UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Jelena Burnik

Vedenjsko oglaševanje v elektronskem komuniciranju

Doktorska disertacija

Ljubljana, 2019

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Jelena Burnik

Mentorica: izr. prof. dr. Urša Podnar Golob

Vedenjsko oglaševanje v elektronskem komuniciranju

Doktorska disertacija

Ljubljana, 2019

ZAHVALA

Iskrena hvala moji družini in staršem, vsem mojim najbližjim. Ta disertacija se brez njihove pomoči, neskončnega razumevanja, ljubezni in časa nikoli ne bi zgodila.

Hvala mentorici, izr. prof. dr. Urši Podnar Golob, ki je moj trud in znanje znala samozavestno in strokovno voditi v pravo smer – proti uspešnemu zaključku doktorskega študija.

In ne nazadnje, hvala izr. prof. dr. Tanji Oblak Črnič ter izr. prof. dr. Alešu Završniku, za vse zelo konstruktivne predloge in prispevke k oblikovanju in dokončanju disertacije.

Jaša, Asja in Luka, hvala, ker ste.

Izjava o avtorstvu

POVZETEK

Vedenjsko oglaševanje je novejše orodje tržnega komuniciranja, katerega posebnost je avtomatizacija procesov oglaševanja in podprtost s sofisticiranimi analizami podatkov o posameznikih, ki lahko vključujejo profiliranje na podlagi tehnologij strojnega učenja. Vedenjsko oglaševanje temelji na sledenju aktivnostim uporabnika elektronskih komunikacijskih tehnologij. Glede na analizo podatkov o njegovih aktivnostih, so uporabniku nato prikazani le zanj relevantni oglasi, oz. druge vsebine (Zuiderveen Borgesius, 2014). Bolj ali manj avtomatizirano se uporablja na različnih tehnoloških platformah, ne le na spletnih straneh in pri spletnih storitvah. Čedalje bolj se širi uporaba na področje interneta stvari, torej pametnih pripomočkov za vsakdanjo rabo, ki so povezani v internet. Poleg tega so čedalje bolj poudarjene težnje povezovanja podatkov o tem, kako posameznik uporablja elektronske naprave, s podatki o njegovih aktivnostih v realnem svetu, nakupih v trgovinah, geolokacijah ter uporaba vedenjskega oglaševanja za namene političnih kampanj. Vedenjsko oglaševanje je bistvo najuspešnejših poslovnih modelov v digitalnem okolju današnjega časa in eden redkih načinov, kako brezplačno storitev na spletu spremeniti v donosno. Obenem pa vedenjsko oglaševanje vzbuja številne pomisleke glede posega v zasebnost uporabnikov (npr. McDonald in Cranor, 2009; McStay, 2011) in v pravico do obveščenosti (Goodman in drugi, 2017), odpira širša vprašanja poslovne etike (Carsten Stahl, 2008), družbene odgovornosti korporacij (Pollach, 2011) in vplivov osebne prilagoditve (personalizacije) vsebin na družbo (Pariser, 2011). V zadnjih letih je čedalje bolj poudarjena tudi vloga vedenjskega profiliranja za namen političnega trženja, kar razgrinja nove razsežnosti vprašanj o vplivu na demokratične procese v družbi (CoE, 2017). Akademskih prispevkov na to temo ni veliko (npr. Busch, 2016; Zuiderveen Borgesius, 2014, 2016) in čeprav odkrivajo marsikatere podrobnosti, ne zagotavljajo celostnega vpogleda v ta pojav.

Namen disertacije je zato oblikovanje celostnega okvira za regulacijo vedenjskega oglaševanja v prihodnosti, s temeljem v uvidih normativne teorije, ki poudarja, da so mediji vpeti v naše družbeno, moralno in politično življenje in je zato včasih pri omejevanju njihovega delovanja potrebno zunanje poseganje v obliki regulacije. V iskanju okvira za prihodnje urejanje elektronskega komuniciranja in novih tehnologij, ki vsebujejo komponente nadzora in posega v zasebnost posameznikov, normativni regulativni pogled v zadnjem času dopolnjuje tudi pristop družbene odgovornosti (King in Mcdonnell, 2012), ki raziskuje etično odgovornost ponudnikov sodobnih komunikacijskih storitev (Taddeo in Floridi, 2016).

V teoretičnem delu disertacija razvije konceptualni okvir za raziskovanje vedenjskega oglaševanja, ki gradi na pristopu kombiniranja različnih teorij s poudarkom na teorijah informacijske zasebnosti, študijah uporabe medijev v vsakdanjem življenju, politične ekonomije komuniciranja, vedenjske ekonomije, normativne teorije in na pristopu družbene odgovornosti. Teoretski okvir s črpanjem iz različnih šol in pristopov dopolni teoretske pristope s področja tržnega komuniciranja: teorija politične ekonomije (Mansell, 2004), ki se sprašuje o vzorcih moči v medijih, in poudarja koncept poblagovljenosti občinstev, študije, katerih fokus je na občinstvu in na načinih, kako so tehnologije in mediji vpete v vsakodnevno medijizirano življenje posameznikov (npr. Livingstone, 2002; Silverstone, 1999), ki so »stalno vključeni« (Turkle, 2008). Ker je glavna značilnost, po kateri se vedenjsko oglaševanje razlikuje od drugih vrst oglaševanja, zbiranje velikih količin podatkov o aktivnostih in preferencah uporabnikov, teoretski okvir raziskave vključuje uvide, ki jih ponujajo teorije informacijske zasebnosti ter vedenjska ekonomija, ki pomaga pojasniti predsodke, ki vodijo posameznike pri odločitvah o varovanju zasebnosti. Z namenom

boljšega razumevanja razsežnosti vedenjskega oglaševanja in profiliranja disertacija vključuje pregled šestih različnih primerov izvajanja vedenjskega oglaševanja: (1) programatično oglaševanje in dražbe uporabniških profilov, (2) spletna družbena omrežja, kot je Facebook, (3) Phorm – vedenjsko oglaševanje na ravni ponudnika dostopa do interneta, (4) preprodajalci podatkov – povezovanje *online* in *offline* virov, (5) internet stvari – posameznik je dosegljiv 24 ur na dan in (6) Cambridge Analytica: vedenjsko ciljanje za namen politične promocije.

Disertacija v empiričnem delu fenomen vedenjskega oglaševanja obravnava s kombinacijo več metod, in sicer sta hkrati uporabljeni dve kvalitativni metodi, pri čemer je ena od njiju prevladujoča, druga pa dopolnjuje rezultate. Opravljena je bila široka analiza vsebine dokumentov ter ekspertni intervjuji z 19 strokovnjaki z različnih področij, povezanih s temo raziskave. Odgovarja na vprašanja, (1) koliko je izvajanje vedenjskega oglaševanja na različnih platformah elektronskega komuniciranja učinkovito, kaj razvoj tehnologij vedenjskega oglaševanja pomeni v okviru razvoja relevantne panoge in kakšne so posledice za preostale deležnike, (2) koliko je vedenjsko oglaševanje invazivno in posega v pravice uporabnikov elektronskih komunikacijskih tehnologij ter koliko so trenutni pristopi k varovanju informacijske zasebnosti uporabnikov uspešni in (3) kakšen naj bo okvir za regulacijo vedenjskega oglaševanja v prihodnosti.

Ugotovitve kažejo, da je vedenjsko oglaševanje učinkovito, ker posameznika nagovarja osebno prilagojeno oz. relevantno (personalizirano) glede na njegovo stanje, vedenje in prepričanja. Tako se povečajo možnosti, da se bo na oglase odzval z zaželenim (nakupnim) vedenjem in bodo premagane omejitve oglaševalske navlake in selektivne zaznave potrošnikov. Temelj osebne prilagoditve je zbiranje podatkov o posameznikih, njihova analiza in umeščanje posameznikov v profile, na podlagi katerih je izbran posamezniku primeren oglas. Podatki posameznikov so tako gorivo današnjih najuspešnejših panog in poslovnih modelov, v katerih je večina storitev posameznikom sicer na voljo brezplačno, prihodke pa ponudniki storitev (najpogosteje) pridobivajo z vedenjskim oglaševanjem. Učinkovitost vedenjskega oglaševanja se veča s tehnološkim napredkom na področju možnosti zbiranja podatkov, njihovih obdelav in analiz ter ciljanja oglasov. Zanj je značilno povezovanje in kombiniranje podatkov, zbranih iz različnih *online* in *offline* virov, uporaba umetne inteligence, algoritmov in strojnega učenja za analizo podatkov ter navsezadnje težnje k čedalje večji avtomatizaciji oglaševanja, ki čedalje bolj temelji na sistemih za dražbo uporabniških profilov v realnem času. Govorimo lahko o vseprisotnem oglaševanju in posamezniku, ki je vedno vključen. Oglaševanje je tako vtkano v vsakodnevne aktivnosti posameznika, kot poudarja koncept mediatizacije, in ni omejeno le na zaslone in čas, ki ga preživi za njimi. V ekosistemu vedenjskega oglaševanja nastopajo različni akterji in kot kažejo ugotovitve, ni nujno, da je za vse subjekte boljša izbira kot tradicionalno oglaševanje, ki ne temelji na osebni prilagoditvi. Prednosti nedvomno prinaša *ad tech* panogi, ki ponuja storitve vedenjskega oglaševanja in povezanih podatkovnih storitev, še zlasti tistim ponudnikom, ki imajo dostop do podatkov velikega števila uporabnikov svojih »osnovnih storitev« (npr. Facebook in Google). Največja prednost vedenjskega oglaševanja za oglaševalce naj bi bila manjša izguba sredstev za nerelevantna občinstva, predvsem za nišne oglaševalce, boljše ciljanje ter merljivost. So pa pri uporabi sistemov avtomatiziranega oglaševanja izpostavljeni večjim možnostim zlorabe podatkov o njihovih strankah s strani *ad tech* panoge. Izdajateljem vedenjsko oglaševanje omogoča več sredstev za ustvarjanje vsebine, zlasti kadar se ta težko trži sama in pri manjših izdajateljih, ki nimajo možnosti neposrednega pogajanja z oglaševalci. Programatičen zakup naj bi po drugi strani oglasnemu prostoru nižal ceno, poleg tega izdajatelji podatkov svojih strank ne izrabljajo sami, temveč

ekonomske koristi večinoma prepustijo *ad tech* panogi, tveganja z vidika varstva osebnih podatkov strank pa so večja. Mediji z vedenjskim oglaševanjem pristopajo k reševanju finančnih težav in pogosto omejujejo dostop do vsebine tistim, ki takega oglaševanja ne želijo (z zidovi in zahtevami po različnih oblikah registracije in prijave posameznika). Zgornje ugotovitve pa kažejo, da vedenjsko oglaševanje ni nujno najučinkovitejša ekonomska možnost financiranja vsebine (rešitve so tudi na področju naročnin ter financiranja s strani države), zlasti če tveganjem prištejemo izpostavljenost ranljivejših posameznikov.

Slika prednosti in izzivov za uporabnike elektronskih komunikacij je podobno mešana. Na eni strani vedenjsko oglaševanje omogoča raznolikost vsebine in storitev, ki so jim na voljo (tudi ranljivejšim skupinam, za katere ob plačljivih modelih uporabe ne bi bilo nujno poskrbljeno), ter boljše, relevantnejše storitve, prihranek virov za iskanje storitev in produktov ipd. Po drugi strani pa je vedenjsko oglaševanje najpogosteje prikrito, posamezniki tehničnega ozadja in posledic ne razumejo, kar prinaša številne izzive za pravice posameznikov:

– poseg v pravico do zasebnosti in varstva osebnih podatkov ter vseprisotni nadzor komercialnih institucij in sledenje prek različnih naprav *online* in *offline*;
– poseg v pravico do enake obravnave: profiliranje posameznikov lahko vodi v diskriminacijo, ki posameznikom otežuje dostop do informacij in storitev, veča družbeno razslojenost in segregacijo ter poustvarja in množi stereotipe;
– oženje izbire (t. i. *filtre bubbles*), ki je posamezniku na voljo, saj profil vedno temelji na zgodovinskih podatkih ter predvidevanju, kaj bo posameznika zanimalo v prihodnosti, ni pa mu na voljo vsebina, ki bi ga zanimala na novo, ustvarjalno, hipno;
– uporaba in zloraba spletnih oglaševalskih sistemov za politični marketing posega v pravico do informiranosti in pravico do svobodnih volitev.

Posamezniki imajo na voljo spekter različnih možnosti za varovanje svoje zasebnosti pri vedenjskem oglaševanju, vendar jih le redko izkoristijo, in sicer zaradi slabe tehnične podkovanosti ter slabega razumevanja posledic vedenjskega oglaševanja, tudi zaradi vezanosti na posameznega ponudnika. V zadnjem obdobju je sicer viden porast uporabe protireklamnih vtičnikov (angl. *adblockers*), vendar najbrž predvsem zaradi izboljšane izkušnje uporabe storitev brez oglasov. Glede tega so zelo aktualna vprašanja digitalne pismenosti, oziroma zasebnostne ločnice med tistimi, ki vprašanja zasebnosti razumejo, in tistimi, ki jih ne. Na posameznika pri izvajanju nadzora nad svojo zasebnostjo prav tako vplivajo številni predsodki, kot sta npr. predsodka statusa quo in kratkovidnosti. Pomemben je tudi premislek o konceptualizaciji osebnih podatkov v smislu njihove ekonomske vrednosti, ki se čedalje bolj pojavlja na različnih ravneh razprave o vedenjskm oglaševanju kot poudarjanje ekonomskih in drugih ugodnosti, ki naj bi jih posameznikom v zameno za njihove osebne podatke ponudili ponudniki storitev. Taka konceptualizacija reducira pomena osebnih podatkov in zasebnosti na njuno ekonomsko vrednost in zasebnosti ne obravnava kot tiste, ki omogoča udejanjanje drugih temeljnih pravic posameznika. Tako lahko govorimo o komodifikaciji osebnih podatkov in občinstev, ki spodbuja diskriminacijo in družbeno segregacijo ter zarisuje zasebnostno ločnico, po kateri bodo imeli več pravice do zasebnosti bogatejši in bolj izobraženi, socialno in izobrazbeno šibkejši pa bodo podvrženi obdelavam njihovih osebnih podatkov, ki vodijo v še večje razslojevanje.

Za boljšo regulacijo področja vedenjskega oglaševanja v prihodnosti je potreben splet strategij in orodij ter usklajeno delovanje globalnih deležnikov, ne le izboljšave zakonodaje na tem področju. Ustrezen splet bi bila lahko ko-regulacija, preplet zakonodaje, ki bi zagotovila ustrezno podlago za varovanje temeljnih pravic in interesov posameznikov (ter določala

kaznovalne elemente oziroma elemente nadzora) ter samoregulacije, ki bi jo dopolnila s podrobnejšimi vsebinskimi pravili. Poenotiti bi bilo treba razumevanje problematike vedenjskega oglaševanja med ZDA in EU, saj so dejavnosti čezmejne. Ključni komponenti za učinkovito ko-regulacijo sta »pameten« nadzor in okrepitev nadzornih organov ter široko izobraževanje in opolnomočenje posameznikov (od šolske ravni dalje), da bodo sposobni in zainteresirani uveljavljati svoje pravice. Ker vedenjsko oglaševanje negativno vpliva tudi na politične pravice in demokratične procese, pravila s področja varovanja zasebnosti in varstva osebnih podatkov problematike ne morejo rešiti celostno. Zato imajo pomembno vlogo pravila ohranjanja konkurence, davčna pravila, medijska pravila, volilna pravila itd. Poleg skladnega izboljšanja različnih relevantnih regulatornih okvirov je rešitve smiselno iskati tudi na področju etike, družbene odgovornosti in vizije trajnostnega razvoja družbe. Boljša regulacija v EU zahteva tudi konkretne vsebinske izboljšave na področju zakonodaje o varovanju zasebnosti in osebnih podatkov (tako v smislu razlag Uredbe (EU) 2016/679 – GDPR kot tudi trenutno nastajajoče Uredbe o zasebnosti in elektronskih komunikacijah – ePR), predvsem glede različnih pravnih podlag, ki omogočajo boljše urejanje predmetnega področja kot pa zgolj legitimacija praks vedenjskega oglaševanja s privolitvijo, ki je pogosto le iluzija privolitve. Najbolj tvegani nameni vedenjskega oglaševanja bi morali biti zakonsko omejeni (npr. v okviru političnega komuniciranja, kadar omogoča zelo specifično diskriminiranje z znatnimi negativnimi posledicami v smislu reproduciranja družbene neenakosti, ali vključuje stalno spremljanje posameznika prek različnih platform). Privolitev bi morala biti omejena na primere, ki pomenijo večje tveganje za pravice posameznika in je hkrati posameznik zmožen situacijo razumeti in podati veljavno privolitev. Večji poudarek bi moral biti na enotnih tehnoloških rešitvah in standardih za pridobivanje privolitve (ena od možnosti je standard ne sledi). V nekaterih primerih bi bila lahko ustrezna pravna podlaga za vedenjsko oglaševanje tudi zakoniti interes izvajalca, kadar npr. v procesu ni obdelave ali sklepanja na občutljive osebne podatke ter je poseg v zasebnost zanemarljiv, ni diskriminacije ali vpliva na politične pravice. Disertacija zato v sklepu ponuja model operacionalizacije procesa tehtanja zakonitega interesa za primer vedenjskega oglaševanja. Pomembne so tudi izboljšave na področju obveščanja o vedenjskem oglaševanju s strani izvajalcev ter izobraževanju posameznikov, da bodo nadzor nad svojimi podatki sposobni in zainteresirani izvajati. Navsezadnje pa sta zelo pomembna upoštevanje načela vgrajene zasebnosti in izvajanje predhodnih ocen vplivov na zasebnost, saj oba usmerjata izvajalce k uporabi poslovnih modelov, ki omejujejo posege v pravice posameznikov.

Izvirnost prispevka disertacije se kaže v postavitvi teoretskega okvira za razumevanje vedenjskega oglaševanja, ki kombinira uvide različnih pristopov, kot tudi v uporabi kombinacije več metod empiričnega raziskovanja. Izvirni prispevek je izdelani celostni konceptualni model za prihodnje urejanje področja vedenjskega oglaševanja ter konkretiziran predlog operacionalizacije modela tehtanja zakonitega interesa za področje vedenjskega oglaševanja. Disertacija ponuja prvi celosten vpogled v tematiko v slovenskem prostoru in prispeva z razvoju slovenskega izrazja na tem področju. Ugotovitve študije so neposredno uporabljive v okviru pogajanj o nastajajoči zakonodaji (npr. ePR) in razlag zahtev Uredbe (EU) 2016/679 glede vedenjskega oglaševanja. Neposreden prispevek za prakso je tudi model operacionalizacije tehtanja zakonitega interesa za področje vedenjskega oglaševanja, ki ga lahko uporabijo upravljavci, izvajalci vedenjskega oglaševanja in nadzorni organi za varstvo osebnih podatkov, oziroma pristojni organi in odločevalci glede politik na tem področju.

Ključne besede: vedenjsko oglaševanje, elektronsko komuniciranje, zasebnost, varstvo osebnih podatkov, regulacija, Uredba (EU) 2016/679

SUMMARY

Behavioural advertising is a marketing communications tool, recently being employed by the industry. Its particularity is automation of advertising processes. It is facilitated by sophisticated analysis of data on individuals, which may include profiling based on machine-learning techniques. Behavioural advertising is based on tracking of users of electronic communication technologies. Based on the analysis of the data on users' activities, they are subsequently served with personalized advertisements (Zuiderveen Borgessius, 2014). It is being employed by many different platforms, not only on websites and by online services. More and more attempts are being made in the context of internet of things, smart devices for everyday use, connected to the internet. In addition, we witness trends of cross device tracking and conncentions of online and offline data, including data on individuals' real world activities, purchases in shops, geolocations, and the use of behavioural advertising for political campaign purposes. Behavioural advertising is at the core of todays' most successful business models in the digital environment and one of the few ways to monetize free online services. At the same time, behavioural advertising raises a number concerns, regarding user privacy (McDonald and Cranor, 2009; McStay, 2011) and the right to information (Goodman et al. 2017), broader issues of business ethics (Carsten Stahl, 2008), corporate social responsibility (Pollach, 2011), and the impact of personalisation of content on society (Parisser, 2011). In recent years, behavioural micro-targeting has also been highlighted in the context of political marketing, raising a new dimension of concerns regarding its influence on democratic processes in society (CoE, 2017). Not many academic contributions offer insights in this field (for example Busch, 2016; Zuiderveen Borgesius, 2014, 2016) and although they uncover many details, they do not provide a comprehensive view of this phenomenon.

The purpose of this dissertation is to establish a comprehensive framework for the regulation of behavioural advertising in the future, building on normative theories which highlight that the media are embedded in our social, moral and political life and, as a result, there is a need for external interference in the form of regulation, necessary to limit their functioning and negative externalities. In the search for a framework for the future regulation of electronic communications and new technologies that are marked by surveillance elements and interference with the privacy of individuals, the normative regulatory view is, recently, also complemented by a corporate social responsibility approach (King and McDonnell, 2012). It explores the ethical responsibility of providers of modern communication services (Taddeo and Floridi, 2016).

In the theoretical part of dissertation, a conceptual framework for research of behavioural advertising is developed, building on multi-theory approach, combining insights of information privacy theories, studies of media consumption in everyday life, political economy of communication, behavioural economics, normative theory and a corporate social responsibility approach. The theoretical framework, drawing from different schools and approaches, combines and complements the theoretical approaches in the field of marketing communications, by including: the theory of political economy of communications (Mansell, 2004), which raises questions about power relations in the media, and stresses the concept of commodification of audiences; studies with a focus on the audience and on the ways technologies and media are embedded in the daily mediatized life of individuals (e.g. Livingstone, 2002; Silverstone, 1999), which are 'always-on' (Turkle, 2008). The main feature distinguishing behavioural advertising from other types of advertising is the collection of large amounts of data on user activities and preferences. The theoretical research

framework therefore draws from insights, offered by information privacy theories and behavioural economics, which help explaining the prejudice that leads individuals in decisions related to their privacy. In order to better understand the dimensions of behavioural advertising and profiling the dissertation includes a review of six different examples of its implementation: (1) Programmatic advertising and real time bidding, (2) online social networks such as Facebook, (3) Phorm — behavioural advertising at the level of the internet service provider, (4) data brokers — connecting *online* and *offline* data sources, (5) Internet of Things — an individual is accessible 24/7 and (6) Cambridge Analytica: political micro targeting.

The empirical research of behavioural advertising is based on multi-method approach, where two qualitative methods are used in parallel, one being dominant and the other complementary. An extensive documentary analysis has been carried out, as well as expert interviews with 19 experts from various fields related to the survey. The research was lead by the following questions: (1) to what the extent is the use of behavioural advertising on different platforms of electronic communication efficient, what does it mean in the context of development of the relevant industry and what are the implications for other stakeholders, (2) to what extent is behavioural advertising invasive and interferes with the rights of users of electronic communications technologies, and to what extent are the current approaches to the protection of users' information privacy efficient and (3) how should the framework for future regulation of behavioural advertising be constructed.

The findings show that behavioural advertising is efficient, because it serves the individuals with personalised content, relevant to their context, behaviour and beliefs. This increases the options that individuals will react to advertising with desirable (purchase) behaviour and overcome restrictions stemming from their selective perception. The basis for personalization is collection of data on individuals, its analysis and the placement of individuals in profiles, based on which the individual is served with an appropriate advertisement. Individuals' data are therefore the fuel of today's growing industries and business models where the majority of services are provided free of charge to individuals and revenues of service providers are (most often) created by behavioural advertising. The efficiency of behavioural advertising increases with technological progress in the area of data collection, processing and analysis, and the targeting options. It is characterised by the integration and combination of data collected from various *online* and *offline* sources, the use of artificial intelligence, algorithms and machine learning to analyse data and, ultimately, the trend towards increasing automation of advertising, which is increasingly based on real-time bidding systems for the auctioning of user profiles. We can speak of ubiquitous advertising and an individual who is always-on. Advertising is embedded into the personal activities of the individual, as suggested by the concept of mediatisation, and is not limited only to the time spent using the devices.

The ecosystem of behavioural advertising includes different actors and as the results suggest, it is not necessarily a better choice than traditional advertising which is not based on personalization. Undoubtedly there are benefits for the *adtech* industry that offers behavioural advertising and related data processing services, especially for those providers who have access to data from a large number of users of their "basic services" (e.g. Facebook and Google).The significant advantage of behavioural advertising for advertisers comes from the fact that less resources are lost on non-relevant audiences, particularly for niche advertisers, to whom better and measurable targeting is crucial. However, when programmatic advertising systems are used, the advertisers are exposed to risks related to misuse of data on their

customers by the *adtech* industry. The publishers benefit from behavioural advertising in the sense that they can gather more resources to create content, especially the publishers that experience difficulty in marketing their own content and smaller publishers who do not have the possibilities to negotiate advertising rates directly with the advertisers. On the other hand, the use of programmatic advertising is lowering the price of advertising space, and additionally, the publishers do not make use of the data of their customers by themselves, but the economic benefits are largely passed on to the *ad tech* industry. The risks related to protection of customers' personal data are also greater. As for online media (news) outlets, they are experiencing financial difficulties and often limit access to content for those who do not want behavioural advertising (with paywalls and requirements for different forms of registration and individual applications). However, the above findings suggest that behavioural advertising is not necessarily the most efficient economic option for financing the content (other funding options include subscriptions and state funding), especially considering the risks the more vulnerable individuals are exposed to.

The views on the advantages and challenges for users of electronic communications are similarly mixed. On the one hand, behavioural advertising allows for the diversity of content and services available to them (including offers for vulnerable groups which might not be catered with special options under the economic models) and better, more relevant services, saving resources spent on the search for services and products, etc. On the other hand, behavioural advertising is most often non-transparent and hard to understand without considerable technical knowledge, which poses a number of challenges for the rights of individuals:

- interference with the right to privacy and the protection of personal data, as well as the increased commercial surveillance and tracking of individuals' *online* and *offline* activities;
- interference with the right to non-discrimination: profiling of individuals may lead to discrimination, which makes access to information and services more difficult for individuals, increases social ineqalities and segregation, and multiplies stereotypes;
- creation of the so called filter bubbles that reduce the range of offers available to an individual, since the choice is related to the user's profile which is always based on historical data and the inferences on future interests of the individual. The individual is not offered new, creative, spontaneous contents.
- the use and misuse of online advertising systems for political micro-targeting undermines the right to information and the right to free elections.

Individuals have a range of possibilities to protect their privacy in relation to behavioural advertising but rarely take advantage of them, due to poor technical knowledge and awareness of its negative consequences, as well as because of lock-in issues. There has been an increase recently in the use of adblockers, however mainly due to an improved user experience without advertising. In this regard it is important to note issues of digital literacy and privacy divide between those who understand privacy concerns and those who do not. Individuals are also affected by a number of prejudices when exercising control over their privacy, such as the status quo bias and myopia bias. It is also important to consider the conceptualisation of personal data in terms of their economic value, which is increasingly gaining momentum at different levels of discussion on behavioural advertising. It emphasises the economic and other benefits offered to individuals by service providers in exchange for their personal data. Such a conceptualisation reduces the importance of personal data and privacy to their economic value and disregards privacy as an enabling right in the exercise of other

fundamental rights of the individual. In this sense we can speak about commodification of personal data and audiences, which promotes discrimination and social inequalities, where more privacy will be offered to those well off and more educated, while the socially and educationally weaker individuals will be subject to more data processing, leading to increase in social ineqalities.

Better regulation of behavioural advertising in the future requires a combination of regulatory strategies and tools and a coordinated functioning of global stakeholders, not only improvements of legislation in this area. In this sense, co-regulation is seen as necessary; a combination of legislation that would provide adequate baseline protection of the fundamental rights and interests of individuals (and lay down punitive elements or supervision elements) and self-regulation to complement it by more detailed substantive rules. It is also important to strive to unify understanding of the behavioural advertising issues at the level of US and the EU, as the activities are of cross-border nature. The key components of effective co-regulation are also 'smart' enforcement and strengthening of supervisory authorities, and extensive education and empowerment of individuals (from school level), to be able and interested in exercising their rights. As behavioural advertising also has a negative impact on political rights and democratic processes, privacy and personal data protection rules cannot be the only silver bullet. The rules in the area of competition, taxes, media, and electoral rules need to be taken into account as well. In addition to the harmonious improvement of the various relevant regulatory frameworks, the solution also requires measures in the area of ethics, social responsibility and development of sustainable society. Better regulation in the EU requires specific substantive improvements in the area of privacy and personal data protection legislation (both in the light of interpretations of Regulation (EU) 2016/679 — GDPR as well as in the currently negotiated ePrivacy Regulation), in particular with regard to the different legal bases available in the context of behavioural advertising that could allow for better regulation of the subject matter than the mere legitimation of behavioural advertising practices with (the illusion of) consent. The most risky options of behavioural advertising should be limited by the law (e.g. in the context of political marketing, or when it allows for specific discrimination with significant negative consequences in terms of reproduction of social inequality, or involves continuous monitoring of the individual through different platforms). Consent should be limited to cases where there is a higher risk for individual rights and at the same time the individual is able to understand the situation and to give valid consent. More emphasis should be put on uniform technological solutions and standards for obtaining consent (do not track standard might be one of the options). In some cases, legitimate interest could be considered as an appropriate legal basis for behavioural advertising, for example, where there is no processing of sensitive personal data and the interference with privacy is negligible, when there is no discrimination or impact on political rights. To this end, the dissertation offers a model for operationalisation of the legitimate interest balancing test for behavioural advertising use case. Improvements are also necessary in the area of transparency and information, as well as in education of individuals to enable them to exercise control over their data. Last but not least, compliance with the principle of privacy by design and the implementation of ex-ante privacy impact assessments are very important, as they both facilitate the development of business models with lower negative impact on the rights of individuals.

The originality of the dissertation contribution is reflected in the establishment of a theoretical framework for understanding behavioural advertising, combining different approaches, as well as in the use of a combination of methods of empirical research. The original

contribution is the comprehensive conceptual model for future regulation of behavioural advertising, and a concrete proposal for the operationalisation of the legitimate interest balancing test. The dissertation also offers a first comprehensive view of the topic in Slovenia and contributes to the development of Slovenian terminology in this area. The findings of the study are directly applicable in the context of negotiations on developing legislation (e.g. ePR) and interpretations of the requirements of Regulation (EU) 2016/679 regarding behavioural advertising. A direct applicable contribution is also the model for the operationalisation of the legitimate interest balancing test, which can be used by data controllers, behavioural advertising industry and supervisory authorities for the protection of personal data, or by competent authorities and decision-makers who develop policies in this area.

Keywords: behavioural advertising, electronic communications, privacy, data protection, regulation, General Data Protection Regulation.

Kazalo vsebine

1 UVOD 19
1.1 Opredelitev problematike in njena znanstvena relevantnost 19
1.2 Namen disertacije in teoretični okvir 24
1.3 Metodologija raziskave 27
1.4 Izvirnost prispevka disertacije 28
1.5 Omejitve dela 30
1.6 Zgradba disertacije 32
2 UVOD V PROBLEMATIKO VEDENJSKEGA OGLAŠEVANJA: PREGLED LITERATURE 34
2.1 Vedenjsko oglaševanje in sledenje uporabnikom 36
2.2 Razvoj vedenjskega oglaševanja: proti avtomatizaciji procesov, povezovanju podatkov iz različnih virov in distribuciji oglasov prek različnih kanalov 37
2.2.1. Programatično oglaševanje in dražbe uporabniških profilov: prevlada Googla in Facebooka 40
2.2.2 Spletna družbena omrežja: Facebook 45
2.2.3 Phorm: Vedenjsko oglaševanje na ravni ponudnika dostopa do interneta 48
2.2.4 Preprodajalci podatkov – povezovanje *online* in *offline* virov 50
2.2.5 Internet stvari – posameznik je dosegljiv 24 ur na dan 54
2.2.6 Cambridge Analytica: vedenjsko ciljanje za namen politične promocije 58
2.3 Zakaj je vedenjsko oglaševanje in sledenje uporabnikom problematično? 62
2.5 Vedenjsko oglaševanje in odnos uporabnikov 73
2.5 Pravno ozadje in prvi poskusi regulacije vedenjskega oglaševanja 79
2.6 Ključne točke pregleda literature s področja vedenjskega oglaševanja 84
3 TEORETSKI OKVIR RAZISKAVE IN RAZISKOVALNA VPRAŠANJA 87
3.1 Pogled na vedenjsko oglaševanje, njegovo delovanje in učinkovitost skozi tržno komuniciranje in kritično perspektivo alternativnih pristopov 88
3.1.1 Prednosti vedenjskega in programatičnega digitalnega oglaševanja 90
3.1.2 Kritični pogled na vrednost vedenjskega oglaševanja za oglaševalce 92
3.1.3 Pristop medijske potrošnje in študije občinstva: družbeni vidiki in vedenjsko oglaševanje v mediatiziranem vsakdanu posameznika 96
3.1.4 Pristop politične ekonomije komuniciranja in vedenjsko oglaševanje 106
3.1.5 Novi mediji, vedenjsko oglaševanje in demokratični procesi: razlogi za regulacijo 111

3.2 Pristopi informacijske zasebnosti: zasebnost in druge temeljne pravice posameznikov pri vedenjskem oglaševanju 117
3.2.1 Pravica do zasebnosti: kontekstualni pristop 118
3.2.2 Informacijska zasebnost oziroma varstvo osebnih podatkov 123
3.2.3 Pristop vedenjske ekonomije 127
3.3 Okvir za preučevanje danes veljavne in prihodnje regulacije področja vedenjskega oglaševanja 129
3.3.1 Teoretični vidiki razlogov za regulacijo vedenjskega oglaševanja 130
3.3.2 Strategije regulacije vedenjskega oglaševanja 134
3.3.4 Pristop družbene odgovornosti 141
3.4 Postavitev celostnega teoretskega okvira 145
3.5 Raziskovalna vprašanja 148
4 EMPIRIČNO RAZISKOVANJE VEDENJSKEGA OGLAŠEVANJA: METODOLOGIJA RAZISKAVE 151
4.1 Analiza dokumentov 153
4.1.1 Proces analize dokumentov 155
4.1.2 Vzorčenje dokumentov in analizirani podatki 156
4.2 Ekspertni intervjuji 158
4.2.1 Vsebinska zasnova intervjujev 159
4.2.2 Vzorčenje, postopek zbiranja in analize podatkov 160
4.2.3 Profili strokovnjakov 163
5 ANALIZA OKVIRA REGULACIJE VEDENJSKEGA OGLAŠEVANJA 166
5.1 Pravni okvir za varovanje zasebnosti in varstva osebnih podatkov v EU 166
5.1.1 Direktiva o zasebnosti in elektronskih komunikacijah 167
5.1.2 Splošna uredba o varstvu osebnih podatkov 169
5.1.3 Pravni okvir in vedenjsko oglaševanje: pravne podlage 174
5.1.4 Obveščanje o vedenjskem oglaševanju 189
5.1.5 Odgovornosti različnih akterjev v ekosistemu vedenjskega oglaševanja 191
5.1.6 Nacionalne razlike in nadzor nad področjem vedenjskega oglaševanja 194
5.1.7 Uredba o zasebnosti in elektronskih komunikacijah 196
5.2 Pravni okvir za varovanje osebnih podatkov v Združenih državah Amerike 202
5.2.1 Sektorske omejitve za obdelavo osebnih podatkov 202
5.2.2 Nadzor na področju varovanja osebnih podatkov 205
5.2.3 Razvoj zakonodaje, ki bi poenotila pravila o varstvu osebnih podatkov 207

5.3 Samoregulacija 210
5.3.1 Samoregulacijski kodeksi 211
5.3.1 Certificiranje in standardizacija 217
5.4 Standard ne sledi 220
5.4.1 Standard ne sledi danes 222
5.4.2 Standard ne sledi kot orodje za regulacijo vedenjskega oglaševanja 228
5.5 Sklepno o regulatornem okviru za vedenjsko oglaševanje 229
6 UGOTOVITVE ANALIZE INTERVJUJEV 232
6.1 Vedenjsko oglaševanje v kontekstu razvijajočih sodobnih tehnologij in novih poslovnih modelov: prednosti in izzivi za deležnike 233
6.1.1 Oglaševalci 233
6.1.2 *Ad tech* panoga 234
6.1.3 Založniki 236
6.1.4 Uporabniki: od prednosti osebne prilagoditve vsebin do sredstev za blokiranje oglasov 240
6.2 Vedenjsko oglaševanje in vpliv na pravice uporabnikov elektronskih komunikacij 241
6.2.1 Izzivi vedenjskega oglaševanja za posameznike in družbene procese 242
6.2.2 Mehanizmi za zaščito uporabnikov pred vedenjskim oglaševanjem in sledenjem 246
6.3 Razvoj in trenutne razmere na področju regulacije vedenjskega oglaševanja 246
6.3.1 Varovanje zasebnosti v ZDA in v EU: varstvo osebnih podatkov kot temeljna človekova pravica ali kot potrošniška pravica 251
6.3.2 Razvoj regulacije glede vedenjskega oglaševanja v ZDA in EU 252
6.3.3 Regulacija vedenjskega oglaševanja v širšem političnem kontekstu konkurenčnosti držav 257
6.4 Boljša regulacija vedenjskega oglaševanja v prihodnosti 259
6.4.1 Splet strategij za boljšo regulacijo vedenjskega oglaševanja 260
6.4.2 Izboljšave na področju EU zakonodaje o varovanju zasebnosti in osebnih podatkov in njenega izvajanja 277
6.5 Sinteza ugotovitev dokumentarne analize in analize intervjujev 288
7 DISKUSIJA UGOTOVITEV GLEDE NA TEORETSKI OKVIR IN ODGOVORI NA RAZISKOVALNA VPRAŠANJA 291
7.1 Diskusija ugotovitev glede na teoretski okvir 291
7.2 Odgovori na raziskovalna vprašanja 316
7.2.1 Odgovor na prvo raziskovalno vprašanje 316
7.2.2 Odgovor na drugo raziskovalno vprašanje 320

7.2.3 Odgovor na tretje raziskovalno vprašanje ... 328
7.3 Operacionalizacija modela tehtanja zakonitega interesa za primer vedenjskega oglaševanja ... 336
7.4 Sinteza odgovorov na raziskovalna vprašanja ... 339
8 ZAKLJUČEK ... 342
8.1 Sklepne misli ... 342
8.2 Omejitve in nadaljnje raziskovanje ... 346
8.3 Prispevki za prakso ... 348
9 VIRI ... 349
PRILOGE ... 383
Priloga A: Povezovanje piškotkov ... 383
Priloga B: Potenciali programatičnega oglaševanja in izzivi za uporabnike elektronskih komunikacij ... 384
Priloga C: Facebook v primežu nadzornih organov in sodišč ... 388
Priloga D: Trženjski produkti trgovcev s podatki ... 392
Priloga E: Priporočila glede dobrih praks in bodoče zakonodaje na področju trgovcev s podatki ... 395
Priloga F: Vedenjsko oglaševanje na digitalni TV ... 399
Priloga G: Cambridge Analytica, Facebook in Brexit referendum ... 401
Priloga H: Priporočila ICO glede politik obdelave osebnih podatkov v političnih kampanjah ... 402
Priloga I: Priporočila Evropskega nadzornika za varstvo podatkov ... 402
Priloga J: Vprašalnik za intervjuje ... 404
Priloga K: Direktiva 2002/58/ES in določbe o piškotkih ... 406
Priloga L: Več o Splošni uredbi za varstvo osebnih podatkov ... 412
Priloga M: Podrobneje o profiliranju ... 414
Priloga N: Psevdonimni podatki ... 416
Priloga O: Obveščanje posameznika po Uredbi 2016/679 ... 417
Priloga P: Pristojnost nadzornih organov v EU ... 418
Priloga R: Sektorska zakonodaja v ZDA ... 419
Priloga S: IAB okvir za vedenjsko oglaševanje ... 420
Priloga T: Tehnologija za konceptom standarda ne sledi in politike glede njegovega upoštevanja ... 421
Priloga U: Odziv Delovne skupine iz člena 29 na standard ne sledi ... 423

Kazalo slik

Slika 1.1: Shematski prikaz sestave disertacije 33
Slika 2.1: Ponudniki v verigi programatičnega oglaševanja in povezave med njimi 42
Slika 2.2: Pregled izvajalcev prikaznega oglaševanja LumaScape 42
Slika 2.3: Proces programatičnega draženja profilov v realnem času 44
Slika 2.4: Ciljano oglaševanje v okolju interneta stvari 57
Slika 2.5: Blokiranje oglasov 78

Kazalo tabel

Tabela 3.1: Multi-teoretski konceptualni okvir za razumevanje ključnih dilem in vprašanj glede vedenjskega oglaševanja in njegove regulacije 146
Tabela 4.1: Vzorčenje dokumentov, ki so bili uporabljeni za analizo, in analizirani podatki 157
Tabela 4.2: Opis intervjuvancev glede na njihove izkušnje in pripadnost skupini deležnikov 165
Tabela 6.1: Sinteza primerjave ugotovitev dokumentarne analize in analize intervjujev 289
Tabela 7.1: Poskus operacionalizacije modela tehtanja zakonitega interesa za primer vedenjskega oglaševanja 337
Tabela 7.2: Sinteza odgovorov na raziskovalna vprašanja 339

Seznam kratic

COE	*Council of Europe* – Svet Evrope
EDPB	*European Data Protection Board* – Evropski odbor za varstvo podatkov
EDPS	*European Data Protection Supervisor* – Evropski nadzornik za varstvo podatkov
ePD	*ePrivacy Directive* – Direktiva 2002/58/ES o zasebnosti in elektronskih komunikacijah
ePR	*ePrivacy Regulation* – Uredba o zasebnosti in elektronskih komunikacijah
EU	Evropska unija
FTC	*Federal Trade Commission* – Zvezna komisija za trgovino iz Združenih držav Amerike
GDPR	*General Data Protection Regulation* – Splošna uredba 2016/679 o varstvu osebnih podatkov
ICO	*Information Commissioner's Office* – britanski nadzorni organ za varstvo osebnih podatkov
IP	Informacijski pooblaščenec Republike Slovenije
W3C	*World Wide Web Consortium*
WP29	*Article 29 Working Group* – Delovna skupina iz člena 29
ZEKom-1	Zakon o elektronskih komunikacijah
ZDA	Združene države Amerike

1 UVOD

1.1 Opredelitev problematike in njena znanstvena relevantnost

Sodobno družbo zaznamuje razvoj informacijskih tehnologij, predvsem interneta, ki spreminja svet komuniciranja in medijev ter pospešuje globalne družbene spremembe, hkrati pa je izziv za veljavne zakone in norme (Bagdikian, 2004, str. 58–59; Benkler, 2003). Dostop do informacij je postal tista ključna razsežnost, ki neprivilegiranim omogoča konkuriranje v družbi (Benkler, 2011). Informacije pomenijo moč, ki pa med akterji v družbi ni enakomerno porazdeljena (Woo, 2006; Castells, 2001). Okolje »novih« medijev«[1] je podvrženo političnim in komercialnim interesom, ki izpodjedajo njegov potencial javnega dobrega (Pariser, 2011). Koncentracija lastništva, širjenje pravic intelektualne lastnine, naraščajoča komercializacija informacij in kulturnih produktov ter porast spletnega oglaševanja so značilnosti razvoja komunikacijskih tehnologij (Bettig, 1997, str. 139–140). Internet kot javno dobro, kjer so informacije iskalcu na voljo tradicionalno brezplačno ali za nizko ceno, večinoma financirajo oglaševalci (LSE, 2009b), podobno kot v tradicionalnih medijih, ki občinstvu prinašajo svoje produkte, oglaševalcem pa v zameno občinstva (Mosco, 1996, str. 148–149). Kritika v tem odnosu poudarja vlogo oglaševalcev kot cenzorjev, ki vplivajo na medijske vsebine (Herman in Chomsky, 1994).

Velika razlika med novimi in starimi mediji je v produktu, ki ga dobijo oglaševalci – v tradicionalnih medijih oglaševalec ni imel na voljo zelo natančnih podatkov o gledalcih in bralcih. Segmentacija glede na nekaj dejavnikov se je v svetu novih medijev spremenila v neposredno ciljanje na enega določenega uporabnika, katerega preference in vedenje je zabeležil ponudnik storitve (Evans, 2009, str. 9) s t. i. »vedenjskim« oglaševanjem[2]. Literatura ponuja kar nekaj opredelitev vedenjskega oglaševanja na spletu in ga tako opisuje kot oglaševanje, ki temelji na aktivnostih spletnega uporabnika prek različnih spletnih strani v nekem obdobju, ki oglaševalcu omogoča, da uporabniku prikaže oglase, ki bolj ustrezajo njegovim interesom (EASA, 2018). Če uporabnik obišče več spletnih strani o avtomobilizmu,

[1] Izraz novi mediji bo vključeval sodobne elektronske komunikacijske tehnologije in storitve na različnih platformah: ponudnike spletnih medijev, storitev, spletnih družbenih omrežij, digitalno televizijo, mobilne komunikacije itd. Kot soznačnici sta uporabljena tudi izraza elektronsko komuniciranje in informacijske tehnologije.

[2] Izraz vedenjsko oglaševanje je preveden iz angleškega *behavioural advertising*. Kljub uporabi različnih angleških izrazov (*targeting, re-targeting, behavioural marketing*) se na ravni EU in ZDA v okviru zakonodajnih dokumentov in praks največ uporablja besedna zveza *online behavioural advertising*.

oglaševalska mreža lahko domneva, da ga zanimajo avtomobili in prikazuje oglase o avtomobilih le tistim uporabnikom spleta, ki naj bi bili zainteresirani za avtomobile (Boerman, Kruikemeier in Zuiderveen Borgesius, 2017).

S pomočjo vedenjskega oglaševanja naj bi oglaševalska industrija izgubljala manj denarja na nerelevantnih trgih (Goldfarb in Tucker, 2010), podatki uporabnikov interneta pa so čedalje vrednejše blago, tudi za ceno posega v njihove temeljne pravice do zasebnosti in nediskriminacije ter politične pravice. Vedenjsko oglaševanje, katerega posebnost je podrobno profiliranje posameznikov, se v zadnjih letih čedalje bolj uporablja tudi na področju poličnega trženja, zaradi česar vzbuja številne pomisleke glede njihove zasebnosti (McDonald in Cranor, 2009; McStay, 2011) in odpira širša vprašanja poslovne etike (Carsten Stahl, 2008), družbene odgovornosti korporacij (Pollach, 2011), vplivov osebne prilagoditve vsebin na družbo (Pariser, 2011) in na politične oziroma demokratične procese. Teoretičnih prispevkov na temo ni veliko, čeprav se v zadnjih letih njihovo število in raznolikost povečuje, vendar pa redki ta pojav obravnavajo celostno. Običajno so namreč osredinjeni na ožje vidike problematike, bodisi tehnične bodisi pravne ali regulativne, manj pa teoretsko utemeljene (npr. Evans, 2009; Battelle, 2010; Pariser, 2011; McDonalds in Cranor, 2010; Goldfarb in Tucker, 2010a; Tucker, 2011; Freudiger, Vratonjic in Hubaux, 2009; posebej pomembni so prispevki Zuiderveen Borgesius, 2014, 2016, 2012; Castelluccia, 2012; Kamara in Kosta, 2016; Busch, 2016; itd.).

Vedenjsko oglaševanje je bistvo najuspešnejših poslovnih modelov današnjega časa in eden redkih načinov, kako brezplačno storitev na spletu spremeniti v donosno. V zadnjih letih je čedalje bolj poudarjena tudi vloga vedenjskega profiliranja za namen političnega trženja ter promocije političnih kandidatov in pogledov, kar razstira nove razsežnosti vprašanj glede vpliva na demokratične procese v družbi. Kritično raziskovanje tega pojava je nujno, tako v smislu prispevka k teoriji tržnega komuniciranja kot tudi v širšem okviru družboslovnih znanosti, da se zapolni pomanjkanje na področju teoretsko utemeljenih virov. Disertacija ponuja okvir za raziskovanje, ki gradi na pristopu kombiniranja različnih teorij, in obravnava vedenjsko oglaševanje pri različnih storitvah elektronskih komunikacij, prek različnih naprav in na različnih tehnoloških ravneh. Hkrati ugotavlja prednosti, ki jih prinaša različnim deležnikom – oglaševalcem, oglaševalski panogi in založnikom, zlasti medijem ter posameznikom. Odkriva tudi negativne plati in posledice, ki jih ima za pravice in interese

posameznikov, za deležnike v celotnem vedenjskooglaševalskem ekosistemu, družbo in demokratične procese. Razišče trenuten okvir regulacije v EU in ZDA, kar zajema zakonodajo, samoregulacijo ter tudi standardizacijske aktivnosti, in predlaga okvir za boljšo regulacijo vedenjskega oglaševanja v prihodnosti – tak, ki bo bolje pretehtal različne interese in bo učinkoviteje omejil negativne posledice s podatkovnimi analizami okrepljenih marketinških strategij. Vedenjsko oglaševanje je raziskano s kombinacijo več metod, in sicer sta sočasno uporabljeni dve kvalitativni metodi, pri čemer je ena od njiju prevladujoča, druga pa rezultate dopolnjuje. Opravljena je bila obširna analiza vsebine dokumentov ter ekspertni intervjuji s strokovnjaki z različnih področij, povezanih s temo raziskave.

