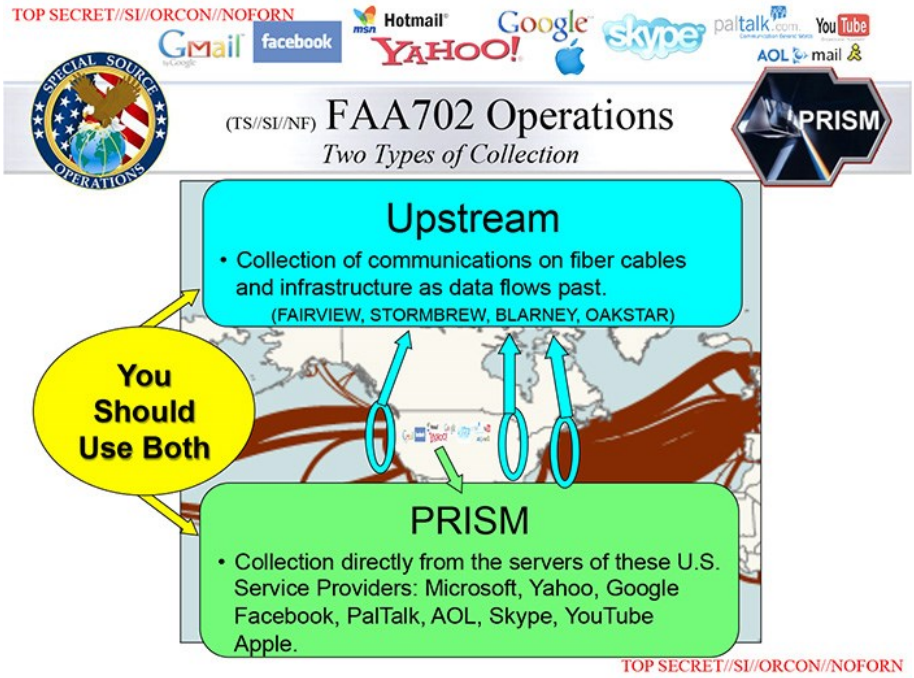
e kojima je program predstavljan vlastitim analitičarima i korisnicima nedvojbeno demantiraju navode o ograničenom nadzoru (vidi sliku 1.)



Slika 1. - Jedan od slajdova prezentacije PRISM/US-984XN Overview iz travnja 2013. godine - preuzeto s https://edwardsnowden.com/2013/06/07/prism-overview-slides/

Iz tih je izvornih dokumenata očigledno kako se radi o prikupljanju širokog raspona podataka poput sadržaja e-pošte, sadržaja čavrljanja, videozapisa, fotografija, pohranjenih dokumenata i podataka, sadržaja telefonskih razgovora upućenih putem određenih aplikacija poput Skype-a, videokonferencija i slično. Donekle sličan program je i GCHQ-ev MUSCULAR, koji je provođen u bliskoj suradnji s NSA-om. Doduše, za razliku od PRISM-a, kojim se pristupalo dekriptiranim podacima direktno s poslužitelja tvrtki, i uz njihovo znanje (Greenwald, MacAskill, Poitras, Ackerman i Rushe, 2013), programom MUSCULAR tajno je provaljeno u glavne komunikacijske veze između podatkovnih centara Googlea i Yahooa (Gellman i Soltani, 2013). Naime, obje su tvrtke kriptirale podatke tek kada bi oni napuštali njihov računalni oblak i kada bi bili slani prema korisnicima, dok podatke koji su kolali između njihovih podatkovnih centara nisu kriptirali. Budući da i Google i Yahoo posjeduju podatkovne centre po cijelome svijetu i da se podaci stalno dijele između tih centara, bilo je moguće pristupiti korisničkome sadržaju dok je on putovao između dva podatkovna centra. Stuart Sumner logiku kojom se Google vodio slikovito je opisao analogijom „ako ljudi ne mogu preskočiti tvoju ogradu, nema potrebe zaključavati vrata kuće“ (Sumner, 2015: 24). Međutim, programom MUSCULAR

preskočena je ograda te su, unatoč snažnoj enkripciji sadržaja koji se razmjenjivao s korisnicima, GCHQ i NSA mogli slobodno prikupljati korisničke podatke. A prikupljali su mnogo. Jedan slajd prikazuje kako je samo u jednom 30-dnevnom razdoblju tijekom prosinca 2012. i siječnja 2013. godine iz britanskih centara za prikupljanje podataka u NSA poslano preko 181 milijun različitih zapisa putem pristupne točke DS-200B putem koje su slani podaci prikupljani programom MUSCULAR (Gellman i DeLong, 2013b, 2013a).



Slika 2 - Jedan od slajdova prezentacije PRISM/US-984XN Overview iz travnja 2013. godine - preuzeto s https://edwardsnowden.com/2013/06/07/prism-overview-slides/

Osim putem tvrtki i pružatelja internetskih usluga (eng. *Internet Service Provider - ISP*) s čijih je poslužitelja direktno preuzimao podatke, NSA-in Odjel za operacije posebnih izvora podatke je prikupljao i tzv. *Upstream* prikupljanjem (slika 2.) Radi se o tajnom prisluškivanju ultrabrzih optičkih kablova koji čine tzv. kralježnicu interneta (Medine i dr., 2014). *Upstream* prikupljanje čini dvadeset programa, a podaci se prikupljaju na tri glavna načina: uz pomoć partnerskih tvrtki na području SAD-a, uz pomoć partnerskih tvrtki izvan SAD-a te putem *unilateralnih operacija*, što zapravo znači tajno i prikriveno prisluškivanje optičkih kablova.

Od svih Upstream programa, najviše se zna o programima FAIRVIEW i STORMBREW koji su korišteni na teritoriju SAD-a uz pomoć telekomunikacijskih tvrtki AT&T i Verizon, o programu BLARNEY kojim se od 1978. godine prikupljaju signali putem različitih

korporativnih partnera, te o programu OAKSTAR putem kojeg se uz pomoć sedam telekoma izvan SAD-a prikupljaju sirovi telekomunikacijski podaci (Greenwald, 2014; "NSA's global interception network," 2013; "Slides about NSA's Upstream collection," 2014). Ne računajući OAKSTAR, korištenjem samo tri navedena programa NSA je navodno imala kapacitet obuhvatiti čak 75% cjelokupnog internetskog prometa unutar granica SAD-a, od kojeg je značajne količine tog prometa i pohranjivala za naknadnu analizu (Gorman i Valentino-DeVries, 2013). Međutim, više podataka od svih NSA-inih Upstream programa prikuplja britanski GCHQ putem svojeg programa TEMPORA kojim se prisluškuju podvodni interkontinentalni optički kablovi (MacAskill, Borger, Hopkins, Davies i Ball, 2013). Radi se o masivnom programu s izuzetnim tehničkim kapacitetima za nadzor i pohranu, a broj osoba koje su zahvaćene nadzorom najbolje opisuje komentar GCHQ-evih odvjetnika kada ih je Guardian zatražio taj podatak, naime, naveli su im kako „bi to bio beskonačan popis koji uopće ne bi mogli sastaviti" (MacAskill i dr., 2013: 1).

Dakako, ovo je samo dio NSA-ine globalne mreže za prikupljanje podataka iz signala. Prema jednom od izvornih slajdova iz Snowdenove objave, djelovanje Odjela za operacije posebnih izvora koji uključuje Upstream i PRISM tek je jedan od pet dijelova globalne SIGINT platforme NSA. Drugi dijelovi uključuju razmjenu podataka u suradnji s partnerskim agencijama, nadzor satelitskih komunikacija te tzv. Uslugu posebnog prikupljanja (eng. *Special Colection Service*) koja označava zajedničku operaciju CIA-e i NSA kojom je posebna oprema za nadzor visokorangiranih meta poput stranih vlada i diplomatskih predstavništava postavljena u američka veleposlanstva i konzulate na 80 lokacija diljem svijeta (Boon, Derix i Modderkolk, 2013). Unatoč tome što su kapaciteti i mogućnosti takvih nadzora izuzetno snažni, ova tri načina naprosto ne spadaju u kategoriju nekritičkog prikupljanja podataka te time izlaze izvan okvira ovog rada. Međutim, posljednji, peti dio platforme, poslovi NSA-ina Odjela za operacije prilagođenog pristupa (eng. *Tailored Access Operations division*) zaslužuju posebnu pažnju te će biti obrađeni u sljedećem odjeljku.

Jasno je kako se radi o nezamislivo velikoj količini podataka koja se prikuplja te se može postaviti opravdano pitanje predstavlja li uopće takav masovni nadzor bez kriterija doista ugrozu privatnosti i ljudskih prava. Naime, čak ni stotine tisuća NSA-inih analitičara ne mogu pregledavati sve što se događa na internetu, u eteru i u ostalim medijima koje NSA nadzire. Međutim, NSA je za pretragu i pregledavanje prikupljanih podataka razvila vrlo sofisticiran i učinkovit alat XKEYSCORE. Taj alat omogućuje analitičarima da preko prijateljskoga sučelja

pretražuju metapodatke[8] i sadržaj, uživo ili pohranjene na poslužiteljima na način da zadaju općenite ili vrlo specifične selektore (Greenwald, 2013b). Putem XKEYSCORE-a može se pretraživati i čitati nečije e-poruke, dopisivanja putem društvenih mreža, pregledavati nečiju povijest web-preglednika, nečije kolačiće, u nekim slučajevima i korisnička imena i lozinke i brojne druge osjetljive podatke (Marquis-Boire, Greenwald i Lee, 2015). Od samog sadržaja kojem se moglo pristupiti, znatno više zapanjuju analitičke mogućnosti softvera koje su omogućavale povezivanje naizgled nespojivih podataka, a koji omogućuju identifikaciju pojedinca i analiziranje njegovih aktivnosti i kontakata. U prezentaciji NSA kojom se program promovira među potencijalnim korisnicima iz sigurnosnog sustava, prikazano je kako se ciljane osobe može pronaći traženjem anomalija poput potrage za nekime tko govori jezikom koji nije uobičajen za regiju u kojoj se nalazi, ili potrage za nekime tko koristi enkripciju ili jednostavno pretražuje na internetu određene sumnjive pojmove. Prikazan je i primjer praćenja jezika te se na taj način može izdvojiti, na primjer, sve osobe koje se nalaze u Pakistanu, a govore njemačkim jezikom. Poznavajući lokaciju pojedine točke od interesa, moguće je doći do svih korisnika koji su pretraživanjem karata na internetu proučavali upravo tu lokaciju (theguardian.com, 2013). Nadalje, za analizu, obradu i prikaz izuzetne količine sirovih metapodataka, NSA je razvila alat BUNDLESS INFORMANT (Greenwald i MacAskill, 2013b). Greenwald navodi kako su „u jednom 30-dnevnom razdoblju prikupljeni podaci o preko 97 milijardi poruka e-pošte i 124 milijarde telefonskih poziva diljem svijeta“ te kako se u drugom dokumentu o tom alatu nalaze podaci o tome kako je u 30-dnevnom razdoblju prikupljeno „500 milijuna podataka iz Njemačke, 2.3 milijarde iz Brazila, 13.5 milijardi iz Indije“, a nastavlja navoditi podatke iz trećih dokumenata „70 milijuna iz Francuske, 60 milijuna iz Španjolske, 47 milijuna iz Italije, 1.8 milijun iz Nizozemske, 33 milijuna iz Norveške i 23 milijuna iz Danske“ (Greenwald, 2014: 94). Navedeni brojevi doista govore sami za sebe. Prikupljanje tolikog broja podataka ne može biti ciljano već se nedvojbeno radi o prikupljanju svega što se može zahvatiti radi kasnije analize. Unatoč sofisticiranim analitičkim alatima, većina prikupljenih podataka nikada neće biti iskorištena niti će biti predmet analize.

[8] U obavještajnom žargonu, potrebno je razlikovati *sadržaj* i *metapodatke*. Za razliku od nadzora sadržaja, koji se odnosi na slušanje nečijeg razgovora, gledanje nečijih fotografija, čitanje nečijih poruka, pošte ili dokumenata, metapodaci se odnose na sve one podatke *o* tom sadržaju. U slučaju telefonskih poziva može se raditi o tome tko je, s koje lokacije, u koje vrijeme, pozivao koga, koristeći koji uređaj i koliko je taj poziv trajao. Za e-poštu metapodaci mogu označavati naslov poruke, e-adrese pošiljatelja i primatelja, IP adresu pošiljatelja, vrijeme slanja i slično (Greenwald, 2014). Unatoč tome što nadzor metapodataka načelno doista predstavlja nižu razinu ugroze od nadzora sadržaja, metapodaci pružaju znatno više informacija nego što se na prvi pogled čini. Uostalom, o značaju i učinkovitosti metapodataka najbolje govori citat bivšeg ravnatelja NSA-e i CIA-e Michaela Haydena „Mi ubijamo ljude temeljem metapodataka“ (Cole, 2014: 1)

Međutim, ti će podaci biti trajno pohranjeni i dostupni za analizu u bilo kojem trenutku. Kao što će biti detaljnije pojašnjeno u idućem poglavlju, jedno od temeljnih načela pri suspenziji ljudskih prava, među kojima je i privatnost, jest načelo proporcionalnosti. Nije moguće razumno opravdati prikupljanje *svega što se može zahvatiti* kao najmanje intruzivnu mjeru kojom je moguće postići ciljani učinak. Opisani masovni nadzor telekomunikacija predstavlja oduzimanje kontrole nad podacima ljudi i nad podacima o ljudima bez njihova znanja. Nije moguće znati je li poruku e-pošte koju smo jutros poslali pročitao netko osim osobe kojoj je namijenjena. Međutim, spoznaja da je može pročitati netko osim osobe kojoj je namijenjena utječe na njezinu formu i sadržaj. Ne samo da se na taj način suspreže mogućnost subverzije i kritike, osobito kod aktivista, zviždača i političke oporbe, već se guši spontanost i sloboda svakog čovjeka koji ulazi u bilo kakvu povjerljivu ili intimnu elektronsku korespondenciju s nekime. Nekritički masovni nadzor komunikacija primjer je sveobuhvatne eksterne ugroze privatnosti koju je teško opravdati.

2.2.4. Podmetanje noge sigurnosti: pokušaji narušavanja i zaobilaženja enkripcije

Osim nekritičkog globalnog nadzora, Snowdenova objava razotkrila je komplementarno djelovanje Odjela za operacije prilagođenog pristupa (eng. *Tailored Access Operations division*). Sintagma *prilagođeni pristup* u nazivu označava uljepšani naziv za računalne upade u osobna računala, mobitele, poslužitelje, mrežnu opremu i sustave te tajno prikupljanje podataka s njih i pomoću njih (Appelbaum, Poitras i dr., 2013). Vjerojatno najpoznatija operacija ovoga tipa jest razvoj zloćudnog softvera *Stuxnet* pomoću kojeg je 2010. godine izvršena sabotaža Iranskog nuklearnog programa (Nakashima i Warrick, 2012). Osim operacija državne sabotaže, upada u poslužitelje e-pošte predsjednika država (Glüsing, Poitras, Rosenbach i Stark, 2013) i sličnih političkih operacija usmjerenih prema visokorangiranim metama, usluge ovog odjela bile su korištene i za brojne druge namjene. Kako bi lakše identificirali osobe od interesa, NSA je infiltriranjem među izlazne čvorove navodno jedno vrijeme uspješno nadzirala korisnike TOR-a, globalne mreže poslužitelja namijenjene anonimnom korištenju interneta (Ball, Schneier i Greenwald, 2013; Gellman, Timberg i Rich, 2013). Nekritički globalni nadzor primarno je problematičan stoga što se njime nadzire osobe koje nisu niti će ikada biti predmetom obrade od strane sigurnosnih službi te se njime prikuplja brojne sigurnosno nerelevantne intimne i osobne podatke čije prikupljanje nije moguće razumno opravdati radi postizanja željenog cilja. Operacije prilagođenog pristupa korištenjem metoda i tehnika za nadzor konkretnih pojedinaca od interesa očigledno uvažava načelo kako

je privatnost moguće ograničiti isključivo prema određenim osobama, dakako, ukoliko za to postoji opravdani razlog prihvaćen od strane nezavisnog suda. No, operacije koje će biti opisane u nastavku predstavljaju izuzetno grubo narušavanje privatnosti, pa i sigurnosti, pojedinaca koji su predmet nadzora čime je ugroženo načelo proporcionalnosti. A najozbiljnija ugroza zapravo proizlazi iz toga što se namjernim slabljenjem enkripcije, slabljenjem sigurnosti informacijskih sustava i ugrađivanjem hardverskih i softverskih ranjivosti zapravo ugrožava sigurnost i privatnost i svih drugih korisnika tih proizvoda budući da ih se čini ranjivima u odnosu na zlonamjerne pojedince ili organizacije poput raznih hakera, kriminalaca, kradljivaca identiteta, stranih špijuna ili suparničkih država.

U tom je smislu posebno zanimljiv katalog opreme napravljene za potrebe Odjela za operacije prilagođenog pristupa. Radi se internom dokumentu NSA-ina Odjela za napredne mrežne tehnologije (eng. *Advanced Network Technology division*), u kojem se na čak pedeset stranica reklamira razna elektronička oprema i softverski alati kojima se iskorištavaju slabosti određenih sustava ili se koriste tajna stražnja vrata (engl. *backdoor*) ugrađena u računalne programe, operacijske sustave ili elektroničke uređaje kako bi se ostvario pristup osobnim računalima, pametnim telefonima, mrežnoj opremi (Appelbaum, Horchert i Stöcker, 2013). NSA i GCHQ dulje vrijeme iskorištavali su slabosti na 13 modela vatrozida vodećeg svjetskog proizvođača mrežne opreme Juniper Networks (Gallagher i Greenwald, 2015), a postoje opravdane sumnje da je NSA sudjelovala i u stvaranju tih slabosti (Zetter, 2015). Uostalom, u internom izvješću NSA iz Snowdenove objave, vrlo eksplicitno se navodi kako NSA rutinski zaprima ili presreće rutere, poslužitelje i ostalu računalnu opremu koja se izvozi iz SAD-a te u nju ugrađuje stražnja vrata koja omogućuju zaobilaženje zaštite i enkripcije te time naknadni nadzor putem tih uređaja (Greenwald, 2014). U potpuno nevjerojatnoj akciji, NSA i GCHQ izveli su 2010. godine hakerski napad na računalni sustav multinacionalne tvrtke Gemalto kako bi ukrali njihove enkripcijske ključeve (Scahill i Begley, 2015a). Ironično, Gemalto je tvrtka koja se bavi razvojem sigurnosnih rješenja i proizvodnjom čipova i tehnologija koje se koriste u mobilnim SIM karticama, u beskontaktnom plaćanju, biometrijskim putovnicama, elektronskim osobnim iskaznicama, kreditnim karticama i slično, a upravo je njima GCHQ ukrao enkripcijske ključeve. Budući da Gemalto svojim SIM karticama opskrbljuje skoro pet stotina telekoma diljem svijeta, posjedovanje Gemaltovih kripto-ključeva omogućilo je NSA-i i GCHQ-u nadzor telefonskih poziva bez ikakve suradnje ili znanja pojedinih mobilnih operatora. Nadziranjem etera bilježena je komunikacija između mobilnih telefona i telekomunikacijskih ćelija mobilnih

operatora, a ta je komunikacija jednostavno dekriptirana uz pomoć pribavljenih kripto-ključeva. Budući da Gemalto proizvodi čak dvije milijarde SIM kartica godišnje, možemo slobodno zaključiti kako enkripcija mobilne telefonije više ne postoji.

Osim ugradnje ranjivosti u računalnu opremu, NSA je iskorištavala niz softverskih ranjivosti i radila je na njihovu ugrađivanju u softverske proizvode. Za razliku od Apple-a, čiji su softver i enkripciju morali zaobići iskorištavanjem ranjivosti, što su i uspjeli (Appelbaum, Horchert i dr., 2013; Scahill i Begley, 2015b), Microsoft je NSA-i omogućio pristup korisničkom sadržaju na svojim uslugama Skype, Outlook.com i Skydrive (Greenwald, 2014). Kako bi mogli izraditi uspješniji zloćudni softver koji bi imao veću šansu zaraziti željena računala, NSA i GCHQ napali su čak i komercijalni antivirusni program Kaspersky (Fishman i Greenwald, 2015; Fishman i Marquis-Boire, 2015). Program TURBINE razvio je Odjel za operacije prilagođenog pristupa kako bi se automatiziralo prikupljanje podataka o što većem broju korisnika pomoću ugradnje milijuna takozvanih implantata, zlonamjernih računalnih softvera kojima se zaobilazi računalna zaštita i enkripcija (Gallagher i Greenwald, 2014).

Od kada je devedesetih godina prošloga stoljeća počela ozbiljnija i sve šira primjena enkripcije u računalnim sustavima i na internetu, sigurnosni sustavi diljem svijeta usmjerili su se na pokušaje razbijanja te enkripcije. I to nije ništa novo, niti išta čudno. Naprotiv, od sigurnosnog sustava se i očekuje da poduzme mjere kako bi prikupile informacije o počiniteljima raznih kaznenih djela, ali i kako bi spriječio njihovo počinjenje ili dovođenje u opasnost nacionalne sigurnosti. Od sigurnosnog se sustava očekuje da uz odgovarajući nalog ima pravo i mogućnost fizičkog pristupa privatnim prostorima pa i zaključanim sefovima. Stoga ne treba čuditi što su tu svoju ovlast, i dužnost, željeli prenijeti i na računalnu enkripciju. Međutim, razvijanje sposobnosti za fizički pristup određenim mjestima sasvim je drugačije od razvijanja sposobnosti za pristup virtualnim mjestima. Naime, mogućnost fizičkog pristupa pretpostavlja da sigurnosni sustav određene države ima, uz opravdani nalog, mogućnost ući u bilo koju prostoriju na svojem teritoriju i provaliti u bilo koji sef. S obzirom na današnju tehnologiju, teško je zamisliti prostor ili sef u koji se ne može pristupiti u razumnom vremenu. Međutim, enkripcija funkcionira sasvim drugačije. Matematičke operacije, koje bez većih problema može odraditi čak i procesor u pametnom telefonu niže klase, mogu osigurati dovoljno snažnu enkripciju da bi čak i NSA-inim superračunalima uz današnju tehnologiju trebali milijuni godina da je razbiju. Tako raširena i tako učinkovita enkripcija bila je trn u oku sigurnosnim službama diljem svijeta.

Vrlo je malo država koje imaju resurse, financijske i kadrovske, kojima bi uopće mogli razmišljati o zaobilaženju ili razbijanju računalne enkripcije. No, SAD je svakako primjer jedne od tih država i ondje su od same pojave enkripcije postojala nastojanja da se u nju ugrade stražnja vrata koja bi pod određenim uvjetima i u određenim slučajevima mogle koristiti službe sigurnosnog sustava. Budući da je javnost u više navrata odbacila takvu mogućnost, sustav je smatrao svojom dužnosti zaobići enkripciju. Kao što je već navedeno, to su činili ugradnjom hardverskih stražnjih vrata u mrežnu opremu, hakiranjem korisničkih uređaja pomoću zlonamjernih programa, krađom enkripcijskih ključeva, pristupanjem podacima na poslužiteljima i podatkovnim centrima brojnih tvrtki prije nego što se podatke kriptiralo, suradnjom s tvrtkama koje su dobrovoljno prepuštale korisničke podatke prije njihova kriptiranja i tako dalje. No, u mnogim slučajevima to jednostavno nije bilo dovoljno. Pojedini su korisnici koristili vrlo snažnu enkripciju i sve je više tvrtki krenulo štititi vlastite podatke i podatke o svojim korisnicima učinkovitom enkripcijom te su korisnicima ponudili usluge uz *end-to-end* enkripciju kojom se osigurava snažna kriptografska zaštita sadržaja, a privatni ključevi nisu dostupni nikome osim korisnicima, odnosno uređajima koje koriste. Stoga je NSA koristila superračunala kako bi pomoću puke snage pokušala razbiti enkripciju, a paralelno s time namjerno su radili na oslabljivanju enkripcijskih standarda (Ball, Borger i Greenwald, 2013). Dokumenti iz Snowdenove objave potvrdili su sumnju kriptografa kako je NSA doista ugradila slabost u enkripcijski standard koji je prihvatila Međunarodna organizacija za standarde, a time i 153 države članice te organizacije. Sve su pobrojane aktivnosti narušavanja i zaobilaženja računalne enkripcije dio dugotrajnog programa BULLRUN, za čiji je razvoj NSA do sada izdvojila gotovo milijardu dolara. Tim programom željelo se zapravo *dešifrirati komunikaciju*, a to uključuje protokole kao što su SSL, HTTPS, 4G, VOIP koje koriste milijarde ljudi diljem svijeta za međusobnu komunikaciju, ali i za plaćanje računa, prijenos novca, korištenje kreditnih kartica ili identifikaciju (Perlroth, Larson i Shane, 2013).

Unatoč tome što sam Snowden nije imao pristup svim detaljima projekta BULLRUN, prema dokumentima iz njegove objave, kao i na temelju njegovih brojnih izjava, nedvojbeno je da ispravno postavljena i korištena snažna enkripcija i dalje predstavlja učinkovitu zaštitu od neželjenog nadzora komunikacija (Appelbaum i dr., 2014). Uostalom, na to upućuje i sama žustrina kojom NSA i GCHQ pokušavaju zaobići enkripciju alternativnim načinima. No, to što enkripcija za sada uspješno drži komunikaciju privatnom ne znači da NSA i ostale službe neće prestati pokušavati razbiti enkripciju ili je zaobići te da već sada ne postoje drugi učinkoviti

načini na koje se i dalje ta enkripcija može zaobići poput ugradnje zlonamjernog softvera ili iskorištavanja slabosti s bilo koje strane komunikacijskog kanala, uključujući i ljudske slabosti. Nedavno je u Velikoj Britaniji donesen (MacAskill, 2016), a u Australiji je upravo u postupku donošenja ("New law would force Facebook and Google to give police access to encrypted messages," 2017), zakon kojim bi se moglo prisiliti tvrtke poput WhatsAppa, Facebooka i Googlea da uz odgovarajući nalog predaju vlastima sadržaj komunikacije korisnika. Budući da *end-to-end* enkripcija funkcionira na način da to nije moguće, kako bi udovoljile zahtjevu za dostavom komunikacije pojedinih svojih korisnika, tvrtke bi morale najprije u potpunosti odustati od korištenja *end-to-end* enkripcije, što bi komunikaciju između *svih* njihovih korisnika učinilo manje sigurnom. Istovremeno, kriminalci i zlonamjernici uvijek bi mogli početi koristiti neku drugu aplikaciju s *end-to-end* enkripcijom u vlasništvu tvrtke nad kojom te države nemaju nadležnost ili jednostavno koristiti enkripciju koju su sami postavili u vlastitoj garaži i čak i takva bi bila neprobojna za današnju razinu tehnologije (Evershed, 2017; Hern, 2017). Ovim zakonima u Velikoj Britaniji i Austrliji dobrim su dijelom legalizirana ranije opisana postupanja u nastojanjima razbijanja i zaobilaženja enkripcije.

Osim obavještajnih službi za obradu signala, postoje podaci koji ukazuju na izuzetno sofisticirane metode nadzora drugih obavještajnih službi poput CIA-e. U ožujku 2017. godine Wikileaks je objavom 8000 dokumenata[9] o hakerskim alatima koje je CIA koristila u razdoblju od 2013. do 2016. godine, započeo niz objava koje su nazvali Vault 7 ("Wikileaks," 2017). Prema tim dokumentima CIA je pomoću specijaliziranih hakerskih alata i zlućudnog softvera te uz korištenje različitih ranjivosti napadala računala, pametne telefone i razne poslužitelje radi prikupljanja podataka o korisnicima (MacAskill, Thielman i Oltermann, 2017). U trenutku objave dokumenata, posebno je odjeknula spoznaja o programu nazvanom WEEPING ANGEL koji je opisivao način na koji je CIA, uz prethodno osiguran fizički pristup određenim modelima Samsungovih televizora koji imaju ugrađene kamere, mogla daljinski promatrati osobe od interesa čak i dok su uređaji bili ugašeni. Prema dokumentima, razmatrane su i mogućnosti hakiranja modernih automobila koji posjeduju sofisticirana računala (Hern, 2017). S očekivanom pojavom samovozećih i autonomnih vozila, ideja o hakiranju vozila otvara potpuno novu dimenziju ugrožavanja sigurnosti korisnika. Ugrađivanje ranjivosti u sustave

[9] Vrijedi napomenuti kako je Wikileaks ovim činom, ali i svojim ranijim objavama, na posebno značajan način narušio privatnost brojnih konkretnih osoba, diplomata, dužnosnika, djelatnika u vojsci i u sigurnosnom sustavu čime je nanesena nemjerljiva osobna šteta osobama čija je korespondencija javno objavljena, od kojih su mnoge malo do nimalo odgovorne za eventualne zlouporabe koje se željelo razotkriti. Osim toga, određene objave su dovele u opasnost pojedince na terenu, agente obavještajnih službi i legitimne sigurnosne operacije.

upravljanja samovozećih i autonomnih vozila, ili prešućivanje spoznaje o postojanju takvih ranjivosti, ne izlaže ugrozi samo korisničke podatke i podatke o njima već i njihovu neposrednu tjelesnu sigurnost. Međutim, s obzirom na visoki financijski i operativni trošak, ovakav tip nadzora nije primjenjivan nekritički i masovno. Doduše, ako je ikada postojala sumnja u to da su svi uređaji umreženi u Internet stvari (eng. *Internet of Things – IoT*), od perilice i hladnjaka preko televizora do automobila bili imuni na nadzor i praćenje, ta je sumnja nedvojbeno nestala s ovom objavom dokumenata.

2.2.5. Izravna i potencijalna ugroza

Metode, tehnike i tehnologije za nadzor koje koriste moćne suvremene obavještajne službe imaju izuzetan doseg kako u širinu, tako i u dubinu. Podaci koji govore o milijardama poruka e-pošte koje se bilježe svakoga sata, o snimanju cjelokupnog interkontinentalnog internetskog prometa i praćenju svega što se nalazi u eteru doista ostavljaju dojam kako malo što može izmaći njihovu nadzoru. S druge strane, posebno skrojeni nadzor kojim se može zaraziti nečije računalo ili mobilni telefon kako bi se zaobišla enkripcija i zaštita ili kojim se koriste kamere i mikrofoni ugrađeni u televizore i automobile kako bi se nadziralo osobu od interesa pokazuju kolike su mogućnosti intruzije u život jednoga pojedinca koji predstavlja interes sustava. Kada se govori o eksternim ugrozama, a to posebno vrijedi za primjere odabrane za ilustriranje državne nadzora, moguće je razlikovati *izravnu ugrozu* privatnosti kao djelovanje kojim se direktno narušava nečija privatnost i *potencijalnu ugrozu* kojom se nekoga čini podložnijim narušavanju, gubitku ili vlastitu odricanju privatnosti. Međutim, iz perspektive definicije privatnosti kao kontrole nad pristupom (podacima o) sebi, u oba se slučaja zapravo radi o gubitku privatnosti. Naime, u oba se slučaja radi o gubitku kontrole nad podacima o sebi. I to neovisno o tome koje posljedice proizlaze iz tog gubitka. Da bi nečija privatnost bila ugrožena nije nužno da je osoba svjesna te ugroze niti da zbog nje ima negativne posljedice. Sama činjenica da je došlo do gubitka kontrole nad podacima o sebi predstavlja gubitak privatnosti. Dakako, pritom postoji cijeli raspon ugroza privatnosti koji seže od sasvim benignih i zanemarivih do onih koje mogu ugroziti nečije blagostanje, zdravlje pa i život.

Izravna ugroza privatnosti zapravo je samorazumljiva. Radi se o onom obliku ugrožavanja privatnosti na koji većina ljudi prvo pomisli kada čuje za ugrožavanje privatnosti. Izravna ugroza privatnosti je slušanje naših povjerljivih telefonskih razgovora, tajno snimanje našeg druženja s prijateljima ili partnerima. Izravnu ugrozu privatnosti svoje kćeri tinejdžerice čini

zabrinuta majka koja joj čita dnevnik, ili u današnje vrijeme možda prikladnije, pregledava sadržaj mobilnog telefona ili profila na društvenim mrežama. S druge strane, potencijalna ugroza nešto je kompleksnija. Definicija privatnosti uključuje najprije kontrolu i samim gubitkom kontrole dolazi do ugroze privatnosti. No, osim gubitka kontrole, važan je i pristup podacima. Kada govorimo o izravnoj ugrozi, uz gubitak kontrole radi se i o neposrednom pristupu nečijim podacima ili podacima o nekome. Međutim, kod potencijalne ugroze privatnosti radi se tek o gubitku kontrole nad pristupom pri čemu (još) nije došlo do pristupa tim podacima. Nema dvojbe kako je potencijalna ugroza manja od izravne, ali jednako tako nema ni dvojbe kako se radi o ozbiljnom obliku ugroze.

Jednom prikupljeni podaci o nama mogu biti pohranjeni ograničeno vrijeme i nakon toga uništeni, mogu biti anonimizirani i agregirani pa tek tada analizirani, a mogu biti i korišteni za stvaranje našeg osobnog psihološkog profila i traženje naših slabosti. Jednako tako, rezultati takvih analiza i profiliranja mogu biti čuvani u najstrožoj tajnosti sukladno visokim etičkim i profesionalnim standardima, a mogu biti i zloupotrijebljeni na razne načine. Osim za zadaće koje su joj povjerene i koje od nje očekujemo, država bi mogla koristiti sigurnosni sustav za kontrolu disidenata i neistomišljenika, političari na vlasti mogli bi kapacitete nadzora i kontrole usmjeriti prema konkurentima, oporbi ili novinarima. Ili bi podaci i analize mogli biti ukradeni od strane neprijateljske države, zlonamjerne ili kriminalne organizacije ili pojedinca. No, unatoč velikim razlikama u ishodu, u svakom slučaju radi se o gubitku kontrole nad pristupom (podacima o) sebi, a time o ugrozi privatnosti.

U slučaju fizičke zaštite prostora, vrlo je lako pristupiti u neki prostor ili otvoriti neki sef, no takva operacija iziskuje vrlo dobro utemeljene i odobrene naloge, mnogo ljudstva, svjedoka, skupa je i u slučaju greške podliježe odgovornosti. Gotovo svaka sigurnosna služba ili policija u svijetu danas ima sposobnost ulaska u gotovo svaki prostor u svojoj nadležnost, pa ipak takve se ovlasti ne koriste masovno. S druge strane, Internet funkcionira drugačije od fizičkoga svijeta. Ako se jednom probije enkripcija, sigurnosne službe ili hakeri s drugog kraja svijeta mogli bi istovremeno nadzirati stotine milijuna računala ili telefona i pristupati podacima koji su na njima zapisani. O važnosti enkripcije, i njezina razbijanja, najviše govori citat iz jednog izvornog dokumenta iz Snowdenove objave u kojem stoji kako će „u budućnosti supersile biti stvarane ili slomljene temeljem snage njihovih kriptoanalitičkih programa“ (Perlroth i dr., 2013: 1). Potkopavanje enkripcijskih standarda i ugradnja slabosti u enkripcijske protokole ima i drugu stranu medalje. Dok s jedne strane moćnim službama omogućuje pristup podacima o

određenim osobama koje nadziru, narušava se sigurnost stotina milijuna drugih sasvim nevinih korisnika. Ugradnja slabosti u operacijske sustave, antivirusne programe i ostali softver, pa čak i samo prešućivanje slabosti koje se otkrije, dovodi do povećane ranjivosti svih korisnika. A to ih izlaže prema neprijateljskim obavještajnim službama, hakerima, zlonamjernim korisnicima pa i teroristima. I upravo je u tome sadržana opasnost koja proizlazi iz potencijalne ugroze.

Radi mogućnosti praćenja terorista, osoba koje stvarno ili potencijalno ugrožavaju nacionalnu sigurnost, ali i savezničkih državnika i diplomata (Appelbaum, Blome i dr., 2013; Ball, 2013; Greenwald i Maurizi, 2013; MacAskill i Borger, 2013; Poitras, Rosenbach, Schmid i Stark, 2013; Poitras, Rosenbach i Stark, 2013), čelnika i samita međunarodnih organizacija poput UN-a (Angwin i dr., 2015; Geist, Gjerding, Moltke i Poitras, 2014; Gjerding, Moltke, Geist i Poitras, 2014), NSA i GCHQ poduzele su mjere kojima su ugrozile sigurnost stotina milijuna ljudi diljem svijeta. Uostalom, ugrozili su i sigurnost vlastitih državljana i građana, upravo onih koje im je zadaća štititi. Nedavni hakerski *ransomware* napad *Wannacry* kojim je zaraženo preko 200 000 računala po cijelome svijetu (BBC, 2017), a zaražen je čak i informatički sustav Ministarstva unutarnjih poslova RH (Dešković, 2017), izveden je upravo korištenjem alata koje je za svoje potrebe nadzora razvila NSA, zbog čega ih je Microsoft javno prozvao (Titcomb, 2017), a Snowden je likovao zbog svojih opetovanih upozorenja kako je bilo samo pitanje vremena kada će razbijanje enkripcije doći na naplatu (Blake, 2017). Primjer hakerskog napada zloćudnim softverom Wannacry prikazuje realiziranu ugrozu koja je proizašla iz nekoliko potencijalnih ugroza opisanih u ovom poglavlju. Za razliku od tog, većina potencijalnih ugroza nije realizirana, a mnoge nikada ni neće biti realizirane. No, to ne znači da njima nije narušena privatnost, a time i dostojanstvo i autonomija ljudi koji su predmet takvih potencijalnih ugroza privatnosti.

2.2.6. Naši i vaši: različito postupanje država prema vlastitim građanima u odnosu na strance

Bez obzira na to što NSA zbog financijskih, kadrovskih, znanstvenih, geografskih pa i političkih razloga ima veliku prednost u odnosu na obavještajne službe za nadzor signala ostalih država u svijetu, ne treba je smatrati izoliranim primjerom. Istina je da SAD, za razliku od gotovo svih drugih država, imaju vanjsku i sigurnosnu politiku definiranu na način da im je cijeli svijet susjedstvo pa time i njihove obavještajne službe imaju nezahvalan zadatak globalnog nadzora. No, postoje brojni primjeri obavještajnih službi koje provode regionalni i nacionalni nadzor znatno gori od onog koji provodi NSA. U tom su smislu kritike određenih svjetskih lidera prema

načinu postupanja NSA bile vrlo licemjerne budući da su njihove obavještajne službe ili koristile podatke NSA-e (Gunnar Rensfeldt, 2013; Spiegel, 2013), dostavljale podatke NSA-i (Biermann i Musharbash, 2015) ili na svojem području od interesa provodile vrlo slične operacije. Pritom je vjerojatno najdalje otišla Kina koja je sustav masovnog nadzora pomoću kamera s automatiziranim prepoznavanjem lica dovela do izuzetnih razmjera te ga obilato koristi, a osim ulica i trgova, ondje, kao u nekom filmu znanstvene fantastike, i policijski službenici nose naočale s kamerama koje atomatski prepoznaju tražene osobe i o tome ih u realnom vremenu upozoravaju (Mozur, 2018).

Povrh toga, službe iz savezništva Five Eyes koristile su različite smicalice kojima su doskočile nacionalnim zakonskim ograničenjima za prikupljanje podataka o vlastitim državljanima. Na primjer, kako bi zaobišla ograničenja za nadzor vlastitih državljana, australska služba ASD putem programa XKEYSCORE-a koristila je vrlo široke podatke o australskim državljanima koje je na području Australije NSA rutinski i sasvim legalno prikupljala (O'Neill i Andersen, 2015). Na sličan je način NSA podatke o američkim državljanima prikupljala putem svojih podatkovnih centara koji su namjerno bili locirani izvan teritorija SAD-a, što je dijelom i razlog za izvrsnu suradnju na programu TEMPORA.

Većina država u smislu zaštite ljudskih prava tretira vlastite državljane drugačije nego strance, a osobito drugačije nego strance koji se ni ne nalaze na njihovom teritoriju. To je posebno izraženo u zakonodavstvu, a time i načinu djelovanja, obavještajnih službi. Uostalom, obavještajne službe su, za razliku od protuobavještajnih službi, dio sigurnosnog sustava usmjerene upravo na prikupljanje podataka izvan države i o osobama od interesa koje se nalaze izvan države. Bez ulaženja u opis kompleksnog sigurnosnog sustava SAD-a, NSA je obavještajna služba, usmjerena na prikupljanje podataka o osobama i procesima izvan SAD-a te u njenom djelovanju postoje značajna ograničenja za prikupljanje podataka o američkim državljanima u odnosu na sve druge osobe. Unatoč tome što su zabilježeni sporadični manji prosvjedi u nekim europskim državama (RT, 2013) i tome što su određeni svjetski lideri, mahom upravo oni osobno zahvaćeni postupanjem NSA, izrazili oštar protest pa i zaprijetili ekonomskim posljedicama za američke tvrtke (Romero i Archibold, 2013; Winter, 2013), pritisak na SAD za prestankom masovnog nadzora komunikacija bio je razmjerno slab. To je potvrđeno i u Izvješću Europskog parlamenta o programu nadzora NSA, gdje stoji kako je rasprava o masovnom nadzoru unutar EU bila vrlo raznolika te kako zapravo „u većini država članica gotovo uopće nije bilo javne rasprave, dok je medijska pažnja varirala" pri čemu je

Njemačka izdvojena kao iznimka (Moraes, 2014: 45). Unatoč relativno slaboj reakciji javnosti, Izvješće je prihvaćeno na plenarnoj sjednici i Europski parlament pokrenuo je aktivnosti s ciljem donošenja novog pravnog okvira zaštite korisničkih podataka i privatnosti, a paralelno su slične aktivnosti, koje će detaljno biti opisane u sljedećem poglavlju, pokrenuli i Ujedinjeni narodi. Nadalje, kao što će biti prikazano u drugom dijelu poglavlja, nakon Snowdenove objave iz straha za gubitkom korisnika i profita, brojne informatičke tvrtke doista su značajno pojačale sigurnost svojih sustava, uvele su snažnu enkripciju i značajno su unaprijedile transparentnost i sigurnost upravljanja podacima svojih korisnika, a pojavile su se i nove tvrtke koje su nudile usluge snažne enkripcije bez prikupljanja korisničkih podataka. Međutim, izostala je glasna i uvjerljiva kritika od strane samih korisnika. Broj korisnika Facebooka i Googlea nije pao već je nastavio strelovit rast (Constine, 2017). S druge strane, u SAD-u je Snowdenova objava izazvala vrlo ozbiljan potres i reakciju javnosti (Kelly, 2013; Newell, 2013). U SAD-u je većina kontroverzi proizašlih iz Snowdenovih objava bila posljedica opravdanih sumnji da je NSA prikupljala vrlo široke i detaljne podatke o američkim državljanima, a ne da je masovnim nadzorom pratila strance.

Posebno je ironično što je na Snowdenove objave snažnije reagirala američka javnost i mediji nego javnost i mediji u ostatku svijeta budući da su upravo svi ostali stanovnici Zemlje, a ne američki državljani potencijalni predmet interesa američkih obavještajnih službi. Uostalom, i hrvatsko zakonodavstvo regulira drugačiji način postupanja prema stranim državljanima u odnosu na hrvatske državljane, a to se osobito odnosi na telekomunikacije koje samo prolaze kroz Hrvatsku (NN, 2006). Međutim, za razliku od Hrvatske preko čijeg teritorija prolazi zanemariv dio svjetskoga telekomunikacijskoga prometa, u SAD-u se nalaze gotovo sve najveće informacijske tvrtke i podaci njihovih korisnika iz cijeloga svijeta dolaze na njihove poslužitelje, gdje ih američke obavještajne službe lako i legalno prikupljaju. Za većinu ljudi na svijetu sasvim je sporedno upravo ono pitanje koje je u SAD-u ključno, a to je pitanje legalnosti primjene ovih programa te osobito njihova primjena za prikupljanje podataka *o američkim državljanima*. Prema većini ljudi na svijetu NSA će moći na jednak način nastaviti postupati nakon navodnih *korjenitih promjena*, kao što su postupali i prije Snowdenovih objava. Upravo je zbog toga pitanje legalnosti određenih NSA-inih programa u okviru zakonodavstva SAD-a u ovom radu ostavljeno sa strane. Zakonitost tih programa ionako je propitkivana samo u onom dijelu u kojem su se prikupljali podaci o američkim državljanima. A dovođenje u pitanje moralnosti globalnog nekritičnog nadzora koji demonstriraju NSA i GCHQ te sukladnosti

takvog postupanja s međunarodnim pravom pa i temeljnim postavkama liberalne demokracije, upravo su jedni od glavnih ciljeva ovog rada.

2.2.7. ~~Disciplinatorno~~ društvo nadzora: je li cilj nadzora izazivanje discipline?

Kao da iz njihovog načina djelovanja nije očito, u izvornim NSA-inim i GCHQ-evim prezentacijama na više mjesta eksplicitno je istaknuta namjera za prikupljanjem *svega*, i *saznavanjem svega*, što je ujedno bio i osobni moto bivšeg ravnatelja NSA Keitha Alexandera (Greenwald, 2013a). Sličnost s Benthamovim panoptikonom ne treba posebno isticati. Namjera za mogućnosti uvida u svaki kutak svijeta, želja da se prikupi sve, čuje sve i sazna sve, prožeta je kroz sve nabrojane primjere NSA-ina postupanja. No, da bi usporedba s Foucaultovom vizijom panoptikona, koju se redovito naglašava u radovima iz područja studija nadzora, nužno je pokazati kako je namjera, osim saznavanja, bila i proizvođenja discipline. Naime, upravo je uspostava discipline kroz potpunu transparentnost prema promatraču bila temelj panopticizma, koji je u srži Foucaultova disciplinarornog društva. Kao što je ranije pojašnjeno, da bi Foucaultov *sveprisutni nadzor* ili Benthamova *očigledna prisutnost* mogla osigurati automatsko djelovanje moći, bilo je potrebno osigurati da su ljudi svjesni kako u bilo kojem trenutku mogu biti promatrani. Međutim, iz tajnovitosti obavještajnih službi o svojim mogućnostima nadzora, iz njihova opiranja da transparentno objasne dosege i mogućnosti svojih aktivnosti te iz njihovih reakcija na propitkivanja javnosti, medija, sudova i političara nakon Snowdenovih objava, evidentno je kako namjera obavještajnog aparata nije bila izazvati automatsko djelovanje moći.

Ne postoji velika zavjera. Nije *netko* promišljeno upogonio sustave masovnog nadzora kako bi kod građana izazvao osjećaj stalne izloženosti, a time i discipline, a i pitanje je bi li to u zadanim okolnostima uopće bilo moguće orkestrirati. Uostalom, očito je kako obavještajne službe skrivaju podatke o tome koliko su zapravo podataka sposobni prikupljati o nama. Međutim, unatoč tome što proizvođenje discipline nije bio primarni cilj (masovnog) nadzora komunikacija, učinci tog nadzora nedvojbeno odgovaraju polugama moći, ali i doprinose sigurnosti. Autocenzura, internaliziranje društvenih normi i samodisciplina nedvojbeno su u skladu s politikom koja se nalazi iza namjere da se *sve prikupi* i da se *sve zna*. Danas, nakon Snowdenovih objava, nakon objava Wikileaksa, nakon brojnih parlamentarnih saslušanja u SAD-u i Europi, nakon brojnih novinskih članaka, knjiga, filmova i emisija o razmjerima i mogućnostima nadzora suvremenih obavještajnih službi malo tko može misliti kako ne može biti predmetom nadzora. Foucaltov citat kojim opisuje temelj učinkovitosti panoptikona kroz

automatsko djelovanje moći „zatvorenik ne smije niti u jednom trenutku znati promatra li se, ali mora biti uvjeren da ga se u svakom trenutku može promatrati“ (Foucault, 1995; 201) dobiva potpuno novo, disciplinatorno, značenje nakon spoznaja o tome kako nas se u svakom trenutku može pratiti, gledati i slušati putem naših mobilnih telefona, računala, televizora i automobila, od kojih se ne odvajamo ni dok spavamo.

2.3. Društvo izlaganja

Ugroze privatnosti koje su obuhvaćene pod sintagmom države nadzora temelje se prvenstveno na eksternim ugrozama privatnosti, onima koje dolaze izvana i koje se odvijaju izvan naše kontrole i/ili bez našega znanja. Unatoč tome što dijelom i sami svojim ponašanjem doprinosimo vlastitoj ranjivosti u odnosu na ranije opisane metode nadzora koje koriste moderne moćne obavještajne službe, ugroze koje proizlaze iz njihova djelovanja prvenstveno su eksterne ugroze privatnosti. Međutim, neovisno o željama, namjerama i aktivnostima moćnih obavještajnih službi, većina nas svojim se ponašanjem svojevoljno odriče vlastite privatnosti. Rasprostranjenost, lagodnost i korisnost digitalnih tehnologija i mrežnih usluga zavela je mnoge od nas do te mjere da smo se ne samo odrekli svoje privatnosti nego se i međusobno natječemo u tome tko će je se više odreći. I čini se da u tome ne vidimo ništa loše, štetno ni opasno. Dok se među nama još i može pronaći nekoliko onih koji se teškom mukom opiru zovu društvenih mreža, ili su blagoslovljeni time da njihova socijalna okolina i/ili zahtjevi radnog mjesta to od njih ne zahtijevaju, većina nas ipak posjeduje pametne telefone, koristi besplatne usluge Googlea, Microsofta, Applea, kupuje preko interneta, Amazona, ebaya, pretplaćena je na Netflix, HBO, PickBox, koristi bilo koju od mora besplatnih i korisnih aplikacija kao što su dropbox, evernote, waze ili jednostavno koristi programe vjernosti trgovaca. Ne samo da koristimo te usluge, nego dobrovoljno dajemo enormne količine podataka o sebi, nerijetko čak i unatoč tome što to od nas nitko nije tražio. Objavljivanjem fotografija na Instagramu upravljamo dojmom o sebi, a slično radimo i konstantnim *tvitanjem* ili objavljivanjem statusa i fotografija na Facebooku, ili jednostavno *klikanjem* na malenu plavu ručicu s palcem prema gore po bespućima interneta svojim prijateljima, neprijateljima, Facebooku i NSA-i dajemo do znanja što volimo i što ne volimo. Potpuno svojevoljno i unatoč tome što to od nas nitko nije tražio. Dobrodošli u *društvo izlaganja*. Harvardski profesor Bernard E. Harcourt tim je terminom želio opisati „novo političko i društveno stanje koje radikalno transformira međuljudske odnose, našu političku zajednicu i nas same; novu virtualnu

transparentnost koja dramatično preoblikuje odnose moći u cijelom društvu, koja iznova dizajnira naš društveni krajolik, koja stvara dramatično novi protok moći u društvu“ (Harcourt, 2015: 15).

U digitalnom svijetu sve se pohranjuje. Dok se podatke pohranjene na lokalnim tvrdim diskovima još uvijek može relativno učinkovito obrisati, odnosno učiniti ih se nedostupnima za čitanje, nakon što se povežemo s internetom i prenesemo određeni sadržaj na poslužitelje diljem planeta, naši podaci mogli bi ostati dostupni praktički zauvijek. Pametni telefon prosječnog korisnika posjeduje toliku količinu podataka o toj osobi da bi se neki internetski korisnici hipotetski bili spremniji podvrgnuti čitanju vlastitih misli nego predati podatke sa svojeg pametnog telefona (Grey, 2016). Naš je mozak doista zadivljujući organ, ali naše pamćenje i mišljenje jednostavno su fiziološki ograničeni. Rijetko tko od nas može za svaki trenutak svakog dana svibnja prošle godine reći gdje se i kada nalazio, kojim je prijevoznim sredstvom ondje došao, s kime je razgovarao, koliko dugo se i s kime dopisivao i o čemu, pregledati fotografije iz toga dana, znati o čemu je razmišljao, što ga je brinulo ili mučilo, na koga je bio ljut, ogorčen ili zbog čega je bio ushićen. Prosječni korisnik pametnog telefona, koji je koristio aplikacije koje koristi većina korisnika, uz postavke koje koristi većina korisnika i uz prosječnu razinu korištenja može biti siguran da bi se iz njegova ili njezina pametnog telefona ti podaci mogli izvući. Takozvani *digitalni pretresi* danas su standardna procedura prilikom ulaska u brojne države poput SAD-a (Waddell, 2017) i Novog Zelanda (1News, 2017). Službenici za nadzor granice mogu vas bez objašnjenja ili naloga zatražiti da im predate svoj elektronski uređaj, prijenosno računalo ili pametni telefon te da im predate lozinku za njegovo otključavanje, odnosno da ga otključate i učinite dostupnim za pregledavanje i preuzimanje sadržaja. Odbijete li učiniti bilo što od navedenoga, možete platiti visoke novčane kazne, biti zadržani satima na ispitivanju, a gotovo sigurno će vam biti zabranjen ulazak u tu državu kao što će i svaki sljedeći prelazak granice za vas značiti brojne neugodnosti (Solon, 2017). Naši pametni telefoni nalaze se unutar jednoga metra od nas gotovo punih 24 sata dnevno, istovremeno bilježeći naše misli, raspoloženje i ponašanje, a slično rade i naša računala, stotine nadzornih kamera pored kojih prođemo svakoga dana kao i ostali uređaji na kojima ostavljamo svoj elektronski trag. Kao da to samo po sebi nije dovoljno razotkrivanja, mnogi od nas još znatno više sadržaja sami dobrovoljno dijele s drugima putem javnih objava na društvenim mrežama, komentara na internetskim portalima.

Kao što je u prošlom poglavlju pojašnjeno, iz definicije privatnosti kao kontrole pristupa (podacima o) sebi, proizlazi kako su ugroze privatnosti one aktivnosti kojima ostajemo bez kontrole. Međutim, ostati bez kontrole možemo tako da nam netko kontrolu oduzme ili tako da je dobrovoljno predamo. I to je osnovna razlika između eksternih i internih ugroza. Dok eksterne ugroze najčešće predstavljaju izravnu ugrozu privatnosti, u slučaju internih ugroza, odnosno u slučaju dobrovoljnog odricanja od kontrole nad pristupom podacima o nama, najčešće se radi o potencijalnoj ugrozi privatnosti. No to ih ne čini manje značajnim ni manje opasnim. Potencijalne ugroze vrlo lako mogu postati izravne ugroze privatnosti s dalekosežnim posljedicama za pojedinca, ali i za društvo. Uostalom, sama činjenica da tako olako predajemo kontrolu nad našim podacima mijenja način na koji gledamo na svijet i način na koji se ponašamo čime već i sama potencijalna ugroza privatnosti ima psihosocijalni utjecaj na pojedinca te utječe na društvene tokove.

2.3.1. Procesi u pozadini društva izlaganja

Najveća društvena mreža Facebook, koja odnedavno ima više od dvije milijarde aktivnih korisnika unutar jednoga mjeseca (Constine, 2017) počeo je s radom u sobi studentskoga doma ne tako davne 2004. godine (Phillips, 2007), a iste je godine s radom započeo Googleov servis e-pošte Gmail (McCracken, 2014). Prvi iPhone na samo sebi svojstven način predstavio je Steve Jobs 2007. godine (Cohen, 2007), a godinu dana kasnije izdan je T-mobileov HTC G1, prvi pametni telefon baziran na Googleovom operacijskom sustavu Android (Aamoth, 2008). To se sve dogodilo prilično nedavno, a za većinu tih uređaja i usluga imamo dojam kao da su oduvijek s nama. Budući da je platforma koja omogućuje i stvara društvo izlaganja praktički sasvim nova, vrlo je malo istraživanja koja objašnjavaju procese u pozadini takvog masovnog razgolićavanja, ali fenomen je toliko intrigantan da unatoč tome postoje uvjerljivi pokušaji i pojedini značajni doprinosi boljem razumijevanju.

Harcourt kao jedan od ključnih elemenata za omogućavanje digitalnog izlaganja ističe ljudsku želju, želju za užitkom (Harcourt, 2015). Pišući o Orwellovoj 1984., o svim analogijama koje taj roman ima s današnjim globalnim nadzorom, s mogućnosti da nas naši televizori gledaju i slušaju upravo poput *teleekrana*, Harcourt Orwellov odnos prema ljudskoj želji smatra najvećom pogreškom u njegovu predviđanju, ili fikciji, te ga izdvaja kao ključnu razliku u odnosu na današnjicu. „Kao da je netko naučio iz Orwellove najveće pogreške: mnogo je lakše ukrotiti ljude putem njihovih strasti – čak i strasti za najjednostavnijim stvarima, poput pravoga

čaja, prave kave i stvarnog šećera za Winstona i Juliju, ili za nas putem *lattea*, frapea, i besplatnoga Wi-Fija - nego ih pokušati ukrotiti zatiranjem njihove želje i požude, pokušavajući poraziti *Čovjekov Duh*" (Harcourt, 2015: 35). I doista, čini se kako je Harcourt u pravu. Orwell je u svojem romanu izabrao teži put kroćenja ljudi. Svijet koji je on opisao ustrojen je kao država potpunog nadzora i discipline. U tom se fiktivnom svijetu koristi izmišljeni pojednostavljeni jezik kako bi se otežao razgovor o kritikama sustava pa i kako bi već samo mišljenje o subverziji bilo otežano. Cilj Velikog Brata u Orwellovoj fiktivnoj Oceaniji bio je poraziti *Čovjekov Duh* potpunim nadzorom, mijenjanjem povijesti, propagandom i silom. Unatoč tome što je Orwell opisao fiktivnu distopiju, nažalost postoje države koje nastojanjima za cenzurom, općim nadzorom, kontrolom i disciplinom u određenim elementima neodoljivo podsjećaju na Oceaniju, a njihove metode na one koje je koristio Veliki Brat. Međutim, osim nekoliko takvih diktatura, većina država nasreću prigrlila je sasvim drugačiji oblik društvenog uređenja. No, gdje je točno Orwell pogriješio? Jednostavno, društvo koje je opisao nije održivo. Prisilom, nadzorom i indoktrinacijom se ponašanje može modificirati, ali bez obzira na Orwellov pesimistični završetak romana, ideju se ne može ubiti. Barem ne u potpunosti. Stoga se čini razumnim umjesto trošenja beskonačnih resursa na poražavanje njihova *Čovjekova Duha*, na gušenje, represiju i apsolutni nadzor, omogućiti ljudima upravo suprotno – stvoriti platformu za slobodno i opće svojevoljno i samostalno potpuno razotkrivanje te ljude u tome dodatno i ohrabrivati. Umjesto prisilne ugradnje *telekrana* u domove ljudi, samo ih treba pustiti i sami će kupiti Samsungove televizore putem kojih ih se može promatrati u njihovu domu. Umjesto da im se ugrade elektronski čipovi za nadzor ili da ih se obilježi barkodovima, sami će kupiti pametne telefone, uključiti pozicioniranje putem GPS-a, dopustiti pristup senzorima, kameri, mikrofonu, sadržaju, kontaktima i pohrani te se od tih uređaja neće odvajati ni trenutka. Sami će na društvenim mrežama objavljivati gdje su bili i s kime bili, što su radili, što su mislili i kako su se osjećali. Te podatke samo treba pokupiti s pladnja na kojem su servirani. Vrijedi još jednom naglasiti kako to nipošto ne znači da se radi o planiranoj velikoj zavjeri radi kontrole stanovništva, već o dobrodošloj posljedici razvoja tehnologije i načina na koji se korisnici služe suvremenim telekomunikacijskim i elektroničkim tehnologijama i uređajima. Doduše, kada bi netko želio ukrotiti stanovništvo, to bi učinkovitije mogao učiniti stvaranjem platforme za jednostavno razoktrivanje intimnih misli i osjećaja svojih građana, nego sveobuhvatnim nadzorom, represijom i cezurom.

Upravo je to prepoznao Neil Postman u kultnoj knjizi *Zabavljamo se do smrti* (*eng. Amusing Ourselves to Death*) u kojoj problematizira način na koji je sredinom osamdesetih godina u SAD-u raširena pojava šoubiznisa i zabavnih emisija na televiziji negativno utjecala na javni diskurs. Njegovo tumačenje o tome kako je zapravo Huxley znatno bolje od Orwella predvidio distopijsku realnost u kojoj se nalazimo najbolje je sadržano u citatu na samom početku knjige:

> Orwell nas je upozoravao kako ćemo biti nadvladani opresijom nametnutom izvana. No, u Huxleyjevoj viziji, ne postoji potreba za Velikim Bratom koji bi ljudima uskratio njihovu autonomiju, zrelost i povijest. Kako je on to vidio, ljudi će zavoljeti vlastitu opresiju, obožavat će tehnologije koje im uskraćuju sposobnost razmišljanja. Ono čega se Orwell bojao bili su oni koji bi zabranili knjige. Ono čega se Huxley bojao bilo je da neće ni biti razloga za zabranu knjiga, jer ih nitko neće ni željeti čitati. Orwell se bojao onih koji će nam uskraćivati informacije. Huxley se bojao onih koji bi nam davali toliko informacija da bismo bili svedeni na pasivnost i egoizam. Orwell se bojao da će se istina skriti od nas. Huxley se bojao da će se istina utopiti u moru nerelevantnosti. Orwell se bojao da ćemo postati društvo zarobljenika. Huxley se bojao da ćemo postati društvo trivijalnosti, zaokupljeni nekim ekvivalentom taktiloskopa (*eng. feelie*), neobaveznog seksa (*eng. orgy porgy*) i dječjih igara (*eng. centrifugal bumblepuppy*) (Postman, 2005: xix)

Postman je svoje uvide temeljio na opažanju utjecaja televizije na Amerikance. Međutim, tek su se s raširenom pojavom interaktivnog interneta njegova tumačenja pokazala u potpunosti ispravnima. Nikada do sada kao danas nismo bili izloženi tolikoj količini informacija iz različitih izvora čiju nam je vjerodostojnost teško procijeniti. Nikada do sada kao danas nismo imali mogućnost istovremeno pratiti što rade naši poznanici i internetski „prijatelji“, odnosno što oni žele da mislimo da rade. *Društvo izlaganja* kako ga je opisao Harcourt znatno više odgovara Huxleyoj viziji društva u kojem se ljude kontrolira na način da se kontrolirano udovoljava njihovim osnovnim potrebama čime im se daje iluzija slobode. No, za razliku od *Vrlog novog svijeta* u kojem se radilo o smišljenoj politici *radi* kontrole stanovništva, u današnjoj realnosti kontrola stanovništva nije cilj već je ona jednostavno moguća *zbog* načina na koji je konzumeristička kultura razvijenog kapitalizma prigrlila moderne telekomunikacijske tehnologije.