Vedenjsko oglaševanje temelji na sledenju aktivnostim uporabnika elektronskih komunikacijskih tehnologij, ki so mu nato glede na analizo podatkov o njegovih aktivnostih prikazani le zanj relevantni oglasi, lahko pa tudi druge vsebine (McDonald in Cranor, 2010; McStay, 2011). Izvajajo ga ponudniki storitev na različnih tehnoloških ravneh elektronskega komuniciranja: ponudniki vsebin, storitev, aplikacij in iskanja (omenimo le nekaj največjih, kot so Google, Microsoft, Yahoo!, Facebook, Amazon, eBay, AOL itd.),[3] lahko ga implementirajo ponudniki dostopa do interneta, lahko je uporabljeno na platformi digitalne televizije (Burke, 2003; Fair, 2017) in napravah v okviru interneta stvari. Namenjen je lahko trženju produktov, storitev, pa tudi širjenju sporočil političnih kandidatov in vplivu na volivce glede na njihove značilnosti. Vedenjsko oglaševanje je bilo posebej poudarjeno pri njegovem uvajanju na ravni ponudnika dostopa do interneta,[4] in sicer zaradi položaja ponudnika, ki mu dovoljuje zajem podatkov o prav vseh aktivnostih uporabnika na internetu[5] (FTC, 2007; NAI, 2008; OFCOM, 2008) ter v zadnjem času ob uporabi za namene politične promocije v okviru kampanje za Brexit in predsedniške volitve v ZDA leta 2016 (Cambridge Analytica in Facebook).

[3] Vedenjsko oglaševanje lahko zajema le beleženje aktivnosti uporabnikov znotraj nekega ponudnika (je npr. omejeno zgolj na to, kaj uporabnik počne znotraj omrežja Facebook) ali pa se beležijo njihove aktivnosti na različnih, nepovezanih spletnih straneh (kot to izvaja Google ali kot lahko izvajajo operaterji omrežja).

[4] Okoli leta 2007 so se začeli sporni poskusi v ZDA (podjetje NebuAd) in v Veliki Britaniji (podjetje Phorm). Sistem ponudnika Phorm v Veliki Britaniji je na podlagi aktivnosti uporabnika na spletu (obiskane strani, iskalni termini) identificiral njegova zanimanja in mu dodelil določene oglase. Uporabnike je med seboj ločeval le po unikatnih identifikatorjih (ICO, 2008;) zaradi česar naj bila obdelava podatkov anonimizirana in tako ne v nasprotju s pravili o varstvu osebnih podatkov (Home Office, 2008; ICO, 2008; 20/80 Thinking, 2008). Ker so bili poskusi tehnologije izvedeni brez vednosti in privolitve uporabnikov je Evropska komisija proti Veliki Britaniji sprožila postopek zaradi kršitve (Evropska komisija, 2009a, 2009b).

[5] Vpogled v podatke, ki se pretakajo prek omrežne opreme ponudnika internetnih storitev, je mogoč s tehnologijo *deep packet inspection*.

Vedenjsko oglaševanje vključuje rabo sledilnih tehnologij, piškotkov in drugih, ki jih izvajalec shrani na terminalni opremi uporabnika. Piškotki vsebujejo unikatni identifikator, po katerem je mogoče posameznega uporabnika prepoznavati pri različnih aktivnostih na spletu. V zadnjih letih se čedalje bolj uporabljajo tudi druge sledilne tehnologije, kot so npr. *flash* piškotki oziroma lokalno deljeni objekti (angl. *locally shared objects*), piksli (svetilniki), ki jih uporabnik z običajnimi orodji v brskalniku ne zazna, prav tako pa jih tam ne more izbrisati. Čedalje več se uporablja tudi sledenje na podlagi odtisa brskalnika ali naprave, kjer izvajalec vedenjskega oglaševanja uporabnika prepoznava na podlagi edinstvenih parametrov njegovega brskalnika ali naprave (jezik, ločljivost grafike ipd.). Tako sledenje je še posebej težko odkriti ali ga preprečiti. Na mobilnih napravah pa se uporablja sledenje na podlagi identifikacijske oznake naprave (Tene in Polonetsky, 2012).

Ker oglaševanje pomembno podpira razmeroma brezplačno vsebino na internetu, kar najbolj koristi prav uporabnikom, je razvoj natančnejšega, vedenjskega ciljanja običajno označen kot velik napredek, in sicer za oglaševalce in uporabnike, ki so jim na voljo zanje relevantne vsebine. Argument za implementacijo na ravni ponudnikov dostopa do interneta so nova sredstva (poleg naročnin), ki jih operaterji potrebujejo za zagotavljanje univerzalnega dostopa in kakovostne storitve (OFCOM, 2008; LSE, 2009b). Kritika vedenjskega ciljanja poudarja predvsem pomisleke glede prestrezanja komuniciranja, kršitve načela nevtralnosti omrežja[6] ter posega v zasebnost in varstvo osebnih podatkov posameznikov. Ena glavnih težav vedenjskega ciljanja je njegova prikritost, ki dovoljuje vpogled v uporabnikove zasebne aktivnosti (McDonald in Cranor, 2010). Z napredkom tehnološke izvedbe vedenjskega oglaševanja v zadnjih nekaj letih v t. i. programatično oglaševanje[7] in porastom industrije preprodajalcev podatkov pa se pojavlja tudi čedalje več skrbi glede trgovanja z uporabniškimi profili v realnem času, seveda večinoma uporabniku prikritem in netransparentnih tokov uporabniških podatkov med velikim številom povezanih oglaševalskih posrednikov in ponudnikov na trgu, kar povečuje možnosti zlorab podatkov, uporabo za drugačne namene in

[6] Načelo nevtralnosti omrežja je načelo, da vsa vsebina po komunikacijskem omrežju potuje brez diskriminiranja. Tako se je internet zgodovinsko razvijal kot odprta platforma, na kateri naj bi lahko enakovredno sodeloval vsak. Z razvojem številnih storitev informacijske družbe in čedalje večjimi potrebami po zmogljivostih omrežja ter učinkovitem upravljanju omrežij so se pojavile ideje po prednostni obravnavi posamezne vrste prometa v omrežju, na podlagi česar bi operaterji omrežij lahko učinkoviteje upravljali omrežje ter si zagotovili nove vire dohodkov. Vprašanje sprejemljivosti uvajanja prednostne obravnava posamezne vrste podatkovnega prometa s stališča načela nevtralnosti omrežja je trenutno na dnevnem redu v EU in širše, kjer se pojavljajo tudi težnje k vključitvi načela v zakonodajo. Pri raziskovanju potenciala vedenjskega oglaševanja za operaterje omrežij se tako ne moremo izogniti vprašanju vpliva na nevtralnost omrežja, na načelo, ki je vodilo razvoj interneta.

[7] Programatično oglaševanje je avtomatizirano vedenjsko oglaševanje, ki deluje na temelju dražb uporabniških profilov v realnem času.

slabo zavarovanje takih podatkov (Datatilsynet, 2015; Crain, 2016). Pri uporabi vedenjskega oglaševanja v okviru političnih kampanj se pojavljajo tudi širše skrbi vpliva na pravice posameznikov do obveščenosti in s tem povezane medijske pluralnosti ter pravice do svobodnih volitev, bistva demokratičnih procesov v družbi.

Pravno ozadje za regulacijo vedenjskega oglaševanja je danes raznoliko in razmeroma neučinkovito pri varovanju pred negativnimi posledicami. V EU temelji na zakonodaji, ki določa tudi dolžnosti razkritja informacij. Področje je trenutno urejeno z Direktivo 2002/58/ES o zasebnosti in elektronskih komunikacijah (v nadaljevanju Direktiva 2002/58/ES, tudi ePD) [8] in Splošno uredbo 2016/679 o varstvu osebnih podatkov[9] (v nadaljevanju Uredba 2016/679) (WP29, 2010a; Kroes 2010), ki primarno določata, da bi morala industrija pred sledenjem s piškotki ali drugimi tehnologijami uporabnike jasno obvestiti in pridobiti njihovo vnaprejšnjo privolitev (WP29, 2010a). Industrija v EU nasprotuje urejanju področja po načelu predhodne privolitve in se zavzema za ureditev področja s kodeksom samoregulacije, po kateri bi bil standard naknadna zavrnitev vedenjskega oglaševanja (Kroes, 2010; EASA, 2011; IAB Europe, 2010b; WP29, 2011). Delovanje v skladu s kodeksom samoregulacije, ki zahteva le omogočanje zavrnitve vedenjskega oglaševanja, tako trenutno ne pomeni tudi delovanja, skladnega z zakonodajo, saj ta določa višje pogoje – vnaprejšnjo privolitev posameznika (Ryan, 2018). V ZDA je pravni okvir glede informacijske zasebnosti razdrobljen, saj ni zakonodaje o temeljnih pravilih za obdelavo osebnih podatkov, le glede dolžnosti razkritja in zavajajočih praksah. Pomembni so tudi elementi samoregulacije. Tako na industrijskem kodeksu temelji večina podrobnejših pravil za vedenjsko oglaševanje (Department of Commerce, 2010a; FTC, 2007; NAI, 2008), katere temelj je načelo naknadne zavrnitve (Council of Better Business Bureaus, 2010a, 2010b). Čeprav samoregulacija ne dosega ciljev večje transparentnosti oglaševanja (FTC, 2010; Department of Commerce, 2010b), so doslej vse pobude za vzpostavitev zvezne zakonodaje na področju varovanja zasebnosti uporabnikov elektronskih storitev v ZDA klavrno propadle (Singer, 2016).

[8] Direktiva 2009/136/ES Evropskega parlamenta in sveta z dne 25. novembra 2009 o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov.

[9] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES.

Odpirajo se možnosti na področju certificiranja in standardizacije: standard »ne sledi« je pravzaprav dokončan, viri pa se vlagajo tudi v standardizacijo področja vgrajene zasebnosti. Standard ne sledi obeta prvo globalno orodje za zaščito uporabnikov, obstajajo pa različne možnosti njegove implementacije – kot rešitev vnaprejšnje privolitve sledenju (angl. *opt-in*) ali naknadne zavrnitve sledenja (angl. *opt-out*), hkrati pa ga industrija (še) ne uporablja (Zuiderveen Borgesius in McDonald, 2015; W3C, 2017).

Zaradi različnih pristopov k regulaciji vedenjskega oglaševanja, ki so večinoma še na ravni pogajanj, je na tem področju veliko trenja (Goldfarb in Tucker, 2010). Eno glavnih vprašanj je privolitev posameznika v sledenje in vedenjsko ciljanje. Industrija večinoma deluje po načelu naknadne zavrnitve sledenja in ne po načelu vnaprejšnje privolitve oziroma vnaprejšnjo privolitev pridobi na podlagi tihega strinjanja uporabnika s pogoji uporabe storitve, kar se je v praksi pri varstvu pravic posameznikov pokazalo kot neučinkovito (McDonald in Cranor, 2010).

1.2 Namen disertacije in teoretični okvir

Opisani razvoj vedenjskega oglaševanja in poskusov njegove regulacije zaradi vplivov na informacijsko zasebnost posameznikov, pravico do nediskriminacije ter demokratične procese v družbi kaže na množico odprtih vprašanj: kakšne so prednosti vedenjskega oglaševanja, koliko je učinkovito, kam umestiti pomisleke o zasebnosti in drugih pravicah ter interesih posameznikov in družbe.

Namen disertacije je teoretično in empirično raziskati koristi, ki jih vedenjsko oglaševanje prinaša, in ugotoviti, kako učinkovito je njegovo izvajanje na različnih platformah elektronskega komuniciranja, kaj razvoj tehnologij vedenjskega oglaševanja pomeni v okviru razvoja relevantne panoge in kakšne so posledice za preostale deležnike, torej kaj razvoj tehnologij osebne prilagoditve oglasnih vsebin pomeni v okviru razvoja različnih platform, kakšne so posledice za izdajatelje, oglaševalske mreže, ponudnike dostopa do interneta, manjša podjetja, velike multinacionalne korporacije, uporabnike in druge deležnike. Nadalje je namen disertacije raziskati, koliko je vedenjsko oglaševanje invazivno in posega v pravice uporabnikov elektronskih komunikacijskih tehnologij ter koliko so trenutni pristopi k

varovanju informacijske zasebnosti uporabnikov v ZDA in EU uspešni, je zasebnost posameznikov varovana v EU in ZDA, kakšna je vloga zakonodaje, samoregulacije, koregulacije, regulacije s programsko kodo.[10] V zaključku pa je namen disertacije prispevati k oblikovanju okvira za boljšo regulacijo vedenjskega oglaševanja v prihodnosti in opredelitvi vloge različnih orodij regulacije.

Teoretski okvir za celostno razumevanje še ni zgrajen, vendar je nujen za prihodnje izkoriščanje prednosti ciljanja (Goldfarb in Tucker, 2010a, str. 33) in konceptualno domišljene predloge izboljšav za prihodnost. Raznolikost raziskav in akademskih prispevkov na temo vedenjskega oglaševanja se v zadnjih letih veča (npr. Evans, 2009; Pariser, 2011; McDonalds in Cranor, 2010; Freudiger in drugi, 2009; Stallworth, 2010; Tutaj in van Reijmersdal, 2012; Petrescu in Korgaonkar, 2011; Castelluccia in Narayanan, 2012; Zuiderveen Borgesius, 2014; itd.), vendar pa le redki prispevki to problematiko obravnavajo celostno. Širši pogled na problematiko osebne prilagoditve vsebin ponuja Pariser (2011). Ogromne količine informacij, ki jih ne moremo več predelati sami, so botrovale nastanku novih struktur moči, ki na podlagi analize naših želja filtrirajo informacije in jih osebno prilagodijo (najbolj sofisticiran primer je Google), to pa oži polje posameznikovega delovanja, saj so mu vsebine onkraj njegovih zabeleženih preferenc in aktivnosti vse manj dosegljive (Pariser, 2011; Woo, 2006, str. 957). Čedalje več prispevkov osvetljuje področje posega v zasebnost in vprašanja pravnega okvira (Zuiderveen Borgesius, 2016, 2012; Kamara in Kosta, 2016) ter tudi področja programatičnega oglaševanja (Olejnik in drugi, 2013, Tran in drugi 2014; Busch, 2016), hkrati pa le malo prispevkov osvetljuje področje uporabe tehnik vedenjskega oglaševanja za namen političnega trženja (Zuderveen Borgesius in drugi, 2018; Goodman in drugi, 2017).

Umestitev vedenjskega oglaševanja v teoretski okvir ni preprosta naloga, zato teoretski okvir črpa iz različnih šol in pristopov. Mansell (2004) v svojem prispevku k oblikovanju okvirja za raziskovanje novih medijev poudarja, da raziskave novih medijev pretežno temeljijo na sociooloških pristopih, ki medije obravnavajo kot pomemben vidik vsakdanjega življenja, vendar se na splošno ne sprašujejo o vzorcih moči in tako sami po sebi ne nudijo celostne slike o njihovem delovanju. Zato vidi prednost v revitalizaciji teorije politične ekonomije, ki

[10] Angleška besedna zveza *regulation by code* pojasnjuje, da je lahko že arhitektura posamezne rešitve v elektronskem komuniciranju »zakon«, ki določa, kako se neka rešitev lahko uporablja (Lessig, 2006). Povezuje se z idejo tehničnih standardov, vgrajene zasebnosti ipd.

skupaj z znanji nekaterih drugih tradicij prinaša celostni pregled nad novimi mediji (Mansell, 2004, str. 97). Pri raziskovanju novih medijev in pojava vedenjskega oglaševanja tako ni mogoče spregledati študij, katerih fokus je na občinstvu in na načinih, kako so tehnologije in mediji vpeti v vsakodnevno življenje posameznikov (npr. Livingstone, 2002; Silverstone, 1999), kako ti kodirajo in dekodirajo sporočila (Fiske, 1987; Hall, 1974) in kako novi mediji vplivajo na stare odnose moči. Družbeni akterji imajo v novih medijih precejšnjo moč, da izbirajo načine njihove uporabe; uporabnik je lahko hkrati tudi ustvarjalec (Zittrain in Palfrey, 2008; Benkler, 2001). Glavna značilnost, ki vedenjsko oglaševanje razlikuje od drugih vrst oglaševanja, je zbiranje velikih količin podatkov o aktivnostih in preferencah uporabnikov, na podlagi katerih dobi uporabnik sebi prilagojen oglas. Poseg v zasebnost posameznika je torej ključna komponenta vedenjskega oglaševanja. Teoretski okvir raziskave tako nujno potrebuje znanja in uvide, ki jih ponujajo teorije informacijske zasebnosti. Namen disertacije je oblikovanje okvira za regulacijo vedenjskega oglaševanja v prihodnosti. Raziskovanje procesov regulacije oglaševanja in komuniciranja pa vodi prek znanj normativne teorije, ki se sprašuje, kako naj bi mediji delovali, če naj izpolnijo naša pričakovanja glede svojega prispevka družbi in razvoju (McQuail, 2002, str. 16). Normativna teorija poudarja, da so mediji vpeti v naše družbeno, moralno in politično življenje in je zato včasih pri omejevanju njihovega delovanja potreben zunanji poseg. Prav tako je nujen poglobljen uvid v teorije regulacije, ki razkrijejo orodja in strategije, ki so na voljo za prihodnje urejanje tega področja. V iskanje okvirov za prihodnje urejanje elektronskega komuniciranja in novih tehnologij, ki vsebujejo komponente nadzora in posega v zasebnost posameznikov, se v zadnjem času čedalje bolj vpleta pristop družbene odgovornosti (King in Mcdonnell, 2012). Izkušnje kažejo, da zgolj poseg v obliki zunanje regulacije pri sodobnih tehnologijah za varstvo interesov in pravic posameznikov ne zadošča. Pravni okviri vedno zaostajajo za silovitim razvojem tehnologije, ki prinaša čedalje nove etične izzive. Samoregulacija ima slabe plati. Zato je v teoretskih pristopih čedalje več poudarka na različnih orodjih, s katerimi lahko posamezen subjekt oceni potencialne negativne vplive konkretne tehnologije in skuša kot družbeno odgovoren te negativne vplive zmanjšati oziroma obvladati; to so npr. koncept vgrajene zasebnosti (angl. *privacy by design*) ali ocene vplivov na zasebnost in etične standarde (angl. *privacy/ethical impact assessment*) (Carsten Stahl, 2011; Wright in de Hert, 2012).

1.3 Metodologija raziskave

V disertaciji je vedenjsko oglaševanje v elektronskem komuniciranju preučevano s pomočjo kombiniranja različnih teorij ter tako oblikovan multi-teoretski okvir s poudarkom na teorijah informacijske zasebnosti, študijah uporabe medijev v vsakdanjem življenju, politične ekonomije komuniciranja, vedenjske ekonomije, normativne teorije in pristop družbene odgovornosti.

Pregled literature gradi na poglobljenem, kritičnem in sistematičnem pregledu vsebine *dokumentov, sekundarnih virov*, ki zajema novinarske prispevke, raziskave in poročila, objavljene s strani spletne oglaševalske panoge, regulatorjev, nevladnih organizacij, tehničnih strokovnjakov in aktivistov ter bloge mnenjskih voditeljev in strokovnjakov. Analizirane so raziskave o odnosu, stališčih in mnenjih uporabnikov storitev informacijske družbe glede sledenja na spletu, osebne prilagoditve vsebin, posegov v zasebnost in vedenjskega oglaševanja. Predstavljeni so konkretni primeri izvajalcev vedenjskega oglaševanja na različnih tehnoloških ravneh elektronskega komuniciranja in prakse, ki so pomembno zaznamovale razvoj področja v zadnjih nekaj letih: (1) vedenjsko oglaševanje na ravni ponudnika dostopa do interneta: Phorm, (2) programatično oglaševanje in dražbe uporabniških profilov: prevlada Googla in Facebooka, (3) spletna družbena omrežja: Facebook, (4) preprodajalci podatkov – povezovanje *online* in *offline* virov, (5) internet stvari – posameznik je v dosegu 24 ur na dan, (6) vedenjsko ciljanje za namen politične promocije – Cambridge Analytica.

V empiričnem delu je pojav raziskan s kombinacijo več metod, in sicer sta sočasno uporabljeni dve kvalitativni metodi, pri čemer ena od njiju prevladuje, druga pa dopolnjuje rezultate. Opravljena je bila obširna analiza vsebine dokumentov ter ekspertni intervjuji z 19 strokovnjaki z različnih področij, povezanih s temo raziskave. Z uporabo različnih metod in virov podatkov raziskovalec išče povezave in zmanjšuje pristranskost ugotovitev, ki bi temeljile na le enem viru podatkov ali eni metodi raziskovanja (Patton, 1990). Dokumentarna analiza se tako lahko povezuje z drugimi viri podatkov, npr. intervjuji ali osebno udeležbo (Yin, 1994). Hitro spreminjajoče okolje regulacije je raziskano z analizo veljavnih in predlaganih pravnih aktov, evropskih direktiv, smernic in mnenj pristojnih inštitucij, mednarodnih dogovorov, nacionalnih zakonodaj držav članic in kodeksov samoregulacije.

Analiza vsebine dokumentov in pravnih virov pa je zaradi kompleksnosti pojava raziskovanja dopolnjena z metodo ekspertnih intervjujev. Na raziskovalna vprašanja trenutno ni globalno konsistentnih odgovorov. Predstavniki različnih strani, panoge, regulatorjev, tehničnih strokovnjakov in nevladnih organizacij ponujajo različna mnenja. Ekspertni intervjuji so orodje, s katerim lahko ta mnenja in znanja, ki niti z analizo dokumentov niti s kvantitativnimi metodami raziskovanja niso dosegljiva, zajamemo. Intervjuji spraševalcu omogočajo postavljanje dodatnih vprašanj in možnost pridobivanja nepričakovanih informacij (Berger, 1998). Predvsem za odgovor na zadnje, toda glavno raziskovalno vprašanje, po katerem nas zanima pogled v prihodnje modele politik glede vedenjskega oglaševanja, so ekspertni intervjuji zelo pomembni. Le z znanjem in mnenji vrhunskih strokovnjakov s področja, ki zastopajo različne poglede, je mogoče najti odgovor na to vprašanje.

1.4 Izvirnost prispevka disertacije

Izvirnost prispevka disertacije k razvoju znanstvenega področja se kaže v več razsežnostih. Najprej se kaže v postavitvi teoretskega okvira za razumevanje vedenjskega oglaševanja, ki kombinira uvide različnih pristopov, kar je tudi prispevek k teoriji tržnega komuniciranja. Vedenjsko oglaševanje je temelj poslovnih modelov večine danes najbolj priljubljenih storitev v elektronskem komuniciranju – od spletnih družbenih omrežij, mobilnih aplikacij, iskalnikov, zemljevidov, storitev za komunikacijo in sporočanje. Številne storitve so uporabnikom na voljo brezplačno, pri čemer prihodek za ponudnika izvira iz oglaševanja na podlagi podatkov uporabnikov storitve. Te storitve so čedalje bolj neločljivo povezane z vsakdanjimi aktivnostmi posameznikov, čedalje nujnejše so tudi za pomenljivo participacijo v družbenih in demokratičnih procesih (glej npr. McDonalds in Cranor, 2010; Zuiderveen Borgesius, 2016, 2012; Tran in drugi, 2014; Kamara in Kosta, 2016; Taddeo in Floridi, 2016; itd.). Vedenjsko oglaševanje je tako eden ključnih pojavov današnjega sveta, in sicer s kritičnimi posledicami za družbo in demokratične procese, zaradi katerih ga ne bi smeli obravnavati parcialno, npr. le v okviru tržnega komuniciranja, saj s tem spregledamo številne razsežnosti, ki pa so med seboj neločljivo povezane. Izvirni prispevek disertacije se kaže v poskusu identifikacije teoretskih okvirjev, ki lahko služijo kot opora za razumevanje vedenjskega oglaševanja. Disertacija tako kombinira prispevke različnih teoretskih pristopov in sloni na teorijah informacijske zasebnosti (npr. Floridi, 2006), politični ekonomiji komuniciranja (Murdock in Golding, 1997) in teorijah uporabe medijev v vsakdanjem

življenju (Livingstone, 2002) ter internetnih študijah, normativni teoriji in teorijah regulacije (McQuail, 2002), vedenjski ekonomiji (npr. Acquisti, 2014) in pristopu družbene odgovornosti (Nerone, 2002; Pollach, 2011). Izvirnost disertacije se tako kaže v multi-teoretskem pristopu k obravnavi pojava, ki ga v literaturi ni zaslediti.

Ključen izvirni prispevek disertacije je izdelava koherentnega konceptualnega modela za prihodnje urejanje področja vedenjskega oglaševanja. Vedenjsko oglaševanje postaja nepogrešljiv del prevladujočih globalnih poslovnih modelov v elektronskem komuniciranju, uporablja se tudi v okviru poličnega trženja, njegova regulacija pa je tudi eden pomembnih izzivov za prihodnost, na katerega globalno še ni konsistentnega odgovora (WP29, 2010a, 2011; Janet, 2012). Disertacija podaja odgovore na glavne dileme glede ureditve vedenjskega oglaševanja v prihodnosti in ponuja konceptualni model za urejanje tega področja, ki bo utemeljen na iskanju ravnotežja med interesi deležnikov. Kot taka bo lahko disertacija pomagala različnim deležnikom (panogi, regulatorjem, civilni družbi) pri reševanju vprašanja prihodnje ureditve vedenjskega oglaševanja.

Izvirnost disertacije je tudi v uporabi kombinacije več metod empiričnega raziskovanja (angl. multimethod approach). Sočasno sta uporabljeni dve kvalitativni metodi, dokumentarna analiza in ekspertni intervjuji, pri čemer ena od metod prevladuje, druga pa dopolnjuje rezultate (angl. QUAL+qual) (glej npr. Morse, 2003, str. 197). Raziskovana problematika je kompleksna in si jo zato prizadevamo pojasniti z več vidikov, pri čemer izbrani metodi omogočata prav to in hkrati povezovanje ugotovitev, njihovo dopolnjevanje in preverjanje. Relevantna literatura kaže, da so bili za raziskovanje področja uporabljeni nestrukturirani intervjuji (npr. McDonald in Cranor, 2009), anketni vprašalniki (npr. Goldfarb and Tucker, 2010) ter analiza vsebine in diskurzivna analiza (Pollach, 2011). Avtorji, ki opisujejo delovanje panoge, uporabljajo metodo intervjuja informatorjev (npr. Pariser, 2011), tudi tehnične analize toka podatkov in sledenja na spletu (npr. Olejnik in drugi, 2013; Tran in drugi, 2014). V zadnjih letih je čedalje več analiz pravnega okvira in zakonodaje (npr. Zuiderveen Borgesius, 2016, 2012; Kamara in Kosta, 2016). V disertaciji je uporabljena metoda analize dokumentarnega gradiva in analize pravnih virov, torej analiza vsebine. Hkrati je opravljeno več elitnih intervjujev s pripadniki skupin deležnikov (panoge, tehničnih strokovnjakov, regulatorjev, nevladnih organizacij, teoretikov itd.). Na podlagi kombiniranja teh metod je prvič izdelan konceptualni okvir za prihodnje urejanje vedenjskega oglaševanja.

Izvirni prispevek disertacije je tudi v predlogu operacionalizacije modela tehtanja zakonitega interesa za področje vedenjskega oglaševanja. Zakoniti interes je ena od dopustnih pravnih podlag za obdelavo osebnih podatkov v okviru evropske pravne ureditve, ki zahteva tehtanje med interesi upravljavca podatkov in interesi posameznika, ki bi bili lahko z obdelavo njegovih osebnih podatkov prizadeti. Hkrati pa pravni viri ne odgovarjajo na vprašanje, kako naj bi bilo to tehtanje izvedeno, da se zagotovi enovito razumevanje in omogoči nadzor nad procesom tehtanja (Kamara in deHert, 2018). Disertacija ponudi izvirno operacionalizacijo modela tehtanja, povzetega po Kamara in deHert (2018), za kontekst vedenjskega oglaševanja, ki upošteva vidike trga izvajalcev vedenjskega oglaševanja ter izdajateljev in oglaševalcev.

Izvirni prispevek predlagane raziskave se navsezadnje kaže tudi v izvirnosti dela v slovenskem znanstvenem prostoru. Pojav vedenjskega oglaševanja v Sloveniji ni bil specifično raziskan, niti pojasnjen v literaturi s področja tržnega komuniciranja ali širše komunikologije in družbenih ved. Disertacija ponuja prvi vpogled v tematiko na področju Slovenije in prvi celostni pristop do teoretskega pojasnjevanja pojava in izdelave modela za regulacijo v prihodnosti. Disertacija pa prispeva tudi k razvoju slovenskega izrazja na tem področju, ki je večinoma še pomanjkljivo in temelji na angleških izrazih.

1.5 Omejitve dela

Disertacija obravnava vedenjsko oglaševanje pri različnih storitvah elektronskih komunikacij, prek različnih naprav in tehnoloških ravni ter se sprašuje o prihodnjem okviru regulacije. Konceptualni okvir gradi na kombiniranju različnih teorij, ki vsaka posebej in v kombinaciji prispevajo k boljšemu razumevanju različnih podrobnosti in vidikov tega pojava. Večteoretski okvir raziskave je tako po eni strani njena prednost in izvirni prispevek, saj ga v literaturi ne zasledimo, po drugi strani pa kombiniranje različnih teoretskih izhodišč lahko pomeni tudi omejitev, v smislu globine, do katere raziskujemo vedenjsko oglaševanje znotraj posameznega pristopa. Vsekakor bi bilo mogoče v vsakem od teoretskih pristopov, ki smo jih uporabili, raziskovati tematiko še globlje in precej podrobneje, npr. glede pogleda uporabnikov, posameznikov, ki se praksam vedenjskega oglaševanja upirajo, ipd. Vendar ob omejitvah že zdaj precejšnjega obsega disertacije teoretski okvir podaja le bistvene poudarke posameznega pristopa, ki nam lahko pomagajo pri razumevanju vedenjskega oglaševanja. Z

vidika namena celostne obravnave pojava je naš namen namreč zlasti nakazati, katere različne teorije nudijo prispevek za razumevanje (tudi tukaj naš izbor ne pomeni edine mogoče kombinacije) in prikazati povezave med različnimi teorijami. Globlje raziskovanje tematike v posameznem teoretskem pristopu pa ostaja možnost za nadaljnje študije.

Iz ugotovitev disertacije izhajajo neenotne ugotovitve o ekonomski učinkovitosti vedenjskega oglaševanja za različne deležnike, vendar pa velja opozorilo, da študija ni vključevala metod ekonomskih analiz in vsi podatki o učinkovitosti izhajajo iz pregleda literature in subjektivnih pogledov ekspertov na tem področju. Na tem področju so tako potrebne nadaljnje raziskave, ki bi omogočile zanesljivejši vpogled v ekonomsko plat vedenjskega oglaševanja in njegovo učinkovitost v različnih kontekstih, v primerjavi z digitalnim oglaševanjem, ki ne gradi tako široko na analizi podatkov posameznikov in nima tako znatnih negativnih posledic.

Študija je usmerjena predvsem na vidike posega v zasebnosti in varstvo osebnih podatkov ter okvir regulacije na tem področju, čeprav se vpliv vedenjskega oglaševanja razteza tudi na druge pravice in interese ter demokratične procese. Disertacija le ponekod omenja relevantne pomisleke tudi z vidika širših posledic. Iz tega izhaja, da si tematika vsekakor zasluži podrobnejšo znanstveno obravnavo tudi z vidika drugih pravic posameznikov, kot je pravica do enake obravnave in nediskriminacije, pravica do obveščenosti, pravica do svobodnih volitev, ter tudi z vidika posega v demokratične procese, medijski pluralizem in konkurenco na trgu ponudnikov sodobnih elektronskih storitev.

Na področju okvira regulacije za varstvo osebnih podatkov je v zadnjem obdobju prišlo do številnih sprememb, predvsem v EU, s sprejemom Uredbe (EU) 2016/679, ki uvaja nove pojme, kot je npr. promocija certificiranja in samoregulacijskih kodeksov, pa orodja za večjo odgovornost upravljavcev, kot so ocene vplivov na zasebnost in koncept vgrajene zasebnosti ter nove pravice posameznikov, npr. do pozabe in prenosljivosti osebnih podatkov. Vsaka od teh novosti ima lahko v prihodnosti na področju vedenjskega oglaševanja pomembno vlogo, vendar jih v okviru te disertacije ni bilo mogoče podrobneje raziskati. Nadaljnje raziskave na teh področjih so pomembne tudi za prihodnji razvoj zakonodaje v drugih državah, ki se lahko zgledujejo po zakonodajnem okviru EU.

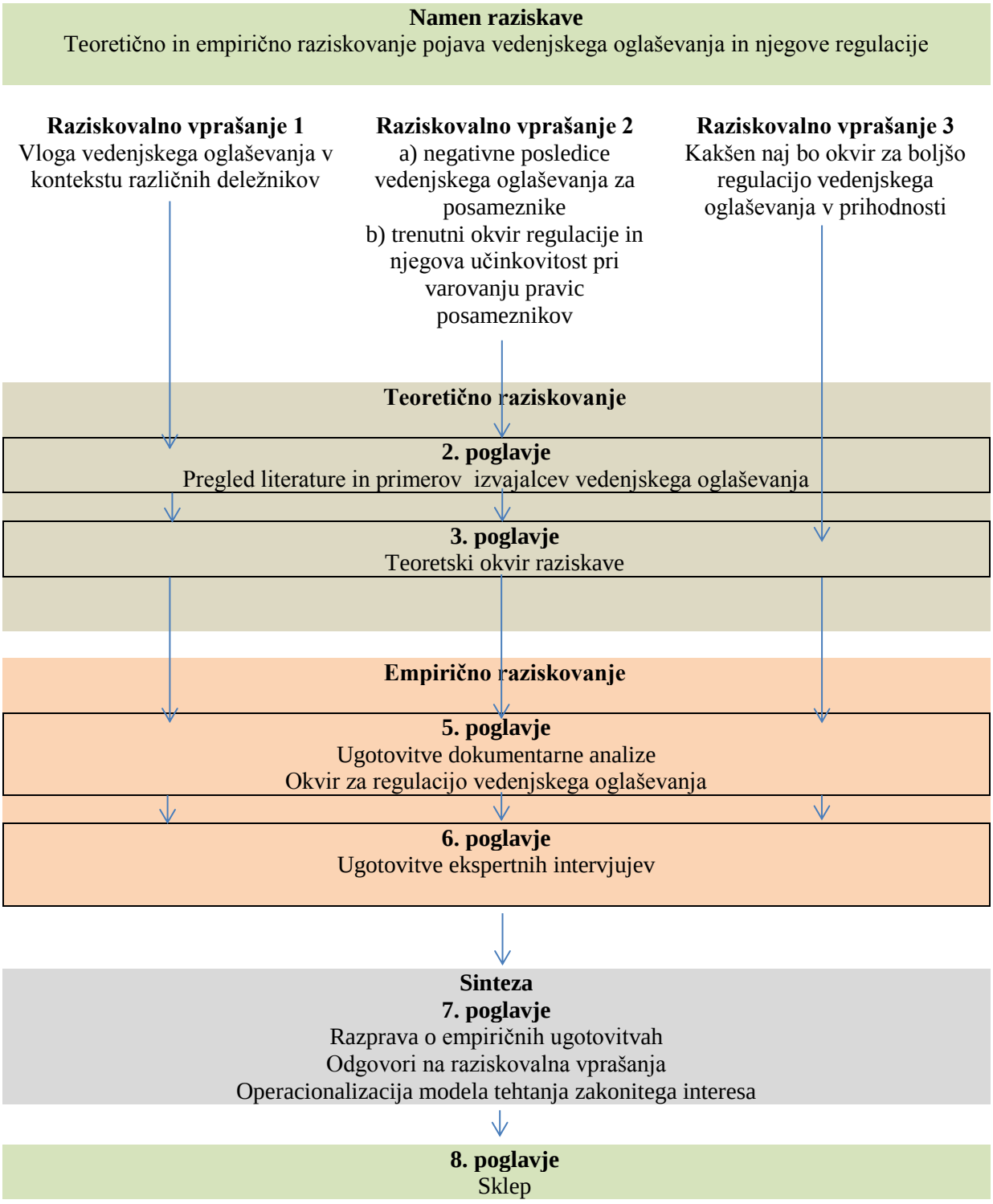
Zadnja omejitev izhaja iz izbrane metode ekspertnih intervjujev v povezavi s položajem raziskovalke, ki prihaja iz nadzornega organa za varstvo osebnih podatkov z dolgoletnimi izkušnjami na tem področju. Gradivo, pridobljeno z ekspertnimi intervjuji, nujno vključuje precej subjektivnih informacij, prav tako je s subjektivnostjo prepletena analiza takih podatkov. Intervjuji so bili primarno uporabljeni za odgovor na vprašanje prihodnje regulacije vedenjskega oglaševanja, ki je nerešeno, tudi politično vprašanje, zato subjektivnost pri odgovorih pravzaprav bogati študijo – pogovori s strokovnjaki odstrejo marsikatero tančico, ki je dokumentarna analiza ne bi mogla, saj so objavljeni dokumenti pogosto očiščeni spornejših izjav in pisani v diplomatskem tonu, iz katerega je lahko težko razbrati nianse. Kljub temu pa strokovnost raziskovalca, podprta z obsežno in globoko analizo dokumentarnih virov ter relevantne zakonodaje, omogoča, da je analiza subjektivnih pogledov na prihodnjo regulacijo še bolj veljavna in objektivna.

1.6 Zgradba disertacije

Drugo poglavje disertacije zajema pregled relevantne literature na temo vedenjskega oglaševanja ter prve poskuse regulacije na tem področju v EU in ZDA. Vsebuje tudi pregled raziskav o odnosu, stališčih in mnenjih uporabnikov storitev informacijske družbe glede vedenjskega oglaševanja ter poglobljen pregled področja vedenjskega oglaševanja na konkretnih primerih izvajalcev vedenjskega oglaševanja na različnih tehnoloških ravneh elektronskega komuniciranja in praksah, ki so pomembno zaznamovale razvoj področja v zadnjih nekaj letih. Tretje poglavje zajema teoretični okvir raziskave, ki temelji na obravnavi pojava z vidika kombiniranja različnih raziskovalnih tradicij: študij o vlogi novih medijev v vsakdanjem življenju, politični ekonomiji, vedenjski ekonomiji, normativni teoriji, teorijah informacijske zasebnosti in pristopu družbene odgovornosti podjetij. Četrto poglavje obsega raziskovalni načrt in pojasnila o uporabljenih metodah empirične raziskave: dokumentarni analizi in ekspertnih intervjujih. V petem poglavju so predstavljeni rezultati dokumentarne analize trenutnega okvira regulacije vedenjskega oglaševanja v EU in ZDA, v šestem pa analiza ekspertnih intervjujev. Ugotovitve so strukturirane glede na tri raziskovalna vprašanja, ki vodijo študijo. Sedmo poglavje zajema razpravo o ugotovitvah empiričnega dela glede na teoretski okvir in odgovore na raziskovalna vprašanja ter model operacionalizacije tehtanja zakonitega interesa za področje vedenjskega oglaševanja. Osmo – sklepno poglavje –

predstavi sklep ter pojasnila o omejitvah raziskave, o predlogih za nadaljnje raziskave in o prispevkih disertacije za prakso (Slika 1.1).

Slika 1.1: Shematski prikaz sestave disertacije



2 UVOD V PROBLEMATIKO VEDENJSKEGA OGLAŠEVANJA: PREGLED LITERATURE

V nadaljevanju sledi pregled literature s področja vedenjskega oglaševanja ter širše krajine digitalnega oglaševanja. Najprej pojasnimo kontekst sledenja posameznikom pri njihovi uporabi elektronskih komunikacij. Nato pozornost namenimo razvoju vedenjskega oglaševanja v obliki avtomatiziranega programatičnega digitalnega oglaševanja, ki trenutno prevladuje na trgu, in predstavimo poglobljen vpogled v šest konkretnih primerov izvajanja vedenjskega oglaševanja na različnih tehnoloških ravneh. Posvetimo se posledicam teh praks za posameznikove pravice in družbo. Nato je predstavljen vidik posameznikov in njihovega odnosa do osebne prilagoditve vsebin, sledenja na spletu in vedenjskega oglaševanja. Poglavje se sklene s kratkim očrtom pravnega ozadja in prvih poskusov regulacije tega kompleksnega področja.

Vedenjsko oglaševanje glede na definicije različnih avtorjev običajno pomeni oglaševanje, ki temelji na beleženju aktivnosti posameznikov na spletu in pri uporabi mobilnih naprav (obiskane spletne strani, podatki, ki jih uporabnik vnese ob registraciji na posamezno spletno stran, vsebina, do katere dostopa, podatki o uporabi aplikacij itd.) ter grajenju njihovih profilov, ki temeljijo na hranjenih in analiziranih podatkih. Posamezniku je nato prikazan le oglas, ki je relevanten glede na njegov profil in aktivnosti (glej npr. Zuiderveen Borgesius, 2014; Kamara in Kosta, 2016; idr.). V zadnjem desetletju so ga pospešeno začeli izvajati ponudniki storitev na različnih tehnoloških ravneh v elektronskih komunikacijah: na aplikativni ravni (ponudniki vsebin, novičarski portali, spletne trgovine, spletna družbena omrežja), na ravni iskanja (spletni iskalniki) ter tudi na ravni povezljivosti (ponudniki dostopa do interneta oz. operaterji omrežja), pojavljajo se implementacije na platformi digitalne televizije in drugih naprav interneta stvari. Namen vseh teh aktivnosti je grajenje čim natančnejših uporabniških profilov, ki so uporabljeni za čim boljše predvidevanje njihovih potencialnih interesov in želja ter tako čim učinkovitejše ciljanje z osebno prilagojenimi oglasi, tudi glede na lokacijo uporabnika, praktično v realnem času (Zuiderveen Borgesius, 2016, 2012).

Boerman, Kruikemeier in Zuiderveen Borgesius (2017) poudarjajo, da imajo definicije vedenjskega oglaševanja na spletu običajno dve skupni značilnosti: (1) sledenje in spremljanje

potrošnikovega vedenja pri uporabi spleta in (2) uporabo zbranih podatkov za individualno ciljanje oglasov. Definicija, ki jo izpeljejo, tako poudarja, da je vedenjsko oglaševanje na spletu praksa spremljanja vedenja posameznikov na spletu in uporabe zbranih podatkov za prikazovanje individualno ciljanih oglasov posameznikom. Vedenje posameznikov na spletu vključuje njihovo brskanje po spletnih straneh, zgodovino iskanj, podatke o uporabi medijev (npr. ogledanih videoposnetkih), podatke o uporabi aplikacij, nakupih, odzivnosti na oglase in komunikacijske podatke, npr. vsebino e-pošte ali objave na spletnih družbenih omrežjih (Zuiderveen Borgesius, 2015a; Boerman, Kruikemeier in Zuiderveen Borgesius, 2017).

Kot kažejo nadaljnja poglavja pa vedenjsko oglaševanje ni omejeno le na področje uporabe spleta in spletnih aplikacij, temveč so širše tako prakse spremljanja posameznikovega vedenja kot tudi prakse prikazovanja oglasov, individualno prilagojenih posameznemu uporabniku, glede na sklepanja o njegovih interesih. Izvajalci vedenjskega oglaševanja lahko spremljajo vedenje posameznika na spletu (Boerman, Kruikemeier in Zuiderveen Borgesius, 2017), pri uporabi mobilnih naprav in aplikacij, pri uporabi naprav interneta stvari, ki delujejo kot podatkovne točke (npr. Busch, 2016), ter podatke iz elektronski sredstev komuniciranja kombinirajo s podatki, pridobljenimi iz realnega sveta (npr. o gibanju posameznika na podlagi beleženja njegove geolokacije, nakupih s kartico ugodnosti, podatki, ki jih o svojih podpornikih vodijo politične stranke ipd.) (npr. FTC, 2014; ICO, 2018a in 2018b). Tudi prikazovanje oglasov posamezniku glede na njegove zabeležene in pričakovane interese se ne dogaja nujno na spletu, na spletnih straneh, ampak so oglasi lahko dostavljeni tudi prek naprav interneta stvari in mobilnih naprav (Aksu in drugi, 2016). Obstoječe definicije spletnega vedenjskega oglaševanja se tako kažejo kot preozke glede na stalno razvijajoče prakse vključevanja novih načinov spremljanja aktivnosti posameznika na spletu, pri uporabi elektronskih naprav in v realnem življenju, na podlagi katerih je izdelan posameznikov profil in so mu prikazani relevantni oglasi.

Osebno prilagojene vsebine in digitalno trženje ena-na-ena naj bi bile za uporabnike pozitivne, saj jim pomagajo najti vsebine glede na njihove navade (Kamara in Kosta, 2016, str. 1). Če profil za posameznega uporabnika pravi, da ima rad suši, bi mu lahko japonska restavracija lahko poslala oglas na njegovo mobilno napravo, ko bi bil v njeni bližini. V realnem svetu je spletno sledenje primerljivo s tem, da bi posamezniku nekdo sledil skozi

nakupovalni center, si zabeležil vsako stran knjige ali revije, ki jo ta bere, vsako vrstico menija v restavraciji (Zuiderveen Borgesius, 2016, str. 258).

V zadnjih letih spremljamo širjenje možnosti in orodij za slednje uporabnikom na spletu in pa tudi v fizičnem svetu, in sicer s slednjem mobilnim napravam in geolokacijam uporabnikov, ter tudi odpiranje novih možnosti kombiniranja podatkov s spleta z drugimi viri, ki vključujejo panogo podjetij, specializiranih za pridobivanje in preprodajanje podatkov o uporabnikih, ter spletne dražbe uporabniških profilov (Castelluccia in Narayanan, 2012; FTC, 2014). Hkrati je viden tudi prehod aktivnosti vedenjskega oglaševanja na področje političnega trženja. Slednje uporabnikovim aktivnostim na spletu omogoča njihovo razvrščanje v skupine glede na politično pripadnost in ciljanje političnih sporočil segmentom, pri katerih je mogoče vplivati na njihovo volilno izbiro (Cadwalladr, 2017).

2.1 Vedenjsko oglaševanje in sledenje uporabnikom

Vedenjsko oglaševanje vključuje zbiranje podatkov o uporabnikih in temelji na uporabi sledilnih tehnologij, najbolj običajno piškotkov, ki jih izvajalec (najpogosteje oglaševalska mreža ali druga oglaševalska platforma) shrani na terminalni opremi uporabnika,[11] lahko pa so to tudi stalni piškotki (angl. *flash/persistent cookies*), spletni svetilniki, sledenje na podlagi identifikatorja naprave (npr. mobilnega telefona), tudi geolokacije telefona ali pa sledenje na podlagi prstnega odtisa naprave. Piškotki nosijo unikatni identifikator, po katerem je mogoče točno določenega uporabnika prepoznavati pri različnih aktivnostih na spletu, in imajo različne roke trajanja, lahko neomejene, kar vodi v akumulacijo velike količine podatkov o uporabnikih in zbuja vprašanja o njihovi zasebnosti ter varstvu osebnih podatkov. Prav tako je prstni odtis naprave unikatni identifikator, prek katerega je mogoče uporabnika prepoznati med brskanjem po spletu (Tene in Polonetsky, 2012), saj pomeni skupek lastnosti sistema, npr. nastavitev operacijskega sistema, jezika, brskalnika itd., ki ima pri vsaki napravi različno kombinacijo vrednosti in je zato z visoko verjetnostjo unikaten (Zuiderveen Borgesius, 2016, str. 258).

Piškotki HTTP so majhne datoteke, ki se naložijo na uporabnikovo napravo in omogočajo, da spletna stran, ki piškotek postavi, ob vnovičnem obisku istega uporabnika prepozna. Osnovne rabe piškotkov so bile torej namenjene temu, da si spletne strani zapomnijo uporabnikove

[11] Kadar piškotek shrani oglaševalska mreža in ne stran, ki jo je uporabnik dejansko obiskal, gre za piškotek tretje strani.

nastavitve jezika, vsebino nakupovalne košarice itd. Piškotek lahko vedno prebere le stran, ki ga je postavila. Obstajajo sejni in stalni piškotki. Sejni pretečejo takoj ob koncu seje brskalnika, trajanje stalnih piškotkov pa je lahko poljubno nastavljeno. Ti so predvsem uporabljeni za to, da uporabnika identificirajo ali omogočajo shranjevanje uporabnikov preferenc ter omogočajo sledenje uporabnikom prek različnih spletnih strani. Piškotki dejansko obiskane spletne strani so piškotki prve strani (angl. *first party cookie*), piškotki, ki jih nalagajo domene, ki jih uporabnik ni dejansko obiskal, pa so piškotki tretjih strani (angl. *third party cookie*), običajno sledilne narave, uporabljene za namen oglaševanja, analitičnih storitev, spletnih družbenih medijev (Tene in Polonetsky, 2012).