Ljudi su društvene životinje. Od samih početaka naše vrste pa sve do modernih vremena, ljudi su imali posebno izraženu potrebu za bliskim kontaktom i pripadanjem (Aronson, Wilson i Akert, 2005; Harari, 2014; Myers, 2005). U čuvenoj teoriji ljudske motivacije, mađarski psiholog Abraham Maslow (1943) predstavio je hijerarhiju ljudskih potreba te je na treće mjesto po važnosti, odmah nakon primarnih fizioloških potreba poput potrebe za zrakom, vodom, hranom i spavanjem te potrebe za sigurnošću, stavio potrebu za pripadanjem. Pojavom

interneta, a osobito tzv. *weba 2.0*, koji podrazumijeva pojavu interneta kakvog znamo, foruma, blogova, društvenih mreža, mobilnih aplikacija omogućeno je do tada nezamislivo umrežavanje ljudi, i kvalitativno i kvantitativno. Odnosno, omogućeno je globalno umrežavanje ljudi, komunikacija s gotovo bilo kime na planetu, a istovremeno ta komunikacija nije ograničena na šturi tekst već se radi o trenutnoj tekstualnoj, glasovnoj i vizualnoj komunikaciji, o razmjeni sadržaja, fotografija, filmova visoke razlučivosti i dokumenata. Harcourt precizno zaključuje kako „želimo biti voljeni, želimo biti popularni, želimo biti željeni i želimo željeti. Upravo ti instinkti potiču digitalno stanje. Oni čine da mnogi od nas tako slobodno i puni entuzijazma dajemo svoje osobne, pa i vrlo intimne podatke. Jednako tako, oni su nas učinili prozirnima i podložnima nadzoru. Zbog njih se naši podaci mogu tako jednostavno prikupljati i analizirati“ (Harcourt, 2015: 41–42).

Postoji čak i fiziološko objašnjenje tolike predanosti vlastitom razotkrivanju. Neuroznanstvenik i psihobiolog Jaan Panksepp (1998) na temelju opsežnog višegodišnjeg istraživanja neuralne podloge emocija i motivacije zaključio je kako je jedan od četiri temeljna sustava u njihovoj pozadini sustav *traženja*. On je povezan s našim laleteralnim hipotalamusom i za njegovo djelovanje ključnu ulogu ima dopamin, neurotransmiter povezan s ugodom i ponašanjem motiviranim nagrađivanjem. Na temeljima Pankseppova istraživanja neuropsiholog Kent Berridge u svojim je istraživanjima došao do zaključka kako se „psihološki proces motivacije za *traženjem* nagrade temelji na moždanim mehanizmima različitima od onoga kada nam se hedonistički *sviđa* ta ista nagrada te da senzitizacija hiperreaktivnosti dopamina specifično potiče pretjerano *traženje*“ (Berridge i Robinson, 2016: 676). Neurološka pozadina *ugode* znatno je jednostavnija od one u pozadini *traženja* užitka, u čijoj je pozadini velik i kompleksan moždani sustav (Berridge i Kringelbach, 2015). Ove spoznaje sugeriraju da je u pozadini različitih, najčešće ovisničkih, ponašanja sam *proces traženja* neke nagrade, a ne *konzumacija* te nagrade. To je suprotno dosadašnjem vjerovanju, ali spoznaje su utemeljene u godinama eksperimentalnog istraživanja na životinjama i ljudima te bacaju novo svjetlo na objašnjenje različitih digitalnih ovisnosti kao što su ovisnost o internetu, društvenim mrežama ili o računalnim igrama. Sama potraga, a ne dostizanje nekog stvarnog ili virtualnog cilja, postaje svrha određene aktivnosti. Klikanje nas vodi u novo klikanje, objavljivanje statusa u novo objavljivanje statusa i dopaminski začarani krug nas obuzima te nastavljamo klikati, objavljivati i *skrolati*. Dakako, osim *traženja*, dodatnu ulogu u želji za silnim otkrivanjem podataka o sebi konačno ima i sama nagrada koju doživimo svaki puta kada netko označi da

mu se sviđa naša fotografija, naš facebook status ili komentar koji smo objavili na nekoj od društvenih mreža. Naš nas mozak elektrokemijskom reakcijom nagradi i osjetimo se bolje. I, poput pravih ovisnika, želimo još.

2.3.2. Ne budi zao: način djelovanja velikih internetskih tvrtki

„Ako ne plaćate, niste kupac, *vi* ste proizvod“ (blue_beetle, 2010)

Promatrajući najveće tvrtke koje pružaju usluge na internetu, Google i Facebook, naizgled nailazimo na kontradikciju. Kako je moguće da tvrtke koje gotovo sve svoje usluge pružaju korisnicima potpuno besplatno imaju godišnje profite koji se broje u desecima milijardi američkih dolara? Kako je moguće da ljudima potpuno besplatno omogućuju međusobno umrežavanje i komuniciranje, kako je moguće da im pružaju i druge beskrajno skupe usluge poput neograničene pohrane za fotografije u oblaku, mapiranje većeg dijela naseljenoga svijeta i brojne druge aplikacije, programe, usluge i alate? Jednostavno - usluge koje Google i Facebook pružaju korisnicima uopće nisu njihov temeljni proizvod. One su tek alati koji služe za iskopavanje, prikupljanje i procesiranje onoga što Google i Facebook zapravo prodaju - podatke o korisnicima (Levine, 2013a: 1). „Mi smo njihov proizvod. Mi, naše želje, fetiši, sklonosti i preferencije, ono je što Google prodaje oglašivačima. Kada mi koristimo Google kako bismo otkrili stvari na mreži, Google koristi naše upite u tražilici kako bi otkrio stvari o nama“ (Vaidhyanathan, 2011: 3). Takav odnos korisnika interneta koji se oslanjaju na besplatne usluge i tvrtki koje pružaju te usluge Paul Bernal opisuje terminom *simbiotska mreža* (Bernal, 2014). Prema Bernalu, u dinamici weba 1.0 pružatelji sadržaja formirali su web koji su onda korisnici pretraživali. Web 2.0 donio je veliku promjenu u smislu da su i korisnici počeli sukreirati web pisanjem blogova, wikija, sudjelovanjem na društvenim mrežama i slično. Simbiotska mreža predstavlja nadgradnja weba 2.0 u odnosu na web 1.0 na način da istovremeno s tokom sadržaja od pružatelja sadržaja prema korisnicima postoji i drugi tok, tok osobnih podataka od korisnika prema pružateljima sadržaja. Zbog toga pružatelji usluga mogu skrojiti verziju weba za svakog korisnika pa time web više nije jedinstven već razlomljen u webove skrojene za svakog korisnika zasebno (Bernal, 2014). Bernal je vrlo dobro uočio ključne procese koji su nastupili. Međutim, iako je Bernal svjestan malignih aspekata tog simbiotskog odnosa i dijelom ih opisuje u svojoj knjizi, drugi dio ovog poglavlja će pokazati kako bi odnos korisnika i velikih internetskih tvrtki primjerenije bilo nazvati *parazitskim* nego *simbiotskim*. Naime, dok u simbiotskom odnosu oba organizma imaju veću korist od njihove

zajednice nego da egzistiraju zasebno, u parazitskom odnosu jedan organizam iskorištava drugi taman toliko koliko je moguće, a da mu fatalno ne našteti. Daleko od toga da korisnici nemaju koristi od usluga koje im pružatelji usluga omogućuju. Značajna je korist za ekonomiju, razvoj znanosti, ideja, umjetnosti i povećanje sigurnosti. Međutim, kao što će biti prikazano u nastavku, odnos internetskih korisnika i velikih internetskih tvrtki izrazito je neravnopravan i često je nevidljiva cijena koju korisnici plaćaju golema.

S pojavom weba 2.0 pristup oglašavanju promijenio se iz korijena. Kako Solove (2004) opisuje u svojoj knjizi *The Digital Person*, direktni marketing dugo je počivao na pravilu *dva posto*, koje govori o tome kako samo dva posto kontaktiranih osoba pozitivno odgovori na reklamu. Povećanje tog postotka od oglašivača je iziskivalo pristup podacima o psihofizičkim i sociodemografskim karakteristikama ciljanih osoba, njihovim navikama, željama, strahovima, uvjerenjima, mislima, zdravstvenim problemima koje su im naprosto bile izvan dosega. Razvoj računalnih baza podataka, umrežavanje putem interneta i opće razotkrivanje predstavljalo je revoluciju tehnologije marketinškog targetiranja. Harcourt takvu novu marketinšku paradigmu naziva *doppelgänger logikom*, logikom dvojnika (Harcourt, 2015). Svrstavanje ljudi u kategorije, proučavanje njihovih međusobnih odnosa, predviđanje njihova ponašanja, traženje uzročno-posljedičnih veza za njega su marketinški alati koji su nakon pedeset godina u ovom desetljeću zamijenjeni potpuno individualiziranim pristupom, traženjem virtualnog dvojnika svake pojedine osobe. To je moguće stoga što je količina podataka o svakom korisniku toliko velika da valjanost korelacija nadilazi kauzalnost te se, prema Harcourtu, pokušava dizajnirati što realnijeg i što vjernijeg digitalnog dvojnika koji će nas poznavati bolje nego što se poznajemo sami. Film koji nam preporuči algoritam temeljem logike dvojnika zasigurno će nam se više svidjeti nego film koji nam preporuči algoritam temeljem ocjena korisnika koji nam po određenim karakteristikama odgovaraju.

Svaki naš klik na internetu ostaje zabilježen. Osim ako nismo poduzeli napredne tehničke korake u svrhu anonimizacije, za koje je osim znanja i vještina potrebno i značajno odricanje od lagodnosti na koju smo do sada već navikli, a katkada i potpuno odricanje od korištenja određenih usluga i aplikacija ili posjećivanja pojedinih internetskih stranica[10], vrlo lako nas se može identificirati. I to čak i u slučaju da svoje osobne podatke nismo javno objavili, a što čini

[10] Tijekom izrade ove disertacije, temeljem spoznaja o razmjerima i oblicima nadzora i praćenja, autor je pokušao vlastitu privatnost uzeti u svoje ruke te je poduzeo brojne korake kako bi osigurao svoju digitalnu anonimnost. Koraci koje je poduzeo, svoje osobno iskustvo i konačni osvrt na učinkovitost i svrsishodnost odricanja te procjenu učinkovitosti poduzetih mjera bit će osnova za izradu jednog od idućih radova.

velika većina internetskih korisnika. Među svim načinima na koje internetski divovi ugrožavaju našu privatnost, doista je teško izdvojiti posebno problematično postupanje. Cilj gotovo svake tvrtke koja pruža usluge na internetu jest prikupiti što više podataka o korisnicima kako bi te podatke obradili i koristili za pružanje bolje usluge, prikazivanje reklama skrojenih baš za korisnika ili, češće, kako bi ih prodali. Kako bi ih prodali oglašivačima, tvrtkama koje nam nude određene usluge, tvrtkama koje žele utjecati na naše političke preferencije ili bilo kome tko je zainteresiran za te podatke. Osim rijetkih časnih iznimki, jednako općenito i nejasno opisan je način postupanja s našim podacima u politikama privatnosti različitih elektronskih usluga ili aplikacija. Uostalom, te politike privatnosti ionako malo tko čita. Kako bi ukazali na tu činjenicu, britanski pružatelj usluge besplatnog wi-fi pristupa Purple u svoje uvjete korištenja usluge na koje svaki korisnik mora pristati ukoliko želi koristiti njihovu besplatnu uslugu, ubacio je odlomak prema kojem:

> Od korisnika se može zahtijevati da, prema Purpleovom nahođenju, obavi 1000 sati društveno korisnog rada koji može uključivati sljedeće: Čišćenje lokalnih parkova od životinjskog izmeta, davanje zagrljaja psima lutalicama, ručno odčepljivanje zaštopanih kanalizacija, čišćenje prijenosnih toaleta na lokalnim festivalima i događajima, oslikavanje ljuski puževa kako bi im se uljepšalo postojanje te struganje žvakaćih guma s ulica (Thompson, 2017: 1)

Na čišćenje javnih zahoda u zamjenu za malo besplatnog wi-fija u dva tjedna pristalo je čak 22000 osoba. Iako se radi o pravno sasvim valjanom ugovoru, Purple ne namjerava od korisnika zatražiti bilo kakav rad, već su željeli ukazati na neučinkovitost mjera davanja nedvojbenog pristanka za prikupljanjem podataka, sudjelovanjem u marketinškim aktivnostima i općenito su željeli kritizirati to što se pristanak na ugovore od nekoliko desetaka, stotina pa i tisuća stranica putem samo jednog klika smatra pravno valjanim.

No, politike privatnosti i uvjeti pružanja usluga internetskih divova nisu neslana šala. Jedan od brojnih patenata koje je Google zaštitio baca svjetlo na konkretnije načine na koje prikuplja naše podatke. Pa tako Google eksplicitno navodi kako korisnički podaci koje prikuplja mogu uključivati:

- sadržaj web-stranica koje korisnik posjećuje
- demografske podatke (podatke o plaći, karakteristike susjedstva, dob, bračni status, razinu obrazovanja, podatke o djeci i sl.)
- geografske podatke (poštanski broj, državu, adresu stanovanja i sl.)
- psihografske podatke (društvenu pripadnost, životni stil, osobine ličnosti i sl.)
- ranije pretrage koje je korisnik zadavao
- podatke o ranijim reklamama koje su korisniku prikazane, koje je odabrao te one nakon kojih je realizirao kupovinu

- podatke o dokumentima koje je korisnik pregledavao ili ih je uređivao
- interese korisnika
- eksplicitne ili implicitne povratke podatke o korisničkim internetskim aktivnostima (koliko je dugo gledao određenu reklamu, je li reagirao na nju i sl.)
- povijest pretraživanja
- povijest kupovanja (Bharat, Lawrence, Sahami i Singhal, 2003: 1)

Osim ovih podataka, Google podatke crpi i iz sadržaja e-pošte koju korisnici šalju i primaju kao i sadržaja svih priloga u tim porukama (Gibbs, 2014). Doduše, krajem lipnja 2017. godine na službenom blogu objavljeno je kako planiraju prestati s tom praksom, iako nije navedeno kada se to može očekivati (Greene, 2017). Levine navodi kako „Google nije samo skenirao korisničku e-poštu radi traženja ključnih riječi, nego je razvio cijelu pozadinsku tehnologiju za sastavljanje sofisticiranih dosjea o svima koji koriste Gmail. Sva komunikacija bila je podložna dubokoj lingvističkoj analizi, što znači da su razgovori analizirani kako bi se identificirale ključne riječi, značenje pa čak i ton kojim je tekst pisan. Pojedinci su povezani s njihovim pravim identitetom pomoću podataka o kontaktima pohranjenima u Gmailovu imeniku, priloženi dokumenti pregledavani su u potrazi za podacima i sve prikupljeno uspoređivano je s prethodnim elektronskim interakcijama te podacima prikupljenima putem ostalih Googleovih servisa kao i drugih izvora“ (Levine, 2013a: 1)

Unatoč tome što je Googleov službeni moto „Ne budi zao“ (Google, n.d.), ne možemo reći kako se Google u svojoj relativno kratkoj povijesti uvijek vodio njime. Vjerojatno najveći propust napravili su u sklopu svojeg projekta *Street view*, kojim se mnogi svjetski gradovi, i druga mjesta, snimaju uz pomoć panoramskih kamera s pogledom od 360 stupnjeva te se te snimke obrađuju i postavljaju na Internet. Ova revolucionarna tehnologija omogućila je da se brojna mjesta, uključujući i mnoge hrvatske gradove, može virtualno posjetiti iz svojeg naslonjača. Međutim, osim čudne video opreme, Google je svoje automobile i tricikle opremio sofisticiranom opremom za snimanje prometa Wi-Fi mreža pored kojih su svojim vozilima krenuli. Na taj način Google je prikupljao ne samo podatke o mrežama na koje je naišao, nego i sadržaj prometa koji uključuje korisnička imena, lozinke, elektroničku poštu, imena, dokumente. Google je najprije poricao da prikuplja sadržaj prometa otvorenih Wi-Fi mreža, a suočen s pritiscima priznao je svoju praksu (Kiss, 2010), a izgubili su i tužbu (Streitfeld, 2013), unatoč tome što su svoju praksu branili do samoga kraja. Vrijedi istaknuti kako je ovo primjer koji zapravo predstavlja eksternu ugrozu privatnosti budući da je, za razliku od sadržaja e-pošte i korisničkih podataka koje su ljudi pristali dijeliti s njima, sadržaj prometa otvorenih Wi-Fi mreža prikupljao bez znanja i dopuštenja. Taj primjer dobro ilustrira kako je granica između

interne i eksterne ugroze vrlo tanka i tek provizorna, slično kao i granica između potencijalne i izravne ugroze privatnosti.

Odličan primjer za ilustriranje punih razmjera potencijalne ugroze privatnosti kao posljedice vlastita odricanja kontrole nad podacima o sebi jest benigno korištenje Googleove tražilice. Njihova najjednostavnija usluga zapravo je najznačajnija. Upiti pretraživaču otkrivaju stvari o nama koje ni čitanje naše pošte ne može otkriti. U interakciji s drugima uvijek zauzimamo određenu socijalnu ulogu, upravljamo dojmovima i ne otkrivamo sve. Ali sami ispred pretraživača slobodni smo Google pitati upravo ono što nas najviše tišti, ono što nikoga nismo pitali, ono što se bojimo pitati, ono što si bojimo priznati, ono čega se sramimo, ono za čime potajno žudimo. Mladi znanstvenik i bivši zaposlenik Googlea Seth Stephens-Davidowitz (2017) četiri je godine koristeći uslugu Google Trends analizirao javno dostupne anonimne podatke o pojmovima koje se pretražuje, s koje lokacije i u koje vrijeme. Podatke je kombinirao s određenim ostalim bazama podataka te je dobio vrlo zanimljive podatke o temama poput mentalnih bolesti, ljudske seksualnosti, abortusa, religije, zdravlja. Prateći tko i odakle traži homoseksualnu pornografiju utvrdio je kako je u SAD-u oko 5% homoseksualaca. Na svaku pretragu o veličini penisa koju zatraži žena, ide 170 pretraga o veličini penisa koju zatraže muškarci. Zaključio je kako se stereotip *zli* pretražuje zajedno uz Židove, muslimane, homoseksualce, ali ne i uz crnce, Meksikance, Azijate i kršćane. Dvostruko češće se pretražuje fraza *je li moja kći pretila* nego *je li moj sin pretio*, unatoč tome što službeni podaci pokazuju kako je pretilih dječaka u SAD-u 35%, a pretilih djevojčica 28%. Najčešća riječ koja se pretražuje u frazi *je li moje dvogodišnje dijete…* je riječ *nadareno*, a roditelji su dva i pol puta češće pretraživali *je li moj sin nadaren* u odnosu na *je li moja kći nadarena*. Ovi podaci pokazali su se dosljedni bez obzira na to dolaze li pretrage iz karakteristično tradicionalnih ili liberalnih područja SAD-a (Stephens-Davidowitz, 2017). Stephens-Davidowitz je svoju analizu radio na agregiranim podacima anonimnih korisnika, ali Google je za većinu tih pretraga znao točno ime i prezime onoga tko pretražuje određeni pojam. Google točno zna tko pretražuje pojmove poput *ubij muslimane* ili *kako kod kuće izazvati pobačaj*.

Facebook je otišao i korak dalje. Oni su pomoću onih malih oznaka *Sviđa mi se*, koje se nalaze posvuda na internetu, pratili sve korisnike koji bi posjetili stranicu s tom oznakom. Niste morali biti korisnici Facebooka niti logirani u svoj korisnički račun, niste morali *lajkati* neki sadržaj, ma niste morali ni ugledati oznaku *Sviđa mi se*, a facebookove skripte već su vas pratile i prikupljale su podatke o vama (Efrati, 2011). Prije nekoliko godina Facebook je od Microsofta

kupio oglašivačku platformu Atlas kojom je želio ugroziti Googleovu apsolutnu dominaciju na tržištu internetskih oglašivača (Marshall, 2014). Ako ništa drugo, vrlo detaljne podatke o čak dvije milijarde korisnika već imaju. Ideja je bila iskoristiti detaljno znanje o korisnicima kako bi potencijalnim klijentima ponudili skrojeno oglašavanje namijenjeno točno određenim precizno odabranim kategorijama korisnika (Goel, 2014). Nakon što su 2016. godine zbog slabih rezultata ugasili dio platforme, nedavno su najavili kako će krenuti u novu marketinšku ofanzivu (Ha, 2017). Cilj im je još bolje pratiti korisnike te klijentima omogućiti individualizirano oglašavanje na svim uređajima koje ciljani korisnici koriste. Nedavno istraživanje napravljeno na Sveučilištu Princeton na uzorku od milijun internetskih stranica korištenjem specijaliziranog softvera za mjerenje privatnosti na internetu pokazalo je kako čak 76% svih analiziranih internetskih stranica ima ugrađen skriven Googleov softver za praćenje, a daleko zaostaju Facebook s i dalje impozantnim prisustvom na čak 24% internetskih stranica te Twitter s 10% (Englehardt i Narayanan, 2016).

Kao što je u prethodnom dijelu istaknuto za NSA i GCHQ, potrebno je istaknuti kako Google i Facebook nisu ni po čemu drugačiji od svojih konkurenata. Oni jednostavno rade isto što i većina tvrtki koja nudi svoje usluge na internetu. Apple, Microsoft, Yahoo, Dropbox prikupljaju i čitaju naše podatke, koriste ih, manipuliraju njima, dijele ih s drugima ili ih prodaju. Dapače, svjesni osjetljivosti teme, ali i činjenice da većinu korisnika ugrožavanje privatnosti zapravo vrlo malo brine, Google je u svojoj politici privatnosti u mnogočemu transparentniji od mnogih drugih sličnih pružatelja usluga. Međutim, Google i Facebook posebno su izdvojeni jer su dobar primjer budući da su toliko veliki da im količina podataka koje posjeduju o milijardama svojih korisnika daje moć kakva je dosad bila nezabilježena u svijetu.

2.3.3. Koga briga: što ima loše u nekritičkom davanju osobnih podataka?

Mnogi se pitaju što ima loše u tome da softverski roboti prate naše kretanje po internetu, što ima loše u tome da automatizirani oglašivači sastavljaju sofisticirane, detaljne i nevjerojatno precizne psihološke profile o nama kako bi nam pružali vrlo precizne reklame? Ne štede li nam oni vrijeme na taj način? Što se može razviti iz tih benignih potencijalnih ugroza privatnosti? Uostalom, u zamjenu za to nevidljivo robotizirano prikupljanje podataka nude nam potpuno besplatno vrlo kvalitetne, i inače vrlo skupe, usluge. Odgovor na ova retorička pitanja naizgled djeluje vrlo jednostavan. Umjesto da sami pretražujemo Internet u potrazi za najboljim proizvodom koji smo poželjeli kupiti, taj nam proizvod već sam iskače iz svakog elektroničkog

uređaja koji uzmemo u ruku. Netflix nam nudi upravo onaj film koji će nam se zasigurno svidjeti, Amazon savršenu knjigu za nas, a Youtube video sadržaj koji savršeno sažima naše misli tijekom dana kao i pjesme koje nam se upravo slušaju.

Međutim, nažalost nije sve tako sjajno kao što se čini. Postoji nekoliko vrlo ozbiljnih opasnosti koje se skrivaju iza automatskog prikupljanja podataka i profiliranja ljudi, odnosno nekoliko vrlo ozbiljnih izravnih ugroza koje mogu lako nastati iz opisanih potencijalnih internih ugroza privatnosti. Podatke koje smo predali različitim tvrtkama, koje smo poslali na poslužitelje diljem planeta, koje smo objavili na društvenim mrežama, podatke o tome što volimo, što ne volimo, što želimo i što ne želimo mogu koristiti pojedinci ili organizacije koje nismo ovlastili. Svojim izlaganjem ne predajemo samo svoje podatke, već predajemo *kontrolu* nad svojim podacima. Kao što će biti prikazano u nastavku, naše podatke tvrtke ili državne institucije mogu izgubiti, oni im mogu biti ukradeni, a mogu ih jednostavno i prodati. Naši podaci mogu biti korišteni u svrhe koje nismo odobrili, ili smo zbog nečitanja ili nerazumijevanja politika privatnosti, bili uvjereni kako ih nismo odobrili. Oni mogu biti korišteni kako bi se manipuliralo našim stavovima, uvjerenjima i osjećajima. Kako bismo kupovali više, provodili više vremena koristeći pojedine usluge ili kako bismo bili skloniji prihvatiti određene javne politike ili političare. Stvaranjem naših digitalnih dvojnika koji nas poznaju bolje od nas samih te istovremeno izlaganjem samo određenom odabranom sadržaju, oduzima nam se stupnjeve slobode, formira se naše preferencije i utječe se na način na koji gledamo i razumijemo svijet.

2.3.3.1. Omogućavanje pristupa podacima trećoj strani

Kada govorimo o realiziranju potencijalne ugroze u izravnu ugrozu, jedan od načina na koji se to najčešće čini svakako je mogućnost da podatke o korisnicima koristi netko koga korisnici nisu ovlastili i da ih koristi na način koji može naštetiti korisnicima. Poslužitelji neke od tvrtki kojoj smo ustupili svoje podatke ili oglašivača koji posjeduje naše profile mogli bi biti izloženi hakerskom napadu u kojem bi naši vrlo vrijedni podaci mogli završiti u rukama ljudi koji se, blago rečeno, u svojem poslu ne vode etičkim načelima i nemaju korporativnu politiku upravljanja osobnim podacima. Osim toga, poslužitelji bi mogli biti i fizički otuđeni, tvrtka bi mogla propasti i prodati naše podatke ili tvrde diskove iz kojih bi se ti podaci relativno jednostavno mogli dohvatiti. Iz Snowdenove objave poznato je i kako je NSA tajno koristila jedan od Googleovih kolačića tzv. PREF kolačić kako bi odabrala korisnike prema kojima je onda ofanzivno postupala (Soltani, Peterson i Gellman, 2013). Unatoč tome što taj kolačić ne posjeduje identifikacijske podatke o korisniku, on omogućuje da se određenog jedinstvenog

korisnika prati dok pretražuje Internet, što u slučaju da je korisnik već poznat znači da ga se vrlo jednostavno uz pomoć tog kolačića može pratiti osobu na internetu. Simpatična igra FarmVille, koja se prije nekoliko godina proširila Facebookom zapravo je prikupljala podatke o korisnicima i prodavala ih je različitim oglašivačima i tvrtkama za praćenje osoba. I u tome nipošto nije usamljena. Prema istraživanju Wall Street Journala, čini se da je većina najpopularnijih aplikacija sa stotinama milijuna korisnika na Facebooku na sličan način zarađivala (Takashi, 2010). Većina aplikacija koje se koriste na Facebooku traže potpuni pristup korisničkome profilu. Jednostavno, to je cijena besplatnog igranja. Slično vrijedi i za aplikacije koje korisnici koriste na svojim pametnim telefonima. Mnoge aplikacije traže pristup brojnim podacima koji se nalaze na pametnim telefonima poput telefonskog imenika, pohrane, fotografija, traže i pristup kameri, mikrofonu te biometrijskim senzorima. Jedna od najpopularnijih mobilnih igara Angry Birds, koja je preuzeta više od potpuno nevjerojatnih tri milijarde puta (Robertson, 2015), prikupljala je identifikacijske podatke o korisnicima i podatke o njihovim uređajima te ih je prodavala, što je proizvođač Rovio priznao cinično uputivši sve zainteresirane na vrlo jasnu politiku privatnosti i uvjete korištenja koje su korisnici preuzimanjem aplikacije prihvatili (Sumner, 2015). To pokazuje kako potencijalna ugroza, pristajanje na uvjete korištenje različitih aplikacija i dopuštanje pristupa svojim osobnim podacima različitim tvrtkama, može lako postati znatno ozbiljnija ugroza naše privatnosti, pa i izravna ugroza. Nadalje, podatke koje je prikupljao Rovio, kao i brojne druge tvrtke, potajno su koristili NSA i GCHQ zadovoljni što je netko drugi umjesto njih odradio posao (Larson, Glanz i Lehren, 2014). To pokazuje kako je ne samo tanka granica između potencijalne i izravne ugroze, već kako je u digitalnom dobu vrlo tanka i granica između interne i eksterne ugroze privatnosti. Dok se u iznesenim primjerima naizgled čini kako se radi o eksternoj ugrozi privatnosti jer nam se kontrola nad pristupom podacima o sebi oduzela bez našeg znanja i odobrenja, to jednostavno nije točno. Preuzimanjem aplikacija na svoj mobilni telefon, preuzimanjem kolačića u svoj internetski preglednik pristali smo na uvjete korištenja. Iste one uvjete u kojima je možda pisalo kako pristajemo čistiti javne toalete. Nečitanje ugovora ne lišava nas obveze za provođenje njegovih odredbi. S obzirom na to, očigledno je kako se zapravo radi o internoj ugrozi, odnosno o tome kako smo se zapravo voljno odrekli kontrole nad svojim podacima.

Podsjetimo, u prošlom je poglavlju prikazana je deskriptivna definicija privatnosti Williama Parenta prema kojoj je privatnost stanje u kojem drugi ne posjeduju podatke o nama koji već

nisu na određeni način dokumentirani u javnim zapisima (Parent, 1983). Parent je smatrao kako otkrivanje, dijeljenje ili obrađivanje bilo kojeg osobnog podatka koji je dio javnog zapisa u širem smislu, ne predstavlja ugrozu nečije privatnosti. Kao što je detaljnije prikazano u prošlom poglavlju, taj je pogled doživio brojne kritike. Dakako, u vrijeme kada je Parent postulirao svoju definiciju privatnosti pojam javnog zapisa bio je različit nego što je danas u digitalno doba. Tada je doista bilo teško očekivati da se smatra kako je svaki podatak koji smo u bilo kojim okolnostima javno podijelili istovremeno predstavlja naše odricanje od privatnosti. Sama tehnologija pohrane i mogućnosti dijeljenja značajno su otežavale mogućnost pristupa i dijeljenje čak i javno dokumentiranih podataka. Međutim, rapidni razvoj informacijske i komunikacijske tehnologije, omogućio je drastičan napredak u mogućnostima pohrane i dijeljenja podataka i zapisa, kako privatnih tako i javnih. Kapaciteti nadzora koje koriste moderne obavještajne službe, sofisticiranost oblika i načina prikupljanja korisničkih podataka internetskih divova, enormne baze podataka i burze za trgovinu osobnim podacima čine Parentovu premisu valjanom. I doista, iz podataka iznesenih u ovom poglavlju lako je zaključiti kako podatke koje jednom objavimo u javnoj sferi više ne možemo smatrati privatnima. Cijeli gradovi prekriveni su kamerama, institucije, trgovine, škole i fakulteti posjeduju sustave koji nas snimaju bez prestanka. Naša računala, pametni telefoni, automobili i televizori gledaju nas i slušaju. Bilježe naše naredbe i preferencije i međusobno ih dijele s partnerskim ili konkurentskim tvrtkama. Temeljem prikupljenih podataka naprednim algoritmima uspijevaju s visokom vjerojatnosti zaključiti i o našim karakteristikama, željama i strahovima koje nikada nismo izrekli, od kojih nekih možda ni samo nismo svjesnu. A u tom pohranjivanju, obrađivanju i dijeljenju našim podacima pokušavaju pristupiti zlonamjerne treće strane poput neprijateljskih država, kriminalaca ili zlonamjernih organizacija.

Ili se jednostavno u najboljoj namjeri može dogoditi pogreška i naši podaci mogu neželjeno završiti u krivim rukama. A pogreške se događaju. I to ne samo malim tvrtkama koje nemaju dovoljno znanja ni resursa kako bi zaštitile i upravljale našim osobnim podacima. Pogreške se događaju i državnim institucijama najvišeg ranga koje posjeduju vrlo osjetljive osobne podatke o svojim građanima, ali i druge osjetljive podatke koji mogu ozbiljno naštetiti nacionalnoj sigurnosti, a time i sigurnosti svojih građana. Sasvim aktualan jest primjer propusta švedske Agencije za promet koja je stranim državljanima bez odgovarajućeg sigurnosnog ovlaštenja učinila dostupnim osobne podatke milijuna svojih građana kao i povjerljive podatke o državnoj infrastrukturi, pripadnicima vojske i osobama sa zaštićenim identitetom (Jones, 2017). Naime,

ta je državna agencija 2015. godine brigu o svojoj bazi podataka i informacijskom sustavu prepustila privatnim tvrtkama u Češkoj i Srbiji. To samo po sebi ne bi bilo problematično da sustavi tvrtki na čijim je poslužiteljima pohranjena baza podataka nisu bili uređeni na način da su toj bazi podataka mogle pristupiti i osobe koje nisu imale odgovarajući sigurnosni certifikat. Baza podataka sastojala se od osobnih podataka o milijunima švedskih državljana, imenima, fotografijama, adresama stanovanja. No, osim toga, baza podataka uključivala je i izuzetno povjerljive podatke poput „osobnih podataka o pripadnicima vojske i tajnovitih specijalnih postrojbi, podatke o sumnjivcima koje je tražila policija, ali i tisućama građana koji se nalaze u sustavu zaštite svjedoka kao i potpune podatke o modelima i stanju svih vojnih vozila te tehničke podatke o cestama i mostovima.“ (Jones, 2017: 1). Ovaj primjer samo pokazuje kako je u digitalnom dobu velikih podataka lako napraviti grešku, a dijelom pokazuje i kako se na dijeljenje osobnih podataka građana više ne gleda kao na nešto što treba čuvati pod svaku cijenu. Dakako, opravdano je zgroziti se nad načinom na koji je Švedska vrlo osjetljive osobne i državne podatke poslala u stranu državu i omogućila je neovlaštenim osobama pristup tim podacima. Međutim, za mnoge od nas takva osuda bila bi licemjerna uzmemo li obzir količinu i sadržaj podataka koje sami javno dijelimo i kakve smo sve privole za korištenje naših podataka dali tvrtkama diljem planeta.

2.3.3.2. Korištenje podataka na način za koji (mislimo da) nismo dali odobrenje

S jedne strane mi dobrovoljno i obilato otkrivamo svoje podatke različitim tvrtkama i objavljujemo ih na društvenim mrežama, a s druge strane bez našega znanja ti se podaci dalje obrađuju, prosljeđuju i koriste u svrhu koju nismo očekivali. A neki od rezultata takve obrade i daljnjeg korištenja mogu nam i ozbiljno naštetiti. Slično kao i u prošlom odjeljku, zbog načina na koji olako pristajemo na uvjete korištenja raznih usluga, može nam se činiti kako se radi o eksternoj ugrozi te kako se podaci bez našeg znanja i protiv naše volje koriste na određeni način, ali u mnogim slučajevima radi se o tome kako smo na sve te uvjete jednostavno pristali.

Osim toga da naše osobne podatke koristi netko koga nismo ovlastili poput drugih tvrtki ili obavještajnih službi, potencijalna ugroza kao posljedica nekritičkog dijeljenja osobnih podataka može se realizirati i na način da se naši podaci koriste na način na koji nismo očekivali. Primjer oca koji je za trudnoću svoje maloljetne kćeri saznao od supermarketa vrlo je plastičan. Naime, New York Times objavio je 2012. godine priču o tome kako je američki supermarket Target prateći potrošačke navike kupaca zaključio da je jedna maloljetna djevojčica trudna te joj je počeo slati reklamne kupone za trudnički, majčinski i novorođenački program. Pronašavši

u poštanskom sandučiću reklame za dječju odjeću i kolica naslovljene na njegovu maloljetnu kćer, otac se bijesan otišao požaliti Targetu. Ondje je dobio ispriku, no svega nekoliko dana kasnije nazvao ih je kako bi se sam ispričao budući da je njegova kći doista bila trudna (Duhigg, 2012). Čini se da je Targetov analitički softver bio besprijekoran, iako odjel marketinga nije iskazao odgovarajuću diskreciju i takt. Target u tome nipošto nije usamljen. Gotovo svi trgovački lanci danas koriste različite oblike praćenja svojih kupaca i njihovih potrošačkih navika. Jedan od njih svakako su različiti programi vjernosti, ali i bez uključivanja u program vjernosti trgovci prate klijente pomoću kartica kojima plaćaju, a neki imaju i modele pomoću kojih prate čak i kupce koji plaćaju gotovinom (Ferguson, 2013). U mnogim trgovinama i trgovačkim centrima nadzorne kamere spojene su na sofisticiran softver koji ima mogućnost prepoznavanja kupaca preko njihova lica, ali i očitavanje brojnih antropometrijskih i bihevioralnih varijabli. Na primjer, pri ulasku u trgovinu softver može iznenađujuće precizno procijeniti dob, spol, visinu, težinu, boju kose i rasu pojedinog kupca te može zabilježiti rutu kojom se kupac kretao po trgovini, koliko je dugo gledao pojedini artikl i je li imao nekakvu fizičku interakciju s pojedinim artiklom. Ti se podaci mogu spojiti i s identitetom kupca ako na blagajni pruži svoju karticu programa vjernosti ili plati kreditnom karticom, a cijeli je postupak potpuno automatiziran.

Na ovaj način prikupljeni podaci najčešće se koriste za oglašavanje, a praćenje korisnika služi tome kako bi se omogućila bolja usluga. Međutim, mnoge tvrtke podatke o korisnicima prodaju ili daju na korištenje trećoj strani, osobama i tvrtkama. Najčešće se radi o drugim oglašivačkim tvrtkama, ali može se raditi i o privatnim tvrtkama koje se bave trgovanjem osobnim podacima. A od njih podatke može kupiti gotovo bilo tko, uključujući i različite prevarante i zlonamjernike (Levine, 2014). Tvrtka MEDbase200 jedna je od podatkovnih brokera koji trguje osobnim podacima vezanima uz zdravstvena pitanja. Prije nekoliko godina došli su pod povećalo javnosti jer su ponudili bazu silovanih osoba za 79 američkih dolara po tisuću osoba. Nastupila je opća konsternacija javnosti i ta je baza ubrzo povučena iz prodaje, no i dalje se od njih za sličnu cijenu mogu kupiti baze osoba oboljelih Alzheimerove bolesti, Aspergerova sindroma, depresije, gonoreje, sifilisa, neplodnosti, genitalnog herpesa, HIV pozitivnih osoba i tako dalje, i tako dalje (Levine, 2013b).

Dakako, većinu vremena samopouzdani smo i slobodni građani koji ne rade ništa pogrešno. Javno i ponosno objavljujemo svoje stavove, fotografije s raznih proslava i događanja na kojima smo sudjelovali. Nemamo ništa za sakriti. Sve dok ne shvatimo da možda ipak imamo. Kao što

je ranije navedeno, ne mora se uopće raditi o skrivanju nečega pogrešnoga. Recimo, radno zakonodavstvo vrlo strogo propisuje kako se prilikom zapošljavanja ne smije diskriminirati kandidate ni po kojoj osnovi osim po onoj koja utječe na radnu uspješnost. Pa tako od potencijalnih kandidata nije dopušteno tražiti podatke o nacionalnosti, spolnoj orijentaciji, vjeroispovijesti, političkim i drugim preferencijama, stavovima, vrijednostima. Nije dopušteno pitati s kime kandidati stanuju i planiraju li imati djecu. Međutim, dok kandidati te podatke skrivaju u svojim životopisima i skloni su tužbama ukoliko ih se tijekom intervjua pita o njima, na društvenim mrežama i internetu ponosno objavljuju upravo te podatke pa i znatno intimnije i detaljnije podatke o sebi. Sve što potencijalni poslodavci trebaju napraviti jest otvoriti internetski preglednik i podaci za koje smo mislili kako su tek nevino komentiranje među prijateljima, kritika određenog političara ili neugodan osvrt na loše iskustvo u restoranu mogu biti presudni u tome hoćemo li biti odabrani za radno mjesto koje baš jako želimo. CareerBuilderovo godišnje istraživanje zapošljavanja temeljem društvenih medija, pokazalo je kako čak 70% poslodavaca koristi društvene medije kako bi provjerilo kandidate prije zapošljavanja, dok je taj postotak bio tek 11% 2006. godine. Više od pola poslodavaca odlučilo je ne zaposliti kandidata nakon što su proučili njegov profil na društvenim mrežama. No, ni brisanje ili skrivanje profila nije rješenje jer je čak 57% poslodavaca nesklono zaposliti kandidata kojeg ne mogu pronaći na internetu (Salm, 2017). Danas se od svakog kandidata kojem je stalo do karijere očekuje da pažljivo uređuje svoj digitalni otisak, da upravlja svojim društvenim profilom poput kakve filmske zvijezde ili javne osobe. Uz ovakvu dostupnost osobnih podataka i javno objavljivanje intimnih podataka o sebi, svatko je danas javna osoba i vlastiti *paparazzi*.

2.3.3.3. Marionete na koncu: manipuliranje korisnicima društvenih mreža

Osim opisanih individualnih opasnosti od korištenja naših podataka u svrhu koju (mislimo da) nismo odobrili, postoji i sasvim druga skupina opasnosti, šireg društveno-političkog karaktera. Temeljem široko prikupljanih velikih podataka (eng. *Big Data*) stvaraju se vrlo detaljni profili korisnika pomoću kojih im se umjetno stvaraju potrebe kako bi trošili više, upravljanjem sadržajem koji je dostupan korisnicima izolira ih se od negativnih stavova kao i onih dijametralno različitih od njihova, a uparivanje psiholoških profila s političkim stavovima, brigama, strahovima i potrebama omogućuju manipulaciju i socijalni inženjering koji može imati globalne političke implikacije. Mladi psiholog Michal Kosinski, za vrijeme svojeg doktorata iz psihometrije na Sveučilištu Cambridge razvio je alat za koji nije mogao ni sanjati

da će samo nekoliko godina kasnije utjecati na svjetsku politiku. Naime, izradio je pojednostavljenu, ali i dalje visoko pouzdanu, verziju inventara ličnosti temeljem općeprihvaćenog peto faktorskog modela ličnosti u obliku aplikacije za Facebook. Korisnici Facebooka mogli su pomoću te aplikacije odgovorom na nekoliko pitanja saznati svoj profil ličnosti prema peto faktorskom modelu. Jedino su prilikom instalacije aplikacije trebali omogućiti potpun pristup svojem Facebook profilu, što većina već rutinski odobrava. Na taj je način Kosinski dobio pristup enormnoj količini podataka o korisnicima koje je mogao povezati s njihovim profilom ličnosti. Jednom kada je na temelju dovoljnog broja korisnika utvrdio zadovoljavajuće visoke korelacije, mogao je donositi zaključke u oba smjera. Mogao je na temelju toga prati li na Facebooku netko Lady Gagu znati da je velika vjerojatnost da se radi o ekstrovertiranoj osobi, te kako je jedna od najpouzdanijih pokazatelja nečije heteroseksualnosti činjenica da im se sviđa bend Wu-Tang Clan. Kosinski je kroz godine unaprijedio i razvijao svoj model te je 2012. godine temeljem prosječno 68 oznaka sviđa mi se mogao s izuzetno visokom točnosti procijeniti korisnikovu boju kože, seksualnu orijentaciju, političku pripadnost, inteligenciju, religijsku pripadnost, uživanje alkohola, cigareta i droga pa čak i to jesu li nečiji roditelji rastavljeni (Grassegger, Krogerus i Dehaye, 2017). Međutim, sve je bilo dobro dok je model služio institutu na Cambridgeu u znanstvene svrhe. Nakon što je Kosinski odbio prodati svoj model sumnjivoj tvrtki koja se bavila utjecajem na izbore, ta je tvrtka uz pomoć Kosinskijevog bivšeg suradnika sama razvila sličan model. Radi se o tvrtki Cambridge Analytica, koja je značajno unaprijedila Kosinskijev model te je dobivene podatke povezala s podacima o korisnicima koje je otkupila od ranije spomenutih brokera privatnim podacima tako da danas tvrde kako za svaku osobu u SAD-u imaju čak 4000 do 5000 podatkovnih točaka (Nix, 2016). To im omogućuje da segmentiraju biračko tijelo kako bi identificirali skupinu potencijalnih birača koja je sklona izlasku na izbore, ali je još uvijek neodlučna. Potom se korištenjem velikih podataka i njihova psihološkog modela razina analize spušta sve do razine korisnika kako bi se skrojile najučinkovitije metode bihevioralnog i persuazivnog djelovanja koje bi ih pomaknule prema željenom ishodu[11]. Cambridge Analytica sudjelovala je u izbornim kampanjama američkog predsjednika Donalda Trumpa, kampanji za izlazak Velike Britanije iz EU, kampanji američkog republikanskog kandidata za predsjedničkog kandidata Teda Cruza kao i u desecima različitih izbornih kampanja diljem svijeta (Cadwalladr, 2017). Cambridge

[11] Za detaljniji prikaz i živi primjer načina na koji Cambridge Analytica koristi velike podatke i psihološke profile kako bi utjecala na birače svakako vrijedi pogledati kratko predavanje izvršnog direktora Alexandera Nixa pod naslovom *The Power of Big Data and Psychographics* na https://www.youtube.com/watch?v=n8Dd5aVXLCc

Analytica nipošto nije jedina tvrtka koja koristi ovakve suvremene marketinške alate i tehnologiju kako bi utjecala na birače ili na potrošače i u budućnosti možemo očekivati značajan porast ovakvog skrojenog marketinškog komuniciranja i uvjeravanja. Ovako učinkovita i perfidna persuazija potencijalnih glasača ima implikacije ne samo na njihovu slobodu neovisnog donošenja odluka i upravljanja svojim životima već ona ima i šire socio-političke implikacije. Cinično parafrazirajući ključne čelnike tzv. Brexit kampanje koji su tvrdili kako su prilikom glasanja za izlazak Ujedinjenog Kraljevstva iz Europske unije „slijedili svoje srce", Harari je upozorio kako bi se „(…) Ovo oslanjanje na srce moglo pokazati kao ahilova peta liberalne demokracije jer kada jednom netko, bilo u Pekingu ili San Franciscu, stekne tehnološke mogućnosti za hakiranjem i manipuliranjem ljudskoga srca, demokratski izbori pretvorit će se u emocionalnu lutkarsku predstavu." (Harari, 2018:1:54:45)

Ranije je spomenut model simbiotske mreže. Prema tom modelu interneta, istovremeno s protokom sadržaja od pružatelja sadržaja prema internetskih korisnicima postoji i paralelni tok kojim osobni podaci teku od korisnika prema pružateljima sadržaja (Bernal, 2014). Kako bi povećali svoj profit, pružatelji sadržaja žele postići da korisnici što duže koriste njihove usluge, te da budu što spremniji dijeliti svoje podatke i trošiti svoj novac. Kako bi to postigli, pružatelji sadržaja kroje zasebno iskustvo za svakog korisnika. Bernal to opisuje kao krojenje zasebne mreže za svakog korisnika (Bernal, 2014). I u pravu je. Kako bi korisnicima pružio bolju uslugu Google prilagođava rezultate pretraživanja pojedinom korisniku (Bryan Horling i Kulick, 2009). To znači da će različitim korisnicima za isti upit biti prikazani različiti rezultati, a posebice je značajno što će im prilikom unosa upita prijedlozi za pretraživanje već biti drugačiji. Započnu li dvije osobe u traku za pretraživanje na Googleovoj tražilicu unositi riječi *Amerika je…* dobit će različite rezultate. Jednoj može biti ponuđen dovršetak *zlo* i *bankrotirala*, a drugoj *otkrivena* i *naseljena*. Facebook također koristi algoritme kako bi od stotina objava prijatelja i aktivnosti, događaja, grupa koje korisnici prate odabrao onih nekoliko koje će im biti prikazane na zidu. Kako bi povećali profit, Facebookovi algoritmi korisnicima prikazuju one objave za koje je veća vjerojatnost da će korisnike dulje zadržati uz ekrane, da će ih potaknuti na dijeljenje sadržaja, da će potaknuti njihove potrošačke aktivnosti. Psiholozi Facebookova znanstvenog odjela na svojim korisnicima u tu svrhu provode eksperimente bez njihova znanja. Jednostavno, pristankom na nekoliko desetaka tisuća stranica dugu politiku korištenja Facebooka, korisnici su pristali i na provođenje eksperimenata na sebi. To znači manipuliranje njihovim ponašanjem, doživljajem i emocijama. Tako su u jednom eksperimentalnom istraživanju iz 2013. godine

provedenom na čak 689003 korisnika istraživači manipuliranjem emocionalnih stanja svojih korisnika potvrdili postojanje emocionalne zaraze, odnosno činjenicu da se određena emocija može prenijeti s korisnika na korisnika čak i uz potpuni izostanak neverbalnih znakova (Kramer, Guillory i Hancock, 2014). Mnogi su primijetili kako je korištenje interneta izmijenilo naše mozgove. Unatoč tome što nam je na dohvat ruke dostupna neizmjerna količina podataka, naši kapaciteti za usvajanje tih podataka smanjuje se. Pisac Nicholas Carr navodi kako zbog interneta više uopće ne može čitati romane, a prenosi i komentar jednog patologa koji tvrdi da je jednostavno „izgubio sposobnost ikada više pročitati roman Rat i mir“ (Carr, 2008: 1).

Predviđanje onoga što želimo reći, sugeriranje dovršetka naših rečenica uzima nam stupnjeve slobode i ukalupljuje nas. Izlaganje stalno istim sadržajima utječe na naše viđenje svijeta kroz brojne višestruko potvrđene psihološke mehanizme. Ideja da računalni softveri tzv. *botovi*, radi povećanja profita, korisnike stavljaju u društvene balone istomišljenika možda djeluje zastrašujuće, ali bliska je istini. Jedan od procesa do kojeg dovodi ovakvo razlamanje weba i krojenje iskustva za svakog korisnika je *grupna polarizacija* (Sunstein, 2007), fenomen koji je u socijalnoj psihologiji vrlo dobro opisan i empirijski potvrđen (Aronson i dr., 2005). Grupna polarizacija odnosi se tendenciju grupe da donosi ekstremnije odluke nego što su ih bili spremniji donijeti članovi grupe zasebno. Osim na odluke, grupna polarizacija utječe i na zauzimanje stavova pa će tako grupa imati tendenciju zauzeti radikalniji stav nego njezini članovi svaki za sebe. Razlamanje weba, stavljanje korisnika u društvene balone istomišljenika i krojenje on-line iskustva samo za njih doprinosi pojavi grupne polarizacije, što je empirijski potvrđeno i na uzorku 30 000 *tweetova* (Yardi i Boyd, 2010). Unatoč tome što grupnu polarizaciju najviše generira ekstremni sadržaj, koji je dio šireg problema lažnih vijesti i lažnih profila na društvenim mrežama, razlamanje weba i krojenje iskustva za svakog korisnika direktna su posljedica prikupljanja podataka o njima. Bez masovnog prikupljanja podataka o korisnicima njihova detaljnog profiliranja i želje da ih se što duže zadrži pred ekranima, ne bi ih se toliko izlagalo istom sadržaju, koji je zbog društvenih okolnosti nažalost nerijetko ekstreman.

Slično kao i u jednoj od epizoda popularne znanstveno-fantastične distopije, serije *Black Mirror*, u kojoj svi ljudi imaju određeni društveni rezultat koji im o(ne)mogućuje pristup određenim uslugama, proizvodima pa i dijelovima grada, Kina je nedavno predstavila sličan projekt (Huang, 2015). Radi se o sustavu bodovanja Sesame Credit kojem se korisnici mogu priključiti kako bi ostvarivali različite pogodnosti. Svaki korisnik može ostvariti rezultat

između 350 i 950 bodova na temelju različitih kriterija među kojima je plaćanje računa na vrijeme, potrošačke navike, osobni i poslovni status te rezultat korisnikovih prijatelja. Određene razine rezultata omogućuju pristup brojnim pogodnostima poput kredita, najma vozila bez pologa, bržeg dobivanja viza za putovanja u strane države i slično. Kupovanje papira, olovaka i kineskih proizvoda pozitivno utječe na rezultat korisnika, dok kupovanje nepoželjnih proizvoda poput računalnih igara negativno utječe na rezultat (Falkvinge, 2015). U ovom trenutku korištenje sustava je dobrovoljno i koristi ga oko 350 milijuna korisnika, a od 2020. godine planira se obvezno korištenje sličnog sustava bodovanja koje bi trebalo biti prošireno i na aktivnosti, objave i komentare na internetu kao i na pristupanje i podržavanje različitih udruga (Denyer, 2016). Sesame Credit nije zla tehnologija iz nekog distopijskog romana, nego tehnologija današnjice koju dobrovoljno koriste stotine milijuna ljudi, a obvezni državni sustav bodovanja bit će implementiran već za nekoliko godina. Govoreći o panoptikonu, Foucault je pisao kako ga se, „osim za nadzor, može koristiti i kao laboratorij; kao stroj za provođenje eksperimenata; za promjenu ponašanja“ (Foucault, 1995: 203), na što Facebookovi eksperimenti i Sesame Credit neodoljivo podsjećaju.

2.4. Društvo (bez) privatnosti

„Date li mi šest redaka koje je napisao najpošteniji čovjek, u njima ću pronaći razlog da ga objesim.“

Francuski državnik i kardinal Richelieu prema (Hoyt, 1896: 763).

Neposredno nakon Snowdenovih otkrića sredinom 2013. godine značajno je porasla prodaja Orwellova romana 1984. (Meredith, 2013) te su se često mogle čuti usporedbe kako masovni nadzor i aktivnosti velikih obavještajnih službi podsjećaju na Orwellovu distopiju. Ne možemo reći kako danas živimo u strahu od stalnog nadzora, kako se konstantno falsificira povijest, kako smo izloženi isključivo propagandi, kako za verbalni delikt pa čak i za samu pomisao na kritiku vlasti možemo biti kažnjeni najstrožom kaznom. Sasvim suprotno, slobodni smo reći što mislimo i kako se osjećamo i u tome nas se dodatno ohrabruje. Izloženi smo tolikom broju podataka i informacija da nam je teško razaznati što je doista točno. Istinu je sve teže pronaći, a i čini se kako smo za to sve manje motivirani. Kako bismo bili umreženi sa svojim prijateljima i poznanicima, ili kako bismo postigli određeni status u društvu, objavljujemo mnogo podataka o sebi i činimo to stalno. Istovremeno, softverski roboti kreiraju izuzetno precizne psihološke

profile temeljem kojih kreiraju našu virtualnu stvarnost kako bismo što dulje bili prikovani uz male ekrane te kako bismo trošili što više. Sličnu je realnost Huxley opisao još tridesetih godina prošloga stoljeća.

Brojni primjeri prikazani u ovom poglavlju imali su za cilj demonstrirati kako mnoge naizgled benigne potencijalne ugroze privatnosti mogu lako postati vrlo ozbiljne izravne ugroze privatnosti kojima se direktno ugrožava autonomija pojedinaca. Osim toga, određeni načini na koje se koriste naši osobni podaci imaju direktne posljedice i na šire socio-političke odnose. Demokracija počiva na ideji slobodnih, autonomnih, nezavisnih pojedinaca koji su kadri donositi racionalne odluke. U idućem će poglavlju biti detaljno prikazano kako zapravo ugroze privatnosti, ograničavanje prava na privatnost i rašireno odricanje od vlastite privatnosti narušavaju autonomiju građana, a time predstavljaju i ugrozu za demokraciju.

Osim toga, primjeri prikazani u drugom dijelu poglavlja ilustrirali su kako podjela na eksterne i interne ugroze privatnosti u digitalno doba zapravo nedovoljno dobro opisuje realnost. Naime, zbog razvoja tehnologije, načina na koji suvremena informacijska tehnologija funkcionira i kapaciteta za nadzor modernih obavještajnih službi, većina internih ugroza zapravo su ujedno i eksterne ugroze privatnosti. Preuzimanjem kolačića u naše internetske preglednike, korištenjem mobilnih aplikacija, besplatnih internetskih usluga ili trgovina u velikoj se mjeri odričemo vlastite privatnosti budući da pristajanjem na opsežne uvjete korištenja pružateljima usluga predajemo ne samo svoje podatke već i kontrolu nad njima. Na taj način jednom prikupljene podatke, dalje mogu prikupljati moćne obavještajne službe, kao što je prikazano u slučaju tzv. PREF kolačića ili Roviovih mobilnih igrica. Ili ti podaci mogu biti izgubljeni, prodani ili ukradeni te završiti u rukama zlonamjernih pojedinaca, organizacija ili država. Isprepletenost državnih i korporativnih interesa za masovnim i globalnim nadzorom upućuje na pojavu cijele jedne nove dinamike moći u našem društvu. Čini se da klasična podjela na državne i korporativne interese više ne uspijeva dovoljno dobro obuhvatiti slojevitost i kompleksnost realnosti nadzora u digitalnome svijetu.

Osim zbog zajedničkog korporativnog i državnog interesa za prikupljanjem i dijeljenjem podataka korisnika, na spajanje internih i eksternih ugroza privatnosti utjecala je činjenica kako olako pristajemo na prikupljanje naših podataka i olako ih predajemo. U narednim poglavljima, a osobito u empirijskom istraživanju koje je provedeno, pokušat će se dati odgovor na pitanje je li ljudima uopće i dalje stalo do njihove privatnosti te ako je zašto je se tako olako odriču.

Jedno od mogućih objašnjenja je da je ljudima doista stalo do njihove privatnosti, ali uvjeti korištenja na koje olako pristaju jednostavno su previše nejasni i kompleksni da bi ih se razumjelo. Iz lakoće kojom ljudi pristaju na različite odredbe uvjeta korištenja digitalnih usluga sasvim je jasno kako je sustav tzv. *nedvojbenog informiranog pristanka* na politike privatnosti, uvjete korištenja i pohranu kolačića zakazao. Takav oblik informiranja korisnika i davanja suglasnosti potpuno je neučinkovit. Ukoliko se doista zaštiti pravo na privatnost, korištenje osobnih podataka potrebno je znatno bolje regulirati. No, vrijedi još jednom istaknuti kako ne postoji velika zavjera za prikupljanjem podataka korisnika. Jednostavno se radi o tome da se s obzirom na razvoj tehnologije i oglašivačke industrije korporativni interes za što većim profitom poklapa s državnim interesom za prikupljanjem što većeg broja podataka o pojedincima i organizacijama koje bi mogle naštetiti nacionalnoj sigurnosti ili interesima.

Drugo moguće objašnjenje za stapanje internih i eksternih ugroza je da prilikom korištenja interneta nismo u potpunosti svjesni svoje publike. Boyd (2008) je došla upravo do tih spoznaja te je zaključila kako kod korisnika Facebooka dolazi do socijalne konvergencije budući da se različiti konteksti sažimaju u jedan. Naime, ljudi su navikli prilagođavati svoje ponašanje i razinu izlaganja pojedinom društvenom kontekstu. Na Facebooku dolazi do *socijalne konvergencije* zbog čega ljudi imaju tendenciju dijeliti sve podatke sa svima, što komunikaciju čini učinkovitijom, ali time u značajnoj mjeri gubimo kontrolu nad pristupom našim podacima. Gubimo privatnost.

I konačno, možda ljudima doista više nije stalo do privatnosti. Godine medijske i političke kampanje kojom je privatnost smatrana nečime što koči razvoj i zaštitu nacionalne sigurnosti, godine izlaganja *ništa-za-sakriti* argumentima u kombinaciji s Huxleyevom *somom* i drugim oblicima odvraćanja pažnje možda su postigli da su, kada se radi o privatnosti, ljudi u stanju naučene bespomoćnosti. Poglavlja koja slijede pokušat će dati odgovor na ovo pitanje.

Ako svako naše svjesno, voljno i kontrolirano odricanje od privatnosti znači da će nam povrh toga privatnost biti dodatno ugrožena i protiv naše volje, ako svaka interna ugroza postaje eksternom ugrozom, postavlja se pitanje je li pravo na privatnost danas uopće održivo i može li ga se zaštiti. Osim toga, zaseban je problem što liberalne demokracije nemaju načina ni mogućnosti poveljama, ustavima i zakonima zajamčeno temeljno ljudsko pravo svojih građana na privatnost zaštiti od opisanog nadzora najvećih oglašivačkih tvrtki i obavještajnih službi čime se direktno dovodi u pitanje njihova suverenost. Razumno je zapitati se je li stoga potrebno

redefinirati pojam države koja prema temeljnim postavkama liberalne demokracije ima ovlast i dužnost osiguravati ljudska prava svojim građanima. Očigledna dobrovoljnost i lakoća kojom se ljudi samoinicijativno odriču svojeg prava na privatnost, i u tome ne vide ništa loše, poziva na razmatranje načina na koji ljudi uopće razumiju privatnost i je li im ona važna. Tek će tada biti moguće razumjeti zašto podržavaju politike i ponašanja koja zatiru njihovu privatnost. U narednim poglavljima bit će riječi o ovim kompleksnim pitanjima na koja će biti pruženi teoretski i empirijski odgovori.

3. Konceptualna analiza značaja i vrijednosti privatnosti

3.1. Uvod

Privatnost je temeljno ljudsko pravo. Privatnost predstavlja kontrolu pristupa (podacima o) sebi, a središnja vrijednost privatnosti jest u njezinoj povezanosti s autonomijom, kao središnjim pojmom liberalne demokracije. Eksterne i interne ugroze privatnosti, odnosno sveprisutni nadzor i lakoća kojom se ljudi odriču svoje privatnosti, dosegli su zabrinjavajuće razine i ugrozili su pravo na privatnost. U ovom poglavlju detaljno će se proučiti implikacije ranije opisanih eksternih i internih ugroza privatnosti na privatnost definiranu u terminima kontrole pristupa s posebnim naglaskom na moguće ugroze autonomije, a time i ugroze temelja liberalne demokracije. Među teoretičarima postoji kontinuirana rasprava o pravu na privatnost, a dio te rasprave ranije je detaljno prikazan. Međutim, iz rasprave o koherentistima i redukcionistima detaljno opisane u prvom poglavlju, možemo vidjeti kako većina autora doista prepoznaje privatnost kao zasebno ljudsko pravo, i prepoznaje njezinu supstancijalnu vrijednost. S jedne strane privatnost je povezana s ljudskim dostojanstvom, temeljem iz kojeg proizlaze sva ostala ljudska prava. Privatnost pojedincu osigurava mogućnost da bude ostavljen na miru, da se realizira i slobodno djeluje. Na taj se način otvara prostor i za drugi značaj privatnosti, onaj za društvo, zajednicu i demokraciju. Autonomni, slobodni, ostvareni pojedinci nužan su preduvjet za uspostavu demokratskih društvenih institucija, a demokratski sustav bez njih jednostavno nije održiv.