Uporabnikom je prek spleta mogoče slediti tudi brez uporabe piškotkov ali podobnih tehnologij. Čedalje bolj se namreč razvija sledenje po prstnem odtisu naprave (angl. *device fingerprinting*) oz. brskalnika (angl. *browser fingerprinting*), pri katerem na uporabnikovo napravo ni naložena nobena datoteka, temveč sledilec uporabnika prepozna in mu sledi na podlagi edinstvene kombinacije različnih informacij, ki jih ta naprava (računalnik, telefon, tablica, igralna konzola, pametni televizijski sprejemnik) oddaja med brskanjem po spletu. To so lahko npr. informacije o nastavitvah naprave, operacijskem sistemu in brskalniku, naslovu IP, informacije o nastavitvah ure, nameščenih pisavah, nastavitvah JavaScript, informacije o vtičnikih ipd. Na podlagi skupka teh informacij je mogoče točno določeno napravo in s tem tudi njenega uporabnika, prepoznati ter podatke uporabiti za namen izdelave analitike, ciljno oglaševanje ipd. (WP29, 2014b; Castelluccia in Narayanan, 2012).

Vplivi na zasebnost in varstvo osebnih podatkov so pri sledenju na podlagi prstnega odtisa naprave daljnosežni, saj se uporabnik takemu sledenju praktično ne more izogniti, zlasti v času razvoja interneta stvari, kjer bo vse več naprav povezanih na internetno omrežje (pametni števci, bela tehnika ipd). Informacij o napravi in njenih konfiguracijah namreč ni mogoče preprosto spreminjati ali preprečiti njihovega spremljanja (WP29, 2014b).

2.2 Razvoj vedenjskega oglaševanja: proti avtomatizaciji procesov, povezovanju podatkov iz različnih virov in distribuciji oglasov prek različnih kanalov

Oglaševalska panoga v spletno oglaševanje vlaga čedalje več, zato je pričakovana nadaljnja rast. Digitalno oglaševanje naj bi leta 2017 celo prehitelo doslej nesporno vodilno televizijsko

oglaševanje (Slefo, 2017). Vedenjsko ciljanje se je začelo razvijati po letu 1990 in se je v zadnjih letih razcvetelo (McStay, 2011), najprej na spletu.

V najpreprostejši obliki vedenjsko oglaševanje na spletu vključuje naslednje akterje: izdajatelje (lastniki spletnih strani, npr. novičarki portali, spletne trgovine itd.), ki oddajajo prostor za oglase, oglaševalske mreže, in druge oglaševalske posrednike, ki distribuirajo oglase različnim izdajateljem glede na pridobljene in analizirane podatke uporabnikov ter oglaševalce (npr. proizvajalce avtomobilov, hotelske verige, trgovci), ki želijo s svojimi oglasi ciljati na zelo specifičen del uporabnikov (LSE, 2009b; WP29, 2010a). Če uporabnik klikne na prikazan oglas (pri modelu cene-na-klik), oglaševalska mreža dobi plačilo oglaševalca tistega oglasa in plača delež izdajatelju, ki je omogočil prikaz oglasa. Oglaševalski mreži je tako v interesu oblikovati čim boljše profile uporabnikov, da se poveča možnost, da bodo kliknili na dostavljen oglas (angl. *click-through rate*) in bodo prihodki višji (Castelluccia in Narayanan, 2012, str. 4).

Spletno vedenjsko oglaševanje lahko zajema beleženje aktivnosti uporabnikov spleta (ne glede na napravo, ki jo uporabljajo za brskanje, bodisi računalnik ali mobilno napravo) zgolj znotraj nekega ponudnika storitve (je npr. omejeno zgolj na to, kaj uporabnik počne znotraj omrežja Facebook) in pomeni sledenje prvi stranki (angl. *first party tracking*). Tak ponudnik sledi uporabniku zato, da mu lahko predlaga produkte iz svoje ponudbe (npr. spletni trgovci), da oblikuje svojo ponudbo glede na njegovo lokacijo (npr. pri sledenju prek aplikacij na mobilnih telefonih) (Castelluccia in Narayanan, 2012, str. 4).

Lahko pa se beležijo uporabnikove aktivnosti na različnih, nepovezanih spletnih straneh, na katerih aktivnosti beležijo tretje stranke (angl. *third party tracking*), npr. oglaševalske mreže pa tudi nekateri ponudniki, ki so hkrati prve in tretje stranke (npr. Facebook, ki prek vtičnikov »všeč mi je« sledi uporabnikom tudi na nepovezanih spletnih straneh, ki imajo nameščen vtičnik). Pogostost sledenja s strani tretjih strank raste iz leta v leto in obsega večino obstoječih spletnih strani, kar pomeni, da se mu pravzaprav ni mogoče izogniti. Poleg tega raziskave kažejo, da dva najmočnejša ponudnika (Google in Facebook) sledita uporabnikom prek večine spletnih strani (Castelluccia in Narayanan, 2012). Kot ugotavljata Engelhardt in Narayanan (2016) v študiji, ki je obsegala pregled milijona spletni strani, te vsebujejo veliko število piškotkov tretjih strank, vendar pa večina teh pripada le majhnemu številu največjih

sledilcev na spletu, to so Google, Facebook, Twitter in Adnexus. Google je npr. prisoten na več kot 80 odstotkov najbolj priljubljenih spletnih strani, Facebook pa na več kot 30 odstotkih (Engelhardt in Narayanan, 2016: 8). Ugotavljata tudi, da je največ sledilcev na novičarskih spletnih straneh in najmanj na straneh javnega sektorja, univerz in nevladnih organizacij, po vsej verjetnosti zaradi drugačnega načina financiranja (Engelhardt in Narayanan, 2016, str. 10). Študije tudi kažejo, da 85 odstotkov tretjih strank med seboj primerja piškotke (angl. *cookie synching*),[12] kar pomeni, da tako potencialno pridobijo tudi podatke drugih sledilcev, kar poseg v zasebnost uporabnikov še poveča (Narayanan in Reisman, 2017, str. 13).

V zadnjih letih se vedenjsko oglaševanje razvija v smer čedalje večje avtomatizacije, v t. i. programatično oglaševanje, za katerega je značilna tudi diverzifikacija ponudnikov, ki so specializirani za naloge, povezane z analizo podatkov za oglaševanje in ciljanje sporočil ter preprodajo teh podatkov. Gre za t. i. *ad tech* panogo (npr. Busch, 2016). Kljub občutku anonimnosti, ki ga imajo uporabniki na spletu, vsak njihov klik, iskanje, povezavo in ogled strani poleg dejansko obiskane strani beleži, shrani, analizira in uporabi cela paleta tretjih strank – oglaševalci in številni oglaševalski posredniki, kot so oglaševalske mreže, platforme za izmenjavo oglasov, ponudniki analitike, tržnih raziskav in ponovnega trženja (angl. *re-targeting*, tudi *re-marketing*) (Tene in Polonetsky, 2012, str. 6). Deljenje podatkov med vsemi ponudniki storitev v tem ekosistemu je zato zelo kompleksno (Zuiderveen Borgesius, 2016).

Vedenjsko oglaševanje, bolj ali manj avtomatizirano, se uporablja na različnih tehnoloških platformah, ne le na spletnih straneh in pri spletnih storitvah. Čedalje bolj se širi uporaba na področje interneta stvari. Poleg tega so čedalje bolj poudarjene tendence povezovanja podatkov o tem, kako posameznik uporablja elektronske naprave, s podatki o njegovih aktivnostih v realnem svetu, nakupih v trgovinah in geolokacijah ter uporaba vedenjskega oglaševanja za politične kampanje. Te prakse so predstavljene v nadaljevanju, in sicer v obliki poglobljenega pregleda šestih različnih primerov izvajanja vedenjskega oglaševanja: (1) programatično oglaševanje in dražbe uporabniških profilov, (2) spletna družbena omrežja: Facebook, (3) vedenjsko oglaševanje na ravni ponudnika dostopa do interneta: Phorm, (4) preprodajalci podatkov – povezovanje *online* in *offline* virov, (5) internet stvari – posameznik je v dosegu 24 ur na dan, (6) vedenjsko ciljanje za namen politične promocije: Cambridge Analytica.

[12] Več v Prilogi A.

2.2.1. Programatično oglaševanje in dražbe uporabniških profilov: prevlada Googla in Facebooka

Programatično oglaševanje oz. tudi oglaševanje v realnem času (angl. *real time advertising*) je eden zadnjih inovativnih pristopov v digitalnem oglaševanju, ki temelji na avtomatizaciji oglaševanja, podprti z uporabniškimi podatki. Lahko ga označimo kot nadaljnjo stopnjo »običajnega« vedenjskega oglaševanja na spletu, ki je temeljilo na oglaševalskih mrežah. Pri programatičnem oglaševanju je temu dodana raven kompleksnosti v obliki dodatka različnih subjektov, ki izvajajo naloge s ciljem dostave oglasa pravemu uporabniku, ne le oglaševalskih mrežah, ter nadaljnji razvoj pri avtomatizaciji tega procesa.[13] Bistvene komponente programatičnega oglaševanja so intenzivna uporaba podatkov, tehnologije in umetne inteligence v trženju, s ciljem povečanja njegove učinkovitosti v realnem času (Busch, 2016, str. 3–4). Kot povzema Nesdale (2018), programatično oglaševanje pomeni dostavo digitalnega oglasa pravi osebi ob pravem času na pravem mestu. Bistveno je, da nakup in oddajo oglaševalskega prostora v realnem času vodijo algoritmi v okviru zmogljive strojne in programske opreme, ki omogoča avtomatizacijo nakupa, serviranja oglasa in optimizacije oglasnega prostora prek sistema dražbe. Ta oglaševalcu omogoča, da točno določeni osebi prilagodi določeno sporočilo in poveča svojo zmožnost, da bo prikazan oglas vodil tudi v nakupno vedenje ali drug želeni cilj oglaševalca (Nesdale, 2018).

Zaradi spremenjene ekonomike medijev in oglaševanja v sodobnem času, kjer prevladuje hiter tehnološki razvoj, potrošniki, ki drugače uporabljajo medije in se selijo na mobilne platforme, njihove hipne pozornosti zaradi poplave informacij, ki so jim izpostavljeni, se ustvarja pritisk na trženjske in oglaševalske sisteme, da postanejo učinkovitejši z manjšo porabo virov. Zato je čedalje pomembnejša ponudba, ki je relevantna za potrošnika v specifičnem času, saj bo takrat večja možnost, da bo zbudila njegovo pozornost. Programatični načini oglaševanja s svojo avtomatizacijo in sposobnostjo natančnega ciljanja naj bi ustrezno odgovarjali na te izzive (Busch, 2016, str. 4–5).

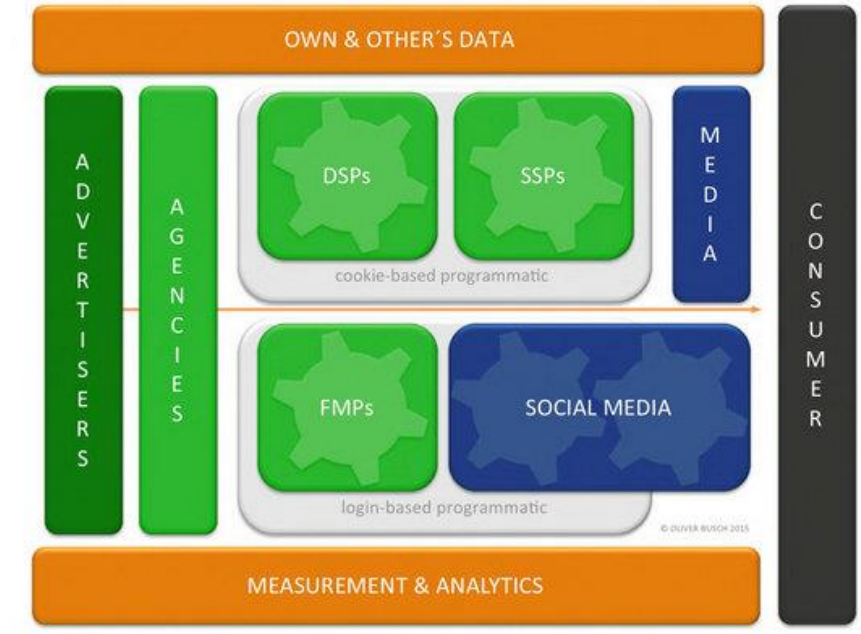
Trg programatičnih oglaševalskih storitev vključuje nove tipe ponudnikov storitev oziroma posrednikov, ki v celotnem sistemu skrbijo za to, da se podatki posameznega uporabnika

[13] Izrazi, s katerimi se označuje dogajanje v okviru programatičnega oglaševanja, so tudi analiza velikega podatkovja in podatkovno pojavno oglaševanje, strojno učenje in algoritmično predvidevanje za analizo empiričnih podatkov, programatični nakup in avtomatizirano menjavanje (angl. *trading*), dražbe v realnem času (angl. *real time bidding*) za dinamično postavljanje cen v realnem času (Busch, 2016, str. 3–4).

posredujejo potencialnim oglaševalcem, ki lahko nato glede na svoje želje ali pretekle izkušnje prav določnemu uporabniku prikažejo oglas, za katerega menijo, da ga bo zanimal. To so npr. platforme za izmenjavo oglasov (angl. *ad exchange*), podjetja, specializirana za avtomatizacijo oddaje oglasnega prostora (angl. *supply side platform* – SSP)[14], specializirana za dostavo oglasov glede na prej opredeljene preference oglaševalcev (angl. *demand side platform* – DSP),[15] pa tudi različni ponudniki analize podatkov in metrike (angl. *data management platform*),[16] od katerih je mogoče pridobiti dodatne podatke o posameznikih, za boljše ciljanje. V to kategorijo spadajo tudi ponudniki, ki omogočajo oglaševanje na različnih platformah na podlagi prijavnih podatkov v spletna družbena omrežja. Ker je med njimi Facebook najpogostejši, so ti ponudniki znani kot Facebook Marketing Partners (FMPs) (Busch, 2016, str. 9). Nekateri od teh igralcev opravljajo več funkcij v verigi, celoten trg je precej pretočen in vloge se hitro spreminjajo, prav tako nenehno prihaja do sprememb na področju tehničnih rešitev. Nekateri najpomembnejši igralci, kot je npr. Google, opravljajo več vlog hkrati – kot prodajalec oglasnega prostora in kot ponudnik podatkov in analitike ter kot platforma za izmenjavo oglasov (Datatilsynet, 2015, str. 11). Številni avtorji celoten sistem poimenujejo »črna skrinja«, saj je praktično nemogoče dobiti vpogled v njegovo delovanje, tako za zunanjega opazovalca kot tudi deloma za tiste, ki so znotraj sistema (Datatilsynet, 2015, str.10). Sledi poenostavljen shematski prikaz ključnih igralcev v verigi programatičnega oglaševanja (Bosch, 2016, str. 11), ki so opisani zgoraj (Slika 2.1) in natančen pregled vseh podjetij po kategorijah, kot ga prikazuje LumaScape (Slika 2.2) in iz katerega je jasno razvidno, kako nepregleden je trg in koliko podjetij obdeluje podatke uporabnikov elektronskih komunikacij.

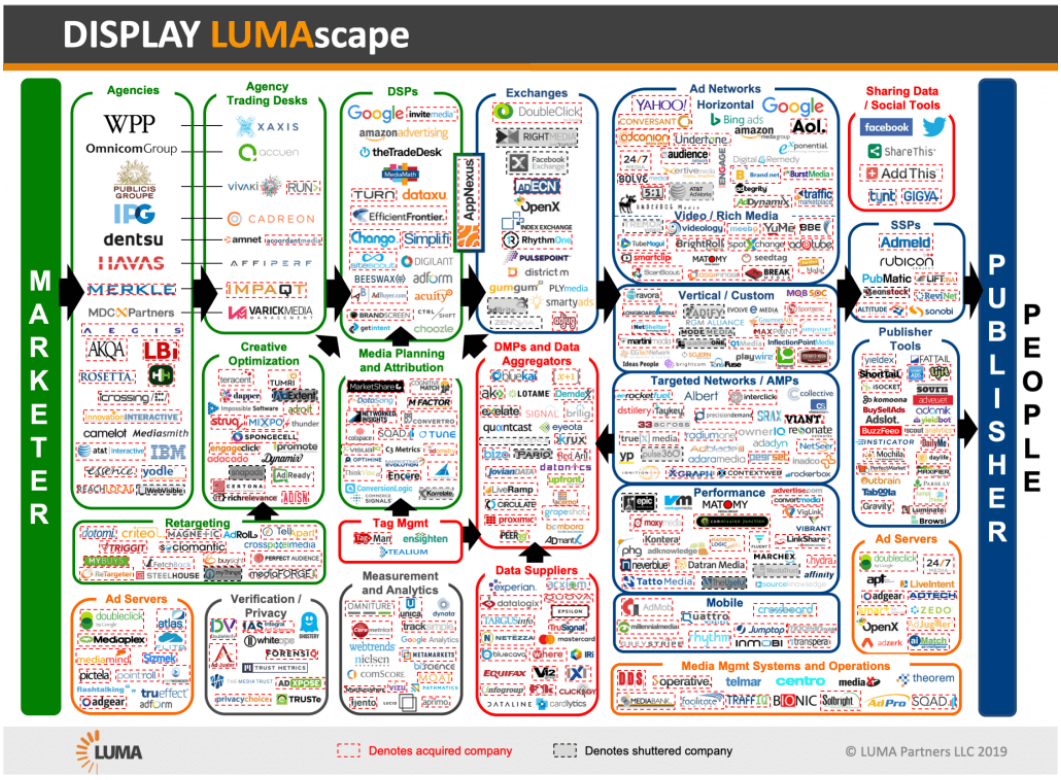
[14] Npr. Admeld (Google), Rubicon Project, Pubmatic in Index Exchange.
[15] Npr. Doublecleck, Bid Manager, MediaMath in Rocktfuel.
[16] Preprodajalci podatkov (Acxiom, Datalogix, Experian itd.), raziskave trga itd.

Slika 2.1: Ponudniki v verigi programatičnega oglaševanja in povezave med njimi



Vir: Bosch (2016, str. 11)

Slika 2.2: Pregled izvajalcev prikaznega oglaševanja LumaScape

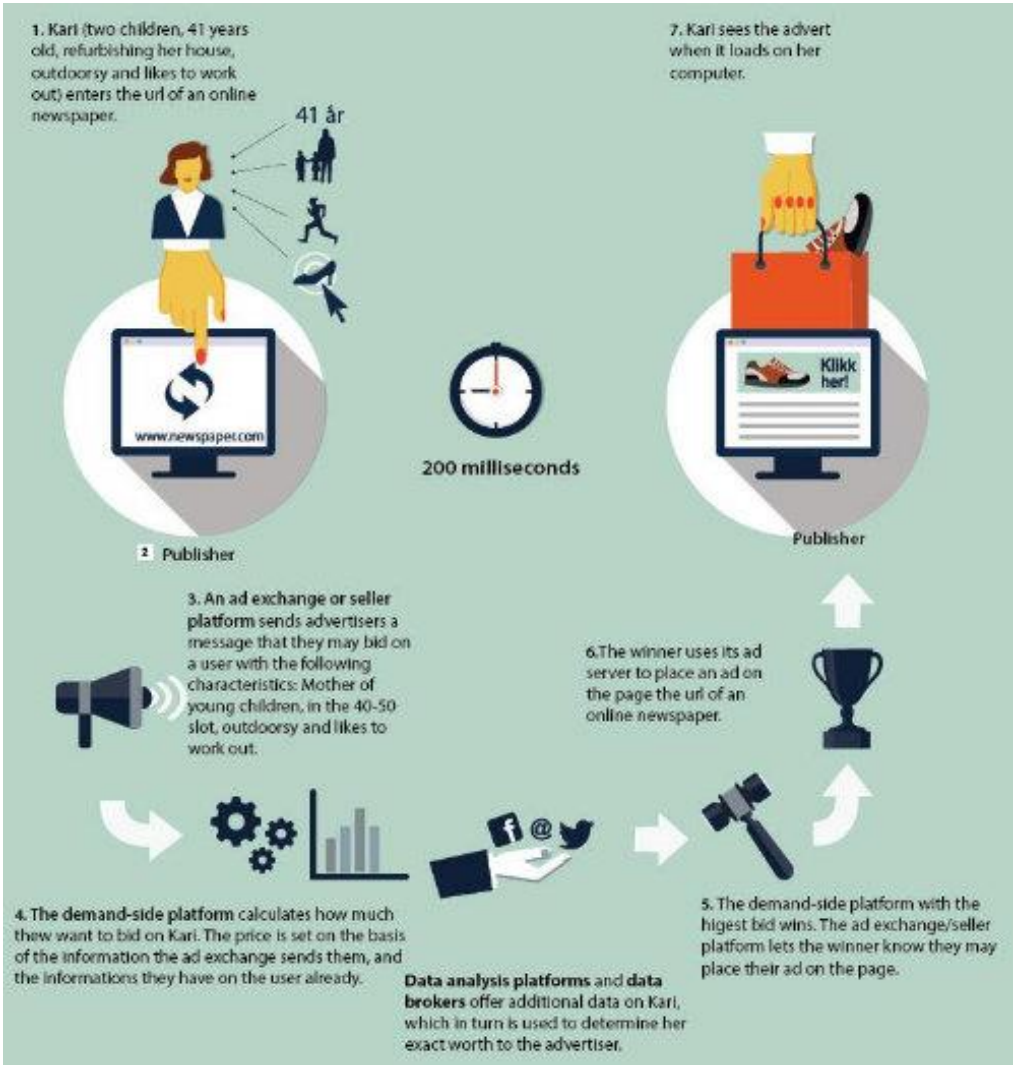


Vir: Luma (2019)

Primer takega oglaševanja so spletne dražbe uporabniških profilov (angl. *real time bidding*), ki jih grafično prikazuje inforgafika na sliki 2.3 (Datatilsynet, 2015, str. 13). Ko uporabnik obišče neko spletno stran, npr. spletne novice, na kateri so objavljeni prikazni oglasi, ki jih ponudi oglaševalski strežnik, ta pošlje zahtevek s podatki uporabnika (npr. Kari, 41 let, prenavlja dom, rada preživlja čas v naravi) založnikovemu partnerju – t. i. *supply side* platformi (SSP), da zapolni prost oglasni prostor na strani za posameznega uporabnika. SSP pošlje obvestilo o uporabniškem profilu platformi za izmenjavo oglasov. Ta pošlje informacijo o uporabnikovem profilu medijskim agencijam in t. i. *demand side* platformam (DSP), ki so registrirane pri njej, da posredujejo svoje ponudbe. Oglas lahko uporabniku prikaže tisti oglaševalec, ki je za uporabnika ponudil največ. Oglaševalec in njegovi posredniki (DSP) ob prejemu informacije o uporabnikovem profilu preverijo, ali o tem uporabniku že imajo kaj podatkov. Če podatke imajo, so za uporabnika pripravljeni plačati več. Celoten proces se odvije v milisekundah, medtem ko se spletna stran nalaga. Proces je kompleksen in lahko vključuje več sto podjetij, ki tekmujejo med seboj za prikaz oglasa konkretnemu uporabniku. Poleg navedenih podjetij je v proces vključenih še več takih, katerih naloga je analiza podatkov o uporabnikih in obogatitev uporabniških podatkov (Datatilsynet, 2015, str. 10–11). Uporabniku je celoten proces draženja uporabniških profilov v realnem času neviden, prav tako nikakor ne more vedeti, s katerimi podjetji se delijo njegovi podatki ob obisku posamezne spletne strani (Castelluccia, 2012).

Daleč najuspešnejše podjetje na globalnem programatičnem trgu je Google, ki prek velikega števila svojih storitev (npr. iskalnik, Gmail, zemljevidi, Street View) neposredno zbira podatke o uporabnikih in jih lahko nato uporablja tudi v okviru svojih oglaševalskih dejavnosti. Podatke zbira tudi posredno, prek svojih storitev, kjer deluje kot tretja stran (Google Analytics Doubleclick, AsSense, AdWords) (Datatilsynet, 2015, str. 24). Zadnje raziskave kažejo, da podatke z mobilnih naprav prejema tudi, ko uporabniki niso aktivni (v smislu uporabe aplikacij, zemljevidov ali drugih dejavnosti), saj naprava pošilja podatke privzeto, tudi ko miruje (npr. o lokaciji) (Schmidt, 2018).

Slika 2.3: Proces programatičnega draženja profilov v realnem času



Vir: Datatilsynet (2015, str. 24)

Oglaševalska sredstva, namenjena programatičnemu oglaševanju, se delijo med številnimi ponudniki v verigi, ki za svoje storitve prejemajo provizije. Manj kot polovico sredstev dobi izdajatelj, več kot polovica pa je namenjena *ad tech* panogi (WFA, 2014, str. 7). Programatično oglaševanje nekateri opisujejo kot transformativno za področje oglaševanja, z zmožnostmi povezovanja trženja prek različnih kanalov. Ker temelji na podatkih o posamezniku, mu lahko prikaže najrelevantnejši oglas glede na njegovo konkretno situacijo, kaj pripomore k nakupnemu vedenju oziroma boljšemu odnosu do znamke, ki se oglašuje (npr. Busch, 2016; Seitz in Zorn, 2016). Pa vendar se zdi, da trenutno stanje še ne ustreza vsem tem kvalifikacijam. Programatično oglaševanje je lahko uporabljeno le za oddajo inventarja, ki je težko unovčljiv (Busch, 2016). Na trgu je veliko ponudnikov, ki nudijo

različno kakovostne storitve, nekateri tudi dvomljive, in kot kaže, je prisotnih tudi veliko zlorab, npr. z neveljavnim prometom (Nesdale, 2018). Konsolidacija ponudnikov naj bi tako pripomogla k večji kakovosti in preglednosti trga, po drugi strani pa vidimo, da tako nastaja duopol, ki vlada na *ad tech* trgu z Googlom in Facebookom, ki imata vsak svoj razvejan model programatičnega vedenjskega oglaševanja in ki skupaj pokrivata 60–70 odstotkov trga (eMarketer, 2017). Do leta 2020 naj bi bilo več kot 85 odstotkov vsega prikaznega oglaševanja programatičnega, pri čemer večina na mobilnih platformah (Fischer, 2018). Približno 80 odstotkov vsega prikaznega oglaševanja je trenutno programatičnega v ZDA, Kanadi in Veliki Britaniji, ki jim sledita Danska in Francija (s 70 in 63 odstotki) (Zenith, 2017). Gonilna sila za rastjo programatičnega oglaševanja je problematika monetizacije mobilnega prometa, potrebe medijev po kombiniranju monetizacije vsebine in podatkov, ki so jim na voljo, ponujajo pa se tudi možnosti kombiniranja podatkov iz realnega in virtualnega sveta (Seitz in Zorn, 2016, str. 38).[17]

2.2.2 Spletna družbena omrežja: Facebook

Splošno bi lahko spletna družbena omrežja oziroma spletne družbene medije opisali kot platforme, ki gostujejo, omogočajo in spodbujajo izmenjavanje vsebin, ki jih ustvarjajo uporabniki in drugi, prek socialne interakcije. V zameno za te, večinoma brezplačne storitve, spletni družbeni mediji pridobijo možnost dostopa do podatkov uporabnikov, njihovega zbiranja in obdelave. Podatki zadevajo uporabnikov socio-demografski profil, interese in preference. Te podatke uporabijo zato, da ustvarjajo in ponujajo oglaševalske storitve, ki so vezane na zelo granularne in prilagodljive možnosti ciljanja (Evropska komisija, 2018a, str. 12). Spletna družbena omrežja so tesno vpeta v posameznikov vsakdan. Raziskave namreč kažejo, da jih povprečni uporabnik uporablja več kot dve uri na dan (Statista, 2017a). Njihovi prihodki večinoma prihajajo od oglaševanja, saj imajo le redki plačljiv poslovni model. Oglaševanje na spletnih družbenih medijih nenehno raste in trenutno predstavlja 16 odstotkov digitalnega oglaševanja v Evropi (Statista, 2017b). Oglaševanje lahko temelji na vsebini uporabnikovega profila ali pa na njegovi zgodovini brskanja po spletu, lahko ga izvajajo s pomočjo lastne oglaševalske mreže ali s pomočjo tretjih oglaševalskih mrež. Facebook je vodilni igralec na trgu, saj zajema 43,6 odstotka vsega prometa spletnim družbenim medijem

[17] Podrobneje o prednostih in izzivih programatičnega oglaševanja v Prilogi B.

(Evropska komisija, 2018a, str. 15, 25). V nadaljevanju zato sledi podrobnejši opis Facebookovih praks v zvezi z vedenjskim oglaševanjem.

Spletno družbeno omrežje Facebook, ki je bilo ustanovljeno leta 2004, združuje več kot dve milijardi uporabnikov iz vsega sveta. Zadnje funkcionalnosti vključujejo pretočni video (*Facebook Live*) in tržnico za direktne nakupe (*Marketplace*). Pod okrilje Facebooka spadajo tudi storitve *Facebook Messenger* (storitev za hipno sporočanje), Instagram (spletni družbeni medij, ki temelji na izmenjavi fotografij, ki ga je Facebook prevzel leta 2014) in WhatsApp (komunikacijska platforma s šifrirano povezavo, ki jo je Facebook prevzel leta 2014). Za uporabo posameznik potrebuje račun, ki je brezplačen. Uporabniki morajo biti stari več kot 13 let. 98 odstotkov svojih prihodkov pridobi od oglaševanja. (Evropska komisija, 2018a, str. 20–22).

Facebook je zelo priljubljeno (in učinkovito) oglaševalsko orodje. Ponuja zelo natančno ciljanje oglasov, merjenje rezultatov, število uporabnikov pa še vedno raste (Burnik, 2012a). Iz spletnega družbenega omrežja, svoje prvotne funkcije, se je tako razvil v ogromno oglaševalsko mrežo, ki temelji na ciljnem, vedenjskem oglaševanju in operira s podatki, pridobljenimi znotraj Facebookove mreže storitev in zunaj nje, da z oglasi cilja na uporabnike znotraj omrežja in na partnerskih spletnih straneh. Zanjo je značilna vertikalna in horizontalna širitev obdelave osebnih podatkov. Za vertikalno širitev gre zato, ker narašča raznovrstnost različnih podatkov, ki jih Facebook o posamezniku obdeluje (tudi s pridruženih platform Instagram in Whatsapp), kar pomeni obsežnejši profil posameznika. Horizontalna širitev pa zato, ker število virov, iz katerih Facebook pridobiva podatke, stalno narašča (van Alsenoy in drugi, 2015, str. 10).

Na podlagi podatkov, zbranih z različnih virov, spletna družbena omrežja ustvarjajo zelo podrobne profile uporabnikov, ki omogočajo podjetjem in organizacijam natančno ciljanje glede na svoje potrebe. Algoritmi, ki profiliranje omogočajo, so najbolj kompleksno in najmanj transparentno področje pri spletnih družbenih omrežjih (Evropska komisija, 2018a, str. 76). Ciljanje je na Facebooku mogoče glede na socio-demografske podatke ali pa veliko natančnejše. Med najspornejšimi praksami je tako grajenje prilagojenih občinstev (*Custom Audiences*) in podobnih občinstev *(Lookalike Audiences)* ter uporaba možnosti prijave spletnega družbenega omrežja (angl. *log-in*). Grajenje prilagojenih občinstev pomeni, da je

točno določenemu uporabniku mogoče poslati sporočilo na podlagi njegove telefonske številke ali e-pošte, oziroma identifikacijske številke naprave, tako da oglaševalec svoje podatke o strankah uvozi v Facebookovo storitev in ta podatke poveže z obstoječimi podatki Facebookovih uporabnikov. Podobna občinstva pa temeljijo na podatkih o strankah nekega subjekta (ki so lahko zbrani iz različnih virov, *online, offline,* s podatkov brskanja, nakupov, podatkov o uporabi aplikacij itd.). Facebookovi algoritmi nato na podlagi teh podatkov poiščejo podobne uporabnike znotraj Facebooka, saj se podobni uporabniki najbrž zanimajo za podobne stvari. Zadnja možnost – rešitve prijave – pa vključujejo orodja za prijavo, ki jih Facebook brezplačno ponuja tretjim stranem, da se stranke v njihove storitve vpišejo s Facebookovimi prijavnimi podatki. Tako podatke o aktivnostih, ki jih uporabnik opravi na tej tretji strani, prejme tudi Facebook. Posamezniki so o teh praksah slabo obveščeni in jih ne razumejo. Čeprav podajo privolitev, ne vedo v kaj točno privolijo, saj informacije o tem, kateri podatki se obdelujejo, iz kakšnih virov, za kakšne namene, kdo vse jih uporablja, niso jasne, prav tako uporabniki nimajo vedno možnosti, da take obdelave zavrnejo (Evropska komisija, 2018a, str. 78–89).

Prakse vedenjskega oglaševanja na omrežju Facebook so tarče čedalje več kritik. Poleg očitkov o netransparentnosti te aktivnosti gre namreč tudi za dvome v veljavnost privolitve uporabnika v oglaševanje (posamezni uporabnik namreč privoli tako, da se strinja s splošnimi pogoji delovanja ter ima možnost vedenjsko oglaševanje zavrniti le naknadno), sporne se zdijo prakse kombiniranja podatkov iz različnih virov podjetij, povezanih s Facebookom (npr. WhatsApp) ter obširno sledenje uporabnikom spleta, ki niso nujno tudi uporabniki Facebooka, in sicer prek vtičnikov »Všeč mi je«, ki so integrirani v ogromno število spletnih strani (van Alsenoy in drugi, 2015, str. 8–9). Med sporne vidike (vseh spletnih družbenih medijev) so umeščene tudi prikrite oglaševalske tehnike, ki uporabnika zavajajo, da gre za vsebino, ki jo je objavil neki uporabnik, v resnici pa gre za plačan oglas: nativni oglasi (ki se zlijejo z vsebino, podobno kot umeščanje produktov v tradicionalnih medijih), trženje s pomočjo vplivnežev in t. i. *advertorials* (ki so videti kot članki, prispevki in gostujejo na zunanjih domenah ter jih poslovni uporabniki objavijo tudi prek Facebooka). (Evropska komisija, 2018a, str. 30–52).

V zadnjih letih beležimo tudi več akcij nadzornih organov in sodišč, tako v ZDA kot tudi v EU, ki ravnanja Facebookovega omrežja presojajo v okviru pravil za varstvo osebnih

podatkov, pa tudi pravil za varstvo potrošnikov.[18] Med naloženimi ukrepi je bila npr. priprava natančnejših pojasnil, kako in kateri podatki se uporabljajo za oglaševanje, pa omejitve pri sledenju uporabnikom prek gumba »všeč mi je« (Burnik, 2012b) in uporabi piškotkov ter podobnih sledilnih tehnologijah na svoji in ne tretjih domenah za namene oglaševanja (Van Canneyt in De Smet, 2018). Prav tako je bilo izrečenih že več finančnih sankcij, med drugim 500.000 evrov zaradi kršitev v primeru Cambridge Analytica (BBC, 2018). Facebook je obravnavalo tudi Sodišče EU in razsodilo glede njegove soodgovornosti v primeru spletnih strani podjetij (t. i. *fanpages*) (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein vs. Wirtschaftsakademie, 2018) ter glede odgovornosti spletnih strani v primeru, da uporabljajo Facebook vtičnike (Fashion ID GmbH & Co. KG vs. Verbraucherzentrale NRW eV, 2019).

Posebno podskupino, namenjeno vprašanjem spletnih družbenih medijev in njihove obdelave podatkov za najrazličnejše namene, predvsem glede oglaševanja in ciljanja, je ustanovila tudi Delovna skupina iz člena 29, ki združuje vse nadzorne organe za varstvo osebnih podatkov iz EU (WP29, 2018). Povod za to so bila predvsem razkritja glede političnega mikro ciljanja, ki ga je s pomočjo Facebooka izvajala družba Cambridge Analytica in ki je vplivalo na predsedniške volitve v ZDA leta 2016 in referendum o izstopu Velike Britanije iz EU (več o tem v poglavju 2.2.6). Krog pravnih omejitev in neugodnih odločitev pristojnih organov okoli Facebooka se torej vztrajno oži, predvsem v Evropi, kjer regulatorji že močno pritiskajo k uvedbi nujnih sprememb, tudi po nedavnem incidentu, ko so hekerji kompromitirali račune skoraj 30 milijonov uporabnikov (Isaac in Frenkel, 2018). Kakšna bo dolgoročna usoda Facebooka, je torej težko napovedati, saj je vprašljivo, ali bo njegov poslovni model iz vseh trenutnih pravnih bitk izšel neokrnjen. Vrstijo se tudi pozivi delničarjev k zamenjavi Marka Zuckerberga, ustanovitelja in direktorja (Tidey, 2018).

2.2.3 Phorm: Vedenjsko oglaševanje na ravni ponudnika dostopa do interneta

Vedenjsko oglaševanje lahko poteka tudi na ravni ponudnika dostopa do omrežja, in sicer pri operaterju elektronskih komunikacij. Operater v tem primeru analizira vsebino komunikacij posameznega uporabnika svojega omrežja ali storitve (katere spletne strani uporabnik obiskuje, kaj išče prek spletnih iskalnikov) in tako ugotovi, kaj uporabnika zanima, kaj išče

[18] Podrobneje v Prilogi C.

ipd. ter mu nato dostavlja oglase, vezane na vsebino komunikacij. To je mogoče s pomočjo uporabe tehnologije orodij za nadzor omrežnega prometa, t. i. *deep packet inspection* (DPI). DPI temelji na pregledovanju vsebine digitalnih paketov, ki sestavljajo sporočilo pri prenosu po omrežju. Vpogled v vsebino podatkov, ki se prenašajo po omrežju, lahko služi marsikateremu cilju: lahko določimo, kateri so škodljivi, in njihov prenos preprečimo, lahko optimiziramo delovanje omrežja, lahko odkrivamo prenašanje nelegalnih vsebin, kot so avtorsko zaščitena dela, ki jih uporabniki prenašajo s spleta, itd. (Burnik in Tomšič, 2011). Mogoča pa je tudi uporaba za namen vedenjskega oglaševanja. Najrazvpitejša primera take prakse sta se zgodila v ZDA in v Veliki Britaniji, kjer sta se dve podjetji (NebuAd in Phorm) povezali z lokalnimi ponudniki dostopa do interneta z namenom izvajanja vedenjskega oglaševanja (Tene in Polonetsky, 2012).

Podjetje Phorm v Veliki Britaniji je v povezavi z največjim ponudnikom dostopa do interneta British Telecom leta 2007 začelo izvajati testne poskuse svoje tehnologije, vendar brez privolitve uporabnikov oz. naročnikov. Bistvo Phormovega sistema je bilo v tem, da je prestrezal promet med uporabnikom in spletnimi stranmi, ki jih je ta obiskal. Če je posameznik npr. obiskal veliko spletnih strani, na katerih se pojavljajo besede potovanje, počitnice, imena krajev in držav ipd., ga je sistem uvrstil v kategorijo »potovanja«. Na drugi strani pa so podjetja, ki jih zanima oglaševanje uporabnikom, ki se zanimajo za potovanja. Phormov sistem je oglase teh podjetij prikazal uporabnikom iz kategorije »potovanja«. (ICO, 2008; Phorm, 2008; Wells, 2006; 20/80 Thinking, 2008).

Poskusi vedenjskega oglaševanja, ki so jih izvajali ponudniki dostopa do interneta v povezavi s tretjimi podjetji, so naleteli na velik odpor javnosti in strokovnjakov (Office of the Privacy Commissioner of Canada, b. d.), predvsem zaradi svoje prikrite narave in vpliva, ki ga lahko ima vedenjsko oglaševanje na zasebnost uporabnika. Ponudniki dostopa do interneta so namreč tisti, ki lahko o uporabniku zberejo največ informacij, poleg tega pa jim pri tem ni mogoče ubežati – vsak uporabnik je namreč vezan na ponudnika dostopa do interneta. Brskanje po internetu tako ni več anonimno, saj ponudnik dostopa do interneta uporabniku stalno sledi (Clayton, 2009; Tene in Polonetsky, 2012). Z uporabo tehnologije DPI torej ponudnik dostopa do interneta v povezavi s tretjim podjetjem dobi natančen vpogled v aktivnosti uporabnika na spletu, ki razkrivajo tudi podatke o uporabnikovem zasebnem življenju, nakupovalnih navadah, preferencah, interesih ipd.

Uporaba tehnologije DPI je običajno povezana z beleženjem naslovov IP oziroma psevdonimiziranih naslovov IP ter naslovov spletnih strani (URL), ki jih obišče posameznik z določenega naslova IP. Naslovi IP pa običajno omogočajo vsaj posredno določljivost posameznika. S stališča varstva osebnih podatkov je uporaba DPI problematična zlasti zato, ker zadeva zbiranje osebnih podatkov in občutljivih osebnih podatkov, ker je zbiranje osebnih podatkov tako razmeroma netransparentno, pojavljajo se vprašanja glede zavarovanja tako zbranih osebnih podatkov, glede roka hrambe podatkov in sekundarne rabe zbranih podatkov za druge namene. Uporaba DPI je sporna tudi zato, ker gre za klasično prestrezanje podatkov v omrežju in s tem povezano vprašanje varstva komunikacijske in informacijske zasebnosti. V EU je brez privolitve uporabnikov oziroma podlage v zakonu prepovedano kakorkoli nadzorovati promet v omrežju,[19] pri čemer pa je veljavno privolitev zelo težko pridobiti (Burnik in Tomšič, 2011). Zaradi močnega odpora proti taki uporabi tehnologije DPI sta podjetji NebuAd in Phorm na koncu propadli, čeprav sta svojo storitev ponujali le pod pogojem uporabnikove privolitve (Tene in Polonetsky, 2012).

Prestrezanje in nadzor nad prometom v elektronskem komunikacijskem omrežju zbujata tudi skrbi glede kršenja načela nevtralnosti omrežja (angl. *net(work) neutrality principle*), cenzuriranja vsebine in posegov v zasebnost posameznikov oziroma uporabnikov. Nevtralno omrežje namreč ne razlikuje med različnimi vsebinami, stranmi ali platformami, ne razlikuje med napravami, ki so priklopljene na omrežje, in komunikacijami, ki so dovoljene. V nevtralnem omrežju noben tok komunikacije ni brez razloga omejen z drugim, mu podrejen ali nadrejen. Tako stališče je sprejela tudi Mednarodna delovna skupina za varstvo osebnih podatkov v telekomunikacijah, ki opozarja operaterje elektronskih komunikacij, naj ne uporabljajo tehnologij DPI za ciljno oziroma vedenjsko oglaševanje (IWGDPT, 2011).

2.2.4 Preprodajalci podatkov – povezovanje *online* in *offline* virov

V ekosistemu vedenjskega oglaševanja imajo čedalje pomembnejšo vlogo trgovci s podatki (angl. *data brokers*),[20] predvsem v ZDA, kjer ne veljajo stroge omejitve glede varovanja osebnih podatkov, in posledično tudi v EU, saj evropska podjetja najemajo njihove storitve (FTC, 2014, str. 29). Trgovci s podatki so podjetja, ki zbirajo osebne podatke potrošnikov in

[19] Operaterje, ki bi želeli uporabljati tehnologijo DPI za vedenjsko oglaševanje v Evropi, zavezuje Direktiva 2002/58/ES, ki v prvem odstavku 5. člena ureja prestrezanje prometa v elektronskem omrežju.
[20] Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf in Recorded Future (FTC, 2014).

jih preprodajajo ali delijo z drugimi in so pomemben del gospodarstva velikega podatkovja (angl. *big data*). Podatke pridobivajo neposredno od posameznika, pa tudi tako, da jih kupujejo od podjetij in ustanov javnega sektorja ali pa jih pridobivajo iz javno dostopnih virov. Podatki tako obsegajo npr. podatke o stečaju, registriranih volivcih, lastnikih nepremičnin, volivcih, nakupih, navadah na spletu itd. Številna podjetja (npr. Disney) s prodajo podatkov svojih kupcev ali uporabnikov trgovcem s podatki ustvarjajo dodaten tok prihodkov (Crain, 2016, str. 3).

Zbirke podatkov trgovcev so lahko ogromne.[21] Iz različnih virov (tudi javno dostopnih) zbirajo več osebnih podatkov, ki jih nato dopolnijo s podatki, na katere sklepajo, npr. glede interesov posameznika. Če je nekdo lastnik čolna, lahko npr. sklepajo, da ga zanima pomorstvo. Iz zbranih podatkov lahko sklepajo tudi na občutljive podatke, recimo o etnični pripadnosti ali zdravju, ki jih lahko klienti nato uporabijo za trženjske namene. Zbrane podatke kombinirajo s pripisanimi kategorijami (npr. *Socer Mums, Rural Everlasting, Mobile Mixers*), ki lahko označujejo posameznike v določeni skupini tudi na način, ki razkriva občutljive osebne situacije ali zdravstvene kategorije. Posameznike lahko označijo tudi glede na predvidevanje o njihovih namenih – npr. *Likely to Seek a Chargeback* ali *Interested in Buying Camping Gear* (FTC, 2014, str. 19–20).

Ker trgovci s podatki načeloma nikoli ne pridejo v neposreden stik s potrošniki, se ti pogosto sploh ne zavedajo njihovega obstoja, še manj pa njihovih praks obdelave osebnih podatkov. Podatke kupujejo od drugih trgovcev, redko zberejo podatke iz originalnih virov, zato potrošnik težko izve, od kod je dejansko prišel njegov podatek. Moral bi namreč slediti več členom v verigi prodaje, da bi prišel do vira. Zbrane podatke ponujajo klientom za izpolnjevanje različnih namenov: za preverjanje posameznikove identitete in zaznavanje oz. odkrivanje prevar, trženje produktov in iskanje informacij o ljudeh (FTC, 2014, str. i–ii).

Trženjski produkti, ki jih trgovci s podatki ponujajo svojim klientom, so lahko namenjeni neposrednemu trženju (klient si kupi bazo e-naslovov, na katere lahko pošlje svojo ponudbo), lahko pa klient kupi podatke o interesih posameznikov, zato da jim lahko pošlje posebne

[21] Acxiom je ponudnik podatkov o potrošnikih in analitike za marketinške kampanje in zaznavanje prevar. V svojih bazah naj bi imel podatke o približno 700 milijonih posameznikov iz vsega sveta in več kot 3.000 segmentov podatkov za vsakega potrošnika iz ZDA. Datalogix je podjetje, ki ponuja trženjske podatke za skoraj vsako gospodinjstvo v ZDA in za več kot trilijon ameriških dolarjev v potrošniških transakcijah. Septembra 2012 je oznanil partnerstvo s Facebookom, da bo lahko meril, kako pogosto Facebookov uporabnik vidi produkt, oglaševan na družbenem omrežju, in ga nato zaključi v trgovini (in ne na spletu) (FTC, 2014, str. 8).

prilagojene ponudbe. Trgovci s podatki prodajajo tudi analitične produkte – analizirajo podatke, ki jih ima klient o svojih kupcih in mu predlagajo medijski kanal za oglaševanje posameznega produkta. Nekateri posameznike tudi razvrščajo glede na izračunano verjetnost, da bodo npr. kupili neki produkt ali storitev ali imeli vpliv na druge. Večina podjetij, ki ponuja trženjske produkte, dopušča posameznikom dostop do podatkov, ki jih o njih hranijo, ni pa nujno, da jim omogočajo popravo napačnih podatkov ali možnost naknadne zavrnitve take obdelave njihovih podatkov. Predvsem pa posamezniki niso obveščeni o teh možnostih. Tako npr. ne obstaja centraliziran portal, na katerem bi izvedli svojo zavrnitev (FTC, 2014, str. iii).[22] Trgovci s podatki kombinirajo podatke, zbrane na spletu, s tistimi zunaj spleta, da tržijo posameznikom na spletu. Na podlagi piškotkov in drugih tehnologij sledijo posameznikom na spletu, podatke združijo s tistimi, ki jih pridobijo zunaj spleta in nato posamezniku na spletu prikažejo prilagojene oglase (FTC, 2014, str. 46–47).

Koristi za potrošnike naj bi izhajale iz številnih namenov in produktov trgovcev s podatki – preprečujejo zlorabe in tako zlonamerneži težje prevzamejo identiteto nedolžnih posameznikov, izboljšujejo ponudbo storitev in produktov ter dostavljajo prilagojene oglase. To pomeni, da potrošniki lažje najdejo storitve in izdelke, ki jih želijo oz. potrebujejo, omogočajo pa tudi vstop na trg manjšim podjetjem, ki se lažje povežejo s potrošniki. Posamezniki tudi lažje ohranjajo stike in najdejo svoje stike in prijatelje iz preteklosti (FTC, 2014, str. 47).

Prav tako pa lahko ti produkti pomenijo grožnjo pravicam potrošnikov, npr. kadar je potrošniku zaradi slabe ocene njegove sposobnosti zavrnjen dostop do neke storitve zaradi napačnih podatkov, ki jih ima trgovec, pa se potrošnik niti ne zaveda, da je bil ocenjen, niti napačnih podatkov ne more popraviti. Tako niti ne more do storitve niti ocenjevanje ni transparentno. Ciljano oglaševanje lahko izrablja podatke o zdravstvenem stanju, etničnem poreklu ali drugih kategorijah, zaradi katerih je potrošniku najmanj neprijetno ali pa te podatke uporabi npr. zavarovalnica in potrošniku zaračuna višjo premijo, in sicer zaradi tveganja. Prav tako pomeni veliko tveganje neomejena hramba takih podatkov. Kraja podrobnih profilov posameznikov, ki nastajajo dalj časa in so precej zanesljivi, lahko pomeni veliko tveganje za posameznika (FTC, 2014, str. 48).

[22] Podrobno o različnih produktih za spletno oglaševanje v Prilogi D.