Istovremeno ugroze i prijetnje privatnosti dolaze sa svih strana, kako izvana, tako i od nas samih. Poštivanje prava pojedinaca direktno je vezano uz legitimnost političkih poredaka koji se definiraju kao liberalno-demokratski. Budući da je privatnost temeljno ljudsko pravo vrijedno zaštite, postoji tenzija između prava i legitimacije liberalno-demokratskih struktura. Država koja pribjegava sveobuhvatnom nadzoru, koja ne štiti svoje građane od zlonamjernih pojedinaca, organizacija i drugih država ili koja stoji po strani dok velike korporacije ugrožavaju privatnost njezinih građana dovodi u pitanje svoj vlastiti liberalno-demokratski legitimitet. Osim toga, građani bez privatnosti su građani bez autonomije. Demokratski legitimitet počiva na autonomnim građanima, slobodnima donositi racionalne i informirane odluke. Bez autonomnih pojedinaca teško je zamisliti demokraciju. Nadalje, s obzirom na kapacitete nadzora najvećih obavještajnih službi kao i na moć najvećih internetskih tvrtki postavlja se pitanje suvereniteta brojnih država koje zbog prirode same tehnologije nisu ni u

mogućnosti osigurati pravo na privatnost svojim građanima. Konačno, pitanje mogućnosti svojevoljnog odricanja prava na privatnost temeljno je za ovaj rad te će njemu biti posvećena posebna pažnja. No, potrebno je početi od značaja i vrijednosti prava na privatnost.

3.2. Pravo na privatnost

Pravo na privatnost „jasno je i nedvojbeno utemeljeno kao temeljno ljudsko pravo vrijedno zaštite“ (Michael, 1994: 1). Kao takvo prepoznato je u brojnim međunarodnim deklaracijama, poveljama, paktima, rezolucijama, ali i u nacionalnim ustavima većine svjetskih država. Vjerojatno najznačajniji dokument kojim se štiti pravo na privatnost jest upravo Opća deklaracija o pravima čovjeka u kojoj se u članku 12. eksplicitno navodi kako „Nitko ne smije biti izvrgnut samovoljnom miješanju u svoj privatni život, obitelj, dom ili dopisivanje, niti napadajima na svoju čast i ugled. Svatko ima pravo na zaštitu zakona protiv takvog miješanja ili napada“ (United Nations, 1948: 1). Činjenica kako je privatnost zaštićena zasebnim člankom u Općoj deklaraciji UN-a već sama po sebi govori o njezinom značaju, a formulacija članka samo dodatno potvrđuje značaj koji je privatnosti dan u tom temeljnom dokumentu. Važnost prava na privatnost kasnije je dodatno potvrđena tako što je ono uvršteno u Međunarodni pakt o građanskim i političkim pravima kroz članak 17. uz nešto izmijenjen tekst „Nitko ne smije biti podvrgnut samovoljnom *ili nezakonitom* miješanju u njegov privatni život, obitelj ili dopisivanje, niti *nezakonitim* napadima na njegovu čast ili ugled. Svatko ima pravo na pravnu zaštitu protiv takvog miješanja ili napada“ (Opća skupština Ujedinjenih naroda, 1966). Radi se o dva temeljna i univerzalno prihvaćena dokumenta kojima se opisuju temeljna ljudska prava. Posebni izvjestitelj za promociju i zaštitu ljudskih prava i temeljnih sloboda za vrijeme borbe protiv terorizma Ben Emmerson istaknuo je Međunarodni pakt o građanskim i političkim pravima kao „najvažniji pravno obvezujući dokument koji osigurava pravo na privatnost na univerzalnoj razini“ (United Nations, 2014: 11). Međutim, unatoč tome što pravo na privatnost ima istaknuto mjesto u temeljnim međunarodnim poveljama o ljudskim pravima, ono je bilo uvelike zapostavljeno od strane mehanizama za zaštitu ljudskih prava Ujedinjenih naroda od 1989. godine pa sve do 2009. godine, kada je tek posredno istaknuto u izvješću posebnog izvjestitelja za borbu protiv terorizma i ljudska prava (Nyst i Falchetta, 2017). Uz iznimku vrlo značajnog izvješća Posebnog izvjestitelja za promicanje i zaštitu prava na slobodu mišljenja i izražavanja Franka La Ruea, koji je istaknuo pravo na „privatnost kao temeljnu pretpostavku prava na slobodu izražavanja“ (United Nations, 2013a: 7), zapravo je tek nakon Snowdenovih

objava pravo na privatnost vraćeno u središte interesa Ujedinjenih naroda te je samo nekoliko mjeseci nakon Snowdenovih objava na Općoj skupštini izglasana prva rezolucija o Pravu na privatnost u digitalno doba (United Nations, 2013b), a već godinu kasnije uslijedila je i druga istoimena rezolucija (United Nations, 2014c) kojima je istaknut značaj prava na privatnost, naglašeno je kako osim država i tvrtke imaju obvezu poštivati pravo na privatnost te je izražena duboka zabrinutost zbog negativnog utjecaja koji masovni nadzor komunikacija i prikupljanje osobnih podataka ima na ljudska prava. Osim toga, UN-ov Odbor za ljudska prava pokrenuo je čitav niz aktivnosti vezanih uz zaštitu i nadzor nad ugrožavanjem prava na privatnost, a 2015. godine s radom je započeo i Posebni izvjestitelj za pravo na privatnost Joseph A. Cannataci koji je već podnio nekoliko izvješća o radu u kojima je izuzetno dobro prepoznao ključne probleme i dao je vrlo konkretne naputke za bolju zaštitu prava na privatnost (United Nations, 2016, 2017).

Kao što se može vidjeti iz temeljnih dokumenata o ljudskim pravima, pravo na privatnost nedvojbeno je prepoznato kao zasebno i temeljno ljudsko pravo. Pogledamo li osnovnu razliku između sadržaja članka 12. Opće deklaracije i članka 17. Međunarodnog pakta, možemo vidjeti kako je u odnosu na Opću deklaraciju u Međunarodnom paktu na dva mjesta dodana formulacija „ili nezakonitom“ čime se jasno sugerira kako dopušteno zakonito miješanje u privatni život i/ili napad na ugled ili čast. S obzirom na sveprisutne ugroze privatnosti, iz današnje perspektive vjerojatno je samorazumljivo kako pravo na privatnost nije apsolutno pravo, odnosno kako ga je moguće pod određenim zakonskim uvjetima ograničiti. Unatoč tome što članak 17. ne propisuje uvjete u kojima se pravo na privatnost može zakonito ograničiti, oni su detaljno opisani i taksativno nabrojani u Principima za ograničavanje odredbi Međunarodnog pakta o građanskim i političkim pravima iz Sirakuze (“The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights,” 1985). Prema tom dokumentu, *zakonito ograničavanje* prava na privatnost podrazumijeva ono utemeljeno na nacionalnom zakonodavstvu koje mora biti javno objavljeno, jasno napisano, mora biti doneseno u demokratskom postupku te i samo mora udovoljavati ostalim odredbama i ciljevima Pakta. To znači da zakonsko reguliranje ograničavanja privatnosti samo po sebi nije dovoljno već je nužno da ono udovoljava navedenim uvjetima. Prema tumačenju Ureda UN-ova Visokog povjerenika za ljudska prava o pravu na privatnost u digitalnom dobu, pozivajući se na tumačenja Odbora za ljudska prava UN-a te na spomenute Principe iz Sirakuze za ograničavanje odredbi Međunarodnog pakta, izbjegavanje *samovoljnog*

miješanja podrazumijeva ograničavanje nečijeg prava na privatnost samo u onim slučajevima kada je to razumno u zadanim uvjetima, a što Odbor preciznije tumači tako da svako uplitanje u privatnost mora biti proporcionalnu cilju koji se želi postići te mora u svakom pojedinom slučaju predstavljati nužnu mjeru koju se ne može izbjeći. Nadalje, kako bi ograničavanje prava na privatnost bilo u skladu s Paktom, ono smije biti ograničeno tek kao najmanje intruzivna mjera kojom se može postići željeni cilj, mora postojati barem određena vjerojatnost da će ukidanje prava dovesti do postizanja željenog legitimnog cilja te procjena i konačna odluka o tome mora biti donesena zasebno za svaki slučaj ograničavanja prava (United Nations, 2014d: 8–9). Tek ispunjavanjem ovih uvjeta može se ograničiti pravo na privatnost, a da bi i dalje bili zadovoljeni standardi zaštite ljudskih prava iz Međunarodnoga pakta. Bilo koji slučaj ograničavanja prava na privatnost koji prethodno ne bi uvažio navedene uvjete predstavljao bi kršenje međunarodnoga prava.

Samo dvije godine nakon usvajanja Opće deklaracije o pravima čovjeka, 1950. godine Europsko vijeće donijelo je Europsku konvenciju o zaštiti ljudskih prava i temeljnih sloboda, koja u članku 8. prepoznaje pravo na privatnost kao pravo na privatni i obiteljski život „(1) Svatko ima pravo na poštovanje svoga privatnog i obiteljskog života, doma i dopisivanja. (2) Javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih.“ (Council of Europe, 1950). Unatoč tome što odredbe same konvencije ne razrađuju detaljno samo pitanje zaštite privatnosti pojedinca te da su navedeni prilično široki izuzeci od zaštite prava, očito je kako je „Konvencija pokušala u najširem smislu obuhvatiti generalno pravo na privatnost pojedinca kao jedno od temeljnih ljudskih prava“ (Klarić, 2016: 989). Konvenciju se smatra najstarijim i najučinkovitijim sustavom za zaštitu ljudskih prava u svijetu (Marochini, 2014), a njome je osnovan i Europski sud za ljudska prava. Republika Hrvatska konvenciju je potpisala 1996. godine i ratificirala 1997. godine čime je preuzela sve obveze koje iz nje proizlaze, a time i poštivanje odluka Europskoga suda. Presuda Suda u slučaju *Liberty vs. UK* nedvojbena je potvrda kako Sud masovni nadzor komunikacija koji nije temeljen na procjeni reciprociteta za svaki pojedini slučaj smatra kršenjem članka 8. Konvencije (European Court of Human Rights, 2008).

Govoreći o Europskoj uniji, 2000. godine donesena je Povelja Europske unije o temeljnim pravima koja je stupanjem na snagu Lisabonskog ugovora 2009. godine postala dio pravne

stečevine EU i pravno obvezujuća za sve institucije EU i nacionalne vlade država članica EU. Sama povelja u skladu je s Europskom konvencijom o zaštiti ljudskih prava i temeljnih sloboda, a budući da je pisana čak 50 godina kasnije, obuhvaća i dodatna prava koja proizlaze iz sudske prakse Suda pravde EU, određena prava i principe koji proizlaze iz tradicija nacionalnih ustavnih tradicija i međunarodnih instrumenata kao i takozvanu *treću generaciju temeljnih prava i sloboda* u koje spadaju pitanja zaštite podataka, bioetike i transparentne administracije (EU, 2012). Konkretno, zaštita prava na privatnost regulirana je člankom 7. „Svatko ima pravo na poštovanje svojeg privatnog i obiteljskog života, doma i komuniciranja." te u širem smislu i člankom 8. koji govori o zaštiti osobnih podataka. Preciznija zaštita i regulacija prava koje proizlaze iz tih dvaju članaka osigurana je dvjema direktivama i to članka 7. Direktive o privatnosti i elektroničkim komunikacijama (Europski parlament i Vijeće Europske unije, 2002), i članka 8. Direktive o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka (Europski parlament i Vijeće Europske unije, 2016a). Početkom 2012. godine Europska komisija započela je reformu legislative za zaštitu podataka kako bi se Europa pripremila za digitalno doba, a to je rezultiralo donošenjem nove Direktive o zaštiti osobnih podataka 2016. godine kao i brojne regulative relevantne za pitanja prikupljanja, obrade i dijeljenja osobnih podataka, osobito u razmjeni s tvrtkama i institucijama izvan EU. Nakon Snowdenovih objava pristupilo se i ažuriranju Direktive o privatnosti i elektroničkim komunikacijama tzv. E-direktive čiji bi prijedlog trebao donijeti značajne mjere u dodatnoj zaštiti privatnosti unutar EU. Unatoč vrlo snažnom lobiranju protiv njezina donošenja i za ublažavanjem mjera kojima se štiti privatnost, krajem listopada 2017. godine prijedlog E-direktive usvojen je na Odboru za građanske slobode, pravosuđe i unutarnje poslove Europskoga parlamenta te je upućen na glasanje na plenarnu sjednicu. Izglasavanje E-direktive od strane Europskoga parlamenta, zajedno s komplementarnom i modernom Direktivom o zaštiti osobnih podataka iz 2016. godine, pružilo bi sveobuhvatnu i visoku razinu zaštite prava na privatnost u EU koja bi bila u skladu s aktualnim izazovima i modernim tehnologijama.

Pravo na privatnost prepoznato je, manje ili više eksplicitno, u gotovo svim ustavima liberalnih demokracija, a njih prate i nacionalni zakoni koji na različite načine osiguravaju pravo na privatnost. Republika Hrvatska nije izuzetak te je ratificirala i potpisnica je ranije spomenutih temeljnih dokumenata. Ustav Republike Hrvatske ne prepoznaje pravo na privatnost i u tom

smislu u Ustavu RH privatnost nema status koji joj je osiguran u ranije spomenutim međunarodnim dokumentima. Doduše, člankom 34. Ustava RH jamči se nepovredivost doma, člankom 36. sloboda i tajnost dopisivanja i svih drugih oblika općenja, člankom 37. jamči se sigurnost i tajnost osobnih podataka, a člankom 38. sloboda mišljenja i izražavanja misli *(Ustav Republike Hrvatske, 1990),* što su slobode koje imaju značajna preklapanja s pravom na privatnosti, ali ne obuhvaćaju pojam i smisao privatnosti u njezinoj cijelosti. U Hrvatskoj je privatnost posredno zaštićena u zakonima kojima se uređuje zaštita osobnih podataka, pitanja informacijske sigurnosti, ali i kojima se uređuju poslovi i ovlasti službi iz obavještajnog i represivnog sustava. No, vjerojatno najviši stupanj pravne zaštite privatnosti u pravnom sustavu RH osigurava glava četrnaesta Kaznenog zakona RH koja govori o kaznenim djelima protiv privatnosti. U njoj su pobrojana kaznena djela poput povrede tajnosti pisama, neovlaštenog prisluškivanja, nedozvoljene uporabe osobnih podataka i neovlaštenog otkrivanja profesionalne tajne (*Kazneni zakon*, 2011).

Unatoč značaju spomenutih temeljnih dokumenata o ljudskim pravima te međunarodnom ugledu i utjecaju međunarodnih organizacija poput Ujedinjenih naroda i Vijeća Europe put od deklarativne zaštite do *de facto* osiguravanja prava na privatnost dug je i pun prepreka. S druge strane, Europska unija posjeduje znatno konkretnije institucionalne mehanizme kojima može osigurati provođenje svoje legislative, no katkada su i njezine institucije potpuno nemoćne pred nacionalnim tijelima država članica koji uporno ignoriraju i krše direktive ili čak povelje. Bilo kako bilo, nema nikakve dvojbe da u ključnim međunarodnim dokumentima o ljudskim pravima, ali i brojnim nacionalnim ustavima i zakonima, pravo na privatnost uživa visoku razinu zaštite. Kao što je već nekoliko puta naglašeno, takav status privatnost je zaslužila upravo zbog svojeg značaja za ljudsko dostojanstvo, što je jedan od temelja svih drugih ljudskih prava, ali i zbog svojeg značaja za demokraciju.

3.3. Obrana prava na privatnost

Nakon što smo utvrdili kako se u relevantnim međunarodnim dokumentima pravo na privatnost smatra temeljnim ljudskim pravom, napustit ćemo pravnu analizu budući da ona, s obzirom na prirodu ovog rada, izlazi izvan njegova dosega. Međutim, ljudska prava osim pravne imaju izražene i snažne političke, filozofske, sociološke, psihološke i općenito društvene implikacije te ih se stoga proučava i u tim disciplinama. Centralno ovom radu jest pitanje obrane prava na privatnost, odnosno pitanje što pravo na privatnost čini temeljnim ljudskim pravom.

Pritom postoje dvije ključne linije argumentacije u obrani prava, *instrumentalna* i *intrinzična*. Instrumentalna obrana vrijednosti prava proizlazi iz njegove korisne funkcije kako bi se njime nešto postiglo, osiguralo, doseglo. Pravo koje ima isključivo instrumentalnu vrijednost, bez svojeg cilja postaje potpuno bezvrijedno. Na primjer, novac ima instrumentalnu vrijednost budući da njime možemo kupiti razna dobra, ali jednom kada novac više ne bismo mogli koristiti kako bismo nešto kupili, on bi izgubio svoju instrumentalnu vrijednost i postao bi gotovo sasvim bezvrijedan. Dio vrijednosti tog papira vjerojatno bi ostao u vidu instrumentalne vrijednosti za ogrjev, recikliranje i slično, ali instrumentalna vrijednost novca bila bi svedena na instrumentalnu vrijednost papira, tkanine ili metala od kojeg je izrađen. S druge strane, osim instrumentalne, pravo može imati i intrinzičnu, supstancijalnu, vrijednost. Ono može biti vrijedno samo po sebi. Može biti vrijedno zbog toga što ga imaju svi ljudi i neodvojivo je vezano za pojedine karakteristike koje su samo ljudske poput dostojanstva, kapaciteta za samoodređenjem ili sposobnosti donošenja autonomnih odluka (Francis i Francis, 2017). Kada govorimo o pravu na privatnost, ono istovremeno ima i instrumentalni značaj i krucijalnu supstancijalnu vrijednost. Oba značaja prava na privatnost imaju svoju vrijednost kako za pojedince tako i za društvo u širem smislu. Činjenica da je privatnost uvrštena i u Opću deklaraciju o pravima čovjeka, ali i u Međunarodni pakt o građanskim i političkim pravima govori kako pravo na privatnost ima trojaki značaj, kao temeljno ljudsko pravo, kao političko pravo i kao građansko pravo.

Zaštita privatnosti za pojedinca ima mnoge instrumentalne vrijednosti. Činjenica da sami možemo odrediti kome ćemo što reći o sebi i na koji način, pomaže nam razviti naš društveni i ekonomski status, a doprinosi i našoj neposrednoj sigurnosti. Upravljanje pristupom podacima o našem mentalnom zdravlju, financijskom stanju, spolnoj orijentaciji, tegobama i brigama za nas ima direktne koristi. Kada bi naše misli i osjećaji bili u potpunosti transparentni prema javnosti, gotovo je sigurno kako bi bila veća mogućnost da postanemo žrtva nasilja, društvenog odbacivanja, da nam netko otuđi vrijednost ili novac. Međutim, najznačajnija instrumentalna vrijednost privatnosti za pojedinca je ona za uspostavu i održavanje međuljudskih odnosa. Kao što je opširno opisano u prvom poglavlju, uvjerljiv je argument kojeg nude Fried (Fried, 1968) i Rachels (Rachels, 1975), a prema kojem bez privatnosti, bez mogućnosti reguliranja i upravljanja podacima o sebi, bez mogućnosti da neke misli, dojmove i uvjerenja zadržimo samo za sebe ili samo za uzak krug ljudi, jednostavno ne bismo mogli ostvarivati intimne odnose. I ne samo intimne odnose, već bilo koji međuljudski odnos. Time što ćemo s nekime odlučiti

podijeliti određene podatke te time koliko je taj podatak ekskluzivan upravljamo kvalitetom i razinom blizine odnosa s nekime. A to je moguće jedino uz uvažavanje naše privatnosti, jedino uz kontrolu toga s kime ćemo, kada, kako i što dijeliti, kome ćemo i pod kojim uvjetima omogućiti pristup (podacima o) sebi. Sasvim je izgledno kako se našem poslodavcu ne bi svidjelo kada bi znao sve što mislimo o njemu i o načinu na koji upravlja tvrtkom. Naša bi djeca vjerojatno znatno manje viđala svoju baku kada bi naša punica znala sve što smo ikada rekli ili pomislili o njoj. Mogućnost čuvanja intimnih podataka štiti našu *nepovredivu osobnost*. To što nam privatnost omogućuje kontrolu nad pristupom (podacima o) nama, stavlja nas u središte upravljanja našim životom. Mogućnost samostalnog i slobodnog donošenja odluka o tome s kime ćemo i što dijeliti neposredan je izraz vlastite autonomije.

Podsjetimo, utjecajni američki pravnici i suci Warren i Brandeis koji se smatraju začetnicima modernog poimanja privatnosti, u svojem su članku iz 1890. godine u privatnosti vidjeli nešto uzvišeno i povezano s *nepovredivom osobnosti* svakoga čovjeka (Warren i Brandeis, 1890). Time su dali naslutiti kako privatnost osim instrumentalne vrijednosti u sebi sadrži i nešto što je vrijedno zaštite samo po sebi. Nešto supstancijalno, bez čega bi svijet bio siromašnije mjesto. Bloustein je nepovredivu osobnost vidio kao termin koji predstavlja samostalnost pojedinca, njegovo dostojanstvo i integritet te ga definira kao samoodređujuće biće (Bloustein, 1984). I doista, pojedinac čije bi sve misli i osjećaji bili predmetom vanjske procjene ne bi bio slobodan, ne bi bio osoba. Privatnost je nužna kako bismo razvili osnovne socijalne odnose, ali i kako bismo izgradili vlastitu osobnost. Stalna izloženost i transparentnost u potpunosti bi otupila našu osobnost te bismo se stopili s masom. Društveni pritisak za poštivanjem pisanih i nepisanih društvenih normi toliko je snažan da bismo bez privatnosti, bez mogućnosti da barem nekada, barem negdje, barem s nekime podijelimo drugačiju misao, neprikladnu šalu ili revolucionarnu ideju, bili osuđeni na bezličnost. Osim toga, iz definicije privatnosti kao kontrole pristupa (podacima o) sebi proizlazi kako su upravo pojedinci ključan čimbenik u donošenju odluka o svojoj budućnosti. Uz to što je privatnost nužan temelj za razvoj samoodređenih i slobodnih pojedinaca, ona je istovremeno neodvojivo povezana sa slobodom i autonomijom. Privatnost stoga možemo smatrati ljudskim pravom zbog toga što je ona esencijalna za razvoj naše osobnosti, zaštitu našeg dostojanstva, osobnu autonomiju i temeljni identitet.

Nadalje, na razini društva, privatnost također ima i instrumentalnu i intrinzičnu vrijednost. Najznačajniju instrumentalna vrijednost privatnosti za društvo predstavlja njezin značaj za demokraciju. Vrlo plastična instrumentalna vrijednost privatnosti u demokratskom procesu je

značaj privatnosti za tajnost glasovanja (Lever, 2015). Naravno da tajnost glasanja sama po sebi nije nužan uvjet demokracije i moguće je zamisliti različite oblike političke participacije koji ne uključuju tajno izražavanje mišljenja. Ali zbog velikih razlika u društvenoj moći i utjecaju pojedinaca i interesnih skupina u svakom društvu, tek se tajnim glasanjem može osigurati slobodan izbor svakog pojedinca. Uostalom, za otvoreno izražavanje vlastitog mišljenja, osobito ako se radi o nepopularnom ili manjinskom mišljenju potrebno je mnogo samopouzdanja i snažna ličnost. A bez privatnosti, malo bi koji pojedinac uspio izrasti u samopouzdanog, stabilnog čovjeka snažna integriteta. Izglednije je kako bi i prije dobivanja mogućnosti javno izraziti svoje mišljenje, pojedinac odavno bio utopljen u mediokritetskom sivilu društva.

Pa tako možemo uvidjeti kako je osim važnosti privatnosti za mogućnost ravnopravnog i slobodnog sudjelovanja u demokratskom procesu, ona važna i za sam nastanak i razvoj nezavisne misli. U prvom poglavlju opširno su prikazane argumentacije autora poput Benna, Reimana, Blousteina, Gersteina, Gavison i Rössler koji upravo u tome vide važnost privatnosti. Bilo koja subverzivna misao zbog potpune transparentnosti bila bi vrlo brzo dovedena u liniju s poželjnom misli. Doduše, zbog snažnog socijalnog pritiska, zbog automatskog djelovanja moći, očigledne sveprisutnosti, ta bi ideja autocenzurom bila ugušena u trenutku njezina nastajanja. Ako bi uopće mogla nastati. Naime, društvo bez imalo privatnosti bilo bi sasvim drugačije od ovoga u kojem živimo. U Orwellovoj viziji takvog društva, malo tko je uopće imao kapacitet kako bi osiromašenim jezikom i pod utjecajem snažne propagande uspio zadržati svoj duh. Kako bi demokracija mogla biti realizirana, potrebno je građanima omogućiti slobodan tok informacija, sigurno mjesto za slobodnu i samostalnu evaluaciju tih informacija, slobodno udruživanje radi razmjene mišljenja, dojmova i kritika, i konačno, slobodu izražavanja vlastitog mišljenja i to bez uplitanja i nadzora (Francis i Francis, 2017). A kako bi to bilo moguće, privatnost je nužna ne samo kao preduvjet već i stoga što direktno osigurava realizaciju kroz izostanak nadzora i uplitanja. Kako je primijetila Hughes, instrumentalni značaj privatnosti za društvo najmanje je trojak. Najprije, kada govorimo o Orwellovoj distopiji, pravo na privatnost osigurava društvo od nastanka i razvoja totalitarizma. Drugo, privatnost omogućuje razvoj društva time što pojedincima osigurava „emocionalni i fizički prostor u kojem ideje mogu biti stvarane, razvijane i istraživane.“ I treće, mogućnost razvijanja međuljudskih odnosa različitih razina intimnosti pozitivno utječe na blagostanje i sreću, kao i na društvenu usklađenost (Hughes, 2015: 226).

Pozivajući se na Rawlsa i Milla, Lever tvrdi kako osim jasnog instrumentalnog značaja privatnosti za političku participaciju, međusobno udruživanje i otvoreno kritiziranje, „mogućnost samostalnog donošenja važnih odluka, uspostavljanja bliskih veza s drugima i slobodnog izražavanja bez straha od neželjene intruzije – sve su redom važni oblici osobne slobode“ (Lever, 2006: 23). I doista, mogućnost samostalne prosudbe i samostalnog djelovanja bez vanjskog uplitanja sastavni je dio osobne slobode. Teško je precizno razlučiti značaj privatnosti za pojedinca i za društvo budući da su te razine u velikom dijelu povezane. Ključni pojam koji povezuje individualnu i društvenu razinu, a koji je istovremeno povezan i s instrumentalnom i intrinzičnom vrijednosti jest autonomija. Kako navodi Johnson, „prema Kantu, autonomija nije tek jedna od mnogo vrijednosti; autonomija je fundamentalna za ono što znači biti čovjekom, za našu vrijednost kao ljudskih bića“ (Johnson, 2000: 437). Zbog toga će pojmu autonomije i njezinoj povezanosti s privatnosti biti dano nešto više prostora.

3.4. Autonomija

Instrumentalni značaj privatnosti za demokraciju dijelom proizlazi iz povezanosti demokracije i autonomije budući da se upravo „promoviranje i zaštita autonomije u liberalnoj misli smatra središnjom za pitanja slobode“ (Raz, 1986: 203), čime se istovremeno naznačuje i njezin intrinzični značaj. U smislu ovog, rada argumentacija će se prvenstveno temeljiti na perfekcionističko-liberalnoj koncepciji autonomije (Wall, 2012) kako je vidi Joseph Raz:

> Autonomna osoba je (djelomično) autor vlastitoga života. Svoj život djelomično kroji sama. Život autonomne osobe obilježen je ne samo onim što jest, već i onim što je mogla postati i načinom na koji je postala ono što jest. Osoba je autonomna samo ako ima različite prihvatljive opcije koje joj stoje na raspolaganju, a njezin je život postao onakav kakvim jest temeljem njezinih izbora tih opcija. (Raz, 1986: 204)

Svaki dio ovog citata ima svoj značaj pa ga je potrebno pojasniti. Ideja autonomne osobe kao *autora* vlastitoga života vrlo je slikovita za ilustriranje slobode i pojmu daje svojevrsnu širinu. Nadalje, Raz se u ovom citatu dotaknuo i još jednog važnog uvida. Autonomiju je moguće gledati kao *kapacitet*, potencijal osobe temeljen na njezinim karakteristikama kao i karakteristikama i okolnostima situacije i okruženja u kojem se našla, ali autonomiju je moguće gledati i kao dostignuće, već ostvaren cilj. To da je osoba *djelomično* autor odnosi se na to kako postoje određeni zadani uvjeti na koje osoba ne može utjecati, a to su njezine mentalne sposobnosti, odgovarajući raspon opcija koje ima na raspolaganju i neovisnost. Zaključno, Raz pruža uvid i u svoje temeljno pitanje, pitanje izbora. Za njega biti autor vlastitoga života znači

donositi odluke i odabirati opcije koje dovode do dobrog života. Pritom se sintagma *prihvatljive opcije* odnosi na to da izbori koje osoba ima na raspolaganju moraju biti smisleni, značajni i moraju dovoditi do pozitivnog ishoda (Raz, 1986). I ovdje za ilustraciju može dobro poslužiti kontrast između dvije znanstveno-fanstastične distopije, Orwellova romana *1984.* u kojem građani Eurazije nemaju na raspolaganju gotovo nikakve izbore i Huxleyeva *Vrlog novog svijeta* u kojem ljudi na raspolaganju imaju čitav niz izbora, a svih redom beznačajnih. Unatoč različitoj mogućnosti pristupa izboru, u oba romana ljudi su bez ikakve autonomije. I bez ikakve slobode.

3.4.1. Autonomija i društvo

„Privatnost se nalazi u samom srcu slobode moderne države“ (Westin, 1967: 350)

Osim evidentnog značaja autonomije za blagostanje i individualnu slobodu, najveći značaj Razove koncepcije autonomije jest u tome što on osim strogo individualnog i racionalnog pogleda na autonomiju vidi i njezin značaj za društvo, koji osim instrumentalne vrijednosti ima i intrinzičnu vrijednost za svakog pojedinog člana društva. Prema Razu, „ideal osobne autonomije nespojiv je s moralnim individualizmom“ (Raz, 1986: 206). Osim što svaki pojedinac želi imati osobnu autonomiju, njemu je ujedno u interesu da i ostali pojedinci u društvu u kojem živi imaju autonomiju. Što je pripadnicima pojedinog društva na raspolaganju više kvalitetnih izbora koje oni mogu informirano i nezavisno donijeti, to će to društvo biti naprednije i bolje. A to je u interesu i svakog pojedinog pripadnika tog društva. Što više karijera pojedinci mogu odabrati, to će društvo biti raznolikije, ali je i veća vjerojatnost da će ljudi biti bolji u svojim karijerama. Za Raza „javno je dobro da je ovo društvo tolerantno društvo, da je obrazovano društvo, da je u njega ugrađeno poštovanje prema ljudskim bićima itd. Živjeti u društvu s ovim karakteristikama općenito je korisno pojedinim članovima“ (Raz, 1986: 199). Pritom vrijedi naglasiti kako je ključna razlika između Raza i većine ostalih teoretičara morala u tome što za njega značaj autonomije kao javnog dobra osim instrumentalne vrijednosti ima i onu intrinzičnu. Za razliku od, recimo, prava na čist zrak koje ima očiglednu instrumentalnu vrijednost za svakog pojedinca u društvu, ostvarivanje visoke razine autonomije osim takve instrumentalne vrijednosti za svakog pojedinca posebno doprinosi i većem dobru.

Ovako postavljen koncept autonomije ne prepoznaje ljude samo kao individualne pojedince nego ih jasno stavlja u društveni kontekst. Bernal iz Razova pisanja izvlači povezanost autonomije i određenog oblika *društvene slobode*, prilike koju pojedinac ima da u potpunosti

djeluje u svim ključnim aspektima društva, bez ograničavanja i diskriminacije (Bernal, 2014). Radi se zapravo o mogućnosti slobodnog sudjelovanja u bilo kojem dijelu društva te o mogućnosti nezavisna i slobodna odabira načina i oblika te društvene aktivnosti. Konačno, budući da Raz autonomiju smatra moralno vrijednom, za njega je razumno da svaki pojedinac želi postići autonomiju te da želi i sve ostale učiniti autonomnima (Raz, 1986: 407). S obzirom da Raz na autonomiju prvenstveno gleda u terminima kapaciteta, on ne misli da je moguće druge učiniti autonomnima, ali je moguće doprinijeti okolnostima u kojima bi pojedinci mogli realizirati svoju autonomiju. Za Raza, učiniti nekoga autonomnim značilo bi stvoriti uvjete u kojima može slobodno odabrati između više prihvatljivih i smislenih opcija. Dakle, ne radi se samo o mogućnosti odabira, već i o postojanju različitih opcija. Izoliranje ljudi u društvene balone (eng. *Echo-chambers*), izlaganje samo sličnom sadržaju, kreiranje virtualne stvarnosti skrojene za svakoga posebno negativno utječe na autonomiju. U svijetu kakav kroje najveći internetski pružatelji usluga, ljudi bi zapravo subjektivno doživljavali autonomiju, ali njihovi izbori bili bi u velikoj mjeri predodređeni zbog snažne i suptilne manipulacije. Autonomija, kao mogućnost krojenja vlastita života kroz odabiranje između različitih smislenih opcija, snažno je povezana s osobnom slobodom. Na taj način istovremeno je važna i za svakog pojedinca, ali i za društvo u cjelini. Kada netko pojedincu zabrani govoriti, ugrozio je njegovu autonomiju i temeljno pravo na slobodu izražavanja. Međutim, kada građanin u demokratskom društvu ne smije govoriti, kada je stvoreno okruženje u kojem se pojedinci ne osjećaju slobodni govoriti, onda je ugrožena autonomija građana u tom društvu, što ima direktne posljedice na slobodu i demokraciju.

3.4.2. Autonomija i privatnost

O vrijednosti privatnosti za autonomiju i slobodu mnogo je napisano u prvom poglavlju. Definiramo li autonomiju kao mogućnost pojedinca da bude autor vlastitoga života, lako je vidjeti da je to gotovo nemoguće bez privatnosti, bez mogućnosti upravljanja pristupom (podacima o) sebi. Kako bismo mogli biti autori vlastita života kada bismo bili izloženi stalnom nadzoru, kada bismo bili lišeni mjesta na kojem smo slobodni od pogleda i dodira? To jednostavno nije moguće. Uostalom, sama mogućnost upravljanja bilo čime već podrazumijeva postojanje autonomije. Kako bi bilo moguće upravljati nečime, potrebno je imati mogućnost slobodnog odabira između različitih opcija. Nemoguće je imati privatnost bez autonomije. Ali nemoguće je imati i autonomiju bez privatnosti. Nemoguće je manifestirati slobodan izbor između različitih smislenih opcija bez slobode od nadziranja, praćenja i pristupa. U moralnoj i

političkoj filozofiji proučavanje koncepta autonomije centralno je za pitanja različitih prava i sloboda, među kojima se posebno izdvaja i pravo na privatnost (Christman, 2015). Jednostavno, „privatnost je ključni zaštitnik autonomije“ (Bernal, 2014: 2).

Helen Nissenbaum (2010) je u pregledu literature o privatnosti pronašla podršku za barem tri oblika odnosa autonomije i privatnosti. Prvi je konceptualni i prema njemu privatnost zapravo predstavlja jedan oblik autonomije. Takav odnos privatnosti i autonomije proizlazi iz njihovih definicija koje su korištene u ovom radu, a koje su naglašene u prethodnom odlomku. Privatnost omogućuje razvoj osobnosti i identiteta te omogućuje ljudima da iskuse i izraze vlastito samoodređenje. Kako se radi o sastavnim elementima mogućnosti krojenja vlastitog života, sastavnim elementima autonomije, možemo reći kako su privatnosti i autonomija u određenoj mjeri konceptualno isprepleteni. Drugi i treći pogled na odnos privatnosti i autonomije su kauzalni, odnosno privatnost se smatra pretečom autonomije, uvjetom bez kojeg nije moguće iskusiti punu autonomiju. Ključna razlika između drugog i trećeg pogleda je u sadržaju te kauzalnosti. Prema drugom pogledu, autonomiju nije moguće u potpunosti ostvariti zbog svojevrsne autocenzure, udovoljavanja (ne)pisanim društvenim normama, zbog *internaliziranja svojih motritelja* (Bentham, 1787; Foucault, 1995), a koje su posljedica nedostatka privatnosti. U prvom poglavlju opisana su četiri rizika kojima se izlažemo u slučaju da naši životi postanu u potpunosti vidljivi drugima (Reiman, 1995). Ono što Nissenbaum podrazumijeva pod drugim pogledom na vezu privatnosti i autonomije moguće je obuhvatiti pomoću dva Reinmanova rizika, *rizikom od ekstrinzičnog gubitka slobode* i *rizikom od intrinzičnog gubitka slobode*. Podsjetimo, radi se o obliku društvenog pritiska na pojedinca lišenog privatnosti kao posljedice izloženosti i transparentnosti prema društvu zbog čega pojedinac bilo svjesno, radi udovoljavanja pisanim i nepisanim društvenim normama i očekivanjima, prilagođava svoje ponašanje ili pak to čini nesvjesno, pritom internalizirajući očekivanja okoline.

I konačno, prema trećem obliku odnosa, autonomiju nije moguće u potpunosti ostvariti zbog ograničenih uvjeta u kojima se pojedinac nalazi, a sve zbog narušene privatnosti. Ovaj je odnos nešto kompleksniji nego prethodna dva, ali bazira se na vrlo uvjerljivom rezoniranju. Za ilustraciju Nissenbaum koristi primjer osobe koja bi željela postati odvjetnica, ali u njezinu društvu to nije omogućeno osobama iz njezine društvene skupine (Nissenbaum, 2010) bilo stoga što ne postoji škola za pravnike ili joj je trošak školovanja ekonomski nedostupan ili nešto treće. Primijenimo li Razov koncept autonomije, prema kojem postoje određeni zadani uvjeti

na koje osoba ne može utjecati koji utječu na to hoće li osoba imati autonomiju, na spomenuti primjer možemo lako vidjeti kako osoba suočena s ovakvim okolnostima zapravo nema na raspolaganju *prihvatljive* opcije, a time ni autonomiju. Manipuliranje ljudima, ali i njihovim okolnostima lišava ih njihove autonomije. Kako bismo vidjeli povezanost privatnosti i manipuliranja ljudima i njihovim okolnostima, prisjetimo se eksternih i internih ugroza privatnosti opisanih u drugom poglavlju. Prikupljanje izuzetno velikih količina podataka o nama, stvaranje nevjerojatno preciznih psiholoških i bihevioralnih profila te korištenje tih podataka za krojenje našeg iskustva na društvenim mrežama, ali i za induciranje emocija, stvaranje potreba i upravljanje našim potrošačkim ponašanjem kao i utjecanje na naše političke preferencije nedvojbeno predstavlja vrlo jasan oblik manipulacije uvjetima i opcijama, što direktno potkopava našu autonomiju.

> Osoba koja nikad nije imala bilo kakav značajan izbor, ili ga nije bila svjesna, ili nikada nije iskusila izbor u značajnim pitanjima već je tek lebdjela kroz život nije autonomna osoba (Raz, 1986: 204).

3.5. Suočavanje teoretskih spoznaja o značaju i vrijednosti privatnosti s razmjerima ugroza privatnosti

Razvoj tehnologije i novi sigurnosni izazovi doveli su do pojave eksternih i internih ugroza privatnosti, opisanih u drugom poglavlju. Jedno od temeljnih pitanja ove disertacije jest jesu li i na koji način novonastali uvjeti utjecali na transformaciju pojma privatnosti. Je li zbog pojave novih tehnologija, redefinicije komunikacije kakvu poznajemo te asimetričnih sigurnosnih prijetnji pojam privatnosti transformiran u temeljnim međunarodnim dokumentima, poveljama i paktima, nacionalnim ustavima i zakonima? Gledaju li međunarodni autoriteti iz područja ljudskih prava, nacionalne vlade, (multinacionalne) kompanije i građani na privatnost i potrebu za njezinom zaštitom drugačije nego što je to bilo ranije? Kako bismo odgovorili na ova pitanja potrebno je primijeniti opisane teoretske spoznaje o privatnosti kao i postojeću međunarodnu legislativu na konkretne slučajeve eksternih i internih ugroza opisane u prethodnom poglavlju.

3.5.1. Eksterne ugroze

Za potrebe ovog rada ugroze privatnosti grupirane su u dvije grube skupine prema tome događaju li se one protiv volje pojedinca, odnosno bez njihova znanja. Pa tako eksterne ugroze načelno predstavljaju one oblike narušavanja privatnosti koji se odvijaju bez znanja pojedinaca i/ili protiv njihove volje. Unatoč tome što postoji čitav niz intruzija u nečiju privatnost koje bi

mogle biti shvaćene kao eksterne ugroze, fokus ovog rada usmjeren je na one koje su direktna posljedica upravo razvoja tehnologije i novih sigurnosnih izazova, a kojima se ujedno i na vrlo značajan način ugrožava privatnost. Konkretno, u drugom poglavlju kroz niz primjera opisano je nekritičko prikupljanje podataka od strane nekoliko najsnažnijih svjetskih obavještajnih službi te je kroz niz primjera opisano njihovo nastojanje razbijanja, oslabljivanja i ograničavanja učinkovite i snažne enkripcije.

3.5.1.1. Nekritičko prikupljanje podataka

Pod nekritičkim prikupljanjem podataka prvenstveno se smatra masovno prikupljanje podataka poput prisluškivanja svog prometa koji prolazi interkontinentalnim podvodnim optičkim kablovima, te poput programa PRISM i MUSCULAR kojima su s poslužitelja najvećih internetskih tvrtki, uz njihovo znanje ili bez njega, prikupljane enormne količine podataka o korisnicima gotovo iz cijeloga svijeta. Pojedine države danas imaju mogućnost osigurati pristup nezamislivoj količini sirovih podataka koji se prikupljaju naveliko. Automatizirani algoritmi naknadno se koriste za pregledavanje takvih baza podataka, za strukturiranje podataka, za povezivanje i ukrštavanje podataka s podacima iz ostalih javnih ili tajnih baza podataka kako bi se uočile pravilnosti. Držimo li se definicije privatnosti koja je opisuje u terminima kontrole pristupa (podacima o) sebi, ovakav oblik masovnog nadzora nedvojbeno predstavlja zadiranje u privatnost. I oko toga se svi slažu. Nekim građanima to smeta više, nekima smeta manje, ali postoji vrlo visok konsenzus oko toga kako masovni nadzor podataka predstavlja ugrožavanje privatnosti.

Vrijedi istaknuti kako pravo na privatnost nije apsolutno pravo već je ono u svim važnijim međunarodnim dokumentima zagarantirano uz određena ograničenja kojima se predviđaju uvjeti za suspenziju prava na privatnost. Kao što je ranije i opisano, Odbor za ljudska prava UN-a te Principi za ograničavanje odredbi Međunarodnog pakta o građanskim i političkim pravima iz Sirakuze preciznije tumače te uvjete. Pa tako se očekuje da bilo kakvo ograničavanje prava bude utemeljeno na jasnim i demokratski donesenim zakonima te da se ono ograničava tek kao najmanje intruzivna mjera kojom se može postići željeni cilj. Osim toga, mora postojati barem određena vjerojatnost da će ukidanje prava dovesti do postizanja željenog legitimnog cilja te procjena i konačna odluka o tome mora biti donesena zasebno za svaki slučaj ograničavanja prava.

Primijenimo li ove standarde na razmjere nadzora opisane u drugom poglavlju lako je zaključiti kako su oni protivni međunarodnome pravu, a to je nedvojbeno zaključeno i u više različitih izvješća UN-ovih posebnih izvjestitelja za ljudska prava (United Nations, 2014a, 2014c, 2017). Prema njihovim izvješćima, borba protiv terorizma može se smatrati se legitimnim ciljem u čiju bi svrhu ograničavanje prava na privatnost moglo biti opravdano, no države koje primjenjuju masovni nadzor telekomunikacija, ugrožavaju enkripciju, koriste računalne napade na korisničke uređaje i nekritički prikupljaju podatke o korisnicima od privatnih tvrtki, nisu do sada jasno obrazložile svoj cilj, nisu transparentno napravile test proporcionalnosti i nužnosti primjene baš tih mjera kao onih koje najmanje zadiru u ljudska prava. „Međunarodni pravni dokumenti o ljudskim pravima nalažu državama da pruže argumentirana i na dokazima utemeljena opravdanja za bilo koje zadiranje u pravo na privatnost bilo na individualnoj ili masovnoj razini“ (United Nations, 2014b: 5). Dakako, *masovni* nadzor komunikacija po samoj definiciji nije i ne može ni uz najbolju volju biti opravdan na temelju procjene za svaki *pojedini slučaj* te je samim time taj oblik nadzora nespojiv s člankom 17. Međunarodnog pakta.

Doduše, Posebni izvjestitelj za promociju i zaštitu ljudskih prava i temeljnih sloboda za vrijeme borbe protiv terorizma Ben Emmerson u svojoj interpretaciji dopustio je kao teoretsku mogućnost čak i primjenu masovnog nadzora pod uvjetom da države koje ga primjenjuju javnosti pruže smislene i opipljive prednosti njegove primjene kao i da metodologija takvog nadzora bude transparentna i utemeljena na jasnim i demokratski donesenim zakonima (United Nations, 2014b). Međutim, budući da države koje su uključene u masovni nadzor do sada nisu uspjele pružiti javnosti opravdanje za njegovu primjenu utemeljeno na dokazima te da gotovo nijedna od tih država nema u nacionalnom zakonodavstvu jasnu legislativu koja omogućuje takav nadzor, Posebni izvjestitelj Emmerson zaključio je kako „tehnologija masovnog nadzora značajno ugrožava privatnost na internetu te podriva samu bit prava zajamčenog člankom 17. Međunarodnog pakta. Bez jasnog i formalnog odrješenja države od njezinih obveza prema Međunarodnome paktu, programi masovnog nadzora predstavljaju direktan i perzistentan izazov uspostavljenoj vladavini međunarodnoga prava“ (United Nations, 2014b: 21). Iza ove formulacije napisane jezikom diplomacije krije se vrlo oštra kritika upućena državama koje provode masovni nadzor komunikacija bez jasnog i demokratski donesenog zakonski reguliranog opravdanja i utemeljenja kako je propisano Principima za ograničavanje odredbi Međunarodnog pakta o građanskim i političkim pravima iz Sirakuze.

Kao što je već u više navrata naglašeno, represivni aparat ne samo da ima legitimitet provođenja nadzora te da ima monopol na primjenu sile, nego mu je upravo to i svrha. No, svaka država koja je utemeljena na poštivanju temeljnih ljudskih prava i sloboda, svaka liberalna demokracija, obvezala se ograničiti doseg represivnog aparata te uvjete za postupanje jasno propisati. Jedan od osnovnih temelja za primjenu bilo kakvog postupanja kojim se ugrožavaju temeljna ljudska prava građana jest postojanje sumnje nad određenim pojedincem ili organizacijom, a čiju opravdanost procjenjuju nezavisna tijela, idealno sud. Međutim, kod masovnog nadzora ne postoji prethodna sumnja, već se ona utvrđuje *post festum*. Takav oblik nadzora ne predstavlja proporcionalno ugrožavanje prava na privatnost s obzirom na prijetnju te nipošto ne predstavlja najmanje intruzivnu mjeru kojom se može postići cilj budući da konkretni pojedinac u trenutku primjene nadzora i u trenutku narušavanja njegove privatnosti uopće nije poznat, a kamoli da je inkriminiran, što su nužni preduvjeti za bilo kakvu odluku o reciprocitetnom ograničavanju njegovih prava.

Govoreći o masovnom nadzoru poseban problem predstavlja i drugačije tretiranje vlastitih državljana u odnosu na strance i/ili osobe koje se nalaze izvan teritorija države koja primjenjuje nadzor. Takva praksa, uobičajena za obavještajne službe diljem svijeta, diskriminirajuća je i nije kompatibilna s člankom 26. Međunarodnoga pakta. Sjedinjene Američke Države, kao država koja najopsežnije primjenjuje masovni nadzor telekomunikacija, a koji posebno i neproporcionalno pogađa osobe koje se nalaze izvan teritorija SAD-a te nisu državljani SAD-a, Odbor za ljudska prava UN-a nedvosmisleno je opomenuo zbog diskriminirajućeg odnosa prema strancima u pogledu svojih obavještajnih aktivnosti (United Nations, 2014a). Naime, trenutna obavještajna metodologija SAD-a, a osobito masovni međunarodni nadzor komunikacija osobama koje su predmet tog nadzora ne omogućuje pristup zakonodavstvu temeljem kojeg se njihova ljudska prava ugrožavaju zbog čega nerijetko nisu ni svjesni mogućnosti da bi mogli biti predmet nadzora. Ovime se otvara i pitanje narušavanja suvereniteta nacionalnih država čiji se građani nadziru i koje nemaju mogućnosti to spriječiti i zaštiti njihova prava, o kojemu će biti više riječi nešto kasnije.

Reperkusije ovakvog masovnog nadzora na autonomiju pojedinaca najlakše je razumjeti pomoću metafore panoptikona. Privatnost nam osigurava štit od stalnog procjenjivanja, odobravanja i neodobravanja drugih. Poput Benthamove *očigledne sveprisutnosti* ili Foucaultova *sveprisutnog nadzora*, nikada ne znamo promatraju li nas moćne obavještajne službe, ali znamo kako u svakom trenutku to mogu činiti. Udovoljavanje društvenim normama,

strah od progona ili jednostavno nelagoda zbog osjećaja promatranosti utječu na našu percepciju vlastite autonomije i čine nas manje slobodnima kada vjerujemo da smo pod nadzorom ili da bismo mogli biti pod nadzorom. Zbog masovnog nadzora postajemo manje slobodni, što ima posljedice i na nas kao pojedince, ali u isto vrijeme ima negativne posljedice i na društvo u kojem živimo. Uostalom, budući da je privatnost zaštićena kao temeljno ljudsko pravo te da postoji uvjerljiva supstancijalna obrana intrinzične vrijednosti prava na privatnost, ugrožavanje tog prava neprihvatljivo je u državama utemeljenima na vladavini prava i temeljnim ljudskih slobodama.

> Rasprostranjeni nadzor te agregiranje i analiziranje podataka jačaju utjecaj koji moćni akteri, kao što su vladine agencije, trgovci i potencijalni poslodavci, mogu imati u oblikovanju ljudskih izbora i djelovanja. (Nissenbaum, 2010: 83)

3.5.1.2. Podmetanje noge sigurnosti: pokušaji narušavanja i zaobilaženja enkripcije

Osim nekritičkog masovnog nadzora, kao drugi primjer aktualnog i značajnog ugrožavanja privatnosti koje je posljedica upravo razvoja tehnologije i novih sigurnosnih izazova, prikazano je nastojanje represivnih i obavještajnih službi za razbijanjem, oslabljivanjem i ograničavanjem učinkovite i snažne enkripcije lako dostupne svima. Razumljivo je da represivni sustav želi pristupiti što većem broju podataka o osobama za koje postoji sumnja da su počinile kazneno djelo ili planiraju na značajan način ugroziti sigurnost građana ili države. Zamislimo li primjer u kojem je na nepoznatoj lokaciji u Zagrebu postavljena eksplozivna naprava te je policija presrela elektroničku komunikaciju osoba koje su planirale taj teroristički napad, ali ona je kriptirana. Teško bi se mogla naći osoba koja u takvom scenariju ne bi poželjela da postoji način za otključavanje enkripcije u iznimnim i opravdanim situacijama. No, zbog tehnoloških razloga detaljnije objašnjenih u drugom poglavlju, enkripcija jednostavno ne može u istom trenutku biti nesigurna za *neke* osobe u *nekim* situacijama, a sigurna za sve ostale.

U izvješću Posebnog izvjestitelja UN-a o pravu na privatnost Josepha Cannatacija posebna pozornost posvećena je upravo pitanjima enkripcije s naglaskom na kontroverzni zakon *Investigatory Powers Act* (Her Majesty's Government, 2016) koji je u Velikoj Britaniji stupio na snagu u studenom 2016. godine. Posebni izvjestitelj je izjave ministara i drugih visokih dužnosnika o zagovaranju mogućnosti (selektivnog) ukidanja enkripcije vrlo oštro odbacio kao „besmislene", a izjave poput „*Policija i obavještajne službe moraju zadržati mogućnost zatražiti od telekomunikacijskih operatora da uklone enkripciju u ograničenim okolnostima*" nazvao je „iluzornima i dalekima od stvarnosti" (United Nations, 2016: 19). Unatoč tome što odredbe o ukidanju enkripcije iz toga zakona još do danas nisu upotrjebljene, zakon je u

Ujedinjenom Kraljevstvu na snazi i u bilo kojem trenutku moglo bi biti zatraženo od tvrtki koje posluju na teritoriju Ujedinjenog Kraljevstva da svoje poslovanje usklade sa zakonom. Za sve tvrtke koje su korisnicima omogućile *end-to-end* enkripciju to bi značilo ili odustajanje od takve enkripcije ili odlazak iz tržišta Ujedinjenog Kraljevstva. Istovremeno moćna *end-to-end* enkripcija ostala bi vrlo lako dostupna bilo kome tko bi je želio primijeniti za svoju komunikaciju s nekime bez obzira na usluge koje pružaju tvrtke usklađene sa zakonom. Izgledno je kako bi to rezultiralo time da bi velika većina građana imala sniženu raznu sigurnosti osobne komunikacije dok bi oni vještiji ili jako motivirani mogli relativno jednostavno i dalje koristiti u ovom trenutku praktički neprobojnu enkripciju.

Dakako, smanjenje razine enkripcije, njezino razbijanje čistom snagom ili zadržavanje tzv. privatnih ključeva od strane pojedinih tvrtki koje bi ih onda sukladno vlastitoj procjeni ili temeljem sudskog naloga mogle ustupiti trećoj strani demonstracija je aktivnosti države u kojoj nemamo kontrolu nad našim podacima. Koristimo li za telefonske razgovore SIM karticu čiji su enkripcijski privatni ključevi u posjedu pojedinih obavještajnih službi nemamo kontrolu nad podacima o sebi. Uspije li vrlo posvećena obavještajna služba čistom računalnom snagom razbiti pojedini enkripcijski protokol, nemamo kontrolu nad podacima koji kolaju tim protokolom. Isto vrijedi i za ostale oblike narušavanja ili ukidanja enkripcije detaljno opisane u drugom poglavlju.

Spoznaja o takvom djelovanju represivnog aparata i mogućnostima nadzora čini da, ukoliko želimo zadržati svoju privatnost, odnosno kontrolu nad podacima o sebi, izbjegavamo slobodno i otvoreno komunicirati putem kompromitiranih komunikacijskih kanala. Takvo ponašanje ponovo predstavlja oblik autocenzure svojstven panoptikonu, a posljedice na autonomiju očigledne su. Ukidanje ili ograničavanje enkripcije predstavlja „ograničenje anonimnosti koje ima zastrašujući učinak na slobodno izražavanje ideja i dijeljenje podataka“ (United Nations, 2013a: 13). Slobodno dijeljenje ideja i slobodno komuniciranje otežavaju se ili onemogućavaju se ne samo indirektno uz pomoć autocenzure, kao posljedice internaliziranja društvenih normi, internaliziranja motriteljevih namjera zbog rasprostranjenog nadzora i ograničavanja sigurne i dostupne enkripcije ,već i direktnim mjerama poput ograničavanja rada pojedinih aplikacija ili internetskih servisa i usluga. Takvim direktnim i indirektnim ograničavanjima stvara se svijet u kojem se *nemaš kamo sakriti*, u kojem je sve teže uopće osmisliti nešto autentično, nešto kreativno, nešto drugačije, a kamoli tu ideju kasnije i realizirati. Takvo ograničavanje autonomije ima nesagledive posljedice na dobrobit svakog pojedinca koji mu je podvrgnut.

Njegov potencijal za intelektualni rast ograničen je, kao što mu je bez slobodnog i neometanog dijeljenja ideja ograničena i mogućnost sklapanja i održavanja smislenih međuljudskih odnosa. Međutim, posljedice ovakvog narušavanja privatnosti imaju i posljedice na društvo. Društvo sputanih pojedinaca osuđeno je na propast, bilo da su sputani od intelektualnog razvoja, od kritičkog mišljenja, od međusobnog udruživanja. Demokracija podrazumijeva autonomne i slobodne pojedince i bez njih ju je nemoguće ostvariti.

3.5.2. Interne ugroze

Osim eksternih ugroza, za ilustriranje utjecaja razvoja tehnologije na transformaciju pojma privatnosti korištene su i tzv. interne ugroze privatnosti. Za razliku od eksternih ugroza koje karakteriziraju mjere kojima se privatnost ograničava bez znanja i/ili bez volje pojedinaca, kod internih ugroza radi se o prijetnjama privatnosti koje su posljedica svjesnog i namjernog djelovanja samih pojedinaca. Tako su u drugom poglavlju detaljno prikazane ugroze privatnosti koje su posljedica čestih i detaljnih objavljivanja na društvenim mrežama prvenstveno osobnih i intimnih podataka, fotografija, stavova, pripadnosti grupama. Nadalje, u eksterne ugroze spadaju i znatno manje očite ugroze koje proizlaze iz samog korištenja brojnih internetskih usluga kao što su servisi e-pošte, pohrane u oblaku, on-line rječnici, kalendari, rokovnici, navigacije ili jednostavno korištenje internetskih tražilica ili samo pretraživanje interneta. Iako je Internet, zbog same digitalne i umrežene prirode, posebno pogodan za prikupljanje podataka i praćenje korisnika, slično su već i znatno prije pojave interneta činile kartičarske kuće, banke, trgovine, knjižnice pa tako eksterne ugroze izvan internetskog okruženja postoje već desetljećima. Baze podataka različitih tvrtki i organizacija koje dobrovoljno punimo osobnim i intimnim podacima nisu nova pojava. No, Internet je zbog tehnologije na kojoj je baziran omogućio umrežavanje i dijeljenje tih podataka kakvo je još prije nekoliko desetaka godina spadalo u domenu znanstvene fantastike.

Činjenica da se radi o svjesnim i namjernim ugrozama privatnosti naizgled djeluje kao da se kod internih ugroza radi o svjesnom i namjernom odricanju privatnosti, no to nije uvijek slučaj. Unatoč brojnim upozorenjima i obveznom prihvaćanju politika privatnosti i uvjeta korištenja usluga, korisnici zapravo u mnogim slučajevima nisu svjesni što se točno događa s njihovim podacima i drugačije bi koristili usluge kada bi znali da se njihovi podaci dalje prodaju (Newton, 2017a) i koriste za manipuliranje njima samima. *Simbiotska mreža* (Bernal, 2014) ili *društvo izlaganja* (Harcourt, 2015), kako god nazvali novonastali odnos korisnika i internetskih

tvrtki u kojem korisnici u zamjenu za osobne podatke besplatno (ili povoljnije) dobivaju pristup različitim inače vrlo skupim uslugama, na površini predstavljaju sasvim legitiman poslovni model. Međutim, ispod površine kriju se brojne opasnosti detaljnije opisane u prošlom poglavlju. Precizno psihološko i bihevioralno profiliranje korisnika i prikupljanje enormnih količina podataka o njima tvrtkama omogućuje manipuliranje, diskriminiranje i raslojavanje društva.

3.5.2.1. Manipuliranje

U ovom kontekstu pojam manipuliranja obuhvaća širok raspon ponašanja koja imaju za cilj utjecanje na ponašanje pojedinca kako bi djelovao na način koji mu ne ide u korist. Bilo bi pretenciozno svaki oblik marketinga nazvati manipuliranjem, ali pojedini pojedinačno skrojeni oblici marketinga svakako imaju elemente manipulacije. Slično kao što su osamdesetih i devedesetih godina prošlog stoljeća putujući prodavači po kućama uspješno prodavali posuđe i kućanske aparate koji nam nisu nikada zatrebali ni prije ni poslije prezentacije i nesretne kupovine, tako nam se danas oglasi skrojeni samo za nas pojavljuju točno onda kada smo najskloniji podlegnuti njihovom utjecaju. Precizno profiliranje može doprinijeti i diskriminaciji na način da se pristup pojedinom sadržaju ili usluzi omogući samo određenim korisnicima ili, pak, da se cijena proizvoda na internetskim trgovinama formira ne samo prema kupovnoj moći pojedine osobe, nego i prema tome koliko ta osoba želi taj proizvod (Bernal, 2014). To može značiti kako će tinejdžerki koja ne ostvaruje nikakva primanja biti prikazana veća cijena određenih, među njezinim vršnjacima, vrlo popularnih cipela nego što će biti prikazana njezinoj majci, koja spada u skupinu kojoj takve cipele nisu zanimljive, ali si ih može s lakoćom priuštiti.

Internetske tražilice neke rezultate naših pretraga mogu učiniti težima za pronaći ili ih mogu potpuno sakriti. Pod posebnim povećalom je daleko najpopularnija tražilica na svijetu – Google. I s dobrim razlogom. Naime, Googleovo upravljanje rezultatima na štetu konkurenata koje su brojni korisnici i sami primijetili, potvrđeno je i u empirijskom istraživanju (Luca, Wu, Couvidat, Frank i Seltzer, 2015), a krajem lipnja 2017. godine Europska komisija kaznila je Google astronomskom kaznom od čak 2,42 milijarde eura za kršenje odredbi o zaštiti tržišnog natjecanja u EU upravo zbog iskorištavanja vlastite dominantne pozicije kao tražilice kako bi u rezultatima pretraživanja davao nelegalnu prednost vlastitim proizvodima u odnosu na konkurentske (European Commission, 2017). Google je rezultate koji su znatno više odgovarali traženom pojmu stavljao niže na listi rezultata ako se radilo o konkurentskim proizvodima. Osim što takva praksa narušava tržišno natjecanje, ona čini i to da se osobama koje pretražuju

određene pojmove prikazuju manje relevantni rezultati zbog čega oni mogu imati i osobne gubitke. U boljem slučaju mogu izgubiti više vremena u potrazi za relevantnijim rezultatom, a u gorem slučaju mogu završiti koristeći skuplji, lošiji ili manje odgovarajući proizvod od onoga koji su željeli.