FTC ugotavlja, da so možnosti izbire, ki jih imajo potrošniki glede obdelave njihovih osebnih podatkov s strani trgovcev podatkov, zelo omejene, večinoma nevidne in nepopolne. Nekateri sicer ponujajo izbiro, vendar ker trgovci s podatki niso v neposrednem stiku s potrošniki, potrošniki ne vedo, kje lahko svoje pravice uveljavljajo. Pogosto tudi ni jasno, kaj možnost zavrnitve dejansko pomeni, predvsem pri trženjskih produktih – ali gre le za omejevanje prikazovanja oglasov ali pa res omejijo obdelavo osebnih podatkov. Večina ponudnikov namreč takim posameznikom prepreči zgolj prikazovanje oglasov, ne pa tudi obdelave njihovih osebnih podatkov. Pri produktih za omejevanje tveganj trgovci s podatki posameznikom običajno niti ne ponujajo dostopa do njihovih podatkov ali možnosti popravkov (FTC, 2014, str. 49).

V ZDA je razmah podjetij, ki so ponujala oceno kreditne in drugih sposobnosti posameznikov, pa pri tem netransparentno zbirala podatke, vodil v sprejetje Zakona o poštenem kreditnem poročanju,[23] ki pa velja le za obdelave osebnih podatkov za namen odločanja o kreditih, zaposlitvi, zavarovanju, stanovanjskih in podobnih odločitvah, ne pokriva pa obdelave podatkov za marketinške namene, kar pomeni, da so tisti trgovci s podatki v ZDA, ki ponujajo podatke za namene trženja, večinoma neregulirani (FTC, 2014, str. i). Crain ta pojav razlaga v smislu koncepta asimetrije izgube zasebnosti. Številni Američani se zavedajo komercialnega nadzora, vendar imajo običajno zelo pomanjkljivo vedenje o dejanskih razsežnostih teh praks. Izpostavljeni so širokemu nadzoru, hkrati pa organizacije, ki nadzor izvajajo, to počnejo prikrito, tako v smislu zavedanja javnosti kot tudi v smislu regulatornih organov in nadzora. Na obeh ravneh imajo namreč subjekti težavo s pridobivanjem informacij o delovanju trgovcev s podatki (Crain, 2016, str. 4).

FTC v zvezi s trženjskimi produkti trgovcev s podatki meni, da bi morala zakonodaja posameznikom omogočiti (1) dostop do podatkov o njih in (2) naknadno zavrnitev obdelave osebnih podatkov. Da bi se lahko posamezniki sploh seznanili s temi pravicami, bi morala zakonodaja zahtevati vzpostavitev centraliziranega mehanizma, kot je npr. internetni portal, kjer si se trgovci s podatki lahko identificirali in objavili orodja za dostop do podatkov in zavrnitev obdelave (FTC, 2014, str. 50–56).[24] Tukaj je treba še dodati, da je opisane aktivnosti trgovcev s podatki sicer mogoče zakonito izvajati na trgu v ZDA, kjer ne veljajo tako stroge omejitve zakonodaje o varstvu osebnih podatkov kot v EU, in trgovci s podatki lahko

[23] *Fair Credit Reporting Act* (FCRA).
[24] Več o priporočilih in njihovi kritiki v Prilogi E.

kupujejo osebne podatke od različnih ponudnikov, ti pa pri posredovanju podatkov prav tako niso tako omejeni. V EU npr. operater elektronskih komunikacij (kamor spadajo tudi ponudniki kabelske televizije) nikakor ne bi smel prodati ali posredovati svojih baz osebnih podatkov tretjim, saj mu to prepoveduje zakonodaja. Prav tako ta omejuje namene, za katere se sme osebne podatke uporabiti.

2.2.5 Internet stvari – posameznik je dosegljiv 24 ur na dan

Koncept interneta stvari se nanaša na običajne naprave za vsakodnevno uporabo, ki vsebujejo posebne senzorje s sposobnostjo zaznavanja, obdelave, hrambe in posredovanja podatkov. Te naprave so povezane v omrežje in lahko komunicirajo z drugimi povezanimi napravami v sistemu, saj vsebujejo unikaten identifikator, ki omogoča njihovo prepoznavo. Primer so gospodinjski aparati (npr. pametni hladilnik) in druge senzorične naprave za upravljanje »pametnega« doma, pametni televizijski sprejemniki, pa avtonomna vozila, nosljive naprave (angl. *wearables*), najpogosteje namenjene merjenju telesnih funkcij, športnih dosežkov, spanja ipd., pa posebna očala itd. Namen naprav je glede na podatke o uporabi uporabniku ponuditi izboljšano storitev. Ker naprave običajno uporablja fizična oseba, ki je s pomočjo naprave določljiva, ti podatki običajno pomenijo osebne podatke uporabnika (WP29, 2014a, str. 4).

Tveganja z vidika zasebnosti uporabnikov naprav interneta stvari vključujejo:

- uporabnik nima nadzora nad tokom podatkov in težko ostaja anonimen;
- pomanjkljive so privolitve uporabnikov v potencialno obširne obdelave osebnih podatkov za najrazličnejše namene, ne le delovanje naprave in povezane storitve;
- pomanjkljivo je obveščanje o obdelavi podatkov;
- tveganja so povezana s podatki, ki so iz zbranih izvedeni – torej sklepanja in profiliranje na podlagi surovih podatkov naprav ter uporaba podatkov za druge namene;
- slabo zavarovanje, vdori, zlorabe, povezane tudi z dejstvom, da je v panogo interneta stvari povezanih veliko subjektov, prek katerih tečejo podatkovni tokovi (WP29, 2014b, str. 6–9). Med njimi so proizvajalci naprav, ki običajno nekatere podatke tudi obdelujejo, konfigurirajo napravo, spletna družbena omrežja, prek katerih lahko posamezniki podatke delijo, razvijalci aplikacij za upravljanje naprav in tretje stranke

(npr. zavarovalnice), ki lahko podatke o uporabi pridobijo od prej navedenih za svoje, popolnoma drugačne namene (WP29, 2014b, str. 11–13).

Raziskave[25] najrazličnejših naprav interneta stvari (od pametnih števcev, nosljivih fitnes števcev, domačih pripomočkov, medicinskih naprav (merilec pritiska in spanja), povezanih avtomobilov, pametnih igrač, pametnih televizijskih sprejemnikov in pametnega videonadzora) kažejo, da je 60 odstotkov naprav brez pojasnila, kako se osebni podatki zbirajo in uporabljajo ter komu so razkriti. Skoraj 70 odstotkov naprav je bilo brez pojasnila, kako so podatki hranjeni. Pri skoraj 40 odstotkih naprav proizvajalec ni ponudil kontaktnega podatka v primeru vprašanj o zasebnosti in pri več kot 70 odstotkih naprav ni ponudil pojasnila, kako se lahko podatki iz naprave izbrišejo (npr. na daljavo, če je ukradena, ali če bi jo želeli prodati) (ICO, 2016). Zelo problematična je tudi raba podatkov, iz katerih je mogoče predvidevati občutljiva stanja posameznika, in to izrabljati za ciljno oglaševanje, npr. na podlagi podatkov o teku sklepati na poškodbo posameznika in temu prilagoditi oglase.

Katayev (2015) poudarja, da je obdelava podatkov v oglaševanju prinesla korenite spremembe – v zadnjih nekaj letih je vsaka stvar postala podatkovna točka. Tako pametne igrače, zapestnice z merilniki, pametne kamere in vse druge naprave, ki so povezane v splet, nudijo podatke o potrošnikih oz. njihovi uporabi teh naprav. Po izboljšanju možnosti za sledenje uporabniku prek različnih naprav po identifikacijskih številkah naprav je nastal preskok k povezovanju spletnega vedenja z vedenjem v realnem svetu. Oglaševalci lahko namreč pošiljajo relevantne oglase na različne naprave, ki jih uporabniki nosijo s seboj, na lokacijah, kjer jim je to relevantno, npr. kupone za popust, ko so v trgovini. Za oglaševanje tako veliko podatkovje, ki ga prinaša internet stvari, pomeni izboljšane možnosti zelo granularnega ciljanja, in nadaljnjo stopnico v razvoju tehnologij za ciljanje. Z rastjo števila povezanih naprav – od hišnih pripomočkov in senzorjev do nosljivih pripomočkov, pametnih televizijskih sprejemnikov itd. – bo mogoče uporabniku prilagoditi oglase glede na načine uporabe teh stvari in njihovo vedenje doma, ne le na javnih krajih. To so podatki, ki oglaševalski industriji nikoli prej niso bili dostopni. Z združevanjem podatkov iz različnih virov, naprav in podatkov iz realnega življenja bo mogoče sestaviti skoraj popolno sliko o potrošniku in njegovem stanju v katerikoli časovni točki (Katayev, 2015). To pa, kot je bilo že

[25] Petindvajset nadzornih organov za varovanje osebnih podatkov iz vsega sveta je leta 2016 pregledalo 314 najrazličnejših naprav interneta stvari.

orisano zgoraj, prinaša plejado različnih tveganj za pravice posameznikov, zlasti kadar se oglaševanje izvaja prikrito in posamezniki o tem niso zadostno obveščeni.

Ob tem je treba omeniti nedavne primere odločitev nadzornih organov za varovanje zasebnosti oz. potrošnikov v primeru pametnih televizijskih sprejemnikov. Ameriški regulator je npr. leta 2017 naložil ponudniku Vizio plačilo globe v višini 2,2 milijona dolarjev, ker je uporabnikom brez ustreznega obvestila in njihove privolitve spremljal, kaj gledajo, in te podatke obdeloval za namen ciljnega oglaševanja. Podatke o gledalskih navadah milijonov uporabnikov je prodal oglaševalcem in preprodajalcem podatkov, da so lahko prek kombiniranja s svojimi bazami identificirali posamezne uporabnike in jim dostavljali oglase na različnih napravah (Fair, 2017). Podatki o gledalskih navadah pa razkrivajo navade in interese naročnikov ter so lahko tudi občutljivi (npr. razkrivajo spolno usmerjenost).[26]

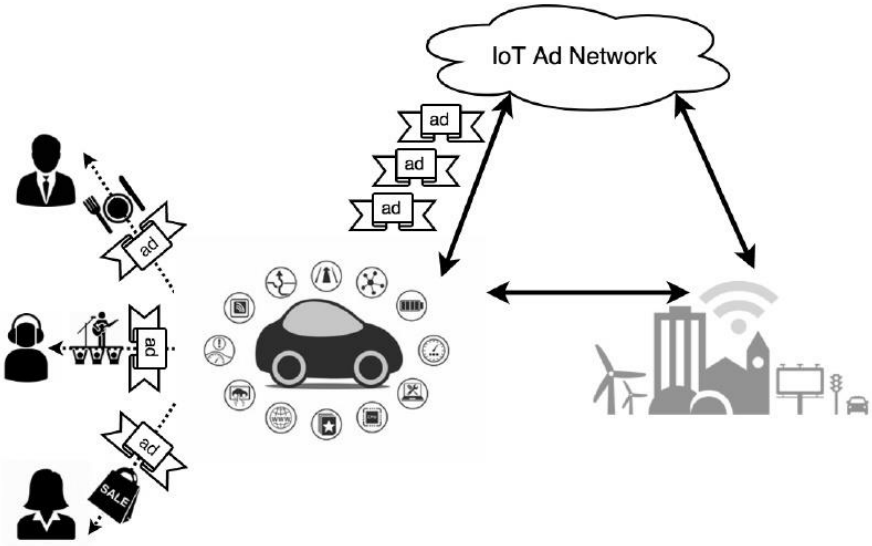
V okviru interneta stvari se odpirajo nove možnosti napredka tudi na področju programatičnega oglaševanja. Število naprav, povezanih na splet, se eksponentno povečuje in napovedi kažejo, da bo količina komunikacij med napravami presegla komunikacijo med osebami. Največji igralci na tehnološkem trgu (npr. Google) so že posegli na področje interneta stvari, kjer upajo na potenciale novega toka podatkov, ki bo bogatil njihove poslovne modele. Aplikacije in naprave za izboljšanje spanca, merjenje atletskih sposobnosti, zdravstvenega stanja, karkoli, kar je lahko izmerjeno, lahko prispevajo podatke, ki jih je mogoče ekonomsko izrabiti. Domače naprave, avtomobili, televizijski sprejemniki idr. so lahko tudi kanal za prikazovanje oglasov in programatično oglaševanje ima tu odprta vrata (Seitz in Zorn, 2016, str. 47).

Internet stvari zaznamujejo raznolikost naprav, visoka povezljivost in prilagodljivost (angl. *scalability*). Oglaševanje ima tako možnost kompleksnejših strategij, ki gradijo na kontekstualnem zavedanju, saj je mogoče uporabiti raznolike naprave (voznik avtomobila bi lahko videl sebi prilagojen oglas na oglasnem mestu ob cesti). Povezljivost in prilagodljivost pa bi omogočila veliko dinamiko, saj nove naprave nenehne prihajajo v omrežje in odhajajo iz njega. V tradicionalnem računalniškem svetu digitalnega oglaševanja je oglaševalec omejen s časom, ki ga uporabnik preživi pred zaslonom – ob premiku k internetu stvari pa je lahko uporabnik »pokrit« pravzaprav 24 ur na dan (Aksu in drugi, 2018, str. 1).

[26] Za več primerov glede pametnih televizijskih sprejemnikov glej Prilogo F.

Aksu in drugi (2018) tako predlagajo inovativen model oglaševanja v pametnih vozilih, ki bi temeljil na podobnem sistemu, kot je programatično oglaševanje z avtomatiziranimi postopki ter trgovanjem profilov v realnem času z oglaševalsko mrežo in platformo za izmenjavo oglasov. Hkrati predvidevajo novo vlogo oglaševalskega koordinatorja, ki bi imel povezovalno vlogo med vsemi napravami na fizični ravni in med oglaševalskim ekosistemom. Tako bi lahko trije potniki v istem avtu, vsak z drugačnim preferencami (enega zanima koncert, drugega kosilo in tretjo nakupovanje), na svoje raznolike naprave prejemali relevantne, njim prilagojene oglase, primerne glede na lokacijo, na kateri bi trenutno bili (Slika 2.4) (Aksu in drugi, 2018, str. 2–4). Avtorji ob tem hipotetičnem primeru poudarjajo tudi nekatere izzive za oglaševanje v okviru interneta stvari, kot so različne zmožnosti in zmogljivosti raznolikih naprav, priklopljenih v internet stvari, zaradi česar bi moral imeti koordinator oglaševanja raznolike strategije za različne naprave omejene zmožnosti dostave oglasa zaradi omejenosti naprav, da prejmejo in prikažejo vizualne vsebine, ter izzive glede zavarovanja podatkov in varovanja zasebnosti posameznikov (Aksu in drugi, 2018). Izziv glede zasebnosti in zavarovanja podatkov ob tako razvejanem sistemu oglaševanja, ki vključuje veliko različnih akterjev in avtomatizirane procese, utemljene na strojnem učenju in algoritmih, ter obdelavo ogromnih količin podatkov o posameznikih, pa je seveda zelo velik, kot izhaja iz tega poglavja in drugih opisanih primerov.

Slika 2.4: Ciljano oglaševanje v okolju interneta stvari



Vir: Aksu in drugi (2018, str. 2–4)

2.2.6 Cambridge Analytica: vedenjsko ciljanje za namen politične promocije

Decembra 2015 je britanski časnik Guardian razkril, da je v predsedniški kampanji ameriškega senatorja Teda Cruza sodelovalo takrat javnosti malo znano podjetje Cambridge Analytica, ki naj bi na podlagi podatkov desetin milijonov Facebookovih uporabnikov izdelovalo njihove psihografske profile, ki naj bili uporabljeni za ciljano promocijo kandidata in prilagajanje sporočil (Davies, 2015a). Zgodba se je razvila v eno največjih odkritij zadnjih let o tem, kako so lahko podatki uporabnikov spleta in posebej spletnih družbenih omrežij brez njihove vednosti in privolitve izrabljeni za namen natančnega profiliranja ter uporabljeni v političnih kampanjah, v katerih lahko zagotovijo ključno prednost zmagovalcu, saj omogočajo natančno ciljanje, ne le segmentiranja, na posameznike, ki jih kampanja želi nagovoriti, in sicer s sporočili, ki so jim pisana na kožo ter v pravem kontekstu. Ključni kampanji v tem okviru naj bi bile ameriške predsedniške volitve leta 2016, na katerih naj bi tudi s pomočjo podatkovne analitike zmagal Donald Trump, in referendum o izstopu Združenega Kraljestva iz EU, na katerem je presenetljivo zmagala opcija za Brexit, ki si je prav tako pomagala s storitvami Cambridge Analytica (Solon in Graham-Harrison, 2018). V začetku leta 2018 je zgodba dobila trdnejše okvire in dokaze v obliki žvižgača, nekdanjega zaposlenega v podjetju, ki je razkril številne podrobnosti delovanja Cambridge Analytice, njenih zmožnosti in povezav v visoki politiki (Rosenberg in Frenkel, 2018).

Družba Cambridge Analytica je uporabila podatke Facebookovih uporabnikov za to, da je na njih izvedla psihografsko tehniko ocenjevanja osebnosti po metodi OCEAN.[27] Glede na rezultate te metode naj bi bilo mogoče vplivati na vedenje volivcev. Študije namreč kažejo, da trženje, ki upošteva prilagajanje sporočila posameznemu tipu osebnosti, lahko ustvari tudi do 50 odstotkov večjo prodajo (Matz in drugi, 2017, str. 13). V primeru Cambridge Analytice so posamezniki rešili osebnostni vprašalnik prek Facebookove aplikacije thisisyourdigitallife, pri čemer je aplikacija pridobila podatke s profila uporabnika, ki je rešil vprašalnik, in s profilov njegovih prijateljev. Aplikacijo je razvil raziskovalec dr. Alexandr Kogan z Univerze v Cambridgeu in podatke pridobival kot raziskovalec, nato pa jih je delil s Cambridge Ananlytico, ki je z njim začela komercialno sodelovati (Rosenberg in Frenkel, 2018; ICO, 2018a, str. 20–21). Na vprašalnik se je odzvalo približno 270.000 Facebookovih uporabnikov, hkrati pa je Kogan pridobil tudi podatke iz profilov prijateljev vseh, ki so izpolnili vprašalnik

[27] Več v ICO, 2018a, str. 18.

(Facebook, 2018), kar naj bi pomenilo podatke več kot 50 milijonov uporabnikov, po podatkih ICO celo do 87 milijonov (ICO, 2018a, str. 9).

Poleg podatkov iz rešenega vprašalnika je aplikacija pridobila še naslednje javne podatke iz profilov Facebookovih uporabnikov: ime, spol, rojstni datum, mesto, fotografije, na katerih so bili označeni, spletne strani, ki so jih všečkali, objave na časovnici, novice, seznam prijateljev, e-naslove in sporočila. Aplikacija je dostopala tudi do podatkov prijateljev uporabnikov, in sicer do javnih podatkov v profilu: ime in spol, rojstni datum, mesto, fotografije, na katerih so bili označeni, in spletne strani, ki so jih všečkali. Podatki približno 30 milijonov ljudi so bili uparjeni z njihovimi rešenimi vprašalniki in nadalje kombinirani s podatki iz drugih virov, kot so bili npr. podatki o volivcih v posameznih območjih, za boljše ciljanje sporočil (ICO, 2018a, str. 20–21)[28].

Po razkritju je Facebook zatrjeval, da gre v tem primeru za kršitve dogovorov o uporabi pridobljenih osebnih podatkov s strani ponudnika aplikacije in ne za varnostne težave, ki naj bi jo omrežje zagotavljalo (Solon in Graham-Harrison, 2018). Kogan naj bi prekršil pravila s tem, ko je podatke delil s tretjimi strankami, vključno s Cambridge Analytico, zato je Facebook njegovo aplikacijo odstranil in zahteval potrdilo, da so vsi, ki so podatke prejeli, te tudi izbrisali, kar naj bi se tudi zgodilo (Facebook, 2018). Pa vendar je v širši javnosti prevladal argument, da to ravnanje ni dovolj in da bi moral Facebook tudi proaktivno zagotavljati, da tako plenilsko zajemanje podatkov uporabnikov sploh ne bi bilo omogočeno in platforma tako izrabljena (Rosenberg in Frenkel, 2018). Družba Cambridge Analytica je slaba dva meseca po vseh razkritjih in začetku nadzornih postopkov v Veliki Britaniji prenehala obstajati. Facebook pa se še vedno sooča z zaslišanji na najvišjih političnih ravneh in s strani nadzornih organov; v Združenem Kraljestvu mu je bila, kot je bilo že omenjeno, izrečena kazen zaradi nezadostnega zagotavljanja preglednih informacij. Odkritja so sprožila val odzivov regulatorjev, nadzornih organov, mednarodnih organizacij, vladnih organov, parlamentarnih zaslišanj, akademskih prispevkov – večinoma ogorčenih nad načini izrabe osebnih podatkov uporabnikov elektronskih storitev za politične namene, v škodo demokratičnim procesom in svobodi. Kot piše Adams (2018), so razkritja vodila k spoznanju, da spletna družbena omrežja naše zgodovine, všečkov, sporočil, zasebnih fotografij in kontaktov ne uporabljajo le za to, da nam posredujejo ciljane oglase za gledališče in počitnice,

[28] Podrobneje v Prilogi G.

temveč tudi za to, da sooblikujejo naše dojemanje sveta in naša politična prepričanja, na način, da tega sploh ne opazimo. Pod vprašaj so postavila tudi monopolistične položaje glavnih spletnih velikanov, ki svoje poslovne modele temeljijo na izrabi podatkov uporabnikov, in načela vprašanje, ali jim res lahko zaupamo upravljanje tako velikih količin osebnih podatkov in kakšne so posledice (Adams, 2018) ter ali bi jih morali regulirati kot ponudnike kritične infrastrukture po vzoru drugih sektorjev (The Economist, 2018).

Mikro ciljanje v političnih kampanjah

Ugotovitve britanskega nadzornega organa za varstvo osebnih podatkov (Information Commissioner's Office – ICO) v primeru družbe Cambridge Analytica kažejo, da politične stranke in kampanje v Združenem kraljestvu in širše čedalje pogosteje uporabljajo osebne podatke in sofisticirane analitične metode za čim natančnejše ciljanje na volivce, po vzoru vedenjskega oglaševanja v komercialnem sektorju. Digitalne kampanje vključujejo različne organizacije v kompleksnem ekosistemu – politične stranke, organizacije, ki vodijo kampanje, spletne družbene medije, preprodajalce podatkov in ponudnike analitičnih storitev. Uporabljene metode ciljanja in obdelav osebnih podatkov pa niso pregledne, posamezniki jih ne razumejo, vprašanje je tudi, koliko so zakonite (ICO, 2018b, str. 3).

ICO je v tem ekosistemu poudaril zlasti odgovornost političnih strank, ki imajo v Združenem Kraljestvu dostop do zbirke podatkov o volivcih, volilnega registra, v katerem so imena, priimki in naslovi upravičenih volivcev. Vse politične stranke imajo tudi svoje podatkovne baze o svojih članih, simpatizerjih in drugih, ki lahko vključujejo raznolike podatke, pridobljene na različne načine: lahko jih pridobijo neposredno od posameznikov, prek e-pošte, telefona, osebno, lahko pa jih pridobijo od tretjih strani, npr. specializiranih družb za trženjske podatke, preprodajalcev podatkov in spletnih platform. Ti podatki so nato združeni in na podlagi analize je mogoče posameznikom pripisati posamezne atribute, npr. njihove odnose do nekaterih ključnih političnih vprašanj (npr. do splava, orožja, socialne politike, migracij ipd.). Te analize lahko opravi stranka sama, lahko pa za to najame specializiranega ponudnika na trgu (ICO, 2018b, str. 22–26).

Na podlagi izvedenih analiz, ki strankam pokažejo, kdo so posamezniki, na katere je »vredno« ciljati z določenimi sporočili ali z določenim tipom sporočila, je mogoče izvesti mikro ciljanje – bodisi na spletnih družbenih omrežjih, na katerih stranke lahko naložijo svoje

podatke o volivcih v platformo ponudnika, ta pa izvede primerjavo (npr. glede na e-naslov) in poišče člane svoje omrežja, ki jim politična stranka želi prikazati sporočila, ali pa zgradi občinstvo podobnih posameznikov, ki bi jih morda prav tako lahko ciljali s takimi sporočili; posameznikom so lahko oglasi prikazani na tretjih, partnerskih spletnih straneh; politične stranke lahko tudi točno določnim posameznikom pošljejo prilagojena sporočila po e-pošti ali navadni pošti, lahko jih celo obiščejo na naslovu (ICO, 2018b, str. 27).

Dejstvo je, da politično komuniciranje v prihodnosti na bo imuno na napredke pri obdelavi osebnih podatkov v okviru velikega podatkovja in na prednosti, ki jih prinaša umetna inteligenca. Podrobna segmentacija volivcev s profiliranjem omogoča, da se sporočilo prilagodi določenemu ozkemu segmentu volivcev, na katerega je mogoče vplivati, da se lahko spremeni izid volitev (t. i. neopredeljeni volivci, angl. *swing voters*) (Goodman in drugi, 2017). Ciljanje prek različnih naprav omogoča, da promocijsko sporočilo doseže volivca v času in kontekstu (in na napravi), ko je bolj dojemljiv za taka sporočila. V tem okviru je pomembno ciljanje glede na geolokacije uporabnikov (npr. udeležencev nekega dogodka ali shoda). Uporaba umetne inteligence za ciljanje, merjenje in izboljšave kampanj ter za samodejno ustvarjanje vsebin glede na profile posameznikov prinašajo neslutene možnosti vplivanja na volivce. Te sisteme je mogoče tudi zlorabiti za ustvarjanje lažnih in zavajajočih vsebin. S pomočjo analize npr. podatkov na spletnih družbenih omrežjih je mogoče identificirati tematike in vprašanja, glede katerih so volivci zaskrbljeni, ter njihov odnos do posameznih tem in tako predvidevati rezultate volitev. Dostava na novih platformah, kot so digitalni video, navidezna resničnost in nosljiva tehnika, je čedalje pomembnejša, predvsem za čustveno nabite vsebine, ki dosežejo posameznika v pravem trenutku in pravem okolju. Tudi podatki o gledanosti televizijskih programov na pametnih sprejemnikih že omogoča boljše ciljanje na televizijske sprejemnike (Demos, 2018, str. 27–37).

Mikro ciljanje političnih sporočil lahko pripomore k učinkovitejšemu nagovarjanju volivcev – glede tematik, ki so jim pomembne, in v formatu, ki je bližje njihovim potrebam in pričakovanjem. Tako se lahko poveča angažiranost volivcev in njihovo seznanjenost s političnimi tematikami ter zmanjša njihovo pasivizacijo. Za politične stranke lahko pomeni večjo učinkovitost, cenejšo komunikacijo ter možnosti doseganja skupin, ki so težko dosegljive (Zuiderveen Borgesius in drugi, 2018, str. 82, 92). Zgoraj opisani način uporabe vedenjskega mikro ciljanja v okviru poličnih kampanj in trendi uporabe tehnologije ter

podatkov v politiki pa prinašajo prenekatere izzive za pravice posameznikov, demokratične procese in družbo kot celoto. Veliko je špekulacij, koliko so te prakse pri prepričevanju volivcev dejansko učinkovite in koliko vplivajo na volilne izide, vendar pa lahko z gotovostjo trdimo, da na tem področju prihaja do velikih napredkov v znanju in tehnologiji, kar je z vidika političnih procesov zelo sporno (Cadwalladr, 2017). Politično mikro ciljanje časovno sovpada tudi z nedavnim pojavom oz. porastom pojava t. i. lažnih novic (angl. *fake news*), pri čemer se pojavlja vprašanje, koliko lažne novice dosežejo svojo vidnost tudi s pomočjo političnega mikro ciljanja, ki okrepi njihovo prisotnost v pravih segmentih volivcev, ki so jim (morda zaradi procesov kognitivne disonance) bolj pripravljeni verjeti in jih širiti dalje. Narayanan in Reisman (2017) pojav političnih kampanj, ki uporabljajo osebne podatke uporabnikov elektronskih komunikacij za mikro ciljanje sporočil volivcem, in prek spletnih oglasov ter vsebin sporočijo za odtenek drugačno sporočilo različnim posameznikom, povezujeta z resnim vplivom na politično sfero in posledicami za zdravo stanje demokracije (Narayanan in Reisman, 2017, str. 4).

2.3 Zakaj je vedenjsko oglaševanje in sledenje uporabnikom problematično?

Ker je oglaševanje največji, če ne celo nujni podpornik razmeroma brezplačne vsebine na internetu, kar najbolj koristi prav uporabnikom, se napredek pri ciljanju in osebni prilagoditvi vsebin običajno označuje kot velik napredek. Izboljša tudi uporabniško izkušnjo – vsebine in oglasi so postali za uporabnika relevantni in zanimivi. Tako uporabnik veliko hitreje in preprosteje najde vsebine in blago, ki ga zanima, prihrani čas in iskalne vire, lažje primerja produkte med seboj in lažje dobi informacije o posebnih ponudbah.

Spletni novičarski ponudniki se borijo z upadom sredstev zaradi padajočih naklad tiskanih edicij ob hkratnih pričakovanjih javnosti, da so novice in vsebine na spletu na voljo brezplačno. Z oglaševanjem spletni novičarski ponudniki pridobijo sredstva za ustvarjanje vsebine, ne da bi morala svoje uporabnike soočiti s plačljivim modelom dostopa do vsebin na spletu. Spletno oglaševanje je vir obstoja za manjše ponudnike vsebin na spletu, ki producirajo le specifično vsebino (npr. različne specializirane spletne strani o potovanjih ali konjičkih) in nimajo drugega vira prihodka, kot bi bila npr. prodaja izdelkov. S spletnim oglaševanjem lahko pridobijo vir sredstev, ki jim zagotavlja obstoj, oz. pokrijejo stroške ustvarjanja vsebine, gostovanja spletne strani in druge administracije. Podobna je usoda

marsikatere »brezplačne« spletne storitve ali mobilne aplikacije, ki se dejansko financira iz oglaševalskih prihodkov oziroma iz »prodaje« uporabniških podatkov za trženjske namene. Argument za uvedbo vedenjskega ciljanja na ravni ponudnikov dostopa do interneta poudarja nov dotok sredstev, ki jih operaterji nujno potrebujejo za dograjevanje in izboljševanje infrastrukture, ki je ni mogoče financirati zgolj z naročninami, da bi uporabnikom ponudili univerzalni dostop in kakovost storitev (OFCOM, 2008; LSE, 2009b).

Zelo pogosti so argumenti, da je sledenje uporabnikom za namen vedenjskega oglaševanja pravzaprav neškodljivo, saj naj bi bile to anonimne sledi uporabnikov, ki niso povezane z njihovo resnično identiteto, imenom in priimkom, ker naj bi bilo to pravzaprav sledenje napravi in ne uporabniku (Castelluccia in Narayanan, 2012, str. 10). Ti argumenti so bili z različnih vidikov že večkrat ovrženi:

- sledi so lahko de-anonimizirane in povezane s konkretnim posameznikom s pomočjo številnih metod: tretja stran, ki uporabniku sledi, je morda hkrati tudi prva stran, ki od istega uporabnika pridobi podatke s pomočjo registracije in tako identificira podatke (npr. Facebook sledi prek Facebookovega vtičnika za všečkanje in registriranih uporabnikov ter podatke med seboj poveže), nekatere prve stranke podatke o registriranih uporabnikih ponujajo v zameno za plačilo, včasih so identitete uporabnikov ukradene ali zlorabljene (Castelluccia in Narayanan, 2012, str. 10–11);
- čeprav uporabnik ni prepoznaven z resnično identiteto, temveč mu izvajalec vedenjskega oglaševanja sledi pod psevdonimom, identifikatorjem, to ne spremeni nobene od negativnih plati vedenjskega oglaševanja. Izvajalec je še vedno zmožen določiti posameznika in mu prikazati njemu prilagojen oglas, še vedno lahko pri tem posega v njegovo zasebnost, ga diskriminira ali z njim manipulira. Ime in priimek sta zgolj dva od identifikatorjev, prav tako identifikacijska številka ali oznaka, če je stalna in je mogoče posameznika dovolj natančno prepoznati, še natančneje kot z imenom in priimkom, kjer je pravzaprav veliko ljudi z enakimi nazivi (Narayanan in Reisman, 2017, str. 5; Zuiderveen Borgesius, 2016, str. 268);
- v tehničnem smislu je oglas sicer res dostavljen na napravo, vendar je namenjen posamezniku, ki napravo uporablja. Na koncu namreč ni naprava tista, ki kupi par rdečih čevljev (IWGDPT, 2013, str. 3).

Vedenjsko oglaševanje tako poraja številne pomisleke, ki izhajajo iz posega v zasebnost in varstvo osebnih podatkov posameznikov, pa tudi diskriminacije, ujetosti v »mehurčke«, ki ožijo posameznikovo zavedanje in posega v politične pravice. Pri vedenjskem oglaševanju na ravni operaterja pa tudi skrbi glede prestrezanja komunikacij in kršitve načela nevtralnosti omrežja. Problematika tako presega zgolj vprašanja zasebnosti uporabnikov in sega npr. na področje etičnosti uporabe zdravstvenih podatkov za trženje izdelkov, na področje diskriminacije posameznikov glede na njihove profile in na področje vpliva na demokratične procese, če je sledenje in profiliranje uporabljeno za promoviranje političnega kandidata posameznikom, ki bodo promocijska sporočila verjetneje dobro sprejeli (Zuiderveen Borgesius, 2014; EDPS, 2018).

Ena glavnih težav vedenjskega ciljanja je njegova nevidnost in (celo zaželena) prikritost, ki dovoljuje vpogled v uporabnikove zasebne aktivnosti. Velika večina uporabnikov se ne zaveda, da ponudniki storitev beležijo njihove aktivnosti in na podlagi tega zanje osebno prilagodijo vsebine. Dejstvo je, da izvajalci vedenjskega ciljanja lahko razločujejo med različnimi uporabniki, na podlagi unikatnih identifikatorjev oziroma odtisov njihovih naprav.

Največje težave vedenjskega oglaševanja z vidika obdelave osebnih podatkov uporabnikov so netransparentnost te aktivnosti, vprašanja privolitve uporabnika v sledenje in s tem povezane ustreznosti obvestila o sledenju, ter vprašanja ustreznega zavarovanja in hrambe podatkov, prav tako posredovanja za druge namene. Posebej je sporna uporaba občutljivih podatkov za oglaševanje ter zloraba zbranih podatkov za druge namene (CNIL, 2009; FTC, 2007; LSE, 2009b; WP29, 2010a). Ker uporabniki najpogosteje ne vedo, da se njihove aktivnosti beležijo in jih vsakodnevno profilira veliko spletnih in mobilnih ponudnikov storitev, zoper tako sledenje ne ukrepajo, niti običajno nimajo dovolj znanja, da bi sledenje preprečili, zlasti če vključuje bolj sofisticirane metode sledenja, kot so zgolj piškotki (Kamara in Kosta, 2016, str. 5).

Običajno je vedenjsko oglaševanje povezano s postopkom profiliranja, torej pripisovanja nekih lastnosti posameznikom glede na prej zbrane podatke, in obravnavo posameznika glede na profil, ki mu pripada. Pri vedenjskem oglaševanju je posamezniku prikazan oglas glede na profil, v katerega je bil uvrščen, npr. »zanimajo ga psi«. Za oblikovanje profila so lahko uporabljeni najrazličnejši podatki o vedenju na spletu, o ogledu video vsebin, rabi spletnih

družbenih medijev in nakupni podatki. Izvajalci te podatke pogosto povežejo tudi z drugimi, npr. demografskimi ali psihografskimi podatki. Bistvo je kombiniranje podatkov ter pripisovanje posameznih oznak ali vrednosti na podlagi analitičnih orodij in izdelanih algoritmov za analizo podatkov, npr. »ljubitelji nogometa«. Profili so lahko posamični, še bolj pogosto pa so skupinski in zajemajo posameznike, ki imajo skupne preference, lokacijo ali kaj drugega (konjičke, nakupe, interese itd.) (Kamara in Kosta, 2016, str. 3).

Profili uporabnikov so primarno namenjeni razlikovanju med posamezniki, kar lahko vodi v neželeno diskriminacijo (Zuiderveen Borgesius, 2016, str. 268), še zlasti kadar ta razlikuje na podlagi občutljivih situacij in podatkov, npr. zdravstvenih, kot je bilo že omenjeno zgoraj, ali pa podatkov o domnevni nacionalnosti. Diskriminacija na podlagi tako občutljivih kategorij, kot je spolna usmerjenost (če spletno družbeno omrežje nekomu stalno ponuja informacije za gejevske dogodke, pa se oseba nikdar ni sama opredelila kot istospolno usmerjena) ali invalidnost, zdravstveni statusi in etnično poreklo, je posebej problematična in odpira številne etične pomisleke, ne le pomisleke z vidika varstva osebnih podatkov. Posameznik lahko zaradi takih opredelitev čuti velike posledice v realnem življenju, pri iskanju službe, najemanju kreditov, zavarovanju, navsezadnje pa se lahko s temi informacijami neželeno seznanijo njegovi bližnji, ko npr. na pametnem televizijskem sprejemniku med predlogi za filme prevladuje npr. gejevska produkcija.

Kot poudarja Zuiderveen Borgesius (2016) množično zbiranje podatkov posameznikov o njihovih *online* aktivnostih, pa tudi navadah uporabe televizije, programih, ki jih gledajo, uporabi mobilnih naprav itd. lahko povzroči, da se pod grožnjo stalnega komercialnega nadzora začnejo drugače obnašati, ne želijo iskati informacij o boleznih, politiki ali drugih temah (Zuiderveen Borgesius, 2016, str. 268), da jih ta iskanja ne bi spravila v napačne profile, ki bi lahko, če bi te podatke npr. pridobila zavarovalnica ali banka, vodili v spremembo ponudbe zanje – višje premije za tiste, za katere obstajajo indikacije, da imajo kronično bolezen, slabši pogoji kredita za tiste, ki imajo radi nevarne športe. Internet uporabljamo za iskanje informacij, za opravljanje vsakodnevnih opravkov, družbeno interakcijo, zdravstvene namene, iskanje informacij o političnih temah in politično udejstvovanje – če je vsak klik nadzorovan in iz njega lahko izhajajo posledice za posameznika na nepredvidenih področjih (po načelu *all data is credit data*) (Aitken, 2017), lahko to pomeni velike omejitve za demokratično delovanje v družbi in osebno svobodo

posameznikov, predvsem občutek izgube zasebnosti, ki izhaja iz tega, da posamezniki ne vedo, katere informacije o njih se zbirajo, kako so uporabljene in s kom jih podjetja nadalje delijo (glej npr. EDPS, 2018).

Poleg tega množično zbiranje osebnih podatkov posameznikov samo po sebi prinaša tveganja, npr. glede zavarovanja podatkov pred nepooblaščenimi posegi vanje in glede vdorov v baze podatkov (Zuiderveen Borgesius, 2016, str. 268). Podatki o aktivnostih uporabnikov na spletu so lahko bogati, vsebujejo tudi občutljive kategorije, in so kot taki lahko zelo zanimivi za potencialne zlorabe in kraje, če seveda baze podatkov niso primerno zavarovane in dostopi do njih niso omejeni. Kot poudarja poročilo norveškega nadzornega organa za varstvo osebnih podatkov, je posebej za panogo programatičnega oglaševanja zadnjih let značilna velika netransparentnost toka podatkov med različnimi ponudniki na oglaševalskem trgu, na katerem so številni posredniki, ki s podatki trgujejo, jih obogatijo ali povezujejo z drugimi. Zato to panogo pogosto opisujejo z izrazom »črna skrinja« (Datatilsynet, 2015, str. 10), saj je pogosto popolnoma jasno le, katero spletno stran je uporabnik obiskal in kateri oglas mu je bil na koncu prikazan. V vmesnem procesu pa lahko nastopa tudi več deset različnih podjetij, ki posameznikove podatke prejmejo in jih obdelujejo. Veliko podjetij v tem ekosistemu izhaja iz ZDA, kjer zakonodaja o varstvu osebnih podatkov ni tako jasno določena in pogosto delujejo pod domnevo, da niti ne obdelujejo osebnih podatkov, ker npr. uporabnike zaznavajo na podlagi različnih identifikatorjev in ne npr. z imenom in priimkom. Podatkov tako ne obravnavajo kot osebnih in vprašljivo je, koliko jih ustrezno zavarujejo pred nepooblaščenim dostopom.

Norveški organ za varstvo osebnih podatkov tako poudarja, da je programatično oglaševanje običajno prikrito in netransparentno. Običajen uporabnik namreč nikakor ne razume obsega podatkovnih tokov, ker želi hiter in preprost dostop do storitev, samodejno pristane na pogoje uporabe storitve in je s tem prepuščen velikim in močnim igralcem na trgu. Veljavna privolitev pa bi morala pomeniti resnično izbiro in svobodno zavrnitev. Avtomatizacija prodaje in prikazovanja oglasov pomeni, da je zelo težko nadzorovati, kdo bo prikazal kakšen oglas in kje, ter kdo bo sledil uporabnikom posamezne spletne strani. Oglaševalska panoga ve o potrošnikih več kot katerakoli druga panoga, zato so potrošniki lahko izpostavljeni prikriti diskriminaciji in manipulaciji. Avtomatizirano oglaševanje, ki ga poganjajo algoritmi, lahko reproducira obstoječe predsodke in stereotipe. Podatki, ki jih obdeluje oglaševalska panoga,

lahko prihajajo iz najrazličnejših virov, lahko so bili zbrani za povsem drugačne začetne namene. Velike zbirke podatkov so bolj ranljive z vidika napadov in incidentov (Datatilsynet, 2015, str. 39–43).

Preglednost tokov podatkov uporabnika je tako zelo problematična, tako tudi omejitve glede nadaljnje rabe uporabnikovih podatkov za različne nepovezane namene, kot so npr. zgoraj omenjene zavarovalnice in banke, v tako bogatih podatkovnih zbirkah pa tudi organi pregona najdejo koristi zase. Kot poudarja Schneier (2013), je poslovni model interneta zgrajen na množičnem nadzoru, vladne obveščevalne službe pa postajajo zasvojene z možnostmi, ki jih ponujajo ti podatki. To po pomeni grožnjo za domnevo nedolžnosti in privilegij zoper samoobtožbo, prav tako pa omejuje svobodo izražanja, saj se posameznik mora samoomejiti, če bi lahko njegova aktivnost in spletu in mobilnih napravah kadarkoli prišla v roke organov pregona (Kamara in Kosta, 2016, str. 5).

Nič novega niso procesi razlikovanja cen produktov in storitev, ki so uporabnikom ponujene glede na profil, v katerega so bili uvrščeni. Prejšnji nakupi ali izkazani interesi lahko vplivajo na višino cene za posamezne produkte, čeprav je npr. drug uporabnik izkazal interes za enako količino in kakovost (Castelluccia in Narayanan, 2012). Znani so primeri spletnih trgovcev, ki so uporabnikom iz druge regije prikazovali drugačne cene, uporabnikom Applovih produktov višje cene, uporabnikom, ki so si večkrat ogledali posamezen produkt, višje cene, hkrati pa je težko dokazati, da so bile to namerne diskriminacije glede na značilnosti uporabnika in ne morda prodajne taktike, nepovezane z lastnostmi uporabnika. Z ekonomskega vidika ima razlikovanje cen seveda prednosti, hkrati pa se zdi nepravično in manipulativno. Predvsem je treba upoštevati, da bi moral biti uporabnik, če prilagajanje cene res temelji na beleženju njegovih osebnih podatkov, o tem obveščen in po evropski zakonodaji v to tudi vnaprej privoliti (Zuiderveen Borgesius, 2015, str. 268).

Posebej problematični so tudi vidiki natančnosti in kakovosti algoritmov, ki posameznike uvrstijo v določene profile ali jim pripišejo lastnosti. Znani so primeri aplikacij za zdrav življenjski slog, ki beležijo število korakov, aktivnosti, hrano, ki jo uporabnik je, itd. Na podlagi teh informacij uporabniku lahko pripišejo nevarnosti za posamezne bolezni in stanja, veliko vprašanje pa je, koliko so te odločitve pravilne, katere vhodne podatke upoštevajo, kakšen je proces odločanja, ki lahko na koncu na posameznika zelo vpliva, če npr. podatek o njegovi domnevni sladkorni bolezni prejme zavarovalnica.

Narayanan in Reisman (2017) poudarjata, da je pomemben del vedenjskega oglaševanja strojno učenje, oziroma koncepti, povezani z umetno inteligenco, in da se najprodornejši umi naše generacije ukvarjajo s tem, kako pripraviti ljudi, da kliknejo na oglase. Strojno učenje tukaj deluje tako, da s statističnimi metodami rudari po uporabniških podatkih, ki so v okviru velikega podatkovja (angl. *big data*) na voljo v čedalje večjih količinah. Avtomatizirano odločanje prinaša uporabniku številne koristi – od dobrih predlogov za filme na platformi za pretočne video vsebine Netflix do avtonomnih avtomobilov, vendar ima hkrati tudi tri pomembne negativne posledice:

1. posegi v zasebnost – strojno učenje omogočajo podatki uporabnikov in podatki o njih, pri čemer je težko napovedati, kdaj in v katerem primeru bodo ti podatki morda uporabljeni za popolnoma drugačen namen, kot je bilo že opisano zgoraj. To vodi v razvoj družbe »najprej zberi podatke in se potem vprašanj, kaj bi z njimi« in v družbo vseprisotnega nadzora;
2. rezultati strojnega učenja odslikavajo človeške predsodke, čeprav se pogosto naivno domneva, da so rezultati avtomatiziranega odločanja matematično čisti in popolni, odločitve pa brez predsodkov. Ker modele za strojno učenje oblikujejo ljudje, so v modele preneseni tudi vsi predsodki in napake, kar je posebej problematično, kadar je posamezniku na tej podlagi potencialno napačne odločitve povzročena škoda, ker je uvrščen v napačen profil glede na samodejno odločitev;
3. tretja negativna posledica pa je nezmožnost vpogleda v odločitve algoritmov umetne inteligence. Čeprav deluje na podlagi določenih pravil, se uči na ogromnem številu vhodnih podatkov in ko sprejme neko strojno naučeno odločitev, je praktično nemogoče ugotoviti, zakaj in kako je bila ta odločitev sprejeta. Če umetna inteligenca odloča o pravicah ljudi, so posledice lahko kafkovske.

Zato avtorja kličeta k javni razpravi o problematiki strojnega učenja in preglednosti algoritmov, ki nas obkrožajo v vsakodnevnem življenju (Narayanan in Reisman, 2017, str. 2–3).

To je posebej pomembno ob zavedanju, da razvoj zmožnosti in tehnologij sledenja čedalje bolj omogoča sledenje prek različnih naprav, kar pomeni, da je mogoče uporabnika prepoznati in mu slediti od njegovega telefona in jutranjega preverjanja e-pošte in novic, na službeno napravo in na prenosno napravo med počitnicami in ob koncih tedna. Pri tem uporabniki na službeni napravi pogosto ne razkrivajo svojih občutljivih podatkov, ampak za

zdravstvenimi podatki brskajo v zasebnosti svoje domače naprave ali pa morda na domači napravi ne pobrskajo za nečim, kar želijo skriti pred družino. Povezovanje vseh teh aktivnosti lahko vodi v neprijetne situacije za posameznika, ki mu je v nepričakovanem okolju prikazan neprimeren oglas (npr. za prstan, ki bi ga želel podariti ženi, na domačem računalniku, ali za zdravila za impotenco na službeni napravi), z večanjem nabora podatkov o uporabniku v različnih kontekstih pa se seveda krepijo tudi vse zgoraj naštete skrbi glede posegov v zasebnost, točnosti strojnih odločitev in diskriminacije posameznikov, še zlasti če vračunamo napake, ki lahko nastanejo, ker katero od naprav uporablja več uporabnikov v družini, podatki pa so nato pripisani eni osebi. V tem kontekstu se čedalje bolj pojavljajo tudi naprave interneta strani, npr. pametni števci električne energije, katerih podatki so lahko vir za ponudnike električne energije, da svojemu odjemalcu pošljejo posebno ponudbo za dražji paket. Pred kratkim je ameriški regulator FTC izdal poročilo, v katerem opisuje prednosti sledenja prek naprav, pa tudi slabosti, povezane s tem, da imajo uporabniki omejen nadzor nad temi praksami in omejeno znanje. Zato je pozval izvajalce, da uporabnike seznanjajo s praksami sledenja in jim ponudijo možnosti glede tega, kako jim sledijo, da pridobijo privolitev pred sledenjem o občutljivih temah in deljenjem natančnih informacij o geolokaciji ter vzdržujejo primerno stopnjo zavarovanja podatkov in se izogibajo nepričakovani sekundarni rabi zbranih podatkov (FTC, 2017).

Navsezadnje je osebna prilagoditev vsebin in storitev skrb vzbujajoča tudi z vidika oženja posameznikovega polja zavedanja, širine možnosti, ki so mu ponujene ob vsakodnevni uporabi elektronskih komunikacij, in iskanja informacij. Vsebine, ki so posamezniku ponujene, in oglasi, ki so mu prikazani, namreč temeljijo na profilu glede na njegove pretekle interese, kar pomeni, da se izgublja prostor za njegove ustvarjalne interese, da postaja zaprt v svoj »mehurček« (angl. *filter bubble*) (Pariser, 2011; Castelluccia in Narayanan, 2012, str. 13–14; Kamara in Kosta, 2016, str. 5). Nekomu, ki je izkazal interes za vrtnarstvo, bodo tako znova in znova prikazane take vsebine, ne pa npr. za navtiko, ki bi ga morda prav tako zanimala.