U drugom poglavlju poseban naglasak stavljen je na mogućnosti korištenja preciznog profiliranja i velikih podataka za političku persuaziju, odnosno utjecaj na ishod izbora i referenduma ili jednostavno na krojenje javnog mnijenja. Osim toga, istaknut je i utjecaj profiliranja na krojenje jedinstvenog iskustva svakog korisnika koje rezultira pojačanim raslojavanjem i polarizacijom društva. Naime, pružateljima usluga na internetu cilj je zadržati korisnike što dulje uz male ekrane kako bi od njih prikupili što više podataka, a pokazalo se kako im je to najlakše učiniti manipuliranjem njihovim emocijama, što uključuje i prikazivanje polarizirajućeg sadržaja (Newton, 2017b). Upravo je to jedna od temeljnih ideja Cassa Sunsteina o kojoj je pisao u knjizi *Republic.com 2.0.* On je još 2007. godine, dok su se kapaciteti Googleova i Facebookova masovnog profiliranja tek zagrijavali, prepoznao kako internetski korisnici pokazuju tendenciju da ne koriste Internet kako bi lakše prikupili objektivne podatke o pojedinim kontroverznim pitanjima, već se svrstavaju u skupine istomišljenika gdje svoje unaprijed određene stavove i poglede još dodatno učvršćuju (Sunstein, 2007). Takvu tendenciju dodatno potpiruju i iskorištavaju velike internetske tvrtke ciljano nas stavljajući u društvene balone, izolirajući nas od drugoga i drugačijega te time polarizirajući internetsku stvarnost.

3.5.2.2. Kontrola (ni)je autonomija

Kod eksternih ugroza privatnosti, a osobito kod konkretnih primjera opisanih u ovom radu, nema nikakve dvojbe kako se radi o ugrozama privatnosti. Privatnost definirana u terminima kontrole pristupa (podacima o) sebi krši se nekritičkim masovnim nadzorom, ali i ciljanim napadima na enkripciju i digitalne komunikacije. Tim postupanjima ugrožena je i autonomija nadziranih pojedinaca, a zbog očigledne sveprisutnosti i svih onih koji samo misle da bi mogli biti nadzirani. Međutim, kod internih ugroza privatnosti odnos kontrole i autonomije nešto je kompleksniji.

Kod internih ugroza svjesno i namjerno predajemo kontrolu nad podacima o sebi u zamjenu za određene usluge ili za umrežavanje s drugima. Dio korisnika nije u potpunosti svjestan što točno predavanje kontrole nad njihovim podacima može značiti, i kada bi bili svjesni svega što se događa s njihovim podacima i toga što bi se moglo dogoditi na njihovu štetu kao posljedice

takvog predavanja kontrole, drugačije bi postupili (Newton, 2017a). Međutim, dobar dio korisnika svjestan je za što se sve njihovi podaci koriste i za što se sve mogu koristiti, no naprosto ih nije briga. Oni nemaju *ništa za sakriti*. Taj argument svojevrsna je mantra skeptika zaštite privatnosti, a najviše ga promoviraju oni koji imaju najveći interes u sprječavanju zaštite privatnosti, to jest obavještajne agencije i multinacionalne kompanije (Solove, 2007). Međutim, znakovito je kako sve više korisnika prihvaća taj argument i skeptični su prema zaštiti privatnosti. Ti korisnici imaju osjećaj kako predavanjem kontrole nad podacima o sebi, oni zadržavaju svoju autonomiju. Dapače, upravo je predavanje osobnih podataka za njih izraz osobne autonomije. I doista jest. Oni se slobodno odriču svoje privatnosti čime demonstriraju autonomiju. Međutim, to je problematično iz najmanje dva razloga.

Prvo, postoji određena iluzija da je Internet znatno zatvoreniji i bliži privatnom prostoru nego javnom prostoru. Općenito, postoji razlika u razini privatnosti koju pojedinci imaju i subjektivnoj percepciji privatnosti koju doživljavaju. Ljudi u javnom prostoru imaju tendenciju osjećati se nenadziranima i anonimnima (Dienlin, 2017) bez obzira na prisutnost nepoznatih ljudi i nadzornih kamera. Ta je razlika veća u internetskom okruženju gdje ljudi često imaju dojam veće privatnosti nego što je doista imaju (Trepte i Reinecke, 2011). Zbog takve pogrešne percepcije razine privatnosti, ljudi su skloniji otvoreno komunicirati i dijeliti intimne podatke (Boyd, 2008). Mnogi pojedinci će u komentarima na prijateljevu Facebook-zidu znatno slobodnije napisati pojedini komentar nego što bi ga bili spremni glasno izgovoriti na javnom mjestu, što pokazuju sve češći primjeri tzv. *Facebook uhićenja*, odnosno kaznenog ili prekršajnog procesuiranja pojedinaca zbog širenja mržnje, upućivanja prijetnji ili vrijeđanja putem interneta (Vlašić, 2017). Kod internih prijetnji privatnosti imamo dojam zadržavanja dijela kontrole i kontroliranog gubitka autonomije, no radi se o iluziji koja je posljedica nepoznavanja modernih tehnologija, računalnih, telekomunikacijskih i onih za nadzor i praćenje. „U međunarodnom pravu postoji opći princip prema kojem se pojedinci mogu odreći zaštite pojedinog ljudskog prava isključivo dobrovoljnim izražavanjem jasne i nedvojbene namjere utemeljene na informiranoj odluci. U modernom digitalnom svijetu puko korištenje interneta kao oblika privatne komunikacije ne može ni u kojem slučaju predstavljati odricanje od prava na privatnost zaštićenog člankom 17. Međunarodnog pakta o građanskim i političkim pravima.“ (United Nations, 2014b: 7). Takozvani *opt-out* sustav davanja suglasnosti prema kojem je zadani uvjet da se podaci prikupljaju dok pojedinac aktivno ne zatraži prestanak prikupljanja podataka o njemu nije u skladu s naputcima Ujedinjenih naroda. Jednostavno

korištenje određene usluge ne može se smatrati odricanjem prava na privatnost bez obzira na sadržaj uvjeta korištenja. Dok je *opt-out* sustav svojstven Sjevernoj Americi, u Europi se značajno više štiti osobne podatke te je na snazi takozvani *opt-in* sustav prema kojem pojedinac mora dati aktivnu suglasnost i privolu prije nego što se podaci o njemu počnu prikupljati. Stupanjem na snagu nove Uredbe o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (Europski parlament i Vijeće Europske unije, 2016b) tzv. *GDPR direktive* u svibnju 2018. godine razina zaštite osobnih podataka građana Europske unije značajno je porasla. Međutim, i dalje je na snazi opt-in sustav prema kojem pojedinci moraju dati jasan i eksplicitnu privolu za prikupljanje, obradu i analizu osobnih podataka. A s obzirom na to koliko olako ljudi daju pristanak za pristupom vlastitim podacima, od *GDPR direktive* ne treba očekivati previše. Osobito ako internetski divovi *ucijene* korisnike na način da im svoje primamljive usluge omoguće samo ako pristanu na odricanje od vlastite privatnosti.

I drugo, postoji ozbiljan problem s bilo kakvim, pa i kontroliranim, gubitkom autonomije zbog posljedica na društvo i demokratske procese i institucije. Naime, Razova koncepcija autonomije osim strogo individualnog i racionalnog pogleda na autonomiju vrednuje i njezin značaj za društvo. Predavanjem kontrole nad podacima o sebi moćnim internacionalnim oglašivačkim kompanijama ili obavještajnim službama, odnosno odricanjem od privatnosti, istovremeno se odričemo i vlastite autonomije čime narušavamo ne samo vlastitu slobodu nego i društvo u kojem živimo činimo manje slobodnim. Govoreći o povezanosti privatnosti i autonomije spomenuta su tri oblika odnosa koje je prepoznala Nissenbaum (2010). Prva dva oblika odnosa objašnjavaju očitu ugrozu autonomije kao posljedicu eksternih ugroza privatnosti, dok treći oblik odnosa objašnjava ugroze autonomije kao posljedicu internih ugroza privatnosti. Naime, dok u drugom pogledu autonomiju nije moguće u potpunosti ostvariti zbog vlastite autocenzure kao posljedice nedostatka privatnosti, prema trećem obliku odnosa autonomiju nije moguće u potpunosti ostvariti zbog ograničenih uvjeta u kojima se pojedinac nalazi. Ako računalni botovi kreiraju naše virtualno iskustvo, odabiru sadržaj kojem ćemo biti izloženi, odabiru koje će nam opcije biti ponuđene na izbor, ne možemo govoriti o autonomiji. Prema Razovu konceptu autonomije, pojedinac je autor vlastitoga života, a svoju autonomiju manifestira slobodnim izborom, vlastitim odabirima između smislenih i značajnih opcija koje dovode do pozitivnih ishoda za njega (Raz, 1986). No, ako internetska tražilica već na temelju nekoliko unesenih slova dovršava naš upit, prikazuje nam modificirane i ograničene rezultate takve pretrage koji

dovode do toga da što više vremena provodimo gledajući u mobitele i računala te da konzumiramo proizvode koje su nam servirali, lako je vidjeti kako smo lišeni autonomije.

> Manipuliranje ljudima, na primjer, ograničava njihovu autonomiju, i to na sličan način i u sličnoj mjeri, kao i korištenje prisile. Pribjegavanje manipulaciji trebalo bi biti moguće isključivo pod jednakim uvjetima kao i pribjegavanje prisili. (Raz, 1986: 420)

3.6. Tenzija između prava i legitimacije

Cijeli politički sustav u liberalnoj demokraciji počiva na pretpostavci kako racionalni građani slobodni čine racionalne izbore između racionalnih opcija. U liberalnoj demokraciji građani prihvaćaju autoritet države i njezinih institucija pod uvjetom da će ta država u njihovo ime osiguravati svakom građaninu sigurnost, temeljna ljudska prava i brinuti o provođenju društvenog ugovora. Prema tome, možemo reći kako je poštivanje prava pojedinaca direktno vezano uz legitimnost političkih poredaka koji sebe definiraju kao liberalno-demokratski. Istovremeno, privatnost je zbog svojeg intrinzičnog značaja za pojedince i društvo, odnosno zbog svoje supstancijalne vrijednosti, nedvojbeno jedno od temeljnih ljudskih prava vrijednih zaštite. Na taj se način na privatnost gleda i u međunarodnome pravu, kao i u ustavima i organskim zakonima država diljem svijeta. Uzmemo li kao temeljnu premisu kako je privatnost kao esencijalni dio osobnosti svakog pojedinca intrinzično vrijedna zaštite kao temeljno ljudsko pravo, tada eksterne i interne ugroze opisane u prošlom poglavlju na težak način podrivaju temeljno ljudsko pravo. Rasprava temeljena na izvješćima i rezolucijama Ujedinjenih naroda u značajnoj je mjeri podržala ovu argumentaciju. Međutim, unatoč tome što predstavlja značajan uvid i u određenoj mjeri podržava argumentaciju ovoga rada, pravna analiza iz aspekta ovog rada je sporedna. U ovom radu temeljno je normativno, a ne pravno, pitanje može li politička zajednica koja cijelu svoju političku legitimaciju temelji na osiguravanju temeljnih ljudskih prava svojim građanima opstati uz opisanu razinu ugrožavanja privatnosti kao temeljnog ljudskog prava.

Pri tome postoji više načina na koje liberalno-demokratska država propušta zaštiti pravo na privatnost i time potkopava vlastitu legitimaciju i dovodi u pitanje svoj status liberalne demokracije utemeljene na vladavini prava i temeljnim ljudskim slobodama. Prvo, a kako je opisano u dijelu u kojem se govori o eksternim ugrozama privatnosti, pojedine države aktivno nadziru i prate svoje građane i prikupljaju velike količine njihovih podataka i osobnih i intimnih podataka o njima. No, budući da većina država na drugačiji način regulira pravni status svojih građana i svih ostalih ljudi, znatno je češća situacija da pojedine države prikupljaju podatke i

prate građane drugih država. Pritom je odgovornost zaštite privatnosti građana na onoj državi čijim se građanima narušava temeljno ljudsko pravo, pravo na privatnost. Pa tako propuštanje zaštite privatnosti od nadzora treće strane predstavlja drugi način na koji država može dovesti u pitanje svoju liberalno-demokratsku legitimaciju. I ne radi se samo o zaštiti privatnosti vlastitih građana od drugih država i njihovih moćnih obavještajnih službi, radi se i o zaštiti privatnosti od velikih multinacionalnih tvrtki i internetskih divova koji prikupljaju enormne količine podataka o građanima, obrađuju ih, analiziraju i prodaju. Jasno je kako zbog inherentne logike umrežene tehnologije interneta kao i financijskih, tehnoloških i kadrovskih ograničenja rijetko koja država može parirati najvećim obavještajnim službama i internetskim divovima. Time se postavlja pitanje suvereniteta pojedine države da zaštiti temeljna ljudska prava svojim građanima. Uzmemo li u obzir i problem koji je istaknut u razmatranju eksternih ugroza, a prema kojem se čini kako značajan dio građana i ne mari za svoju privatnost te je se olako odriču, postavlja se pitanje smije li, i treba li, država štititi pravo na privatnost svojih građana unatoč tome što oni to ne žele. Bi li nametanje ograničenja i reguliranje korištenja usluga radi povećanja privatnosti građana predstavljalo doprinos općoj slobodi ili gušenje slobode i autonomije. I konačno, država zbog svoje uloge u značajnoj mjeri ima sasvim legitimnu obvezu prikupljanja, skladištenja i obrade različitih osobnih podataka svojih građana. Radi se o birokratsko-upravnim podacima, vođenju raznih matica, registara, zemljišnih knjiga, zdravstvenih kartona i slično. Država je uglavnom vrlo dobra u zaštiti takvih podataka, ali sve većim digitaliziranjem različitih javnih baza podataka, čini ih se sve podložnijima neovlaštenom pristupu. U tom smislu, država ima dužnost zaštite takvih podataka od neovlaštenog pristupa trećih strana, drugih država, organizacija, pojedinaca, kriminalaca, hakera ili odmetnutih državnih službenika.

Budući da pitanje legitimiteta državnih institucija i autoriteta države proizlazi direktno iz ideje prava, navedeni oblici ugrožavanja prava na privatnost ili propuštanja njegove zaštite direktno potkopavaju legitimnost države kao seta liberalno-demokratskih institucija. Pritom svaki oblik propuštanja zašite privatnosti otvara zasebno pitanje, pitanje paternalizma kao zaštite prava unatoč tome što ga se građani odriču, pitanje suvereniteta kao nemogućnosti osiguranja prava svojim građanima čak i uz najbolju volju i podršku građana te pitanje isprepletenih državno-korporativnih interesa. U nastavku će ova pitanja biti raspravljena nakon čega će biti prikazani rezultati empirijskog istraživanja. No, najprije je potrebno raspraviti pitanje pronalaska

ravnoteže između više suprotstavljenih prava, odnosno u ovom slučaju između sigurnosti i privatnosti, odnosno u širem smislu građanskih sloboda i ljudskih prava.

3.6.1. Ravnoteža između sigurnosti i privatnosti

Osim rapidnog razvoja telekomunikacijske tehnologije u posljednjih nekoliko desetljeća, a posebice razvoja novih internetskih tehnologija, za derogiranje prava na privatnost zaslužni su i novi sigurnosni izazovi. Kao određenu prekretnicu mogli bismo smatrati teroristički napad na njujorški Svjetski trgovinski centar 2001. godine, ali zapravo se radi o kontinuiranom procesu. Napadi koji bi se mogli okarakterizirati kao teroristički poznati su još od 19. stoljeća, ali tek nakon II. svjetskog rata teroristički napadi postali su češće korišteni. Osim toga, moguće je uočiti i određeni porast razornosti napada kao i pomicanje napada prema metama većeg ranga, zapadnim simbolima te općenito ciljevima koji će izazvati što veći teror kako bi napad bio učinkovit još dugo nakon samog izvođenja. Bez ulaženja u zahtjevan zadatak definiranja pojma sigurnosti, možemo reći kako je osobna sigurnost jedno od najvažnijih prava svakog čovjeka kojeg većina ljudi vrednuje više od svih ostalih. Suočen sa stvarnom prijetnjom vlastitoj osobnoj sigurnosti ili sigurnosti najbližih osoba, gotovo bi se svatko odrekao svega ostaloga kako bi zadržao vlastitu sigurnost[12]. Privatnosti bismo se zasigurno vrlo lako odrekli. No, u stvarnosti smo rijetko suočeni s neposrednom opasnosti i uglavnom raspolažemo dojmovima, izjavama političara, floskulama, medijskim napisima, načelnim i nejasnim ugrozama za koje je najčešće nepoznata vjerojatnost ugroze. Jedna je stvar biti žrtva otmičara koji kao otkupninu traže osobne podatke, a sasvim je druga stvar živjeti u društvu u kojem postoji određena vjerojatnost da biste mogli postati žrtvom terorističkog napada. No, s jačanjem (percepcije) terorističkih prijetnji, raste i spremnost odricanja od osobnih sloboda u zamjenu za jačanje sigurnosti. Jeremy Waldron bavio se pitanjem opravdava li promjena u broju i razmjeru prijetnji sigurnosti promjenu u razini naših osobnih sloboda (Waldron, 2003a).

Podizanje razine sigurnosti, bilo objektivne, realne sigurnosti ili subjektivnog osjećaja sigurnosti, može se postići samo uz odricanje od nečega – novca, vremena, udobnosti, mogućnosti, slobode, ljudskih prava, privatnosti. Kako bismo jednostavno mogli spriječiti da se u budućnost ponovi teroristički napad na Svjetski trgovinski centar u New Yorku? Mogli

[12] U psihologiji se razlikuju situacije prema njihovom utjecaju na manifestiranje karakteristika ličnosti. Pa tako u lakim situacijama, kao što je na primjer šetnja parkom, ljudi mogu slobodno iskazati svoju ličnost u njezinoj punini. S druge strane u teškim situacijama, ukoliko im u toj šetnji priđe razbojnik, većina će ljudi reagirati slično i njihove razlike u ličnosti manje će doći do izražaja. Područje socijalne psihologije proučava upravo sličnosti u načinu na koji različite situacije utječu na različite osobe.

bismo trajno prizemljiti sve avione na svijetu. Takav se napad više ne bi mogao ponoviti. Dakako, to bi bilo učinkovito, ali bi i cijena bila prevelika pa zbog toga nismo spremni na takav radikalan ustupak radi povećanja sigurnosti. Doduše, u prvim satima nakon napada upravo se to dogodilo, prizemljeni su svi avioni, i ljudi su to prihvatili. S druge strane spektra mogli bismo zamisliti anarhiju u kojoj je zajamčeno pravo na privatnost svakog pojedinca bez iznimki. Osim što bi to bilo nemoguće provesti, u takvom zamišljenom društvu cvjetala bi bilo kakva patološka ili kriminalna aktivnost te ono ne bi bilo mjesto na kojem bismo željeli živjeti. Ovi ekstremi imaju funkciju istaknuti nužnost pronalaska ravnoteže između dvaju suprotstavljenih prava. No, to nije nimalo jednostavno.

Za ilustraciju odnosa sigurnosti i ostalih temeljnih prava i sloboda, među koje se ubraja i privatnost, Waldron koristi sliku klasične trgovačke vage na kojoj se s jedne strane nalazi sigurnost, a s druge strane zaštita prava na privatnost. Prema njegovu rezoniranju, postoje dva moguća pristupa pronalaženju ravnoteže u slučaju da dođe do promjene s jedne od strana na vagi. Prema prvom pristupu imamo ideju maksimalnog sigurnosnog rizika koji smo spremni podnijeti uz trenutnu razinu zaštite građanskih sloboda, a u slučaju porasta rizika dolazi do narušavanja ravnoteže kojeg usklađujemo na način da smanjujemo razinu osobnih sloboda. Taj bi pristup pretpostavljao da su zbog povećanog sigurnosnog rizika ljudi spremni odreći se određene razine privatnosti radi povećanja sigurnosti. Međutim, problemu je moguće pristupiti i s druge strane. Mogli bismo pretpostaviti kako ljudi imaju minimalnu razinu temeljenih ljudskih sloboda koje se nisu spremni odreći. Prema tome, u slučaju da dođe do narušavanja ravnoteže na vagi i poraste sigurnosni rizik, kako bismo ponovo uspostavili ravnotežu, a budući da dodatno smanjenje temeljnih sloboda nije moguće, morali bismo postati hrabriji i jednostavno povećanje sigurnosnog rizika prestati smatrati povećanjem sigurnosnog rizika. Takav bi pristup pretpostavljao da ljudi kada ih se izloži povećanom riziku postaju hrabriji i korištenjem različitih svjesnih i nesvjesnih psiholoških prečaca, pristranosti, racionaliziranja taj povećani rizik prestaju smatrati stvarnim rizikom njihovoj sigurnosti. Sasvim je izvjesno kako oba ova procesa djeluju paralelno kako bi se uspostavila ravnoteža na vagi, a to je zaključio i Waldron (Waldron, 2003b).

Međutim, pronalaženju ravnoteže valja pristupiti vrlo oprezno. Unatoč tome što je metafora vage vrlo ilustrativna, ona nas može odvesti i na krivi put. Naime, koncepti poput sigurnosti, privatnosti, prava i slobode nisu banalni i nije moguće direktno, jednostavnim matematičkim zbrajanjem, uspoređivati promjene u sigurnosti i promjene u privatnosti. Za početak, Waldron

upozorava kako prava ne mogu biti podređena svakodnevnim promjenama javnih politika. U terminima naše vage, to znači dvije stvari. Prvo, neće *svaka* promjena sigurnosnog rizika izazvati prilagođavanje prava na privatnost i drugo, promjena sigurnosnog rizika neće nužno *odmah* dovesti do prilagodbe prava na privatnost (Waldron, 2003b). Samim time možemo vidjeti kako je zapravo slika trgovačke vage neodgovarajuća za ilustriranje ovako kompleksnog odnosa.

U procesu pronalaženju ravnoteže između sigurnosti i građanskih sloboda, Waldron ističe četiri važna razloga za posebno oprezan pristup. Najprije, sam *konzekvencijalizam*, koji je u srži svakog sličnog traženja ravnoteže između dvaju ili više prava, nespojiv je s diskursom građanskih sloboda (Waldron, 2003b). Kao što je detaljnije objašnjeno ranije u poglavlju, pravo na privatnosti nije apsolutno pravo i postoje jasni uvjeti u kojima je opravdano, pa i nužno, njegovo derogiranje. No, to nipošto ne znači da cilj opravdava sredstvo te da se u bilo kojem slučaju povećanog sigurnosnog rizika može ukidati pravo na privatnost. Puko povećanje sigurnosnog rizika nije dovoljno za smanjenje prava na privatnost, već su potrebni kompleksni razlozi i postojanje znatno širih uvjeta i konteksta kako bi se moglo uopće pristupiti razmatranju smanjenja temeljnih ljudskih prava.

Sljedeća stvar koju valja imati na umu prilikom prilagođavanja ravnoteže jest *distribucija* sigurnosnog rizika, odnosno distribucija ugrožavanja prava (Waldron, 2003b). Naime, zamislimo kako se i s jedne i s druge strane vage nalazi cjelokupna populacija. Kada bismo povećali sigurnost samo jedne male privilegirane skupine unutar populacije s jedne strane vage, recimo političara ili predsjednika uprava velikih korporacija, nauštrb ugrožavanja građanskih sloboda samo jedne male skupine građana s druge strane vage, recimo Arapa ili homoseksualaca, ravnoteža na vagi ne bi bila narušena. Time bismo učinili neprihvatljivu nepravdu. Međutim, čini se kako je upravo to blisko našoj realnosti. Podsjetimo, zakoni većine država, uključujući i hrvatske, razlikuju državljane te države od stranaca u lakoći kojom dopuštaju ograničavanje ljudskih prava. Uzmemo li u obzir ljude koji nemaju status stranaca nego su ilegalni imigranti ili osobe bez državljanstva, stvar postaje još više zabrinjavajuća.

Treći važan razlog koji je nužno uzeti u obzir pri razmatranju pitanja ravnoteže koji ističe Waldron jest pitanje *neželjenih učinaka* prilagodbe ravnoteže (Waldron, 2003b). Uzmimo da smo spremni ustupiti dio naših građanskih sloboda za povećanu sigurnost. Kako bismo to postigli, netko nam tu sigurnost mora omogućiti. Budući da u liberalnoj demokraciji država ima

monopol na nasilje, i dio izvora njezina legitimiteta jest upravo osiguravanje sigurnosti vlastitim građanima, našu ćemo sigurnost postići tako da osnažimo državu, odnosno, da ojačamo državne kapacitete za nošenje s povećanim prijetnjama sigurnosti. Međutim, bili bismo naivni kada bismo vjerovali da jačanje države može biti korišteno jedino za borbu protiv loših dečki. „Trebali bismo imati na umu kako će država ista sredstva koja su joj dana na raspolaganje za borbu protiv *naših neprijatelja*, koristiti za borbu protiv *svojih neprijatelja*. A unatoč tome što se te dvije kategorije, *neprijatelji naroda* i *neprijatelji države*, u velikoj mjeri preklapaju, one nisu nužno u potpunosti identične“ (Waldron, 2003: 206). Iskustvo i spoznaje iz socijalne psihologije pokazuju nam na koji način moć može utjecati na ljude. Unatoč tome što je veći dio metoda opisanih u prošlom poglavlju pod eksternim ugrozama bio utemeljen na američkim, britanskim ili australskim zakonima, određeni postupci izlazili su izvan okvira legalnosti. Visoki dužnosnici američkog obavještajnog sustava svjesno su navodili javnost na pogrešne zaključke (Contorno, 2014), a pojedini nelegalni postupci skrivani su ne samo od javnosti već i od američkog državnog odvjetništva, ministarstva pravosuđa ili predsjednika (Kirk, 2014). Niska razina transparentnosti, izostanak kontinuiranog i nezavisnog nadzora poznati su uvjeti koji dovode do toga da dobri ljudi čine loše stvari.

Posljednja stvar koju je potrebno imati na umu kod promišljanja o prilagođavanju ravnoteže jest pitanje *stvarnih ili simboličkih posljedi*ca (Waldron, 2003b). Recimo da smo pristali na konzekvencijalizam, rizik i ograničavanje prava smo pravedno rasporedili unutar populacije, primijenili smo učinkovita osiguranja od neželjenih učinaka jačanja države i odlučili smo nauštrb privatnosti primijeti određenu mjeru kako bismo povećali sigurnost. Ono na što Waldron upozorava jest koliko smo pritom imali jasan cilj koji želimo postići te koliko smo bili sigurni da će mjera koju smo primijenili dovesti do željenog cilja. Nažalost ne postoje ozbiljna istraživanja koja bi nam dala odgovore na ta pitanja. Najvećim dijelom zbog toga što ih je metodološki vrlo teško osmisliti i provesti. Kada se odlučuje na primjenu novih sigurnosnih mjera rijetko se pružaju jasni, uvjerljivi i metodološki korektni podaci o opravdanosti primjene pojedine mjere. Jednako tako, države se ne trude provesti kvalitetnu validaciju primjene pojedinih mjera. Nije moguće pronaći podatak koliko je masovni nadzor interneta doista spriječio terorističkih napada. Nije moguće pronaći takav podatak niti za ostale eksterne prijetnje koje su opisane u ovom radu. Za pojedine mjere postoje određeni podaci o konkretnom broju kaznenih djela koja su riješena korištenjem javnih nadzornih kamera ili slično, ali takvi su podaci rijetko temeljeni na metodološki kvalitetnoj validaciji koja bi uključivala ili

postojanje komparativnih slučajeva ili longitudinalnog praćenja uz kontroliranje relevantnih varijabli. Upravo su na tu praksu upozorili i posebni izvjestitelji Ujedinjenih naroda te su u svojim izvješćima opetovano upozoravali na to kako svako ograničavanje prava na privatnost potrebno mora biti temeljeno na nacionalnom zakonodavstvu koje mora biti javno objavljeno, jasno napisano, mora biti doneseno u demokratskom postupku te ono smije biti ograničeno tek kao najmanje intruzivna mjera kojom se može postići željeni cilj i mora postojati barem određena vjerojatnost da će ukidanje prava dovesti do postizanja željenog legitimnog cilja (United Nations, 2014d: 8–9). Upravo taj temeljni test opravdanosti nedostaje kod većine odluka o derogiranju prava na privatnost te time stavlja takve odluke s druge strane legalnosti u smislu međunarodnoga prava.

Sve u svemu, možemo reći kako je pitanje tenzije dvaju prava vrlo kompleksno. Konkretno, pravo na privatnost i pravo na sigurnost često se stavljaju u antagonistički položaj, ali to ne mora uvijek biti tako. U brojnim slučajevima upravo povećana privatnost doprinosi osobnoj sigurnosti pojedinca. A briga o privatnosti kroz jačanje autonomije, slobode i demokracije doprinosi i većoj sigurnosti društva, nacionalnim interesima i nacionalnoj sigurnosti. Dakako, katkada je nužno radi smanjenja sigurnosnog rizika primijeniti određene mjere kojima se ograničava pravo na privatnost, no pri razmatranju tih mjera nužno je imati na umu uvjete opisane u Principima za ograničavanje odredbi Međunarodnog pakta o građanskim i političkim pravima iz Sirakuze te uvide na koje je upozorio Jeremy Waldron.

Opisano pitanje tenzije primarno se odnosilo na eksterne ugroze privatnosti, one koje bi proizlazile iz primjene različitih mjera koje bi država primijenila radi smanjenja sigurnosnog rizika. Međutim, interne ugroze inherentno sadrže sasvim druge probleme. Jedan od njih posljedica je promišljanja o potrebi države da zaštiti pravo na privatnost svojih građana unatoč tome što ga se oni žele odreći. Postojanje neautonomnih pojedinaca delegitimira demokratske procese i dovodi u pitanje osnovne postavke liberalne demokracije. Ako autonomno odricanje od privatnosti pojedince čini manje autonomnima, u pitanje se dovodi opstanak cijelog političkog sustava. Iz ovakvog rezoniranja nameće se pitanje smije li, pa i treba li, država onemogućiti ili otežati odricanje privatnosti radi očuvanja demokratskih institucija i političkog sustava.

3.6.2. Paternalizam

Mnogi suvremeni politički teoretičari, među kojima su Dworkin, Ackerman, Larmore, Rawls, drže kako bi država trebala biti neutralna u pristupu suprotstavljanim razumijevanjima *dobroga*, međutim, perfekcionistički pristup odbacuje taj pogled (Wall, 2012). Simpatizer te ideje, koju bismo mogli nazvati *perfekcionistički liberalizam* jest i Raz. Naime, on vidi jasnu ulogu države u zaštiti autonomije pojedinaca. Budući da Raz jasno prepoznaje razliku između potencijala za uživanje autonomije i njezina ostvarenja, smatra kako postoji odgovornost države da se pojedincu pruže što bolji uvjeti u kojima bi mogao realizirati svoju autonomiju. Za njega je jedna od ključnih zadaća države upravo uklanjanje prepreka za realiziranje što većeg broja smislenih izbora građana. Ne samo da smatra kako je uplitanje države u ovom kontekstu opravdano, nego Raz smatra kako je nužno, a upravo zbog značaja za demokratski proces on vidi i instrumentalni interes liberalno-demokratske države za takvim uplitanjem (Raz, 1986). Doduše, Raz uplitanje države vidi kao vrlo posredno i diskretno. Njegov je pogled najlakše prikazati suočimo li ga s liberalnim *principom štete*.

Princip štete, temeljni je koncept liberalne misli John Stuarta Milla, a cijelo svoje najveće djelo *O slobodi* posvetio je upravo pitanju traženja granica legitimne intervencije države u život pojedinca. Naime, Mill je tu granicu definirao u terminima *negativne slobode*, odnosno za njega princip štete podrazumijeva kako jedino opravdanje za prisilno uplitanje u nečiji život može biti isključivo sprječavanje nanošenja štete drugima. Pritom je Mill, kako bi izbjegao nesporazum, već u idućoj rečenici naveo kako „vlastito dobro pojedinca, bilo tjelesno ili moralno, ne predstavlja dovoljan temelj“ (za prisilno uplitanje u njegov ili njezin život) (Mill, 2009: 18). Mill odbacuje mogućnost prisilnog osiguravanja dobrobiti ljudima protiv njihove volje. I tu se Raz ne slaže s Millom. Dakako, kao liberal, Raz se protivi bilo kakvom tvrdom paternalizmu i prisilnom uplitanju u život pojedinca, osim u slučaju krajnje nužde. No, on krajnju nuždu, odnosno *štetu*, definira drugačije od Milla. Inspiriran liberalno-komunitarnim pogledom na autonomiju, te slijedom vlastita naglaska na realizaciji autonomije, Raz tvrdi kako je „uskraćivanje osobi prilika, ili mogućnosti da ih iskoristi, oblik nanošenja štete“ (Raz, 1986: 413). Takav široki pogled na *štetu* ima značajne reperkusije na *princip štete* koji je Raz pomirio sa svojim liberalno-perfekcionističkim pogledom ponudivši redefiniciju principa štete kao principa „koji se odnosi na sprječavanje nanošenja štete bilo kome (*uključujući i samome sebi*) kao jedini opravdani temelj za prisilno uplitanje prema osobi“ (Raz, 1986: 413). Za razliku od Milla, Raz smatra kako je opravdanje za uplitanje u nečiji život protiv njegove volje opravdano

u svrhu sprječavanja štete, uključujući i sprječavanja štete za tog pojedinca, čemu se Mill eksplicitno protivi. Međutim, Raz uplitanje države vidi drugačije nego što je ga je zamišljao Mill kada je pisao *O slobodi*. Naime, dok je Mill na umu imao zaštitu pojedinaca od neovlaštenog prisilnog uplitanja države u njihovo privatno vlasništvo i osobne slobode, Raz uplitanje države vidi kroz poboljšanje uvjeta, povećavanje broja i smislenosti izbora koje pojedinci imaju na raspolaganju. Samim time, Razovo viđenje paternalizma u potpunosti je kompatibilno s vrijednosnim pluralizmom i zapravo je pluralizam okolnosti i izbora sama svrha uplitanja države.

No, što ako nečije ponašanje i djelovanje ugrožava tuđu privatnost? Što ako postupanja (multinacionalnih) tvrtki i (moćnih) obavještajnih službi ugrožavaju privatnost građana, i time im čine štetu na način da im uskraćuju izbore, uz pomoć *očigledne sveprisutnosti* ili *sveprisutnog nadzora* čine ih podložnima vanjskom pritisku, čine ih manje autonomnima? Kod eksternih ugroza koje manifestiraju države, opravdanje za ograničavanje privatnosti je briga o sigurnosti i opstanku države. U međunarodnom pravu, pravo na privatnost ne smatra se apsolutnim pravom i pod određenim uvjetima može ga se ograničiti. Države vrlo učinkovito koriste princip štete kako bi opravdale ograničavanje prava na privatnost svojih građana. Predstavlja li doista netko prijetnju nečijem tjelesnom integritetu i sigurnosti, sasvim je opravdano ograničiti mu pravo na privatnost, ali i druga prava. Kod eksternih ugroza ne možemo govoriti o paternalizmu budući da je upravo država izvor ugroza privatnosti. No, kod internih ugroza stvar je ponovo nešto kompleksnija prvenstveno stoga što interne ugroze proizlaze iz slobodnog ponašanja autonomnih pojedinaca. Postoje barem dva opravdanja za neki oblik paternalizma u slučaju internih ugroza privatnosti, odnosno vlastitog odricanja prava na privatnost.

Prvo, budući da pojedinci svjesno i dobrovoljno čine stvari kojima se sami odriču svoje privatnosti, Millov klasični liberalni princip štete ne može nam pomoći. No, prihvatimo li Razovu proširenu definiciju koja uključuje i sprječavanje činjenja štete samom pojedincu, moguće je vidjeti prostor za određenom intervencijom države. Doduše, valja istaknuti kako Raz, unatoč redefiniranju principa štete na način da uključuje i pojedinca koji je predmet prisile, paternalizam nije vidio na način kojim bi se pojedince sprječavalo da si nanose štetu, već na način kojim bi im se stvarale prilike i nudili izbori da lakše ostvare svoj potencijal autonomije. U tom smjeru idu pokušaji Europske unije da u novim direktivama što više olakša pojedincima upravljanje vlastitim podacima, da učini transparentnim način na koji će podaci biti prikupljani

i korišteni. Doduše, moguće je problematizirati i to može li se svojevoljno odricanje privatnosti smatrati činjenjem štete samome sebi, no dobar dio prošlog i ovog poglavlja služio je tome kako bi se te dvije stvari moglo dovesti u jasnu vezu.

Nadalje, drugo opravdanje paternalizma proizlazi iz komunitarne misli, sadržane u vezi autonomije i društva, a odnosi se na činjenicu da liberalne demokracije ovise o autonomnim pojedincima. Ako je privatnost konceptualno i kauzalno povezana s autonomijom kao što je u ovom poglavlju opisano, te ako su autonomni pojedinci nužni za uspostavu i održavanje demokratskih institucija i liberalne demokracije, onda se svako ugrožavanje privatnosti može smatrati ugrožavanjem demokracije. U tom bi slučaju država utemeljena na liberalnoj demokraciji trebala poduzeti mjere kako bi zaštitila svoje temeljne vrijednosti, ali i opstanak svojih institucija.

Međutim, država istovremeno ima i direktne koristi od postojeće razine odricanja prava na privatnost. To što su građani zbog svojevoljnog izlaganja na Instagramu i Facebooku manje osjetljivi na ugroze privatnosti, država koristi za slobodniju primjenu nadzora, koji ima i sekundarne pozitivne posljedice za državu - usklađivanje ponašanja s očekivanim normama zbog djelovanja *očigledne sveprisutnosti*. No, čak kada bi država unatoč svemu tome iz ideoloških razloga i predanosti ideji liberalne demokracije i vladavini ljudskih prava htjela zaštiti pravo na privatnost svojih građana, problem je u tome što bi to morala činiti protiv volje vlastitih građana. Bilo kakva pojačana regulacija radi povećanja privatnosti korisnika otežala bi ili onemogućila korištenje društvenih mreža, za posljedicu bi imala (skupo) plaćanje brojnih trenutno besplatnih usluga te bi izazvala val nezadovoljstva i velik otpor upravo među građanima koji bi se zauzimali za svoje pravo za odricanjem od privatnosti. Pravo za odricanjem od autonomije, pravo za derogiranjem demokracije.

3.7. Transformacija pojma prava na privatnost

Dramatičan razvoj komunikacijske tehnologije drastično je transformirao pojam privatnosti iz ljudskog prava u robu kojom se trguje (Davies, 1997). Davies takvu radikalnu promjenu pripisuje posljedici pet različitih tranzicija koje su se paralelno odvile. Prva je pravna i odnosi se na *skretanje fokusa sa zaštite privatnosti na zaštitu podataka*, odnosno sa zaštite osoba na zaštitu podataka. Prema Daviesu, države su ovo činile jer im je tako bilo jednostavnije budući da je zaštita podataka nešto puno konkretnije od zaštite privatnosti, ali i zato jer im je tako više

odgovaralo. Kao što je ranije opisano, Ustav Republike Hrvatske ne poznaje privatnost, već tajnost dopisivanja i svih drugih oblika općenja tajnost osobnih podataka, slobodu mišljenja i izražavanja te nepovredivost doma. Nadalje, Davies je primijetio kako su *predmeti nadzora postali partneri u nadziranju*, a mogli bismo reći kako su Harcourtovo *društvo izlaganja* i Bernalova *simbiotska mreža* zapravo tek nastavak procesa koje je Davies primijetio još 1997. godine. Iduća tranzicija odnosi se na *iluziju dobrovoljnosti*, odnosno na činjenicu kako mnoge tehnologije nadzora uključuju određeni stupanj dobrovoljnog davanja podataka koji dovodi do raširenog neutraliziranja javne zabrinutosti za ugroze privatnosti. Komercijalizacija osobnih podataka, nuđenje usluga u zamjenu za osobne podatke doveli su do toga da su građani na privatnost i na svoje osobne podatke i sami počeli gledati kao na *robu kojom mogu trgovati*. Istovremeno su desenzitizirani za ugroze privatnosti iz drugih izvora. I posljednja tranzicija koju je Davies istaknuo jest *trijumf javnog interesa*, a odnosi se na to kako pojedine države koriste javni interes kao generičko opravdanje za sve aktivnosti države. Kao što se može vidjeti, svi procesi koje je Davies zamijetio 1997. godine rapidno su nastavljeni kasnije. Rašireno korištenje interneta, pametnih telefona, društvenih mreža sve je ove procese dodatno ubrzalo i intenziviralo što je za posljedicu imalo dubinsko redefiniranje pojma privatnosti i pojma prava na privatnost. Davies je u potpunosti u pravu kada tvrdi kako se „ne radi o tome da su ljudi manje zabrinuti za privatnost, nego su pojam privatnosti i ideja ugroze privatnosti radikalno redefinirani zbog čega su ljudi postali ambivalentni prema ugrozama privatnosti“ (Davies, 1997: 144).

Tako transformiran pojam privatnosti i zaštita takvog redefiniranog pojma prava na privatnost nespojiva je s idejom da nacionalna država u okviru liberalne demokracije na učinkovit način štiti prava svojih građana, u ovom slučaju pravo na privatnost. Trenutni odnos građana i države prema privatnosti i pravu na privatnost nije spojiv s temeljnim postavkama liberalne demokracije. Ova se tenzija može ublažiti samo na dva načina: ili je potrebno odbaciti privatnost kao temeljno ljudsko pravo ili je ga je potrebno na dosljedan i učinkovit način osiguravati, štititi i vrednovati. Kako bi se dobio bolji uvid u to kako doista građani gledaju na privatnost, koliko im je važna i pod kojim su je se uvjetima spremni odreći, provedeno je empirijsko istraživanje na prigodnom uzorku. Dobiveni rezultati bit će interpretirani zajedno s ovim zaključkom kako bi pružili cjelovitu sliku problema transformacije pojma privatnosti.

4. Empirijsko istraživanje

Komplementarno normativnoj teoretskoj raspravi o održivosti prava na privatnost kao temeljnog ljudskog prava, provedeno je i empirijsko istraživanje čiji je cilj bio utvrditi način na koji ljudi razumiju koncept privatnosti i prava na privatnost. Uz to, kako bi se provjerilo drugo istraživačko pitanje, odnosno kako bi se provjerilo postojanje paradoksa privatnosti, bilo je potrebno utvrditi koliko je privatnost pojedincima važna te koliko su je se lako spremni odreći. Bez obzira na (ne)potvrđivanje istraživačke hipoteze, dobiveni rezultati predstavljat će značajan doprinos razumijevanju privatnosti. Naime, potvrđivanje istraživačke hipoteze značilo bi da je i među pojedincima došlo do svojevrsnog odricanja prava na privatnost, što bi moglo objasniti zašto tako olako i bez prevelikog opiranja dopuštaju pa i podržavaju, korporativne i državne politike koje zatiru privatnost. Međutim, i suprotni rezultati, oni koji bi pokazali da je pojedincima privatnost važna te da je se nisu spremni olako odreći, bili bi barem jednako toliko zanimljivi. Naime, u tom bi slučaju bilo potrebno objasniti kako i zašto osobe kojima je privatnost visoko važna dopuštaju i podržavaju politike koje zatiru privatnost i koriste usluge kojima se odriču svoje privatnosti.

4.1. Predistraživanje

Prije nego što se pristupilo izradi i provedbi ankete, bilo je potrebno provjeriti način na koji različite osobe uopće razumiju pojam privatnosti, kolika je važnost privatnosti za njih, vide li i u čemu vrijednost privatnosti te kako razmišljaju o ugrozama privatnosti. Stoga je provedeno kvalitativno predistraživanje korištenjem polustrukturiranog intervjua. Intervjui su provedeni tijekom svibnja 2017. godine na prigodnom uzorku od 16 osoba, no u odabiru sudionika pokušalo se odabrati osobe različitih sociodemografskih karakteristika pa su tako u istraživanju sudjelovali majstor svjetla u kazalištu, profesorica u srednjoj školi, biotehnolog, liječnik, medicinske sestre, magistar tehničkih znanosti, umirovljenica, maturanti i studenti različitih fakulteta pri čemu je sudjelovalo devetero ženskih sudionica i sedmero muških sudionika. Prosječna dob sudionika bila je 34 godine, a raspon je bio od 18 do 63 godine. Unatoč tome što je u predistraživanju korišten raznolik uzorak sudionika, važno je naglasiti kako namjera nije bila korištenje reprezentativnog uzorka radi donošenja zaključaka o populaciji. Sama priroda kvalitativnog istraživanja jest takva da se njime željelo dosegnuti individualna iskustva

pojedinaca, jezik koji koriste kada razmišljaju i govore o privatnosti i ugrozama privatnosti te njihove interpretacije i očekivanja.

Teme u intervjuu sezale su od načina na koji sudionici razumiju i doživljavaju privatnost i pravo na privatnost, preko osobnih iskustava u kojima je njihova privatnost bila narušena, njihova promišljanja o ugrozama privatnosti, impresijama, osobnom osjećaju i iskustvu prilikom narušavanja privatnosti pa sve do određenih pitanja o načinu na koji sudionici koriste tehnologiju i društvene mreže te implikacijama njihova korištenja na privatnost sudionika. Trajanje intervjua bilo je od 15 do 45 minuta, a sve je razgovore obavio jedan intervjuer. Svi su intervjui tonski snimljeni uz eksplicitni i zabilježeni pristanak sudionika, a kasnije su transkribirani te su obrađeni tematskom analizom sadržaja.

4.1.1. Rezultati

Osnovni cilj predistraživanja bio je provjeriti način na koji različite osobe uopće razumiju ključne pojmove koji će biti korišteni u glavnom dijelu istraživanja, anketnom istraživanju provedenom na znatno većem uzorku. Velike razlike u načinu na koji sudionici razumiju pojam privatnosti značile bi da korištenje tog pojma u anketnim pitanjima nije prikladno budući da se dobivene rezultate ne bi moglo na odgovarajući način interpretirati. Naime, velike razlike u razumijevanju određenog pojma predstavljale bi ozbiljan metodološki problem te se takav pojam ne bi mogao mjeriti bez prethodnog jasnog definiranja. Osim provjere jednoznačnosti pojma, za konstrukciju konkretnih čestica koje su korištene u anketnom istraživanju upotrjebljen je konkretan leksik koji su sudionici koristili u intervjuima, njihova razmišljanja i osobni doživljaji. I konačno, već je i samo kvalitativno predistraživanje pružilo određene odgovore na drugi istraživački problem, odnosno na pitanje značaja privatnosti za pojedinca u današnjem društvu te na pitanje jesu li se sudionici, i pod kojim uvjetima, spremni odreći svoje privatnosti.

Gotovo svi sudionici naveli su kako ranije nisu mnogo ili nisu uopće razmišljali o privatnosti, no većina je s lakoćom odgovarala na postavljena pitanja. Svi sudionici, osim dvoje, naveli su kako im je privatnost važna ili izrazito važna.

4.1.1.1. Definicija i važnost privatnosti

Sudionicima je uglavnom bilo vrlo teško postulirati definiciju privatnosti, što i ne čudi budući da se i ozbiljni znanstvenici koji su cijelu karijeru posvetili istraživanju privatnosti i sami muče

s pronalaskom odgovarajuće definicije. No, većina sudionika u svojim je opisima privatnost definirala kao *nešto samo njihovo, nešto što ne žele dijeliti s drugima*. Pri tome se *nešto* najčešće odnosilo na intimne informacije i podatke povezane s domom i obitelji. Zanimljivo je kako je većina sudionika privatnost operacionalizirala u terminima kontrole pristupa, što se poklapa s autorima koji privatnost definiraju kroz mogućnost kontrole pristupa sebi (Allen, 1988; Gavison, 1980; Moore, 2003) i kao kontrolu nad informacijama o sebi (Parent, 1983). Tako je na primjer sudionica S01 navela „ (…) *to bi bili podaci o zdravstvenom stanju, moji stavovi o bilo čemu, ja ću ih podijeliti rado, ali samo s onima s kojima želim. Pa čak i moje tijelo fizičko, ne želim da me bilo tko vidi golu* (…)", sudionik S04 naveo je „ (…) *znači to je taj dio (osobnog integriteta) za koji ja odlučujem s kime ću ga dijeliti.*", sudionik S06 naveo je „*Privatnost je ono što svaki čovjek treba čuvati za sebe, (...) da ne želi to pokazati bilo kome, nego određenom krugu ljudi poput obitelji. Na primjer, na internetu fotografije koje želi podijeliti samo s nekime, a ne sa svima.*", a sudionik S07 opisao je različite razine pristupa te je naveo „*Ja sam otvoren i nemam problema s time, ali neke stvari želim zadržati za sebe, neke podijeliti samo s nekim ljudima, a neke sa svima.*" U svim citiranim opisima prisutna je određena razina kontrole. Sudionici su prepoznali privatnost kao mogućnost upravljanja podacima o sebi za koje će nekome omogućiti pristup njima, a drugima neće omogućiti pristup. Nadalje, ove spoznaje upućuju na to da ljudi prepoznaju privatnost kao konstrukt i koriste ga u svakodnevnom životu kako bi razlikovali najmanje dvije domene, dvije sfere, u kojima djeluju. Pri tome privatna sfera obuhvaća intimne odnose, osobne stavove, a za nekoliko sudionika i fizičku lokaciju doma, kao i sve što dom predstavlja u društvenom smislu. Poistovjećivanje doma s privatnom sferom na tragu je pogledu na privatnosti koji ima Iris Marion Young, koja smatra kako je izostavljanje privatnog prostora, kao fizičkog prostora u kojem se privatnost može manifestirati, veliki nedostatak postojećih teorija privatnosti. „Barem u suvremenim društvima, važan aspekt vrijednosti privatnosti jest sposobnost imati vlastiti prostor za obitavanje, kojemu osoba može kontrolirati pristup i u kojem živi među onim stvarima koje podupiru narativ njezina života.", ističe Young (2005: 155), dok sudionica S03 svojim riječima navodi „*Privatnost doživljavam povezano s domom, obitelji, mojom intimom. To je moja privatnost. Sve što se događa u kući, u domu, u mojoj obitelji i što se tiče obitelji i doma*". Ista sudionica, i samo ona, privatnost je opisala višedimenzionalno te je navela kako za nju postoji više privatnosti, među kojima je izdvojila političku privatnost, privatnost u vjeri, tjelesnu privatnost i privatnost spolnosti. Ostali sudionici nisu opisivali različite kategorije privatnosti te stoga u ovom istraživanju ne možemo reći kako smo potvrdili postojanje više dimenzija privatnosti, kako su pojedini autori poput

Judee Burgoon (1982; Burgoon i dr., 1989) i u određenom smislu Daniela Solovea (2006) dali naslutiti. No, unatoč tome, vrijedi istaknuti kako je sudionica S03 svakako bila na tome tragu te njezini uvidi ukazuju na to kako postoje pojedinci koji prepoznaju različite dimenzije privatnosti.

Nadalje, svi sudionici, osim dvoje sudionika koji će biti posebno obrađeni, naveli su kako im je privatnost važna ili izrazito važna. Pritom su kao vrijednost privatnosti prvenstveno isticali njezinu važnost za uspostavu i održavanje intimnih odnosa, a nekoliko ih je istaknulo važnost privatnosti za ljudsko dostojanstvo. Posebno je zanimljiva izjava sudionice S01 u kojoj je navela „*Vrijednost privatnosti postoji kod dvoje ljudi, ljubavnika, u najintimnijim situacijama jer ona čini tu situaciju baš samo njihovom*“ budući da tom izjavom odlično opisuje viđenje važnosti privatnosti koje je imao Charles Fried, a to je da se upravljanjem iznošenja intimnih podataka o sebi mogu stvarati i održavati različiti međuljudski odnosi (Fried, 1968). Sudionica S12 navela je „*Nekada u odnosu neke stvari pomisliš i ne podijeliš ih s tom osobom jer bi to narušilo odnos, ne prihvaćaju svi ljudi sve na isti način i onda to zadržiš za sebe*.“ Fried je govorio upravo o tome kako bez mogućnosti reguliranja i upravljanja podacima o sebi, bez mogućnosti da neke misli, dojmove i uvjerenja zadržimo samo za sebe ili samo za uzak krug ljudi, a što nam omogućuje upravo privatnost, jednostavno ne bismo mogli ostvarivati intimne odnose.

Sudionica S12 nešto kasnije u intervjuu istaknula je i drugu važnost privatnosti, onu za ljudsko dostojanstvo „*Pa da nemaš privatnost, ne bi imao svoj život. (...) Privatnost mi je važna jer je to ono što nas čini, zbog tog si ono što jesi*“, čime podsjeća na Blousteinov koncept nepovredive osobnosti, koji je za njega predstavljao samostalnost pojedinca, njegovo dostojanstvo i integritet te je pojedinca definirao kao samoodređujuće biće (Bloustein, 1984). Sudionik S04 upravo je koristio sličan rječnik te je govoreći o gubitku privatnosti naveo „ (…) *čovjek se otuđuje od svoje biti. (...) Privatnost je nešto što je dio mog vlastitog osobnog integriteta koje ja kao osoba smatram da ne trebam dijeliti s drugima.*“ Sudionik S08 jedini je u tvrdnji „*Želim imati pravo nekada biti onakav kakav nisam pred svima*“ implicitno sugerirao važnost privatnosti za autonomiju, koja je temelj stvaranja bilo koje nezavisne misli. Osim toga, nekoliko sudionika navelo je kako im privatnost „*pruža sigurnost*“ (S10), odnosno opisali su je kao „*nešto gdje se osjećaš sigurno*“ (S09), što je zanimljivo budući da se u određenim suvremenim političkim raspravama pravo na privatnost stavlja nasuprot prava na sigurnost kao da se radi o međusobno isključujućim pravima. Međutim, ideja kako upravo privatnost

osigurava, a ne ugrožava, sigurnost te kako je privatnost *ono gdje se osjećaš sigurno*, znači kako su privatnost i sigurnost neodvojivo povezani. Osim toga, govoreći o tenziji između privatnosti i sigurnosti u prošlom je poglavlju zaključeno kako se privatnost i sigurnost često stavljaju u antagonistički položaj, no kako u brojnim slučajevima upravo povećana privatnost doprinosi osobnoj sigurnosti pojedinca, a kroz jačanje autonomije, slobode i demokracije doprinosi i većoj sigurnosti društva i nacionalnoj sigurnosti.

Nadalje, dvoje sudionika koji su naveli kako im privatnost nije važna, isticali su vlastitu otvorenost, dosljednost i izostanak tajni kao razloge zbog kojih im privatnost nije važna pa je tako sudionica S16 navela „*Nije mi važna privatnost. Osoba sam koja voli pričati, otvorena sam, nemam tajni. (...) Ne mogu zamisliti ugrozu moje privatnosti. Nemam ništa za sakriti, ništa ne radim pogrešno. (...) Pa ne bi mi ništa smetalo, može se sve znati o meni, nemam nikakve tajne posebne.*“ Ovo predstavlja klasični ništa-za-sakriti argument, o kojem je Solove napisao cijelu knjigu u kojoj je argumentirano pobio svaki element tog argumenta te je pokazao kako je u njegovoj pozadini nerazumijevanje koncepta privatnosti (Solove, 2011). S druge strane, sudionik S02 naveo je „*Nisam baš opterećen privatnosti. (...) Volim misliti da mi privatnost nije važna. Ne bih si stvarao paniku ili tjeskobu da me netko vidi u trenucima koji su za mene privatni. Volim taj osjećaj da mogu stati iza svega što govorim pred svakime tako da sve što govorim može se predstaviti bilo kome.*“. Njegov cijeli intervju posebno je zanimljiv budući da je unatoč deklariranoj nevažnosti privatnosti u više navrata naveo kako postoje podaci koje smatra intimnima i čije bi mu razotkrivanje izrazito smetalo. Ostavio je dojam kao da je deklariranje nevažnosti privatnosti više njegovo uvjerenje nastalo kao svojevrsna racionalizacija, odnosno, način na koji se nosi sa sveobuhvatnom transparentnosti kojoj je izložen, a ne da njime opisuje svoju istinsku nezainteresiranost za privatnost. Ova spoznaja vrlo je intrigantna te je stoga bila na odgovarajući način testirana u anketnom istraživanju.

4.1.1.2. Ljudska priroda

Jedna od značajnijih spoznaja proizašlih iz intervjua bila je ta da su određeni sudionici važnost i vrijednost privatnosti procjenjivali ovisno o načinu na koji vide ljudsku prirodu. Naime, sudionici su isticali dva ključna obilježja ljudske prirode zbog kojih je privatnost u ovom trenutku nužna kako bi nas zaštitila, a to su *manjak samopouzdanja* i *zlonamjernost drugih*. Prema njihovu tumačenju, kada bi ljudi bili lišeni vlastitih kompleksa i/ili kada drugi ljudi ne bi bili zlonamjerni, privatnost nam ne bi bila potrebna. Tako je sudionik S02 naveo „*Lako iznosim svoje privatne detalje jer vjerujem da su ljudi s kojima komuniciram dobri i da neće*

zloupotrijebiti moje podatke“, dok je sudionik S08 imao potpuno drugačije viđenje svoje okoline „*Imao sam svakakvih problema, ali sam naučio nešto o životu – 70% ljudi ti želi loše i ne želim se nikome otvarati.*“ Kao što je ranije navedeno, sudionik S02 je vrlo nisko vrednovao privatnost, dok je sudionik S08 vrlo visoko vrednovao privatnost, što je u skladu s njihovim pogledom na ljudsku prirodu. Na sličan način, no uz nešto više elaboriranja, sudionik S04 naveo je kako smatra da u idealnom svijetu privatnost uopće ne bi bila potrebna „ (…) *jer bi ljudi bili načisto sami sa sobom i ne bi morali skrivati svoje ranjivosti*“. Na tom je tragu i sudionica S01 koja je navela „*Da su ljudi normalni, privatnost ne bi bila važna. Da su ljudi dobrohotni, da su tolerantni, da nemaju predrasuda, da imaju više razumijevanja, onda možda ne bih imala potrebu za tolikom privatnosti, ali budući da znam da je velika većina ljudi puna predrasuda, da su netolerantni i primitivni te da bi mogli zloupotrijebiti i zbog toga mi je to važno i inače mi to ne bi uopće bilo važno. (...) Po meni, ja bih mogla biti puno otvorenija i manje inzistirati na privatnosti kada bi sredina bila drugačija.*“ Ove su spoznaje vrlo zanimljive i bacaju novo svjetlo na način na koji ljudi razumiju privatnost. Unatoč tome što su različiti autori značaj privatnosti u određenoj mjeri definirali negativistički, kao nužnu za zaštitu od narušavanja dostojanstva, integriteta, autonomije i intime, na nju se nije gledalo kao na nužni nusproizvod zaštite vlastite nesavršenosti od zlonamjernosti drugih. Za pojedine sudionike, idealan svijet je onaj u kojem privatnost nije ni potrebna, u kojem su ljudi samopouzdani, zadovoljni i ne bave se životima drugih. Prema njima, privatnost bi tada izgubila svoju instrumentalnu funkciju. Doduše, instrumentalni značaj privatnosti za uspostavu i održavanje međuljudskih odnosa i dalje bi zadržao svoj značaj i ulogu. Uostalom, razmišljanja pojedinih sudionika imala su prvenstveno funkciju naglasiti instrumentalni značaj privatnosti zbog nesavršenosti ljudi, a budući da su ljudi nesavršeni i da će takvi zauvijek biti, privatnost će uvijek imati svoj značaj za pojedince i društvo. Iako promišljanja pojedinih sudionika nemaju funkciju redefiniranja privatnosti ili njezina značaja, ove spoznaje pružaju vrijedan pogled na način na koji pojedinci razumiju privatnost. Stoga, kako bi se dodatno provjerila povezanost načina na koji sudionici gledaju na ljudsku prirodu i njihova vrednovanja privatnosti, u anketno istraživanje uključeno je i nekoliko odgovarajućih varijabli.

4.1.1.3. Narušavanje privatnosti i zaštita privatnosti

Tijekom intervjua sudionicima su postavljana pitanja o tome jesu li zadovoljni razinom zaštite privatnosti koju uživaju, smatraju li da je njihova privatnost narušena, i na koji način, te smatraju li da pojedina tehnička rješenja ili načini postupanja privatnih tvrtki i državnih službi

ugrožavaju njihovu privatnost. Niti jedan sudionik nije naveo kako se osjeća nadziranim i većina se teško mogla sjetiti ijednog slučaja u kojem je njihova privatnost bila ugrožena, neovisno o njihovim različitim definicijama i konceptualizacijama privatnosti. Gotovo svi sudionici bili su zadovoljni trenutnom razinom privatnosti koju uživaju, unatoč tome što su svi, osim jedne sudionice, naveli kako njihova privatnost može vrlo lako biti narušena. Odnosno, u velikoj su mjeri precjenjivali kapacitete nadzora koje policija i sigurnosne službe imaju na raspolaganju uz navode kako *je normalno da policija i hakeri mogu čitati sve i pristupiti svoj elektronskoj komunikaciji*. No, uvjerenje kako specijalizirane državne agencije i hakeri mogu pristupiti *svemu*, ni za koga od njih nije predstavljala problem te su navodili kako smatraju da su oni osobno *nebitni*, da nikome *nisu interesantni* ili jednostavno da im *ne smeta ako netko čita i sluša njihovu privatnu korespondenciju* te su gotovo svi naveli kako spoznaja da njihovoj privatnoj komunikaciji može imati pristup i netko kome ona nije namijenjena ne utječe na način na koji komuniciraju. Jedino je sudionica S14 navela kako *ne razmišlja o tome da netko može čitati njezine poruke* i kako bi je *jako uznemirilo kada bi znala da je tako nešto moguće*.