Še pred nekaj leti sta Castelluccia in Narayanan (2012, str. 14) zapisala, da je taka osebna prilagoditev lahko v bolj avtoritarnih režimih uporabljena tudi za cenzuriranje, tako da se posamezne novice prikažejo le določenim uporabnikom. Danes v okviru političnih kampanj že poteka politično mikro ciljanje na ozke segmente volivcev, opredeljene s pomočjo analize

podatkov o posameznikovih demografskih značilnostih ter potrošniških in življenjskih navadah (Gorton, 2016, str. 62). V primeru mikro ciljanja za politične namene s strani družbe Cambridge Analytica je bilo s strani nadzornega organa v Združenem kraljestvu poudarjeno kronično pomanjkanje informacij o obdelavi podatkov pri vseh udeležencih ekosistema, političnih strankah in spletnih platformah ter preprodajalcih podatkov, še zlasti ker gre za vprašanje poštene obdelave osebnih podatkov posameznikov iz volilnega registra pri mikro ciljanju teh volivcev na družabnih omrežjih (za kar je potreben vnos podatkov volilnega registra v platformo spletnega družbenega omrežja) in kombiniranje podatkov, dodatno pridobljenih od preprodajalcev podatkov. Uporabniki spletnih družbenih omrežij ob pomanjkanju informacij težko razumejo, kako in zakaj so podvrženi političnemu ciljanju posamezne politične stranke ali kampanje. Problematično je tudi ciljanje, ki vključuje občutljive kategorije podatkov ter pomanjkljive možnosti posameznika, da zavrne take obdelave osebnih podatkov oziroma upravlja možnosti. Problematika je precej širša od področja varstva osebnih podatkov in zadeva tudi vprašanja volilne zakonodaje in njenemu sledenju tehnološkim napredkom (ICO, 2018b, str. 28–47).

Tukaj je treba opozoriti, da so zgornje ugotovitve usmerjene le na vprašanja preglednosti in informiranosti volivcev o procesih obdelave osebnih podatkov za namen poličnega komuniciranja – sicer je informiranost eden od temeljev zakonitosti, pa vendar zakonodaja v Evropi, v nasprotju z ameriškim modelom urejanja obdelave osebnih podatkov, določa posebne omejitve v smislu omejenih dopustnih pravnih podlag za obdelavo podatkov. V okviru dejavnosti političnih strank bi bila to najverjetneje bodisi privolitev posameznika bodisi pa bi bile omejitve določene v zakonu, podlaga pa bi bila redko v zakonitem interesu (glej tudi Evropska komisija, 2018b, str. 3–4). Zelo verjetno je, da vsaj za postopke kombiniranja podatkov iz različnih virov, njihovega pridobivanja od posrednikov in posredovanja spletnim platformam ter spletnim družbenim omrežjem nobena od dopustnih podlag ne bi prišla v poštev. Kot ugotavlja ICO, posamezniki niso bili dovolj obveščeni, kar pomeni, da tudi njihove potencialno pridobljene privolitve najverjetneje niso veljavne, niti ni verjetno, da specifična volilna zakonodaja dovoljuje tako obdelavo osebnih podatkov. Tako kljub obširnim poročilom ICO o njihovih ugotovitvah ni jasno, kakšne pravne podlage naj bi bile v konkretnih primerih dopustne ter ali in kako naj bi bili akterji za nezakonito obdelavo sankcionirani. ICO sicer navaja, da so bile izrečene sankcije Facebooku in izdana opozorila političnim strankam – pa vendar predvsem zaradi nezadostne preglednosti, kar je mogoče

popraviti in tako zagotoviti skladnost z zakonom. Drugačno pa je vprašanje zakonitosti, če za obdelavo osebnih podatkov ni bila izkazana nobena od pravnih podlag. V takih primerih bi namreč subjekti tako obdelavo morali prenehati izvajati in podatke izbrisati. Tako daleč pa ICO v svojih dosedanjih prizadevanjih ne gre – najverjetneje v pragmatičnem duhu ne (pre)hudih omejitev za že vzpostavljene prakse. ICO napoveduje objavo dodatnih ugotovitev na tem področju, toda če bodo ostale le na ravni konceptov preglednosti, je veliko vprašanje, ali lahko taki ukrepi pomembno učinkujejo – v svetu, v katerem posamezniki nimajo zadostnega razumevanja kompleksnih obdelav podatkov, niti tega ni mogoče od njih realno pričakovati (kot je podrobneje pojasnjeno na več mestih te študije).

Tveganja političnega mikro ciljanja so večplastna in zadevajo:

- zasebnost volivcev – če bodo politične kampanje polno izrabljale vse možnosti obdelav podatkov in ciljanja, ki so na voljo v komercialnem sektorju, to pomeni veliko tveganje za zasebnost posameznikov, zlasti ker gre na tem področju pogosto za obdelavo podatkov glede politične pripadnosti in drugih občutljivih podatkov;
- privolitev in seznanjenost posameznikov – ker so sodobne obdelave osebnih podatkov za ciljanje zelo kompleksne, zlasti ko govorimo o ciljanju prek različnih naprav, v okviru interneta stvari in umetne inteligence, bodo posamezniki težko veljavno soglašali, saj bodo te procese zelo težko sploh razumeli;
- neprimerno profiliranje in sporočila – avtomatizirano ustvarjanje vsebine bi lahko postalo pomemben del političnih kampanj, saj bi lahko tako volivci prejeli osebno prilagojena sporočila – kar ni mogoče ob običajnem človeškem posredovanju. To bi lahko vodilo v neprimerna, netočna ali diskriminirajoča sporočila, kar bi odprlo vprašanja pravičnosti in bi lahko povečali nezaupanje v politične stranke;
- odgovornost – avtomatizirano ustvarjanje vsebine pomeni ogromne količine različnih osebno prilagojenih sporočil, ki odpirajo tudi vprašanja nadzora – kako bo mogoče shraniti in pregledati tako veliko količino dokumentov, npr. ali je vsebina neprimerna, diskriminirajoča itd. Odpirajo se vprašanja preglednosti in politične odgovornosti v kampanjah;
- čustvena manipulacija – psihografija ali širše ciljanje na podlagi analize čustev se bo s količino dostopnih podatkov izboljšalo, kar pa pomeni, da bodo lahko oglasna in politična sporočila dosegla posameznike v ranljivih trenutkih oziroma, ko bodo za to bolj dovzetni (tudi npr. depresivni, živčni ipd.), ter pri tem uporabljala čustven naboj

jeze, strahu ali predsodkov, kar pa lahko vodi v čustveno manipulacijo volivcev in v dolgoročne negativne učinke na stanje demokracije;

- konkurenca – prevladujoč položaj nekaterih ponudnikov na trgu *ad tech* (npr. Facebook in Google) pomeni tudi, da bodo najbrž čedalje pomembnejša orodja v političnih kampanjah, kar pomeni tveganje za pravičnost in legitimnost poličnih procesov ter zaupanje vanje;
- ustvarjanje novih oblik osebnih podatkov – na podlagi procesov umetne inteligence ter profiliranja na velikih podatkovnih setih je mogoče sklepati, koliko je npr. posameznika mogoče prepričati o nekem političnem sporočilu. Tu se odpirajo vprašanja preglednosti takega profiliranja in pravic posameznika, da v ta proces poseže, ga prepreči ali podatke popravi (Demos, 2018, str. 38–41).

Posledice podatkovne analitike za mikro ciljanje v političnem prostoru so dolgoročne, saj vplivajo na temeljne pravice posameznikov, njihovo pravico do zasebnosti in varstvo osebnih podatkov, pa tudi pravico do svobode govora in obveščenosti. Negativno vpliva na pluralnost medijev, na raznolikost dostopnih informacij in virov ter na pravico državljanov do svobodnih volitev, ki so pregledne, svobodne in poštene (EDPS, 2018, str. 12–13). Svobodne in poštene volitve pa so bistvo demokratične družbe, zato je ključno, da tudi v elektronskih komunikacijah veljajo enaka pravila, kot vežejo subjekte v političnih procesih v realnem svetu (ICO, 2018b, str. 11).

Če povzamemo, vedenjsko oglaševanje je najpogosteje povezano s postopki profiliranja posameznikov oz. uporabnikov elektronskih komunikacij, kar pomeni, da so posamezniku glede na njegovo zgodovino uporabe naprav in vsebin pripisane določene lastnosti, na podlagi katerih prejema temu ustrezne oglasne vsebine. Kot poudarja tudi Delovna skupina iz člena 29, ima profiliranje in avtomatizirano odločanje lahko velike prednosti za posameznike in organizacije, in sicer v smislu večje učinkovitosti (izvajanja storitev, pridobivanje informacij ipd.) ter prihranka virov. V komercialnem smislu je lahko koristno uporabljeno za boljšo segmentacijo trgov in za prilagajanje storitev posameznikovim potrebam, kar ni le prednost za marketinške aktivnosti, temveč tudi za optimizacije v transportu, medicini, izobraževanju, zdravstvu, bančništvu in na področju davkov, zavarovalništvu itd. (WP29, 2017a, str. 5).

Hkrati pa tehnološki hiter napredek in zmogljivosti na področju velikega podatkovja, umetne inteligence in strojnega učenja omogoča preprostejše, vendar obsežnejše profiliranje s potencialno precej resnejšimi posegi v pravice posameznika. Široka dostopnost osebnih podatkov na spletu ter z raznolikih naprav, povezanih v internet stvari, in povečane zmogljivosti iskanja korelacij in povezav med podatki omogočajo čedalje obsežnejšo analizo in napovedovanje posameznikovih interesov, navad in osebnostnih značilnosti, kar prinaša številna tveganja za njegove pravice (WP29, 2017a, str. 5–6). Ko je uporabljeno za namene politične promocije, pa ima lahko dolgoročne negativne posledice za stanje demokracije, saj posega v sam temelj demokratičnih procesov – v volitve, ki bi morale biti svobodne, poštene in pregledne, volivci pa ne podvrženi manipulaciji na podlagi prikritih postopkov analize njihovih aktivnosti, stanj, mnenj in nagnjenj (EDPS, 2018; Goodman in drugi, 2017; COE, 2018).

2.5 Vedenjsko oglaševanje in odnos uporabnikov

Raziskave o odnosu posameznikov do vedenjskega oglaševanja na splošno kažejo, da so posamezniki zaskrbljeni zaradi praks sledenja na spletu in da si želijo orodij, s katerimi bi se bilo mogoče temu izogniti. Hkrati se številni posamezniki ne zavedajo, kako oglaševanje na spletu poteka. McDonald (2011) v svoji študiji ugotavlja, da odnos posameznikov niha med podporo vedenjskemu oglaševanju in globokimi skrbmi glede tega, čeprav posamezniki na splošno razumejo, da oglaševalski prihodki večinoma zagotavljajo brezplačne vsebine na spletu. Čeprav situacijo razumejo, posameznike frustrira in jezi način, na katerega se vedenjsko oglaševanje izvaja, s prikritim zbiranjem zelo natančnih podatkov o vsakem posamezniku. Zasebnost je med pomisleki prva. Skoraj polovici se vedenjsko oglaševanje zdi srhljivo (angl. *creepy*) (McDonald, 2011). Podobne ugotovitve izhajajo tudi iz drugih raziskav na temo odnosa posameznikov do vedenjskega oglaševanja (npr. Anton, Earp in Young, 2009; Turow in drugi, 2009), iz česar sledi, da to vsekakor ne uživa nadpovprečnega razumevanja in podpore med uporabniki, ampak pri njih vzbuja številne pomisleke, predvsem glede zasebnosti.

Turow in drugi (2009) so ugotovili, da skoraj dve tretjini Američanov verjameta, da spletne strani, ki imajo izjavo o varovanju zasebnosti, ne smejo deliti podatkov o svojih uporabnikih z drugimi podjetji brez njihove privolitve. Prav tako je večina zmotno mislila, da morajo

ponudniki spletnih storitev uporabnike vprašati za dovoljenje, preden jim sledijo prek različnih spletnih strani. Dve tretjini uporabnikov v isti študiji ni želelo prejemati osebno prilagojenega oglaševanja, 84 odstotkov pa jih je zavračalo ciljano oglaševanje, ki temelji na analizi njihovega vedenja na spletu (Turow in drugi, 2009). McDonaldova in Cranorjeva sta leta 2010 v ZDA izvedli raziskavo, kaj uporabniki o vedenjskem oglaševanju vedo, in ugotovili, da je glede praks uporabe piškotkov in sledenja na spletu med uporabniki veliko zmede. Polovica uporabnikov je bila npr. prepričana, da njihova lokacija ne more biti identificirana, če ne sprejmejo piškotkov, in da piškotki vsebujejo vse informacije, odkar so kupili računalnik, vključno z njihovim imenom in domačim naslovom. Druge zmote so vključevale zmedo glede piškotkov in zgodovine brskanja, nevednost, ali blokiranje piškotkov ohranja zasebnost lokacije, in glede tega, katere podatke ščitijo politike zasebnosti (McDonald in Cranor, 2010).

Podobno so pozneje Van Noort, Smit in Voorveld (2013) raziskovali, kakšno znanje o vedenjskem oglaševanju imajo uporabniki na Nizozemskem ter kakšne so njihove skrbi glede zasebnosti na spletu in kako se z njimi spopadajo. Raziskava je nastala v času po spremembi pravil o piškotkih v EU. Pred raziskavo je bila v medijih živahna razprava o piškotkih, vedenjskem oglaševanju in zasebnosti, zaradi česar avtorji domnevajo, da bi uporabniki lahko imeli več znanja o teh aktivnostih. Avtorji menijo, da je znanje uporabnikov bistveno, če želimo, da je regulacija vedenjskega oglaševanja, ki temelji na informirani privolitvi, uspešna. Če naj uporabniki sami nadzorujejo deljenje svojih podatkov na spletu, morajo te prakse tudi razumeti. Avtorje je zanimalo, kaj uporabniki vedo o vedenjskem oglaševanju, koliko jih skrbi njihova zasebnost na spletu, kako se odzivajo oz. spopadajo z vedenjskim oglaševanjem in kako pristopiti k različnim uporabnikom v zvezi z regulacijo vedenjskega oglaševanja. Ugotovili so, da tudi uporabniki na Nizozemskem, čeprav je bila tema vedenjskega oglaševanja medijsko neposredno pred raziskavo zelo odmevna, nimajo zadostnega znanja in razumevanja vedenjskega oglaševanja. V vzorcu so bili pretežno zelo pogosti uporabniki interneta, zaradi česar avtorji domnevajo, da je v splošni populaciji zavedanje in znanje še nižje. Največkrat so uporabniki zmotno menili, da je organizacijam prepovedano zbirati podatke o spletnih aktivnostih uporabnikov interneta. Prav tako so zmotno menili, da piškotki shranjujejo zgodovino brskanja, da so vezani na osebo in da računalniki delajo počasneje, če piškotki niso pravilno odstranjeni. Povprečno so uporabniki pravilno odgovorili na štiri od osmih vprašanj glede delovanja piškotkov in pet od osmih trditev glede vedenjskega

oglaševanja. Vprašanje je, ali je regulacija na podlagi informirane privolitve, učinkovita, če uporabniki evidentno nimajo zadostnega znanja, ki je edino lahko temelj privolitve (Van Noort, Smit in Voorveld, 2013, str. 18–20).

Skrb uporabnikov za njihovo zasebnost na spletu razkrivajo pravzaprav vse raziskave na to temo v zadnjem času. Uporabniki so predvsem zaskrbljeni, kaj podjetja o njih vedo in kako te podatke uporabljajo (Phelps, Nowak in Ferrel, 2000). Več kot polovici ni prijetno oglaševanje na podlagi njihove zgodovine brskanja, čeprav ta ne bi bila povezana z njihovim imenom ali drugimi osebnimi podatki (TRUSTe, 2012). Van Noort in drugi (2013) skladno s tem ugotavljajo, da tudi uporabniki v njihovi študiji izražajo nadpovprečno zaskrbljenost nad varstvom zasebnosti na spletu, še zlasti glede zlorabe njihovih osebnih podatkov. Prav tako v povprečju gojijo negativne občutke do praks vedenjskega oglaševanja. Še posebej negativno so se odzvali na trditev, da nadzor nad uporabo spleta pomeni poseg v zasebnost (Van Noort in drugi, 2013, str. 19)

Van Noort in drugi (2013) načine, na katere se uporabniki spopadajo z vedenjskim oglaševanjem, delijo na dve strategiji. Uporabniki se spopadajo z odzivom ali z izogibanjem. Odziv vključuje branje politik zasebnosti in nameščanje programske opreme za izogibanje grožnjam zasebnosti. Izogibanje pa vključuje dejavnosti, s katerimi uporabniki preprečujejo, da bi se na njihove naprave naložili piškotki, ki omogočajo sledenje, torej blokiranje ali sprejem samo določenih piškotkov. Alternativni model izogibanja bi vključeval plačevanje za vsebino, namesto prejemanja oglasov in sledenja (Van Noort in drugi, 2013, str. 16).

V svoji raziskavi ugotavljajo, da se uporabniki spopadajo z ohranjanjem zasebnosti na spletu s preverjanjem škodljivih kod, z blokiranjem pojavnih oken in s čiščenjem zgodovine obiskov spletnih strani. Najmanjkrat se zaščitijo z branjem politik zasebnosti, kar je za avtorje zanimivo, saj trenutna regulacija piškotkov temelji na branju izjav o varovanju zasebnosti. Po tem, ko je bila uporabnikom pojasnjena nova zakonodaja in kaj pomeni, je tretjina menila, da ne bi sprejeli nobenega piškotka, nadaljnja tretjina pa je bila pripravljena sprejeti le lastne piškotke spletne strani, ki so jo obiskali. Le 10 odstotkov jih je bilo pripravljenih sprejeti vse piškotke, tudi tiste od tretjih strani. Glede na tip spletne strani so bili prej pripravljeni sprejeti piškotke na novičarskih straneh, pri ponudnikih e-pošte, spletnih družbenih omrežjih in iskalnikih, kot na spletnih straneh podjetij in organizacij. Rezultat je skladen z ugotovitvijo,

da imajo uporabniki kljub vedenjskemu oglaševanju še vedno raje, da so storitve na novičarskih portalih in glasbenih spletnih straneh brezplačne in za te vsebine niso pripravljeni plačevati (Van Noort in drugi, 2013, str. 20).

Van Noort in drugi (2013) tudi domnevajo, da bi bilo treba za uspešno regulacijo vedenjskega oglaševanja pristopiti k različnim uporabnikom na različne načine. To utemeljujejo na raziskavah v preteklosti, ki so pokazale, da zasebnost bolj skrbi ženske, nižje izobražene in take z manj dohodka (Fogel in Nehmad, 2009, v: Van Noort in drugi, 2013, str. 17). Glede vpliva starosti so bili rezultati v preteklosti nejasni.

Van Noort in drugi (2013) v svoji raziskavi ugotavljajo, da se uporabniki glede na stopnjo zaskrbljenosti glede zasebnosti na spletu delijo v tri skupine. Skoraj polovica jih je zelo zaskrbljenih, imeli so najnižjo stopnjo znanja o vedenjskem oglaševanju in piškotkih, hkrati pa so imeli najbolj negativno mnenje o tem oglaševanju. Najbolj so bili tudi aktivni pri zaščiti zasebnosti, toda morda bolj iz strahu kot na podlagi znanja. Med njimi je bilo več žensk, nižje izobraženih in z nižjim prihodkom, kar je skladno prejšnjimi raziskavami, hkrati pa so bili v tej skupini starejši uporabniki. V skupini, ki je bila najmanj zaskrbljena za zasebnost, je bilo približno 10 odstotkov uporabnikov, ki niso imeli negativnega mnenja o vedenjskem oglaševanju. Največ so tudi vedeli o takem oglaševanju in piškotkih, čeprav tudi ti niso imeli popolnega znanja. Avtorji menijo, da bi se ustvarjalci politik in regulatorji morali najbolj usmeriti k skupini najbolj zaskrbljenih, saj je teh največ, poleg tega pa imajo najbolj pomanjkljivo zunanje in hkrati najbolj negativen odnos do sledenja na spletu. Učinkovitost privolitve kot orodja regulacije je pri tej skupini najbolj vprašljiva. Najbolj je avtorje presenetilo to, da uporabniki niso bili pripravljeni brati izjav o zasebnosti, čeprav so bili glede zasebnosti zelo zaskrbljeni. Morebiten razlog iščejo v načinu uporabe interneta, kjer uporabnik hkrati opravlja več nalog, pri tem pa mu je lažje samo klikniti na izbiro, kot pa obvestilo o piškotkih dejansko prebrati (Van Noort in drugi, 2013, str. 20).

Van Noort, Smit in Voorveld (2013) še dodajajo, da so besedila večine obvestil o piškotkih nejasni. Prav tako ni jasno, ali običajna obvestila sploh nagovorijo uporabnike v smislu njihovih skrbi za zasebnost, ali uporabniki besedila sploh razumejo. Avtorji tukaj vidijo priložnost, da bi obvestila jasno odgovarjala na konkretne skrbi glede zasebnosti, ki jih imajo uporabniki, in bi tako postala razumljivejša (Van Noort in drugi, 2013, str. 20).

Študija Evrobarometer prav tako razkriva, da sta dve tretjini sodelujočih (67 odstotkov) zaskrbljeni, da nimajo popolnega nadzora nad svojimi informacijami na spletu. Večini (53 odstotkov) je neprijetno ob spletnem digitalnem oglaševanju in profiliranju, od teh 17 odstotkom zelo neprijetno. Poročilo kaže, da posamezniki nimajo dovolj znanja o vedenjskem oglaševanju, njegovem delovanju in namenih. Ker nimajo znanja, se pred vedenjskim oglaševanjem ne morejo zaščititi, čeprav jim je ponujena možnost zavrnitve sodelovanja (angl. *opt-out*) (Evropska komisija, 2015).

Tudi raziskave ameriškega Pew Research Centra kažejo, da imajo Američani nizko stopnjo zaupanja v organizacije z dejavnostjo zbiranja podatkov in nadzorovanja, tako v javnem kot tudi v zasebnem sektorju. Kljub temu le redki uporabljajo napredne nastavitve za varovanje zasebnosti. Ne glede na to pa večina meni, da bi morale obstajati časovne omejitve hrambe podatkov o njihovih aktivnostih in komunikacijah. Glede zaupanja organizacijam, da bodo njihove podatke ohranjale zasebne in zavarovane, 76 odstotkov vprašanih ne zaupa spletnim oglaševalcem, 69 odstotkov ne zaupa družabnim omrežjem, 66 odstotkov ne zaupa iskalnikom in prav toliko ponudnikom video storitev. Kar nekaj uporabnikov uporablja preprostejše načine izogibanja posegom v zasebnost: 59 odstotkov jih briše zgodovino iskanj in piškotkov, 57 odstotkov je že zavrnilo posredovanje osebnih podatkov, če to ni bilo relevantno za transakcijo, 25 odstotkov jih uporablja začasni e-naslov, 24 odstotkov podaja lažne informacije o sebi, 23 odstotkov se je odločilo, da ne bodo uporabljali spletne storitve, ker zahteva resnično ime (Pew Reasearch Center, 2015).

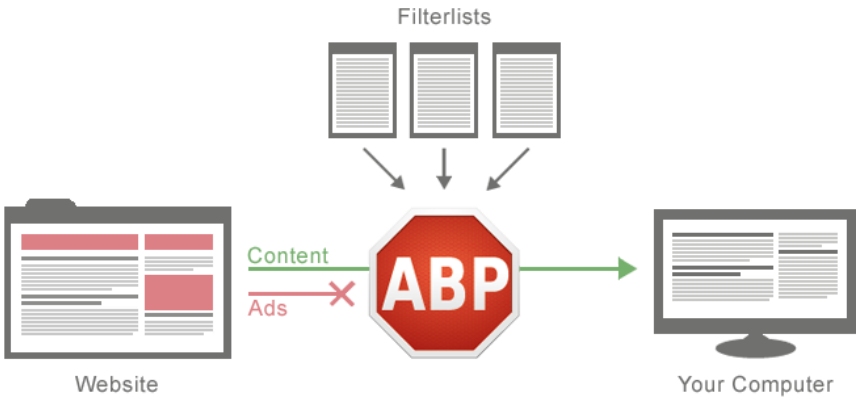
Čeprav je veliko Američanov pripravljenih deliti osebne podatke v zameno za otipljivo korist, so ob tem pogosto previdni in nezadovoljni glede tega, kaj se s podatki nato dogaja. Raziskava kaže, da je odnos vprašanih do zasebnosti oziroma razkritja pogosto ambivalenten in različen v različnih kontekstih, vpliv ima zaupanje, ki ga čutijo do podjetja ali organizacije, ki podatke zbira, ali podatke posreduje tretjim in koliko časa hrani podatke. Široko zaznavna je zaskrbljenost pred neželeno pošto in hekerji ter želje po varovanju podatkov o lokaciji na mobilnem telefonu. Profiliranje tisti, ki so zaskrbljeni glede varstva podatkov, opisujejo kot »strašljivo«, »veliki brat« in »zalezovanje« (Pew Research Center, 2016).

Na podlagi različnih raziskav podobno ugotavlja tudi Acquisti (2014), in sicer da na posameznikovo zaskrbljenost glede zasebnosti vplivajo številni dejavniki in konteksti. Tako ti

izvajajo številne mentalne kalkulacije, ko se odločajo med razkrivanjem in varovanjem informacij. Ugotovljene so bile tudi razlike med zatrjevanimi stališči do zasebnosti in resničnim razkrivanjem informacij o sebi, kar kaže na paradoks – ljudje si želijo zasebnosti, nočejo pa plačati zanjo in so pripravljeni razkriti svoje podatke že za majhne nagrade. Dodatno na odločitve vpliva zaznavanje in poznavanje tveganj, povezanih z zasebnostjo. Acquisti (2014) je odločitve posameznikov glede zasebnosti preučeval z vidika vedenjske ekonomike.

V zadnjih letih čedalje bolj narašča uporaba tehničnih orodij, ki blokirajo oglase oziroma sledenje, na podlagi katerega so prikazani oglasi (protireklamni vtičniki oz. angl. *adblockers*). Protireklamne vtičnike uporabniki namestijo na svojo napravo (računalnik ali mobilno napravo). Kot kažejo raziskave, se za to odločijo iz različnih razlogov – da izboljšajo delovanje spletnih strani (hitrost nalaganja) ali pa zaradi varovanja zasebnosti in zaščite proti zlonamerni kodi (Nithyanand in drugi, 2016, str. 1). Slika 2.5 predstavlja delovanje blokade oglasov. Na spletni strani se prikaže le vsebina, ne pa tudi oglasi. Ponudniki oglasnih vsebin so blokirani na podlagi posebnega seznama, filtrov.

Slika 2.5: Blokiranje oglasov



Vir: Adblockplus (2019)

Število posameznikov z nameščenimi protireklamnimi vtičniki lahko v nekaterih starostnih skupinah zraste tudi do 30 odstotkov (Ahmad, 2019), kar za oglaševalsko panogo pomeni veliko izgubo, saj spletni ekosistem temelji na monetizaciji s pomočjo izrabe podatkov uporabnikov in oglaševanja. Oglaševalska panoga se odziva z razvojem in uporabo orodij, ki

zaznajo uporabnikovo blokiranje oglasov in ga skušajo od tega odvrniti ali blokado tehnično obiti. Zakonska skladnost takih rešitev je vprašljiva (Nithyanand in drugi, 2016).

2.5 Pravno ozadje in prvi poskusi regulacije vedenjskega oglaševanja

Pravno ozadje za regulacijo vedenjskega oglaševanja je danes precej raznoliko. Zaradi različnih pristopov k regulaciji, ki so še vedno večinoma na ravni pogajanj in dogovarjanj, je na tem področju veliko trenj. Eno glavnih vprašanj je še vedno privolitev posameznika v sledenje in vedenjsko ciljanje ter obveščanje posameznikov o tem. Panoga vedenjskega oglaševanja večinoma deluje po načelu naknadne zavrnitve sledenja (angl. *opt out*) oziroma po načelu domnevne vnaprejšnje privolitve (angl. *opt in*), kar se je v praksi izkazalo kot neučinkovito glede varstva pravic posameznika. Sledenje je večinoma prikrit proces, uporabniki večinoma niti ne vedo, da se dogaja, niso poučeni o delovanju sledenja in oglaševanja ter ne znajo izrabiti možnosti zavrnite ko oz. če jim je sploh ponujena.

Večina najpomembnejših akterjev s področja vedenjskega oglaševanja prihaja iz ZDA in je močno prisotna na evropskem trgu. Pravni okvir v ZDA je tako zelo pomemben tudi za evropske državljane, saj so ponudniki iz ZDA primarno zavezani tamkajšnji zakonodaji.[29] Hkrati pa evropska zakonodaja deloma sega tudi onkraj državnih meja in naj bi jo upoštevala tudi podjetja iz ZDA, kadar ponujajo storitve državljanom v EU ali spremljajo njihovo vedenje (Uredba 2016/679, 2016, 5. člen). Pravna sistema sta zelo različna in veliko je še nejasnosti. ZDA zagovarja samoregulacijo, Evropa pa si je izbrala pristop regulacije z zakonodajo, ki jo lahko dopolnjuje samoregulacija (WP29, 2010a; Kroes, 2010).

EU je leta 2009 s spremembo Direktive 2002/58/ES o zasebnosti v elektronskih komunikacijah določila, da mora oglaševalska panoga pridobiti vnaprejšnjo privolitev uporabnikov, preden na njihovo opremo shrani piškotek ali podobno sredstvo, s katerim bi zbirala podatke o njihovem vedenju (5(3). člen). Sprememba Direktive 2002/58/ES je povzročila veliko negodovanje pri ponudnikih storitev (IAB Europe, 2010b), ki so oblikovali samoregulacijski kodeks, ki temelji na obvestilu uporabnikom in na posebni spletni strani, na kateri lahko izrazijo svoje nestrinjanje glede sledenja za namen vedenjskega oglaševanja

[29] Nekatere pomanjkljivosti pravne ureditve v ZDA so: sledenje otrokom ni posebej prepovedano, izvajanje vedenjskega oglaševanja s strani ponudnikov dostopa do interneta ni posebej opredeljeno itd.

(EASA, 2011). Evropski nadzorni organi za varstvo osebnih podatkov so kodeks označili za neskladen s spremenjeno Direktivo 2002/58/ES, ki izrecno zahteva vnaprejšnjo privolitev posameznikov (WP29, 2011). Od maja 2018 se v EU uporablja Uredba 2016/679 o varstvu osebnih podatkov, ki uvaja strožja pravila glede profiliranja in hkrati določa, da lahko neposredno trženje pomeni zakoniti interes upravljavca osebnih podatkov (Burnik, 2016a). Januarja 2017 je bil predstavljen tudi predlog Uredbe o zasebnosti v elektronskih komunikacijah, ki naj bi nadomestila veljavno Direktivo 2002/58/ES (WP29, 2017d; EDPS, 2017). Na ravni EU torej na področju vedenjskega oglaševanja prevladuje strategija pravil in nadzora (po Baldwin in Cave, 1999), pri čemer zakonodaja vsebuje razmeroma natančna pravila glede izvajanja vedenjskega oglaševanja (glede uporabe piškotkov, obdelave osebnih podatkov, njihove hrambe, zavarovanja ipd.), kljub temu pa so v različnih državah članicah prisotne razlike na ravni nadzora nad tem pravili in na ravni njihove razlage (WP29, 2015b).

Na področju vedenjskega oglaševanja so ključni nadzorni organi na področju zasebnosti in varstva osebnih podatkov, glede na pravni sistem v posamezni državi.[30] V EU ima vsaka država članica neodvisen nadzorni organ za varstvo osebnih podatkov (v Sloveniji je to Informacijski pooblaščenec RS). Pravno varstvo pravic posameznikov je v skladu s temi pravili urejeno tudi na sodni ravni. Posebno vlogo v evropskem sistemu ima Evropski nadzornik za varstvo osebnih podatkov. Evropski nadzorni organi formalno in neformalno sodelujejo v okviru Evropskega odbora za varstvo podatkov (naslednika Delovne skupine iz člena 29), ki skrbi za enotno razlago in implementacijo pravic v vseh državah članicah. Vsi ti organi so aktivni tudi pri pripravi priporočil o politikah na področju tehnološkega napredka, ki zadeva obdelavo osebnih podatkov, profiliranje in umetno inteligenco, ter ponujajo obsežno zbirko mnenj in priporočil za nadzorne organe, subjekte, ki obdelujejo osebne podatke in posameznike, državljane.

Ameriški pravni okvir za varstvo osebnih podatkov ne pozna splošnega pravnega akta, ki bi bil veljaven horizontalno v vseh sektorjih. Tako so v ZDA le določena področja urejena s posebnimi akti,[31] Zvezna komisija za trgovino je regulator, ki se bori proti nepoštenim poslovnim praksam, tudi kršitvam pravice do zasebnosti. Oglaševanje na internetu je primarno prepuščeno samoregulaciji (Department of Commerce, 2010a; FTC, 2007; NAI,

[30] Za podroben pregled o nadzornih organih globalno glej Wright, David in Paul DeHert (2016).
[31] Npr. Communications Act, ki določa varovanje zasebnosti v telekomunikacijskem sektorju, ipd. (Department of Commerce, 2010a).

2008). Temelj samoregulacijskega kodeksa za vedenjsko oglaševanje je načelo naknadne zavrnitve, najpomembnejši argument pa izobraževanje uporabnikov, da bodo znali izrabiti svoje pravice in uveljavljati svojo izbiro. Do danes so spodleteli vsi poskusi urejanja pravice do zasebnosti na spletu na zakonodajni zvezni ravni (Singer, 2016), so pa nastali nekateri zakoni po vzoru evropske zakonodaje v posameznih zveznih državah (npr. v Kaliforniji). Ameriški regulator FTC je zelo aktiven na ravni raziskovanja in podajanja priporočil. Prav tako ni zanemarljiva praksa regulatorja, ki sicer z zelo ozkega vidika nepoštenih praks zajema veliko primerov varovanja zasebnosti s strani ponudnikov elektronskih storitev (npr. Moriarty, 2017). V ZDA prevladuje prepričanje, da je samoregulacija zaradi svoje prožnosti bolj primarna pot kot način regulacije v EU, ki naj bi premalo poudarjal obveščenost in izobraževanje potrošnikov. Ti se lahko sami odločijo, kaj od panoge želijo (Department of Commerce, 2010b). Ali imajo trenutno uporabniki informacijskih tehnologij dovolj znanja in sploh zavedanja, da bi uspešno izvajali svojo pravico do naknadne zavrnitve sledenja, pa je vprašanje, ki budi dvom v uspešnost ZDA modela regulacije (Boucher Ferguson, 2008).

V ZDA na področju reguliranja vedenjskega oglaševanja torej prevladujejo predvsem pravila razkritja informacij (po Baldwin in Cave, 1999), za katera organizacije odgovarjajo, v smislu zavajanja potrošnikov, če jih ne spoštujejo. Številna podjetja tako objavljajo svoje politike zasebnosti oz. izjave o zasebnosti, ki so nastale kot odgovor na skrbi uporabnikov glede njihove zasebnosti oziroma kot odziv na zakonodajne zapovedi. Pogosto so izjave o zasebnosti težko razumljive in je za njihovo razumevanje potrebna visokošolska izobrazba (Sherman, 2008; Anton in drugi, 2008). Čedalje več raziskav tudi kaže, da uporabniki izjav o zasebnosti pogosto ne berejo (Milne in Culnan, 2004) ali pa izjave ne naslovijo najpogostejših skrbi potrošnikov (Earp in drugi, 2005; Pollach, 2007). Na spletu so pogosti tudi različni kazalci, znaki, pečati, certifikati, s katerimi želijo ponudniki povečati preglednost informacij in graditi zaupanje potrošnikov. Kljub temu pa raziskave kažejo, da prisotnost kazalca za varovanje zasebnosti ne pomeni nujno, da ponudniki spletnih storitev dejansko imajo zasebnosti prijazne prakse (Moores, 2005). Poleg tega je vprašljivo, koliko uporabniki znake sploh prepoznajo oz. vedo, kaj pomenijo. Moores (2005) npr. ugotavlja, da je 15 odstotkov uporabnikov v njegovi raziskavi zatrdilo, da prepoznajo izmišljen pečat zasebnosti, ki je bil ustvarjen izključno za potrebe raziskave. Hkrati pa je resnične pečate prepoznala le dobra četrtina sodelujočih (Moores, 2005).

Za področje regulacije vedenjskega oglaševanja so pomembni tudi dosežki na področju standardizacije, in sicer predvsem razvoj standarda »ne-sledi« (angl. *do-not-track standard*). Z nastavitvijo v brskalniku bi uporabnik sporočal ponudnikom storitev v elektronskih komunikacijah, naj mu ne sledijo. Razvoj standarda je prevzel World Wide Web Consortium (v nadaljevanju W3C),[32] ki pri reševanju ključnih tem razvoja elektronskih komunikacij združuje regulatorje, teoretike in panogo iz vsega sveta (Fontana, 2012). Leta 2017 je bil standard po dolgih letih bojev za različne razlage tehnično pravzaprav dokončan, hkrati pa obstajajo različne možnosti njegove izvedbe – kot rešitev *opt-in* ali *opt-out*, kar pomeni, da bo izvedba sicer enotnega standarda na koncu različna. Kaj to pomeni za uporabnike in njihovo uporabniško izkušnjo, je veliko vprašanje. Dejstvo je tudi, da ga panoga (še) ne uporablja (Zuiderveen Borgesius in McDonald, 2015).

Možnosti regulatornih posegov zaradi neželenih posledic uporabe vedenjskega oglaševanja za namen političnega mikro ciljanja se v Evropi kažejo na različnih področjih: temeljno prek zakonodaje s področja varovanja osebnih podatkov in zasebnosti v elektronskih komunikacijah (o čemer podrobneje v poglavju o analizi pravnega okvira), pa vendar to ni edino področje:

- možnosti regulacije so tudi na področju pravil o avdiovizualnih medijskih storitvah (ki jih ureja evropska Direktiva 2010/13/EU o avdiovizualnih medijskih storitvah[33]) ter na področju nacionalnih zakonodaj glede nepristranosti pri poročanju s strani javnih RTV servisov, glede volilnega molka in glede časovnih okvirov, namenjenih posameznim kandidatom na volitvah. Podobne zahteve bi lahko veljale tudi za netradicionalne medije. Evropski nadzornik za varstvo podatkov (EDPS) poudarja, da bi lahko obstajala tudi pravila o transparentnosti algoritmičnega predvidevanja;
- volilna zakonodaja je še eno od področij, ki lahko pripomore k večji preglednosti političnega ciljanja, predvsem prek jasnih podatkov o financiranju kampanj in o sredstvih, namenjenih posameznim podatkovnim storitvam;
- pravo varovanja potrošnikov opolnomoči potrošnike v situacijah, v katerih so šibkejša stranka, kar je nedvomno res tudi v odnosu do sodobnih ponudnikov

[32] *World Wide Web Consortium* (W3C) je mednarodna skupnost, ki razvija odprtokodne standarde za namen dolgoročnega razvoja interneta.
[33] Direktiva 2010/13/EU Evropskega parlamenta in Sveta z dne 10. marca 2010 o usklajevanju nekaterih zakonov in drugih predpisov držav članic o opravljanju avdiovizualnih medijskih storitev

spletnih storitev. Evropska Direktiva 2005/29/ES o nepoštenih poslovnih praksah[34] prepoveduje zavajajoče, agresivne ali drugače nepoštene poslovne prakse, ne velja pa za politično komunikacijo; pa vendar so na področju komercialnega in nekomercialnega vedenjskega ciljanja zelo podobne nepoštene prakse;

- s pravom varstva konkurence bi lahko posegli v primeru združitev na trgu ponudnikov elektronskih storitev, ki lahko zlorabljajo svoj prevladujoči položaj, predvsem pa bi tako posredovanje imelo vlogo v kontekstu spletnih velikanov (EDPS, 2018, str. 16–17).

ICO v tem smislu denimo poziva tudi k »etičnem postanku«, da bi lahko ključni igralci na političnem področju (vlada, parlament, regulatorji, politične stranke, spletne platforme in državljani) razmislili o svojih odgovornostih glede uporabe osebnih podatkov posameznikov za namene političnih kampanj, preden se trendi obdelav velikega podatkovja še bolj nenadzorovano razširijo. Tako poudarja tudi priporočila glede politik obdelave osebnih podatkov v političnih kampanjah,[35] ki napeljujejo na to, da uspešna zajezitev škodljivih praks ni stvar enega samega pristopa regulacije in nikakor ni rešljiva le z zakonodajnimi ukrepi, s prepovedmi in nadzorom. ICO pomembno vlogo pripisuje koregulaciji, torej predpisanim kodeksom za politično oglaševanje, in sodelovanju med različnimi organi, pristojnimi na tem področju, in hkratnem sodelovanju s strankami. Omenja vlogo revizij s strani tretjih strank in odgovornosti ponudnikov storitev za vedenjsko oglaševanje, da prilagodijo svoje ukrepe za transparentnost in svojim strankam proaktivno pomagajo. Vlogo pripisuje opolnomočenju posameznikov in spodbudam etičnega ravnanja ter široki javni razpravi o vlogi političnega oglaševanja ter slabostih za demokracijo in družbo. Podobna so tudi priporočila Evropskega nadzornika za varstvo podatkov, ki poudarjajo sodelovanje organov s področja varstva osebnih podatkov, varuhov konkurence, volilnih komisij, varuhov potrošniških pravic, pa tudi regulatorjev na področju elektronskih komunikacij, ki skrbijo za pravilno delovanje javnih RTV servisov in avdio-vizualnih del.[36] Da so posledice mikro ciljanja na političnem področju zelo resne, saj to vpliva na poštene demokratične procese, opozarja tudi Evropska komisija in poudarja, da bi morali organi za varstvo osebnih podatkov to težo posledic upoštevati pri izreku sankcij.

[34] Direktiva Evropskega parlamenta in Sveta 2005/29/ES z dne 11. maja 2005 o nepoštenih poslovnih praksah podjetij v razmerju do potrošnikov na notranjem trgu ter o spremembi Direktive Sveta 84/450/EGS, direktiv Evropskega parlamenta in Sveta 97/7/ES, 98/27/ES in 2002/65/ES ter Uredbe (ES) št. 2006/2004 Evropskega parlamenta in Sveta

[35] Glej Prilogo H.

[36] Glej Prilogo I.

Trenutne strategije regulacije vedenjskega oglaševanja so torej raznolike, vendar med seboj slabo povezane in pod črto precej neučinkovite, kar izhaja iz cvetoče panoge vedenjskega oglaševanja, ki se širi in diverzificira na vse naprave, ki so zmožne povezovanja v splet. Posameznik je lahko stalno nadzorovan prek različnih lokacij, zmožnosti komercialne izrabe vedenjskega oglaševanja pa je začela uporabljati tudi politika. Kljub negativnim posledicam, ki jih ima vedenjsko oglaševanje na različne pravice posameznikov in družbo, regulacijskim organom do danes ni uspelo ustvariti jasne obrambe pred škodljivimi posledicami.

2.6 Ključne točke pregleda literature s področja vedenjskega oglaševanja

Razvoj vedenjskega oglaševanja in orodij za njegovo urejanje odpira številna vprašanja, zaradi katerih je potreben poglobljen akademski vpogled v predmet raziskave, ki bo omogočil celostno razumevanje problematike in konceptualno domišljene predloge izboljšav za prihodnost. Kot je pokazal pregled literature in specifičnih primerov izvajanja vedenjskega oglaševanja, so podatki posameznikov gorivo današnjih najuspešnejših panog in poslovnih modelov. Možnosti obdelave najrazličnejših podatkov – od demografskih pa do podatkov o vedenju in stališčih, občutljivih osebnih podatkov in lokacij – se nezadržno širijo, predvsem ob upoštevanju razmaha uporabe mobilnih naprav in naprav, povezanih v internet stvari (WP29, 2014b). Sofisticirane tehnike analize podatkov in kombiniranja za organizacije pomenijo čedalje bolj ključen vir njihovih prihodkov v najširšem smislu, saj omogočajo izboljšave produktov in storitev, inovacije in širitev kroga uporabnikov, še zlasti, če je mogoče povezati prej ločene zbirke podatkov (Katayev 2015). Stalno se izpopolnjujejo možnosti natančnega ciljanja oglaševanja na posameznika, in sicer na podlagi njegovega naslova IP, lokacije in podatkov o uporabi spleta in podatkov, zbranih z njegovih drugih naprav in senzorjev. Trženje ni več omejeno le na posamezno področje ali platformo, temveč je mogoče posamezniku slediti prek različnih naprav in mu na različnih napravah in v različnih okoljih tudi prikazovati oglase (Demos, 2018, str. 13).

Ob teh razvojnih gibanjih je zrastel nov sektor podjetij, ki delujejo na področju zbiranja, analize in posredovanja podatkov ter omogočajo organizacijam – svojim strankam – boljšo izrabo potenciala podatkov, ki so jim na voljo (so jih npr. pridobili od svojih strank) in ki jih lahko dodatno pridobijo (kupijo) od različnih takih posrednikov. V podatkovni panogi so tako

bistven sektor preprodajalci podatkov (FTC, 2014; Crain, 2016) in tudi oglaševalski posredniki – *ad tech* panoga in ponudniki storitev, ki jim je na voljo veliko podatkov lastnih uporabnikov (npr. spletna družbena omrežja, Google itd.) in ki lahko omogočijo posreden dostop oglaševalcev do njih (Datatylsinet, 2015; Van Alsenoy in drugi, 2015). Ta trg ponudnikov raste, najuspešnejši ponudniki – spletni velikani pa imajo skoraj monopolne položaje. Na drugi strani poslovni modeli spletnih medijev in ponudnikov vsebin, ki nimajo lastne podatkovne storitve in lastnega oglaševalskega sistema, trpijo in imajo težave s financiranjem. Trženje v elektronskih komunikacijah se čedalje bolj avtomatizira in temelji na sistemih za dražbo uporabniških profilov v realnem času, strojno ustvarjanje pa se seli tudi na področje vsebine. Segmentacija občinstev za trženje je čedalje ožja in natančnejša, in sicer glede na velike količine podatkov, ki so na voljo (Busch, 2016; Aksu in drugi, 2018). Najpomembnejša globalna igralca na trgu digitalnega oglaševanja, Facebook in Google, ponujata orodja za zelo preprosto, vendar tudi zelo natančno ciljanje na njune uporabnike, tako da oglaševalec podatke o svojih strankah uvozi v njune sisteme, kjer se kombinirajo z obstoječimi in tako omogočajo veliko natančnejše ciljanje.

Nove možnosti analiz podatkov, ki temeljijo na umetni inteligenci, strojnem učenju in drugih podobnih algoritmih, omogočajo pridobivanje zelo specifičnih podatkov prek sklepanja iz neobčutljivih podatkov ali celo na videz neosebnih podatkov, in nadaljnje profiliranje posameznikov, ki zaradi prikritosti takih postopkov ne morejo učinkovito posredovati. Sofisticirani načini analize kombinacije podatkov iz različnih virov pomenijo globlji vpogled v situacijo posameznika čez čas in prostor in omogočajo funkcionalne prednosti, hkrati pa so zelo resen izziv za zasebnost posameznika, saj omogočajo razkritja in sklepanja glede zelo intimnih situacij. Zaradi kompleksnega sistema obdelave podatkov ter nepredvidljivosti virov, iz katerih so lahko pridobljeni, je posamezniku situacijo težko razumeti in posledično veljavno soglašati oziroma nadzorovati obdelavo svojih podatkov (Demos, 2018, str. 1–7). Politično področje ni imuno na napredek v podatkovnem trženju. Volitve namreč postajajo čedalje bolj podprte s podatkovnimi storitvami, ki jih za politične stranke izvajajo specializirana podjetja in analitiki podatkov, in so usmerjeni v sofisticirano razčlenitev volivcev in vedenjsko ciljanje političnih sporočil – mikro ciljanje. Tehnologije in tehnike za to temeljijo na tistih razvitih v običajnem okolju trženja produktov in storitve. Politične kampanje kombinirajo svoje podatke o volivcih in njihovem vedenju s komercialnimi podatki, pridobljenimi od ponudnikov teh storitev na trgu, da lahko zgradijo natančnejše profile

volivcev. Največ sredstev za digitalno promocijo trenutno prejme Facebook. Cveti tudi trg specializiranih podatkovnih storitev, namenjenih političnemu kontekstu[37] (EDPS, 2018; Goodman in drugi, 2017; COE, 2017).

Ključni izzivi uporabe novih tehnologij obdelave podatkov v političnih kampanjah so posegi v zasebnost volivcev, težavno vprašanje privolitev in seznanjenosti posameznikov, potencialno neprimerno profiliranje in netočna ali diskriminirajoča sporočila, vprašanja odgovornost in nadzora nad izvajalci, preglednosti in politične odgovornosti v kampanjah. Poudarjene so nevarnosti čustvene manipulacije ob uporabi psihografije ali ciljanja na podlagi analize čustev, vpliva prevladujočega položaja nekaterih ponudnikov na trgu *ad tech* (npr. Facebook in Google) ter vprašanja ustvarjanja novih oblik osebnih podatkov na podlagi procesov umetne inteligence ter profiliranja na velikih podatkovnih setih (Demos, 2018, str. 38–41). Mikro ciljanje tako posega v več temeljnih pravic posameznikov in bistvo demokratičnega procesa: v pravico do zasebnosti in varstva osebnih podatkov, pravico do informiranja in obveščenosti, saj je na tnalu zagotavljanje medijske pluralnosti ter v pravico do svobodnih volitev, ki bi morale biti poštene in transparentne (EDPS, 2018). Čeprav je odnos z volivci za demokratični proces bistven in lahko sofisticirane analize podatkov pri tem pomagajo, imajo volivci vsekakor pravico pričakovati, da so pri takih analizah spoštovane njihove pravice in pravo. Brez preglednosti in zakonitosti takih praks lahko nastane škoda za zaupanje volivcev v pošten volilni sistem in demokratične procese (ICO, 2018b, str. 9). V tem kontekstu nekateri poudarjajo, da ni rešitev le omejevanje tehnologije na račun strožjega varstva pravic posameznikov. Pravica do zasebnosti ni cilj sama po sebi, ampak je pravica, ki posameznikom omogoča uveljavljanje svojih interesov (ICO, 2016, str. 3). Panoga vedenjskega oglaševanja je prepredena z izzivi in različnimi pogledi na urejanje področja v prihodnosti, da bi lahko zagotovili njene prednosti, toda hkrati varovali posameznika in družbo pred neželenimi posledicami.

[37] Npr. NationBuilder.

3 TEORETSKI OKVIR RAZISKAVE IN RAZISKOVALNA VPRAŠANJA

V tem poglavju je predstavljen teoretski okvir za raziskovanje pojava vedenjskega oglaševanja. Z multi-teoretskim pristopom (angl. *multi-teory approach*) pojasnjujemo vedenjsko oglaševanje, njegove posledice in vprašanja regulacije na več ravneh problematike (angl. *multi-level*). Različne teoretske tradicije in pristopi vsaka posebej in skupno prispevajo ključne gradnike teoretskega okvira, v katerem je mogoče iskati odgovore na raziskovalna vprašanja in pojasnjevati problematiko vedenjskega oglaševanja na mikro, srednji in makro ravni (glej npr. Frynas in Stephens, 2014, str. 485). Pregled literature s področja vedenjskega oglaševanja je pokazal pomanjkanje teoretsko utemeljenih virov, ki bi problematiko osvetlili v vsej njeni širini in z vseh vidikov. Vedenjsko oglaševanje je temelj poslovnih modelov večine danes najbolj priljubljenih storitev v elektronskem komuniciranju, ki so čedalje bolj neločljivo povezane z vsakdanjimi aktivnostmi posameznikov in nujne za pomenljivo participacijo v družbenih in demokratičnih procesih (glej npr. Zuiderveen Borgesius, 2016, 2012; Tran in drugi, 2014; Kamara in Kosta, 2016, Burnik 2013). Ker so uporabnikom običajno na voljo brezplačno, prihodek za ponudnika izvira iz oglaševanja na podlagi podatkov uporabnikov storitve. Vedenjsko oglaševanje je tako eden ključnih pojavov današnjega sveta, s kritičnimi posledicami za družbo in demokratične procese, zaradi katerih ga ne bi smeli obravnavati parcialno, npr. le v okviru tržnega komuniciranja, saj s tem spregledamo številne razsežnosti, ki pa so med seboj neločljivo povezane. Vedenjsko oglaševanje odpira dileme glede posega v zasebnost posameznikov in posledične diskriminacije ter oženja izbir, ki so na voljo posamezniku. Ker izvajalci vedenjskega oglaševanja pogosto nastopajo kot vratarji do vsebin, ki so nam na voljo, so prisotne tudi dileme glede etike, odprtosti in demokratičnosti interneta ter vpliva osebne prilagoditve vsebin na posameznika ter posegov v demokratične procese in politične pravice.

S pomočjo pregleda literature so bili identificirani teoretski pristopi, ki bi bili lahko temelj za razlago problematike vedenjskega oglaševanja in njegove regulacije zaradi negativnih posledic na več ravneh (npr. Frynas in Stephens, 2014, str. 485; Bies in drugi, 2007). Na mikro ravni nas zanima, kako vedenjsko oglaševanje zadeva posameznika in kakšne so njegove možnosti odzivov ter kako ga varuje oziroma bi ga v prihodnje lahko varovala regulacija. Na srednji ravni nas zanima ekosistem vedenjskega oglaševanja oziroma različni deležniki v njem (oglaševalska panoga, založniki, oglaševalci), kaj zanje vedenjsko

oglaševanje pomeni in kako se zanje uporabi regulacija. Na makro ravni pa nas problematika vedenjskega oglaševanja zanima z vidika širše politične, ekonomske in družbene dinamike (po Frynas in Stephens, 2014, str. 485).

Ker vedenjsko oglaševanje pojasnjuje le malo teoretsko utemeljenih virov, smo k iskanju teoretskih pristopov, ki bi pojav lahko pojasnili z več vidikov, pristopili širše in se osredinili na vire s področja elektronskih medijev, novih komunikacijskih tehnologij, interneta, oglaševanja v elektronskih medijih itd. S pomočjo pregleda smo izluščili različne teorije, ki so posebej pomembne za pojasnjevanje raznolikih vidikov vedenjskega oglaševanja, pri čemer nobena sama po sebi ne ponuja zadostnega pojasnila za vse vidike obravnavane tematike v smislu celostnega teoretskega temelja, ampak se med seboj dopolnjujejo v multi-teoretskem pristopu. Pregled literature je pokazal na pomembnost teorij tržnega komuniciranja, študij medijske potrošnje, pristopa politične ekonomije, normativne teorije, teorije informacijske zasebnosti in vedenjske ekonomije ter pristopa družbene odgovornosti, s po močjo katerih odkrivamo vedenjsko oglaševanje, njegove posledice za posameznika, oglaševalski ekosistem in družbo ter s tem povezana vprašanja regulacije. V nadaljevanju sledi pregled izbranih teoretskih pristopov, povezanih s problematiko vedenjskega oglaševanja, poudarjeni so vidiki, ki jih specifično pojasnjuje vsak posamezen teoretski pristop in pomanjkljivosti, ki jih posamezen pristop ne pojasnjuje, ampak je potrebno kombiniranje z drugimi. Poglavje se konča s sintezo večteoretskega pristopa.

3.1 Pogled na vedenjsko oglaševanje, njegovo delovanje in učinkovitost skozi tržno komuniciranje in kritično perspektivo alternativnih pristopov

Ko se v iskanju odgovora na vprašanje, kako učinkovito je pravzaprav vedenjsko oglaševanje in kakšne so njegove posledice za posameznike, podjetja, oglaševalce, izdajatelje ter širšo družbo, obrnemo k literaturi s področja tržnega komuniciranja, celostnega odgovora ne najdemo. Vedenjsko oglaševanje je novo orodje tržnega komuniciranja, toda literatura ga redko obravnava celostno, predvsem so prispevki osredotočeni na posamezne pojave (npr. Kang, 2011; Stallworth, 2010; Person, 2010; Goldfarb in Tucker, 2010b). Na temo oglaševanja v elektronskem komuniciranju najdemo raziskave o učinkovitosti specifičnih možnosti oglaševanja na internetu, npr. o učinkovitosti oglasov v primerjavi s sponzoriranimi povezavami, kjer ugotovitve kažejo večjo učinkovitost sponzoriranih povezav (Tutaj in van

Reijmersdal, 2012) ali o učinkovitosti kontekstualno umeščenih oglasov v primerjavi z vpadljivimi oglasi (Goldfarb in Tucker, 2010a), kjer se avtorja dotakneta tudi pomislekov glede zasebnosti, ki negativno vplivajo na učinkovitost spletnega oglaševanja. Velik poudarek je na raziskavah spletnih družbenih omrežij, na učinkovitosti virusnega trženja (npr. Petrescu in Korgaonkar, 2011). Tucker (2011) v raziskavi o osebno prilagojenem oglaševanju na omrežju Facebook preučuje učinkovitost takega oglaševanja tudi z vidika spremembe mehanizmov za varovanje zasebnosti na spletnem družbenem omrežju. Vedenjsko ciljanje avtorji pojasnjujejo skozi prizmo odziva uporabnikov na osebno prilagojeno vsebino in na sledenje (Kim, 2010; Person, 2010). Pariser (2011) ponudi širši pogled na problematiko osebne prilagoditve vsebin. Ogromne količine informacij, ki jih ne moremo več predelati sami, so botrovale nastanku novih struktur moči, ki na podlagi analize naših želja filtrirajo informacije in jih osebno prilagodijo (najbolj sofisticiran primer je Google), to pa oži polje posameznikovega delovanja, saj so mu vsebine onkraj njegovih zabeleženih preferenc in aktivnosti vse manj dosegljive (Pariser, 2011; Woo, 2006, str. 957).

Vedenjsko oglaševanje naj bi imelo velik potencial v smislu učinkovitosti oglaševanja in spletnih poslovnih modelov. Z dobrim poznavanjem uporabnika je mogoče natančneje in učinkoviteje ciljati, hkrati pa zaradi svoje razmeroma prikrite narave in spremljanja uporabnika vedenjsko oglaševanje odpira številne pomisleke glede njegovih pravic in etike. Kritično raziskovanje tematike je zato v okviru teorije in prakse oglaševanja zelo relevantno. Nekatere etične dileme sicer niso novost. Oglaševanje je tako pogosto vsiljena komunikacija, ki lahko zajema neetične prakse (npr. kontroverzni izdelki, prikrito oglaševanje, zavajajoče trditve ipd.). Kot tako je oglaševanje stalna tarča kritike, produkt katere je natančna regulacija celotne panoge, od samoregulacije pa do zakonodaje, ki jasno zapoveduje določene standarde (Jančič, 1999). Nov izziv pri vedenjskem oglaševanju je predvsem edinstveno invaziven poseg v zasebnost in pravice posameznika, ki ga oglaševalec spremlja, da bi ugotovil, kakšne vsebine mu ponuditi. To izvajalcu omogočajo sodobne tehnologije, ki so močno vpete v naš vsakdanjik in komuniciranje.

3.1.1 Prednosti vedenjskega in programatičnega digitalnega oglaševanja

Vedenjsko oglaševanje je razmeroma mlad pojav in na temo njegove učinkovitosti še ni popolnoma enoznačnih odgovorov. Študija Interactive Advetising Bureu (IAB) v sodelovanju s Harvard Business School je že leta 2013 pokazala, da polovica ekonomske vrednosti interneta temelji na zbiranju podatkov posameznikov, in da skoraj vsa vsebina na internetu deloma temelji na oglaševanju. Vložki v digitalno oglaševanje pa so v zadnjih letih že presegli vložke v oglaševanje na televiziji (Kafka in Molla, 2017).

Na učinkovitost vedenjskega oglaševanja lahko gledamo z različnih vidikov, npr. z vidika t. i. oglaševalske navlake (angl. *advertising clutter*), kar je posebej uporabno v kontekstu spletnega oglaševanja. Oglaševalska navlaka se nanaša na pojav velike količine neuredniških vsebin v medijih. Ker se mediji financirajo z oglasi, to lahko pomeni velike količne oglaševalskih vsebin na enem kraju – ko ta preseže raven, pri kateri potrošnik oglaševanje še sprejema, je označeno kot navlaka oziroma neželen pojav, tako za oglaševalce kot tudi za potrošnike (Ha, 1996, v Ha in McCann, 2008, str. 570). V tem smislu teorija preobremenitve (angl. *overload theory*) pojasnjuje, zakaj navlaka zmanjšuje učinkovitost oglaševanja, saj imajo posamezniki omejene zmožnosti za predelavo informacij. Ko so soočeni s preveč oglasi ob istem času, predelava enega dela informacij poteka na škodo drugega dela (Schneider in drugi, 1984).

Podobna je argumentacija v okviru teorije selektivne zaznave, ki pojasnjuje, da je selektivno zaznavanje objektov varovalni mehanizem, ki ga ljudje uporabljajo, da so zmožni usmeriti svoje omejene vire pozornosti glede na svoje potrebe (Smith in Buchholz, 1991). Odločitve potrošnikov, da niso pozorni na oglase, so tako rezultat njihovega dojemanja oglasov kot nerelevantnih glede na njihovo življenje in so njihovi viri namenjeni uredniškim vsebinam (Ha in McCann, 2008, str. 574). Model verjetne vpletenosti (angl. *elaboration likelihood model*) tudi opredeljuje, da je učinkovitost oglaševanja odvisna od vpletenosti posameznika v oglaševan produkt. Če je posameznik zelo vpleten v oglaševan produkt, ko je izpostavljen oglasu, je zelo verjetno, da bo namenil veliko truda v obdelavo sporočila in nadaljnje elaboriranje idej v sporočilu. Nasprotno pa, če ni vpleten v produkt, oglaševalsko sporočilo obdela prek periferne poti in imajo večjo težo dejavniki, kot je barva. V okviru oglaševalske navlake je tako zelo pomembna izvedba oglaševanja, ki dobro izrablja uporabo perifernih

dejavnikov, saj si posameznik le take oglase zapomni (Ha, 1999, v Ha in McCann, 2008, str. 574). Apliciranje teh ugotovitev na vedenjsko oglaševanje kaže, da njegova učinkovitost izhaja iz moči premagovanja ovir oglaševalske navlake, saj mu kljub njihovih selektivnim omejitvam uspe pritegniti pozornost potrošnikov. Pozornost pritegne, ker so oglasi za posameznika glede na njegove interese in želje relevantni ter ker ga dosežejo v primernem času in na primernem kraju, ko je njegova pozornost bolj usmerjena ali dostopna sporočilu oglasa. V osebno prilagojene vsebine je posameznik bolj vpleten in tako je verjetnejša tudi možnost, da bo trud usmeril v obdelavo sporočila oglasa.

Picker (2009) tako trdi, da ciljano oglaševanje zmanjšuje stroške iskanja in je tako za uporabnika koristno. Izboljša tudi uporabniško izkušnjo – vsebine in oglasi so postali za uporabnika relevantni in zanimivi. Tako uporabnik veliko hitreje in preprosteje najde vsebine in blago, ki ga zanima, prihrani čas in iskalne vire (Picker, 2009). Lažje primerja produkte med seboj in lažje dobi informacije o posebnih ponudbah. Beales (2010) je npr. analiziral podatke iz spletnih oglaševalskih mrež in ugotovil, da so cene in pretvorba v nakupno vedenje pri vedenjskem oglaševanju več kot dvakrat višje kot pri tradicionalnem oglaševanju na spletu (Beales, 2010).

Spletno oglaševanje je vir obstoja za manjše ponudnike vsebin na spletu, ki producirajo le specifično vsebino (npr. različne specializirane spletne strani o potovanjih, konjičkih itd.) in nimajo drugega vira prihodka, kot bi bila npr. prodaja svojih izdelkov. S spletnim oglaševanjem lahko pridobijo vir sredstev, ki jim zagotavlja obstoj oziroma pokrije stroške ustvarjanja vsebine, gostovanja spletne strani in druge administrativne stroške. Podobna je usoda marsikatere »brezplačne« spletne storitve ali mobilne aplikacije, ki se dejansko financira iz oglaševalskih prihodkov oziroma iz »prodaje« uporabniških podatkov za trženjske namene. Manjšim založnikom je uporaba sistemov za vedenjsko oglaševanje velikih ponudnikov preprostejša kot neposredno iskanje oglaševalcev za njihove razmeroma neznane storitve. Prav tako z uporabo teh sistemov prostor na spletni strani lahko učinkoviteje oddajo tudi spletne strani, ki težko neposredno oddajo prostor. Spletni novičarski ponudniki se borijo z upadom sredstev zaradi padajočih naklad tiskanih edicij ob hkratnih velikih pričakovanjih javnosti, da so novice in vsebine na spletu na voljo brezplačno. Z oglaševanjem spletni novičarski ponudniki pridobijo sredstva za ustvarjanje vsebine, ne da bi morala svoje uporabnike soočiti s plačljivim modelom dostopa do vsebin na spletu.

V zadnjih letih se dogaja pospešen prehod na popolnoma avtomatizirane načine prikazovanja oglasov v elektronskih medijih, na spletnih straneh, pametnih telefonih, tudi v okviru interneta stvari, ki temeljijo na obširni analizi uporabniških podatkov z uporabo strojnega učenja in umetne inteligence (t. i. programatično oglaševanje). Kot poudarjajo različni avtorji, je potencial učinkovitosti takega oglaševanja neprimerljiv, saj je mogoče posameznika doseči z relevantno informacijo v realnem času in primernem kontekstu, kar poveča možnost posameznikovega angažmaja v smislu nakupnega vedenja (npr. Seitz in Zorn, 2016; Busch, 2016; Aksu in drugi, 2018).

3.1.2 Kritični pogled na vrednost vedenjskega oglaševanja za oglaševalce

Za celostno obravnavo vedenjskega oglaševanja ni dovolj le odkrivanje njegovih funkcionalnosti in ekonomskih prednosti, ampak je potrebno tudi aktivno odkrivanje in odzivanje na njegove potencialne negativne vplive. S tega vidika lahko vedenjsko oglaševanje dojemamo kot še eno od oblik oglaševanja, ki zaradi invazivnosti kliče po omejevalnih ukrepih. Regulacija oglaševanja je ena ključnih tematik tržnega komuniciranja, saj deluje na temelju vzpostavljanja zaupanja potrošnikov v prakse oglaševalcev. Zaupanje oziroma »pristanek potrošnika« (Jančič, 1999, str. 958) pa je za učinkovitost oglaševanja ključno.

Raziskave kažejo tudi na to, da niti ekonomska slika koristi vedenjskega oglaševanja ni tako enoznačna. Chen in Stallaert (2014) sta avtorja ene prvih akademskih raziskav, ki podrobneje odkriva ekonomske posledice vedenjskega oglaševanja na spletu. Njun cilj je bil analizirati, kako vedenjsko oglaševanje vpliva na prihodke izdajateljev (torej na cene, ki jih za najem oglasnega prostora zaračunajo oglaševalcem) in prihodke oglaševalcev ter na družbeno blaginjo. Pri analizi izdajateljevih prihodkov vedenjsko oglaševanje primerjata s tradicionalnim oglaševanjem na spletu, ki deluje po sistemu dražbe. Najboljši ponudnik, tj. oglaševalec zakupi oglaševalski prostor pri izdajatelju za določeno ceno in tako lahko prikaže oglas nediferencirani skupini uporabnikov. Pri vedenjskem oglaševanju pa je oglas prikazan le posameznemu uporabniku. Izdajatelj tako oglaševalcem dejansko ponuja produkt – uporabnika. Zgodnja predvidevanja glede učinkovitosti vedenjskega oglaševanja so sledila preprosti logiki: ker obstaja večja verjetnost, da bodo uporabniki kliknili na oglase, bodo izdajatelji lahko za oglaševalski prostor zaračunali več. Chen in Stallaert (2014) ugotavljata,

da to razmerje med ceno in kliki na dražbi oglasnega prostora ne nastane nujno, ampak je možnih več situacij in rezultatov. Vedenjsko oglaševanje ima podoben učinek kot različnost produktov in posledično je možno, da oglaševalci za prostor plačajo manj, kot bi v primeru tradicionalnega zakupa oglaševalskega prostora. Ker se manj oglaševalcev fokusira na posameznega uporabnika, je večja možnost, da imajo ti oglaševalci manjšo možnost, da bo ta konkreten uporabnik kliknil na oglas, kar na koncu najboljšemu ponudniku omogoči, da plača za oglaševalski prostor manj. Avtorja to imenujeta tekmovalni učinek vedenjskega oglaševanja, ki lahko negativno vpliva na prihodke izdajatelja, saj niža dohodek od klika uporabnika na oglas (Chen in Stallaert, 2014). Nadaljnje raziskave so prav tako pokazale, koliko so oglaševalci pripravljeni plačati za posamezen ogled oglasa s strani posameznika v sistemu programatičnega oglaševanja po sistemu dražbe uporabniških profilov v realnem času (RTB) in kako se ta vrednost razlikuje v različnih državah na svetu. Predvsem so cene za posamezen ogled precej nizke (Tran in drugi, 2014).

Po drugi strani pa Chen in Stallaert (2014) ugotavljata, da ta negativni učinek lahko preseže pozitivne učinke tega, da je posamezniku oglas prilagojen in je tako večja možnost, da ga bo zanimal, kar pomeni povečanje verjetnosti za to, da bo uporabnik kliknil na oglas, to pa pomeni večjo pričakovano količino klikov (angl. *propensity effect*), kar pozitivno vpliva na prihodek izdajateljev. Ali bo izdajatelj z omogočanjem vedenjskega oglaševanja imel korist, je torej odvisno od tega, ali učinek nagnjenosti prevlada nad negativnim učnikom konkurence. To se zgodi predvsem takrat, ko za isti oglasni prostor tekmuje več oglaševalcev, ki so med seboj primerljivi, in ko so uporabniki heterogeni. V tem primeru se prihodek izdajatelja v primerjavi s tradicionalnim načinom oglaševanja lahko podvoji. Za majhne izdajatelje, ki nimajo veliko povpraševanja po svojem oglasnem prostoru, pa je torej tradicionalno oglaševanje boljša izbira. Še zlasti zato, ker vzpostavitev sistema za vedenjsko oglaševanje prinaša dodatne stroške, že brez teh pa njim glede na analizo vedenjsko oglaševanje ne bi prineslo novih prihodkov. Veliki založniki imajo z vedenjskim oglaševanjem možnost podvojiti prihodke v primerjavi s tradicionalnim oglaševanjem. Ti imajo prav tako veliko oglaševalskih virov in lahko za priljubljene oglaševalce uporabijo tehnologijo vedenjskega oglaševanja, za manj priljubljene pa tradicionalnega.[38] Pri analizi situacije za oglaševalce avtorja ugotavljata, da je vpliv vedenjskega oglaševanja na njihove dohodke asimetričen. Manjši oglaševalci so tako načeloma v boljšem položaju, saj pridobijo le tiste uporabnike, na

[38] Avtorja navedeta primer YouTubea.

katere ciljajo. Prevladujoči oglaševalci pa z vedenjskim oglaševanjem ne pridobijo, kadar imajo pomembno konkurenčno prednost pred tekmeci, saj bi s tradicionalnim oglaševanjem imeli na voljo večjo skupino uporabnikov in bi še vedno pridobili pomembne prihodke (Chen in Stallaert, 2014).

Avtorja skleneta, da so prava prednost vedenjskega oglaševanja pred tradicionalnim višji skupni prihodki izdajateljev in oglaševalcev, zato tudi večja družbena blaginja, vendar pod pogojem, da ima uporabnik možnost, da lahko vedenjsko oglaševanje zavrne. Tudi če del uporabnikov vedenjsko oglaševanje zavrne, rezultati analize še vedno držijo, toda avtorja pojasnjujeta, da so prednosti vedenjskega oglaševanja za vse deležnike večji, če je vanj vključenih več uporabnikov. Zato menita, da bi morali regulatorji vedenjsko oglaševanje spodbujati, pod pogojem, da so skrbi uporabnikov glede njihove zasebnosti upoštevane in je oglaševanje tudi zanje koristnejše. Samoregulacija, ki jo spodbuja FTC, naj bi bila po njunem mnenju ustrezno orodje, saj omogoča uporabnikom, da se od vedenjskega oglaševanja odjavijo. Predlagata tudi, da bi ameriški regulator (FTC) subvencioniral prehod na vedenjsko oglaševanje, npr. tako, da bi ponujal standardna orodja za sledenje in njegovo izvajanje (Chen in Stallaert, 2014).

Če kritično povzamemo ugotovitve študije, vidimo, da vedenjsko oglaševanje najbolj koristi velikim izdajateljem, tj. velikim ponudnikov spletnih vsebin in storitev (npr. spletni družbeni mediji, novičarski portali, spletni trgovci, multimedijski ponudniki), ki imajo veliko heterogenih uporabnikov in zato tudi veliko oglaševalcev, ki so med seboj primerljivi. Ti lahko z vedenjskim oglaševanjem veliko pridobijo. Vedenjsko oglaševanje so prav ti ponudniki uvedli in ga izpopolnili. Mali izdajatelji – teh je na spletu večina – pa s takim oglaševanjem naj ne bi pridobili, kot tudi ne nujno oglaševalci.

Argumenti, da vedenjsko oglaševanje koristi razvoju spletnih storitev in vsebin ter da podpira brezplačni internet, so glede na rezultate te raziskave na majavih nogah. Vedenjsko oglaševanje podpira velike ponudnike oz. izdajatelje ter razvoj njihovih storitev, vprašljiva pa je njegova vloga pri zagotavljanju ponudbe drugih, manjših ponudnikov vsebin. Vedenjsko oglaševanje je po drugi strani zelo invazivna praksa, ki ima širše posledice kot le vdor v zasebnost. Poleg tega običajno poteka brez vednosti uporabnika in uporabniki za zdaj nimajo

možnosti, da se mu odpovejo. Vse to postavlja trditve avtorjev o večji družbeni blaginji, ki naj bi jo vedenjsko oglaševanje omogočalo, pod velik vprašaj.

K temu lahko prištejemo tudi raziskave o odnosu posameznikov do vedenjskega oglaševanja, ki v splošnem kažejo, da so posamezniki zaskrbljeni zaradi praks sledenja na spletu in da si želijo orodij, s katerimi bi se bilo mogoče temu izogniti. Hkrati se številni posamezniki ne zavedajo, kako oglaševanje na spletu poteka. McDonald (2011) denimo v svoji študiji ugotavlja, da odnos posameznikov niha od podpore vedenjskemu oglaševanju, pa do globoke zaskrbljenosti glede tega, čeprav v splošnem posamezniki razumejo, da večinoma oglaševalski prihodki zagotavljajo brezplačne vsebine na spletu. Kot je bilo podrobneje predstavljeno že v poglavju 2.5 te naloge, čeprav situacijo razumejo, posameznike frustrira in jezi način, na katerega se vedenjsko oglaševanje izvaja, s prikritim zbiranjem zelo natančnih podatkov o vsakem posamezniku.

Čeprav bi bilo mogoče pojav vedenjskega oglaševanja raziskovati zgolj v okviru teorij tržnega komuniciranja in vedenja uporabnikov, tako z vidika učinkovitosti delovanja in vpliva na porabnike kot tudi z vidika oglaševalske etike oz. odgovornega komuniciranja (in širše poslovne etike, ki nastopa tudi v okviru pristopa družbene odgovornosti), bi tako marsikatera dilema, ki jo vedenjsko oglaševanje odpira, ostala nezadovoljivo pojasnjena, saj razsežnosti problematike presegajo okvir tržnega komuniciranja. Zato bo bistvo naslednjih poglavij te naloge poskus oblikovanja konceptualnega okvira s pomočjo multi-teoretskega pristopa, ki temelji na kombiniranju različnih teorij, s katerim je mogoče fenomen raziskovati v vsej svoji širini, po vzoru internetnih študij, ki črpajo iz teorij s področja družboslovja, humanistike in računalniških ved (Wellman, 2013). V nadaljevanju so predstavljeni različni teoretični pristopi in pogledi, ki vsi prispevajo k boljšemu razumevanju fenomena vedenjskega oglaševanja na različnih ravneh. Študije občinstva in medijske potrošnje odkrivajo, kako so tehnologije in mediji vpete in mediatizirajo vsakodnevno življenje posameznikov. Vidiki politične ekonomije komuniciranja se ukvarjajo z odnosi moči v medijski proizvodnji in potrošnji ter izpostavijo pomemben koncept poblagovljenosti uporabnikov sodobnih tehnologij, s katerimi se na digitalnem oglaševalskem trgu danes trguje. Prav tako nudijo vpogled študije informacijske zasebnosti, s katerimi je mogoče globlje razumevanje problematike posega v zasebnost in njenih implikacij za digitalno oglaševanje. Normativne teorije osvetlijo procese regulacije, vedenjska ekonomija pa predsodke, ki usmerjajo

posameznika v odločanju. Pristop družbene odgovornosti pa prinaša svež pogled na možnosti regulacije vedenjskega oglaševanja v prihodnosti.

3.1.3 Pristop medijske potrošnje in študije občinstva: družbeni vidiki in vedenjsko oglaševanje v mediatiziranem vsakdanu posameznika

Pristop medijske potrošnje odkriva, kako so tehnologije in mediji vpeti v vsakodnevno življenje posameznikov (npr. Livingstone, 2002; Silverstone, 1999). Z novimi mediji in sodobnimi komunikacijskimi tehnologijami se je medijska potrošnja bistveno spremenila, prav tako razmerja med občinstvom in mediji (Luthar in Oblak Črnič, 2015; Rosen, 2006). Spremembe zadevajo tudi vlogo občinstva, uporabnikov novih medijev. Družbeni akterji imajo v novih medijih precejšnjo moč, da izbirajo načine njihove uporabe. Uporabnik je tako lahko hkrati tudi ustvarjalec vsebine (Zittrain in Palfrey, 2008; Benkler, 2001). Odkrivanje in raziskovanje različnih vidikov potrošnje novih medijev je v okviru naše raziskave zelo pomembno, saj nas zanima vidik posameznikov, uporabnikov naprav in storitev elektronskega komuniciranja. Kako ti uporabljajo nove medije, kako so vtkani v njihov vsakdan in ali imajo možnost vplivati na procese vedenjskega oglaševanja. Po eni strani nas zanima posameznik kot ustvarjalec, ki se lahko aktivno odloča glede sodelovanja v procesih novih medijev in po drugi posameznik kot prejemnik vsebin in storitev ter omejitve, ki mu preprečujejo aktivnejše poseganje v problematiko vedenjskega oglaševanja.

Spremembe medijske potrošnje v zadnjih dveh desetletjih zadevajo večjo interaktivnost in »množenje« osebnih medijev v vsakdanjem življenju posameznikov ter privatizacijo medijske potrošnje, ki je prej potekala npr. v družinski dnevni sobi (Luthar in Oblak Črnič, 2015, str. 9). Pojem interaktivnosti Lievrouw in Livingstone (2006b) vežeta predvsem na izkušnjo, ki jo imajo uporabniki z novimi tehnologijami, niso pa je imeli pri starih medijih. Uporabniki imajo možnosti hipnega neposrednega komuniciranja in odzivnosti (Lievrouw in Livingstone, 2006b, str. 23–24), čeprav še potekajo razprave o kakovosti takega komuniciranja v primerjavi z medosebno komunikacijo »v živo«, ki naj bi bila ideal komunikacije (Turkle, 2008). Novi mediji, posebej internet, so postali del vsakdana, njihova uporaba je rutinska in vtkana v družbo (Lievrow in Livingstone, 2006a, str. 1). Niso nadomestili starih medijev, temveč so načini uporabe medijev postali bolj individualizirani, poblagovljeni in združujejo tisk, video in avdio, telekomunikacije, računalništvo in druge načine komuniciranja ter

širjenja informacij. Informacijsko-komunikacijske tehnologije so se z razvojem spreminjale, od radikalnih k rutinskim, od novosti k zahtevam po varnosti regulaciji, rutinizaciji. Raziskovanje, ki se je prej osredinjalo na načine sprejemanja medijev pri občinstvih in učinke, se mora zdaj soočati z uporabo in uporabniki, interaktivnostjo ter vzajemnostjo. Žanri, ki smo jih poznali v starih medijih, se spreminjajo v hibridne vsebine, ki jih je mogoče ustvarjati in deliti prek različnih kanalov (Lievrow in Livingstone, 2006a, str. 1). Pri nekaterih medijih se res spreminja njihova uporaba, kot npr. upad uporabe časopisov med mladimi, kjer so različice na spletu dober nadomestek, vendar hkrati pri drugih medijih ni videti sprememb ali upada, npr. pri televiziji (Couldry, 2009, str. 445).

Še ena od bistvenih sprememb zadeva vseprisotnost novih medijev – novih tehnologij in komuniciranja, ki jih te tehnologije omogočajo (računalnik, mobilni telefon, digitalna televizija, različne oblike internetne komunikacije, kot so npr. spletna družbena omrežja) (Luthar, 2010). Na vseprisotnost novih tehnologij lahko pogledamo z vidika večanja javnega dobrega in napredka (Lievrow in Livingstone, 2006, str. 23–24), hkrati pa posledično trčimo ob vprašanja digitalnih ločnic med področji in ljudmi, ki nimajo tehnoloških (z)možnosti, ter tudi ob negativne vidike vseprisotnosti tehnologij, ki jih nekateri avtorji združujejo pod pojmom družba nadzora (npr. Kovačič, 2006). Množenje osebnih medijev in njihova vseprisotnost pomenita, da se je v raziskovanju medijske potrošnje treba osrediniti na hkratno uporabo več medijev in ne le na uporabo in učinke vsakega posameznega (npr. le televizije ali spletnih družbenih omrežij). Luthar in Črnič Oblak (2015) tako npr. v svoji študiji uvedeta pojem »medijski repertoarji«, ki označuje »medsebojno povezano konfiguracijo medijev pri človeku in se nanaša na način kombiniranja različnih medijev in ustvarjanje celostnega tipičnega vzorca medijske uporabe« (Luthar in Črnič Oblak, 2015, str. 8). Podobno ugotavlja tudi Silverstone (2006), ki poudarja, da je internet, tako kot drugi mediji, konstitutiven del vsakdanjega življenja in ne le dodatek k socialnim, političnim, ekonomskim ali kulturnim procesom. Čedalje bolj je vtkan v vse procese v našem vsakdanjem življenju, ima številne stične in povezovalne točke z drugimi mediji in tehnologijami. Zato ga je treba raziskovati kot takega, del širšega medijskega okolja, ki ga oblikuje in je oblikovano s strani interneta. Raziskovanje virtualnega mora biti povezano z raziskovanjem realnega in drugih medijev (Silverstone, 2006, v Orgad, 2007, str. 34).

V tem smislu nam pojav novih medijev osvetli pristop družbenega oblikovanja informacijsko-komunikacijskih tehnologij. Ta poudarja, da imajo ljudje vedno možnosti glede tega, kako se bodo tehnologije razvile, kako bodo razumljene in uporabljene. Hkrati pa se na točki, ko postane uporaba posamezne tehnologije tako pogosta in vpeta v vsakdan, to spremeni in lahko postanejo možnosti uporabe in izbire omejene (Daryl Slack in MacGregor Wise, 2006; Lievrow in Livingstone, 2006b, str. 21). V vsakodnevnem življenju se uporabniki poigravajo z napravami in aplikacijami, kar lahko dodaja nepričakovane plasti družbenemu razumevanju in neposredno ali posredno k funkcionalnostim tehnologij. Hkrati pa je družbena konstrukcija tehnologije dvosmeren proces, v katerem se sooblikujejo tudi uporabniki (glej npr. Pinch in Bijker, 1984). V ozadju te miselnosti je model udomačevanja (domestikacije) medijskih tehnologij, ki je bil sprva uporabljen pri raziskavah uporabe televizije v gospodinjstvih, načinov, na katere je televizija apropriirana in pomešana v zasebno življenje družine in v t. i. moralno ekonomijo gospodinjstva (npr. Silverstone, 1994). Širša ideja udomačevanja kot procesa, pri katerem uporabniki internet vzamejo za svoj, je navdahnila veliko kakovostnih raziskav, ki dajejo vpogled v vsakodnevne prakse uporabe interneta in hkrati usmerjajo pozornost na družbeni in kulturni kontekst uporabnikov (Bakardjieva, 2013, str. 69–74).

Mediatizacija je nadaljnji ključni pojem v okviru študij medijske potrošnje. Predmet preteklih raziskav so bila predvsem vprašanja vplivov (vsebine) medijev na druge družbene sfere, sodobne raziskave pa poudarjajo proces splošne mediatizacije družbenega prek medijev (Hepp, 2010). Proces mediatizacije omogoča in podpira dejanja komuniciranja in reprezentacije, pri čemer komunikacija pomeni koordinirano akcijo, usmerjeno k razumevanju in deljenju pomena, reprezentacija pa je bistvo informacije – ta pomeni organiziran, izražen produkt komunikacije. Mediatizacija vsebuje vse tri elemente, naprave, prakse in ureditve. Vseprisotnost komunikacije, rekombiniranje načinov dostopa, uporabe in vsebine, dinamične strukture omrežja in interaktivnsot so tiste poteze sodobne mediatizacije, ki se razlikujejo od mediatizacije v starih medijih (Lievrow in Livingstone, 2006a, str. 8–9). V časovnem smislu to pomeni, da je čedalje večje število tehnoloških medijev uporabniku neprekinjeno čedalje dostopnejših (televizijska oddaja 24 ur na dan, internet je prav tako vedno dostopen). Krajevno so novi mediji dostopni na čedalje bolj raznolikih lokacijah in nas ne vežejo le na eno (npr. mobilni telefon). Vse to vpliva na družbeno raven mediatizacije, kjer čedalje več družbenih stikov temelji na uporabi novih tehnologij (npr. spletnih družbenih omrežij), in je čedalje več pričakovanj, da so posamezniki vedno dosegljivi (Hepp, 2010, str. 39–43). Luthar

tako ugotavlja, da uveljavitev novih kulturnih tehnologij, njihova domestikacija ter zlitje in povezanost različnih medijev, po drugi strani pa komodifikacija kulture, pomenijo družbenih premik, ki ga lahko primerjamo le še s prihodom radija in potem televizije pred več kot petdesetimi leti (Luthar, 2010, str. 73–74).

Spremembe medijske potrošnje v kontekstu novih medijev zadevajo tudi vlogo občinstva, uporabnikov novih medijev. Zlasti z vzponom družbenih omrežij postaja čedalje pomembnejši pogled na uporabnika kot ustvarjalca, ne le potrošnika medijskih vsebin, oziroma prakse »pro-trošnje«, kjer uporabnik ustvarja vsebine za druge uporabnike, ter proizvodnja vsebine kot način potrošnje (Luthar in Oblak Črnič, 2015, str. 11). V literaturi je mogoče najti številne optimistične prispevke na temo razlik med novimi in starimi mediji pa tudi kritične prispevke, ki spremembe ocenjujejo bolj trezno in opažajo, da nove tehnologije vendarle še niso prinesle radikalnih sprememb. Avtorjem novi mediji prinašajo nove priložnosti (npr. blogi, zvezde youtuba), vendar je njihova prepoznavnost precej odvisna od pozornosti, ki jo za svojo objavo prejmejo – tukaj prave spremembe pri novih medijih ni opaziti, še več, široko prepoznavo je morda celo težje doseči brez sodelovanja tradicionalnih medijev. Izdajateljeva vloga se v novih medijih deloma prav tako spreminja – na spletu je mogoče neposredno objavljati avtorska dela, brez vratarjev in urednikov. Hkrati pa so tudi založniki ohranili številne poslovne modele na spletu, kjer prav tako najdemo veliko klasično urejenih in izdanih vsebin (spletne izdaje časopisov, e-knjige itd.) (McQuail, 2005, str. 138–139).

Študije občinstva na različne načine preiskujejo vprašanja razmerja med mediji in občinstvom, torej, kakšen je vpliv medijev na občinstvo in kaj občinstvo počne z mediji. Kot pravi Luthar (2010, str. 73), med pristopi ni enotnosti glede konceptualizacije občinstva ali pojmovanja komuniciranja, obstajajo tudi velike razlike v metodologijah raziskovanja. V tem okviru lahko kot eno ključnih poudarimo teorijo uporab in gratifikacij, ki v središče raziskovanja vpliva medijev na občinstva postavi vprašanje uporabe medijev in zadovoljitve. Luthar (2010, str. 9–10) sicer tukaj kritično poudarja, da tradicija medijskih učinkov premalo upošteva problematike, povezane z distribucijo moči v družbi in distribucijo življenjskih priložnosti, ki prav tako vplivata na potrošnjo medijev in občinstva. Zgodnejše raziskave so občinstva dojemale kot poenotena, posameznike pa kot neaktivne, v okviru konceptov množične kulture (npr. Adorno in Horkheimer, 1944; Habermas, 1974), pluralistični pogledi

pa medije štejejo kot le eno od množice institucij, ki zagotavljajo informacije o svetu in zastopajo različne interese. Občinstva so tako dojeta kot aktivna, razdrobljena in zahtevna (npr. Fiske, 1987). V zadnjem času pa avtorji čedalje bolj raziskujejo medije kot del vsakdanjega življenja, vpete in nujno potrebne v življenju državljana in potrošnika. Proces mediatizacije tukaj označuje dialog med ustvarjalci in občinstvi (npr. Hepp, 2010; Couldry, 2003).

Množični mediji naj bi botrovali nastanku množičnega občinstva, katerega značilnost naj bi bila njegova velikost, heterogenost in razpršenost, dojemljivost za manipulacije, povezana z značilnostmi množičnih medijev. V ta okvir spada tudi koncept občinstva kot trga, na katerem naj bi bili občinstvo le potrošniki in ne tudi državljani, produkt, ki ga mediji ponujajo oglaševalcem, v zameno za njihovo financiranje. Vendar hkrati številni mediji delujejo v lokalnem okolju in so vtkani v lokalne kulture, občinstvo pa lahko marsikdaj medije svobodno izbira za uporabo v vsakdanjem življenju. Kritični pogledi na občinstvo tako pogosto zanemarjajo interakcije med posamezniki v občinstvu in njihovo motivacijo ter aktivno uporabo medijev (McQuail, 2005, str. 396–403). Pasivna občinstva naj bi bila izrabljena in podvržena manipulaciji. Zato naj bi se borili proti pasivnemu in neselektivnemu spremljanju medijev, predvsem pri otrocih. Aktivna raba medijev naj bi bila instrumentalna in namensko selektivna ter predvsem boljša kot pasivna (McQuail, 2005, str. 415).

Z razvojem novih medijev so se spreminjali tudi pogledi na občinstvo, ki naj bi postajalo vse manj podobno množičnemu občinstvu iz časa množičnih medijev. Raziskovalci so začeli omenjati koncepte aktivnega, razpršenega občinstva (Livingstone, 2004b), vendar današnja slika kliče po še radikalnejših spremembah v dojemanju občinstev. Mediatizirane vsebine in interakcije so danes družbeno raznolike in niso usmerjene k enotnemu množičnemu občinstvu, kanali so različni, komunikacija pa je interaktivna in ne enosmerna. Novi mediji odpirajo nove možnosti aktivne uporabe, od brskanja do iskanja, odgovarjanja, bloganja, tvitanja, udeleževanja na spletnih družbenih omrežjih itd. Nekatere aktivnosti so individualne, druge kolektivne. Tako je mogoče medije dojemati tudi onkraj tradicionalnega pogleda mogočnih ustvarjalcev informacij, ki vplivajo na družbo, in sicer tudi kot vire, ki ljudem pomenijo priložnosti za aktivno uporabo in udeležbo, ter se osredotočiti na to, kaj ljudje počnejo z mediji in drug z drugim (Lievrouw in Livingstone, 2006a, str. 7–9). S tehnološkimi napravami si postajamo čedalje intimnejši, so vseprisotne, z njimi si gradimo pomembnost v

sodobnem poslovnem življenju. Spreminjajo pa se tudi navade in načela olike, po pametnem telefonu je sprejemljivo brskati tudi med pogovorom z drugo osebo, kar bi bilo v času pisem nesprejemljivo. Turkle (2008) to poimenuje kot »vedno vključeno« komunikacijsko kulturo (Turkle, 2008).

Vloga občinstva se tako spreminja. Več je namreč možnosti za avtonomijo in enakost v smislu dostopnosti virov in preverjanja informacij. Občinstvo je lahko hkrati tudi avtor. Občinstvo se iz množice spreminja v omrežja ali posebne javnosti ali posameznika. Poudarek se od prejemanja informacij premika k aktivnemu iskanju, svetovanju in interakciji (McQuail, 2005, str. 138–139). Uporabniki imajo tudi vpliv. Ko je npr. Facebook uvedel svoj sistem sledenja nakupom uporabnikov in sporočanja teh informacij drugim uporabnikom, so se uporabniki na ta sistem slabo odzvali in Facebook je storitev ukinil, iz česar bi lahko sklepali na večjo moč uporabnikov omrežja, pa vendar podrobnejši pogled pokaže, da je Facebook obdržal in na subtilnejši način nadgradil vse druge možnosti ciljanja in analize ter sledenja uporabnikovim aktivnostim, čeprav je sporni sistem sporočanja nakupov ukinil (Baym, 2013). Primer jasno pokaže dvojnost sprememb v vlogi občinstva. Po eno strani imajo tako nove možnosti vplivanja na vsebino novih medijev, po drugi pa velika izbira vsebin od uporabnikov zahteva več znanja, aktivnosti in napora. Interaktivnost pa ni prevladujoča povsod – številni posamezniki nimajo možnosti, znanja ali želje po aktivni udeležbi v okolju novih medijev (McQuail, 2005, str. 138–139). Aktivni upor uporabnikov proti Facebookovim politikam tako na koncu na prakse tega spletnega družbenega omrežja ni imel kvalitativnega učinka. Vidimo pa tudi, da je uporabnikom bolj problematično, da bi za njihove nakupe izvedeli njihovi bližnji, kot pa da ponudnik, kot je Facebook še vedno nadzoruje vsako njihovo aktivnost in jim dostavlja prilagojene oglase, celo na podlagi etnične pripadnosti, hkrati pa imajo občutek, da so znotraj tako velikega sistema pravzaprav nekako anonimni. Zasebnost uporabnike bolj skrbi v odnosu do tistih, za katere menijo, da bi lahko informacije uporabili in izrabili v nasprotju z njihovimi željami in pričakovanji, kar kaže na to, da posamezniki svojo zasebnost konstruiramo v razmerju do posameznega subjekta, za katerega menimo, da ne bi smel imeti vpogleda v naše življenje. Kot dalje pojasnjujemo v nadaljnjih poglavjih (glej predvsem 3.2.2), kontekst močno vpliva na osmišljanje pravice in želje posameznikov po zasebnosti.

V zadnjih 15 letih je internet s svojim podsistemom svetovnim spletom postal tudi svojstvena medijska forma, ki se razlikuje od svojih predhodnih medijskih oblik. Marshall (2013) poudarja, da tradicionalne oblike medijev ne izginjajo, temveč uporabljajo nove vzorce distribucije, nove formate in roke za produkcijo gradiva, tehnike za ustvarjanje prihodkov in nove oblike ter konceptualizacije občinstev (Marshall, 2013, str. 406). Marshall (2013) se pri analiziranju razlik med starimi in novimi mediji osredinja na to, kako stari mediji uporabljajo internet in se z njim povezujejo. Kot glavni element tega povezovanja vidi promocijo in trdi, da internet stare medijske oblike (TV, film, radio, časopisi) uporablja predvsem kot element promocije svojih vsebin na drugi platformi. Repliciranje naj bi bila druga značilnost povezovanja, saj večina medijev svoje vsebine replicira na internetu, ob čemer jim dodajajo nove možnosti vzorcev uporabe. Prihodek je tema, ki ostaja temelj medijske panoge in njenih *online* utelešenj. Po eni strani prihodki zaradi novih platform rastejo, po drugi strani pa lahko nove oblike podajanja vsebin ogrozijo prihodkovne modele tradicionalnih medijev na internetu. Zavezništva med tradicionalnimi mediji in novimi internetnimi podjetji so naslednji element povezovanja starih in novih medijev (npr. povezovanje medijskih hiš s spletnimi podjetji in ustvarjanje novih skupnih novičarskih portalov ali serviranje izbranih novic, na katere se naroči uporabnik npr. Googla, Yahooja itd). Zadnja značilnost je nadomeščanje, kjer stari mediji v internetu iščejo nove distribucijske poti. Starih kanalov ne opuščajo, temveč nove tehnologije izkoriščajo za dodatne platforme, prek katerih lahko uporabniku vsebino ponudijo bolj prilagodljivo (npr. različni predvajalniki televizijskih hiš). Marshall (2013) ugotavlja, da internet vnaša nove oblike medosebne komunikacije in osebno prilagojenega raziskovanja medijev. Stari mediji so privlačili množična občinstva, oglaševalci pa so to znali dobro izrabljati. Agregiranje zdaj zamenjujejo bogatejši podatki o uporabnikih, ki omogočajo ciljanje in osebno prilagoditev. Zbiranje podatkov pa vključuje veliko več angažiranosti in interakcije s strani uporabnikov (Marshal, 2013).