Činjenica da su sudionici uvjereni kako je njihova privatna korespondencija lako dostupna državnim službama, velikim tvrtkama i vještim korisnicima te da su istovremeno zadovoljni zaštitom privatnosti koju uživaju, s psihološkog aspekta vrlo je intrigantna. Istovremeno, ta spoznaja ukazuje na mogućnost da je već došlo do transformacije pojma privatnosti i da se o privatnosti više ne može razmišljati na način na koji se na nju gledalo posljednjih stotinjak godina. Naime, ako je doista istina da ljudi smatraju kako u svakom trenutku mogu biti nadzirani bez vlastita znanja, a da istovremeno ta spoznaja ne utječe na njihovo ponašanje, onda uvidi Benthama i Foucaulta o *očiglednoj sveprisutnosti*, odnosno o *sveprisutnom nadzoru* više ne vrijede. Podsjetimo, Bentham je govoreći o učinkovitosti arhitektonskog projekta panoptikona isticao kao jednu od najvećih prednosti činjenicu da bi kroz stalnu izloženost pogledu nadglednika te istovremenu nemogućnost određivanja gleda li ga doista u pojedinom trenutku nadglednik ili ne, svaki zatvorenik internalizirao ponašanje koje se od njega očekuje. Foucault je arhitektonski nacrt panoptikona proširio na cijelo moderno društvo te je govorio o *automatskom djelovanju moći* kada bi došlo do takve internalizacije. Današnje je digitalno društvo najbliže panoptikonu što smo ikada do sada bili. Značajan dio naše digitalne korespondencije i općenito digitalnih iskustava u svakom trenutku može biti dostupan *nadglednicima*, a istovremeno ne postoji način na koji bismo jednostavno i sa sigurnošću mogli znati jesmo li u pojedinom trenutku nadzirani ili ne. Međutim, rezultati provedenih intervjua

sugeriraju da kod većine sudionika nije došlo do automatskog djelovanja moći. Očigledno je kako sudionici imaju svijest o tome da u bilo kojem trenutku mogu postati predmetom nadzora i da njihova elektronska korespondencija i privatni podaci mogu biti prikupljani bez njihova znanja, ali svi sudionici osim sudionice S12, i sudionice S14 koja jedina nije ni razmišljala o tome kako netko može imati pristup njezinoj privatnoj korespondenciji, naveli su kako ta spoznaja ne utječe na način na koji komuniciraju na internetu i koriste digitalne usluge. Moguće je da je ideja o potpunoj digitalnoj transparentnosti, odnosno svijest o potencijalnim ugrozama koje proizlaze iz takvog digitalnog izlaganja, preapstraktna da bi natjerala ljude da odustanu od lagodnosti korištenja besplatnih usluga i nekritičkog dijeljenja osobnih podataka radi umrežavanja s ostalim korisnicima. Osim toga, u socijalnoj psihologiji poznata je teorija kognitivne disonance Leona Festingera (Festinger, 1957, 1962) koja opisuje nelagodu koju ljudi osjećaju kada su njihova uvjerenja u sukobu ili kada se ponašaju na način koji nije konzistentan s njihovim uvjerenjem. Budući da kognitivna disonanca izaziva nelagodu, ljudi žele umanjiti nelagodu i to čine na tri osnovna načina: mogu promijeniti svoje ponašanje kako bi ga uskladili s uvjerenjem, mogu pokušati opravdati svoje ponašanje promjenom uvjerenja ili mogu pokušati opravdati ponašanje dodavanjem novih uvjerenja (Aronson, Wilson, Akert i Sommers, 2016: 159). Na taj će način, na primjer, pušači koje se izloži uvjerljivim znanstvenim spoznajama o štetnosti pušenja imati opciju prestati pušiti, odbaciti spoznaje o štetnosti pušenja kao antipušačku propagandu, pribjeći jednoj od brojnih heuristika poput vjerovanja kako se loše stvari događaju drugima ili dodavati nova uvjerenja o tome kako pušenje ima i pozitivne učinke ili koristiti primjer nečijeg djeda koji je pušio, a doživio je sto godina. No, promjena ponašanja je nerijetko znatno teža nego promjena vlastitih uvjerenja pa tako mnogi pušači imaju brojna maštovita opravdanja za svoje ustrajanje u toj štetnoj aktivnosti ili pak maštovita objašnjenja zašto pušenje nije toliko štetno koliko se govori. Slično tome, ljudi koje se izloži spoznaji o masovnom nadzoru, spoznaji o potpunoj digitalnoj transparentnosti te ugrozama i opasnostima koje proizlaze iz nje, puno će prije početi vjerovati kako su oni osobno *nebitni*, kako nikome *nisu interesantni* te kako im *ne smeta ako netko čita i sluša njihovu privatnu korespondenciju* i uz to će nastaviti ustrajati u aktivnostima koje su im ugodne, a koje su loše za njih nego što će biti spremni promijeniti svoje ponašanje.

Sudionica S12 jedina je od petnaest sudionika koji su smatrali kako je njihova elektronska korespondencija gotovo u potpunosti transparentna, a koja je navela kako to utječe na način na koji komunicira s drugima „*Mislim da policija može vidjeti moje poruke, a to mogu i hakeri i*

tvrtke, Facebook, Google. Ne mislim da osobno meni rade, ali ako nešto posumnjaju mislim da mogu doći do svih podataka. Zbog te spoznaje ne pišem bilo što. Mislim da dosta ljudi tako razmišlja i da ne pišu sve. U četiri oka im sve kažem, ali neke stvari ne volim pisati. Pomirila sam se s time da ne mogu sve povjerljivo napisati. Tehnologija toliko napreduje da je nerealno boriti se protiv toga." Kao i svi ostali sudionici, osim sudionice S14, i sudionica S12 svjesna je razvoja tehnoloških mogućnosti nadzora elektronskih komunikacija, ali za razliku od ostalih sudionika, ona je jedina iskazivala kako zbog toga više vodi računa o tome što, kome i na koji način komunicira. I dok na taj način u određenoj mjeri štiti svoju privatnost od znatiželjnih očiju, na nju se odnosi automatsko djelovanje moći te je sputava i ograničava u njezinim društvenim kontaktima.

Dok je elektronska korespondencija za pojedine sudionike i bila vrijedna zaštite, gotovo nijednom sudioniku nisu smetale kamere za nadzor koje su postavljene u brojnim otvorenim i zatvorenim javnim prostorima, kao što im nije smetalo ni to što različite tvrtke prikupljaju i obrađuju brojne njihove podatke. Svi sudionici pokazali su kako ne znaju što se događa s njihovim podacima nakon što ih se prikupi, no nisu pokazali ni interes saznati. Stavljanje informacija o tome što se događa s njihovim podacima izvan vlastite spoznaje ide u prilog mogućem objašnjenju kako ljudi ne žele ni znati negativne učinke ponašanja koje im je toliko ugodno i drago. Zbog nelagode koju izaziva kognitivna disonanca, ljudi katkada izbjegavaju doći u kontakt sa saznanjima koja bi mogla izazvati pojavu nelagodne kognitivne disonance.

Tijekom razgovora o narušavanju privatnosti kod više sudionika bilo je očigledno kako bi im znatno manje smetalo kada bi anonimni analitičar u nekoj domaćoj ili stranoj sigurnosnoj službi ili multinacionalnoj tvrtki prikupljao brojne detaljne podatke o njima nego što bi im smetalo kada bi poneki od tih podataka saznala njima bliska osoba, prijatelj ili poznanik. Sudionica S01 navela je kako joj nije problem da nepoznata osoba zna podatke o njoj te je izjavila kako to narušavanje privatnosti „*da neki činovnik ili djelatnik neke firme zna podatke o mojim kupovnim navikama je za mene nebitan.*" dok je sudionik S08 bio još eksplicitniji: „*Policija može čitati i neka to čitaju, to me ne dira. Samo osobe koje su dio mojeg života ne želim da znaju o meni.*" Ova je spoznaja naizgled kontraintuitivna jer bi se moglo reći kako bliskim osobama više vjerujemo te smo s njima spremni više toga podijeliti. Međutim, prijetnja koja proizlazi iz činjenice da naše podatke, pa makar i intimne ili kompromitirajuće, posjeduje anonimni zaposlenik neke strane službe kome smo *nebitni*, ili pak da iste te podatke obrađuje i pohranjuje

automatizirani računalni softver, znatno je manja i znatno je više apstraktna od prijetnje koja proizlazi iz mogućnosti da naši prijatelji znaju o nama više nego što bismo im željeli reći.

4.1.2. Zaključak

Provedenim istraživanjem dobiveni su vrlo značajni i dijelom neočekivani rezultati. Najprije vrijedi istaknuti kako rezultati predistraživanja sugeriraju da ljudi o privatnosti vrlo rijetko razmišljaju. A kada razmišljaju o privatnosti, definiraju je u terminima kontrole pristupa sebi i informacijama o sebi. Nadalje, rezultati upućuju na to kako je privatnost većini vrlo važna i drže do nje, a njezinu vrijednost vide u važnosti za uspostavu i održavanje intimnih odnosa, važnosti za vlastito dostojanstvo i autonomiju. No, rezultati ukazuju na to da istovremeno postoje i ljudi koji privatnost smatraju reliktom prošlosti, nečime što u današnje vrijeme nije moguće osigurati ili nečim sasvim bezvrijednim. U tom smislu vrijedna je i spoznaja o tome kako uvjerenje jesu li ljudi prvenstveno dobronamjerni ili zlonamjerni direktno utječe na to hoće li se na privatnost gledati kao na nešto suvišno ili na nešto vrijedno zaštite.

Nadalje, potrebno je istaknuti uvide o neodvojivoj povezanosti privatnosti i sigurnosti, odnosno činjenice da za pojedine sudionike upravo privatnost osigurava osjećaj sigurnosti, dok izloženost izaziva osjećaj tjeskobe i moguće ugroženosti, psihološke ili fizičke. U razgovoru s nekoliko sudionika, mahom onih mlađih od 30 godina, zamijećeno je kako postoji određena razina desenzitizacije prema ugrozama njihove privatnosti, pomirenosti s brojnim oblicima ugroze, svojevrsna *naučena bespomoćnost*[13]. Neslavni *ništa-za-sakriti* argument kod pojedinih sudionika igrao je značajnu ulogu u prosuđivanju mogućnosti i razine narušavanja privatnosti te razmišljanju o zaštiti privatnosti. Sudionici su u velikoj mjeri precjenjivali kapacitete nadzora policije i sigurnosnih službi te je većina svu elektronsku komunikaciju i elektronske podatke smatrala u određenoj mjeri dostupnima trećim osobama, no zbog toga nisu bili zabrinuti.

Ove spoznaje ukazuju na to kako je pojam privatnosti transformiran na način predviđen u prošlom poglavlju i na razini građana, odnosno kako je postojeća domena privatnosti i intenzitet kojom će je se braniti znatno drugačiji nego što bi se očekivalo za jedno temeljno ljudsko pravo. Ne radi se o tome da je granica između privatne i javne sfere obrisana, već se ona značajno

[13] Radi se o terminu iz područja psihologije učenja koji označava izostanak adaptivne reakcije na nelagodu kao naučenu reakciju zbog opetovanog izlaganja podražaju bez mogućnost izbjegavanja tog podražaja (Seligman, 1972). S vremenom je ustanovljeno kako naučena bespomoćnost može objasniti pasivna ponašanja i u različitim društvenim situacijama.

pomaknula na način da je privatna sfera minimizirana i sada predstavlja tek one najosnovnije, najintimnije i najvrijednije dijelove ljudskog ponašanja.

Kao što je bilo i planirano, spoznaje prikupljene kvalitativnim predistraživanjem poslužile su za konstrukciju dijela upitnika anketnog tipa koji je primijenjen na znatno većem uzorku u kvantitativnom dijelu istraživanja. Osim što su u istraživanje uvršteni i određeni istraživački problemi proizašli iz analize intervjua, pojedine su čestice direktno inspirirane intervjuima s pojedinim sudionicima, a u mjeri u kojoj je to bilo moguće, korišten je i leksik koji su koristili sudionici.

4.2. Kvantitativno istraživanje[14]

Kvantitativno istraživanje motivirano je željom da se teoretska rasprava o privatnosti iz prethodnog poglavlja, ona koja na transformaciju pojma privatnosti gleda normativno, odozgo, nadopuni spoznajama o tome na koji način građani razumiju privatnost i ugroze privatnosti. Kako bi dobiveni rezultati imali veću valjanosti, odnosno kako bi se zaključci s određenom razinom sigurnosti mogli odnositi na populaciju bilo je potrebno provesti istraživanje na znatno većem i po mogućnosti reprezentativnom uzorku. U tom je istraživanju primarni cilj bio odgovoriti na drugi istraživački problem, odnosno testirati drugu istraživačku hipotezu:

- **H2: Rezultati istraživanja pokazat će postojanje značajne diskrepancije između deklarirane visoke važnosti privatnosti za pojedince i lakoće kojom su je se spremni odreći.**

4.2.1. Paradoks privatnosti

Druga istraživačka hipoteza zapravo označava ono što se u literaturi naziva *paradoksom privatnosti*. Prva je taj pojam skovala Susan Barnes u eseju o privatnosti na društvenim mrežama u kojem je primijetila kako postoji velika razlika između lakoće kojom tinejdžeri odaju svoje privatne i intimne podatke na društvenim mrežama i zgroženosti kada njihovi roditelji naiđu na neki od tih podataka. Za Barnes, paradoks privatnosti proizlazi iz toga što su „Odrasli zabrinuti za ugroze privatnosti, dok tinejdžeri slobodno odaju privatne podatke. To se događa jer tinejdžeri često nisu svjesni javne prirode interneta“ (Barnes, 2006: 3). Ubrzo nakon

[14] Ovaj dio poglavlja temelji se na radu Paradoks privatnosti: empirijska provjera fenomena, prihvaćenom za objavu u časopisu *Politička misao*, Vol 56. (2019). br. 1.

Barnesina eseja paradoks privatnosti ušao je u literaturu o privatnosti gdje označava poopćen fenomen, odnosno diskrepanciju između deklariranog izražavanja visoke brige za privatnost i istovremena ponašanja kojim se iskazuje nebriga za privatnost, osobito kada su u pitanju društvene mreže i korištenje interneta.

Paradoks privatnosti kao fenomen istraživan je na brojne načine i u mnogim istraživanjima (Acquisti i Gross, 2006; Anić, Škare i Kursan Milaković, 2016; Berendt, Günther i Spiekermann, 2005; Commission, 2011; Debatin, Lovejoy, Horn i Hughes, 2009; Dienlin i Trepte, 2015; Fogel i Nehmad, 2009; Joinson, Reips, Buchanan i Paine Schofield, 2010; Korzaan i Boswell, 2008; Krasnova, Spiekermann, Koroleva i Hildebrand, 2010; Mohamed i Ahmad, 2012; Son i Kim, 2008; Stutzman, Vitak, Ellison, Gray i Lampe, 2012; Taddei i Contena, 2013; Trepte, Dienlin i Reinecke, 2014; Tufekci, 2008; Utz i Krämer, 2009). Značajan dio istraživanja pokazao je kako postoji određena razina diskrepancije između zabrinutosti za privatnost i objavljivanja određenih podataka na društvenim mrežama. Na primjer, Tufekci je na temelju proučavanja razine otkrivanja osobnih podataka na društvenim mrežama na uzorku studenata zaključio kako „kao i u prethodnim istraživanjima, opća zabrinutost za privatnost nije bila relevantna za odluku o objavi osobnih podataka“ (Tufekci, 2008: 31–33), što jednostavno znači kako nije pronašao povezanost između te dvije varijable, što govori u prilog postojanju paradoksa privatnosti. Naime, intuitivno bi bilo za očekivati da će postojati barem umjerena negativna korelacija između njih, odnosno da će zabrinutost za privatnost biti prediktor vjerojatnosti objavljivanja osobnih podataka na način da će pojedinci koji su zabrinutiji za privatnost biti manje skloni objavljivati osobne podatke u usporedbi s pojedincima koji su manje zabrinuti za privatnosti. Međutim, ni u nešto novijem istraživanju Taddei i Contene (2013) nije pronađena veza između zabrinutosti za privatnost i samoobjavljivanja osobnih podataka. U vrlo opsežnom istraživanju o korištenju Facebooka, Acquisti i Gross (2006) su, između ostaloga, provjeravali i povezanost mjera zabrinutosti za privatnosti i konkretnih osobnih podataka koje su sudionici objavljivali na Facebooku te nisu pronašli vezu između zabrinutosti za privatnost i vjerojatnosti objave osobnih podataka na svojem profilu (Acquisti i Gross, 2006). Njihovi rezultati sugeriraju kako stavovi o privatnosti i zabrinutost za privatnost imaju određeni utjecaj na to hoće li se pojedinci uopće pridružiti Facebooku, ali jednom kada mu se pridruže utjecaj na objavljivanje osobnih podataka je marginalan. Dapače, pronašli su kako je među sudionicima koji su izražavali najveću zabrinutost za to da bi pet godina od danas netko mogao iskoristiti njihove osobne podatke poput seksualne orijentacije, političkih

opredjeljenja, imena partnera i slično, njih čak 48% imalo navedeno barem svoju seksualnu orijentaciju, 47% barem svoje političke stavove i 21% barem partnerovo ime, a njih čak 16% imalo je navedeno sve navedene podatke, unatoč tome što su izrazili maksimalnu zabrinutost da bi netko u budućnosti mogao doći do tih podataka (Acquisti i Gross, 2006).

Međutim, nisu u svim istraživanjima u kojima je proučavan paradoks privatnosti dobiveni konzistentni nalazi. Dok je u većini istraživanja fenomen potvrđen, u nekim istraživanjima to nije bio slučaj i paradoks privatnosti nije potvrđen. Na primjer, Krasnova i sur. utvrdili su kako je percipirani rizik privatnosti, varijabla koja u određenoj mjeri odgovara zabrinutosti za privatnost, negativno korelirana s aktivnosti i objavljivanjem podataka na društvenim mrežama (Krasnova i dr., 2010). Analizirajući metodološke i teoretske pristupe u istraživanjima paradoksa privatnosti Dienlin i Trebke (Dienlin i Trepte, 2015) došli su do zaključka kako na pojavu paradoksa privatnosti može utjecati različita operacionalizacija privatnosti, osobito ona višedimenzionalna kako ju je predložila Burgoon (Burgoon, 1982), odnosno fizička, društvena, psihološka i informacijska privatnost. Stoga su na temelju provedenog istraživanja zaključili kako je paradoks privatnosti fenomen koji je i dalje prisutan ukoliko se istraživanje metodološki provode na način kao što su provedena i ranija istraživanja u kojima je potvrđen, a koji oni smatraju višestruko manjkavim. Međutim, utvrdili su kako paradoks privatnosti nestaje kada se u nacrtu istraživanja razluči između mjera zabrinutosti za privatnost i stavova o privatnosti, kada se za operacionalizaciju teoretskog okvira koristi teorija planiranog ponašanja (Ajzen, 1991) te kada se koriste višedimenzionalne mjere privatnosti, kako je predložila Burgoon.

Kako bi bilo moguće odgovoriti na postavljeni istraživački problem, odnosno kako bi bilo moguće testirati istraživačku hipotezu i provjeriti postojanje paradoksa privatnosti, bilo je potrebno izmjeriti deklariranu važnost privatnosti te, još važnije, lakoću kojom su je se sudionici spremni odreći. U provedenom istraživanju, dijelom su uvažene spoznaje Dienlina i Trebke te je za operacionalizaciju varijabli kojima je mjerena zabrinutost za privatnost te ponašanje sudionika korišteno više različitih mjera.

4.2.1.1. Mjerenje zabrinutosti za privatnost

Važnost privatnosti moguće je mjeriti na razne načine. Jedan od njih jest uz pomoć korištenja jedne jedine čestice, jednostavnim direktnim pitanjem sudionika. Takav je pristup korišten i u ovom istraživanju, kao jedan od načina mjerenja važnosti privatnosti. Međutim, budući da je za mjerenje kompleksnih psiholoških konstrukata, kakav privatnost svakako jest, korištenje

samo jedne čestice vrlo nepouzdano, istovremeno smo koristili više različitih mjera utemeljenih na postojećim skalama, ali i na podacima prikupljenima u predistraživanju. Zbog različitih konceptualizacija privatnosti, ali i zbog dinamične prirode konstrukta s obzirom na razvoj tehnologije i društveno-kontekstualne faktore, postoje brojni modeli za mjerenje zabrinutosti za privatnost, od vrlo sličnih do sasvim različitih u svojoj prirodi (Buchanan, Paine, Joinson i Reips, 2007; Dinev i Hart, 2004; Malhotra, Kim i Agarwal, 2004; Smith, Milberg i Burke, 1996; Xu, Dinev, Smith i Hart, 2011). Detaljnije će biti prikazani samo oni koji su u značajnije utjecali na izradu mjera korištenih u ovom istraživanju.

U razdoblju od 1978. do 2004. godine, jedan od najznačajnijih autora o privatnosti, Alan Westin, proveo je preko trideset istraživanja privatnosti te je konstruirao više mjera privatnosti kako bi mogao mjeriti trendove i promjene u zabrinutosti za privatnost koju su sudionici iskazivali (Kumaraguru i Cranor, 2005). U većini istraživanja sudionike je prema njihovim odgovorima svrstavao u jednu od tri kategorije, fundamentaliste, pragmatike i nezainteresirane. Prema preglednom radu Westinovih istraživanja Kumaraguru i Cranor, fundamentaliste je opisao kao osobe nepovjerljive prema organizacijama koje ih traže osobne podatke, kao one koji smatraju kako bi pojedinci trebali biti proaktivniji u zaštiti svoje privatnosti te osobe koje podržavaju snažnije reguliranje privatnosti pojedinaca. Nezainteresirane za privatnost opisao je kao osobe koje ne znaju čemu sva ta strka oko privatnosti, kao osobe koje zagovaraju prednosti koje proizlaze iz objave i dijeljenja osobnih podataka te koje ne vide potrebu za nametanjem zaštite privatnosti. Konačno, pragmatike je opisao kao osobe koje pažljivo odvaguju osobne i društvene prednosti i nedostatke koji proizlaze iz objave i dijeljenja određenih osobnih podataka s različitim tvrtkama i državnim institucijama. Iako se postotak s vremenom mijenjao, Westin je koristeći različite mjere dobivao slične rezultate i to kako je u američkom društvu oko 25-35% fundamentalista, 10-20% nezabrinutih i 55-65% umjerenih pragmatika. Konkretne čestice kao i metodologija koju je Westin koristio nisu prikladne za mjerenje privatnosti u današnjem kontekstu, ali njegov je rad inspirirao naredne pokušaje mjerenja privatnosti, a time i anketu korištenu u ovom istraživanju.

Jedan od vjerojatno najznačajnijih pokušaja mjerenja zabrinutosti za privatnost bio je instrument zabrinutosti za informacijsku privatnosti CFIP (eng. *Concern For Information Privacy*) kojeg su nakon opsežnog i sustavnog rada formirali i validirali Smith i suradnici još 1996. godine (Smith i dr., 1996). CFIP, odnosno instrument zabrinutosti za informacijsku privatnost, sadrži 15 čestica koje u prvom redu tvore četiri korelirana faktora: prikupljanje,

greške, naknadno korištenje i nedopušteni pristup. Naime, Smith i suradnici su nakon višegodišnjeg rada zaključili kako pojedinci koji na značajan način iskazuju zabrinutost za informacijsku privatnost imaju osjećaj da se previše njihovih podataka prikuplja, brinu da je značajan dio prikupljenih podataka u bazama netočan ili nedovoljno precizan, vjeruju da se prikupljeni podaci koriste na nedopušteni način i da se nedovoljno dobro njihove podatke štiti od mogućeg neovlaštenog pristupa. Na uzorku od 355 sudionika, 2002. godine Stewart i Segars empirijski su potvrdili, ali i poboljšali psihometrijska svojstva instrumenta (Stewart i Segars, 2002). Zaključili su i kako se CFIP zapravo može bolje izraziti kao faktor drugog reda. Pritom su pronašli kako je korelacija između faktora prikupljanje u prvom redu i latentnog konstrukta CFIP relativno visokih r=0.72, što je relevantno za ovaj rad budući da će za mjerenje zabrinutosti za privatnost iz CFIP-a biti korištene samo čestice faktora *prikupljanje*. Budući da je CFIP konstruiran 1996. godine, odražavao je tadašnji pogled na privatnost, i tadašnji pogled na ugroze privatnosti. Široka dostupnost interneta, koja je tih godina tek započela, kao i pojava društvenih mreža i modernih marketinških alata, o kojima je opširno pisano u drugom poglavlju, značajno je utjecala na način prikupljanja i obrade osobnih podataka. Rani pokušaj svojevrsne prilagodbe CFIP-a za korištenje u internetskom okruženju napravili su Malhotra i suradnici 2004. godine (Malhotra i dr., 2004). Naziv njihova konstrukta bio je IUIPC, odnosno zabrinutost internetskih korisnika za informacijsku privatnost (eng. *Internet Users' Information Privacy Concerns*). Postavili su i kauzalni model koji je uključivao kontekstualno specifične faktore poput *povjerenja* i *rizika* te kao svojevrsni kriterij *bihevioralne namjere*. Njihov model pretpostavlja kako na latentni faktor zabrinutosti za privatnost, odnosno u njihovu slučaju IUIPC, utječu nešto drugačiji faktori prvog reda, a to je ponovo bio faktor *prikupljanje osobnih podataka*, pri čemu su koristili gotovo identične čestice kao i CFIP te nešto drugačiji faktori *kontrole nad osobnim podacima* i *svijesti o načinima na koje tvrtke postupaju s privatnim podacima*. Iako je model koji su predstavili Malhotra i suradnici u teoretskom smislu bio na dobrom tragu, osobito u dijelu u kojem su uzeli u obzir kontekstualne faktore poput rizika i povjerenja, čini se da nisu dovoljno pažnje posvetili formiranju skale i njihov indeks nije pridobio značajniju podršku istraživača u području privatnosti.

Paine i suradnici (Paine, Reips, Stieger, Joinson i Buchanan, 2007) prepoznali su kako ključni indeksi i skale zabrinutosti za privatnost naglasak stavljaju isključivo na jedan aspekt privatnosti, na informacijsku privatnost. U svojem su radu bili ohrabreni skeptičnom analizom Singeltona i Harpera, koji su napravili pregled 23 studije privatnosti s naglaskom na nedostatke

tih istraživanja te na ograničenja pri interpretaciji i generalizaciji rezultata (Singleton i Harper, 2002). Unatoč vrlo skeptičnom tonu kojim je članak pisan, Singelton i Harper izuzetno su dobro potkrijepili svoje argumente, a određeni uvidi potpuno su pogođeni. Njihova upozorenja korištena su i pri konstrukciji ankete u ovom istraživanju. Isto su učinili i Paine i suradnici te su u istraživanju privatnosti željeli postavljati otvorena pitanja kako bi prikupili podatke o tome što doista brine sudionike kada govore o privatnosti, čega se doista boje i do čega im je doista stalo. Sudionicima su pristupili putem računalne aplikacije za čavrljanje ICQ na način da su programirali računalni bot koji je komunicirao s korisnicima temeljem unaprijed zadanih smjernica te ih je ispitivao o njihovoj zabrinutosti za privatnosti te o njihovim ponašanjima koja poduzimaju kako bi zaštitili svoju privatnost (Paine i dr., 2007). Između ostaloga, na temelju dobivenih rezultata zaključili su kako sudionici nisu zabrinuti samo za informacijsku privatnost, već i za druge oblike ugrožavanja privatnosti kao što je dobivanje neželjene pošte ili čak napadi računalnim virusima. Uvažavajući njihove spoznaje, kao i argumente Harpera i Singeltona, Buchanan i suradnici formirali su svoju mjeru zabrinutosti za privatnosti čije su čestice zahvaćale više dimenzija privatnosti (Buchanan i dr., 2007). U tom su smislu vjerojatno najdalje otišli Burgoon i suradnici koji su testirali svoju teoriju multidimenzionalnosti privatnosti (Burgoon i dr., 1989). Najprije su proveli 43 otvorena intervjua na temelju kojih su izradili upitnik koji su primijenili na 444 sudionika kojim su provjeravali koje su taktike sudionici koristili kako bi osigurali vlastitu privatnosti. Na temelju dobivenih rezultata zaključili su kako se ugroze privatnosti mogu grupirati u pet dimenzija: psihološke i informacijske ugroze poput kritiziranja, ispiranja mozga, uvjeravanja i slično; neverbalne interakcijske ugroze poput ulaženja u nečiji osobni prostor, iskazivanje javnih izraza pažnje; verbalne interakcijske ugroze poput komentiranja nečijeg raspoloženja, izgleda ili ponašanja; fizičke ugroze poput nadziranja ili fizičkog kontakta te neosobne ugroze poput prometne buke, zaprimanja neželjene pošte ili telemarketinga, a svaku od tih dimenzija testirali su i za različite razine odnosa, s liječnikom, nadređenom osobom na poslu, s partnerom, učiteljem, roditeljem i bratom/sestrom. U empirijskom istraživanju pronašli su kako su sudionici privatnima smatrali one situacije koje u većoj mjeri omogućuju slobodnu introspekciju i refleksiju, koje ograničavaju prilike za nadzorom i prisluškivanjem, u kojima se postavlja manje zapreka za slobodno ponašanje, koje minimiziraju nepredviđena uplitanja i koje omogućuju veću kontrolu nad fizičkim prostorom (Burgoon i dr., 1989).

Paradoks privatnosti postuliran je upravo kako bi objasnio razliku između zabrinutosti za privatnost s jedne strane i istovremene visoke razine objavljivanja privatnih podataka na društvenim mrežama s druge strane. Međutim, odricanje od privatnosti, nebriga za privatnost, objavljivanje privatnih podataka ne mora biti manifestirana samo putem društvenih mreža. Dakako, danas je to vjerojatno najzastupljeniji način na koji se ljudi lišavaju svoje privatnosti, ali on nipošto nije jedini. Stoga je jedan od ciljeva ovog istraživanja bio provjeriti postoji li razlika između zabrinutosti za privatnost i određenih bihevioralnih varijabli koje se ne odnose samo na društvene mreže, a kojima se pojedinci odriču svoje privatnosti, ili njima iskazuju nebrigu za vlastitu privatnost. Prilikom konstruiranja mjera zabrinutosti za privatnost, vodili smo se spoznajama, ograničenjima i uvidima iz dosad provedenih istraživanja i validiranih indeksa privatnosti, posebice onima opisanima u ovome poglavlju, ali i spoznajama i rezultatima dobivenim u predistraživanju kroz intervjue sa sudionicima.

4.2.1.2. Bihevioralne varijable

Za provjeru postojanja paradoksa privatnosti, a time i druge istraživačke hipoteze, osim mjera zabrinutosti za privatnost bilo je potrebno na neki način izmjeriti i ponašanje sudionika. Postoje brojni načini na koje se ponašanje sudionika može zabilježiti, od neposrednog opažanja, preko individualnog vođenja dnevnika do mjerenja uz pomoć bihevioralnih skala. Dakako, neposredno opažanje kao metoda ima daleko najveću valjanost, ali izuzetno je zahtjevno za provođenje i potpuno neprikladno za mjerenje ponašanja vezanih uz privatnost. Kao i u većini istraživanja paradoksa privatnosti, za mjerenje ponašanja odabrane su bihevioralne skale budući da ih je jednostavno primijeniti na velikom uzorku sudionika. Koristeći vrlo slične bihevioralne mjere, Acquisti i Gross su usporedbom izjava sudionika o vlastitu ponašanju i neposrednog opažanja njihova ponašanja pronašli kako gotovo 80% sudionika daje točne i iskrene procjene o svojem ponašanju (Acquisti i Gross, 2006). Oni su kao bihevioralne mjere koristili količinu i sadržaj podataka koji se nalaze na Facebook profilima sudionika pri čemu su opažali ime, prezime, fotografiju, adresu, broj telefona i druge osobne podatke, te su kao mjere koristili podatke o otvorenosti profila te aktivnosti na društvenoj mreži Facebook. Takve su mjere vrlo dobre budući da se radi o konkretnom podatku koji je sudionicima najčešće lako dostupan i pogreške u dosjećanju su vrlo male, što su Acquisti i Gross u svojoj naknadnoj validaciji i pokazali. Nadalje, radi se o objektivnim i visoko valjanim pokazateljima koji direktno ukazuju na razinu zaštite privatnosti koju sudionici manifestiraju.

U prethodnom odlomku spomenut je rad Buchanana i suradnika, koji su željeli konstruirati robusnu i pouzdanu mjeru zabrinutosti za privatnost i bihevioralne mjere privatnosti koje bi se mogle primjenjivati putem interneta (Buchanan i dr., 2007). Pritom su posebni naglasak stavili na širu definiciju privatnosti koja osim informacijske privatnosti obuhvaća i sve ostale različite teoretske aspekte privatnosti poput pristupa podacima, fizičke privatnosti, izražajne privatnosti pa i mogućih prednosti odricanja privatnosti. Temeljem postojeće literature i istraživanja odabrali su set od 82 čestice među kojima su neke preuzeli iz prethodnih istraživanja, a neke su sami osmislili. Trideset i četiri čestice ticale su se ponašanja povezanog s privatnosti (na primjer, *Brišete li redovito povijest pretraživanja u svojem internetskom pregledniku*), a odgovori su prikupljani na skali od nikada do uvijek. Nakon što su proveli istraživanje, čestice su obradili faktorskom analizom, a nakon primjene Saucierova kriterija za povećanje čistoće faktora pronašli su dva bihevioralna faktora s po šest čestica koje su nazvali faktor *općeg opreza* i faktor *tehničke zaštite*.

Promišljajući o načinima neutraliziranja i opiranja tzv. novom nadzoru, kako je opisao određene eksterne ugroze privatnosti, Marx je opisao jedanaest osnovnih bihevioralnih odgovora na te ugroze (G. T. Marx, 2003). Unatoč tome što svoja teoretska promišljanja nije empirijski testirao, inspirirao je druge autore prilikom izrade bihevioralnih skala. Jedan od njih je i Park koji je konstruirao skalu od osam čestica za *društvenu dimenziju ponašanja vezanog za privatnost* te četiri čestice za *tehničku dimenziju ponašanja vezanih uz privatnost* (Park, 2013), a koja se u značajnoj mjeri poklapa s Buchananovim faktorom tehničke zaštite. Upravo je rad Parka i Buchanana i suradnika najviše utjecao na izradu bihevioralnih mjera privatnosti koje su korištene u ovom istraživanju.

4.2.2. Postupak

Istraživanje je provedeno primjenom ankete u razdoblju od 29.6. do 16.7.2017. godine putem internetskog servisa *Google Docs*, odnosno *Google Forms*. Poziv za sudjelovanjem u istraživanju poslan je putem elektroničke pošte i društvenih mreža većem broju osoba i postavljen je na nekoliko otvorenih i zatvorenih korisničkih grupa na društvenih mrežama, a osim poveznice na anketu sadržavao je i molbu za daljnjim dijeljenjem poziva. Sukladno tome, možemo reći kako se radi o prigodnom uzorku, pri čemu valja istaknuti kako je posebna pozornost bila usmjerena na pozivanje različitih skupina sudionika kako bi se u što većoj mjeri i sukladno mogućnostima pokušalo približiti reprezentativnom uzorku.

4.2.2.1. Metoda

Sama anketa sadržavala je nekoliko sastavnih dijelova[15]. Najprije, za mjerenje privatnosti u provedenom istraživanju upotrijebljena je samo jedna čestica i to *Koliko Vam je važna Vaša privatnost?* za koju su sudionici procjenjivali važnost na skali Likertova tipa s pet stupnjeva koji su se kretali od *nimalo mi nije važna* do *izrazito mi je važna*. Nakon nje nalazila se čestica *Koliko ste zadovoljni razinom privatnosti koju uživate?*. Nadalje, temeljem opisane literature i spoznaja iz predistraživanja formirane su ukupno 22 čestice koje su sadržajno grupirane u četiri kategorije, *briga o privatnosti*, *pristup podacima o sebi*, *vjerovanje u ljudsku prirodu* te *stavovi o privatnosti*. Tim je česticama pridodan modificirani faktor *prikupljanje* iz CFIP-a koji se sastoji od četiri čestice (Smith i dr., 1996). Faktor prikupljanje iz CFIP-a modificiran je na način da su čestice koje ga čine prevedene te je iz svake izostavljena riječ *tvrtke/kompanije* (eng. companies), čime su čestice uopćene na generalnu zabrinutost za prikupljanje podataka. Drugi faktori iz CFIP-a nisu primijenjeni radi ekonomičnosti primjene cijelog upitnika. Uostalom, sadržaj ostalih faktora CFIP-a ionako je znatno više usmjeren na način na koji tvrtke postupaju s osobnim podacima nego na samu zabrinutost za privatnost. Unatoč tome što je CFIP zamišljen kao latentni konstrukt i mjera drugog reda, Stewart i Segars pokazali su kako je korelacija faktora prikupljanje s faktorom nedopuštenog pristupa i naknadnog korištenja r=0.44, a s faktorom grešaka r=0.42 (Stewart i Segars, 2002), što znači da faktori međusobno dijele relativno niskih 20% varijance u čemu se očituje opravdanje za korištenje tek pojedinog faktora. Čestice iz pojedinih faktora međusobno su izmiješane, a svih 26 čestica provjeravano je pomoću skale likertova tipa s pet stupnjeva pomoću kojih su sudionici određivali svoje slaganje s pojedinom tvrdnjom u rasponu od *uopće se ne slažem* do *u potpunosti se slažem*.

U idućem dijelu sudionike se tražilo da na modificiranoj skali socijalne udaljenosti odrede za različite kategorije privatnih podataka (podaci o zaposlenju, biografski podaci, antropomentrijski podaci, vrijednosti i stavovi, podaci o lokaciji, podaci o ljubavnim vezama, medicinski podaci i financijski podaci) označe s kojim su ih sve osobama i institucijama spremni podijeliti, a ponuđeni odgovori bili su Ni sa kime, s partnerom/icom, s članom obitelji, s prijateljem, s poznanikom, s nepoznatom osobom, s privatnim tvrtkama, s državnim institucijama. Naime, tijekom provođenja intervjua prikupljeni su podaci o tome kako određeni sudionici različito vrednuju pojedine kategorije podataka te kako postoje značajne razlike u tome s kime su spremni podijeliti pojedine privatne podatke. Kao što je ranije opisano, sličnu

[15] Potpuni prikaz ankete korištene u istraživanju nalazi se u prilogu 1.

ideju imali su Burgoon i suradnici (Burgoon i dr., 1989) kako bi provjerili eventualno postojanje razlika u različitim dimenzijama privatnosti s obzirom na nekoliko različitih kategorija odnosa.

Potom se pristupilo mjerenju ponašanja i ono je mjereno na dva načina. Najprije je primijenjeno ukupno 17 čestica koje su predstavljale različita ponašanja te se od sudionika tražilo da procijene koliko su često u posljednjih šest mjeseci postupili na pojedini način, a to su označavali na skali od pet stupnjeva koji su bili u rasponu od *niti jednom* do *vrlo često*. Čestice su dijelom preuzete iz opisanih istraživanja Buchanana i suradnika (Buchanan i dr., 2007) i Parka (Park, 2013), no za razliku od načina na koji su oni primijenili svoje čestice, u ovom je istraživanju naglašen vremenski rok od posljednjih šest mjeseci za koji su sudionici trebali procijeniti čestinu kojom su postupili na određeni način. Od ukupno 17 čestica, prvih šest čestica izabrane su između ukupno osam čestica bihevioralne mjere *društvene dimenzije kontrole ponašanja* koju je Park koristio. Posljednje dvije Parkove čestice nisu upotrijebljene jer je prema diskrecijskoj procjeni donesen zaključak kako bi varijanca odgovora na te dvije čestice bila premalena, odnosno da one po svome sadržaju ne odgovaraju predmetu ispitivanja i društveno-kulturalnim običajima u Hrvatskoj. Nadalje, osim šest čestica preuzetih iz Parkova faktora društvene dimenzije kontrole ponašanja, naredne tri čestice preuzete su iz Buchananova faktora *općeg opreza*, a idućih pet iz njegova faktora *tehničke zaštite* (Buchanan i dr., 2007). Preostale tri čestice iz faktora općeg opreza kao i preostala čestica iz faktora tehničke zaštite nisu korištene iz istih razloga zbog kojih su izostavljene i pojedine čestice iz Parkovog faktora. Posljednje tri čestice kojima je mjereno ponašanje formulirane su samo za ovo istraživanje temeljem intervjua provedenih u predistraživanju. Na taj je način konstruirana bihevioralna skala od ukupno sedamnaest čestica.

Nadalje, kao mjere zaštite privatnosti korišteni su objektivni podaci o korištenju internetskih pretraživača, servisa za elektroničku poštu, prisustva na društvenim mrežama, otvorenosti profila na društvenoj mreži te konkretnih podataka koje sudionici imaju navedene na svojem profilu. Za korištenje tražilica, servisa za elektroničku poštu, i društvenih mreža sudionicima je ponuđeno nekoliko najčešćih odgovora i opcija da sami navedu svoj odgovor. Za pitanje otvorenosti profila ponuđene su opcije koje nudi Facebook (prijatelji, prijatelji prijatelja ili javnost) te je ponuđena opcija za odabir *nitko, koristite lažni profil* i *ne koristim društvene mreže*. Konačno, sudionicima je ponuđeno da označe svaki osobni podatak koji je naveden na profilu bilo koje od društvenih mreža koje koriste, a ponuđeni su podaci *pravo ime, pravo prezime, adresa stanovanja, broj telefona ili mobitela, e-adresa, fotografija, podaci o*

školovanju, podaci o zaposlenju, religijski ili politički stavovi, pripadnost klubovima, udrugama i/ili inicijativama, omiljene knjige, filmovi, glazba ili ideje koje podržavate i opcija *ne koristim društvene mreže*. Takve su mjere vrlo dobre budući da se radi o konkretnom podatku koji je sudionicima najčešće lako dostupan i pogreške u dosjećanju su vrlo male, što su Acquisti i Gross u svojoj naknadnoj validaciji i pokazali (Acquisti i Gross, 2006).

U idućem se dijelu od sudionika tražilo da za nekoliko kategorija podataka i oblika komunikacije (telefonski razgovori, dopisivanje i razgovori putem mobilnih aplikacija, sadržaj e-pošte, fotografije na mobitelu ili računalu, dokumenti i podaci pohranjeni u oblaku, praćenje lokacije mobilnog telefona, podaci zaštićeni snažnom enkripcijom te gledanje kroz kameru na mobilnom telefonu ili računalu) odrede tko im sve, prema njihovu mišljenju, može pristupiti, a ponuđeni odgovori bili su *Nitko, ti podaci su za sada sigurni, hrvatska policija i obavještajne službe na temelju odgovarajućeg naloga, određene strane policije i obavještajne službe, pružatelji internetskih usluga te hakeri ili vješti korisnici*. Ovaj dio upitnika konstruiran je isključivo za potrebe provedenog istraživanja kako bi se mogla procijeniti informiranost sudionika o mogućnostima i kapacitetima mogućeg nadzora i narušavanja privatnosti.

Zaključno, od sudionika je prikupljeno nekoliko osnovnih demografskih podataka poput dobi, spola, najvišeg završenog stupnja obrazovanja te ih s tražilo da na skali od devet stupnjeva odrede svoju političku pripadnost pri čemu je jedan označavao *lijevo*, a devet *desno*.

4.2.3. Rezultati

Po završetku provođenja istraživanja, sudjelovanje u anketi je onemogućeno te su podaci preuzeti u formatu .xls radi daljnje obrade. Inicijalna priprema podataka napravljena je u programu Microsoft Excel te su potom podaci uvezeni u program za statističku obradu podataka SPSS v. 23 u kojem je napravljena daljnja obrada i statistička analiza.

4.2.3.1. Sociodemografski podaci

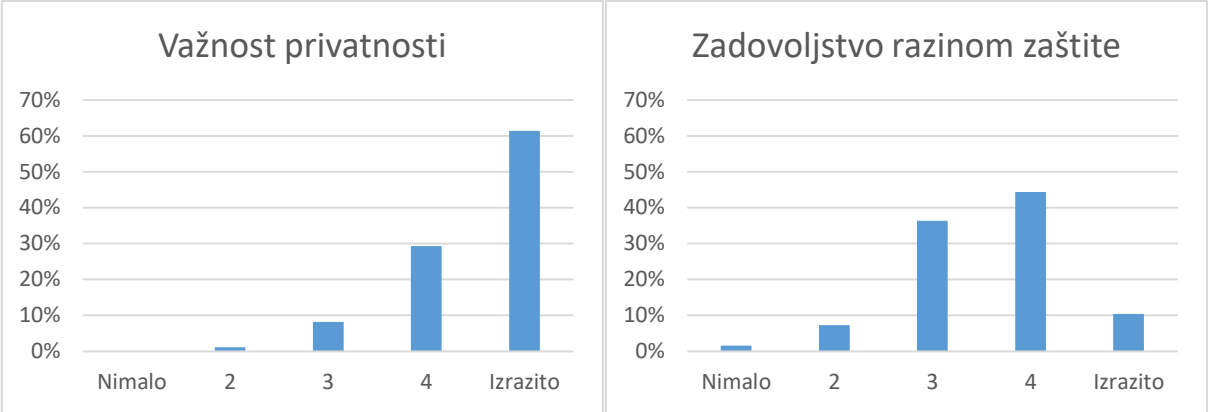
Budući da servis *Google Forms* evidentira jedino u potpunosti ispunjene ankete, ne raspolažemo podatkom koliko je osoba pristupilo ispunjavanju ankete, ali u predviđenom vremenskom rasponu anketu je u potpunosti ispunilo 975 sudionika. Budući da je na nekoliko pitanja postojala mogućnost slobodnog unosa odgovora, u inicijalnoj obradi podataka pregledani su svi uneseni podaci te su sudionici koji su davali očigledno neiskrene ili provokativne odgovore izbačeni iz uzorka te je konačni uzorak sadržavao ukupno 966

sudionika, odnosno 721 sudionicu (74,6%) i 245 sudionika (25,4%). Što se tiče obrazovanja, najveći dio sudionika imao je završen diplomski ili dodiplomski studij (55,4%), zatim srednju školu (17%), preddiplomski studij ili višu školu (12,9%), doktorski studij (7,2%), poslijediplomski specijalistički ili znanstveni magisterij (6,8%) te osnovnu školu (0,6%). Dob sudionika kretala se u velikom rasponu od 14 do 75 godina, prosječna dob bila je 35,86 godina uz standardnu devijaciju od 10,91, a medijan je bio 34 godine. Izjašnjavajući se o političkim preferencijama, prosječna vrijednost uzorka na skali od 1 do 9 bila je 4,33 uz standardnu devijaciju 2,05. Slikovito, 49,5% sudionika odabralo je jednu od četiri opcije s lijeve strane političkoga spektra, čak 26,9% odabralo je broj 5 koji je označavao samu sredinu, a preostalih 23,6% odabralo je jednu od četiri opcije s desne strane političkog spektra.

Unatoč tome što cilj ovog istraživanja nije bilo poopćavanje rezultata s reprezentativnog uzorka na populaciju te je korišten prigodni uzorak, karakteristike uzorka treba uzeti u obzir pri interpretaciji rezultata. Naime, radi se o istraživanju stavova i određenih specifičnih ponašanja na koja bi mogle utjecati sociodemografske varijable poput spola, dobi i obrazovanja. U tom smislu, valja naglasiti kako uzorak sudionika u ovom istraživanju, u usporedbi s populacijom hrvatskih građana, ima značajno veći udio osoba ženskog spola, uzorak je nešto mlađi od hrvatskoga prosjeka te je struktura obrazovanja uzorka znatno viša od hrvatskog prosjeka (Burušić, 2013; Grizelj, 2016). Ne računajući osobe sa završenim preddiplomskim studijem ili višom školom, čak 69,4% uzorka ima završen diplomski ili dodiplomski studij, a među njima je i čak 14% osoba sa završenim nekim stupnjem poslijediplomskog obrazovanja te čak 7,2% doktora znanosti. Pri interpretaciji rezultata posebna će se pozornost obratiti na uvažavanje karakteristika uzorka, koje u većoj mjeri odstupaju od hrvatskoga prosjeka.

4.2.3.2. Zabrinutost za privatnost

Osnovni cilj istraživanja bio je utvrditi usklađenost stavova i ponašanja vezanih uz privatnost. Konkretno, kako bi bilo moguće odgovoriti na istraživačku hipotezu bilo je potrebno najprije izmjeriti deklariranu zabrinutost za privatnost kako bi je se moglo dovesti u vezu s ponašanjima koje sudionici manifestiraju. Kao što je ranije detaljno opisano, zabrinutost za privatnost mjerena je na više načina. Najprije, važnost privatnosti i zadovoljstvo razinom zaštite privatnosti testirani su pomoću samo jedne čestice te je za važnost privatnosti dobivena vrijednost M=4,5; SD=0.7, a za zadovoljstvo razinom zaštite M=3,54; SD=0,83. Ukupni postotak odabira pojedinih odgovora prikazan je u grafovima u nastavku.



Slika 3 - Udjeli odgovora na pitanje o procjeni važnosti privatnosti i zadovoljstva razinom zaštite privatnosti

Rezultati sugeriraju kako je sudionicima u istraživanju njihova privatnost izrazito važna te kako su uglavnom zadovoljni razinom zaštite privatnosti koju uživaju.

Nadalje, kao što je ranije opisano, sudionicima su prezentirane 22 čestice, sadržajno grupirane u četiri kategorije: brigu o privatnosti, pristup podacima o sebi, vjerovanje u ljudsku prirodu te stavove o privatnosti. Tim je česticama pridodan i faktor *Prikupljanje* iz CFIP-a. Negativno formulirane čestice najprije su rekodirane te je nad svakom zasebnom kategorijom provedena faktorska analiza koja ima zadovoljavajuće rezultate, detaljno prikazane u dodatku disertacije. Osim toga, mjera unutarnje konzistencije Cronbach alfa ima zadovoljavajuće razine za sve faktore.

Budući da je postojala teoretska pretpostavka da bi i pojedine čestice iz kategorije *pristup podacima o sebi* mogle mjeriti *zabrinutost za privatnosti*, provedena je nova, eksploratorna, faktorska analiza nad sve 22 čestice. Napravljena je rotacija faktora Varimax metodom koristeći Kaiser normalizaciju te je faktorskom analizom ekstrahirano ukupno sedam faktora, od kojih su samo dva bila teorijski smislena i ujedno su imala zadovoljavajuće razine faktorskih zasićenja (vidi tablicu 2.)

Ukupan rezultat na pojedinom faktoru izračunat je kao prosjek odgovora na pojedinim česticama koje sačinjavaju taj faktor pri čemu su odgovori mogli biti u teoretskom rasponu od 1 do 5. Na taj način izračunata prosječna vrijednost na faktoru Zabrinutosti za privatnost bila je 3,33, a na faktoru CFIP bila je 3,79. Takvi rezultati sugeriraju kako su sudionici umjereno zabrinuti za svoju privatnost.

Tablica 2. - prikaz faktorskih zasićenja i mjera unutarnje konzistencije

Sadržaj čestice	Faktorsko zasićenje
Zabrinutost za privatnost	α=,678
Općenito, zabrinut/a sam za svoju privatnost.	,474
Smatram kako davanje osobnih podataka drugima nosi sa sobom određene rizike.	,331
Bojim se da bi neovlaštene osobe mogle pristupiti mojim osobnim podacima.	,383
U usporedbi s drugima, manje sam osjetljiv/a na način na koji se koriste moji osobni podaci.	,710
Kamere na javnim površinama i u trgovinama uopće mi ne smetaju.	,676
Većina tvrtki vrlo pažljivo postupa s privatnim podacima svojih korisnika.	,391
Nemam ništa protiv da se anonimni podaci o meni koriste kako bih dobivao/la preciznije reklame.	,331
Vjerovanje u ljudsku prirodu	α=,646
Ljudi su po svojoj prirodi dobronamjerni.	,749
Postoje stvari koje ne želim ni sa kime podijeliti.	,316
Mnogi ljudi se hrane tuđim slabostima.	,759
Većina ljudi okoristit će se tuđim tajnama ako im se ukaže prilika.	,773
CFIP – faktor prikupljanje	α=,755
Obično me smeta kada me se traži moje osobne podatke	,785
Kada me se traži davanje osobnih podataka, ponekad razmislim dvaput prije nego što ih pružim.	,714
Smeta me davati osobne podatke na toliko mjesta.	,832
Zabrinut/a sam da se prikuplja previše podataka o meni.	,708

Međutim, taj nam podatak ne pomaže mnogo u odgovoru na istraživačku hipotezu. Kako bi bilo moguće testirati istraživačku hipotezu, odnosno postojanje diskrepancije između visoke zabrinutosti za privatnost i ponašanja kojim se odriče privatnosti, bilo je potrebno sudionike podijeliti u skupine temeljem njihove zabrinutosti za privatnost. Koristeći sličnu metodologiju kakvu je za formiranje različitih *Indeksa potrošačke zabrinutosti za privatnost* u svojim istraživanjima koristio Westin (Kumaraguru i Cranor, 2005), sudionike smo prema njihovim odgovorima svrstavali u jednu od tri skupine: fundamentaliste, pragmatike i nezainteresirane.

Slično kao što je činio Westin, sudionike smo kategorizirali prema broju čestica na koje su dali odgovore kojima ukazuju na visoku zabrinutost za privatnost. Konkretno, budući da je u istraživanju korištena skala Likertova tipa s pet razina, kao visok odgovor smatrani su odgovori 4 i 5, koji opisno odgovaraju frazama *slažem se* i u *potpunosti se slažem*. S obzirom da je ranije provedena faktorska analiza kojom je točno utvrđeno koje čestice na odgovarajući način čine latentnu strukturu zabrinutosti za privatnost, prilikom tipologiziranja sudionika korištene su

upravo čestice faktora zabrinutosti za privatnost. U kategoriju *fundamentalista* dodani su sudionici koji su dali visoke odgovore na 5, 6 ili svih sedam mogućih čestica, u kategoriju *nezainteresiranih* oni koji su na samo jednu česticu dali visoki odgovor ili pak nisu ni na jednu česticu dali visoki odgovor, dok su *pragmaticima* označeni svi ostali. Isto smo načelo primijenili i na faktor zabrinutosti CFIP-a te smo fundamentalistima označili osobe koje su na sve četiri čestice dale visoke odgovore, nezainteresiranima one koji ni na jednu nisu dali visoku odgovor, a pragmaticima one koji su na jednu, dvije ili tri čestice dali visoki odgovor (vidi tablicu 3.)

Tablica 3. - prikaz rasporeda sudionika prema broju čestica na koje su dali visoki odgovor

	Zabrinutost za privatnost		CFIP - prikupljanje		Westin
	Br. čestica na koje su dali visoki odg.	Udio sudionika	Broj čestica	Udio sudionika	Udio sudionika
Fundamentalisti	5, 6 ili 7	23%	4	33%	25% - 34 %
Pragmatici	2, 3 ili 4	58%	1, 2 ili 3	49%	55% - 64%
Nezainteresirani	0 ili 1	19%	0	18%	8% - 25%

Raspored sudionika u kategorije ugrubo odgovara postotcima koje je u svojim brojnim istraživanjima dobivao i sam Westin (Kumaraguru i Cranor, 2005).

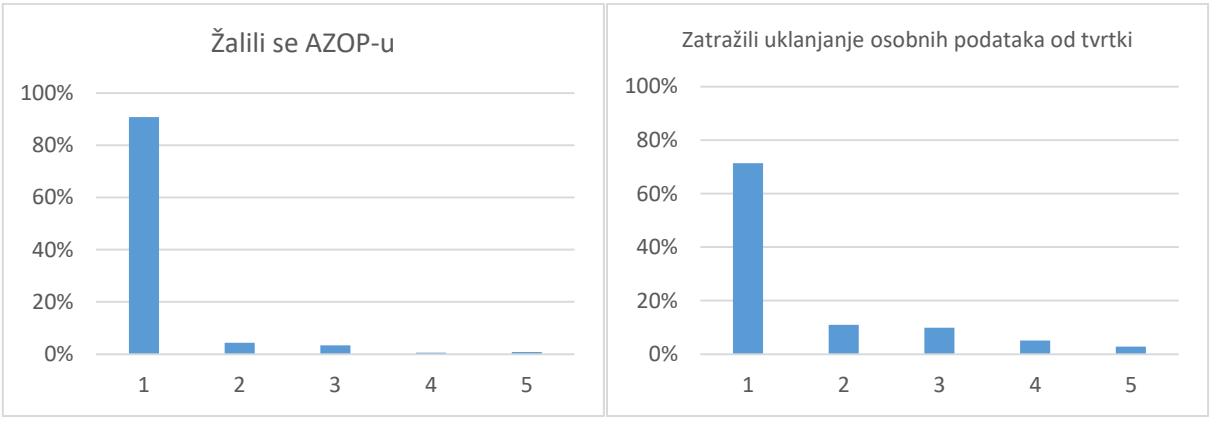
Statistički značajne razlike u spolu nisu pronađene niti na faktoru Zabrinutosti za privatnost ($t = -1{,}670$; $df = 964$; $p > 0{,}05$) niti na faktoru CFIP – prikupljanje ($t = -0{,}101$; $df = 964$; $p > 0{,}05$), što znači da se muškarci i žene ne razlikuju u svojem rezultatu na tim faktorima. Nadalje, nije pronađena ni statistički značajna korelacija dobi i rezultata na faktorima Zabrinutosti za privatnost ($r = 0{,}022$; $N = 965$) i CFIP – prikupljanje ($r = 0{,}047$; $N = 965$), što znači da dob nije ni na koji način povezana s rezultatom na pojedinom faktoru.

Razlike u rezultatu između sudionika s različitim obrazovanjem provjeravane su uz pomoć analize varijance na način da su od ukupno šest kategorija najprije stvorene četiri: srednja škola ili niže, preddiplomski studij, diplomski studij i postdiplomski studij. Utvrđeno je kako različit stupanj obrazovanja nije statistički značajno utjecao na razlike na faktoru CFIP – prikupljanje, dok je na faktoru Zabrinutosti za privatnost pronađen statistički značajan utjecaj ($F(3,962) = 3{,}128$; $p < 0.05$), a Scheffeovim post-hoc testom utvrđeno je kako je jedina pronađena statistički značajna razlika između sudionika koji su završili postdiplomski studij u odnosu na sudionike koji su završili diplomski studij na način da su prvi imali viši rezultat.

4.2.3.3. Bihevioralne mjere

Nakon što su utvrđene mjere zabrinutosti za privatnost, kako bismo testirali paradoks privatnosti, bilo je potrebno na odgovarajući način izmjeriti ponašanje sudionika. Kao što je ranije detaljno pojašnjeno, za to je korišteno nekoliko bihevioralnih mjera. Konkretno, korištena su tri modificirana faktora i to *društvena dimenzija kontrole ponašanja*, *opći oprez* i *tehnička zaštita*, te dodatne tri čestice osmišljene na temelju intervjua u predistraživanju (tablica 4.)

Kao što je ranije opisano, od ukupno osam čestica koliko je obuhvaćao Parkov faktor *društvena dimenzija ponašanja vezanog za privatnost*, u istraživanju je zbog procjene kako ne bi zadovoljile psihometrijske karakteristike korišteno samo prvih šest čestica. Nad tih je šest čestica provedena faktorska analiza koja je rezultirala s dva latentna faktora. Uvidom u faktorska zasićenja utvrdili smo kako su drugi, neočekivani, faktor zapravo činile dvije čestice i to (koliko ste puta u posljednjih šest mjeseci) *Požalili Agenciji za zaštitu osobnih podataka zbog narušavanja Vaše privatnosti?* i *Zatražili od neke tvrtke ili internetskog servisa da ukloni ili obriše Vaše osobne podatke koji su javno objavljeni ili koje imaju u svojoj evidenciji?*. Uvidom u strukturu odgovora na navedenim česticama utvrdili smo kako zbog nedovoljno velike varijance odgovora nemaju odgovarajuće psihometrijske karakteristike da bi se koristile u daljnjoj analizi (slika 4.)



Slika 4. - Udjeli odgovora na pitanja o učestalosti podnošenja žalbi AZOP-u i podnošenja zahtjeva za uklanjanjem osobnih podataka od tvrtki pri čemu 1 označava odgovor uopće se ne slažem, a 5 označava odgovor u potpunosti se slažem

Ovakve rezultate očekivali smo na dvije čestice koje smo izostavili iz istraživanja te smo stoga iz daljnje obrade izostavili i ove dvije čestice. Faktorska analiza stoga je provedena na preostale

četiri čestice te je dobiven jedan faktor sa zadovoljavajućom pouzdanosti i psihometrijskim karakteristikama.

Nadalje, nad pet čestica Buchananova faktora tehničke zaštite provedena je faktorska analiza te je dobiven jedan faktor sa zadovoljavajućom pouzdanosti i psihometrijskim karakteristikama. Konačno, i nad tri čestice Buchananova faktora općeg opreza provedena je faktorska analiza te je također dobiven jedan faktor, doduše, s nižom pouzdanosti izraženom preko mjere unutarnje konzistencije Cronbachov alfa α=,499.

Ukupan rezultat na pojedinom faktoru izračunat je kao prosjek odgovora na pojedinim česticama koje sačinjavaju taj faktor pri čemu su odgovori mogli biti u teoretskom rasponu od 1 do 5. Na taj način izračunata prosječna vrijednost na faktoru *Društvena dimenzija kontrole ponašanja* bila je 3,06, na faktoru tehnička zaštita bila je 2,63, a na faktoru opći oprez bila je 3,26. Dobiveni rezultati sugeriraju kako su sudionici u proteklih šest mjeseci rijetko do ponekad iskazivali ponašanja kojima su štitili svoju privatnost.