Z vidika odkrivanja odtenkov med javnimi in zasebnimi komunikacijami na spletu ter posledicami za varovanje zasebnosti so pomembne raziskave spletnih družbenih medijev, pojava zadnjega desetletja, ki interakcijo in osebno izražanje iz zasebnosti prenesejo v včasih javno dostopne prostore. To sproži kompleksna vprašanja glede vlog, ki jih imamo v interakcijah z drugimi, v javnih, deloma javnih in zasebnih spletnih prostorih in primernosti našega samoizražanja. Deljenje zasebnih informacij pomeni najmanj dve ključni dilemi s stališča zasebnosti: (1) pogosto je težko oceniti in razlagati pomen splošnih pogojev varovanja

zasebnosti, posebej ker imajo ponudniki storitev komercialno logiko ponujanja brezplačnih vsebin v zameno za osebne podatke uporabnikov ter uporabljajo zapletene metode križanja in analiz podatkov med storitvami; (2) uporabniki pogosto nimajo nadzora nad podatki, ki jih o njih delijo njihovi bližnji in znanci ali glede ponovne objave gradiva, ki so ga javno objavili sami. Kljub tveganjem, ki jih izpostavljanje zasebnih informacij prinaša, pa marsikdo nima realne alternative, saj prek spletnih družbenih omrežij poteka že tako veliko interakcije in se tam, predvsem za mlade, odvija pomemben del njihovega družbenega sveta (Lueders, 2013, str. 459). Prostore na spletnih družbenih omrežjih lahko delimo na javne in zasebne, med njimi pa je točka, »le prijatelji«. Teoretično naj bi bili varni, če razkrivamo podatke v zasebnih prostorih oz. anonimno nastopamo v javnih in tudi zasebnih prostorih. Prepoznavnost med prijatelji naj ne bi bila tvegana. Tvegano pa naj bi bilo razkrivanje informacij v javni sferi. Spletna družbena omrežja in storitve glede tega ponujajo številna orodja, s katerimi lahko uporabnik omeji, katere informacije bo delil v kakšne vrste prostoru. Lueders (2013) ne glede na to svari, da so ta orodja pogosto preveč kompleksna in jih uporabniki ne znajo uporabljati (Lueders, 2013, str. 461). Kljub želji po varovanju zasebnosti tako uporabniki niso vedno zmožni uporabiti orodij, ki so na voljo, oz. ponudniki storitev ne ponujajo transparentnih načinov varovanja zasebnih informacij. Lueders (2013) prav tako poudarja, da ni nujno bolj tvegano objavljanje informacij v javnih prostorih. Tveganja, povezana z zasebnimi komunikacijami z neznanci, ki vodijo v osebna srečanja, lahko pomenijo bolj tvegano vedenje kot to, da ima nekdo javen profil pa se hkrati izogiba drugim tveganim dejanjem, srečevanjem z neznanci, obiskovanjem spletnih strani s seksualno vsebino itd. Lueders (2013) poudarja, da bi morale prihodnje raziskave obravnavati vprašanje, kako naj uporabniki pridobijo tehnične kompetence in znanja ter pismenost, da se jim zaradi sodelovanja v medijiziranih prostorih ne bo treba odreči zasebnosti. K temi vedenja uporabnikov na spletu in zasebnosti bi morali pristopiti iz sociološkega, pravnega, filozofskega in psihološkega vidika ter z vidika ustvarjanja uporabniku prijaznih medijev in posrednikov, kjer uporabnik dejansko razume orodja, ki so mu na voljo za zaščito njegovih interesov (Lueders, 2013, str. 463). Kot podrobneje pojasnjujemo v naslednjem poglavju je na spletna družbena omrežja zelo pomembno pogledati tudi s širšega vidika družbenih odnosov in moči, ne le z vidika študij občinstev. Pomembna je njihova vpetost v spremembe obstoječih družbenih razmerij in družbene moči ter vpletenost v vsakdanje življenje posameznika, v njegovo neformalno komuniciranje, kot tudi institucionalne strukture in profesionalne rutine (Van Dijck in Poell, 2013, str. 3–6).

Pri iskanju razumevanja vedenjskega oglaševanja skozi optiko teorij medijske potrošnje in študij občinstva naletimo na prenekatere pojme in teorije, ki nam pomagajo razumeti problematiko z vidika posameznika in njegovega vsakdanjega življenja. Čeprav se lahko s številnimi avtorji strinjamo (npr. Livingstone, 2007), da je občinstvo v novih medijih bolj avtonomno, aktivno in komunicira interaktivno, se zdi, da v kontekstu vedenjskega oglaševanja te značilnosti niso prevladujoče. Prva težava je zelo pogosta prikritost izvajanja vedenjskega oglaševanja in še pogostejša neozaveščenost uporabnikov o razširjenosti sledilnih praks na spletu ter nemoč in nepoznavanje načinov, na katere bi lahko svoje pravice uveljavljali in se sledenju izognili. Pogosto ta možnost izogibanja uporabniku niti ni dana, zato imamo vsa ta prizadevanja, ki se vlagajo v regulacijo, ki naj bi omogočala več možnosti izbire na spletu. Pozitivni vidik vedenjskega oglaševanja s stališča posameznikov je zagotovo izboljšana uporabniška izkušnja, uporabnejše storitve in brezplačna vsebina. Nekatere kritike nove medije označujejo kot prepolne informacij, iz katerih uporabnik še težje izlušči bistvo in v tem smislu je osebna prilagoditev vsekakor dobrodošla, saj informacije uredi glede na preference v kontekstu hitrega ritma današnjega življenja. Kot kažejo raziskave panožnih združenj, si del uporabnikov take osebne prilagoditve zagotovo želi (IAB Europe, 2010b). Občinstvo lahko marsikdaj svobodno izbira medije za uporabo v vsakdanjem življenju. Kritični pogledi na občinstvo pa pogosto zanemarjajo interakcije med posamezniki v občinstvu in njihovo motivacijo ter aktivno uporabo medijev (McQuail, 2005, str. 396–403). Uporabniki imajo na spletu široko izbiro storitev, ki jih lahko uporabijo, in med njimi lahko izbirajo ponudnike glede na različne potrebe, preference, ali želje, tudi po merilu varovanja zasebnosti in izpostavljenosti oglaševanju na podlagi profiliranja. Deloma se lahko uporabniki zagotovo razmeroma svobodno odločijo, ali jih bo informacija iz osebno prilagojenega oglasa posrkala vase ali jo bodo delili in se o njej pogovorili z bližnjimi, o ponujenem poiskali več informacij na drugih mestih in tako sami preverili, kako primerna ali ugodna je, ali pa bodo morda stvar prezrli. Cheney-Lippold (2017) kot primer upora posameznika proti opodatkovljenju in izkoriščanju v okviru algoritemske kulture omenja tehnike vnašanja šuma v podatke (angl. *obfuscation*) (glej tudi Finn in Nissenbaum 2016). Posameznik z načrtnim vnašanjem napačnih in nerelevantnih podatkov o sebi vpliva na delovanje algoritmov in tako beži determiniranosti z njihovimi odločitvami (Cheney-Lippold, 2017).

Na drugi strani pa se prav tako izkaže, da je svoboda in opolnomočenje posameznika, uporabnika novih medijev, bolj ali manj le utvara, predvsem pri globalno najbolj priljubljenih

storitvah, ki pravzaprav nimajo več tekmecev, kot je npr. najbolj priljubljeno spletno družbeno omrežje Facebook. Uporabnik se tukaj mora strinjati s pogoji uporabe, ki vključujejo vedenjsko oglaševanje, saj je v nasprotnem primeru izključen iz (za mnoge) pomembnega dela komunikacijske in družbene dnevne aktivnosti. Težavna je tudi vseprisotnost spletnih storitev, ki smo jih čedalje bolj prisiljeni uporabljati v vsakdanjem komuniciranju in opravljanju dnevnih obveznosti (npr. e-pošta, spletne trgovine). Njihovi uporabi se zelo težko izognemo in tako nimamo izbire, kadar ponudnik take storitve izvaja vedenjsko oglaševanje in ne ponuja možnosti izbire. V primeru tako široko uporabljanih hierarhičnih storitev, kot so Googlove in Facebookove storitve, zagotovo lahko najdemo tudi vzporednice s starimi mediji in njihovimi odnosi z občinstvom. Pariser (2011) ponudi tudi širši pogled na problematiko osebne prilagoditve vsebin. Ponudniki, ki na podlagi analize naših želja filtrirajo informacije in jih osebno prilagodijo, ožijo polje posameznikovega delovanja, saj so mu vsebine onkraj njegovih zabeleženih preferenc in aktivnosti čedalje manj dosegljive. Posameznik postaja čedalje bolj ujet v svoje pretekle interese in izgublja možnost spontanega odkrivanja novih znanj in novih nepričakovanih informacij (Pariser, 2011; Woo, 2006, str. 957). Zelo pomemben negativen vidik za občinstvo je poseg v informacijsko zasebnost posameznika. Spet povezano s konceptom vseprisotnosti novih medijev in procesov mediatizacije (Lievrouw in Livingstone, 2006a) ter vedno vključene oz. povezane družbe (Turkle, 2008) lahko trdimo, da je uporaba spletnih storitev tako močno vtkana v naše vsakdanje aktivnosti, da v komunikaciji prek novih medijev razkrijemo veliko več zasebnih informacij, kot jih je bilo mogoče razkriti v preteklosti. Ker nam tehnologije omogočajo komuniciranje, prav tako pa aktivno iskanje informacij in opravljanje dejavnosti, med temi aktivnostmi ponudnikom storitev zaupamo velik del svoje zasebnosti. Dodatna razsežnost je shranjevanje teh informacij, do katerega prihaja po naravi stvari digitalnih medijev in ki odpira popolnoma nove možnosti in razsežnosti izkoriščanja shranjenih zasebnih podatkov (v tržne namene, za namen nadzora) in njihove potencialne zlorabe. Uporabniki v kontekstu vedenjskega oglaševanja nastopajo v vlogi produkta, ki ga sodobni mediji ponujajo oglaševalcem. Ta produkt je lahko zelo natančno opredeljen z natančnim profilom, ki mu je mogoče ponuditi vsebino glede njegove domnevne zabeležene preference. V tem kontekstu so aktualne vse kritike, ki naj bi sicer ciljale na svet starih medijev, o manipulaciji, izkoriščanju občinstva, in njegovi pasivnosti. Na primeru vedenjskega oglaševanja tako zelo jasno vidimo, kot zatrjuje Amon Prodnik (2013) »da lahko prav aktivnost in angažiranost občinstev, ki je z digitalizacijo postala pravilo, vodi v njihovo objektivizacijo, eksploatacijo, poblagovljenje in

posledično menjavo na trgu (tudi če občinstva sama tega nočejo ali samo ne vedo)«. Prav tako se lahko strinjamo z njegovo ugotovitvijo, da je vseobsegajoča mediatizacija pravzaprav le drugo ime za intenzivno poblagovljenje (Amon Prodnik, 2013, str. 359), o čemer podrobneje spregovorimo v naslednjem poglavju.

3.1.4 Pristop politične ekonomije komuniciranja in vedenjsko oglaševanje

Za ekosistem elektronskega komuniciranja so značilne za uporabnika razmeroma brezplačne vsebine, ki jih izdajatelji financirajo z oglaševalskimi prihodki, zaradi česar oglaševanje neposredno vpliva na vsebino in kakovost storitev v elektronskem komuniciranju (OFCOM, 2008; LSE, 2009b). Oglaševanje pa temelji na izrabi podatkov uporabnikov, saj se ti pozitivno odzivajo na zanje relevantne oglase (McDonald in Cranor, 2009; IAB Europe, 2010b; Woo, 2006, str. 955). Omejevanje vedenjskega oglaševanja zaradi negativnih posledic, ki jih ima za pravice posameznikov, pomeni delno regulacijo, ki pa naj bi škodljivo vplivala na razvoj trga informacijskih tehnologij ter konkurenčnost v tem sektorju (WFA, 2010; IAB Europe, 2010a; EACA, 2010; GPA, 2010). Iskanje rešitev na tem področju je kompleksno in kliče po podrobnem poznavanju ekonomije delovanja panoge vedenjskega oglaševanja in ekosistema, ki ga obdaja. Pri tem nam koristijo vpogledi, ki jih ponuja politična ekonomija.

Mansell (2004, str. 97) pri raziskovanju novih medijev poudarja pomen teorije politične ekonomije skupaj z znanji nekaterih drugih tradicij. Podobno Bakardjieva (2013) ugotavlja, da interpretativni pristopi raziskovanja interneta odkrivajo aktivnost uporabnikov v uporabi in prilagajanju internetnih aplikacij svoji situaciji in dnevnim potrebam, hkrati pa je vprašljivo, koliko dinamiko interneta kritično obravnavajo. Uporabniki sicer niso tehnološko zaostali, temveč se aktivno upirajo silam, ki bi lahko ogrozili njihove posamične in družinske moralne ekonomije. Prevzemajo tiste funkcionalnosti novih medijev, ki jim omogočajo, da imajo pod nadzorom svoje dnevne aktivnosti. Vendar pa ne smemo pozabiti na negativne vidike interneta – alienacijo, zatiranje in izkoriščanje. Internetna infrastruktura je podvržena korporativni prevladi in zato je še pomembnejši kritičen pogled na vsakodnevne prakse uporabe, kot je npr. zavajanje uporabnikov, posebej kadar so ti otroci, na prakse izvabljanja podatkov od uporabnikov in njihovega analiziranja. Nujno je kritično osvetliti, katere prakse uporabe spleta uporabnike resnično opolnomočijo, jim dvigujejo raven kakovosti življenja in pri tem upoštevati ter razkrivati negativne silnice internetnega ekosistema, odtujitve, ki so

zamaskirane v uporabnost, priljubljenost ali užitek (Bakardjieva, 2013, str. 74–78). Da je treba k raziskovanju praks uporabe interneta pristopiti kritično, meni tudi Consalvo (2013), ki poudarja še ne dovolj raziskana vprašanja lastnine in poslovnih praks, ki so podstat internetne aktivnosti, in pomembnost vpogleda v to, kako posamezna podjetja in območja, kot je Silicijeva dolina, ter kulturni elementi oblikujejo in omejujejo, kaj in kako je na internetu zgrajeno ali ni zgrajeno (Consalvo, 2013, str. 306).

Politična ekonomija komuniciranja poudarja, da so mediji predvsem komercialne organizacije, ki ustvarjajo in distribuirajo blago (Murdock in Golding, 1997) ter poblagovljajo kulturo in občinstva (Adorno in Horkheimer, 1944; Mosco, 1996). Delujejo na dvojnem trgu, svoje produkte ponujajo občinstvu, hkrati pa producirajo občinstva in jih ponujajo oglaševalcem (Mosco, 1996, str. 148–149). Proizvajanje občinstev in njihova menjava na trgu je posledica odvisnosti medijske panoge od oglaševalskega denarja – ključnega finančnega modela medijev v sodobnosti (Amon Prodnik, 2013, str. 22–23). Značilnost dvojnega trga je še zlasti razvidna v primeru vedenjskega oglaševanja – občinstvo običajno prejme brezplačno storitev, oglaševalci pa zelo natančno opredeljeno občinstvo, kjer je za vsakega posameznika izdelan profil glede na njegove preference. Občinstvo torej postane produkt. Oglaševalec si lahko natančno izbere, komu želi poslati svoje sporočilo, občinstvo pa storitev dejansko plača s svojimi podatki.

Tu se lahko navežemo na idejo, da je komercializacija interneta problematična, saj so ponudniki storitev in vsebin na spletu razvili komercialno logiko, po kateri ponujajo svoje gradivo brezplačno, v zameno za osebne podatke uporabnikov (Shapiro, 1999). Kultura konzumerizma, zgrajena ob spletnih straneh, ki ponujajo osebno prilagojeno oglaševanje tudi čedalje bolj oblikuje identitete mladih. Uporabnike vabijo, da svojo identiteto gradijo skozi potrošniške preference (glasba, filmi, oboževalstvo), ki jih usmerjajo močni komercialni interesi modne in glasbene panoge *online* in *offline* (Lueders, 2013, str. 4). Livingstone tako govori o poblagovljenem uporabniku (angl. *commodified user*), vezanem na urejen profil na spletnem družbenem omrežju (Livingstone, 2013). Kultura na internetu je zelo povezana s konzumerizmom, uporabniki so podvrženi ciljanim oglasom in trženju, razvoj okusov in življenjskega stila pa je tako možno oblikovan s strani mogočnih komercialnih interesov v modni in glasbeni panogi (Marwick, 2005, v Livingstone, 2013, str. 354).

Povezave med digitalizacijo in poblagovljenjem poudarja Mosco (2004), ki opozarja, da je na vzpon kibernetskega prostora treba pogledati z vidika poblagovljenja celotnega komunikacijskega procesa (Mosco, 2004, str. 156–157). Komuniciranje in tehnologija podpirata poblagovljenje prek celotne družbe, digitalizacija pa te procese še okrepi. Poblagovljenje prodira tudi v vse družbene prakse in institucije, ki so povezane s komuniciranjem (Mosco, 2009, str. 12–13, 130). Amon Prodnik (2013, str. 187) v tem smislu poziva h globokemu zgodovinskemu vpogledu na mediatizacijo iz vidika politične ekonomije komuniciranja in kot pomoč pri osmišljanju družbenih sprememb poudarja pojem pronicajočega poblagovljenja (angl. *seeping commodification*). Obče poblagovljenje komunikacijskih procesov pomeni kvalitativni preskok v potencialni nadaljnji širitvi poblagovljenja. Ker komuniciranje ne pozna več klasičnih meja ali fizičnih omejitev, poblagovljenje pronica v vse družbene pore in človeška življenja (Amon Prodnik, 2013, str. 183). Ob tem je treba poudariti družbene neenakosti v porazdelitvi komunikacijske moči, informiranosti in posledično zmožnosti za dostop do javne sfere. Kot poudarja Amon Prodnik (2013), se te kažejo na številnih ravneh: v procesih koncentracije kapitala in oženja možnosti družbenih akterjev za vplivanje na odnose v družbi, v procesih omejevanja dostopa do informacij in komunikacijske sfere, kar kaže razširjanje pravic intelektualne lastnine, poblagovljenje medijev, kulture in javno dostopnih informacij, ki ustvarja informacijske neenakosti (oz. kot jih poimenuje Woo (2006), *information have and have-nots*) ter v poskusih legitimacije širitve kapitalizma in kulturnega imperializma oz. vzpostavljanja monopolov nad znanjem (Innis, 1951/2008, v Amon Prodnik, 2013, str. 23), s čimer se ohranja družbena hierarhija (Amon Prodnik, 2013, str. 23).

Van Dijck in Poell (2013) obravnavata politično ekonomijo platform spletnih družbenih medijev, kot so Facebook, Twitter, LinkedIn, YouTube in Flickr, ter raziskujeta, kako te platforme spreminjajo obstoječa družbena razmerja in razmerja družbene moči v medijskih sistemih, s svojo globoko vpetostjo v vsakdanje življenje posameznika, v njegovo neformalno komuniciranje, kot tudi institucionalne strukture in profesionalne rutine. Logika družbenih medijev počasi pronica v vsa področja javnega življenja; kulturne in komercialne dinamike pa se mešajo z oglaševalskimi. Daleč od tega, da bi bile to nevtralne platforme, ki bi pošteno predstavljale različne glasove v družbi, vplivajo na vsa pravila družbenih interakcij. Pri tem delujejo kot vratarji ali filtri, prek katerih nekateri dobijo več pozornosti kot drugi. Avtorja gradita svojo argumentacijo na pojmu »opodatkovljenja« (angl. *datafication*), tj. procesu

kvantificiranja in predstave našega življenja v obliki podatkov – ne le tistih, ki jih posamezniki delimo o sebi, temveč tudi metapodatkov, ki jih zajema ponudnik elektronskih storitev. Hkrati ugotavljata, da vzpon spletnih družbenih medijev in proces opodatkovljenja po eni strani opolnomoči uporabnike, po drug strani pa daje platformam moč pri vodenju in izrabljanju svojih uporabnikov (Van Dijck in Poell, 2013, str. 3–6). Baym (2013) v tem smislu poudarja nujnost kritičnega vpogleda v delovanje spletnih družbenih medijev. Pri raziskovanju spletnih družbenih omrežij ugotavlja, da je področje etike tisto, na katerem so nadaljnje raziskave najnujnejše. Kakšne so praktične in etične posledice prehoda druženja iz neprofitnih na platforme, ki so v zasebni lasti in jih poganja izključno komercialni interes? Ko spletna družbena omrežja številnim posameznikom postajajo čedalje nujnejša za vzdrževanje svojega družbenega življenja, postajamo ujetniki korporacij, ki so odgovorne svojim delničarjem in ne uporabnikom. Njihov imperativ je dostava uporabnikov oglaševalcem in ne vzpostavljanje pristnih osebnih razmerij in zvez. Tako so pogoji uporabe teh mest običajno zelo problematični in enostranski. Seveda pa imajo tudi uporabniki na drugi strani vzvode moči in včasih morajo korporacije svoje načrte spremeniti (tako se je npr. zgodilo s Facebookovo aplikacijo Beacon). Drugi etični vidik pa je sledenje uporabnikom s strani ponudnikov storitev in iskalnikov. Uporabniki pravzaprav nimajo možnosti, da bi se stalnemu sledenju izognili, običajno so o dogajanju z njihovimi podatki slabo obveščeni. Ponudniki platform pa imajo čedalje večje možnosti sledenja obsežnim družbenim in intelektualnim aktivnostim uporabnikov prek inovativnih storitev in zbiranja podatkov za osebno prilagoditev storitev in oglaševanje (Baym, 2013, str. 399–400).

Pomemben prispevek politične ekonomije k analizi sodobnih gibanj velikega podatkovja in računalništva v oblaku je podal Mosco (2016), ki je z različnih vidikov analiziral oblačno panogo in poslovne modele, ki temeljijo na izrabi podatkov uporabnikov. Hkrati podaja kritiko mita potenciala tehnološkega napredka na tem področju, ki naj bi omogočil skoraj neomejene možnosti človeškega napredka s povezovanjem ljudi, manjšimi stroški in večjo učinkovitostjo, hkrati pa ima v resničnosti številne negativne posledice – politične, ekonomske in okoljske. Predvsem slednji niso pogosto javno izpostavljeni, vendar so kljub temu zelo resni. Velike zmožnosti računalništva namreč zahtevajo tudi veliko tehnične infrastrukture, ogromne podatkovne centre, ogromno rabo energije, ki računalniške zmogljivosti poganja, in energije, ki je potrebna za ohlajanje infrastrukture (npr. izrabo

naravne hladne vode – zato so veliki podatkovni centri v hladnejših predelih). Okoljski davek digitalizacije je tako zelo velik, vendar pogosto spregledan (Mosco, 2016).

Cheney-Lippold (2017) je to razpravo razširil tudi na algoritme, in sicer kako ti ustvarjajo naš današnji jaz, kako vse bolj interpretirajo in vplivajo na naše vedenje. Avtor uporablja pojem opodatkovljenega jaza (angl. *datafied self*), ki podobno kot Floridijev koncept infosfere (2006, več v poglavju 3.2.2) poudarja, da posameznikov jaz v sodobnosti čedalje bolj gradijo podatki, algoritmi pa na podlagi naših podatkov govorijo o nas in namesto nas – na področju trženja, političnih kampanj in storitev javnih institucij. Znanje, ki oblikuje svet in posameznike, čedalje bolj gradijo algoritmi ter podatki in logika, ki jih poganjajo (Cheney-Lippold, 2017, str. xiii). Poudaril je, da obsesivna uporaba naprav, ki zbirajo podatke o našem spanju, gibanju in drugih rutinah, ne pomeni le preprostega kvantificiranja in prepisa življenja v strojno berljive podatke, temveč so te podatkovne točke povezane z močjo, ki ima zmožnost nadzora nad nami in našo intimnostjo. Algoritmična regulacija tako opisuje nadzor, ki ga imajo nad posameznikom algoritmi oziroma kode (Cheney-Lippold, 2017, str. 107), hkrati pa so tudi ti vedno del širših struktur družbene moči, akterjev, ki algoritme razvijajo in določajo njihove glavne parametre za razvrščanje podatkov in odločanje.

Crain (2016) je z vidika politične ekonomije analiziral pojav preprodajalcev osebnih podatkov v ZDA in je ugotovil, da lahko v tej panogi vidimo dejansko komodifikacijo uporabnika in njegovih podatkov. S podatki posameznika se trguje in preprodaja ter so produkt in gorivo celotne nove panoge. Med proučevanjem ohlapne regulacije tega področja, ki v ZDA temelji predvsem na pozivih k večji transparentnosti, ugotavlja tudi, da po eni strani struktura in načini poslovanja te panoge sami po sebi omejujejo njeno transparentnost, saj gre za družbe, ki niso v neposrednem stiku s posamezniki. Po drugi strani pa trgovci s podatki uporabijo sporočila o transparentnosti v svojih odzivih pri odnosih z javnostmi in tako odganjajo poskuse strožje zunanje regulacije pod krinko spoštovanja svobodne izbire informiranega posameznika. Na zunaj tako ustvarjajo videz reforme svojih praks, medtem ko ostajajo razmerja moči pravzaprav nespremenjena (Crain, 2016). Politična ekonomija poudarja, da je delovanje medijev odvisno od ekonomskih in političnih sil njihovih lastnikov (McQuail, 2002, str. 10). Konkurenčnost držav v smislu medijskih trgov postaja v informacijski družbi čedalje pomembnejša razsežnost (Galperin, 2004). Želja po globalni konkurenčnosti pa pogosto ustvarja tako regulacijo medijskih trgov, ki primarno podpira rast in razvoj njih samih

(Grant, 2006). Pogled politične ekonomije osvetli procese poskusov regulacije vedenjskega oglaševanja v EU in ZDA. ZDA so tradicionalno usmerjene k uspehu digitalne ekonomije in inovacijam ter oblikujejo regulacijo, ki podpira te cilje (WFA, 2010; IAB Europe, 2010a; Burnik, 2011a), EU pa je sicer stopila na pot večje zaščite uporabnikov elektronskih komunikacij, vendar kot kaže razvoj zakonodaje in različne prakse uveljavljanja te zakonodaje, tudi EU ni imuna na dejavnik konkurenčnosti njenega gospodarstva nasproti ameriškemu.

3.1.5 Novi mediji, vedenjsko oglaševanje in demokratični procesi: razlogi za regulacijo

Pogled na področje novih medijev in vedenjskega oglaševanja z vidika teorij tržnega komuniciranja, medijske potrošnje, raziskovanja občinstev in politične ekonomije nam razkrije številne podrobnosti te problematike – od učinkovitosti vedenjskega oglaševanja in razlogov zanjo, do procesa mediatizacije, ki zaznamuje področje novih medijev in komuniciranja ter za posameznike in družbo pomeni neizogibnost vedenjskega oglaševanja v njihovem vsakdanjem življenju. Pomembni so ozadje odnosov moči na področju novih medijev in procesi poblagovljenja, s katerimi posamezniki postanemo le skup podatkovnih točk, opodatkovljeni in pripravljeni za prodajo in izrabo na trgu. Kontekst kliče po premisleku o prihodnji regulaciji, ki bi omejila negativne vplive teh praks na družbo, tu pa nam koristne koncepte za osmišljanje razlogov za regulacijo in stanja, ki ga želimo z regulacijo pojava vedenjskega oglaševanja v novih medijih doseči, ponujajo teorije, ki se ukvarjajo z normativnimi vprašanji delovanja medijev v družbi.

Teorija je tradicionalnim medijem pripisovala veliko vlogo pri delovanju demokracije, in sicer kot kritikom in nadzorovalcem oblasti, hkrati pa je odkrivala tudi številne pomanjkljivosti zaradi prevlade le nekaterih glasov v medijih, integracije in koncentracije lastništva ter komercializacije vsebine. Novi elektronski mediji naj bi prinesli olajšanje od hierarhičnih odnosov v starih medijih in pripomogli k neposrednejši participaciji državljanov, raznolikosti vsebine itd. (McQuail, 2005, str. 151).Koncept javne sfere, v kateri se oblikuje javno mnenje, ki nadzoruje oblast (Habermas, 1974), naj bi novi mediji oživili in omogočili njeno boljše delovanje. Tako se v literaturi pogosto pojavljajo premisleki o potencialnem prispevku interneta k delovanju civilne družbe (npr. Poster, 1995; Dahlgren, 2005; Bennet, 2003; Benkler, 2006). Hkrati pa Dahlgren (2005) ugotavlja, da je za internet, tako kot to velja

za stare medije, značilna postopna komercializacija (Dahlgren, 2005, str. 151). Bentivegna (2002) tako trdi, da internet politične participacije ni izboljšal, saj količine informacij omejujejo njihovo učinkovito uporabo, internet ustvarja zasebne življenjske stile (kot so virtualne skupnosti) kot protiutež javnemu in političnemu življenju, raznolikost glasov onemogoča resno razpravo, poleg tega pa za namen političnega udejstvovanja internet uporablja le peščica, ki je že politično zainteresirana in motivirana (Bentivegna, 2002, v McQuail, 2005, str. 151).

Tesno povezana s temo demokratičnosti je tudi tema svobode, ki naj bi jo novi mediji omogočali. Za komunikacijo naj bi bil dovolj le priklop na omrežje, poleg tega pa naj omrežje ne bi diskriminiralo med uporabniki, temveč naj bi vso komunikacijo obravnavalo enakovredno, po načelu nevtralnosti omrežja. Odprtost omrežja je bistveno za zagotavljanje svobodne komunikacije, zato sta Benkler (2000, 2001, 2004, 2006) in Zittrain (2008) kritična do zapiranja dostopa do informacij tako s strani oblasti kot tudi s strani komercialnih entitet. Castells (2000) je na konceptu družbe omrežij razvil celostno družbeno teorijo interneta in opaža, da zmožnost družb, da obvladajo tehnologijo (v tem primeru informacijsko) večinoma oblikuje njihovo usodo in da je internet ustvaril novo družbeno obliko, družbo omrežij (2011, str. 275). Tehnologija sicer ne determinira zgodovinskega razvoja in družbenih sprememb, vendar pa pomeni zmožnost družb, da transformirajo same sebe (Castells, 2000, str. 7). Globalno gledano je vzpon družb omrežij neenak. Družbe, ki so bile počasne pri tranziciji k omrežni družbeni strukturi (struktura, ki omogoča inovacije, brez ogrožanja lastnega ravnotežja), naj bi bile ujete na drugi strani digitalne ločnice (Castells, 2000, str. 502; Wheeler, 2013, str. 198).

Čeprav ostaja internet večinoma nereguliran in v tem smislu svobodnejši od drugih medijev, je hkrati tudi čedalje več zlorab, izrabe spleta za komercialne namene in izrabe tehnologije za namen nadzora. Številni avtorji glede tega omenjajo težnje po čedalje večjem približevanju družbi nadzora in ne toliko svobodi (Turkle, 2008, str. 130). Predvsem so na udaru pravice posameznikov, kot je npr. pravica do informacijske zasebnosti (varstvo osebnih podatkov) (Kovačič, 2006). Ta razsežnost je posebej pomembna v okolju elektronskega komuniciranja, v katerem je posameznikova infosfera podvržena večjim pritiskom, kot so prikrito zbiranje podatkov, rudarjenje po podatkih, profiliranje ipd. (Floridi, 2006, str. 117). Z novimi mediji se povezujejo upi za večjo enakost v družbi, toda številni avtorji kritičnih pristopov poudarjajo,

da je sodobna družba zaznamovana z digitalnimi ločnicami, ki povečujejo neenakosti med tistimi z dostopom do komunikacijskih tehnologij in znanja, ter tistimi, ki tega privilegija nimajo (npr. Norris, 2002). Prav tako naj bi se novi mediji razvijali s prevladujočimi vrednotami zahodnega sveta, kot sta individualizem in osebna svoboda (McQuail, 2005, str. 157).

Pomembno je vprašanje pismenosti v novih medijih, digitalne pismenosti, ki zajema vprašanje dostopa do medijev, enakosti in znanja, kulture in participacije, na katerih temeljijo zmožnosti ocenjevanja in presojanja vsebine. V času, ko je vsakdo lahko ustvarjalec vsebine, je slednje bistveno, prav tako kot zmožnosti ustvarjanja vsebine (Livingstone, 2004). Pri vedenjskem oglaševanju se uporabniki najpogosteje ne zavedajo vedenjskega oglaševanja in svojih pravic. Velike so razlike med tistimi, ki se zavedajo problematike zasebnosti, in tistimi, ki tega znanja nimajo. Woo (2006, str. 958) tako govori o zasebnostni ločnici (angl. *privacy divide*). Ker uporabniki ne znajo uveljaviti svojih pravic do zavrnitve sledenja, prevladujoča samoregulacija področja, ki poudarja naknadno zavrnitev sledenja, pa ni uspešna, saj uporabniki te pravice ne uveljavljajo (McDonald in Cranor, 2009). Pa tudi mehanizem privolitve ni splošno zagotovilo za varovanje pravic uporabnikov, saj je to pogosto le navidezno prostovoljna privolitev (Woo, 2006, str. 958). Analiza politik zasebnosti spletnih podjetij, s katerimi se morajo uporabniki navidezno prostovoljno strinjati, pa pokaže, da te ne zagotavljajo varovanja zasebnosti potrošnikov, temveč predvsem legalizirajo dejanja podjetij (Fernback in Papacharissi, 2007).

Pomemben prispevek k razumevanju etike in morale v svetu novih medijev je oblikoval Silverstone (2006). Kljub začetnemu optimizmu poudarja, da so uporabniki novih medijev še vedno omejeni s prevladujočimi normami in s svojim družbenim kontekstom, ki je večinoma onkraj njihovega nadzora (Livingstone, 2007). Medije razume kot okolje, v katerem so pomembne moralne posledice. Tako kot v naravnem okolju tudi v medijskem okolju nastajajo viri, ki so lahko uporabljeni ali zlorabljeni, zavrnjeni, popačeni ali povečani. Načini, na katere te vire uporabljamo, lahko onesnažujejo medijsko okolje ali pa pripomorejo k njegovemu zdravju. Internet je eden od virov tega okolja in načini njegove uporabe imajo lahko pozitivne ali negativne vplive. Silverstone (2006) meni, da je treba te problematike raziskovati in iskati načine soočanja z onesnaževanjem globalnega medijskega okolja. Tako odpira koncept interneta kot moralnega prostora (Silverstone, 2006, v Orgad, 2007, str. 34). Silverstone

(2004, str. 440) poudarja pomen odgovorne medijske kulture, ki naj temelji na medijsko kritičnem in pismenem državljanstvu. Bistvo medijske pismenosti pa mora biti moralna agenda, ki naj bo vedno del javnih diskurzov in zasebnih praks ter ki prepoznava našo odgovornost in humanost do drugih v svetu konflikta, netolerance in brezbrižnosti.

Še posebej so ti vidiki pomembni ob primerih uporabe vedenjskega oglaševanja oziroma političnega mikro ciljanja v okviru političnih kampanj leta 2016 (Confessore in Hakim, 2017; Cadwalladr, 2017), ki pomembno vplivajo na politično sfero in zdravo stanje demokracije (Narayanan in Reisman, 2017, str. 4; Goodman in drugi, 2017). Časovno ti pojavi sovpadajo s pojavom oz. porastom pojava lažnih novic (angl. *fake news*), pri čemer se pojavlja vprašanje, ali morda lažne novice svoje vidnosti ne dosežejo hitreje tudi s pomočjo političnega mikro ciljanja, ki okrepi njihovo navzočnost v pravih segmentih volivcev, ki so jim (morda zaradi procesov kognitivne disonance) bolj pripravljeni verjeti in jih širiti dalje.

Po eni strani mikro ciljanje volivcu olajša pridobivanje informacij v vsem informacijskem šumu. Zuiderveen Borgesius in drugi (2018) navajajo tudi prednosti v smislu večjih možnosti, da politična sporočila dosežejo skupine volivcev, ki jih je težko doseči (npr. mladi), na platformah, ki so jim bliže (npr. spletni družbeni mediji) in glede tematik, ki so jim bolj v interesu in jih bodo mobilizirale, da se bodo udeležili volitev in s tem prispevali k legitimnosti demokratičnega procesa in izida. Taka komunikacija je lahko za politične stranke cenejša in učinkovitejša kot klasično televizijsko oglaševanje ter doseže več volivcev. S tem lahko pozitivno vpliva na večjo obveščenost volivcev o tematikah, ki so relevantne, in zmanjša alienacijo od političnega procesa ter volilno abstinenco (Zuiderveen Borgesius in drugi, 2018, str. 85–86). Po drugi strani pa mikro ciljanje volivce omejuje v mehurček vedno istih vsebin in s tem posega v pravico do svobode misli, vesti in vere, svobodo izražanja in obveščanja ter svobodo zbiranja in združevanja (EDPS, 2018, str. 12). Številni ponudniki elektronskih storitev, predvsem prevladujoči na trgu, so v vlogi vratarjev ali okna v svet informacij, ki so dostopne posamezniku. Obširni vzorci profiliranja služijo tudi filtriranju informacij, ki so posamezniku priporočene oziroma preprosto dostopne. Posameznikom je dostopnih manj različnih mnenj, kar se kaže v ideološki polarizaciji in prepričljivosti lažnih zgodb pa tudi v potencialih manipulacije – politika lahko volivcem prikazuje sporočila, ki jih angažirajo zaradi čustvene povezanosti z vročimi temami, kot so ksenofobija, migracije, spolna usmerjenost in pravica do splava.

Medijski pluralizem je bistven del pravice do svobode izražanja in obveščanja, saj omogoča raznolikost mnenj in vsebin, dostopnih državljanom. Koncentracija medijev temu škoduje – prevladujoči ponudniki namreč zapirajo širino dostopnih vsebin glede na svoje, običajno komercialne interese (Doyle, 2004). Na trgu novih medijev je, kot je bilo že večkrat poudarjeno, izrazit pojav koncentracije moči v rokah le peščice največjih ponudnikov vsebin in oglaševalskih storitev (med njimi sta najpomembnejša Google in Facebook), kar negativno vpliva na medijski pluralizem (EDPS, 2018, str. 13). Sodobni elektronski mediji, spletni velikani, upravljavci najuspešnejših platform in posrednikov, spletna družbena omrežja, iskalniki itd. so čedalje pomembnejši ponudniki informacij, saj se spreminjajo načini konzumiranja novic, zato tradicionalni mediji niso več edini ponudniki, ampak dve tretjini posameznikov novice raje najde na platformah, ki temeljijo na algoritmičnem in ne uredniškem odločanju (Martens in drugi, 2018, str. 16). V smislu političnega diskurza je pomembno, da novih medijev (izključeni so spletni mediji[39]) običajno ne vežejo standardi novinarskega poročanja in uredniških politik, ki bi delovali v smeri enakovredne zastopanosti mnenj in pogledov, in je izpostavljenost informacij ter njihova pomembnost prepuščena drugim merilom, običajno komercialnim, ki jih vodijo algoritmi (kaj se bolje prodaja oziroma večkrat klikne). Posebej so v zadnjem času kot problematična izpostavljena spletna družbena omrežja, in sicer zaradi pojavnosti lažnih informacij, ki se viralno delijo.

Politično mikro ciljanje posega tudi v pravico do svobodnih volitev. Svoboda, poštenost in preglednost so načela demokratičnih volitev, pri čemer se svoboda nanaša na možnost kandidatov, da tekmujejo brez oviranja in imajo volivci možnost izbire ter svoboden dostop do informacij o možnostih izbire. Če te možnosti ni, tudi v smislu informacij o financiranju, je pod vprašajem preglednost volitev. Poštenost se nanaša na to, da ni nekomu s strani države zagotovljena nepoštena prednost v tekmi. Spletna manipulacija spodjeda vsa ta načela in pravice (EDPS, 2018, str. 13; Evropska komisija, 2018b, str. 1). Poročilo Sveta Evrope med ključne izzive za svobodne volitve prišteva vpliv novih tehnologij za politično mikro ciljanje na običajna pravila o kampanjah (npr. o volilnem molku, poročanju o volilnih rezultatih itd.), na transparentnost financiranja, politično komuniciranje spornih tematik (kot npr. migracij), na politično izločanje (tistih volivcev, na katere ni »vredno« ciljati), na prominentnost posrednikov v volilnem procesu (*adtech* podjetja), na samoregulacijo v novinarstvu in etiki

[39] Poudariti je treba, da tudi spletne edicije tradicionalnih medijev niso imune na komercialno komponento prezentacije informacij – vidni so trendi tabloidizacije, glede na vsebino in glede na obliko predstavljenih informacij. Več v Burnik (2008).

(lažne novice), na zasebnost volivcev in na preglednost virov za financiranjem političnih kampanj (COE, 2017, str. 18–20).

Priljubljene tehnološke platforme omogočajo neposreden dostop do volivcev, kjer sporočil ne filtrirajo novinarji in uredniška politika ter tako nosijo veliko moč kot vratarji do informacij – lahko omogočajo ali omejujejo razširjanje posameznih sporočil. Lahko ponujajo drugačne pogoje različnim kampanjam in pogledom (tako finančno kot tudi drugače), lahko celo zavrnejo sodelovanje s posamezno kampanjo, vse glede na svoje politike odločanja, ki so bolj ali manj komercialne, kar lahko v teoriji pomeni veliko omejevanje raznolikosti informacij, ki bodo volivcem na voljo. Tako so npr. vzniknile obtožbe, da Facebook v ZDA v svojem avtomatiziranem sistemu omejuje novice konservativne politike, na kar je ta opustil svoje človeške urednike in objave novic v celoti prepustil algoritmom, zaradi česar se je povečala vidnost lažnih in žaljivih vsebin (Goodman in drugi, 2017, str. 13).

Zagotavljanje svobode obveščenosti in pluralnosti informacij ter enakega dostopa političnih opcij do predstavitve volivcem je v zvezi z demokratičnimi volilnimi procesi regulirano na več področjih, običajno na ravni nacionalnih zakonodaj, pa tudi na evropski ravni, vendar predvsem velja za tradicionalne medije (kot sta televizija in radio). Pluralnost medijev deloma zagotavljajo pravila na področju konkurenčnega prava, pluralnost informacij vsaj v delu javnih RTV servisov zagotavljajo pravila glede komunikacije in informacij pred volitvami, s katerimi so določeni časovni okviri, ki morajo biti na voljo posameznim političnim opcijam pa tudi njihovo uravnoteženo predstavljanje. Nove platforme tem pravilom načeloma ubežijo, pa vendar večina volivcev informacije prejme prav prek teh platform. (Goodman in drugi, 2017; COE, 2017). Če so te informacije izkrivljene glede na profil volivca, to jasno pomeni, da mu je onemogočena polna obveščenost, s tem pa poseženo v bistvo svobodnih volitev.

Pomembna so tudi vprašanja financiranja političnih kampanj – tako z vidika preglednosti kot tudi z vidika zmožnosti političnih opcij, da jim zaradi nesorazmernih stroškov ni onemogočeno svobodno tekmovanje z drugimi na relevantnih platformah. Preglednost sredstev, ki so bila namenjena posameznim medijem ali platformam, je bistvena zato, da volivci vedo, kje so jim politična sporočila prikazana, in v tem smislu niso podvrženi manipulaciji. Avtorji poudarjajo, da je na ravni pravil o financiranju političnih kapanj veliko prostora za izboljšave transparentnosti glede porabe sredstev, saj redka pravila zahtevajo

natančno poročanje o porabi za digitalno oglaševanje, ter še posebej za porabo v tehnološkem sektorju analitik podatkov o volivcih (Goodman, 2017; ICO, 2018b). Financiranje političnih strank običajno ureja nacionalna zakonodaja, pri čemer so stranke deloma tudi financirane s strani države. Sofisticirane podatkovne analize, ki so podlaga za mikro ciljanje, so lahko drage in presegajo vire manjših političnih strank ter jim s tem onemogočajo pošteno tekmovanje z velikimi, finančno bolje podprtimi opcijami (Zuiderveen Borgesius in drugi, 2018, str. 89). Seveda so na mestu tudi vprašanja o morebitnih političnih interesih lastnikov platform, ki niso zavezane k pravilom neodvisnosti.

3.2 Pristopi informacijske zasebnosti: zasebnost in druge temeljne pravice posameznikov pri vedenjskem oglaševanju

Vpliv na zasebnost uporabnikov je eden temeljnih pomislekov pri izvajanju vedenjskega oglaševanja (npr. Tucker, 2011). Posebej na političnem področju pa se mu pridružujejo še pomisleki glede vpliva na druge temeljne pravice, tj. pravico do svobode informiranja in s tem povezanega vprašanja pluralnosti medijev ter na pravico do svobodnih volitev, centra demokratičnih procesov v družbi (Goodman in drugi, 2017; COE, 2018; EDPS, 2018).

Pomembna so tudi vprašanja privolitve uporabnikov v sledenje njihovim aktivnostmi in analizo njihovega vedenja, stanj in prepričanj, vprašanja transparentnosti oglaševanja, nadaljnje uporabe zbranih podatkov (Bohm, 2008; WP29, 2010a) in izobraževanja uporabnikov (Woo, 2006). Uporabniki se namreč vedenjskega oglaševanja najpogosteje ne zavedajo, svojih pravic pa ne poznajo. Velike so razlike med tistimi, ki se zavedajo problematike široke uporabe njihovih osebnih podatkov za namen različnega oglaševanja, in tistimi, ki tega znanja nimajo. Kot je bilo že omenjeno, Woo (2006, str. 958) tako govori o zasebnostni ločnici.

Ker uporabniki svojih pravic do zavrnitve sledenja ne znajo uveljaviti, zgolj samoregulacija tega področja ne more biti uspešna (McDonald in Cranor, 2009). Tudi mehanizem privolitve ni splošno zagotovilo za varovanje pravic uporabnikov, saj je to pogosto le navidezno prostovoljna privolitev (Woo, 2006, str. 958). Analiza politik zasebnosti spletnih podjetij prav tako pokaže, da te ne zagotavljajo varovanja zasebnosti potrošnikov, ampak predvsem legalizirajo dejanja podjetij (Fernback in Papacharissi, 2007). Bistven je odgovor na

vprašanje, koliko je vedenjsko oglaševanje invazivno in posega v pravice uporabnikov elektronskih komunikacijskih tehnologij ter koliko so trenutni pristopi k varovanju informacijske zasebnosti uporabnikov uspešni, ob upoštevanju sposobnosti uporabnikov, da svoje pravice uveljavljajo.

Glavna značilnost, po kateri se vedenjsko oglaševanje razlikuje od drugih vrst oglaševanja, je zbiranje velikih količin podatkov o aktivnostih in preferencah uporabnikov, na podlagi katerih dobi uporabnik njemu prilagojen oglas. Poseg v zasebnost posameznika je torej bistvena komponenta vedenjskega oglaševanja. Teoretski okvir raziskave tako na začetku nujno potrebuje znanja in uvide, ki jih ponujajo teorije informacijske zasebnosti.

3.2.1 Pravica do zasebnosti: kontekstualni pristop

Pravico do zasebnosti običajno dojemamo kot prvi pogoj svobode posameznika do lastne misli, izražanja, združevanja, ustvarjanja in politične volje. K izvoru pravnega varstva in oblikovanja te pravice je veliko pripomogel razvoj tehnologije, ki omogoča različne oblike nadzora (Solove, 2006, str. 3). Opredelitev pravice do zasebnosti se je čez čas razvijala – od znamenitega opisa, da je to »pravica, da te pustijo pri miru« (angl. *the right to be left alone*) (Warren in Brandeis, 1890) do podrobnejših opredelitev o naravi in vlogi pravice do zasebnosti ter njenem razmerju do drugih pravic posameznikov v družbi (Westin, 1967; Perri, 1998; Rule, 2007).

Hkrati pa je zasebnost precej pretočen koncept, za katerega ne poznamo enotne opredelitve, kljub številnim poskusom v to smer. Zasebnost tako povezujemo s svobodo misli, nadzorom nad lastnim telesom, nadzorom nad lastnimi informacijami, svobodo pred nadzorom, varovanjem posameznikovega ugleda in svobodo pred preiskavami in zasliševanji. Bistvo in obseg pravice do zasebnosti se spreminjata in sta prav tako odvisna od stanja družbe. Konceptualizacija pravice do zasebnosti pa je nujna zaradi pravnih razlag in politik na tam področju, saj mora biti pri vprašanjih posega v pravico do zasebnosti najprej jasno, v čem je ta poseg in kaj naj bi zasebnost pravzaprav varovala. Solove (2002) je v svojem poskusu konceptualizacije pravice do zasebnosti ob pregledu prispevkov različnih teoretikov predstavil šest kategorij dojemanja zasebnosti, pri čemer je poudaril, da se včasih med seboj prekrivajo,

da nekatere temeljijo na cilju in nekatere na orodjih za doseganje cilja ter da skratka ne pomenijo taksonomije (Solove, 2002).

Pravica, da te pustijo pri miru. Izvira iz slavnega članka ameriških sodnikov (Warren in Brandeis, 1890), ki je postal temelj prava zasebnosti v ZDA in je postavil okvir za razpravo o tej tematiki v 20. stoletju. Temelj njunega razumevanja zasebnosti je bil v nedotakljivosti osebnosti. Opažala sta, da je posledica sodobnega razvoja poseganje v zasebnost, ki povzroča duševne bolečine, ki so večje, kot bi jih povzročile fizične poškodbe, toda hkrati v pravu tistega časa taka kršitev ni bila opredeljena. Kritika sicer poudarja, da je taka opredelitev zelo široka in ne konceptualna, vendar je bil glavni namen avtorjev odkriti pomanjkljivosti v takrat veljavni zakonodaji (Solove, 2002, str. 1100–1102).

Omejen dostop do sebstva oziroma zmožnost, da se zaščitiš pred neželenim dostopom drugih. Ta koncept prepoznava posameznikovo željo, da se zakrije in loči od drugih ter sam odloča, koliko bodo njegove zadeve del javne razprave in vedenja. V tem smislu je pomemben premislek, da se želja po zasebnosti konstituira v razmerju do drugih v družbi, da je to družbeno ustvarjena potreba. Pomanjkljivost takega pojmovanja je v tem, da ne pomeni vsak dostop do nekoga tudi kršitve njegove zasebnosti, to je le v odnosu do posameznih sfer, informacij o nekom. Vprašanje je torej, koliko dopuščati dostop do nekoga kot upravičen. To je mogoče razumeti le skozi pomen in vrednost tega, katere zadeve so zasebne (Solove, 2002, str. 1102–1105).