Tablica 4. - prikaz faktorskih zasićenja i mjera unutarnje konzistencije

Sadržaj čestice	Faktorsko zasićenje
Društvena dimenzija kontrole ponašanja	α=,723
Izbjegli posjetiti određenu internetsku stranicu iz straha da bi mogla zaraziti Vaše računalo ili kompromitirati Vaše osobne podatke?	,722
Prilikom registracije za određenu uslugu dali lažne osobne podatke ili lažnu e-adresu?	,606
Odlučili odustati od započete internetske kupovine jer niste bili sigurni što će se dogoditi s Vašim podacima?	,817
Odlučili se ne registrirati na internetsku stranicu jer se od Vas tražilo davanje osobnih podataka koje niste bili spremni dati?	,807
Tehnička zaštita	α=,729
Obrisali sve kolačiće (eng. cookies) iz internetskog preglednika?	,821
Provjerili nalazi li se na Vašem računalu spyware?	,700
Obrisali povijest pretraživanja u internetskom pregledniku?	,714
Koristili incognito način za pregledavanje interneta?	,618
Koristili VPN ili TOR prilikom spajanja na Internet?	,604
Opći oprez	α=,499
Uništili dokumente koji sadrže Vaše osobne podatke prije nego što ste ih odložili u otpad?	,679
Sakrili rukom PIN broj prilikom korištenja bankovnih kartica?	,722
Pročitali politiku privatnosti prije registracije na internetsku stranicu ili prije instaliranja aplikacija na mobilni telefon?	,730

Jednako kao i u slučaju mjerenja stavova, odnosno mjerenja zabrinutosti za privatnost, bilo je potrebno sudionike podijeliti u skupine temeljem njihovih rezultata na bihevioralnim mjerama. To je ponovo učinjeno ranije opisanom metodologijom te su na faktoru *društvene dimenzije kontrole ponašanja* kao fundamentalisti označeni sudionici koji su na sve četiri čestice dali visoki odgovor, nezainteresirani oni koji ni na jednoj čestici nisu dali visoki odgovor, a pragmatični svi ostali. Za faktor *tehničke zaštite* sudionike smo kategorizirali kao fundamentaliste ako su dali visoki odgovor na četiri ili pet čestica, kao nezainteresirane ako ni na jednu česticu nisu dali visoki odgovor, a kao pragmatike sve ostale. Budući da se faktor općeg opreza sastoji od svega tri čestice, fundamentalisti su, razumljivo, bili oni koji su na sve tri čestice dali visok odgovor, nezainteresirani oni koji ni na jednu nisu dali visoki odgovor, a pragmatici svi ostali.

Tablica 5. - prikaz rasporeda sudionika prema broju čestica na koje su dali visoki odgovor

	Društvena dimenzija		Tehnička zaštita		Opći oprez	
	Broj čestica	Udio sudionika	Broj čestica	Udio sudionika	Broj čestica	Udio sudionika
Fundamentalisti	4	12%	4 ili 5	12%	3	15%
Pragmatici	1, 2, ili 3	65%	1, 2 ili 3	58%	1 ili 2	70%
Nezainteresirani	0	23%	0	30%	0	15%

Ovakav raspored sudionika u kategorije pokazuje kako se u kategoriji nezainteresirani nalazi relativno velik broj sudionika, i to čak i kad je ona definirana na način da obuhvaća samo one sudionike koji ni na jednu česticu nisu dali visok odgovor, odnosno nisu nijednom naveli kako su u posljednjih šest mjeseci često ili vrlo često iskazali pojedino ponašanje kojim su štitili svoju privatnost.

Testirane su razlike u spolu za sva tri faktora te su pronađene razlike na sva tri faktora. Pri tome na faktorima Društvene dimenzije kontrole ponašanja ($t = 2{,}164$; $df = 964$; $p < 0{,}05$) i Općeg opreza ($t = 2{,}704$; $df = 964$; $p < 0{,}01$) rezultati pokazali kako žene ostvaruju statistički značajno veće rezultate od muškaraca, dok na faktoru Tehničke zaštite ($t = -6{,}634$; $df = 964$; $p < 0{,}001$) muškarci ostvaruju statistički značajno veći rezultat. Nadalje, pronađene su vrlo niske, ali zbog veličine uzorka statistički značajne, korelacije dobi i sva tri faktora i to na način da je dob nisko i pozitivno korelirana s faktorom Općeg opreza ($r = 0{,}175$; $N = 965$), dok je nisko i negativno korelirana s faktorima Društvene dimenzije kontrole ponašanja ($r = -0{,}089$; $N = 965$) i Tehničke zaštite ($r = -0{,}105$; $N = 965$).

Razlike u rezultatu između sudionika s različitim obrazovanjem i u ovom slučaju provjeravane su uz pomoć analize varijance na način da su od ukupno šest kategorija najprije stvorene ranije opisane četiri. Utvrđeno je kako različit stupanj obrazovanja nije statistički značajno utjecao na razlike na faktorima Društvene dimenzije privatnosti i Tehničke zaštite, dok je na faktoru Općeg opreza pronađen statistički značajan utjecaj ($F(3,962) = 5,321$; $p < 0,001$), a Scheffeovim post-hoc testom statistički značajna razlika pronađena je između sudionika koji su završili postdiplomski studij u odnosu na sudionike koji su završili srednju školu ili niže te između sudionika koji su završili diplomski studij i srednju školu ili niže na način da su sudionici koji su kao najviši završeni stupanj obrazovanja naveli srednju školu ili niže imali statistički značajno niži rezultat na faktoru Općeg opreza u odnosu na sudionike koji završili diplomski studij i postdiplomski studij.

4.2.4. Paradoks privatnosti

Nakon što su definirane mjere stavova o privatnosti i bihevioralne mjere, moglo se pristupiti provjeri paradoksa privatnosti. Kao mjere zabrinutosti za privatnost korišteni su faktor zabrinutosti za privatnost i faktor prikupljanje CFIP-a, a kao bihevioralne mjere korištena su tri bihevioralna faktora društvena dimenzija kontrole ponašanja, tehnička zaštita i opći oprez.

Najprije su izračunate korelacije između mjera stavova o privatnosti i bihevioralnih mjera. Dobivene su niske do umjerene pozitivne korelacije prikazane u tablici 6., koje su sve značajne uz razinu rizika $p<0.01$. Preciznije, faktor društvene dimenzije umjereno je povezan s mjerama stavova, dok je faktor tehničke zaštite nisko povezan s mjerama stavova. To znači da postoji tendencija da osobe koje izražavaju veću zabrinutost za privatnost više iskazuju ponašanja kojima tu privatnost štite.

Tablica 6. - prikaz korelacija između mjera stavova i bihevioralnih mjera

		Bihevioralne mjere		
		Društvena dimenzija	Tehnička zaštita	Opći oprez
Mjere stavova	Zabrinutost za privatnost	,377*	,246*	,227*
	CFIP - prikupljanje	,421*	,234*	,310*

* - značajno uz razinu značajnosti $p<0.01$

Međutim, korelacija stavova i ponašanja malo nam pomaže u testiranju paradoksa privatnosti. Naime, paradoks privatnosti definiran je kao diskrepancija između iskazivanja visoke

zabrinutosti za privatnost i istovremenog iskazivanja ponašanja kojim se odriče od privatnosti. Korelacija govori samo o trendu u variranju stavova i ponašanja. Pa tako dobiveni rezultati sugeriraju kako postoji trend da ljudi koji, u relativnim terminima izražavaju veću zabrinutost za privatnost, u relativnim terminima više iskazuju ponašanja brige za privatnost. Međutim, korelacija ne govori ništa o tome na koji način se ponašaju osobe koje visoko vrednuju privatnost, odnosno izražavaju visoku zabrinutost za privatnost u apsolutnim terminima. Upravo su zbog toga sudionici kategorizirani u različite skupine prema tome koliko visoko vrednuju privatnost.

Fundamentalisti označavaju one sudionike koji su na značajan broj čestica dali visoke odgovore. Kako bi se testirao paradoks privatnosti, bilo je potrebno provjeriti koju razinu brige za privatnost na bihevioralnim mjerama iskazuju sudionici kategorizirani kao fundamentalisti prema svojim odgovorima na mjerama stavova. Odnosno, bilo je potrebno testirati iskazuju li sudionici kategorizirani kao fundamentalisti prema svojim odgovorima na mjerama stavova visoku razinu i na bihevioralnim mjerama.

Kao kriterij za određivanje razine koja bi bila označena kao visoka, uzet je najmanji ukupni broj odgovora za pojedinu bihevioralnu mjeru koji bi bio dovoljan kako bi se sudionika kategoriziralo kao fundamentalista. Pa je tako za faktor društvene dimenzije kontrole ponašanja bilo potrebno izraziti visok odgovor na sve četiri čestice koje su sačinjavale taj faktor, a budući da je visok odgovor označen kao 4 ili 5, minimalni broj odgovora koji je sudionik morao imati da bi ga se kategoriziralo kao fundamentalista je 16. Jednaka je logika primijenjena i na preostala dva faktora te je za faktor tehničke zaštite kriterij također iznosio 16, a za faktor općeg opreza 12. Valja istaknuti kako je kategorizacija sudionika napravljena temeljem broja čestica na koje su sudionici dali visok odgovor, a da su kriteriji za određivanje visoke razine odgovora dobiveni temeljem ukupnog rezultata na pojedinom faktoru. Takvim drugačijim izračunom, ostavljen je prostor za manja odstupanja u kategorizacijama, ali radi se o zanemarivim odstupanjima.

Napravljeno je ukupno šest t-testova na način da je za sudionike kategorizirane kao fundamentalisti prema odgovorima na objema mjerama stavova provjeravano jesu li na trima bihevioralnim mjerama iskazivali odgovore više od kriterija. Rezultati prikazani u tablici 7. pokazali su kako su sudionici kategorizirani kao fundamentalisti iskazivali značajno niže razine na bihevioralnim mjerama od teoretskog kriterija.

Tablica 7. - rezultati usporedbe rezultata na bihevioralnim mjerama koje su ostvarili sudionici kategorizirani kao fundamentalisti prema mjerama stavova sa zadanim teoretski očekivanim kriterijem

Mjere stavova	Bihevioralne mjera	Arit. sredina	Kriterij	t	df	Značajnost
Zabrinutost za privatnost	Društvena dim.	13,8909	16	-9,06	219	p<0,0001
	Tehnička zaštita	14,6273	16	-6,74	219	p<0,0001
	Opći oprez	10,5136	12	-7,79	219	p<0,0001
CFIP - prikupljanje	Društvena dim.	13,8019	16	-11,1	322	p<0,0001
	Tehnička zaštita	14,4118	16	-5,59	322	p<0,0001
	Opći oprez	10,5449	12	-9,36	322	p<0,0001

To zapravo znači kako čak ni sudionici koji su deklarativno najviše vrednovali privatnost nisu često izražavali ponašanja kojima štite privatnost. Time možemo reći kako je potvrđen paradoks privatnosti, odnosno kako postoji diskrepancija između deklariranja visoke važnosti privatnosti i istovremeno demonstriranja ponašanja kojima se privatnost nedovoljno štiti.

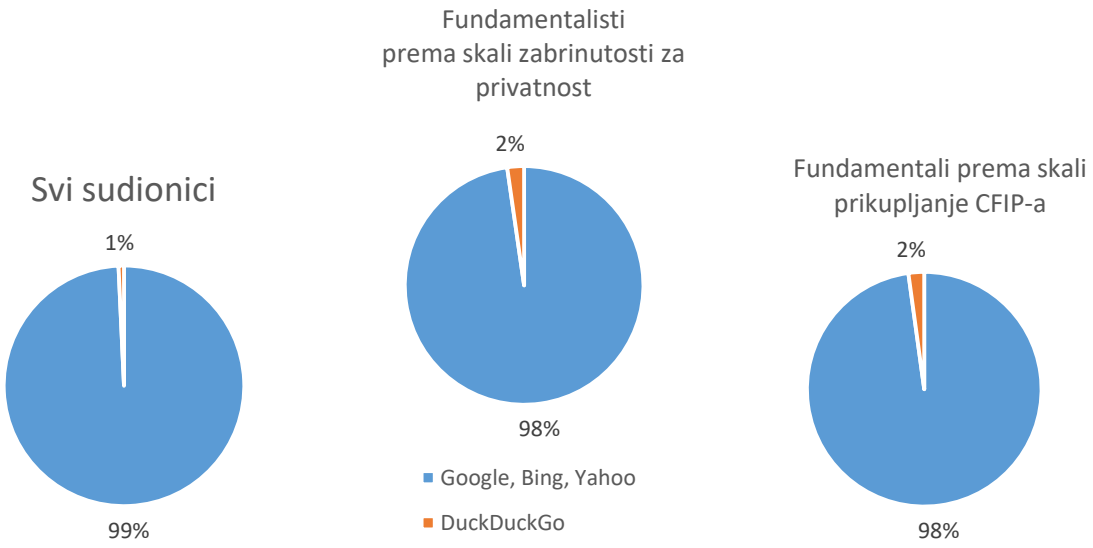
4.2.4.1. Korištenje interneta i društvene mreže

Podsjetimo, pored bihevioralnih mjera utemeljenih na faktorima Parka i Buchanana, sudionicima je postavljeno i nekoliko konkretnih pitanja o korištenju interneta i društvenim mrežama poput pitanja o internetskim tražilicama, servisima za elektroničku poštu, prisustva na društvenim mrežama, te konkretnih podataka koje sudionici imaju navedene na svojem profilu. Objektivne mjere toga tipa vrlo su dobre budući da se radi o konkretnom podatku koji je sudionicima najčešće lako dostupan i pogreške u dosjećanju su vrlo male, što ih čini objektivnim i visoko valjanim pokazateljima koji direktno ukazuju na razinu zaštite privatnosti koju sudionici manifestiraju.

Od sudionika je najprije zatraženo da navedu koju tražilicu za pretraživanje interneta najčešće koriste. Sudionicima su ponuđena samo dva odgovora pri čemu je jedan odgovor obuhvaćao tri popularne tražilice Google, Bing i Yahoo te je sudionicima ostavljena mogućnost da sami navedu tražilicu koju koriste ukoliko ona nije nijedna od tri navedene. Pitanje je na taj način primijenjeno kako bi se učinak efekta udovoljavanja hipotezi smanjio, odnosno kako se sudionicima ne bi unaprijed sugerirali odgovori. Pretpostavka je bila da će sudionici lako znati navesti tražilicu koju svakodnevno koriste, ukoliko se ne radi o jednoj od navedenih. Jednako tako, unatoč tome što je Google daleko najpopularnija tražilica na svijetu, ona je u ponuđenom

odgovoru navedena zajedno s još dvije popularne tražilice budući da u terminima zadiranja u privatnost, praćenja korisnika i korištenja njihovih podataka Microsoft i Yahoo ne odstupaju značajno od Googlea, kao što je detaljnije pojašnjeno u drugom poglavlju.

Rezultati su pokazali kako od ukupno 966 sudionika svega njih 7 koristi neku tražilicu različitu od one tri koje su bile ponuđene i svih sedmero sudionika navelo je kako se radi o tražilici DuckDuckGo, tražilici koja svoj poslovni model bazira na tome da ne prati korisnike i poštuje njihovu privatnost (slika 5.)

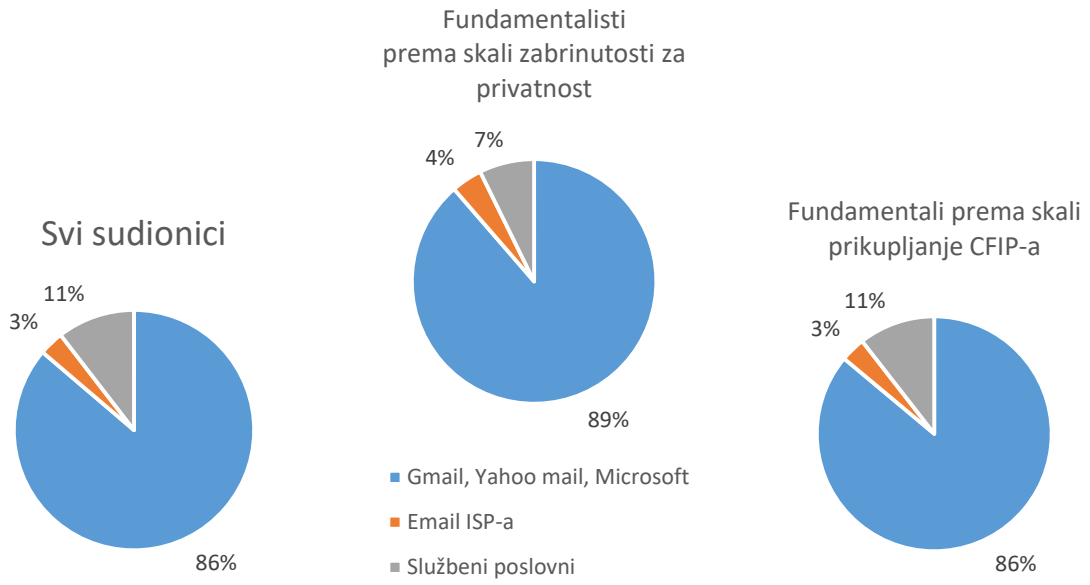


Slika 5. - Udio odgovora na pitanje „Za pretraživanje interneta najčešće koristim tražilicu“

Međutim, ono što je još zanimljivije u kontekstu rasprave o paradoksu privatnosti jest činjenica da su gotovo svi sudionici koji su osobito visoko vrednovali privatnost, odnosno koji su kategorizirani kao fundamentalisti bilo prema faktoru zabrinutost ili CFIP, također najčešće koristili tražilice koje ugrožavaju njihovu privatnost, prikupljaju i prodaju njihove podatke te manipuliraju njihovim internetskim iskustvom prilagođavanjem rezultata čime ih stavljaju u svojevrsne društvene balone.

Nadalje, od sudionika je zatraženo da navedu koji servis elektroničke pošte najčešće koriste. Slično kao i u proteklom pitanju, odgovori su grupirani prema razmjerima ugrožavanja privatnosti te je sudionicima ostavljena mogućnost da sami navedu servis koji koriste ukoliko on nije bio naveden. U skupini servisa koja najviše ugrožava privatnost bili su ponuđeni Gmail, Yahoo mail i Microsoft mail, u skupini koja nešto manje narušava privatnost korisnika ponuđeni su servisi e-pošte pružatelja internetskih usluga u Hrvatskoj, a kao treća opcija

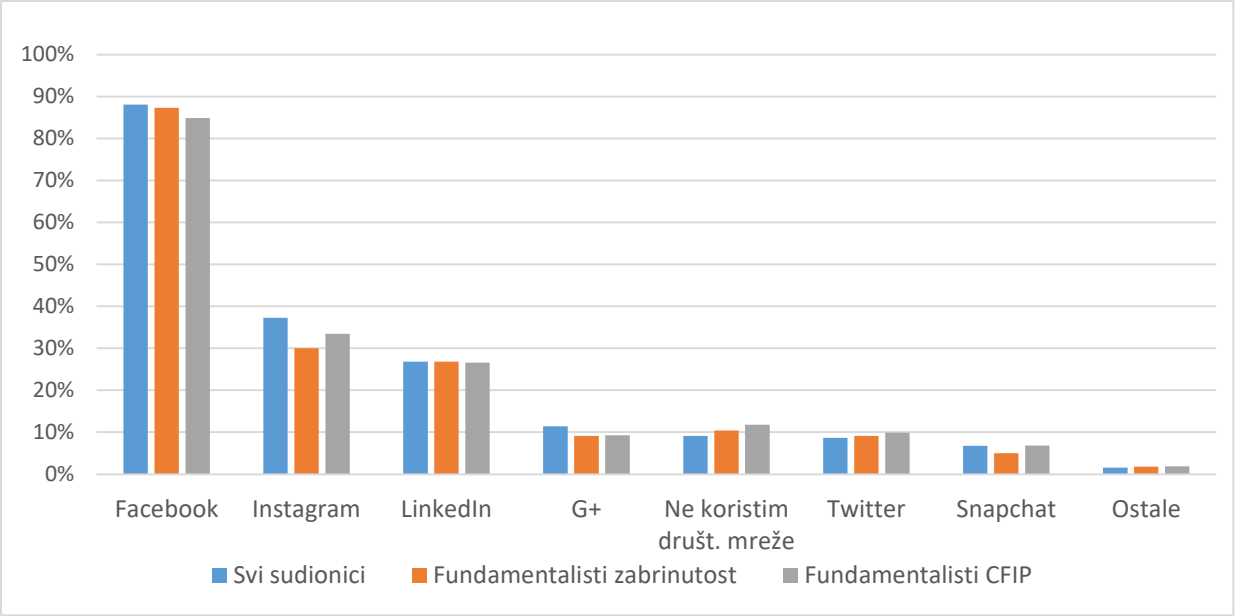
ponuđena je opcija da odaberu kako koriste službeni poslovni servis e-pošte. Pojedini sudionici navodili su servise e-pošte koji nisu bili ponuđeni, ali svi su se nakon analize mogli s visokom sigurnošću svrstati u jednu od tri ponuđene kategorije (slika 6.) Niti jedan sudionik nije naveo kako koristi bilo koji od brojnih servisa e-pošte koji u potpunosti poštuju privatnost korisnika.



Slika 6. - Udio odgovora na pitanje „Za elektroničku poštu najčešće koristim sljedeći servis“

U sljedećem dijelu istraživanja od sudionika je traženo da navedu sve društvene mreže koje su koristili u posljednjih šest mjeseci. Bile su ponuđene popularne društvene mreže Facebook, Instagram, G+, Twitter, LinkedIn, Snapchat, opcija kako ne koriste društvene mreže te mogućnost slobodnog unosa društvene mreže koja nije navedena. Rezultati prikazani na slici 7. pokazuju kako je daleko najpopularnija društvena mreža Facebook koju je koristilo gotovo 90% sudionika u istraživanju. Društvenu mreža za dijeljenje fotografija Instagram i društvena mreža za poslovnu suradnju LinkedIn prema vlastitim navodima koristilo je oko 30% sudionika, a G+, Twiter i Snapchat oko 10% sudionika.

Usporedba korištenja društvenih mreža između cjelokupnog uzorka i sudionika kategoriziranih kao fundamentalisti pokazuje kako ne možemo reći da postoje velike razlike u korištenju društvenih mreža.



Slika 7. - Udio odgovora na pitanje „Navedite društvene mreže koje ste koristili u proteklih šest mjeseci“

I konačno, od sudionika je zatraženo da označe sve podatke o njima koji su navedeni na profilu društvenih mreža koje koriste (tablica 8.) Osobno ime i prezime na društvenim mrežama koristi više od 75% sudionika, a gotovo toliko ih na profilu ima i svoju fotografiju. Nadalje, podaci sugeriraju kako pola sudionika ima na vlastitom profilu navedene i određene biografske poput podataka o školovanju (54%) ili zaposlenju (37%), a značajan je i udio korisnika koji ima navedene podatke osobito pogodne za profiliranje kao što su podaci o omiljenim knjigama, filmovima, glazbi ili idejama koje podržavaju (28%), pripadnosti klubovima, udrugama ili inicijativama (12%) te religijske ili političke stavove (9%).

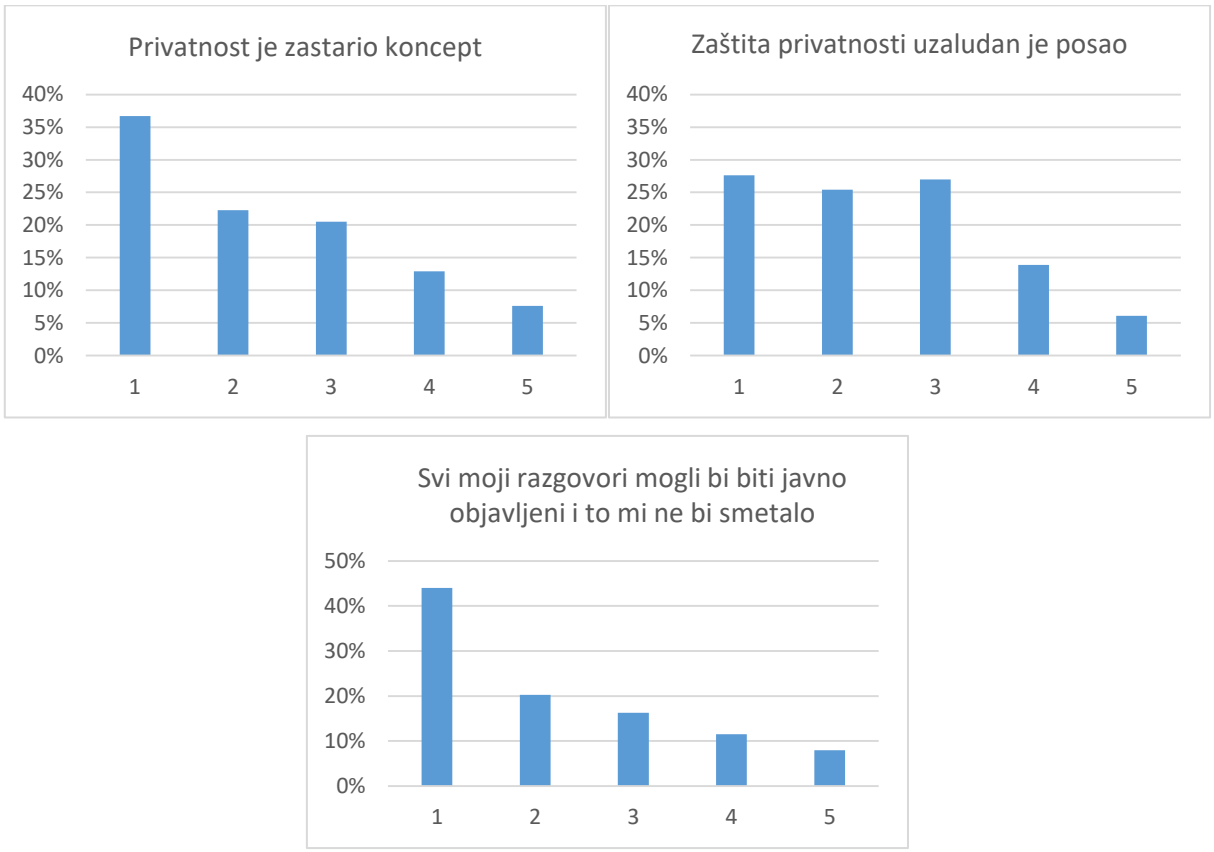
Tablica 8. – Postotak sudionika koji su za pojedini podatak naveli kako se nalazi na njihovom profilu društvene mreže

	Svi sudionici	Fund. CFIP	Fund. zabrinutost
Pravo ime	84%	80%	79%
Pravo prezime	77%	73%	70%
Fotografija	73%	67%	70%
Podaci o školovanju	54%	48%	41%
Podaci o zaposlenju	37%	32%	29%
Omiljene knjige, filmovi, glazba ili ideje	28%	24%	25%
E-adresa	28%	22%	24%
Pripadnost klubovima, udrugama i sl.	12%	10%	12%
Broj telefona ili mobitela	11%	9%	7%
Ne koristim društvene mreže	9%	12%	10%
Religijski ili politički stavovi	9%	7%	10%
Adresa stanovanja	6%	5%	4%

4.2.4.2. Stavovi o privatnosti

Osim provjeravanja postojanja paradoksa privatnosti, ovo istraživanje imalo je i sekundarni cilj. Kroz kvalitativno istraživanje metodom intervjua, ali i pojedinim pitanjima u kvantitativnom dijelu istraživanja primijenjenima na velikome uzorku, željelo se bolje razumjeti način na koji sudionici razumiju privatnost te time doprinijeti odgovoru na ključno pitanje ove disertacije – je li i u kojoj mjeri došlo do transformacije pojma prava na privatnost.

Od sudionika je zatraženo da se na skali od pet stupnjeva koja se kretala od uopće se ne slažem do u potpunosti se slažem odrede u kojoj se mjeri slažu s tvrdnjama Privatnost je zastario koncept koji u 21. stoljeću više nema mnogo smisla, tvrdnjom Zaštita privatnosti uzaludan je posao i tvrdnjom Svi moji razgovori mogli bi biti javno objavljeni i to mi ne bi smetalo (slika 8.) Rezultati pokazuju kako se tek nešto više od polovice sudionika ne slaže s tim trima tvrdnjama. Preciznije, 59% sudionika navelo je kako se ne slaže ili uopće se ne slaže s prvom tvrdnjom, 53% s drugom tvrdnjom, a 64,3% s trećom tvrdnjom. Pri tome vrijedi istaknuti kako je čak 44% sudionika navelo kako se uopće ne slaže s trećom tvrdnjom.

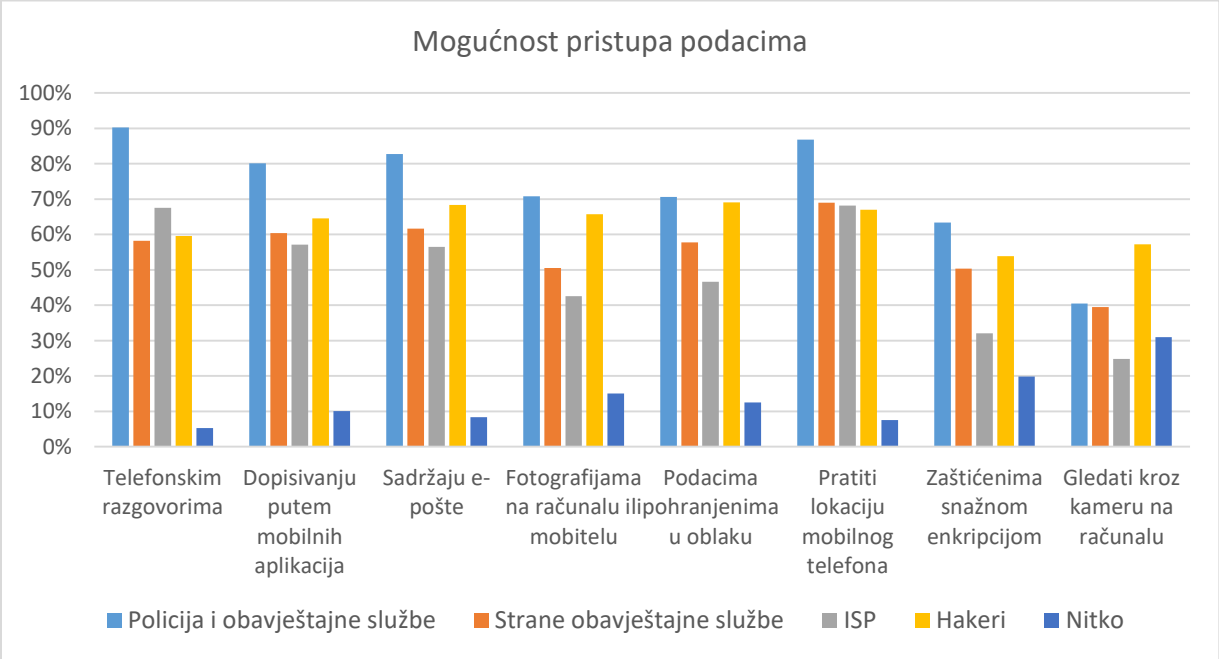


Slika 8. - Udjeli odgovora procjene slaganja s tvrdnjama „Privatnost je zastario koncept koji u 21. stoljeću više nema mnogo smisla“, „Zaštita privatnosti uzaludan je posao“ i „Svi moji razgovori mogli bi biti javno objavljeni i to mi ne bi smetalo“

Međutim, zanimljivije je obratiti pozornost na broj sudionika koji su se s tim tvrdnjama složili. Naime, čak petina sudionika navela je kako se slaže ili se u potpunosti slaže s navedenim tvrdnjama. Preciznije, 20,5% sudionika složilo se tvrdnjom kako je privatnost zastario koncept koji danas nema mnogo smisla, 20% sudionika složilo se s tvrdnjom kako je zaštita privatnosti uzaludan posao, a 19,5% sudionika složilo se s tvrdnjom kako im ne bi smetalo kada bi svi njihovi razgovori bili javno objavljeni.

Podsjetimo, na pitanje o važnosti privatnosti niti jedan sudionik nije naveo kako mu je ona izrazito nevažna, a njih svega 1,1% navelo je kako im je nevažna. Posebno je zanimljiva činjenica da od 20,5% sudionika koji su se složili s tvrdnjom o tome kako je privatnost zastario koncept njih je čak 85,8% navelo kako im je privatnost važna ili izrazito važna, od 20% sudionika koji su se složili s tvrdnjom kako je zaštita privatnosti uzaludan posao njih je čak 87% navelo kako im je privatnost važna ili izrazito važna, a od 19,5% sudionika koji su se složili s tvrdnjom kako bi svi njihovi razgovori mogli biti javno objavljeni, čak 85,9% navelo je kako im je privatnost važna ili izrazito važna. Ovi podaci ukazuju na to da sudionici zaštitu privatnosti ne smatraju uzaludnom jer ne misle da je privatnost vrijedna zaštite, već iz nekog drugog razloga.

Nadalje, kako bi se dobio bolji uvid u to do koje su mjere sudionici u istraživanju bili uvjereni u mogućnosti i kapacitete nadzora od njih je zatraženo da za nekoliko kategorija podataka procijene tko im sve ima mogućnost pristupa (slika 9.)



Slika 9. – Procjena sudionika tko sve ima mogućnost pristupa kategorijama podataka

Dobivene rezultate moguće je vrlo detaljno tumačiti, no za razumijevanje toga koliko su sudionici smatrali da su njihovi podaci dostupni nadzoru, dovoljno je podatke sagledati na načelnoj razini. Pogledamo li rezultate, odmah upada u oči kako je izuzetno velik broj sudionika uvjeren da je moguće pristupiti njihovim podacima. Pri tome je lako uočiti kako se posebno izdvaja mogućnost pristupa hrvatske policije i obavještajnih službi. Naime, iznenađujuće velik broj sudionika smatra kako hrvatska policija i obavještajne službe uz odgovarajući nalog mogu pristupiti gotovo bilo kojoj kategoriji podataka. Čak 80% sudionika vjeruje kako mogu pristupiti sadržaju njihova dopisivanja i razgovora putem mobilnih aplikacija (whatsapp, viber i slično) te sadržaju njihove e-pošte, 71% vjeruje da mogu pristupiti fotografijama pohranjenima na njihovom mobilnom telefonu ili računalu ili podacima i dokumentima pohranjenima u oblaku (iCloud, dropbox, onedrive, gdrive), 63% vjeruje da hrvatska policija i obavještajne službe mogu pristupiti podacima zaštićenima snažnom enkripcijom (AES256 ili snažnija), a čak 40% sudionika vjeruje da im mogu gledati kroz kameru na njihovom mobitelu ili računalu. U procjeni mogućnosti pristupa podacima na drugom su mjestu hakeri ili vješti korisnici za koje, ovisno o vrsti podataka, 54%-69% sudionika smatra kako im imaju mogućnost pristupa. Strane obavještajne službe nalaze se iza hakera i za njih, ovisno o vrsti podataka, 39%-69% sudionika smatra kako im imaju mogućnost pristupa. Posebno je zanimljivo kako za pružatelje internetskih usluga, odnosno hrvatske telekomunikacijske tvrtke, ovisno o vrsti podataka, čak 25%-68% sudionika smatra kako im imaju mogućnost pristupa. Za većinu kategorija podataka vrlo je malo sudionika označilo kako smatra da im nitko ne može pristupiti, odnosno kako su ti podaci za sada sigurno, a od tog broja značajnije se izdvaja procjena kako nitko ne može pristupiti podacima zaštićenima snažnom enkripcijom (20%) te kako ih nitko ne može gledati kroz kameru na njihovu računalu ili mobilnom telefonu (31%).

4.3. Zaključak

Primarni cilj empirijskog istraživanja bio je odgovoriti na drugu istraživačku hipotezu, odnosno provjeriti postojanje paradoksa privatnosti. U tom smislu možemo reći kako je potvrđeno postojanje paradoksa privatnosti, odnosno dobiveni rezultati pokazuju kako postoji diskrepancija između visoke važnosti privatnosti za pojedince i lakoće kojom su je se spremni odreći.

Naime, sudionici koji su najviše vrednovali svoju privatnost iskazivali su kako se ponašaju na način statistički značajno različit od onog koji bi se mogao očekivati od osoba koje visoko

vrednuju svoju privatnost. To je dodatno naglašeno uzmemo li u obzir čestinu korištenja tražilica koje ne poštuju privatnost korisnika, servisa e-pošte koji čitaju korisničke poruke i mešetare njihovim podacima i podacima osoba s kojima se oni dopisuju te konačno podatke o učestalosti korištenja društvenih mreža i razine do koje sudionici, pa i oni koji najviše vrednuju svoju privatnost, otkrivaju svoje osobne podatke i odriču se svoje privatnosti budući da ti podaci svakako idu u prilog postojanju paradoksa privatnosti.

No, osim testiranja paradoksa privatnosti, ovo istraživanje imalo za cilj doprinijeti boljem razumijevanju načina na koji sudionici shvaćaju privatnost. Budući da je temeljno pitanje ove disertacije je li i u kojoj mjeri došlo do transformacije pojma prava na privatnost, dio rezultata bit će prikazan u narednom poglavlju zajedno s opsežnom raspravom o implikacijama istraživanja na dosadašnje spoznaje o privatnosti. U idućem će se poglavlju suočiti rezultate dobivene empirijskim istraživanjem s normativnom raspravom o privatnosti prikazanom u proteklom poglavlju radi boljeg razumijevanja transformacije pojma privatnosti, odnosno razmjera takve transformacije.

5. Implikacije novih spoznaja na normativnu raspravu o privatnosti

Opsežna normativna rasprava o ulozi privatnosti, njezinu značaju i vrijednosti zaključena je konstatacijom kako došlo do dubinskog redefiniranja pojma privatnosti i pojma prava na privatnost. Izlažući primjere eksternih i internih ugroza privatnosti te reakcije javnosti na otkrića o razmjerima ugroza privatnosti zaključeno je kako se ne radi o tome da su ljudi manje zabrinuti za privatnost, nego su pojam privatnosti i ideja ugroze privatnosti radikalno redefinirani zbog čega su ljudi postali ambivalentni prema ugrozama privatnosti.

Budući da je privatnost temeljeno ljudsko pravo koje ima instrumentalni i intrinzični značaj za pojedinca i društvo, trenutna razina zaštite, odnosno ugrožavanja, privatnosti nije spojiva s jednom od osnovnih ideja liberalne demokracije prema kojoj nacionalna država na učinkovit način štiti prava svojih građana. Tu je tenziju moguće razriješiti samo na dva načina. Prvo, ili je potrebno odbaciti privatnost kao temeljno ljudsko pravo vrijedno učinkovite zaštite i uvažavanja. Ili je, drugo, privatnost potrebno početi na dosljedan i učinkovit način osiguravati, štititi i vrednovati.

Kao doprinos daljnjoj raspravi provedeno je empirijsko istraživanje prikazano u prošlom poglavlju. Osnovni cilj bio je dobiti uvid u način na koji pojedinci razumiju privatnost, te smatraju li je vrijednom zaštite i zbog čega. I, konačno, cilj je bio utvrditi razmjere odricanja od privatnosti, odnosno lakoću kojom su se pojedinci spremni odreći privatnosti.

5.1. Implikacije rezultata na normativnu raspravu

Rezultati empirijskog istraživanja ukazuju na nekoliko vrlo značajnih fenomena. Najprije, velika većina sudionika navela je kako im je privatnost izrazito važna, dok su rezultati dobiveni indirektnim mjerenjem zabrinutosti za privatnost pomoću dvaju skala pokazali kako su sudionici u provedenom istraživanju umjereno zabrinuti za vlastitu privatnost. Istovremeno, dobiveni rezultati pokazuju kako su sudionici u proteklih šest mjeseci rijetko iskazivali ponašanja kojima su štitili svoju privatnost. Ova spoznaja već sama po sebi znači kako postoji diskrepancija između stavova o visokoj važnosti privatnosti i ponašanja sudionika kojima sudionici zapravo svoju privatnost ne štite u mjeri u kojoj bi se to očekivalo ako je doista visoko vrednuju.

Nastavno na tu tezu, testiran je i paradoks privatnosti, odnosno hipoteza o tome kako sudionici koji izražavaju visoku zabrinutost za privatnost ne manifestiraju ponašanja kojima se na značajan način štiti privatnosti. Rezultati su pokazali kako je potvrđen paradoks privatnosti, odnosno kako čak ni sudionici koji su deklarativno najviše vrednovali privatnost nisu često izražavali ponašanja kojima štite privatnost.

5.1.1. Transformacija pojma privatnosti

Budući da je osnovna teza ovog rada ta da je došlo do transformacije pojma privatnosti, pitanje je na koji način rezultati empirijskog istraživanja doprinose boljem razumijevanju te osnovne teze. Provedenim istraživanjem nije eksplicitno i nedvosmisleno dan odgovor na pitanje je li došlo do transformacije pojma privatnosti, niti je to bilo moguće utvrditi bez korištenja jednog od istraživačkih nacrta koji uključuju mjerenja u više vremenskih točaka. Međutim, pojedini rezultati dobiveni u istraživanju svakako daju određeni uvid u način na koji ljudi danas razumiju privatnost, koliko im je ona važna i na koji se način odnose prema zaštiti svoje privatnosti. Na taj je način moguće posredno donijeti određene zaključke i o transformaciji pojma privatnosti, odnosno moguće je uvidjeti odražava li se transformacija pojma privatnosti, opisana u konceptualnoj raspravi, u načinu na koji sudionici danas gledaju na privatnost te je li takav, transformirani, pogled na privatnost već postao dominantan pogled na privatnost.

5.1.1.1. Diskrepancija između deklarirane visoke važnosti privatnosti i lakoće odricanja od privatnosti

U kvalitativnom predistraživanju većina sudionika je u intervjuima dala naslutiti kako im je privatnost važna, a mnogima je bila čak i izrazito važna, ali su istovremeno iskazivali određenu pomirenost s brojnim ugrozama privatnosti kojima su izloženi. Upravo ta pomirenost, ta kontradikcija, tenzija između istovremene deklarativne važnosti privatnosti i ravnodušnosti prema njezinu ugrožavanju jedan je od najvećih pokazatelja da je došlo do transformacije pojma privatnosti. Tko god privatnost doista smatra temeljnim ljudskim pravom, ne bi mogao ostati ravnodušan prema rasprostranjenom ugrožavanju privatnosti i odricanju od vlastite privatnosti te bi mu ono zasigurno teško palo.

Slični su rezultati dobiveni i u kvantitativnom istraživanju te je preko 90% sudionika odgovorilo kako im je privatnost važna ili izrazito važna. Nadalje, kada govorimo o zabrinutosti za privatnost mjerenoj pomoću dvije različite skale, sudionici su bili tek umjereno zabrinuti za svoju privatnost. Ranije spomenuta diskrepancija između deklarirane važnosti privatnosti i

pomirenosti s ugrozama dijelom se očituje već u tome što sudionici privatnost smatraju važnom, a tek su umjereno zabrinuti za vlastitu privatnosti, odnosno tek im je umjereno stalo do toga na koji se način prikupljaju i koriste podaci o njima. Međutim, znatno je zanimljivije obratiti pozornost na pojedine bihevioralne varijable, odnosno na izjave sudionika o tome koliko su često u posljednjih šest mjeseci iskazali određeno ponašanje kojim se štiti njihova privatnost. Na pitanje o korištenju programa vjernosti trgovaca prilikom kupovine, čak 41,9% sudionika navelo je kako je u posljednjih šest mjeseci *vrlo često* koristilo program vjernosti, a dodatnih 17,4% sudionika navelo je kako su to činili *često*. Politiku privatnosti prije registracije na internetsku stranicu ili prije instaliranja aplikacija na mobilni telefon u posljednjih šest mjeseci čak 30,3% sudionika nije pročitalo *niti jednom*, a 22,8% sudionika to je činilo tek *rijetko*. Pri tome, valja imati na umu kako se cijelo vrijeme radi o uzorku sudionika među kojima je čak 90% navelo kako im je privatnost *važna* ili *izrazito važna*.

Uzmemo li u obzir podatke o korištenju interneta i društvenih mreža, poanta je još jasnija. Naime, od ukupno 966 sudionika njih je čak 959 ili 99,3% navelo kako za pretraživanje interneta najčešće koriste jednu od tri poznate tražilice Google, Bing ili Yahoo, čiji je cijeli poslovni model baziran na prikupljanju, analiziranju i dijeljenju korisničkih podataka. Jednako tako, čak 86% sudionika navelo je kako kao servis e-pošte koriste Googleov Gmail, Yahoo mail ili neki od Microsoftovih servisa, servise koji čitaju i indeksiraju korisničke e-poruke, kontakte i dokumente kako bi ih preciznije profilirali. Međutim, razinu vlastite izloženosti i digitalne transparentnosti najbolje oslikavaju rezultati o korištenju društvenih mreža. Gotovo 90% sudionika navelo je kako koriste društvenu mrežu Facebook, čije su metode prikupljanja i korištenja korisničkih podataka kao i upravljanja njihovom virtualnom stvarnosti detaljno opisane u poglavlju u kojem se govorilo o ugrozama privatnosti. Rezultati o raširenosti korištenja društvenih mreža, osobito Facebooka, te podaci o razmjeru objavljivanja i sadržaju osobnih podataka na društvenim mrežama ukazuju na to kako se već nalazimo u *društvu razotkrivanja* (Harcourt, 2015).

Empirijskim istraživanjem testirana je druga istraživačka hipoteza, odnosno potvrđeno je postojanje paradoksa privatnosti. Dobiveni rezultati potvrdili su kako postoji diskrepancija između visoke važnosti privatnosti za pojedince i lakoće kojom su je se spremni odreći, odnosno sudionici koji su bili najviše zabrinuti za svoju privatnost navodili su kako se ponašaju na način statistički značajno različit od onog koji bi se mogao očekivati od osoba koje visoko vrednuju svoju privatnost.

Sve u svemu, možemo reći kako su sudionici u istraživanju pokazali kako se ponašaju na brojne načine kojima se odriču svoje privatnosti te kako istovremeno tek ponekad poduzimaju ponašanja kojima štite svoju privatnost. Takva spoznaja ide u prilog zaključku normativne rasprave prema kojem je zbog rapidnog razvoja telekomunikacijske tehnologije i pojave asinkronih sigurnosnih prijetnji došlo do transformacije pojma privatnosti. Naime, tako raširenо odricanje od privatnosti moguće je samo ako se na privatnost više ne gleda na način na koji je ona branjena u normativnoj raspravi, ako se na nju više ne gleda kao na temeljno ljudsko pravo vrijedno zaštite.

A činjenica da se gotovo na jednak način privatnosti odriču i pojedinci koji je najviše vrednuju, ukazuje na to da stavovi o važnosti privatnosti i zabrinutosti za privatnost očigledno ne igraju značajnu ulogu u zaštiti privatnosti, osobito zaštiti privatnosti na internetu i na društvenim mrežama.

5.1.1.2. Privatnost kao relikt prošlosti

Unatoč tome što nisu redovito iskazivali ponašanja kojima vode brigu o vlastitoj privatnosti, većina sudionika na razini stavova privatnost i zaštitu privatnosti smatrala je važnom. Međutim, istovremeno rezultati su pokazali kako postoje i ljudi koji privatnost smatraju *reliktom prošlosti*, nečime što u današnje vrijeme nije moguće osigurati ili nečim sasvim bezvrijednim. Radi se o manjem dijelu sudionika, ali njihovi tvrdi i dosljedni stavovi o privatnosti pokazuju kako postoji dio ljudi koji uopće ne mare za privatnost ili, pak, zaštitu privatnosti smatraju unaprijed izgubljenom bitkom. U predistraživanju je svega dvoje sudionika navelo kako im privatnost nije važna, a kao obrazloženje su isticali vlastitu otvorenost, dosljednost i izostanak tajni. No, u empirijskom istraživanju udio skeptičnih sudionika bio je znatno veći.

Unatoč tome što je preko 90% sudionika navelo kako im je privatnost važna, na određena pitanja o privatnosti pružili su vrlo skeptične odgovore. Tri takve tvrdnje bile su *Privatnost je zastario koncept koji u 21. stoljeću više nema mnogo smisla*, tvrdnja *Zaštita privatnosti uzaludan je posao* te tvrdnja *Svi moji razgovori mogli bi biti javno objavljeni i to mi ne bi smetalo*. Rezultati su pokazali kako se čak 20% sudionika složilo s tim tvrdnjama. Posebno je zanimljiva činjenica da je od tih 20% skeptičnih sudionika njih preko 85% navelo kako privatnost smatraju važnom ili izrazito važnom. Činjenica da zaštitu privatnosti uzaludnom smatraju upravo oni koji je smatraju važnom baca drugačije svjetlo na rezultate. Naime, očigledno je kako se ne radi o osobama koje ne vide vrijednost privatnosti pa stoga njezinu

zaštitu smatraju uzaludnom, nego to smatraju iz nekog drugog razloga. Ovi rezultati odlično nadopunjuju pretpostavke, ili zabrinutost, iznesene u normativnoj raspravi. Po svemu sudeći, radi se o tome kako sudionici zapravo vjeruju da je borba za privatnost već izgubljena. Pomireni su sa sveprisutnosti nadzora, vlastitim razotkrivanjem koje ne mogu, ili ne žele, kontrolirati i vjeruju kako je privatnost zastario koncept koji je potrebno redefinirati. A upravo je osnovna argumentacija ove disertacije ta da sve više ljudi diže ruke od privatnosti dok se istovremeno nove generacije rađaju u društvu izlaganja te nemaju ni priliku iskusiti anonimnost.

5.1.2. Automatsko djelovanje moći

Prilikom opisivanja eksternih ugroza, onih kojima se privatnost ugrožava bez znanja ili volje pojedinca, opisan je Benthamov panoptikon kao arhitektonska građevina koja je omogućavala kontinuirani nadzor nad subjektima pri čemu oni istovremeno niti u jednom trenutku nisu mogli znati jesu li pod nadzorom. Bentham je činjenicu da subjekti nisu znali jesu li u određenom trenutku pod nadzorom, a da su u svakom trenutku mogli biti promatrani, tu stalnu neizvjesnost nazvao očiglednom sveprisutnosti (Bentham, 1787). Osnovna teza bila je da se ljudi ljepše ponašaju kada vjeruju da su nadzirani, a time što je postigao da nisu sigurni jesu li u pojedinom trenutku promatrani smatrao je da će subjekti internalizirati pravila te će se uvijek ponašati u skladu s njima. Benthamovu ideju Foucault je proširio na metaforu za sveprisutni nadzor u modernoj državi. Za Foucaulta, ključni pojam bio je automatsko djelovanje moći, koje je trebalo biti posljedica stalne i svjesne vidljivosti (Foucault, 1995: 201). Konačan cilj takvog disciplinatornog društva bio je građane disciplinirati bez primjene sile, odnosno postići to da internaliziraju pravila, da se iz straha od kazne sami cenzuriraju, korigiraju i usklade svoje ponašanje s normama.

Mnogi aspekti moderne države nadzora uvelike odgovaraju Foucaultovu opisu disciplinatorne države. Zbog toga je vrlo teško pronaći rad iz područja sigurnosnih studija koji se ne referira na panoptikon, odnosno na rad Benthama i Foucaulta. Međutim, kao što je objašnjeno u normativnoj raspravi, pogrešno je vjerovati da je moderna država nadzora uspostavljena radi automatskog djelovanja moći već je ono (ne)željena posljedica razvoja tehnologije i novih sigurnosnih izazova. Razvoj tehnologije doveo je do potpunog razotkrivanja građana i njihove digitalne transparentnosti, kao što je pokazano i u rezultatima istraživanja. Istovremeno strah od terorizma, rat s nepoznatim neprijateljem, želja za pronalaskom prijetnje doveo je do jačanja kapaciteta modernih obavještajnih službi do te mjere da najjače obavještajne službe na svijetu

danas imaju pristup velikom djelu digitalne stvarnosti. Najbolji pokazatelj toga da automatsko djelovanje moći nije bilo cilj, nego nuspojava, jest to da je izuzetan trud uložen u skrivanje stvarnih mogućnosti nadzora obavještajnih službi. Međutim, danas kada su nevjerojatne mogućnosti nadzora u značajnoj mjeri poznate, više nije važno je li automatsko djelovanje moći nastupilo kao cilj ili kao nuspojava. Ono je na snazi.

U tom je smislu bilo zanimljivo vidjeti do koje su mjere sudionici u istraživanju bili uvjereni u mogućnosti i kapacitete nadzora te na koji je način to utjecalo na njihovo ponašanje. Tako je u empirijskom istraživanju od sudionika zatraženo da za nekoliko kategorija podataka procijene tko im sve ima mogućnost pristupa. Pogledamo li rezultate, odmah upada u oči kako je izuzetno velik broj sudionika uvjeren da je moguće pristupiti njihovim podacima. Pritom se posebno ističe to kako velik broj sudionika smatra da hrvatska policija i obavještajne službe uz odgovarajući nalog mogu pristupiti gotovo bilo kojoj kategoriji podataka. Čak 80% sudionika vjeruje kako mogu pristupiti sadržaju njihova dopisivanja i razgovora putem mobilnih aplikacija te sadržaju njihove e-pošte, 71% vjeruje da mogu pristupiti fotografijama pohranjenima na njihovom mobilnom telefonu ili računalu ili podacima i dokumentima pohranjenima u oblaku, 63% vjeruje da hrvatska policija i obavještajne službe mogu pristupiti podacima zaštićenima snažnom enkripcijom, a čak 40% sudionika vjeruje da im mogu gledati kroz kameru na njihovom mobitelu ili računalu.

Drugi zanimljiv podatak je taj kako sudionici vjeruju da hrvatska policija i obavještajne službe imaju znatno veću mogućnost pristupa njihovim podacima od bilo koje druge kategorije korisnika, ali osobito je znakovito kako to vjeruju i u odnosu na mogućnost pristupa podacima koji imaju strane obavještajne službe i to u svim kategorijama podataka. Značajan dio drugog poglavlja bio je posvećen argumentaciji kako su kapaciteti nadzora najvećih obavještajnih službi neprikosnoveni, no ne i neograničeni. Naime, u kriptografskoj zajednici postoji konsenzus kako su suvremeni snažni kriptografski protokoli i dalje sigurni i za sada neprobojni pa je u tom smislu potrebno sagledati procjenu sudionika za mogućnosti pristupa podacima zaštićenima snažnom enkripcijom. Dakako, vrlo je teško sa sigurnošću odrediti točne odgovore za ovo pitanje no to i nije presudno budući da cilj ovog pitanja nije bio testiranje znanja sudionika već prikupljanje podataka o njihovu uvjerenju o izloženosti nadzoru. Međutim, postoje određene uvjerljive naznake koje sugeriraju da je realnost ipak značajno drugačija od onoga kako je vide sudionici u ovom istraživanju na način da je navedenim kategorijama podataka ipak znatno teže pristupiti nego što su sudionici u istraživanju procjenjivali.

No, i bez ulaženja u ocjenu točnosti procjena sudionika, evidentno je kako sudionici u istraživanju u velikoj mjeri smatraju kako njihovi osobni podaci mogu biti dostupni različitim pojedincima, tvrtkama i institucijama. Kada govorimo o automatskom djelovanju moći, jedino je to i važno. Kao što su Foucault i Bentham definirali kao *sveprisutni nadzor*, odnosno *očiglednu prisutnost*, uopće nije važno jesu li ljudi doista pod nadzorom već je jedino važno vjeruju li da u svakom trenutku mogu biti nadzirani. U tom smislu dobiveni podaci ukazuju na to izuzetno velik broj ljudi vjeruje kako mogu biti nadzirani, kako njihova lokacija može biti praćena, kako njihovi razgovori i privatno dopisivanje mogu biti nadzirani, kako njihove privatne fotografije pohranjene na osobnom računalu mogu biti nadzirani, pa čak i da ih se može gledati kroz kameru na mobilnom telefonu ili računalu.

Podsjetimo, slični su rezultati dobiveni i u kvalitativnom predistraživanju. Gotovo svi sudionici smatrali su kako njihova privatnost može vrlo lako biti narušena i u velikoj su mjeri precjenjivali kapacitete nadzora koje policija, sigurnosne službe i/ili hakeri imaju na raspolaganju. Istovremeno, svi su sudionici, osim jedne sudionice, naveli kako njihovo uvjerenje da vlastitoj privatnoj komunikaciji može imati pristup i netko kome ona nije namijenjena ne utječe na način na koji komuniciraju. Naime, ako je doista istina da ljudi smatraju kako u svakom trenutku mogu biti nadzirani bez vlastita znanja, a da istovremeno ta spoznaja ne utječe na njihovo ponašanje, onda uvidi Benthama i Foucaulta o *očiglednoj sveprisutnosti*, odnosno o *sveprisutnom nadzoru* više ne vrijede. Zbog toga je u kvantitativnom istraživanju sudionicima postavljeno pitanje o tome koliko su često u posljednjih šest mjeseci *U telefonskom razgovoru prešutjeli reći nešto što ste željeli reći iz straha od prisluškivanja?* (slika 10.)

Ono što je odmah vidljivo iz rezultata jest to da je najveći dio sudionika, njih 44%, naveo kako u posljednjih šest mjeseci *nijednom* nisu prešutjeli reći nešto što su željeli zbog straha od prisluškivanja. Međutim, na rezultate je moguće gledati i iz drugoga kuta te je moguće reći kako je čak 55% sudionika u posljednjih šest mjeseci *najmanje jednom* prešutjelo nešto reći iz straha od prisluškivanja pri čemu je čak 17,3% sudionika to činilo *često* ili *vrlo često*. Na temelju ovih rezultata teško je dati jednoznačan odgovor na pitanje je li na snazi automatsko djelovanje moći, ali činjenica da je u posljednjih šest mjeseci više od pola sudionika najmanje jednom u privatnom telefonskom razgovoru prešutjela reći nešto što su željeli samo iz straha od prisluškivanja svakako govori u prilog postojanju autocenzure, prilagođavanja našeg ponašanja nepoznatim motriteljima.

Slika 10. - Udjeli odgovora procjene slaganja s tvrdnjom „U telefonskom razgovoru prešutjeli reći nešto što ste željeli reći iz straha od prisluškivanja“, pri čemu 1 označava odgovor uopće se ne slažem, a 5 označava odgovor u potpunosti se slažem

Podatak kako izuzetno velik broj sudionika smatra kako su njihovi digitalni podaci i privatna korespondencija ponuđeni na pladnju različitim nadzirateljima te kako više od polovice sudionika povremeno modificira svoje ponašanje iz straha od nadzora daje dobar uvid u to kakav status privatnost danas ima. Tendencija da imamo sve manje privatnosti, da smo toga sve više svjesni i da sve manje radimo kako bismo je zaštitili jest osnova transformacije pojma privatnosti na koju ovaj rad želi ukazati.

5.2. Zašto se nitko ne buni?

Empirijsko istraživanje nije imalo pretenziju odgovoriti na pitanje zašto. Zašto imamo sve manje privatnosti, zašto nam je sve manje stalo, zašto se ne borimo za svoju privatnost. Na ta pitanja nije jednostavno odgovoriti i ona u velikom dijelu izlaze izvan okvira ovog rada. No, određene spoznaje dobivene u intervjuima i anketnom istraživanju zajedno sa spoznajama iz socijalne psihologije mogu pomoći u boljem razumijevanju kognitivnih i društvenih procesa koji su u pozadini ovakvog našeg odnosa prema privatnosti i njezinim ugrozama.

Kao što je već više puta istaknuto, osnovna je pretpostavka kako se radi o tome da su ljudi postali neosjetljivi za ugroze privatnosti zbog vlastitog postepenog, ali kontinuiranog i dugotrajnog, uključivanja u modernu konzumerističku kulturu koja je sve više bazirana na prikupljanju, analiziranju i razmjeni osobnih podataka korisnika. I to nije nova ideja. Whitaker je još 1999. godine pisao o *kraju privatnosti* i to upravo zbog sve učestalijeg žrtvovanja privatnosti radi konzumerističkih pogodnosti (Whitaker, 1999). Na njegovo promišljanje

nadovezao se Harcourt te ga je proširio u ideju tzv. *društva izlaganja*, nove društvene i političke stvarnosti u kojoj otkrivamo podatke o sebi, sve i svima, čak i kada nas ih nitko nije tražio (Harcourt, 2015). Paul Bernal je odnos korisnika interneta koji se oslanjaju na besplatne usluge i tvrtki koje pružaju te usluge opisao terminom *simbiotska mreža* (Bernal, 2014), iako bi taj odnos, kao što je argumentirano u drugom poglavlju, bilo primjerenije nazvati parazitskim. Kod sva tri autora provlači se ideja kako se ljude na odricanje od privatnosti motivira nagradama, a ne kaznama. Ta je teza sasvim sigurno točna. Umjesto da servis e-pošte platimo nekoliko dolara, radije ćemo se odlučiti koristiti naizgled besplatni Gmail, čije korištenje plaćamo svojim osobnim podacima. Radi nerijetko beznačajnog popusta u trgovinama, učlanit ćemo se u program vjernosti i predat ćemo svoje osobne podatke, podatke o tome što i kada kupujemo na milost i nemilost trgovcima. A mnoge usluge, kao što su društvene mreže, brojne mobilne aplikacije i računalni softver nije ni moguće koristiti bez prepuštanja vlastitih podataka. Želite li se umrežiti s prijateljima i obitelji putem društvene mreže, promovirati svoj posao, hobi ili projekt putem Facebooka, morate pristati na to da će vaši podaci biti prikupljani, obrađivani i dijeljeni. Po svemu sudeći, mnogi s time nemaju preveliki problem.

Rezultati provedenog istraživanja pokazuju kako je ljudima, barem na deklarativnoj razini, stalo do privatnosti, kako vjeruju da je njihova privatnost ugrožena, a osobni podaci stavljeni na raspolaganje državnim agencijama, privatnim tvrtkama i vještim korisnicima te, ono najvažnije od svega, kako malo rade kako bi svoju privatnost zaštitili. Podaci o učestalom korištenju programa vjernosti trgovaca, čija je jedina svrha prikupljanje, obrada i analiza vrlo detaljnih osobnih podataka kao i podataka o aktivnostima i navikama korisnika, te podaci o tome koliko zapravo mnogo ljudi koristi servise e-pošte, tražilice i društvene mreže onih tvrtki čiji je osnovni poslovni model prikupljanje, obrada, analiza njihovih osobnih podataka pokazuju današnju razotkrivajuću stvarnost. U zamjenu za naše vrijedne, intimne i osobne podatke dobivamo zanemarive popuste, mogućnost korištenja besplatnih usluga i softvera ili pristup društvenim mrežama.

5.2.1. Odnos stavova i ponašanja

Kada govorimo o odnosu stavova i ponašanja, on je dvosmjeran. Sasvim je jasno kako stavovi utječu na ponašanje, međutim, i ponašanje može utjecati na stavove. Prilikom interpretacije intervjua spomenuta je teorija kognitivne disonance, koja objašnjava našu potrebu za opravdavanjem vlastita ponašanja. U provedenom istraživanju dobivene su niske do umjerene

pozitivne korelacije između mjera stavova o privatnosti i bihevioralnih mjera, koje su sve statistički značajne. To znači da postoji tendencija da osobe koje izražavaju veću zabrinutost za privatnost više iskazuju ponašanja kojima tu privatnost štite. Ali i obratno. Naime, korelacija govori samo o povezanosti fenomena i temeljem korelacije nije moguće govoriti o uzročnosti, osim u iznimnim situacijama kada je evidentan i teoretski opravdan smjer uzročnosti. Međutim, u slučaju stavova o privatnosti i bihevioralnih mjera privatnosti ne možemo sa sigurnošću reći radi li se o tome da su ponašanja rezultat postojećih stavova ili su stavovi nastali kao posljedica nesvjesnog prilagođavanja i opravdavanja samootkrivajućeg ponašanja. Za precizan odgovor na to pitanje potrebno je provesti novo istraživanje korištenjem eksperimentalnog nacrta istraživanja. Međutim, izgledno je kako se radi o kompleksnom međuodnosu koji je zapravo dvosmjeran te kontekstulano i kulturno ovisan.

5.2.1.1. Utjecaj stavova na ponašanje

Najpoznatija teorija koja govori o predviđanju ponašanja temeljem stavova jest *teorija planiranog ponašanja* (Ajzen, 1991; Fishbein i Ajzen, 2010), a odnosi se na ona ponašanja za koja imamo vremena promisliti. Prema toj teoriji, osnovni prediktor ponašanja jest *namjera za izvođenjem* određenog ponašanja, a ona je „indikator toga koliko su se ljudi spremni truditi, koliko truda planiraju uložiti kako bi izveli određeno ponašanje“ (Ajzen, 1991: 181). Na namjeru za izvođenjem ponašanja utječu tri osnovna prediktora, a oni su *stavovi prema ponašanju*, *subjektivne norme* i *percipirana kontrola ponašanja*. Stavovi prema ponašanju odnose se na specifične stavove o konkretnom ponašanju, što znači da moraju biti definirani na način da uključuju konkretnu akciju, cilj, kontekst i vrijeme (Fishbein i Ajzen, 2010). Pa tako, prema ovoj teoriji, stav prema *korištenju društvenih mreža* nije dovoljno specifičan da bi mogao predvidjeti konkretno ponašanje. Dobar primjer stava kojim bi se moglo predvidjeti ponašanje trebao bi biti specificiran kao stav prema *korištenju Facebooka za privatne potrebe u narednih šest mjeseci*. Nadalje, teorija planiranog ponašanja osim specifičnih stavova za predviđanje namjere za ponašanjem podrazumijeva i subjektivne norme, odnosno vjerovanje kako ljudi do kojih im je stalo gledaju na pojedino ponašanje. Uzmimo da osoba ima negativan stav prema korištenju Facebooka, ali osoba do koje joj je jako stalo ima silno pozitivan stav prema korištenju Facebooka. Uvjerenje o tome na koji način osobe do kojih nam je stalo gledaju na određeno ponašanje također utječe na našu namjeru za izvođenjem pojedinog ponašanja. I konačno, treći faktor je percipirana kontrola ponašanja, a odnosi se na to koliko smatramo da nam je određeno ponašanje jednostavno izvesti. Registrirati se na Facebook vrlo je jednostavno,

ali obrisati Facebook i prestati ga koristiti vrlo je teško. Ne samo zbog toga što se radi o posebno zahtjevnom postupku, iako je postupak otežan koliko god je to moguće u okvirima postojećih regulatornih normi, već zbog toga što se osoba može osjećati isključenom iz različitih društvenih događanja, isključenom od društva s kojim je do tada bila povezana i slično. Lakše bi bilo usmjeriti se prema ponašanju prilagodbe postavki privatnosti kako bi se barem do neke mjere podigla razina zaštite osobnih podataka.

Ova nam teorija može pomoći razumjeti zašto može postojati raskorak između stavova o zaštiti privatnosti i ponašanja kojim se privatnost štiti. Naime, prema teoriji, stavovi o ponašanju samo su jedan od tri elemenata koji čine namjeru za izvođenjem ponašanja. Prema tome, moguće je da ljudi koji žele bolje zaštiti svoju privatnost ne poduzimaju ponašanja kojima bi je zaštitili zbog toga što vjeruju kako ljudi do kojih im je stalo imaju negativan stav prema njihovu planiranom ponašanju i/ili zbog toga što imaju percepciju da je bi im to ponašanje bilo teško za izvesti. Bilo bi vrlo zanimljivo provesti istraživanje kojim bi se na odgovarajući način i u skladu s teorijom planiranog ponašanja mjerili stavovi, subjektivne norme i percipirana kontrola ponašanja te njihova povezanost s namjerom za izvođenjem ponašanja, odnosno izvođenjem ponašanja. Istraživanje tog tipa u potpunosti pripada području socijalne psihologije, ali rezultati i spoznaja o tome što i na koji način doprinosi ponašanju kojim se privatnost štiti ima implikacije na znatno širi spektar društvenih i humanističkih područja. Vrijedi napomenuti kako su psiholozi Dienlin i Trebte (2015) primijenili novi pristup baziran na teoriji planiranog ponašanja kako bi testirali paradoks privatnosti te oni nisu pronašli postojanje paradoksa privatnosti u situaciji u kojoj su, umjesto zabrinutosti za privatnost, kao prediktori ponašanja korišteni specifično formulirani stavovi o privatnosti te u kojoj je konstrukt privatnosti dodatno diferenciralo na informacijsku, društvenu i psihološku. No, kada su za operacionalizaciju varijabli koristili zabrinutost za privatnost te privatnost kao jedinstven konstrukt dobili su rezultate slične onima u prikazanima u prošlom poglavlju, odnosno pokazali su kako je zabrinutost za privatnost uglavnom nepovezana s ponašanjima ljudi na društvenim mrežama te da pojedinci koji su bili zabrinuti za privatnost nisu ništa manje od onih nezabrinutih za privatnost bili skloni na Facebooku objaviti svoje puno ime i prezime, broj telefona ili političke stavove (Dienlin i Trepte, 2015). Proučavajući antecedente zabrinutosti za privatnost Taddei i Contena (2013) pronašli su kako su glavni prediktori zabrinutosti za privatnost *opće povjerenje* i *percipirana kontrola* nad podacima. Za činjenicu kako zabrinutost za privatnost ne utječe direktno na razinu samootkrivanja na internetu naveli su da ona „ (…) može ukazivati na to da

korisnici interneta, a osobito mladi ljudi, nemaju štetan strah za njihovu privatnost koji određuje njihovo ponašanje na internetu, ali kako bi na njihovo saomotkrivajuće ponašanje mogli značajno utjecati percipirana kontrola nad informacijama i opća povjerljivost“ (Taddei i Contena, 2013: 825). Sundar i suradnici (2013) u eksperimentalnom su istraživanju pokazali kako je samoobjavljivanje podataka na internetu više posljedica kognitivnih heuristika nego što je posljedica dobro promišljenih odluka. U svakom slučaju, potrebna su dodatna istraživanja kako bi se stekao bolji uvid u povezanost stavova i ponašanja povezanih s privatnosti, ali čini se da zabrinutost za privatnost nije dobar prediktor samootkrivajućih ponašanja na internetu.

5.2.1.2. Utjecaj ponašanja na stavove

Čak niti nakon relativno velikog medijskog i političkog odjeka skandala koji je u ožujku 2018. godine potresao Facebook zbog prepuštanja korisničkih podataka Cambridge Analytici, tvrtki koja je te podatke koristila diljem svijeta za ciljano oglašavanje korištenjem manipulativnih tehnika kako bi bila ostvarena određena politička agenda, nije zabilježen očekivani pad korisnika Facebooka, već su podaci pokazali kako su korisnici zapravo povećali korištenje Facebooka[16] (Katner, 2018). Jednako tako, dionica Facebooka se nakon početnog pada već za svega dva mjeseca vratila na istu razinu kao i prije izbijanja skandala (Sonenshine, 2018). Ti podaci pokazuju kako je zapravo teško promijeniti ponašanje i obrisati Facebook bez obzira ne to što nam se ne sviđa način na koji koriste naše osobne podatke.

Rezultati intervjua provedenih u predistraživanju pokazali su kako sudionici vjeruju da se njihovim podacima može lako pristupiti. Istovremeno, svi su pokazali kako ne znaju što se događa s njihovim podacima nakon što ih se prikupi, no nisu pokazali ni interes saznati. Nekoliko mlađih sudionika iskazivalo je određenu desenzitizaciju prema ugrozama privatnosti, odnosno izvještavali su o pomirenosti s različitim mogućim ugrozama njihove privatnosti s kojima su bili suočeni. Sudionica S12 navela je „*Pomirila sam se s time da ne mogu sve povjerljivo napisati. Tehnologija toliko napreduje da je nerealno boriti se protiv toga.*“ Komplementarno tome, u anketnom je istraživanju dobiven rezultat prema kojem čak petina sudionika tvrdi da im *ne bi smetalo kada bi svi njihovi razgovori bili javno objavljeni*. Činjenica

[16] Takva reakcija, odnosno izostanak reakcije, nije neočekivan iz perspektive socijalne psihologije. Dio objašnjenja vjerojatno se nalazi u defanzivnoj pristranosti koju se u literaturi naziva vjerovanjem u pravedan svijet (Lerner, 1980). Radi se pogrešci koju ljudi čine prilikom atribuiranja uzroka nekom ponašanju i to na način da pretpostavljaju da se loše stvari događaju lošim ljudima, a dobre stvari dobrim ljudima. Drugi dio objašnjenja nalazi se u već poznatom fenomenu prema kojem ljudi misle da manipulacije djeluju na sve, osim na njih same. Smatraju kako su imuni na mentalno zagađenje, odnosno na neželjene utjecaje na njihove prosudbe (Wilson & Brekke, 1994).

da je i sudionica S12 u svojem intervjuu navela kako joj je privatnost važna kao i činjenica da je od petine sudionika koji su naveli kako im ne bi smetalo kada bi njihovi razgovori bili javno objavljeni njih više od 85% navelo kako im je privatnost važna govori u prilog tome da na njihovo otkrivajuće ponašanje možda nisu utjecali stavovi.

U prošlom je poglavlju opisana teorija kognitivne disonance prema kojoj ljudi u situacijama u kojima dolazi do nesklada između stavova i ponašanja imaju potrebu uspostaviti sklad. To mogu učiniti bilo prilagodbom ponašanja stavovima ili obratno. No, budući da je znatno lakše promijeniti stavove nego ponašanje, teorija kognitivne disonance govori o tome kako će ljudi prilagoditi svoja uvjerenja ponašanju znatno prije nego što će promijeniti vlastito ponašanje. Kada govorimo o privatnosti, prema teoriji kognitivne disonance možemo očekivati da će oni pojedinci koji postanu svjesni raširenog i nekritičkog nadzora, industrije prikupljanja, obrade i dijeljenja korisničkih podataka te ugroza i opasnosti koje iz njih proizlaze, puno prije, poput više sudionika u kvalitativnom istraživanju, početi vjerovati kako su oni osobno *nebitni*, kako *nikome nisu interesantni* te kako im ne smeta ako netko čita i sluša njihovu privatnu korespondenciju te će nastaviti ustrajati u aktivnostima koje su im ugodne. Jednako tako, teorija kognitivne disonance predviđa i to da bi ljudi nakon donošenja određenog izbora mogli biti skloniji odbaciti nove informacije koji taj izbor dovode u pitanje, a sve kako bi očuvali svoje samopoštovanje i zadržali kognitivni sklad. Ti mentalni procesi adaptivni su i u načelu nam pomažu funkcionirati, ali katkada nam mogu i odmoći. Na primjer, prema teoriji, odaberemo li biti prisutni na Facebooku, bit ćemo manje skloni uopće se dalje informirati o mogućim ugrozama koje proizlaze iz našeg prisustva na toj društvenoj mreži. Dođemo li u nekom trenutku u kontakt s informacijom koja govori o ugrozama koje proizlaze iz korištenja Facebooka, bit ćemo skloniji primijeniti jednu od brojnih racionalizacija ili mentalnih akrobacija kako bismo je uklopili u naše vjerovanje te ćemo pomisliti da mi zasigurno nikome nismo interesantni, da bismo zasigurno mogli prozreti bilo kakav pokušaj manipulacije te da reklame na nas ne djeluju. Tu bismo, dakako, bili sasvim u krivu. Ali sačuvali bismo kognitivni sklad i pozitivnu sliku o sebi.

Iz toga proizlazi dilema koju je dobro ilustrirati na temelju intervjua sa sudionicom S12. Naime, ona je kao i gotovo svi ostali sudionici bila svjesna kapaciteta za nadzor komunikacija, ali za razliku od većine ostalih sudionika, ona se nije u potpunosti prepustila društvu izlaganja već je navela kako vodi računa o tome što, kome i na koji način komunicira. I dok na taj način u određenoj mjeri štiti svoju privatnost od znatiželjnih očiju i ušiju, na nju se odnosi Foucaultovo

automatsko djelovanje moći te joj narušava autonomiju i u određenoj mjeri joj ograničava ostvarivanje i produbljivanje međuljudskih odnosa. Prema tome, postavlja se pitanje je li bolje brinuti o vlastitoj privatnosti i biti žrtva konstantne autocenzure preko automatskog djelovanja moći ili, kao i većina ostalih, prepustiti se nadzoru, ali uživati u besplatnim uslugama, kakvim multiplus bonovima te živjeti slobodni od autocenzure i straha od nadzora. Dakako, gubitak autonomije, a time i slobode, te odricanje od vlastite privatnosti ne može biti valjan izbor. Niti ga većina ljudi donosi svjesno. No, bez obzira na to, čini se da ipak odabiru lakši put, put izlaganja, put opće digitalne transparentnosti.

Teško je sa sigurnošću reći zašto se ljudi aktivnije ne opiru ugrozama vlastite privatnosti, zašto je se barem sami manje ne odriču. Tim više što istraživanja konzistentno pokazuju kako ih većina privatnost deklarativno smatra visoko važnom. Odgovor na to pitanje spada u područje psihologije i izlazi izvan okvira ovog rada, ali sasvim je izvjesno kako se radi o porastu opće neosjetljivosti na ugroze privatnosti zbog postepenog usvajanja novih pravila igre u digitalnom svijetu koja su postavile velike internetske tvrtke oglašivači. A to što smo sve manje osjetljivi na interne ugroze privatnosti dovodi do toga da smo sve manje osjetljivi i na eksterne ugroze. Zbog toga što često i obilno objavljujemo svoje podatke na internetu, manje nam smeta sluša li netko naše privatne razgovore. Zbog toga što objavljujemo svoje fotografije na Instagramu, manje nam smeta gleda li nas netko kroz kameru na našem računalu ili mobitelu.

5.3. Društvene implikacije

5.3.1. Hobotnica: postoji li sprega države i multinacionalnih kompanija?

Kroz ovaj rad provlače se tri ključne skupine aktera: države, tvrtke i građani. Svaki od tih aktera ima različite interese. Pojednostavljeno, države su najviše zainteresirane za vlastitu sigurnost i stabilnost, građani žele imati autonomiju, a tvrtke jednostavno žele zaraditi što više novca. Iz perspektive privatnosti, interesi tih triju aktera međusobno su suprotstavljeni i teško ih je pomiriti. No, čini se da je realnost nešto drugačija. Naime, međusobni interesi znatno su više isprepleteni nego što to tradicionalni pogled pretpostavlja. Građani i tvrtke koegzistiraju u *simbiotskoj mreži* međusobne trampe osobnih podataka, iskustava, misli i osjećaja za besplatne usluge i pristup sadržajima. S druge strane moćne obavještajne službe legalno od istih tih tvrtki prikupljaju podatke o građanima ili, ako im netko stane na put, provaljuju u njihove baze podataka. Istovremeno, velike multinacionalne tvrtke o kojima je bilo riječi u ovom radu imaju

godišnji promet višestruko veći od bruto domaćeg proizvoda mnogih razvijenih država, uključujući i Hrvatsku, te svoju moć i utjecaj koriste kako bi se države prilagodile njihovim željama.

S obzirom na razvoj tehnologije, u digitalno doba ne možemo više govoriti o državi nadzora, već o cijelom *društvu nadzora*. Harcourt za ilustraciju koristi sliku hobotnice koja je za njega „amalgam Googlea i NSA, Microsofta i NSA, Netflixa i lokalne policijske uprave, odjela za telekomunikacijske tehnologije s gornjeg kata u našoj tvrtki i lokalnog voajera koja se hrani i održava na životu našim digitalnim izlaganjem i samim tehnologijama koje su misteriozno spojile informacije i podatke u mehanizam nadzora“ (Harcourt, 2015: 79). Tu pojavu prepoznao je i Posebni izvjestitelj za promociju i zaštitu ljudskih prava i temeljnih sloboda za vrijeme borbe protiv terorizma Ben Emmerson te je u izvješću Općoj skupštini UN-a jasno izdvojio kako se države sve više oslanjaju na privatni sektor da nadzire građane za njih (United Nations, 2014b), a Visoki povjerenik za ljudska prava takvu je praksu opisao kao „delegiranje represivnih i kvazi-pravosudnih odgovornosti internetskim posrednicima“ (United Nations, 2014d: 14) što je ocijenio zabrinjavajućim te je pozvao privatne tvrtke da državne zahtjeve pravno tumače što uže te da svaki zahtjev kojim bi se prekršilo međunarodno pravo dovedu u pitanje.

Opravdano se postavlja pitanje trebamo li u digitalnom dobu redefinirati sam pojam države (Harcourt, 2015). Whitaker je još 1999. godine, u vrijeme kada je cijeli Google bio tek mladi dvojac u garaži, a Facebook je od te faze bio udaljen pet godina, pisao o izazovima digitalnog doba za opstanak države (Whitaker, 1999). Posebno je znakovito još ranije predviđanje Mowshowitza koji je već pri prvoj pojavi interneta 1992. godine vidio propadanje pa čak i kraj nacionalne države. Jednostavno, u dramatično drugačijem načinu organizacije i komunikacije vidio je sličnost s razlikom između načina na koji je država bila uređena u feudalizmu s dramatičnom promjenom koju je donijela pojava kapitalizma pa je cijelu svoju ideju gubitka financijske i političke moći država u koristi privatnih centara moći u toj novoj umreženoj stvarnosti nazvao *virtualnim feudalizmom* (Mowshowitz, 1997). Sve šira primjena *blockchain* tehnologije koja omogućuje uspostavu decentraliziranog i distribuiranog povjerenja dovest će do slabljenja utjecaja moćnih društvenih aktera kao što su banke i osiguravajuća društva, ali i slabljenja državnog autoriteta kroz slabljenje različitih državnih registara, javnih bilježnika, patentnih ureda i slično. Blockchain tehnologija kroz decentralizirano i distribuirano povjerenje

dokida držani monopol na potvrđivanje legitimiteta, identiteta i točnosti, čime značajno slabi njezinu ulogu.

5.3.1.1. Suverenitet

I doista, čini se da su Mowshowitz, Whitaker i drugi bili puno bliže istini nego što bismo to željeli priznati. Google je u 2016. godini imao preko 90 milijardi dolara prometa i gotovo 20 milijardi dolara neto dobiti. Facebook zaostaje sa 27 milijardi dolara prometa i 10 milijardi dolara neto dobiti. Bruto nacionalni dohodak Republike Hrvatske za 2016. godinu bio je oko 50 milijuna dolara ili dvije tisuće puta manje od Googleovog godišnjeg prometa. Europska unija sa svojim snažnim nasljeđem poštivanja ljudskih prava i temeljnih sloboda uspijeva se nekako nositi s pritiscima multinacionalnih tvrtki, ali pojedine države, pa čak i one najveće, vrlo se teško mogu samostalno nositi s tehnološkim divovima.

No, osim novca i političke moći, državama znatno veći problem predstavlja sama priroda tehnologije. Dok iz svoje radne sobe na osobnom računalu pišemo e-poruku putem Gmaila, tekst koji unosimo u pretraživač gotovo trenutno sprema se na Googleove poslužitelje diljem svijeta. Naši podaci u treptaju oka napuštaju Republiku Hrvatsku i njezina regulatorna tijela, represivne organe i pravosudni sustav te odlaze izvan njihova dosega na poslužitelje u Aziji, SAD-u ili čak izvan bilo koje jurisdikcije u podatkovne centre koji plutaju međunarodnim vodama (Carroll, 2013). Europska unija pokušava dosljedno provoditi standarde zaštite osobnih podataka te je upravo u tijeku velika reforma pravnih dokumenata o osobnim podacima i privatnosti na internetu. No, unatoč astronomskim kaznama i strogim propisima realnost ostavlja gorak okus unaprijed izgubljene bitke. Tehnološki, politički i potrošački trendovi nisu na strani bolje zaštite prava na privatnost, a eurozastupnici su već danas izloženi stalnom pritisku lobista multinacionalnih tvrtki, vlada nacionalnih država i građana skeptičnih oko zaštite privatnosti. Najbolji je primjer nedavno produženje valjanosti sekcije 702 nepopularnog američkog zakona FISA (Foreign Intelligence Surveillance Act – engl.) krajem 2017. godine temeljem kojeg se provodi masovni nadzor i praćenje neameričkih državljana. Unatoč otkrićima zviždača, burnoj reakciji šefova najjačih država svijeta na otkriće razmjera masovnog nadzora koje SAD provode, ta je praksa nedavno legalizirana na razdoblje od dodatnih deset godina. Znakovito je kako se uskoro očekuje i revizija procjene Suda Europske unije načina na koji zakonodavstvo SAD-a štiti prava na privatnost europskih klijenata i može li biti dopušteno američkim tvrtkama iznositi osobne podatke Europljana na poslužitelje u SAD. Ove dvije odluke značajno su povezane. Naime, iz dosadašnjih odluka Suda Europske unije, a osobito iz

presude u slučaju Schrems protiv Data Protection Commissioner (Sud Europske unije, 2015) kojom je ukinuta Odluka Europske komisije o tome kako načela privatnosti u SAD-u pružaju „sigurnu luku“, evidentan je eksplicitan stav Suda kako programi masovnog nadzora koje primjenjuje SAD nisu nužni ni proporcionalni te kako stranci koji su predmet nadzora nemaju pravo propitkivanja postupanje prema njima. Zbog toga sasvim je izgledno kako bi Sud mogao zauzeti dosljedan stav i pri procjeni opravdanosti prijenosa podataka o Europljanima u SAD, što bi moglo najviše pogoditi internetske gigante kojima je takva praksa poslovni model. Postojala je određena nada da bi se najveće internetske tvrtke mogle pri nedavnoj reviziji Sekcije 702 FISA-e zauzeti za veću zaštitu neameričkih državljana i bolju zaštitu privatnosti od američkih obavještajnih službi (O'Brien, 2017). Međutim, unatoč tome što bi ovakav preokret unutar amalgama društva nadzora mogao predstavljati moguću točku preokreta u kontinuiranoj transformaciji privatnosti i derogiranju prava na privatnost, on je bio sasvim malo izgledan i nažalost nije se dogodio.

Kapaciteti najvećih obavještajnih službi za nadzor komunikacija, kao što su mogućnosti masovnog nadzora koje primjenjuju službe iz Five Eyes alijanse, a osobito NSA i GCHQ, toliko su moćni da im se nijedna pojedina država ne može suprotstaviti. Ako NSA snima sav internetski promet na interkontinentalnim optičkim kablovima, ako pomoću opreme u veleposlanstvima i konzulatima snima komunikaciju iz etera, ako ciljano ugrađuje zlonamjerni hardver i softver u računala i druge elektroničke uređaje, nijedna nacionalna država ne može joj se suprotstaviti. Budući da su u liberalnoj demokraciji nositelji ljudskih prava građani, a ta im prava osigurava nacionalna država, postavlja se pitanje može li s obzirom na razvoj tehnologije pravo na privatnost u virtualnom prostoru danas uopće biti zaštićeno. Nadalje, jesu li nacionalne države uopće suvereni nad digitalnom tehnologijom koju koriste njihovi građani na njihovom teritoriju? Po svemu sudeći, nisu. Digitalna tehnologija toliko je decentralizirana da ju je vrlo teško kontrolirati i njome upravljati, a širenje učinkovite *end-to-end* enkripcije, korištenje VPN tunela, *blockchain* tehnologije i decentraliziranih anonimnih kriptovaluta državi ne ostavljaju mnogo prostora za demonstraciju vlastita suvereniteta. Neke od navedenih tehnologija već su ušle u široku uporabu, a ostale galopiraju prema masovnoj uporabi znatno brže nego što im se trome birokracije mogu prilagoditi. Raširena primjena navedenih tehnologija radikalno će izmijeniti odnos države i pojedinca i drastično će smanjiti utjecaj i moć države.

5.4. Održivost (transformiranog) pojma prava na privatnost

O transformaciji prava na privatnost iz ljudskog prava u robu kojom se trguje još je 1997. godine pisao Simon Davies: „Ono što se pojavilo još 1980. godine jest pomak u percepciji privatnosti i ugroza privatnosti, a ne smanjenje zabrinutosti javnosti. Rezultat je ravnodušnost koja sputava potrošački i politički aktivizam čak i prema najočitijim ugrozama privatnosti." (Davies, 1997: 144). Točno se to i dogodilo. S time da je od 1997. godine do danas razvoj tehnologije dodatno doveo do pojave pametnih telefona, društvenih mreža i opće digitalne umreženosti, što je Daviesova predviđanja dodatno intenziviralo. Paralelno s razvojem tehnologije, nakon napada na Svjetski trgovinski centar u New Yorku 2001. godine mijenjala se i sigurnosna paradigma te su novi sigurnosni izazovi doveli do jačanja države nadzora. Time su i države postale motivirane ne regulirati korporativno ugrožavanje privatnosti, što je omogućilo još snažniju transformaciju pojma privatnosti. Danas su pojam privatnosti i ideja ugroze privatnosti radikalno redefinirani. Na davanje osobnih podataka pristajanjem na korištenje Gmaila ili Facebooka danas se ne gleda kao na ugrozu privatnosti već kao na nužnost koja nema alternative.

No, je li tako transformiran pojam prava na privatnost u skladu s jednom od temeljnih postavki liberalne demokracije prema kojoj je nacionalna država dužna osigurati zaštitu ljudskih prava svojih građana? Je li činjenica da se s privatnosti danas trguje uopće spojiva s temeljima liberalne demokracije? Nije. Trgovanje bilo kojim ljudskim pravom nije u skladu s liberalnom demokracijom. Kroz normativnu raspravu o intrinzičnoj i instrumentalnoj vrijednosti privatnosti detaljno je obrazloženo kako je privatnost temeljno ljudsko pravo koje istovremeno ima svoj značaj za pojedinca, društvo, političku zajednicu i demokraciju. Takvim pravom nije moguće trgovati i nije ga se moguće odreći. Svaka država koja se smatra liberalno-demokratskom morala bi poduzeti odgovarajuće mjere kako bi zaštitila privatnost svojih građana.

Suočimo li privatnost definiranu kao temeljno ljudsko pravo koje ima značaj za autonomiju, slobodu i demokraciju s eksternim i internim ugrozama privatnosti opisanima u drugom poglavlju, odnosno sa sveobuhvatnim nekritičkim državnim nadzorom i istovremeno raširenim odricanjem od privatnosti kroz samoobjavljivanje i samootkrivanje osobnih podataka, dolazimo do zaključka kako je postojeća razina zaštite privatnosti neodrživa u okvirima liberalne demokracije. Način na koji se države odnose prema privatnosti svojih građana, način na koji se

tvrtke odnose prema privatnosti svojih klijenata i zaposlenika te, ono najozbiljnije, način na koji se sami građani odnose prema vlastitoj privatnosti jednostavno nije održiv u liberalno-demokratskom sustavu vrijednosti. Tako će biti dokle god privatnost definiramo na način na koji je ona definirana u ovom radu, kao temeljno ljudsko pravo vrijedno zaštite zbog svojeg instrumentalnog značaja za dostojanstvo i autonomiju svakog čovjeka, za uspostavu i održavanje bliskih međuljudskih odnosa, za razvoj kritičke misli, za slobodu i demokraciju.

5.4.1. Što dalje?

Postoje samo dva načina na koje je moguće razriješiti problem prema kojem je postojeća razina zaštite privatnosti neodrživa u okvirima liberalne demokracije: ili je potrebno odbaciti privatnost kao temeljno ljudsko pravo i prihvatiti transformirani pogled na privatnost, ili je privatnost potrebno na dosljedan i učinkovit način osiguravati, štititi i vrednovati.

Kada bismo na normativnoj razini prihvatili transformirani pogled na privatnost i pogled na ugroze privatnosti, morali bismo privatnost odbaciti kao temeljno ljudsko pravo i početi je smatrati tek nečim poželjnim, nečime što se može odbaciti, čega se može odreći i što se može oduzeti. Ili bi se privatnost moglo početi smatrati čak i nečim nepoželjnim. Podsjetimo kako je u kvalitativnom dijelu istraživanja pronađeno kako su pojedini sudionici isticali *manjak samopouzdanja* i *zlonamjernost drugih* kao ljudske karakteristike zbog kojih su privatnost u ovom trenutku smatrali nužnom. Prema njima, kada bi ljudi bili oslobođeni vlastitih kompleksa i/ili kada drugi ljudi ne bi bili zlonamjerni, privatnost nam uopće ne bi bila potrebna. Bilo kako bilo, ukoliko bismo odbacili pravo na privatnost kao temeljno ljudsko pravo vrijedno učinkovite zaštite i uvažavanja unutar okvira liberalne demokracije, tada bi se doista mogao zadržati ovakav transformirani pogled na privatnost i bilo bi legitimizirano neosiguravanje privatnosti unutar liberalnih institucija. Međutim, na taj bi se način istovremeno otvorio još veći problem za liberalnu demokraciju budući da bi u tom slučaju bilo potrebno unutar liberalnog diskursa opravdati ukidanje statusa temeljnog ljudskog prava koje privatnost trenutno uživa. S obzirom na argumentaciju iznesenu u ovome radu, odnosno na značaj privatnosti za autonomiju i demokraciju, za dostojanstvo i međuljudske odnose, to naprosto nije moguće napraviti unutar okvira liberalne demokracije. U Izvješću o programu nadzora Agencije za nacionalnu sigurnost SAD-a (NSA), nadzornim tijelima u različitim državama članicama i njihovu utjecaju na temeljna prava građana EU-a, te o transatlantskoj suradnji u pravosuđu i unutarnjim poslovima koje izvjestitelja Claudea Moraesa, usvojenom na Odboru za građanske slobode, pravosuđe i

unutarnje poslove Europskog parlamenta stoji kako su „(…) temeljna prava, uključujući pravo na privatnost, zaštitu podataka, slobodu tiska i pravično suđenje sadržani u Ugovorima EU, Povelji o temeljnim pravima i Europskoj konvenciji o ljudskim pravima. Ova prava ne mogu se zaobići niti se može pregovarati o bilo kakvoj prednosti koja bi se ostvarila u zamjenu za njih, osim ako je drugačije propisno propisano pravnim instrumentima i u potpunosti u skladu s ugovorima.“ (Moraes, 2014: 48). Stoga je mogućnost redefiniranja i transformacije privatnosti na normativnoj razini potrebno odbaciti kao jedan od načina usklađivanja postojeće razine ugrožavanja privatnosti s temeljnim postavkama liberalne demokracije.

Prema tome, jedini preostali način za usklađivanje tenzije između trenutne neodgovarajuće razine poštivanja prava na privatnost i temeljnih postavki liberalne demokracije jest taj da se žurno započne na dosljedan i učinkovit način osiguravati barem minimalnu razinu prava na privatnost. No, i ovo rješenje sa sobom povlači vrlo ozbiljne probleme. Najprije, interne ugroze privatnosti pokazuju kako značajan dio ugroza privatnosti dolazi od samih građana, odnosno njihovo ponašanje ukazuje na to da im vlastita privatnost nije važna. Ovi su nalazi potvrđeni i u empirijskom istraživanju. Dok je doista 90% sudionika deklarativno navelo kako im je privatnost važna ili izrazito važna, bihevioralne mjere pokazale su kako tek rijetko poduzimaju ponašanja kojima štite svoju privatnost. Kada govorimo o internim ugrozama privatnosti, najbolju sliku razine odricanja od privatnosti daje upravo podatak o tome kako 99% sudionika za pretraživanje interneta koristi Google, Bing ili Yahoo, kako čak 86% sudionika koristi Gmail, Yahoo mail ili Microsoft mail, kako ih je 88% prisutno na Facebooku gdje većina njih objavljuje svoje osobne podatke. Značajan dio drugog poglavlja posvećen je opisivanju opasnosti koje proizlaze iz odricanja od privatnosti i odavanja svojih osobnih podataka upravo navedenim tvrtkama.

Iz toga je moguće zaključiti kako je pojam privatnosti već transformiran do te mjere da su građani internalizirali odricanje od privatnosti. Iako je većina sudionika deklarativno isticala važnost privatnosti, svojim ponašanjem pokazali su kako je se lako odriču. Vrijedi istaknuti i kako je čak 20% sudionika već i na deklarativnoj razini navelo kako je privatnost *relikt prošlosti* te kako je *zaštita privatnosti uzaludan posao*. S obzirom na ovako raširenu pojavu internih ugroza privatnosti, odnosno olakog odricanja vlastite privatnosti, bilo koje nastojanje države da ponovo etablira privatnost kao temeljno ljudsko pravo, da dodatno i dosljedno regulira ograničavanje prava na privatnost moglo bi kod građana izazvati suprotan učinak. Dodajmo tome i to da države uopće nisu ni motivirane dosljedno regulirati ograničavanje prava na

privatnost i povećati zaštitu privatnosti budući da im postojeće stanje odgovora pa je lako uvidjeti problem i s ovim pristupom usklađivanju tenzije između trenutne neodgovarajuće razine poštivanja prava na privatnost i temeljnih postavki liberalne demokracije.

U normativnoj raspravi izložena je ideja perfekcionističkog liberalizma Josepha Raza prema kojoj postoji jasna uloga države u zaštiti autonomije pojedinca. Budući da liberalne demokracije ovise o autonomnim pojedincima, a privatnost je konceptualno i kauzalno povezana s autonomijom, svako ugrožavanje privatnosti istovremeno je ugrožavanje autonomije. Prema tome, liberalno-demokratske države imaju dužnost, radi očuvanja temeljnih vrijednosti na kojima su utemeljene, ali i vlastitoga opstanka, osigurati očuvanje autonomije svojih građana. Međutim, država istovremeno ima i direktne koristi od postojeće razine odricanja prava na privatnost. To što su građani zbog svojevoljnog izlaganja na Instagramu i Facebooku manje osjetljivi na ugroze privatnosti, država koristi za slobodniju primjenu vlastita nadzora, koji osim primarnog cilja suprotstavljanja prijetnjama sigurnosti ima i sekundarne pozitivne posljedice za državu - usklađivanje ponašanja građana s očekivanim normama zbog automatskog djelovanja moći preko *očigledne sveprisutnosti*.

No, čak kada bi država unatoč svemu tome iz ideoloških razloga i predanosti ideji liberalne demokracije i vladavini ljudskih prava ili radi puke zaštite vlastitih liberalno-demokratskih institucija od manipuliranih građana lišenih osobne autonomije, htjela zaštiti pravo na privatnost svojih građana, problem je u tome što bi to morala činiti *protiv volje* vlastitih građana. Bilo kakva pojačana regulacija radi povećanja privatnosti korisnika i radi učinkovitijeg i dosljednijeg osiguravanja prava na privatnost otežala bi ili onemogućila korištenje društvenih mreža, za posljedicu bi imala (skupo) plaćanje brojnih trenutno besplatnih usluga te bi izazvala val nezadovoljstva i velik otpor upravo među građanima koji bi se zauzimali za svoje pravo za odricanjem od privatnosti. Pravo za odricanjem od autonomije, pravo za derogiranjem demokracije.

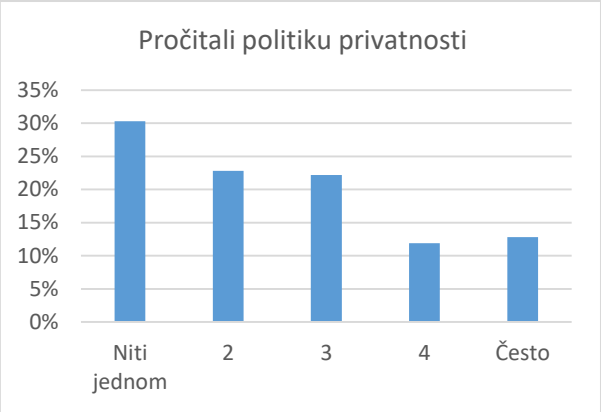
> Mora postojati spoznaja da, osim ako se potrošači ne počnu truditi istinski razumjeti ono za što daju pristanak i kome sve daju svoje osobne podatke, njihov osjećaj osobne privatnosti nastavit će se pogoršavati. Kako ljudi sve više koriste kanale podatkovne razmjene kao što je Internet, tako dramatično raste potreba za razumijevanjem kamo odlaze podaci. (Norberg, Horne i Horne, 2007: 120).

5.4.1.1. Pristanak

Nedugo nakon Snowdenovih objava, izvjestitelj Odbora za građanske slobode, pravosuđe i unutarnje poslove Europskog parlamenta u prihvaćenom Izvješću o programu nadzora Agencije

za nacionalnu sigurnost SAD-a (NSA) postavio je nekoliko pitanja kojima je jasno sugerirao smjer u kojem će se europska legislativa kretati u pogledu zaštite privatnosti i osobnih podataka građana: „Je li situacija stvorena Snowdenovim otkrićima pokazatelj općeg društvenog zaokreta prema prihvaćanju kraja privatnosti u zamjenu za sigurnost? Suočavamo li se s ugrozama privatnosti i intimnosti toliko velikim da je ne samo kriminalcima već i IT tvrtkama i obavještajnim službama omogućeno znati svaki detalj života građana? Je li ta činjenica prihvaćena bez daljnje rasprave? Ili je odgovornost zakonodavca prilagoditi postojeće politike i pravne instrumente kako bi ograničio rizike i spriječio daljnju štetu u slučaju da na vlast dođi manje demokratični igrači?“ (Moraes, 2014: 48). Dakako, izvješće nije stalo na postavljanju retoričkih pitanja već je njime jasno zadan akcijski plan usvajanja europskoga digitalnoga *Habeas corpusa*, instituta koji u digitalnom dobu štiti temeljna osobna prava i slobode od samovoljnog uplitanja države, u osam točaka. U pogledu zaštite osobnih podataka u Europskoj uniji posebno je značajna Uredba o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka tzv. GDPR direktiva, koja je stupila na snagu u svibnju 2018. godine. Iako ta direktiva ne govori izrijekom o privatnosti, njome će razina zaštite osobnih podataka građana Europske unije značajno porasti. Barem u teoriji. Naime, uredba predviđa davanje jasnog i eksplicitnog pristanka za svaki pojedinačni oblik prikupljanja, obrade i analize osobnih podataka te za njihovo korištenje za svaku pojedinu svrhu.

Međutim, ljudi izuzetno olako daju pristup svojim podacima. Svakako je dobro što će umjesto tisuća stranica nejasnoga teksta obrazloženje onoga što se čini s korisničkim podacima sada biti znatno jasnije navedeno i transparentno, ali iluzorno je očekivati da će značajno manje ljudi pristati na te uvjete. Uostalom, alternativa u slučaju nedavanja suglasnosti bit će nemogućnost korištenja usluga, a ne nastavak korištenja bez prikupljanja njihovih podataka. Dosadašnja reakcija javnosti na skandale zlouporabe korisničkih podataka pokazuje kako nije realno očekivati značajnije uskraćivanje pristanka za prikupljanje i korištenje osobnih podataka. U provedenom empirijskom istraživanju od sudionika je zatraženo da procijene koliko su puta u proteklih šest mjeseci pročitali politiku privatnosti prije registracije na internetsku stranicu ili prije instaliranja aplikacija na mobilni telefon. Rezultati su pokazali kako 30,3% sudionika politiku privatnosti nije pročitalo niti jednom, a 22,8% to je činilo rijetko (slika 11.)



Slika 11. - Udjeli odgovora procjene slaganja s tvrdnjom „U telefonskom razgovoru prešutjeli reći nešto što ste željeli reći iz straha od prisluškivanja“, pri čemu 1 označava odgovor uopće se ne slažem, a 5 označava odgovor u potpunosti se slažem

Prema tome, uzmemo li u obzir koliko olako ljudi daju pristanak za pristup svojim podacima možemo očekivati kako će GDPR direktiva dovesti do toga kako će većini korisnika opetovano davanje pristanka samo predstavljati gnjavažu koju će željeti što prije izbjeći kako bi mogli pristupiti sadržaju i uslugama. Na sličan se način provodi tzv. Direktiva o e-privatnosti ili Direktiva o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Europski parlament i Vijeće Europske unije, 2002), osobito u dijelu u kojem svaka internetska stranica prije korištenja kolačića mora ishoditi informirani pristanak korisnika. Upravo je zbog toga upravo u postupku donošenje nove, moderne direktive o e-privatnosti koja će zajedno s GDPR direktivom nesumnjivo dići razinu zaštite osobnih podataka i privatnosti korisnika.

Međutim, s obzirom na razinu do koje je pojam privatnosti već transformiran te na lakoću kojom se pojedinci odriču svoje privatnosti i kontrole nad svojim osobnim podacima teško je biti optimističan. Nije realno očekivati da će ove direktive zaustaviti nastavak transformacije pojma privatnosti, a kamoli da će uspjeti preokrenuti trendove. Globalna priroda interneta značajno otežava njegovu regulaciju. A kada bi na razini kreatora politika i postojao globalni konsenzus oko zaštite privatnosti, sasvim je izvjesno kako bi se građani vrlo žustro usprotivili bilo kakvom pokušaju zaštite njihove privatnosti koji bi im otežao ili poskupio korištenje usluga na koje su naviknuli. Prema tome, osim ako se ne dogodi katastrofalna zlouporaba privatnosti ili korisničkih podataka zbog koje će stotine milijuna ljudi diljem svijeta osjetiti konkretne posljedice, trend transformacije pojma privatnosti će se polako nastaviti. Privatnost će ljudima sve manje značiti i sve će je teže biti osigurati.

Zaključak

Osnovni cilj ove disertacije bio je utvrditi je li zbog rapidnog razvoja tehnologije i novih sigurnosnih izazova u posljednjih petnaestak godina došlo do transformacije pojma prava na privatnost. Problemu se pristupilo s dvije razine i to u normativnoj raspravi s razine nacionalne države te u empirijskom istraživanju s razine građana. Na prvoj razini prikazana je detaljna normativna rasprava o transformaciji pojma prava na privatnost koja je propitkivala koliko je uopće koncept prava na privatnost održiv u današnjem kontekstu. Specifičnost ovog istraživanja jest u tome što osim odozgo, iz perspektive legitimiteta nacionalne države, problemu transformacije pojma prava na privatnost pristupilo se i odozdo, iz perspektive građana. Teorijska rasprava o pravu na privatnost suočena je s podacima dobivenim empirijskim istraživanjem u pokušaju boljeg razumijevanja evidentne normativne i manifesne transformacije prava na privatnost.

No, najprije je privatnost definirana kao mogućnost kontrole pristupa (podacima o) sebi. Upravo je kontrola ključan dio definicije privatnosti. S jedne strane sama potreba za zaštitom intime i sebstva omogućuje pojedincima razvoj autonomije. Istovremeno, mogućnost odabira hoćemo li, kome i kada otkriti sebe, nužna je za uspostavljanje i održavanje intimnih veza. S obzirom na utemeljene argumente feminističke i komunitarne kritike privatnosti kao i suvremene višedimenzionalne i kontekstualne konceptualizacije privatnosti, definiciji privatnosti u terminima kontrole pristupa (podacima o) sebi u ovom radu dan je osobito snažan integrativni i kontekstualni naglasak kroz višekratno isticanje dispozicijskih, situacijskih i kulturalnih razlika u doživljavanju i manifestiranju potreba za privatnosti. Jednako tako u razmišljanju o privatnosti kao temeljnom ljudskom pravu i njezinoj vrijednosti osobito je naglašen značaj privatnosti za društvo u cjelini.Nadalje, prikazane su ugroze privatnosti, koje su prema stupnju kontrole koju pojedinac nad njima ima ugrubo podijeljene na interne i eksterne ugroze privatnosti, odnosno na one ugroze u kojima kontrolu nad (podacima o) nama nekome dobrovoljno predajemo ili nam je netko oduzima bez našega znanja i/ili volje. Na primjeru masovnog nekritičkog nadzora koji provode pojedine strane obavještajne službe prikazane su opasnosti koje proizlaze iz eksternih ugroza privatnosti. S druge strane za ilustriranje opasnosti koje proizlaze iz internih ugroza korišten je odnos najvećih svjetskih informacijskih tvrtki prema korisničkim podacima, a posebice činjenica kako ljudi olako prepuštaju svoje osobne podatke u zamjenu za digitalne usluge ili trgovačke pogodnosti. Značajan doprinos ovog rada literaturi koja proučava privatnost jest upravo u ovoj jedinstvenoj kategorizaciji ugroza

privatnosti uz detaljan i temeljit prikaz mnoštva konkretnih i aktualnih primjera pojedinih ugroza. Takvom podjelom ugroza istaknut je dvojaki utjecaj na transformaciju pojma prava na privatnost, kako onaj eksterni, tako i interni, o kojem se u literaturi o privatnosti znatno manje govori.

Kroz normativnu raspravu o intrinzičnoj i instrumentalnoj vrijednosti privatnosti detaljno je obrazloženo kako je privatnost temeljno ljudsko pravo koje istovremeno ima svoj značaj za pojedinca, društvo, političku zajednicu i demokraciju. Na taj način definirana privatnost suočena je s opsegom i razinom eksternih i internih ugroza privatnosti s kojom smo danas suočeni te je zaključeno kako je pojam privatnosti radikalno transformiran iz temeljnog ljudskog prava u robu kojom se trguje.

Kao što je ranije navedeno, poseban značaj ovog rada jest u tome što je normativna rasprava nadopunjena ekstenzivnim i obuhvatnim empirijskim istraživanjem kojim su u dva zasebna dijela kvalitativnim i kvalitativnim metodama prikupljeni određeni vrlo vrijedni podaci o načinu na koji ljudi razumiju privatnost. U provedenom kvalitativnom predistraživanju metodom polustrukturiranog intervjua prikupljena su saznanja o tome kako ljudi o privatnosti vrlo rijetko razmišljaju, ali kada o njoj razmišljaju većini je vrlo važna i drže do nje. Spoznaje iz predistraživanja iskorištene su za kvantitativno istraživanje koje je provedeno na uzorku od gotovo 1000 sudionika, što je velik broj osobito za istraživanja ovog tipa. Primarni cilj bio je testirati postojanje paradoksa privatnosti, odnosno postojanja nesklada između visoke važnosti privatnosti za pojedince i lakoće kojom su je se spremni odreći. Rezultati su potvrdili postojanje paradoksa privatnosti, odnosno sudionici koji su najviše vrednovali svoju privatnost iskazivali su kako se ponašaju na način statistički značajno različit od onog koji bi se mogao očekivati od osoba koje visoko vrednuju svoju privatnost. Pritom je dodana vrijednost i u korištenju triangulacije metoda, odnosno u povezivanju kvalitativne analize provedene u predistraživanju s kvantitativnom analizom provedenom na razmjerno velikom uzorku, što doprinosti valjanosti istraživanja budući da se različite metode međusobno upotpunjuju i kontroliraju.

Osim potvrde postojanja paradoksa privatnosti, u kvalitativnom i u kvantitativnom istraživanju prikupljeni su brojni empirijski podaci koji su doprinijeli boljem razumijevanju načina na koji pojedinci shvaćaju privatnost. Ti su podaci u potpunosti komplementarni sa zaključkom normativne rasprave o radikalnoj transformaciji pojma privatnosti. Rezultati istraživanja pokazuju kako većina ljudi i dalje deklarativno visoko vrednuje važnost privatnosti. No,

istovremeno su tek umjereno zabrinuti za privatnost te, ono značajnije, tek rijetko iskazuju ponašanja kojima štite vlastitu privatnost. Prema tome, zaključeno je kako je trenutni odnos pojedinaca prema vlastitoj privatnosti te odnos država prema privatnosti svojih građana nespojiv s temeljnim postavkama liberalne demokracije. Budući da se temeljno ljudsko pravo na privatnost unutar liberalno-demokratske paradigme ne može normativno redefinirati, potrebno je bez odgode početi na odgovarajući način osiguravati, štititi i vrednovati pravo na privatnost svakog čovjeka.

Međutim, zbog rasprostranjenosti dobrovoljnog odricanja od privatnosti radi pristupa različitim uslugama i pogodnostima, osiguravanje prava na privatnost države bi trebale provesti unatoč želji svojih građana da ga se odreknu. Iako bi ovakav paternalizam u određenoj mjeri mogao biti opravdan unutar liberalne paradigme, nerealno je očekivati da će se realizirati. Tim više što su države i same motivirane zadržati postojeće stanje budući da su građani zbog smanjene osjetljivosti na interne ugroze istovremeno postali manje osjetljivi i na eksterne ugroze privatnosti. Današnji potrošač želi besplatnu uslugu, trgovačke pogodnosti i popuste, precizne preporuke, skrojene reklame i smatra kako je dijeljenje osobnih podataka mala cijena za to.

Unatoč tome što su pažljivom pripremom poduzete mjere kako bi njihov značaj bio sveden na najmanju moguću mjeru, ovaj radi ima određena ograničenja. Prvo, i najveće, proizlazi iz činjenice da je radi pisan iz liberalne paradigme te su njezine temeljne postavke aksiomatski uzete kao zadane. Imajući to na umu, na više mjesta u radu pružen je elementarni uvid u alternativne poglede na privatnost kao i na kritike pojma. Komunitarna i socijalistička kritika na privatnost gledaju kao na nepotrebni, pa i štetni, nusprodukt individualizma. S druge strane post-strukturalistička kritika dovodi u pitanje samu cjelovitost subjekta, odnosno postavlja pitanje postoji li uopće autentična unutarnja jezgra koja bi mogla biti nositelj ljudskih prava ili je ona tek produkt našeg doživljaja cjelovitosti. Radi se o vrlo intrigantnim pitanjima na koja je potrebno pronaći odgovore, ili barem otvoriti široku znanstvenu raspravu, međutim, to je pothvat koji izlazi izvan okvira ovog rada, kako sadržajem, tako i opsegom.

Osim toga, samo empirijsko istraživanje ima više ograničenja. Ona su dominantno vezana uz metodologiju te donekle ograničavaju vanjsku valjanost dobivenih rezultata, odnosno ograničavaju njihovu poopćivost na populaciju. Među njima, značajnije se ističe problem reprezentativnosti uzorka sudionika u kvantitativnom istraživanju. Naime, unatoč tome što je u istraživanju sudjelovalo relativno mnogo sudionika, uzorak je bio prigodan te je značajno

odudarao od hrvatskoga prosjeka u udjelu sudionica u uzorku te još i više prema obrazovanosti uzorka. Za spol ne postoji niti jedna teoretska pretpostavka koja bi ukazivala da bi mogao predstavljati značajni problem pri interpretaciji rezultata, a ta je pretpostavka dijelom i potvrđena budući da ni na jednoj mjeri zabrinutosti za privatnost nisu pronađene razlike među spolovima.

Slično tome, empirijski je provjeren i mogući utjecaj stupnja obrazovanosti sudionika na način da su uspoređene razlike u rezultatu na mjerama stavova i na bihevioralnim mjerama prema različitim kategorijama najviše završenog obrazovanja. Rezultati su pokazali kako na jednoj od dvije mjere stavova nije pronađen nikakav utjecaj obrazovanja na rezultat, dok su na drugoj mjeri jedino sudionici koji su završili postdiplomski studij imali statistički značajno viši rezultat od onih koji su završili diplomski ili dodiplomski studij. Razlike između svih ostalih razina obrazovanja na mjerama zabrinutosti za privatnost nisu pronađene. Slični rezultati dobiveni su i na bihevioralnim mjerama gdje nisu pronađene nikakve razlike u obrazovanju na dvama faktorima, a jedino na faktoru općeg opreza utvrđena je kako su sudionici koji su završili postdiplomski i diplomski studij imali statistički značajno viši rezultat od onih koji su kao najviši završeni stupanj obrazovanja odabrali srednju školu ili niže. Uzevši u obzir da je u korištenom uzorku bilo čak 14% sudionika koji su završili postdiplomski studij te čak 55% sudionika koji su završili diplomski ili dodiplomski studij te da je potvrđeno kako jedino te dvije kategorije imaju statistički značajno veći rezultat na dvije od pet korištenih mjera, možemo zaključiti da je neproporcionalno visoko udio tih sudionika u uzorku mogao djelovati u smjeru suprotnome od hipoteze, odnosno mogao je otežati njezino potvrđivanje. Prema tome, utjecaj visoke obrazovanosti uzorka bio je vrlo malen te je otežao potvrđivanje paradoksa privatnosti.

Ovim radom otvorena su brojna pitanja na koja nije bilo moguće odgovoriti bilo zbog toga što sadržajem, bilo zbog toga što opsegom izlaze izvan zadanog okvira. Osim spomenutih alternativnih pogleda na privatnost te uopće na cjelovitost subjekta, otvoreno je i nekoliko pitanja unutar liberalne paradigme. Nakon spoznaje kako značajnom broju sudionika nije stalo do privatnosti, postavlja se pitanje zbog čega je tome tako i što bi se moglo učiniti da ljudi više brinu za svoju privatnosti. Gledaju li ljudi na značaj i vrijednost privatnosti, te iskazuju li češće ponašanja kojima je štite, nakon što su svjesno bili izloženi (ozbiljnoj) ugrozi vlastite privatnosti? Nameće se i pitanje povezanosti razlika u osobinama ličnosti između sudionika svrstanih u različite skupine prema stupnju njihove zabrinutosti za privatnost. Postoji li kakva

sustavna razlika u osobinama ličnosti između tzv. fundamentalista, nezainteresiranih i pragmatičnih sudionika. Ovo su samo neka od brojnih pitanja koje je ovaj rad otvorio i na koje autor planira pokušati dati odgovor u svojem budućem znanstveno-istraživačkom radu.

Pitanje transformacije pojma prava na privatnost doista je danas aktualnije nego ikada. Radi se o raspravi koju vode parlamenti najvećih država Europe i Europski parlament, a u SAD-u je održano nekoliko kongresnih saslušanja na temu ugrožavanja privatnosti. Pitanja državnog i korporativnog nadzora u posljednjih nekoliko godina poprimaju i svoje pravosudne dimenzije, a prve presude već su objavljene. Najveći svjetski mediji redovito izvještavaju o transformaciji pojma prava na privatnost, a i akademska zajednica pokazuje sve veći interes za tom gorućom temom. Harari smatra kako će upravo „pitanje reguliranja vlasništva nad podacima biti najvažnije političko pitanje našega doba“ te nastavlja pesimistično „Ukoliko uskoro ne uspijemo pronaći rješenje toga pitanja, naš bi se društveno-politički sustav mogao urušiti. Ljudi već predosjećaju nadolazeću kataklizmu. Možda upravo zbog toga građani diljem svijeta gube vjeru u liberalnu priču, dok se ona još do prije samo deset godina činila neodoljivom.“ (Harari, 2018:3:11:40)

Na ovaj rad treba gledati kao na pokušaj akademskog aktualiziranja goruće teme, ali i kao tek mali dio opsežne rasprave o ulozi i značaju privatnosti koji tek treba uslijediti. Unatoč tome što ovaj rad predstavlja doprinos vraćanju privatnosti u svoje zaslužene normativne okvire, s obzirom na rezultate istraživanja, teško je zadržati optimizam.

Literatura

1News. (2017). "Digital strip searches" at NZ airports force hundreds of Kiwis to surrender mobile and laptop passwords each year. *1News*. Preuzeto s https://www.tvnz.co.nz/one-news/new-zealand/digital-strip-searches-nz-airports-force-hundreds-kiwis-surrender-mobile-and-laptop-passwords-each-year

Aamoth, D. (2008, September 23). T-Mobile officially announces the G1 Android phone. *TechCrunch*. Preuzeto s https://techcrunch.com/2008/09/23/t-mobile-officially-announces-the-g1-android-phone/

Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science* (Vol. 4258, pp. 36–58). Berlin, Heidelberg: Springer. https://doi.org/10.1007/11957454_3

Ajzen, I. (1991). The theory of planned behavior. *Orgnizational Behavior and Human Decision Processes*, *50*, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Allen, A. L. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Totowa: Rowman and Littlefield.

Allen, A. L. (2003). *Why Privacy Isn't Everything. Feminist reflections on personal accountability*. Preuzeto s http://papers.ssrn.com/abstract=503263

Allen, A. L. (2004). Privacy in American Law. In B. Rössler (Ed.), *Privacies: Philosophical evaluations* (pp. 19–40). Stanford: Stanford University Press.

Angwin, J., Savage, C., Larson, J., Moltke, H., Poitras, L., & Risen, J. (2015, August 15). AT&T Helped U.S. Spy on Internet on a Vast Scale. *The New York Times*. Preuzeto s https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html

Anić, I.-D., Škare, V., & Kursan Milaković, I. (2016). Determinants and Behavioural Consequences of Online Privacy Concerns Among Young Consumers in Croatia. *Ekonomski Pregled*, *67*(5), 377–398.

Appelbaum, J., Blome, N., Gude, H., Neukirch, R., Pfister, R., Poitras, L., … Stark, H. (2013, October 27). The NSA's Secret Spy Hub in Berlin. *Der Spiegel*. Preuzeto s http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html

Appelbaum, J., Gibson, A., Grothoff, C., Müller-Maguhn, A., Poitras, L., Sontheimer, M., & Stöcker, C. (2014, December 28). Inside the NSA's War on Internet Security. *Der Spiegel*. Preuzeto s http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html

Appelbaum, J., Horchert, J., & Stöcker, C. (2013, December 29). Catalog Advertises NSA Toolbox. *Der Spiegel*. Preuzeto s http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

Appelbaum, J., Poitras, L., Rosenbach, M., Stöcker, C., Schindler, J., & Stark, H. (2013,

December 29). Documents Reveal Top NSA Hacking Unit. *Der Spiegel*. Preuzeto s http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html

Arendt, H. (1958). *The Human Condition.* (2nd ed.). Chicago: The University of Chicago Press.

Aronson, E., Wilson, T. D., & Akert, R. M. (2005). *Socijalna psihologija*. Zagreb: Mate.

Aronson, E., Wilson, T. D., Akert, R. M., & Sommers, S. R. (2016). *Social Psychology* (Ninth Edit). Pearson Education.

Balkin, J. M. (2008). The Constitution in the National Surveillance State. *Minnesota Law Review*, *1*, 1–25.

Ball, J. (2013, October 25). NSA monitored calls of 35 world leaders after US official handed over contacts. *The Guardian*. Preuzeto s https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls

Ball, J., Borger, J., & Greenwald, G. (2013, September 6). Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian*. Preuzeto s https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Ball, J., Schneier, B., & Greenwald, G. (2013, October 4). NSA and GCHQ target Tor network that protects anonymity of web users. *The Guardian*. Preuzeto s https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9), 1–12. Preuzeto s http://journals.uic.edu/ojs/index.php/fm/article/view/1394/1312

BBC. (2017, May 13). Cyber-attack: Europol says it was unprecedented in scale. *BBC*. Preuzeto s http://www.bbc.com/news/world-europe-39907965

Benn, S. I. (1971). Privacy, freedom, and respect for persons. *NOMOS XIII: Privacy*, 1–26.

Bentham, J. (1787). *The Works of Jeremy Bentham*. *The Works of Jeremy Bentham* (Vol. 4). Edinburgh: William Tait. Preuzeto s http://oll.libertyfund.org/titles/1925

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated Preferences vs. Actual Behavior. *Communications of the ACM*, *48*(4), 101–106.

Bernal, P. (2014). *Internet privacy rights: rights to protect autonomy*. New York: Cambridge University Press.

Berridge, K. C., & Kringelbach, M. L. (2015). Pleasure Systems in the Brain. *Neuron*, *86*(3), 646–664. https://doi.org/10.1016/j.neuron.2015.02.018

Berridge, K. C., & Robinson, T. E. (2016). Liking, wanting, and the incentive-sensitization theory of addiction. *American Psychologist*, *71*(8), 670–679. https://doi.org/10.1037/amp0000059

Bharat, K., Lawrence, S., Sahami, M., & Singhal, A. (2003). Serving advertisements using user request information and user information. USA. Preuzeto s https://www.google.de/patents/US20120095837?hl=de&cl=en

Biermann, K., & Musharbash, Y. (2015, August 26). A Dubious Deal with the NSA. *Zeit*. Preuzeto s http://www.zeit.de/digital/datenschutz/2015-08/xkeyscore-nsa-domestic-intelligence-agency

Blake, A. (2017, May 16). Snowden blames NSA for enabling unprecedented cyberattack. *The Washington Times*. Preuzeto s http://www.washingtontimes.com/news/2017/may/16/edward-snowden-blames-nsa-enabling-unprecedented-w/

Bloustein, E. J. (1984). Privacy as an Aspect of Human Dignity. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 156–203). Cambridge University Press.

blue_beetle. (2010). User-driven discontent. Retrieved January 1, 2017, from http://www.metafilter.com/95152/Userdriven-discontent#3256046

Boon, F., Derix, S., & Modderkolk, H. (2013, November 23). NSA infected 50,000 computer networks with malicious software. *NCR*. Preuzeto s https://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software-a1429487

Boyd, D. (2008). Facebook's privacy trainwreck: Exposure, Invasion, and Social Convergence. *Convergence: The International Journal of Research into New Media Technologies*, *14*(1), 13–20. https://doi.org/10.1177/1354856507084416

Bryan Horling, & Kulick, M. (2009). Personalized Search for everyone. Retrieved January 1, 2018, from https://googleblog.blogspot.com.es/2009/12/personalized-search-for-everyone.html

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157–165. https://doi.org/10.1002/asi.20459

Burgoon, J. K. (1982). Privacy and Communication. *Annals of the International Communication Association*, *6*(1), 206–249. https://doi.org/10.1080/23808985.1982.11678499

Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and Restoring Privacy through Communication in different types of Relationships. *Journal of Social and Personal Relationships*, *6*, 131–158.

Burušić, I. (2013). *Statističko izvješće 1468. Popis stanovništva, kućanstava i stanova 2011. Stanovništvo prema spolu i starosti*. Zagreb. Preuzeto s https://www.dzs.hr/Hrv_Eng/publication/2012/SI-1468.pdf

Cadwalladr, C. (2017, May 7). The great British Brexit robbery: how our democracy was hijacked. *The Guardian*. Preuzeto s

https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

Carr, N. (2008). Is Google Making Us Stupid? *The Atlantic*. Preuzeto s https://www.theatlantic.com/magazine/archive/2008/07/is-google-making-us-stupid/306868/

Carroll, R. (2013, October 30). Google's worst-kept secret: floating data centers off US coasts. *The Guardian*. Preuzeto s https://www.theguardian.com/technology/2013/oct/30/google-secret-floating-data-centers-california-maine

Christman, J. (2015). Autonomy in Moral and Political Philosophy. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Spring2015 ed.). Metaphysics Research Lab, Stanford University. Preuzeto s https://plato.stanford.edu/archives/spr2015/entries/autonomy-moral/

Clark, M. S., & Mills, J. (1993). The Difference Between Communal and Ecxange Relationships: What It Is and Is Not. *Personality and Social Psychology*, *19*(6), 684–691.

Cohen, P. (2007, January 9). Macworld Expo Keynote Live Update: Introducing the iPhone. *Macworld*. Preuzeto s http://www.macworld.com/article/1054764/macworld-expo/liveupdate.html

Cole, D. (2014, May 10). 'We Kill People Based on Metadata.' *New York Review of Books*. Preuzeto s http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/

Commission, E. (2011). *SPECIAL EUROBAROMETER 359: Attitudes on Data Protection and Electronic Identity in the European Union*. Preuzeto s http://ec.europa.eu/public_opinion/index_en.htm

Constine, J. (2017, June 27). Facebook now has 2 billion monthly users… and responsibility. *TechCrunch*. Preuzeto s https://techcrunch.com/2017/06/27/facebook-2-billion-users/

Contorno, S. (2014, March 11). James Clapper's testimony one year later. *Politifact*. Preuzeto s http://www.politifact.com/truth-o-meter/article/2014/mar/11/james-clappers-testimony-one-year-later/

Council of Europe. European Convention on Human Rights (1950). Rome: Council of Europe. Preuzeto s https://narodne-novine.nn.hr/clanci/medunarodni/1999_05_6_142.html

Davies, S. G. (1997). Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity. In P. E. Agre & M. Rotenberg (Eds.), *Technology and Privacy: The New Landscape* (pp. 143–167). Cambridge, Massachusetts: MIT Press. https://doi.org/10.1353/tech.2000.0173

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

DeCew, J. (2013). Privacy. In Edward N. Zalta (Ed.), *The Stanford Encyclopedia of*

Philosophy (Spring2015 ed.). Metaphysics Research Lab, Stanford University. Preuzeto s https://plato.stanford.edu/archives/spr2015/entries/privacy/

Denyer, S. (2016, October 22). China wants to give all of its citizens a score – and their rating could affect every area of their lives. *Independent*. Preuzeto s https://www.independent.co.uk/news/world/asia/china-surveillance-big-data-score-censorship-a7375221.html

Dešković, M. (2017, May 13). I Hrvatska na udaru najvećeg hakerskog napada u povijesti: Virus Wannacry zarazio glavni informatički sustav MUP-a. *Jutarnji List*. Preuzeto s http://www.jutarnji.hr/vijesti/hrvatska/jutarnji-ekskluzivno-doznaje-i-hrvatska-na-udaru-najveceg-hakerskog-napada-u-povijesti-virus-wannacry-zarazio-glavni-informaticki-sustav-mup-a/6057999/

Dienlin, T. (2017). *The psychology of privacy: Analyzing processes of media use and interpersonal communication*. University of Hohenheim. Preuzeto s http://opus.uni-hohenheim.de/voll-texte/2017/1315/

Dienlin, T., & Trepte, S. (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. https://doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413–422. https://doi.org/10.1080/01449290410001715723

Duhigg, C. (2012, February 16). How Companies Learn Your Secrets. *The New York Times*. Preuzeto s http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&hp=&pagewanted=all

Efrati, A. (2011, May 18). "Like" Button Follows Web Users. *The Wall Street Journal*. Preuzeto s https://www.wsj.com/articles/SB10001424052748704281504576329441432995616

Elmer, G. (2012). Panopticon - discipline - control. In *Routledge Handbook of Surveillance Studies* (pp. 21–29). New York: Routledge.

Englehardt, S., & Narayanan, A. (2016). Online Tracking. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, (1), 1388–1401. https://doi.org/10.1145/2976749.2978313

Etzioni, A. (2004). *From Empire to Community: A New Approach to International Relations*.

Etzioni, A. (2005). *How Patriotic is the Patriot Act? Freedom versus security in the age of terrorism*.

Etzioni, A. (2007). *Security First: For a Muscular, Moral Foreign Policy*. *Contemporary Sociology: A Journal of Reviews*. New Haven & London: Yale University Press.

Etzioni, A. (2015). *Privacy in a cyber age: policy and practice*. New York: Palgrave Macmillan.

Etzioni, A., & Marsh, J. H. (2003). *Rights vs Public Safety After 9/11*. Oxford: Rowman &

Littlefield Publishers, Inc.

EU. (2012). Charter of Fundamental Rights of the European Union. *Official Journal of the European Union*, 391–407. https://doi.org/10.1108/03090550310770974

European Commission. (2017). *Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service*. Preuzeto s http://europa.eu/rapid/press-release_IP-17-1784_en.htm

European Court of Human Rights. Case of Liberty and others v. The United Kingdom (2008).

Europski parlament i Vijeće Europske unije. (2002). Direktiva o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija. *Službeni List Europske Unije*, *13*(52), 111–121.

Europski parlament i Vijeće Europske unije. (2016a). Direktiva o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka. *Službeni List Europske Unije*, *L*(119), 89–131.

Europski parlament i Vijeće Europske unije. (2016b). Uredba o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ. *Službeni List Europske Unije*, *L*(119), 1–88.

Evershed, N. (2017, July 14). Australia's plan to force tech giants to give up encrypted messages may not add up. *The Guardian*. Preuzeto s https://www.theguardian.com/technology/2017/jul/14/forcing-facebook-google-to-give-police-access-to-encrypted-messages-doesnt-add-up

Falkvinge, R. (2015, October 3). In China, Your Credit Score Is Now Affected By Your Political Opinions – And Your Friends' Political Opinions. *Privacy News Online*. Preuzeto s https://www.privateinternetaccess.com/blog/2015/10/in-china-your-credit-score-is-now-affected-by-your-political-opinions-and-your-friends-political-opinions/

Ferguson, D. (2013, June 8). How supermarkets get your data – and what they do with it. *The Guardian*. Preuzeto s https://www.theguardian.com/money/2013/jun/08/supermarkets-get-your-data

Festinger, L. (1957). *A Theory of Cognitive Dissonance*. California: Stanford University Press.

Festinger, L. (1962). Cognitive Dissonance. *Scientific American*, *207*(4), 93–106. https://doi.org/10.1038/scientificamerican1062-93

Fishbein, M., & Ajzen, I. (2010). *Predicting and Changing Behavior*. New York: Psychology Press.

Fishman, A., & Greenwald, G. (2015, June 22). SPIES HACKED COMPUTERS THANKS TO SWEEPING SECRET WARRANTS, AGGRESSIVELY STRETCHING U.K. LAW. *The Intercept*. Preuzeto s https://theintercept.com/2015/06/22/gchq-reverse-engineering-warrants/

Fishman, A., & Marquis-Boire, M. (2015, June 22). POPULAR SECURITY SOFTWARE

CAME UNDER RELENTLESS NSA AND GCHQ ATTACKS. *The Intercept*. Preuzeto s https://theintercept.com/2015/06/22/nsa-gchq-targeted-kaspersky/

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. https://doi.org/10.1016/j.chb.2008.08.006

Foucault, M. (1995). *Discipline and Punish: The Birth of the Prison* (Second Cin). New York: Vintage Books.

Francis, L. P., & Francis, J. G. (2017). *Privacy: What Everyone Needs to Know*. New York: Oxford University Press.

Fried, C. (1968). Privacy [A moral analysis]. *Yale Law Journal*, *77*, 475–493.

Fuchs, C. (2011). Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society*, *9*(4), 220–237.

Gajda, A. (2007). What if Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage that Led to The Right to Privacy. *Illinois Public Law and Legal Theory Research Paper Series*, *07*(06).

Gallagher, R., & Greenwald, G. (2014, March 12). How NSA plans to infect "milions" of computers with malware. *The Intercept*. Preuzeto s https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

Gallagher, R., & Greenwald, G. (2015, December 23). NSA helped British spies find security holes in Juniper firewalls. *The Intercept*. Preuzeto s https://theintercept.com/2015/12/23/juniper-firewalls-successfully-targeted-by-nsa-and-gchq/

Gavison, R. (1980). Privacy and the limits of law. *Yale Law Journal*, *89*, 421–471.

Geist, A., Gjerding, S., Moltke, H., & Poitras, L. (2014, November 1). Snowden documents reveal British climate espionage – Copenhagen climate summit targeted. *Information*. Preuzeto s https://www.information.dk/udland/2014/11/snowden-documents-reveal-british-climate-espionage-copenhagen-climate-summit-targeted

Gellman, B., & DeLong, M. (2013a, October 30). How the NSA's MUSCULAR program collects too much data from Yahoo and Google. *The Washington Post*. Preuzeto s https://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/#document/p3/a129339

Gellman, B., & DeLong, M. (2013b, October 30). One month, hundreds of millions of records collected. *The Washington Post*. Preuzeto s https://apps.washingtonpost.com/g/page/world/one-month-hundreds-of-millions-of-records-collected/554/

Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. Preuzeto s https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Gellman, B., Timberg, C., & Rich, S. (2013, October 4). Secret NSA documents show campaign against Tor encrypted network. *The Washington Post*. Preuzeto s https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html

Gerhard Schmid. (2001). *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*. Temporary Committee on the ECHELON Interception System. Preuzeto s http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&format=XML&language=EN

Gerstein, R. S. (1970). Privacy and self-incrimination. *Ethics*, *80*, 87–101.

Gerstein, R. S. (1978). Intimacy and privacy. *Ethics*, *89*, 79–81.

Gibbs, S. (2014, April 15). Gmail does scan all emails, new Google terms clarify. *The Guardian*. Preuzeto s https://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify

Gjerding, S., Moltke, H., Geist, A., & Poitras, L. (2014, January 30). NSA spied against UN climate negotiations. *Information*. Preuzeto s https://www.information.dk/udland/2014/01/nsa-spied-against-un-climate-negotiations

Glüsing, J., Poitras, L., Rosenbach, M., & Stark, H. (2013, October 20). NSA Accessed Mexican President's Email. *Spiegel*. Preuzeto s http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html

Goel, V. (2014, September 28). With New Ad Platform, Facebook Opens Gates to Its Vault of User Data. *The New York Times*. Preuzeto s https://www.nytimes.com/2014/09/29/business/with-new-ad-platform-facebook-opens-the-gates-to-its-vault-of-consumer-data.html

Google. (n.d.). Google Code of Conduct. Retrieved January 1, 2017, from https://abc.xyz/investor/other/google-code-of-conduct.html

Google CEO On Privacy (VIDEO): 'If You Have Something You Don't Want Anyone To Know, Maybe You Shouldn't Be Doing It'. (2010, March 18). *Huffington Post*. Preuzeto s http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html

Gorman, S., & Valentino-DeVries, J. (2013, August 20). New Details Show Broader NSA Surveillance Reach. *The Wall Street Journal*. Preuzeto s https://www.wsj.com/articles/new-details-show-broader-nsa-surveillance-reach-1377044261?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424127887324108204579022874091732470.html&tesla=y#

Grassegger, H., Krogerus, M., & Dehaye, P.-O. (2017, January 28). The Data That Turned the World Upside Down. *Das Magazin & Motherboard Vice*. Preuzeto s https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

Greene, D. (2017, June 23). As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align. *The Keyword*. Preuzeto s https://www.blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/

Greenwald, G. (2013a, July 15). The crux of the NSA story in one phrase: "collect it all." *The Guardian*. Preuzeto s https://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all

Greenwald, G. (2013b, July 31). XKeyscore: NSA tool collects "nearly everything a user does on the internet." *The Guardian*. Preuzeto s https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Greenwald, G. (2014). *No Place to Hide*. London: Penguin Books.

Greenwald, G., & MacAskill, E. (2013a, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Preuzeto s https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, G., & MacAskill, E. (2013b, June 11). Boundless Informant: the NSA's secret tool to track global surveillance data. *The Guardian*. Preuzeto s https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 11). Edward Snowden: the whistleblower behind the NSA surveillance revelations. Hong Kong. Preuzeto s https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rushe, D. (2013). Microsoft handed the NSA access to encrypted messages. *The Guardian*. Preuzeto s https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Greenwald, G., & Maurizi, S. (2013, December 5). Revealed: How the Nsa Targets Italy. *L'Espresso*. Preuzeto s http://espresso.repubblica.it/inchieste/2013/12/05/news/revealed-how-the-nsa-targets-italy-1.144428

Grey, C. (2016). Footnote *: I, Phone. Preuzeto s https://www.youtube.com/watch?v=e-ZpsxnmmbE

Grizelj, M. (2016). *Statističko izvješće 1582. Popis stanovništva, kućanstava i stanova 2011. Stanovništvo prema obrazovnim obilježjima*. Zagreb. Preuzeto s https://www.dzs.hr/Hrv_Eng/publication/2016/SI-1582.pdf

Gunnar Rensfeldt. (2013, December 11). FRA has access to controversial surveillance system. *SVT*. Preuzeto s https://www.svt.se/nyheter/granskning/ug/fra-has-access-to-controversial-surveillance-system

Ha, A. (2017, March 7). Facebook is making its cross-device Atlas data available to more advertisers. *TechCrunch*. Preuzeto s https://techcrunch.com/2017/03/07/facebook-advanced-measurement/

Haggerty, K. D. (2006). Tear down the walls: on demolishing the panopticon. In *Theorizing*

Surveillance The panopticon and beyond (pp. 23–45). Devon: Willan Publishing.

Harari, Y. N. (2014). *Sapiens: a brief history of humankind*. Harper.

Harari, Y. N. (2018). *21 Lessons for the 21st Century* (Audioknjig). Audible.

Harcourt, B. E. (2015). *Exposed: desire and disobediance in the digital age*. Cambridge, Massachusetts: Harvard University Press.

Her Majesty's Government. Investigatory Powers Act 2016 (2016). Parliament of the United Kingdom. https://doi.org/http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf

Hern, A. (2017, March 8). "Am I at risk of being hacked?" What you need to know about the "Vault 7" documents. *The Guardian*. Preuzeto s https://www.theguardian.com/technology/2017/mar/08/wikileaks-vault-7-cia-documents-hacked-what-you-need-to-know

Hoyt, J. K. (1896). *The Cyclopedia of Practical Quotations*.

Huang, Z. (2015, October 9). All Chinese citizens now have a score based on how well we live, and mine sucks. *Quartz*. Preuzeto s https://qz.com/519737/all-chinese-citizens-now-have-a-score-based-on-how-well-we-live-and-mine-sucks/

Hughes, K. (2015). The social value of privacy, the value of privacy to society and human rights discourse. In B. Rössler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (pp. 225–244). Cambridge: Cambridge University Press.

Huxley, A. (2000). *Brave New World*. New York: Rosetta Books.

Ignatius, D. (2014, June 5). David Ignatius: Edward Snowden took less than previously thought, says James Clapper. *The Washington Post*. Preuzeto s https://www.washingtonpost.com/opinions/edward-snowden-took-less-than-previously-thought-says-james-clapper/2014/06/05/054cb9f2-ecee-11e3-93d2-edd4be1f5d9e_story.html

Iness, J. C. (1992). *Privacy, Intimacy and Isolation*. New York: Oxford University Press.

Johnson, D. G. (2000). *Computer Ethics* (3rd Editio). Upper Saddle River: Prentice Hall.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Paine Schofield, C. B. (2010). Privacy, Trust, and Self-Disclosure Oonline. *Human-Computer Interaction*, *25*(1), 1–24. https://doi.org/10.1080/07370020903586662

Jones, R. (2017, July 24). Sweden Leaks the Personal Information of Millions of Its Own Citizens. *Gizmodo*. Preuzeto s https://gizmodo.com/sweden-leaks-the-personal-information-of-millions-of-it-1797208092

Juvenal. (n.d.). *Satire VI*. Preuzeto s http://www.thelatinlibrary.com/juvenal/6.shtml

Kalven, H. J. (1966). Privacy in Tort Law: Were Warren and Brandeis Wrong? *Law and Contemporary Problems*, *31*(2), 326–341. https://doi.org/10.1525/sp.2007.54.1.23.

Kaštelan, J., & Duda, B. (Eds.). (1983). *Biblija*. Zagreb: Kršćanska sadašnjost.

Katner, J. (2018, May 20). The backlash that never happened: New data shows people actually increased their Facebook usage after the Cambridge Analytica scandal. *Business Insider*. Preuzeto s http://uk.businessinsider.com/people-increased-facebook-usage-after-cambridge-analytica-scandal-2018-5?r=US&IR=T

Kazneni zakon (2011). Hrvatski Sabor.

Kelly, H. (2013, July 5). Protests against the NSA spring up across U.S. *CNN*. Preuzeto s https://edition.cnn.com/2013/07/04/tech/web/restore-nsa-protests

Kirk, M. (2014). *United States of Secrets*. SAD: PBS Frontline.

Kiss, J. (2010, May 15). Google admits collecting Wi-Fi data through Street View cars. *The Guardian*. Preuzeto s https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data

Klarić, M. (2016). Zaštita osobnih podataka i Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda. *Zbornik Radova Pravnog Fakulteta u Splitu*, *53*(4), 973–990.

Korzaan, M. L., & Boswell, K. T. (2008). The Influence of Personality Traits and Information Privacy Concerns on Behavioral Intentions. *Journal of Computer Information Systems*, *48*(4), 15–24. https://doi.org/10.1080/08874417.2008.11646031

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences of the United States of America*, *111*(24), 8788–90. https://doi.org/10.1073/pnas.1320040111

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Kumaraguru, P., & Cranor, L. F. (2005). *Privacy Indexes: A Survey of Westin's Studies*. *Technical Report*.

Kundera, M. (1987). *The Unbereable Lightness of Being*. New York: Harper & Row.

Kundera, M. (1996). *Testaments Betryed: An Esay in Nine Parts*. New York: Harper Perennial.

Lane, F. S. (2009). *American Privacy: The 400-year History of Our Most Contested Right*. Boston: Beacon Press.

Larson, J., Glanz, J., & Lehren, A. W. (2014, January 27). Spy Agencies Probe Angry Birds and Other Apps for Personal Data. *Pro Publica*. Preuzeto s https://www.propublica.org/article/spy-agencies-probe-angry-birds-and-other-apps-for-personal-data

Lerner, M. J. (1980). *The Belief in a Just World: A Fundamental Delusion*. *Contemporary Sociology* (Vol. 11). New York: Springer.

Lever, A. (2006). Privacy Rights and Democracy: A Contradiction in Terms? *Contemporary Political Theory*, *5*(2), 142–162. https://doi.org/10.1057/palgrave.cpt.9300187

Lever, A. (2015). Privacy and Democracy: What the Secret Ballot Reveals. *Law, Culture and the Humanities*, *11*(2), 164–183. https://doi.org/10.1177/1743872112458745

Levine, Y. (2013a, December 16). Google's for-profit surveillance problem. *Pando*. Preuzeto s https://pando.com/2013/12/16/googles-for-profit-surveillance-problem/

Levine, Y. (2013b, December 22). What Surveillance Valley knows about you. *Pando*. Preuzeto s https://pando.com/2013/12/22/a-peek-into-surveillance-valley/

Levine, Y. (2014, January 8). Surveillance Valley scammers! Why hack our data when you can just buy it? *Pando*. Preuzeto s https://pando.com/2014/01/08/surveillance-valley-scammers-why-hack-our-data-when-you-can-just-buy-it/

Locke, J. (2015). *Pismo o toleranciji*. Zagreb: Srpsko narodno vijeće.

Luca, M., Wu, T., Couvidat, S., Frank, D., & Seltzer, W. (2015). *Does Google Content Degrade Google Search? Experimental Evidence* (No. 16-035). Preuzeto s http://www.slideshare.net/lutherlowe/wu-l

Lyon, D. (1993). An electronic panopticon? A sociological critique of surveillance theory. *The Sociological Review*, *41*, 653–678. https://doi.org/10.1111/j.1467-954X.1993.tb00896.x

MacAskill, E. (2016, November 19). "Extreme surveillance" becomes UK law with barely a whimper. *The Guardian*. Preuzeto s https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper

MacAskill, E., & Borger, J. (2013, June 30). New NSA leaks show how US is bugging its European allies. *The Guardian*. Preuzeto s https://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013, June 21). GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*. Preuzeto s https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

MacAskill, E., Thielman, S., & Oltermann, P. (2017, March 7). WikiLeaks publishes "biggest ever leak of secret CIA documents." *The Guardian*. Preuzeto s https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance

MacKinnon, C. A. (1989). *Toward a Feminist Theory of the State*. Cambridge: Harvard University Press. https://doi.org/10.2307/1963549

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. Preuzeto s http://www.jstor.org/stable/23015787

Marochini, M. (2014). The interpretation of the European Convention on Human Rights.

Zbornik Radova Pravnog Fakulteta u Splitu, *51*(1), 63–84.

Marquis-Boire, M., Greenwald, G., & Lee, M. (2015, July 1). XKEYSCORE: NSA's Google for the World's Private Communications. *The Intercept*. Preuzeto s https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/

Marshall, J. (2014, September 22). Facebook Extends Reach With New Advertising Platform. *The Wall Street Journal*. Preuzeto s https://www.wsj.com/articles/facebook-extends-reach-withad-platform-1411428726

Marx, G. T. (2003). A tack in the shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues*, *59*(2), 369–390. https://doi.org/10.1111/1540-4560.00069

Marx, K. (1976). *Capital* (Vol. 1). London: Penguin Books.

Maslow, A. (1943). A Theory of human Motivation. *Psychological Review*, 370–396.

Mathiesen, T. (1997). The Viewer Society: Michel Foucault's "Panopticon" Revisited. *Theoretical Criminology*, *1*(2), 215–234. https://doi.org/0803973233

McCracken, H. (2014, April 1). How Gmail Happened: The Inside Story of Its Launch 10 Years Ago. *Time*. Preuzeto s http://time.com/43263/gmail-10th-anniversary/

Medine, D., Brand, R., Cook, E. C., Dempsey, J., & Wald, P. (2014). *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. Preuzeto s http://www.pclob.gov/library/702-Report.pdf

Meredith, C. (2013). Big Brother is watching: Sales of George Orwell's "1984" up 337% after NSA spying scandal. Retrieved January 1, 2018, from https://www.express.co.uk/news/world/406709/Big-Brother-is-watching-Sales-of-George-Orwell-s-1984-up-337-after-NSA-spying-scandal

Michael, J. (1994). *Privacy and human rights*. Paris: United Nations and Dartmouth Publishing Company Limited.

Mill, J. S. (2009). *On Liberty*. The Floating Press.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008

Moore, A. D. (2003). Privacy : Its Meaning and Value. *American Philosophical Quarterly*, *40*(3), 215–227.

Moraes, C. (2014). *Izvješće o programu nadzora Agencije za nacionalnu sigurnost SAD-a (NSA), nadzornim tijelima u različitim državama članicama i njihovu utjecaju na temeljna prava građana EU-a te o transatlantskoj suradnji u pravosuđu i unutarnjim poslovima*. Preuzeto s http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//HR

Mowshowitz, A. (1997). Beyond calculation : the next fifty years of computing. In P. J. Denning & R. M. Metcalfe (Eds.), *Beyond calculation: the next fiffty years of computing* (pp. 213–233). New York: Springer. https://doi.org/10.1108/itp.1998.11.2.152.1

Mozur, P. (2018). Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras. *The New York Times*. Preuzeto s https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

Murakami Wood, D. (2007). Beyond the Panopticon? Foucault and Surveillance Studies. In *Space, Knowledge and Power: Foucault and Geography* (pp. 245–264). Hampshire: Ashgate.

Murphy, R. F. (1964). Social distance and the veil. *American Anthropologist*, *66*(6), 1257–1274.

Myers, D. (2005). *Social Psychology* (8th ed.). New York: McGraw-Hill.

Nagel, T. (2002). *Concealment and Exposure And Other Essays*. New York: Oxford University Press.

Nakashima, E., & Warrick, J. (2012, June 2). Stuxnet was work of U.S. and Israeli experts, officials say. *The Washington Post*. Preuzeto s https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

New law would force Facebook and Google to give police access to encrypted messages. (2017, July 14). *The Guardian*. Preuzeto s https://www.theguardian.com/technology/2017/jul/14/new-law-would-force-facebook-and-google-to-give-police-access-to-encrypted-messages

Newell, J. (2013, October 26). Thousands gather in Washington for anti-NSA "Stop Watching Us" rally. *The Guardian*.

Newton, C. (2017a). America doesn't trust Facebook. Retrieved January 1, 2017, from https://www.theverge.com/2017/10/27/16552620/facebook-trust-survey-usage-popularity-fake-news

Newton, C. (2017b). How Facebook rewards polarizing political ads. Retrieved January 1, 2017, from https://www.theverge.com/2017/10/11/16449976/facebook-political-ads-trump-russia-election-news-feed

Nissenbaum, H. F. (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford: Stanford University Press.

Nix, A. (2016). *The Power of Big Data and Psychographics*. Preuzeto s https://www.youtube.com/watch?v=n8Dd5aVXLCc

NN. Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske (2006). Preuzeto s http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors, *41*(1), 100–126.

NSA's global interception network. (2013). Retrieved January 1, 2017, from https://electrospaces.blogspot.com.es/2013/12/nsas-global-interception-network.html#largecable

Nyst, C., & Falchetta, T. (2017). The Right to Privacy in the Digital Age. *Journal of Human Rights Practice*, *9*(1), 104–118. https://doi.org/10.1093/jhuman/huw026

O'Brien, D. (2017, October 30). Who Speaks for The Billions of Victims of Mass Surveillance? Tech Companies Could. *Electronic Frontier Foundation*. Preuzeto s https://www.eff.org/deeplinks/2017/10/tech-companies-could-fight-non-us-surveillance

O'Neill, M., & Andersen, B. (2015, October 15). Australia accessed NSA spy data more than UK over 12 months: Edward Snowden document. *ABC*. Preuzeto s http://www.abc.net.au/news/2015-10-15/edward-snowden-docs-show-australia-accessed-nsa-spy-data/6856994

Opća skupština Ujedinjenih naroda. Međunarodni pakt o građanskim i političkim pravima (1966). Opća skupština UN-a. Preuzeto s https://pravosudje.gov.hr/UserDocsImages/dokumenti/Pravo na pristup informacijama/Zakoni i ostali propisi/UN konvencije/Medjunarodni_pakt_o_gradjanskim_i_politickim_pravima_HR.pdf

Orwell, G. (2016). *1984*. Meloburne: The Text Publishing Company.

Paine, C., Reips, U. D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of "privacy concerns" and "privacy actions." *International Journal of Human Computer Studies*, *65*(6), 526–536. https://doi.org/10.1016/j.ijhcs.2006.12.001

Panksepp, J. (1998). *Affective neuroscience: the foundations of human and animal*. New York: Oxford University Press.

Parent, W. A. (1983). Privacy, Morality, and the Law. *Philosophy & Public Affairs*, *12*(4), 269–288.

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Pedlow, G. W., & Welzenbach, D. E. (1998). The CIA and the U-2 Program, 1954-1974. *Central Intelligence Agency*. Preuzeto s https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/the-cia-and-the-u-2-program-1954-1974/u2.pdf

Perlroth, N., Larson, J., & Shane, S. (2013, September 5). N.S.A. Able to Foil Basic Safeguards of Privacy on Web. *The New York Times*.

Phillips, S. (2007, July 25). A brief history of Facebook. *The Guardian*. Preuzeto s https://www.theguardian.com/technology/2007/jul/25/media.newmedia

Platon. (2009). *Država* (Filozofska). Zagreb: Naklada Jurčić.

Pohlman, H. L. (1993). *Political Thought and the American Judiciary*. Amherst: University of Massachusetts Press.

Poitras, L., Rosenbach, M., Schmid, F., & Stark, H. (2013, June 29). NSA Spied on European Union Offices. *Der Spiegel*. Preuzeto s http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html

Poitras, L., Rosenbach, M., & Stark, H. (2013, August 26). How America Spies on Europe and the UN. *Der Spiegel*. Preuzeto s http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

Posner, R. A. (1978). An economic theory of privacy. *AEA Papers and Proceedings*, *71*(May/June), 19–26.

Postman, N. (2005). *Amusing Ourselves to Death* (20th Anniv). London: Penguin Books.

Prosser, W. L. (1960). Privacy. *California Law Review*, *48*, 338–423.

Rachels, J. (1975). Why privacy is important. *Philosophy and Public Affairs*, *4*(4), 323–333.

Raz, J. (1986). *The Morality of Freedom*. New York: Oxford University Press. https://doi.org/10.1093/0198248075.001.0001

Reiman, J. H. (1976). Privacy, intimacy, and personhood. *Philosophy & Public Affairs*, *6*(1), 26–44.

Reiman, J. H. (1995). Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. *Computer & High Technology Law Journal*, *11*(1), 27–44.

Richards, N. M. (2015). *Intellectual privacy : rethinking civil liberties in the digital age*. New York: Oxford University Press.

Richards, N. M., & Solove, D. J. (2010). Prosser‘s Privacy Law: A Mixed Legacy. *California Law Review*, *98*(6), 1887. https://doi.org/10.15779/Z38541P

Robertson, A. (2015, July 16). “Angry Birds 2” Arrives 6 Years And 3 Billion Downloads After First Game. *Forbes*. Preuzeto s https://www.forbes.com/sites/andyrobertson/2015/07/16/angry-birds-2/#503b0394702d

Romero, S., & Archibold, R. C. (2013, September 2). Brazil Angered Over Report N.S.A. Spied on President. *The New York Times*. Preuzeto s http://www.nytimes.com/2013/09/03/world/americas/brazil-angered-over-report-nsa-spied-on-president.html?_r=0

Rössler, B. (2004a). Gender and Privacy: A Critique of the Liberal Tradition. In B. Rössler (Ed.), *Privacies: Philosophical evaluations* (pp. 52–72). Stanford: Stanford University Press.

Rössler, B. (2004b). Privacies. In B. Rössler (Ed.), *Privacies: Philosophical Evaluations* (pp. 1–19). Stanford: Stanford University Press.

Rössler, B. (2005). *The Value of Privacy*. Cambridge: Polity.

Rössler, B. (2006). New Ways of Thinking about Privacy. In J. S. Dryzek, B. Honig, & A. Phillips (Eds.), *The Oxford Handbook of Political Theory* (pp. 694–713). New York: Oxford University Press.

RT. (2013, July 27). Thousands fill German streets to protest Berlin’s NSA spying involvement. *Russia Today*. Preuzeto s https://www.rt.com/news/germany-nsa-merkel-

writers-669/

Rushe, D. (2013, June 8). Facebook and Google insist they did not know of Prism surveillance program. *The Guardian*. Preuzeto s https://www.theguardian.com/world/2013/jun/07/google-facebook-prism-surveillance-program

Salm, L. (2017). 70% of employers are snooping candidates' social media profiles. Retrieved January 1, 2017, from https://www.careerbuilder.com/advice/social-media-survey-2017

Scahill, J., & Begley, J. (2015a, February 19). The great SIM heist. *The Intercept*. Preuzeto s https://theintercept.com/2015/02/19/great-sim-heist/

Scahill, J., & Begley, J. (2015b, March 10). THE CIA CAMPAIGN TO STEAL APPLE'S SECRETS. *The Intercept*. Preuzeto s https://theintercept.com/2015/03/10/ispy-cia-campaign-steal-apples-secrets/

Scanlon, T. (1975). Thomson on Privacy. *Philosophy & Public Affairs*, *4*(4), 315–322.

Schoeman, F. D. (1984). *Philosophical Dimensions of Privacy: An Anthology*. (F. D. Schoeman, Ed.), *Philosophical Dimensions of Privacy* (Digitally). Cambridge: Cambridge University Press.

Schofield, P. (2009). *Bentham: A Guide for the Perplexed*. London: Continuum.

Schwartz, B. (1968). The Social Psychology of Privacy. *American Journal of Sociology*, *73*(6), 741–752.

Seligman, M. E. P. (1972). Learned helplessness. *Annual Review of Medicine*, *23*(1), 407–412. Preuzeto s http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=4566487

Simmel, G. (1908). *Soziologie. Untersuchungen über die formen der vergesellschaftung*. Leipzig: Duncker & Humbolt.

Singleton, S. M., & Harper, J. (2002). With A Grain of Salt: What Consumer Privacy Surveys Don't Tell Us. *SSRN Electronic Journal*, (June). https://doi.org/10.2139/ssrn.299930

Slides about NSA's Upstream collection. (2014). Retrieved January 1, 2017, from https://electrospaces.blogspot.com.es/2014/01/slides-about-nsas-upstream-collection.html

Smith, J. H., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, *20*(2), 167–196.

Solomon, D. (2003). *Data Privacy and Security*. New York: Springer-Verlag.

Solon, O. (2017, March 31). US border agents are doing "digital strip searches". Here's how to protect yourself. *The Guardian*. Preuzeto s https://www.theguardian.com/us-news/2017/mar/31/us-border-phone-computer-searches-how-to-protect

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087–1155.

https://doi.org/10.1145/1929609.1929610

Solove, D. J. (2004). *The digital person: technology and privacy in the information age*. New York and London: New York University Press.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477. https://doi.org/10.2307/40041279

Solove, D. J. (2007). "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review*, *44*(May), 1–23. https://doi.org/10.2139/ssrn.998565

Solove, D. J. (2008). *Understanding Privacy*. Cambridge: Harvard University Press.

Solove, D. J. (2011). *Nothing to hide : the false tradeoff between privacy and security*. New Haven & London: Yale University Press.

Solove, D. J., & Richards, N. M. (2007). Privacy's Other Path. *George Washington Law Journal*, *96*(123), 123–182.

Soltani, A., Peterson, A., & Gellman, B. (2013, December 10). NSA uses Google cookies to pinpoint targets for hacking. *The Washington Post*. Preuzeto s https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/

Son, J.-Y., & Kim, S. S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly*, *32*(3), 503–529. https://doi.org/Article

Sonenshine, J. (2018, May 10). Facebook wipes out all of its losses following the Cambridge Analytica data scandal. *Business Insider*. Preuzeto s http://uk.businessinsider.com/facebook-stock-price-wipes-out-cambridge-analytica-data-scandal-losses-2018-5?r=UK&IR=T

Spiegel. (2013, July 22). Secret Links Between Germany and the NSA. *Spiegel*. Preuzeto s http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html

Stephens-Davidowitz, S. (2017). *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are*. New York: Dey Street Books.

Stewart, K. A., & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy InstrumentInstrument. *Information Systems Research*, *13*(1), 36–49. https://doi.org/DOI 10.1287/isre.13.1.36.97

Streitfeld, D. (2013, March 12). Google Concedes That Drive-By Prying Violated Privacy. *The New York Times*. Preuzeto s http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html

Strohm, C., & Wilber, D. Q. (2014, January 10). Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers. *Bloomberg News*. Preuzeto s http://www.bloomberg.com/news/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.html

Stutzman, F., Vitak, J., Ellison, N. B., Gray, R., & Lampe, C. (2012). Privacy in Interaction: Exploring Disclosure and Social Capital in Facebook. In J. Breslin (Ed.), *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media* (pp. 330–337). Palo Alto: AAAI Press. Preuzeto s http://www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/view/4666

Sud Europske unije. Maximillian Schrems protiv Data Protection Commissioner (2015). Preuzeto s http://curia.europa.eu/juris/documents.jsf?num=C-362/14

Sumner, S. (2015). *You: For Sale: Protecting Your Personal Data and Privacy Online*. Syngress.

Sundar, S. S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013). Unlocking the Privacy Paradox: Do Cognitive Heuristics Hold the Key? In *CHI 2013: Changing Perpectives* (pp. 811–816).

Sunstein, C. R. (2007). *Republic.com 2.0*. *Republic.com 2.0*. Woodstock: Princeton University Press. https://doi.org/papers3://publication/uuid/2D5DD160-94D4-47E3-BAA9-6ABC6A8B7BB6

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. https://doi.org/10.1016/j.chb.2012.11.022

Takashi, D. (2010, October 17). WSJ reports Facebook apps — including banned LOLapps games — transmitted private user data. *Venture Beat*. Preuzeto s https://venturebeat.com/2010/10/17/wsj-reports-facebook-apps-including-banned-lolapps-games-transmitted-private-user-data/

TED. (2014). How we take back the internet | Edward Snowden. Preuzeto s https://www.youtube.com/watch?v=yVwAodrjZMY

The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights. (1985). *Human Rights Quarterly*, *7*(1), 3. https://doi.org/10.2307/762035

theguardian.com. (2013). XKeyscore presentation from 2008 – read in full. Retrieved January 1, 2018, from https://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

Thompson, R. (2017, July 13). 22,000 people accidentally signed up to clean toilets because people don't read Wi-Fi terms. *Mashable*. Preuzeto s http://mashable.com/2017/07/13/wifi-terms-conditions-toilets/#E4vK5DzRiiq8

Thomson, J. J. (1975). The Right to Privacy. *Philosophy and Public Affairs*, *4*(4), 295–314.

Titcomb, J. (2017, May 15). Microsoft slams US government over global cyber attack. *The Telegraph*. Preuzeto s http://www.telegraph.co.uk/technology/2017/05/15/microsoft-slams-us-government-global-cyber-attack/

Trepte, S., Dienlin, T., & Reinecke, L. (2014). Risky behaviors: How online experiences influence privacy behaviors. In N. Jackob, O. Quiring, & B. Stark (Eds.), *Von der Gutenberg-Galaxis zur Google-Galaxis [From the Gutenberg Galaxy to the Google*

Galaxy] (English un, pp. 225–244). Wiesbaden: UVK.

Trepte, S., & Reinecke, L. (2011). The Social Web as a Shelter for Privacy and Authentic Living. In S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. Berlin, Heidelberg: Springer-Verlag.

Tucker, R. C. (1978). *The Marx-Engels Reader*. (R. C. Tucker, Ed.) (Second edi). New York: W. W. Norton & Company.

Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, *28*(1), 20–36. https://doi.org/10.1177/0270467607311484

United Nations. Opća deklaracija o pravima čovjeka (1948). Paris: Opća skupština UN-a. Preuzeto s http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=src2

United Nations. (2013a). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinio and Expression, Frank La Rue. *Human Rights Council Report*, (A/HRC/23/40), 22. https://doi.org/A/HRC/23/40

United Nations. The right to privacy in the digital age (2013). United Nations General Assembly. Preuzeto s http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

United Nations. (2014a). *Concluding observations on the fourth periodic report of the United States of America*.

United Nations. (2014b). Promotion and protection of human rights and fundamental freedoms while countering terrorism. *United Nations General Assembly*, *A/69/397*.

United Nations. The right to privacy in the digital age (2014). United Nations General Assembly. Preuzeto s http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166

United Nations. (2014d). The right to privacy in the digital age. *United Nations General Assembly*, (A/HRC/27/37).

United Nations. (2016). Right to Privacy. *United Nations General Assembly*, (A/71/368). Preuzeto s http://ap.ohchr.org/documents/dpage_e.aspx?si=A/71/368

United Nations. (2017). Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. *Human Rights Council Report*, (A/HRC/34/6). Preuzeto s http://www.ohchr.org/Documents/Issues/Privacy/A_HRC_34_60_EN.docx

Ustav Republike Hrvatske (1990). Hrvatski Sabor. Preuzeto s https://narodne-novine.nn.hr/clanci/sluzbeni/2001_05_41_705.html

Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*(2).

Vaidhyanathan, S. (2011). *The Googlization of Everything: And Why We Should Worry*. Berkley and Los Angeles: University of California press. https://doi.org/10.1111/1540-

4560.00071

Vlašić, T. (2017). Policija je prijetnje na fejsu, čini se, počela shvaćati prilično ozbiljno, izvukli smo nedavne slučajeve uhićenja. Retrieved January 1, 2017, from http://www.telegram.hr/politika-kriminal/policija-je-prijetnje-na-fejsu-cini-se-pocela-shvacati-prilicno-ozbiljno-izvukli-smo-nedavne-slucajeve-uhicenja/

Waddell, K. (2017, April 12). The Steady Rise of Digital Border Searches. *The Atlantic*. Preuzeto s https://www.theatlantic.com/technology/archive/2017/04/the-steady-rise-of-digital-border-searches/522723/

Waldron, J. (2003a). Security and liberty: The image of balance. *Journal of Political Philosophy*, *11*(2), 191–210. https://doi.org/10.1111/1467-9760.00174

Waldron, J. (2003b). Security and liberty: The image of balance. *Journal of Political Philosophy*, *11*(2), 191–210.

Wall, S. (2012). Perfectionism in Moral and Political Philosophy. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Winter 201). Metaphysics Research Lab, Stanford University.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5).

Wasserstrom, R. (1984). Privacy: Some arguments and assumptions. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 317–333). Cambridge University Press.

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

Whitaker, R. (1999). *The end of privacy: how total surveilance is becoming reality*. New York: The New Press.

Wikileaks. (2017). Retrieved January 1, 2017, from https://www.wikileaks.org/

Wilson, T. D., & Brekke, N. (1994). Mental Contamination and Mental Correction: Unwanted Influences on Judgements and Evaluations. *Psycological Bulletin*, *116*(1), 117–142.

Winter, B. (2013, September 4). Exclusive: Brazil's Rousseff wants U.S. apology for NSA spying. *Reuters*. Preuzeto s https://www.reuters.com/article/us-usa-security-snowden-brazil/exclusive-brazils-rousseff-wants-u-s-apology-for-nsa-spying-idUSBRE98314N20130904

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824.

Yardi, S., & Boyd, D. (2010). Dynamic Debates: An Analysis of Group Polarization Over Time on Twitter. *Bulletin of Science, Technology & Society*, *30*(5), 316–327. https://doi.org/10.1177/0270467610380011

Young, I. M. (2005). A Room of One's Own: Old Age, Extended Care, and Privacy. In *On female body experience : "Throwing like a girl" and other essays* (pp. 155–171). New York: Oxford University Press.

Zamyatin, Y. (1972). *We*. New York: Viking Press.

Zetter, K. (2015, December 22). RESEARCHERS SOLVE JUNIPER BACKDOOR MYSTERY; SIGNS POINT TO NSA. *Wired*. Preuzeto s https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/

Prilozi

Prilog 1 – Sadržaj ankete korištene u empirijskom istraživanju

Istraživanje o privatnosti

Poštovani, pred Vama se nalazi kratki upitnik o mišljenju i ponašanju vezanome uz privatnost. Istraživanje je anonimno i podaci će biti analizirani isključivo na razini grupe. Od ispunjavanja upitnika možete odustati u bilo kojem trenutku. Molim Vas da odgovorite na sva pitanja te da na pitanja odgovarate iskreno. Hvala

1. Koliko Vam je važna Vaša privatnost?

1	2	3	4	5
Nimalo mi nije važna				Izrazito mi je važna

2. Koliko ste zadovoljni razinom privatnosti koju uživate?

1	2	3	4	5
Izrazito nezadovoljan/a				Izrazito zadovoljan/a

Općenito o privatnosti

U nastavku se nalazi niz tvrdnji za koje Vas molim da odredite u kojoj se mjeri slažete s pojedinom tvrdnjom.

3. Općenito, zabrinut/a sam za svoju privatnost.

1	2	3	4	5
Uopće se ne slažem				U potpunosti se slažem

4. Do mojih osobnih podataka lako je doći.

1	2	3	4	5
Uopće se ne slažem				U potpunosti se slažem

5. Nemam ništa za sakriti.

1	2	3	4	5
Uopće se ne slažem				U potpunosti se slažem

6. Svatko bi trebao imati mogućnost u javnosti prikriti svoje mane i prikazati se u boljem svjetlu.

1	2	3	4	5

Uopće se ne slažem U potpunosti se slažem

7. Obično me smeta kada me se traži moje osobne podatke.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

8. Smatram kako davanje osobnih podataka drugima nosi sa sobom određene rizike.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

9. Svi moji razgovori s drugima mogli bi biti javno objavljeni i to mi ne bi smetalo.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

10. Ljudi su po svojoj prirodi dobronamjerni.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

11. Svatko bi trebao moći odabrati kome će i što reći o sebi.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

12. Kada me se traži davanje osobnih podataka, ponekad razmislim dvaput prije nego što ih pružim.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

13. Bojim se da bi neovlaštene osobe mogle pristupiti mojim osobnim podacima.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

14. Vjerujem da imam kontrolu nad svojim osobnim podacima.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

15. Većina ljudi ima tajne.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

16. Grozim se ideje da ljudi imaju ugrađene čipove pomoću kojih ih se može pratiti.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

17. Smeta me davati osobne podatke na toliko mjesta.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

18. U usporedbi s drugima, manje sam osjetljiv/a na način na koji se koriste moji osobni podaci.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

19. Većina tvrtki vrlo pažljivo postupa s privatnim podacima svojih korisnika.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

20. Postoje stvari koje ne želim ni sa kime podijeliti.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

21. Neprihvatljivo mi je da me se može neovlašteno snimiti ili slušati unutar mojeg doma.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

22. Zabrinut/a sam da se prikuplja previše podataka o meni.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

23. Kamere na javnim površinama i u trgovinama uopće mi ne smetaju.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

24. Nemam ništa protiv da se anonimni podaci o meni koriste kako bih dobivao/la preciznije reklame.

1 2 3 4 5

Uopće se ne slažem U potpunosti se slažem

25. Mnogi ljudi se hrane tuđim slabostima.

1	2	3	4	5
Uopće se ne slažem				U potpunosti se slažem

26. Privatnost je zastario koncept koji u 21. stoljeću više nema puno smisla.

1	2	3	4	5
Uopće se ne slažem				U potpunosti se slažem

27. Većina ljudi okoristit će se tuđim tajnama ako im se ukaže prilika.

1	2	3	4	5
Uopće se ne slažem				U potpunosti se slažem

28. Zaštita privatnosti uzaludan je posao.

1	2	3	4	5
Uopće se ne slažem				U potpunosti se slažem

Skala socijalne udaljenosti

Molim Vas da za sljedeće podatke odredite kojima ste ih sve osobama i institucijama spremni ustupiti. Odaberite sve točne odgovore.

29. Podaci o zaposlenju (poslodavac, radno mjesto, pozicija u tvrtki, radno vrijeme, broj dana godišnjeg odmora...)

- □ Ni sa kime
- □ S partnerom/icom
- □ S članom obitelji
- □ S prijateljem
- □ S poznanikom
- □ S nepoznatom osobom
- □ S privatnim tvrtkama
- □ S državnim institucijama

30. Biografski podaci (životopis, adresa, dob, e-adresa, broj mobitela...)

- □ Ni sa kime
- □ S partnerom/icom
- □ S članom obitelji
- □ S prijateljem
- □ S poznanikom
- □ S nepoznatom osobom
- □ S privatnim tvrtkama
- □ S državnim institucijama

31. Antropometrijski podaci (visina, težina, boja očiju, boja kose...)

- □ Ni sa kime
- □ S partnerom/icom
- □ S članom obitelji
- □ S prijateljem
- □ S poznanikom
- □ S nepoznatom osobom
- □ S privatnim tvrtkama
- □ S državnim institucijama

32. Ukusi, vrijednosti i stavovi (politička pripadnost, stav o pobačaju, vjeroispovijest, hobiji, preferencije općenito...)

- □ Ni sa kime
- □ S partnerom/icom
- □ S članom obitelji
- □ S prijateljem
- □ S poznanikom
- □ S nepoznatom osobom
- □ S privatnim tvrtkama
- □ S državnim institucijama

33. Podaci o lokaciji (gdje se trenutno nalazite i gdje ste se nalazili)

- □ Ni sa kime
- □ S partnerom/icom
- □ S članom obitelji
- □ S prijateljem
- □ S poznanikom
- □ S nepoznatom osobom
- □ S privatnim tvrtkama
- □ S državnim institucijama

34. Podatke o sadašnjim i bivšim ljubavnim vezama (s kime ste (bili) u vezi, koliko dugo i koliko intenzivno)

- □ Ni sa kime
- □ S partnerom/icom
- □ S članom obitelji
- □ S prijateljem
- □ S poznanikom
- □ S nepoznatom osobom
- □ S privatnim tvrtkama
- □ S državnim institucijama

35. Medicinske podatke (medicinski karton, lijekove koje ste uzimali, zahvate koje ste imali...)

- □ Ni sa kime
- □ S partnerom/icom
- □ S članom obitelji
- □ S prijateljem
- □ S poznanikom
- □ S nepoznatom osobom
- □ S privatnim tvrtkama
- □ S državnim institucijama

36. Financijski podaci (plaća, imovina, ušteđevina, dugovi, na što trošite novac)

- □ Ni sa kime
- □ S partnerom/icom
- □ S članom obitelji
- □ S prijateljem
- □ S poznanikom
- □ S nepoznatom osobom
- □ S privatnim tvrtkama
- □ S državnim institucijama

Ponašanje

Molim Vas da za sljedeća ponašanja odredite koliko ste često u posljednjih šest mjeseci postupili na pojedini način.

37. Izbjegli posjetiti određenu internetsku stranicu iz straha da bi mogla zaraziti Vaše računalo ili kompromitirati Vaše osobne podatke?

1	2	3	4	5
Niti jednom				Vrlo često

38. Prilikom registracije za određenu uslugu dali lažne osobne podatke ili lažnu e-adresu?

1	2	3	4	5
Niti jednom				Vrlo često

39. Odlučili odustati od započete internetske kupovine jer niste bili sigurni što će se dogoditi s Vašim podacima?

1	2	3	4	5
Niti jednom				Vrlo često

40. Odlučili se ne registrirati na internetsku stranicu jer se od Vas tražilo davanje osobnih podataka koje niste bili spremni dati?

1 2 3 4 5

Niti jednom Vrlo često

41. Požalili se Agenciji za zaštitu osobnih podataka zbog narušavanja Vaše privatnosti?

1 2 3 4 5

Niti jednom Vrlo često

42. Zatražili od neke tvrtke ili internetskog servisa da ukloni ili obriše Vaše osobne podatke koji su javno objavljeni ili koje imaju u svojoj evidenciji?

1 2 3 4 5

Niti jednom Vrlo često

43. Uništili dokumente koji sadrže Vaše osobne podatke prije nego što ste ih odložili u otpad?

1 2 3 4 5

Niti jednom Vrlo često

44. Sakrili rukom PIN broj prilikom korištenja bankovnih kartica?

1 2 3 4 5

Niti jednom Vrlo često

45. Pročitali politiku privatnosti prije registracije na internetsku stranicu ili prije instaliranja aplikacija na mobilni telefon?

1 2 3 4 5

Niti jednom Vrlo često

46. Obrisali sve kolačiće (eng. cookies) iz internetskog preglednika?

1 2 3 4 5

Niti jednom Vrlo često

47. Provjerili nalazi li se na Vašem računalu spyware?

1 2 3 4 5

Niti jednom Vrlo često

48. Obrisali povijest pretraživanja u internetskom pregledniku?

1 2 3 4 5

Niti jednom Vrlo često

49. Koristili incognito/tajni način rada za pregledavanje interneta?

1	2	3	4	5
Niti jednom				Vrlo često

50. Koristili VPN ili TOR prilikom spajanja na internet?

1	2	3	4	5
Niti jednom				Vrlo često

51. Prilikom kupovine koristili program vjernosti trgovaca (multiplus card, DM active beauty, IKEA family card, nagradne milje i sl.)

1	2	3	4	5
Niti jednom				Vrlo često

52. Kupovali putem interneta?

1	2	3	4	5
Niti jednom				Vrlo često

53. U telefonskom razgovoru prešutjeli reći nešto što ste željeli reći iz straha od prisluškivanja?

1	2	3	4	5
Niti jednom				Vrlo često

Korištenje interneta

U nastavku se nalazi niz pitanja o načinu na koji koristite Internet, e-poštu i društvene mreže. Odaberite sve točne odgovore.

54. Za pretraživanje interneta najčešće koristim sljedeći pretraživač.

Ukoliko pretraživač koji najčešće koristite nije naveden, molim Vas da ga navedete pod ostalo.

- □ Google, Bing, Yahoo
- □ Ostalo:_____

55. Za elektroničku poštu najčešće koristim sljedeći servis.

Ukoliko email servis koji najčešće koristite nije naveden, molim Vas da ga navedete pod ostalo.

- □ Gmail, Yahoo mail, Microsoft (hotmail.com, outlook.com...)
- □ Email ISP-a (bnet, t-com, vipnet, iskon...)
- □ Službeni poslovni
- □ Ostalo:_____

56. Navedite društvene mreže koje ste koristili u posljednjih šest mjeseci.

- □ Facebook
- □ G+
- □ Instagram
- □ Twitter
- □ LinkedIn
- □ Snapchat
- □ Ne koristim društvene mreže
- □ Ostalo:_____

57. Tko sve može vidjeti Vaš profil na društvenim mrežama?

- □ Nitko (koristite lažni profil)
- □ Prijatelji
- □ Prijatelji prijatelja
- □ Svi (javnost)
- □ Ne koristim društvene mreže.

58. Na Vašem profilu na društvenim mrežama nalazi se:

Ako se pojedini podatak nalazi na bilo kojoj od društvenih mreža koju koristite, molim

Vas da ga označite. Odaberite sve točne odgovore.

- □ Pravo ime
- □ Pravo prezime
- □ Adresa stanovanja
- □ Broj telefona ili mobitela
- □ E-adresa
- □ Fotografija
- □ Podaci o školovanju
- □ Podaci o zaposlenju
- □ Religijski ili politički stavovi
- □ Pripadnost klubovima, udrugama i/ili inicijativama
- □ Omiljene knjige, filmovi, glazba ili ideje koje podržavate
- □ Ne koristim društvene mreže.

Mogućnost pristupa podacima

Molim vas da za sljedeće kategorije podataka navedete tko im sve, prema vašem mišljenju, može pristupiti. Odaberite sve točne odgovore.

59. Telefonski razgovori (fiksni i mobilni)

- □ Hrvatska policija i obavještajne službe na temelju odgovarajućeg naloga.
- □ Određene strane policije i obavještajne službe
- □ Pružatelji internetskih usluga (t-com, vipnet, tele2, optima, iskon...)
- □ Hakeri ili vješti korisnici
- □ Nitko - ti podaci su za sada sigurni.

60. Dopisivanje i razgovori putem mobilnih aplikacija (whatsapp, viber...)

- □ Hrvatska policija i obavještajne službe na temelju odgovarajućeg naloga.
- □ Određene strane policije i obavještajne službe
- □ Pružatelji internetskih usluga (t-com, vipnet, tele2, optima, iskon...)
- □ Hakeri ili vješti korisnici
- □ Nitko - ti podaci su za sada sigurni.

61. Sadržaj e-pošte koju šaljete ili primate

- □ Hrvatska policija i obavještajne službe na temelju odgovarajućeg naloga.
- □ Određene strane policije i obavještajne službe
- □ Pružatelji internetskih usluga (t-com, vipnet, tele2, optima, iskon...)
- □ Hakeri ili vješti korisnici
- □ Nitko - ti podaci su za sada sigurni.

62. Fotografije na Vašem mobitelu ili računalu

- □ Hrvatska policija i obavještajne službe na temelju odgovarajućeg naloga.
- □ Određene strane policije i obavještajne službe
- □ Pružatelji internetskih usluga (t-com, vipnet, tele2, optima, iskon...)
- □ Hakeri ili vješti korisnici
- □ Nitko - ti podaci su za sada sigurni.

63. Dokumenti i podaci pohranjeni u oblaku (icloud, dropbox, onedrive, google disk...)

- □ Hrvatska policija i obavještajne službe na temelju odgovarajućeg naloga.
- □ Određene strane policije i obavještajne službe
- □ Pružatelji internetskih usluga (t-com, vipnet, tele2, optima, iskon...)
- □ Hakeri ili vješti korisnici
- □ Nitko - ti podaci su za sada sigurni.

64. Pratiti lokaciju mojeg mobilnog telefona

- □ Hrvatska policija i obavještajne službe na temelju odgovarajućeg naloga.

- □ Određene strane policije i obavještajne službe
- □ Pružatelji internetskih usluga (t-com, vipnet, tele2, optima, iskon...)
- □ Hakeri ili vješti korisnici
- □ Nitko - ti podaci su za sada sigurni.

65. Podacima koji su zaštićeni snažnom enkripcijom (AES256 ili jačom).

- □ Hrvatska policija i obavještajne službe na temelju odgovarajućeg naloga.
- □ Određene strane policije i obavještajne službe
- □ Pružatelji internetskih usluga (t-com, vipnet, tele2, optima, iskon...)
- □ Hakeri ili vješti korisnici
- □ Nitko - ti podaci su za sada sigurni.

66. Gledati kroz kameru na mojem mobilnom telefonu ili računalu.

- □ Hrvatska policija i obavještajne službe na temelju odgovarajućeg naloga.
- □ Određene strane policije i obavještajne službe
- □ Pružatelji internetskih usluga (t-com, vipnet, tele2, optima, iskon...)
- □ Hakeri ili vješti korisnici
- □ Nitko - ti podaci su za sada sigurni.

Demografski podaci

67. Spol

- Muški
- Ženski

68. Dob:_____

69. Najviši završeni stupanj obrazovanja

- Osnovna škola
- Srednja škola
- Preddiplomski studij (viša škola)
- Diplomski ili dodiplomski studij (VSS)
- Poslijediplomski specijalistički studij ili znanstveni magisterij
- Doktorski studij

70. Ideologija

Kada se govori o politici, često se koriste termini lijevo-desno. Molim vas da na sljedećoj skali odaberete broj koji najviše odgovara vašoj političkoj pripadnosti.

1	2	3	4	5	6	7	8	9
Lijevo								Desno

Prilog 2 – Okvirni protokol za polustrukturirani intervju korišten u kvalitativnom dijelu istraživanja

Protokol

- Možete li se prisjetiti posljednje situacije u kojoj je Vaša privatnost bila narušena?
    - Zbog čega
    - Kako ste se tada osjećali?
- Što je prema Vašem mišljenju privatnost?
    - Što sve taj pojam obuhvaća?
- Kako doživljavate pojam privatnosti?
- Što je za Vas pravo na privatnost?
    - Smatrate li privatnost temeljnim ljudskim pravom?
    - Što to za Vas znači?
    - Zbog čega?
- Je li Vama važna privatnost?
    - U kojoj mjeri?
    - Zbog čega?
    - U čemu vidite vrijednost privatnosti?
- Čega biste se bili spremni odreći za veću privatnost?
- Jeste li zadovoljni trenutnom zaštitom privatnosti koju uživate?
    - Ako niste, s čime biste bili zadovoljniji?
- Što su za Vas ugoze privatnosti?
- Imate li osjećaj da je ugrožena Vaša privatnost?
    - Na koji način?
    - Kako se zbog toga osjećate?
- Osjećate li se nadziranima?
    - Ako da, pojasnite kada, kako?
    - Kako se zbog toga osjećate?
- Smetaju li Vam kamere koje snimaju javni prostor?
    - Zbog čega?
- Mijenjate li svoje ponašanje u prostoru za koji mislite da je nadziran kamerama?
    - Zašto
    - Jeste li zadovoljni time?
- Mislite li da netko može čitati vaše poruke i elektroničku poštu?
    - Tko? Kako? Zašto?
    - Utječe li to na način na koji koristite elektronsku komunikaciju? Sputava li Vas to?
- Do koje razine informacija o vama mislite da ima pravo znati potpuni stranac?

Životopis autora

Andro Pavuna rođen je 1987. godine u Zagrebu, gdje je završio osnovnu i srednju školu. Preddiplomski studij psihologije upisao je 2005. godine na Odsjeku za psihologiju Filozofskog fakulteta u Zagrebu, gdje je odmah potom upisao i diplomski studij psihologije koji je završio 2010. godine. Dobitnik je rektorove nagrade za znanstveni rad, a bio je angažiran i kao demonstrator na Odsjeku za psihologiju. Za vrijeme studija bio je vrlo aktivan u radu strukovnih udruga psihologa i studenata psihologije na nacionalnoj i međunarodnoj razini, gdje je sudjelovao u radu strukovnih odbora za prometnu psihologiju te je bio jedan od osnivača i prvi pročelnik Studenske sekcije Hrvatskog psihološkog društva. Krajem 2012. godine upisao je poslijediplomski doktorski studij Politologija, smjer Međunarodni odnosi na Fakultetu političkih znanosti.

Nakon diplomiranja kraće je vrijeme radio kao stručnjak za ljudske potencijale na poslovima selekcije i edukacije kadrova te na poslovima voditelja projekta, a imao je i kratko iskustvo rada kao psiholog stručni suradnik u osnovnoj školi u Zagrebu. Od 2011. godine zaposlen je u sigurnosnom sustavu Republike Hrvatske, gdje se kao državni službenik kontinuirano stručno usavršava i obrazuje.

S izlaganjem je sudjelovao na nizu međunarodnih znanstvenih i stručnih skupova i kongresa. Oženjen je i otac djevojčice.

Lista objavljenih radova:

- Pavuna, A. (u tisku). Paradoks privatnosti: empirijska provjera fenomena. *Politička misao*. Rad je prihvaćen za objavu u Vol 56. (2019). br. 1.
- Pavuna, A. i Ivanec, D. (2012). Utjecaj alkohola na učinak u zadatku sljepoće zbog nepažnje u simuliranoj situaciji vožnje automobila. *Psihologijske teme*, 21 (1), 121-138.