Zaupnost (skrivnostnost) oziroma prikrivanje nekaterih zadev pred drugimi. Eno najpogostejših razumevanj zasebnosti je, da so nekatere zadeve skrivnost, zasebnost pa je kršena s tem, da so te zadeve razkrite javnosti. Za nekatere je to v vlogi prikrivanja informacij o sebi, zato da bi javnosti prikrili posamezna dejstva, ki bi osebi lahko škodovala (Posner, 1998, str. 234, v Solove, 2002, str. 1106). Tak pogled je tudi osnova za pravico do informacijske zasebnosti. Bistvo take konceptualizacije je v logiki, da ko je nekaj razkrito v javnosti, čeprav v ozkem krogu, ne more več ostati zasebno. V tem smislu zasebnost pomeni popolno zaupnost informacij, kar nekateri kritizirajo kot preozko pojmovanje, saj ne upošteva t. i. skupinske zasebnosti. Če posameznik nekaj o sebi deli s sodelavcem, to še ne pomeni, da želi to deliti tudi z nadrejenim, da torej govorimo o selektivni zaupnosti in da ima posameznik, kot poudarja Etizioni (1999), možnost, da so podatki o njem uporabljeni za

namene, ki jih sam želi (Etizioni, 1999, str. 196). Prav tako pogosto pričakujemo zasebnost tudi v javnosti. Čeprav knjige, ki jih beremo, produkti, ki jih kupujemo, in naši prijatelji načeloma niso skrivnost, jih vendarle štejemo za zasebno stvar (Solove, 2002, str. 1106–1110).

Nadzor nad osebnimi podatki oziroma zmožnost, da nadzorujemo informacije o sebi. Med najbolj prevladujočimi teorijami zasebnosti je ta o nadzoru nad osebnimi podatki, po kateri je zasebnost zahteva posameznikov, skupin ali institucij do samoodločbe o tem kdaj, kako in koliko se njihovi podatki delijo z drugimi (Westin, 1967, str. 7). Ta pogled je ožji kot prej predstavljena razsežnost omejevanja dostopa do sebe, saj zadeva le informacije o nekom, ne pa tudi odločitev glede telesa, reprodukcije itd. Prav tako se ideja nadzora nad informacijami nanaša na različne stvari. Westin (1967, str. 324) jo npr. povezuje z lastniško pravico nad svojimi podatki, čeprav je taka konceptualizacija težavna. Isto informacijo si namreč lahko deli več ljudi, lahko imajo enake značilnosti (npr. v primeru genetskih podatkov, kjer so deli DNK skupni sorodnikom in je lahko to podatek očeta in otrok). Tudi primer podatkov o posameznikovi aktivnosti na spletu pokaže težave. V tem primeru podjetja podatkom dodajo svoja sklepanja, kategorizacije, ki uvrstijo nekoga v profil, in ne gre le za informacije, ki so lastne posamezniku. Težavno je tudi pojmovanje nadzora v smislu izključnega nadzora posameznika nad tem, kako se delijo njegovi podatki – v svetu sodobnih tehnologij posamezniki dejansko nimajo možnosti in znanja, da bi lahko nadzorovali deljenje svojih informacij. V tem smislu je pomembno spoznanje, da zasebnost ne vključuje le nadzora posameznika, temveč tudi družbeno regulacijo informacij, saj je zasebnost del družbene strukture in arhitekture informacij ter ne le stvar posameznikove odločitve (Solove, 2002, str.1109–1115).

Varovanje sebstva (angl. personhood) osebnosti, individualnosti in dostojanstva. Ta teorija se razlikuje od prejšnjih, saj pojasnjuje normativni element zasebnosti, torej varovanje integritete osebnosti. Pogosto uporabljena skupaj z drugimi pojasnjuje, zakaj je zasebnost tako pomembna, kateri vidiki sebe mi morali biti ograjeni ali nad katerimi informacijami bi morali imeti nadzor. Zasebnost naj bi tako varovala individualnost, položaj posameznika, kot tistega, ki izbira – njegovo ustvarjalnost, ki jo lahko zmoti že opazovanje. Nadzor tako omejuje posameznikovo izbiro in tako njegovo svobodo (Benn, 1971, str. 26, v Solove, 2002, str. 1116–1117). Prav tako se glede tega pojavi konceptualizacija zasebnosti kot nevmešavanje

države v posamezne odločitve, ki so bistvene za definiranje sebstva. Kritika pa poudarja, da se pri taki konceptualizaciji združujeta zasebnost in avtonomija ter da je razumevanje zasebnosti skozi varovanje sebstva preširoko. Nekatere informacije ali dejanja, ki odslikavajo sebstvo posameznika, so pogosto javne (npr. umetniške stvaritve). Osredinjanje le na nevmešavanje države v naše odločitve pa pogosto ni dovolj za varovanje zasebnosti – prav tako ali še bolj smo namreč podvrženi nadzoru in vmešavanju komercialnih organizacij. Zasebnost pa je pravzaprav tako pozitivna kot tudi negativna pravica: ne pomeni le svoboščine v smislu posega s strani države, ampak tudi nalaga obveznost državi, da zagotovi posameznikove svoboščine z orodji lastninske pravice, civilnega in kazenskega prava ter drugimi pravnimi možnostmi (Solove, 2002, str. 1116–1120).

Nadzor nad posegi v intimna razmerja ali dele življenja. Čedalje bolj priljubljena postaja teorija, ki zasebnost razume kot obliko intimnosti in pravilno ugotavlja, da zasebnost ni ključna le za samouresničevanje, ampak tudi v medčloveških odnosih. Zasebnost je sestavljena iz neke vrste omejenega dostopa oziroma nadzora, vrednost zasebnosti pa določa v odnosu razvoja osebnih odnosov. Odnose z drugimi namreč oblikujemo z različnimi stopnjami intimnosti in razkritja sebe, tako da lahko vzdržujemo želene ravni intimnosti v vsakem od razmerij. Ta teorija si prizadeva definirati, pri katerih vidikih življenja bi morali biti zmožni omejiti dostop oziroma katere informacije bi morali biti zmožni imeti pod nadzorom oziroma zadržati zaupne. Ob poskusih definicije intimnosti se poleg deljenja informacij o sebi pojavlja tudi ideja skrbi za druge, bližine in ljubezni, zaradi česar je taka vrsta teorij zasebnosti preširoka, hkrati pa so teorije zasebnost s fokusom zgolj na medosebna razmerja preozke, saj ne pojasnjujejo vidikov komercialnega in državnega nadzora, kjer velike baze podatkov načeloma ne posegajo v intimne medosebne sfere med posamezniki, pa vendarle lahko močno posežejo v zasebnost (Solove, 2002, str. 1121–1124).

Zaradi pomanjkljivosti vseh navedenih pristopov k zasebnosti Solove predlaga konceptualizacijo, ki temelji na pragmatizmu in se osredinja na posamezne problematične situacije, ne pa na univerzalno določene opredelitve, ki jih nato vežemo na konkretno situacijo. Bistvo je razumevanje zasebnosti v posameznih kontekstualnih situacijah. Glede tega je poudaril pomen različnih vsakdanjih dejavnosti posameznikov, pri katerih moramo razumeti zasebnost kot njihov bistveni del in ne kot ločeno kategorijo. Poseg v zasebnost pomeni motnjo pri izvajanju teh dejavnosti. Motnja je npr. nadzor – opazovanje lahko posega

v posameznikov mir in zavira dnevne aktivnosti, ali pa razkritje – če so razkrite informacije o kriminalni preteklosti posameznika, to zmoti njegov proces rehabilitacije. Dejavnosti Solove (2002) razlikuje po javno-zasebni dihotomiji, pri čemer ga ne zamejuje njeno prostorsko dojemanje, saj na primeru koncepta družine, telesa in doma pokaže, da je pripisovanje zasebnosti tem kategorijam zelo zgodovinsko in družbeno pogojeno. Po njegovem mnenju ni nekih stalnih dejavnosti, ki jih vedno dojemamo pot zasebne, ampak morajo odločitve o tem, kaj naj varujemo kot zasebno, temeljiti na empirični, zgodovinski in normativni presoji posamezne dejavnosti. Empirični pogled zajema trenutno kulturno razumevanje zasebnosti in njeno družbeno resničnost. Ker se dejavnosti razvijajo in spreminjajo čez čas, je pomemben tudi historičen pogled. Normativa komponenta pa nas vodi k oblikovanju prava in politik za varovanje zasebnosti v prihodnosti, ne le sedanjosti, pomeni širši pogled v posledice za zasebnost v prihodnosti, kar je posebej pomembno v današnjem svetu hitrega tehnološkega napredka. V tem smislu je bistvena vrednost zasebnosti (Solove, 2002, str. 1126–1143).

Vrednota ali vrednost zasebnosti ne osvetli le, kaj je zasebnost, ampak omogoča tudi njeno tehtanje z drugimi vrednotami, s katerimi prihaja v konflikt. Solove (2002) meni, da je vrednost zasebnosti odvisna od namena posamezne dejavnosti. Zasebnost je stvar moči: vpliva na to, kako se ljudje obnašajo, ter na njihove izbire in dejanja. Kadar želimo obraniti, ustvariti, zmotiti ali ustaviti posamezne dejavnosti, naša odločitev temelji na tem, kako pomembni so nameni teh dejavnosti, kako pomembni so njihovi cilji. V primeru koncepta doma moramo torej ugotoviti, kakšen je njegov namen – npr. možnost pobega pred vrvežem vsakdanjega sveta. Zasebnost ima vrednost v odvisnosti do zasledovanja tega namena. Vprašati se moramo, koliko je zasebnost del neke dejavnosti in kako nanjo vpliva – če vpliva negativno, je zmanjšanje zasebnosti bolj zaželeno. Če vpliva pozitivno, pa je dobro povečanje zasebnosti.

Zasebnost bi morali vrednotiti instrumentalno in ne kot vrednost ali vrednoto samo po sebi, saj predvsem omogoča druge cilje oz. namene. Sama po sebi pa brez konteksta nima intrinzičnega pomena. Zato je ključno ovrednotiti zasebnost v konkretni situaciji, saj ima pri različnih dejavnostih različen pomen. Konceptualizacija zasebnosti na abstraktni ravni tako ne more odkriti pravega pomena zasebnosti. Solove (2002) to utemeljuje z analizo sodnih odločitev iz ZDA, kjer je konceptualizacija zasebnosti slonela na abstraktnih pojmovanjih, ki pa ob prenosu na novo situacijo, predvsem v okviru novih tehnologij, ni zmogla ponuditi

zadovoljivega razlogovanja in so bile odločitve v svojem bistvu zgrešene, vezane na abstraktni pojem zasebnosti, čeprav so bile posameznikom kršene različne pravice, npr. do dostojanstva, prav zaradi razkritja njihovih zasebnih informacij. Zato je pomembno odkrivanje pomena zasebnosti v konkretnih situacijah, deloma posplošenih, še zlasti v dobi informacijskih storitev in hitrih tehnoloških sprememb (Solove, 2002, str. 1143–1155).

3.2.2 Informacijska zasebnost oziroma varstvo osebnih podatkov

Ena od razsežnosti zasebnosti je informacijska zasebnost (v pravu običajno poimenovana varstvo osebnih podatkov), tj. pravica posameznika do nadzora nad podatki, ki se o njem zbirajo in obdelujejo. Sprva naj bi pravica ščitila posameznika predvsem pred oblastnim delovanjem države, ki je imela primat nad zbiranjem podatkov o državljanih, ti pa zoper pooblastila države niso imeli oz. še vedno nimajo pravih orodij (Solove, 2006), v sodobnosti pa se čedalje bolj poudarja njena vloga ščitenja pred interesi zasebnega sektorja, ki v posameznikovih podatkih najde komercialne koristi (Kovačič, 2006). Informacijsko zasebnost še posebej pogosto obravnavajo raziskovalci interneta in modernih tehnologij, katerih delovanje je utemeljeno na pretoku uporabnikovih podatkov, na zmožnostih beleženja tega toka in analize tako zabeleženih podatkov za različne namene. Prav eksponentno naraščajoče sposobnosti beleženja in analize uporabniških podatkov sodobnih komunikacijskih tehnologij sprožajo možnosti posegov v pravico do zasebnosti uporabnikov – posameznikov, ki z uporabo tehnologij za seboj puščajo prenekatere elektronske sledi, ki so bile še pred nekaj desetletji neslutene, panoga pa jih lahko čedalje bolj s pridom uporablja za izboljšave svojih produktov, za trženjske aktivnosti, prilagajanje produktov in storitev ter zavarovanje pred zlorabami. Vedenjsko oglaševanje, torej prilagajanje vsebine posameznemu uporabniku in prakse prilagajanja cen točno določenim uporabnikom spleta so modeli delovanja, ki se v elektronskem komuniciranju čedalje hitreje razvijajo in ki temeljijo na izrabi polnega potenciala podatkov, ki jih uporabniki puščamo za seboj. Pogosto v tem kontekstu zasledimo argumente, da so uporabniški podatki prosto dostopni na spletu, da so jih ti sami objavili, da so privolili v njihovo obdelavo (čeprav za nenatančno opisane namene), da pravzaprav ne gre za analizo osebnih podatkov, temveč meta podatkov, kot je npr. naslov IP, ali identifikacijska številka piškotka, pri katerem uporabnika ni mogoče prepoznati po imenu in priimku, tako da pri obdelavi podatkov in ciljanju na konkretnega posameznika torej ne gre za poseg v njegovo

pravico do informacijske zasebnosti. Odgovore na te in podobne dileme podajajo različni avtorji, pogosto z zelo različnih vidikov in raziskovalnih tradicij.

Celostno informacijsko zasebnost obravnava Floridi (2006), ki razume identiteto posameznika in njegovo informacijsko sfero kot celoto – posameznik je hkrati tudi informacija (Floridi, 2006, str. 111). Informacijske zasebnosti tako ne obravnava le v okviru koncepta posameznikove lastnine svojih podatkov, ampak razvije širši pogled, po katerem razlikuje med pasivno in aktivno informacijsko zasebnostjo (pravica posameznika, da drugi ne posegajo v njegovo informacijsko sfero in priznavanje prostora informacijske zasebnosti drugim) ter svari pred poenostavljenim dojemanjem informacijske zasebnosti v okviru javne in zasebne sfere. Tudi v javni sferi ima posameznik pravico do informacijske zasebnosti. Ta razsežnost je posebej pomembna v okolju elektronskega komuniciranja, v katerem je posameznikova infosfera podvržena večjim pritiskom, kot so prikrito zbiranje podatkov, rudarjenje po podatkih, profiliranje ipd. (Floridi, 2006, str. 117).

Nissenbaumova (2010) v svojem vplivnem delu Zasebnost v kontekstu obravnava naraščajoče grožnje zasebnosti s strani informacijskih tehnologij in njihovih čedalje večjih zmožnosti zbiranja, hrambe, analize in posredovanja osebnih podatkov. Informacije, zbrane v posameznem kontekstu, so tako zelo pogosto uporabljene za druge namene ali posredovane neprimernim tretjim strankam. Množični (komercialni) nadzor, ki smo mu posamezniki rutinsko podvrženi, pa vpliva na možnosti, ki so nam ponujene, in na ceno, ki jo plačamo za blago in storitve. Hkrati so vse naše dejavnosti vsakodnevno ali posledično oplemenitene s podatki. Nissenbaumova (2010) je v tem kontekstu opredelila koncept moralno primernega toka osebnih podatkov, pri katerem so norme, ki omejujejo tok, kontekstualno opredeljene. Kršitev kontekstualnih norm pomeni nekaj slabega, odgovornost za utemeljevanje kršitev pa mora biti na strani kršiteljev. Za primer navaja zdravnika, ki posameznikove osebne podatke lahko zakonito posreduje drugemu specialistu, hkrati pa bi posredovanje tržnikom ali delodajalcu brez pacientovega soglasja pomenilo kršitev norm (Nissenbaum, 2010, str. 24).

V poznejšem prispevku, v katerem analizira predlog zakonodaje o varovanju informacijske zasebnosti v ZDA, je Nissenbaumova (2015) tudi podrobneje opredelila koncept spoštovanja konteksta, ki naj bi bil eden od temeljev pravice do informacijske zasebnosti. Pri tem razlikuje med kontekstom v smislu tehnološke platforme ali sistema, kontekstom v smislu sektorja ali

panoge, kontekstom v smislu poslovnega modela ali prakse ter kontekstom v smislu družbene domene. Med analizo praktičnih posledic je pokazala na slabosti prvih treh konceptualizacij kot preširokih in ki dopuščajo velike posege v zasebnost posameznikov na račun prevladujočih interesov platform, panoge in poslovnih modelov, ter je pokazala na pomembnost zadnje, ožje opredelitve konteksta kot družbene domene, kjer dejansko pridejo v poštev interesi posameznikov v posameznih družbenih situacijah (Nissenbaum, 2015). Če za kontekst npr. vzamemo panogo vedenjskega oglaševanja, so prakse, ki so zanjo sprejemljive, popolnoma drugačne od interesa posameznika. Ta razlika je npr. vidna med prevladujočim modelom rešitev *opt-out* in rešitev *opt-in*, ki posamezniku dejansko dajo več moči odločanja. Hkrati pa šele v odkrivanju, kaj vedenjsko oglaševanje v posameznih družbenih situacijah pomeni, zagledamo širšo problematiko. Vedenjsko oglaševanje kot orodje za politično trženje in promocijo političnih kandidatov tako npr. odpira popolnoma drugačne razsežnosti spornosti takih praks v smislu vpliva na demokratične procese. Enako velja za uporabo zdravstvenih podatkov za namen trženja prehranskih dopolnil, ki so lahko nekakovostna in škodujejo posameznikovi (pravilno ali ne) pripisani domnevni diagnozi. Razumevanje pravila spoštovanja konteksta mora biti torej precej ozko usmerjeno na posamezne družbene situacije, da lahko z njim razločimo med škodljivimi in manj škodljivimi praksami za zasebnost in druge človekove pravice.

Na kontekstualne norme pri raziskovanju zasebnosti na spletu napotuje tudi Martin (2015), ki, podobno kot Solove (2002), razlikuje (1.) vidik dostopa, pri katerem posamezniki nimajo možnosti ali pričakovanj glede zasebnosti, (2) vidik nadzora nad obdelavo informacij, ki ga povezuje predvsem z uveljavljanjem načel pravičnega informiranja (angl. *fair information principles*)[40] in (3.) kontekstualno določene norme, ki pomenijo izpogajane norme oz. dogovore glede zasebnosti v posamezni družbi ali situaciji. Glede zasebnosti oz. predvsem informacijske zasebnosti na spletu je razvil svoje videnje pomembnosti zadnje kategorije, tj. kontekstualnih norm oz. norm glede zasebnosti, ki so v svojem bistvu družbene pogodbe, tihi dogovori, ki jih posamezniki in družbene skupine sklepajo v različnih kontekstih, skupnostih in odnosih, pri čemer te zajemajo tako makro kot tudi mikro družbene pogodbe. Tako lahko norme zasebnosti obravnavamo kot trajnostne in vzajemno dobrodošle. Tudi raziskave kažejo, da je velika večina posameznikov pripravljena deliti podatke o sebi v okviru vzpostavljenega

[40] Pri tem je treba dodati pojasnilo, da se to nanaša na sistem v ZDA, kjer so načela pravičnega informiranja prevladujoč model regulacije zasebnosti *online.*

odnosa ali posamezne skupnosti ali ekipe, torej v konkretnem kontekstu, v katerem je jasno, kakšna so pravila glede varovanja zasebnosti (Marin, 2015, str. 553).

Obravnava zasebnosti z vidika družbene pogodbe jasno poudarja prednosti, ki jih ima sklenitev in upoštevanje take pogodbe za podjetja in organizacije, tudi v smislu poslovne etike – če poznajo pričakovanja potrošnikov oz. državljanov glede zasebnosti v posamezni situaciji in ravnajo po pričakovanjih, to pozitivno vpliva na nakupne namene in verjetnost, da bodo posamezniki poslovali z organizacijo, saj spoštovanje pogodbe poveča zaupanje v organizacijo, nasprotno pa nespoštovanje vodi v negativne odzive potrošnikov in posameznikov (Cases in drugi, 2010; Eastlick in drugi, 2006; McCole in drugi, 2010, v Marin, 2015, str. 553). Martinova ugotavlja, da pogled z vidika družbene pogodbe usmerja fokus stran od nuje pridobivanja soglasja posameznika za obdelavo njegovih podatkov, ki je pogosto dvomljivo veljavno, k odgovornostim organizacije, da ustvari pogoje, ki ustrezajo obema stranema in pomenijo trajnostni dogovor (Martin, 2015, str. 553). Koncept zasebnosti kot družbene pogodbe temelji na (1.) vrsti informacij, (2.) kdo ima dostop do informacij in (3.) kako so informacije uporabljene znotraj dane skupnosti. Na različnih primerih nato avtorica pokaže nezadostnost konceptualizacije zgolj z vidika omejevanja dostopa ali nadzora nad informacijami in prednosti pristopa družbene pogodbe, ki omogoča uvid v dejansko stanje, pri katerem posamezniki delimo informacije o sebi, vendar ne neomejeno. Če npr. delimo podatke s ponudnikom družbenega omrežja, to ne pomeni, da se strinjamo s tem, da jih posreduje drugemu ponudniku – čeprav je to morda zapisano v pogojih uporabe. Morda se ne strinjamo s tem, da informacije uporabi za drugačen namen, itd. (Martin, 2005, str. 557).

Treba je seveda razumeti, da avtorica pri konceptualizaciji zasebnosti na spletu izhaja iz realnosti sproščene regulacije v ZDA, kjer je zasebnost na spletu pogosto dojeta kot pogodbena potrošniška pravica, iz česar izhaja poplava izjav o zasebnosti, pri čemer ponudniki storitev niso omejeni glede namenov, za katere smejo uporabljati podatke posameznikov, niti glede njihovega posredovanja – če so to jasno navedli in posameznika obvestili. Resničnost v EU je drugačna, saj je varstvo osebnih podatkov temeljna človekova pravica, glede temeljev, ki jih Martinova navaja, pa obstaja tako podrobna zakonodaja kot tudi bogata praksa sodišč. Temelji varstva osebnih podatkov, kot je v EU zakonsko urejeno, so prav v omejenem naboru osebnih podatkov, ki jih sme obdelovati organizacija, kot tudi v preprečevanju njihove uporabe za druge namene in s strani drugih organizacij. Vse to je

mogoče le ob pogoju, da za rabo podatkov, ki se razlikuje od prvotne, obstaja primerna pravna podlaga – običajno privolitev posameznika. Prav v tem delu pa je tudi na ravni EU aktualen prispevek Martinove (2015) in njen poziv k odmiku od soglasja in premiku k večji odgovornosti podjetij. Ta prehod miselnosti vidimo udejanjen tudi v novem pravnem okviru za varovanje osebnih podatkov v EU, v katerem je prav odgovornost (angl. *accountability*) upravljavcev eden novih nosilnih temeljev, praktična orodja, s katerimi bodo upravljavci iskali odgovore na vprašanja, kakšna zasebnost je v dani situaciji pričakovana, pa bodo obsegala npr. izdelavo ocen vpliva na zasebnost in sprejem ustreznih ukrepov za njihovo omejitev, vzpostavitev odgovornih oseb za varstvo osebnih podatkov itd.

Za razumevanje praks vedenjskega oglaševanja in vpliva na pravico do informacijske zasebnosti je zanimivo tudi vprašanje neenakosti med posamezniki, katerih podatki se obdelujejo (najpogosteje brez njihove vednosti), in organizacijami, ki podatke za namen oglaševanja obdelujejo. Brunton and Nissenbaum (2016) vprašanje neenakosti (asimetrije) razumeta v smislu razlike med tistimi, ki so in tistimi, ki niso informirani (angl. *information haves and have-nots*), pri čemer razlikujeta med neenakostjo v moči in znanju. Neenakost moči izhaja iz dejstva, da posamezniki običajno nimajo moči odločanja o tem, kaj se bo dogajalo z njihovimi osebnimi podatki ali kako bo njihova uporaba vplivala nanje. Neenakost v znanju pa je posledica dejstva, da večina ljudi ignorira ali v najboljšem primeru le slabo zaznava zbiranje, agregiranje, analizo in deljenje njihovih podatkov. Avtorja priznavata, da številne organizacije morajo zbirati podatke posameznikov, nasprotujeta pa temu, da je zbiranje povezano z velikimi neenakostmi moči in znanja. Primeroma omenjata videonadzor, pri katerem, čeprav je kamera posameznikom vidna, ti nimajo informacij, kaj se dogaja s posnetki, komu se posredujejo in za katere namene se obdelujejo, oziroma še bolj perečo problematiko velikega podatkovja (angl. *big data*), pri katerem posameznikom niso znani nameni nadaljnje obdelave takih podatkov, niti načini njihove analize ali predvidevanj (Brunton and Nissenbaum, 2016).

3.2.3 Pristop vedenjske ekonomije

Vedenjska ekonomija ponuja uvide v vedenje uporabnikov elektronskih komunikacij, posebej v paradoks, pri katerem zatrjujejo, da si želijo več zasebnosti in ne želijo sledenja na spletu, hkrati pa s svojim vedenjem tega ne izkazujejo in ne izrabijo možnosti, ki so jim dane za

nadzor nad obdelavo njihovih osebnih podatkov (npr. le klikajo na polja »strinjam se«, ne prilagodijo nastavitev zasebnosti, na družbenih omrežjih delijo velike količine podatkov o sebi itd.).

Avtorji ugotavljajo, da je posameznikom zasebnost pomembna, vendar imajo težave z ravnanjem v skladu s svojimi preferencami (Acquisti in Grossklags, 2017; Cranor in McDonald, 2010). Deloma tudi zato, ker je preprosto manipulirati z vrednostjo, ki jo pripisujejo svojim osebnim podatkom (Acquisti in drugi, 2013a). Prav tako na posameznike vplivajo različni predsodki, ki njihovo vedenje zapeljejo v eno ali drugo stran.

Predsodek *statusa quo* (angl. *status quo bias*) se nanaša na to, da smo ljudje nagnjeni k temu, da obdržimo privzete možnosti in ne izvajamo sprememb. To pojasnjuje, zakaj posamezniki ne spreminjajo pogosto privzetih nastavitev in raje obdržijo stanje, kot je nastavljeno privzeto, čeprav to pomeni, da se npr. strinjajo z obširnim sledenjem na spletu. Zato je panogi zelo pomembna razlika med privzetimi nastavitvami *opt-in* oz. *opt-out*. Če mora posameznik sam vklopiti sledenje in s tem spremeniti začetno nastavitev, je velika verjetnost, da tega ne bo storil, kar pa pomeni slabši izplen za panogo (Zuiderveen Borgesius, 2014, str. 298).

Predsodek kratkovidnosti (angl. *myopia bias*) pa se nanaša na to, da ljudje stremimo k čimprejšnji nagradi in nismo pozorni na prihodnje stroške in posledice neke naše odločitve. Če ima spletna stran »zid«, pri katerem se mora uporabnik strinjati z vsemi pogoji, da lahko uporablja storitev, je velika verjetnost, da se bo strinjal in ignoriral morebitne prihodnje slabosti tega (Zuiderveen Borgesius, 2014, str. 298).

Predsodek prevelike samozavesti in optimizma se povezuje s kratkovidnostjo. Ljudje s(m)o nagnjeni k podcenjevanju možnosti nesreč in bolezni ter precenjevanju možnosti dolgega življenja. Podcenjujejo možnosti kraje identitete in reidentifikacije anonimiziranih podatkov (Acquisti in Grossklags, 2005, v Zuiderveen Borgesius, 2014, str. 292). Poleg tega je veliko odvisno od načina, kako so informacije predstavljene, ohlapnejši jezik, izbira prijaznejših izrazov, izpostavljene informacije o zasebnosti, čeprav pomanjkljive, vključevanje ikon, ki naj bi pomenile varovanje podatkov, čeprav dejansko to ni nujno, itd. so možnosti, ki uporabnika zlahka zavedejo v prepričanje, da varuje svojo zasebnost (Zuiderveen Borgesius, 2014, str. 292).

3.3 Okvir za preučevanje danes veljavne in prihodnje regulacije področja vedenjskega oglaševanja

Kot nakazujeta predhodni poglavji, je vedenjsko oglaševanje na spletu povezano s številnimi dilemami, tako glede njegove učinkovitosti in prednosti, ki jih prinaša deležnikom ekosistema elektronskega komuniciranja, kot tudi glede negativnega vpliva na pravice uporabnikov spleta in v splet povezanih naprav. Da bi lahko začeli razmišljati o učinkoviti izrabi prednosti vedenjskega oglaševanja, je zaradi omenjenih negativnih eksternalij torej potreben premislek o prihodnji regulaciji, s katero bi lahko vedenjsko oglaševanje pridobilo zaupanje.

Na pristope k regulaciji vedenjskega oglaševanja poleg dilem v zvezi z varovanjem pravic posameznikov močno vplivajo značilnosti trgov elektronskih komunikacij in odnosi med različnimi deležniki. Trgi elektronskih komunikacij so namreč zaznamovani s koncentracijo moči v rokah peščice multinacionalnih korporacij (Van Couvering, 2003; Noam, 2009; Pariser, 2011). Pomembna razsežnost je tudi konkurenčnost trgov v razmerju med ZDA in EU ter deloma tudi sodelovanje med tema silama (Goldsmith in Wu, 2006). Bistveno vprašanje za regulacijo področja je, kje je ravnotežje med interesi panoge in posameznikov ter kako se to ravnotežje spreminja.

Raziskovanje procesov regulacije oglaševanja in komuniciranja nujno vodi prek znanj normativne teorije, ki se sprašuje, kako naj bi mediji delovali, če naj izpolnijo naša pričakovanja glede svojega prispevka družbi in razvoju (McQuail, 2002, str. 16). Normativna teorija poudarja, da so mediji vpeti v naše družbeno, moralno in politično življenje in je zaradi tega včasih pri omejevanju njihovega delovanja potreben zunanji poseg. Koncept javne sfere, v kateri se oblikuje javno mnenje, ki nadzoruje oblast (Habermas, 1974), je eden temeljnih v tem okviru. Mediji naj bi delovanje javne sfere omogočali, zato se v literaturi pogosto pojavljajo premisleki o potencialnem prispevku interneta k delovanju civilne družbe (npr. Poster, 1995; Dahlgren, 2005; Bennet, 2003; Benkler, 2006). Hkrati pa Dahlgren (2005) ugotavlja, da je za internet, enako kot za stare medije, značilna postopna komercializacija (Dahlgren, 2005, str. 151). V imenu težko opredeljivega javnega interesa, pogosto v nasprotju s komercialnim ciljem medija, so vzniknili načini regulacije medijev, ki naj bi zagotavljali njihovo odgovornost za produkcijo družbeno zaželenih dobrin, zagotavljanje dostopa do informacij tudi tistim, za katere ni ekonomskega razloga (Feintuck, 2004). Zaradi negativnih

učinkov, ki jih ima vedenjsko oglaševanje na pravice uporabnikov informacijskih tehnologij ter zaradi »zapiranja« interneta s strani peščice velikih ponudnikov storitev (kot so npr. iskalniki – okno v svet za povprečnega uporabnika) so tudi v okviru vedenjskega oglaševanja razmeroma hitro vzniknile razprave o regulaciji te aktivnosti, ki bi zagotavljala spoštovanje pravic uporabnikov.

V nadaljevanju sledijo opredelitve koncepta regulacije in razlogov za regulacijo vedenjskega oglaševanja, predstavljeno je področje internetnih politik oziroma specifike in značilnosti reguliranja interneta ter posamezne strategije regulacije, ki so in bi lahko bile uporabljene pri urejanju praks vedenjskega oglaševanja. Vprašanja, na katera iščemo odgovore, vključujejo tematiko ustreznosti trenutno prevladujoče samoregulacije, vlogo strožje zakonodaje, regulacije s kodo, zasebnosti prijaznih tehnologij, certificiranja, izobraževanja, ocen vplivov na zasebnost in koncepta vgrajene zasebnosti. V tem okviru bomo v zaključku pogledali tudi na področje družbene odgovornosti podjetij, ki bi lahko prinesla pomembne odgovore na vprašanja negativnih posledic vedenjskega oglaševanja.

3.3.1 Teoretični vidiki razlogov za regulacijo vedenjskega oglaševanja

Regulacijo najbolj običajno pojmujemo kot dejavnost nadzora nekega javnega organa nad aktivnostmi, ki za družbo pomenijo neko vrednost oziroma neželene posledice. Hkrati pa sem spadajo tudi dejavnosti, ki želene dejavnosti omogočajo. Baldwin in Cave (1999) koncept regulacije razlagata širše, in sicer kot:

- skupek pravil, ki jih uveljavljajo nadzorni organi, določeni za ta namen (npr. glede varstva pri delu);
- namenski vpliv države – regulacija v tem smislu pomeni vse dejavnosti države, ki so usmerjene k vplivanju na korporativno ali družbeno vedenje: pravila, pa tudi drugi načini vplivanja, kot so ekonomske spodbude (davki, nadomestila), pogodbena razmerja, licenciranje, razkrivanje informacij itd.;
- vse oblike družbenega nadzora in vpliva – ne le s strani države, temveč tudi s strani drugih akterjev (trga) (Baldwin in Cave, 1999, str. 2).

Kot je bilo že pojasnjeno, regulacija običajno vznikne v imenu obrambe javnega interesa oziroma javnega dobrega, ki ga trg sam, brez zunanjega posega ne zagotovi. Teorije javnega interesa tako poudarjajo vlogo regulatorjev oz. nadzorih organov kot zaupanja vrednih, strokovnih akterjev, ki učinkovito zasledujejo ta javni interes. Argumenti, ki takemu stališču nasprotujejo, vključujejo dejstvo, da je javni interes včasih težko enoznačno opredeliti in da obstajajo različne interpretacije, ki se med seboj ne skladajo nujno. Prav tako je vprašljiva neodvisnost, strokovnost in učinkovitost nadzornih organov, pri čemer regulacija lahko postane »ujeta« s strani ekonomsko in politično opredeljenih interesov panoge in ne javnega interesa. Rezultat take regulacije je očitana neučinkovitost pri zagotavljanju javnega dobrega. Nasprotno teorije interesnih skupin poudarjajo, da je regulacija plod odnosov med različnimi skupinami in državo. Ne vodi je iskanje javnega interesa, ampak predvsem tekmovanje za prevlado. Teorije zasebnih interesov podobno regulacijo obravnavajo predvsem kot plod zasledovanja zasebnih oz. korporativnih ciljev po večanju ekonomskih interesov. Regulacija se glede na pristop teorije življenjskega cikla začne zaradi obrambe javnosti pred neželenimi dejavnostmi, ustvarjeno je nadzorno telo, ki v začetku deluje zagnano, čez čas se njegova strokovnost poveča, hkrati pa čedalje bolj drsi k interesom panoge in neučinkovitemu nadzoru. Teorije moči idej poudarjajo, da včasih za regulatornimi akcijami slonijo predvsem politične ideje in intelektualni koncepti, institucionalne teorije pa vloge ne pripisujejo le ekonomskim interesom, ampak tudi institucionalnim strukturam in dogovorom v družbi ter družbenemu napredku, ki pomembno zaznamujejo oblikovanje regulacije (Baldwin in Cave, 1999, str. 18–33).

Če se osredinimo le na tehnične razloge za regulacijo in pustimo ob strani vprašanja politične ali ekonomske motiviranosti, vidimo, da regulacija običajno vznikne iz situacije, v kateri neregulirani trg ne deluje v skladu z določenim javnim interesom (ne glede na to, kdo in kako ta javni interes določi). Med običajne razloge spadajo:

— monopolni položaj ponudnika: ker ponudnika ne omejuje konkurenca, to vpliva na reduciran produkt, višjo ceno ter prenos prihodka od potrošnika k ponudniku. Monopolni položaj nastane, kadar en sam ponudnik obvladuje trg, kadar edinstven produkt nima dovolj bližnje zamenjave in kadar obstajajo precejšnje ovire za vstop drugih podjetij na trg in je izstop težaven;

— ekscesni profit: kadar zaradi neke danosti, odkritega bogatega vira ali podobne situacije, povezane s srečo in ne investicijo, en ponudnik pride do ekscesnega profita;

— zunanji učinki oz. eksternalije: kadar cena blaga ali storitve ne odslikava resničnih stroškov, ki vključujejo tudi druge negativne zunanje učinke, npr. onesnaževanje okolja;
— nezadostna informiranost potrošnikov: konkurenčni trg lahko deluje ustrezno le, če so potrošniki dovolj informirani, da lahko ocenijo konkurenčne produkte. Če potrošniki iz različnih razlogov (visoka cena informiranja, nizka zavzetost za informiranje in nagnjenost k zavajanju, nizka sposobnost potrošnikov, da preverjajo točnost informacij) ne prejmejo dovolj informacij, lahko razkritje dostopnih in točnih informacij naloži regulacija in tako spodbudi razvoj zdravega trga;
— dostopnost storitve: kadar ponudba storitve na posameznih območjih ali v obdobjih ni dobičkonosna, je pa pomembna za javno dobro, lahko regulacija naloži obveznost ponudbe tudi potrošnikom na takih območjih oz. v takih obdobjih (npr. univerzalna storitev telekomunikacij);
— nekonkurenčno vedenje in dumpinške cene: cilj je njegovo preprečenje in vzpostavitev konkurence na trgu;
— javno dobro in moralni hazard: nekatere dobrine pomenijo prednosti za vse (npr. zdravstvo, obramba), vendar pa obstaja problem neplačnikov, ki kljub temu izrabljajo te dobrine, čeprav jih plačujejo drugi;
— neenaka pogajalska izhodišča: npr. na področju delovnih razmerij, kjer v odnose zato poseže regulacija, ki omejuje močnejšega;
— omejenost naravnih virov: ko lahko pri njihovem razdeljevanju prevladajo merila glede na javne interese in ne le cenovno merilo (npr. radijski spekter);
— distribucija javnih dobrin: kjer je potrebna redistribucija javnih dobrin ali prenos virov tistemu, ki utrpi škodo;
— racionalizacija in koordinacija: kadar bi bilo zelo drago, da bi posamezniki ali manjše skupine s ponudniki sklepale posamezne učinkovite dogovore, lahko pogoje predpiše regulacija ali standardi;
— načrtovanje: trgi običajno ne skrbijo za blaginjo prihodnjih generacij, ampak le za trenutne potrebe potrošnikov, zato temu namenu služi regulacija (Baldwin in Cave, 1999, str. 9–17).

Iz tega lahko izluščimo številne razloge za regulacijo vedenjskega oglaševanja – od elementov monopolnega položaja največjih ponudnikov vedenjskega oglaševanja na različnih

ravneh spletnih storitev do dobrobiti prihodnjih generacij, ki so pri trenutnem razvoju tehnologij za vedenjsko oglaševanje vsekakor vprašljive – od skoraj monopolnega položaja največjih ponudnikov Googla in Facebooka do negativnih zunanjih učinkov, ki vključujejo poseg v temeljne pravice posameznikov. Za trg vedenjskega oglaševanja je značilna velika informacijska asimetrija – nezadovoljivo informiranje uporabnikov spleta. Ker so posamezniki tudi za opravljanje dnevnih opravkov prisiljeni uporabljati internet, je dejstvo, da so pri tem tudi izpostavljeni komercialnemu sledenju, lahko razlog za regulacijo v smislu dostopnosti storitve in javnega dobrega. Prav tako lahko v odnosu velikih ponudnikov, kot sta Google in Facebook, in uporabnikov vidimo odnos neenakih moči, v katerem so uporabniki pogosto prisiljeni v strinjanje s splošnimi pogoji.

Od razlogov za regulacijo področja vedenjskega oglaševanja se obrnimo k načinom regulacije. Lessig regulacijo na internetu razume kot splet in preplet prava (zakonodaje), družbenih norm (npr. pravil obnašanja pri spletnih storitvah), trga (cenovne dostopnosti ipd.) ter arhitekture omrežja (koda: kdo lahko uporablja storitev in kako). Spremembe katerekoli razsežnosti imajo posledice na druge, bodisi jih krepijo ali slabijo. Njegov argument je, da lahko v primeru posamezne neželene dejavnosti ali njene posledice regulacija poteka prek vseh štirih razsežnosti in ni nujno, da se bo npr. pravna izkazala kot najučinkovitejša (Lessig, 2006, str. 122–125).

O načrtovanju tehnologije in arhitekturi omrežja oziroma po njegovih besedah »kodi kot načinu regulacije« obširno razpravo prispeva Lessig (2006). Njegova teza je, da je »regulabilnost« interneta, torej zmožnost regulacije interneta, povezana z odgovori na vprašanje: kdo je naredil kaj in kje? Arhitektura interneta je bila načeloma načrtovana tako, da mreža sama ne beleži odgovorov na ta vprašanja, ampak dopušča uporabo vsakemu, ki uporablja za to potreben protokolni sklad TCP/IP in se je tako zmožen povezati v internet. Jedro mreže je preprosto, saj je njegova edina naloga pošiljanje digitalnih paketov po mreži, inteligenca pa je na končnih točkah, t. i. načelo *end to end* in s tem povezano načelo nevtralnosti omrežja, pri katerem mreža ne razlikuje med različno vsebino in aplikacijami (video, e-pošta itd.) in ne daje prednosti nobeni specifični vrsti prometa ali vsebine, kar pomeni, da imajo vsi paketi enake možnosti dostave. Ti načeli sta omogočili razvoj interneta in inovativnih storitev, saj omrežje ni bilo podvrženo korporativnim interesom, ki bi

prednostno obravnavali le nekatere informacije, druge vsebine pa bi ostajale v ozadju (Lessig, 2006, str. 38–61, tudi Wu in Goldsmith, 2006, str. 23).

Zmožnost reguliranja interneta tako ni v omrežju samem, ampak na njegovih koncih, ki so prek razvoja razvijali različne sposobnosti beleženja odgovorov na zgornje vprašanje, tako da so se morali uporabniki pred uporabo storitev avtenticirati (Kdo?), tako da se beležijo dostopi do storitev, s piškotki itd. (Kaj?). Vse to se dogaja z vidika različnih interesov, komercialnih, pa tudi interesov pregona nezakonitih dejanj na spletu. Odgovor na vprašanje »Kje?« je pomemben predvsem z vidika pregona nezakonitih dejanj, saj je pristojnost nadzornih organov še vedno določena z mejami v fizičnem svetu, čedalje bolj pa določanje geolokacije uporabnikov omogoča tudi komercialne prednosti prilagajanja storitev in ponudbe. Tehnologije, ki so omogočile učinkovitejše poslovanje na internetu, so posledično prinesle tudi večje možnosti za nadzor in regulacijo dejavnosti. (Lessig, 2006, str. 38–61).

Z drugimi besedami, če ni mogoče regulirati neke dejavnosti na internetu neposredno, jo je mogoče posredno, tako da neposredno reguliramo tehnologijo, ki vpliva na dejavnost, torej reguliramo s kodo. Lahko npr. reguliramo možnosti dostopa do interneta, tako da je zahtevan izkaz z osebno identifikacijo – arhitektura omrežja tako odloča, kaj ljudje lahko počnejo. Koda tako postaja čedalje pomembnejši element regulacije, vprašanja, kaj koda dopušča, kdo jo je ustvaril in kdo ga nadzoruje, pa so v okviru regulacije kibernetskega prostora čedalje pomembnejša (Lessig, 2006, str. 77–78).

3.3.2 Strategije regulacije vedenjskega oglaševanja

Strategije regulacije so raznolike, vsaka pa ima prednosti in slabosti. Baldwin in Cave (1999, str. 34–62) sta jih razvrstila v naslednje skupine: pravila in nadzor, samoregulacija, spodbude, ukrepi za vzpostavljanje trga (konkurenčno pravo, franšize in licence, reguliranje s pogodbami, dovoljenja, s katerimi je mogoče trgovati), dolžnost razkritja, neposredno vpletanje, zakonodaja o pravicah in obligacijah, javna nadomestila in socialno zavarovanje. V nadaljevanju so predstavljene glavne značilnosti strategij, ki so ali bi lahko bile uporabljene na primeru vedenjskega oglaševanja.

1. Pravila in nadzor

Bistvo so jasna pravila in sankcije za kršitve pravil, ki jih določa zakonodaja in uveljavljajo regulatorji. Standardi so določeni na minimalni ravni dopustne dejavnosti. Nalaganje sankcij naj bi zahtevale močan nadzorni organ. Pomanjkljivosti vključujejo poseganje v učinkovito vodenje podjetij, nagnjenost k »ujetosti«, postavljanje kompleksnih pravil in težnjo k prenormiranju področja. Je neprožna in draga za izvajanje. Postavljanje dobrih standardov je težavno in drago, pri čemer panoga teži k spoštovanju minimalnega praga, ne pa višjih standardov (Baldwin in Cave, 1999, str. 39–41).

2. Samoregulacija

Običajno vključuje organizacijo ali panožno združenje, ki razvije sistem pravil in jih v svojem krogu članstva nadzoruje in kršitve sankcionira. V ta okvir spadajo tudi različne certifikacijske sheme, pečati in kvalifikacije. Tako panoga obdrži ob strani nadzor države in pravila, ki bi jih postavili zunanji akterji. Samoregulacija je lahko popolnoma prostovoljna in precej neformalna, lahko pa jo zapoveduje tudi zakonodaja, ki lahko določa tudi sankcije in lahko določa odobritev pravil samoregulacije. Prednosti vključujejo višjo predanost spoštovanju pravil, ki si jih panoga določi sama, dobro informiran postopek uveljavljanja pravil in oblikovanja standardov, večjo učinkovitost pri ugotavljanju kršitev in postopkih za podajo prijav kršitev. Na negativni strani pa je treba upoštevati ceno, ki jo ima odobravanje pravil, »ujetost« s strani panožnih interesov, pri čemer so pravila prav tako lahko neprožna in legalistična, dodatno pa so lahko postopki sprejema in izvajanja pravil netransparentni in s pomanjkanjem odgovornosti do javnosti. Samoregulacija je lahko učinkovita strategija v kombinaciji z drugimi pristopi, kot prvi odziv na neželeno dogajanje – šele če samoregulacijski pristopi niso učinkoviti, je čas za zunanje postavljanje pravil in kaznovanje (Baldwin in Cave, 1999, str. 39–41, 63–65).

3. Ekonomske spodbude

Regulacija z ekonomskimi spodbudami (bodisi davkov za tiste, ki ne dosegajo določenih standardov, ali olajšave za tiste, ki jih dosegajo) je lahko učinkovita, saj pomeni malo stroškov za regulatorja in malo njegove vpletenosti v odločanje, s tem pa tudi manjšo stopnjo »ujetosti«. Vodje podjetij so svobodni pri odločanju o svojih dejavnostih in usklajevanju svojih finančnih obveznosti. Na negativni strani pa vidimo kompleksen sistem pravil, ki spremlja tak način reguliranja (npr. sistem davkov), potreben je nadzor nad spoštovanjem

pravil, ki je lahko drag in na koncu postane tak sistem regulacije podoben prvi strategiji »pravil in nadzora« (Baldwin in Cave, 1999, str. 41–44).

4. Dolžnost razkritja

Zapovedovanje dolžnosti razkritja informacij je oblika regulacije, ki ne posega v produkcijski proces, v produkt, ceno in porazdelitev produkta sam po sebi, ampak prepoveduje le posredovanje nepopolnih ali zavajajočih informacij o produktu oziroma zapoveduje posredovanje nekaterih informacij (kot npr. sestavo pri prehranskih izdelkih, količine soli, maščob itd.). Informacije lahko javnosti posreduje tudi regulator. Razkritje informacij pa naj bi potrošniku (pa tudi državljanu oz. volivcu) omogočilo, da sam sprejme odločitev glede produkta in sprejemljivosti njegove proizvodnje. Negativni vidiki izhajajo iz dejstva, da (1.) posamezniki niso nezmotljivi, morda uporabijo informacije nepravilno, morda ne razumejo posledic, ki izhajajo iz podatkov, narobe presodijo tveganja, ne zberejo vseh relevantnih informacij, nimajo virov za podrobnejšo raziskavo problematike, in tako kljub vsemu pride do škodljivih posledic zanje; (2.) lahko se na informacije ne odzovejo predvideno oz. racionalno, morda kupujejo le po enem merilu (npr. ceni) in se ne odzovejo na informacije glede nevarnosti produkta; (3.) cena produkcije informacije je lahko visoka, prav tako stroški pregledovanja informacij, saj posamezniki pogosto nimajo virov, da bi lahko pregledali in preverili vse informacije o produktih. V takem primeru so lahko pravila, ki temeljijo na ekspertizi regulatorja, učinkovitejša; (4.) pri nekaterih produktih so tveganja lahko tako velika, da zgolj informiranje vpletenih ne bi doseglo učinka in bi bilo primerneje uporabiti strategijo pravil in nadzora; (5.) vedno obstaja nevarnost, da informacije niso točne in zavajajo. Včasih so potrebni standardi sporočanja, ki zagotavljajo, da bodo lahko posamezniki informacije ustrezno uporabili. Zato je uporaba te strategije predvsem učinkovita tam, kjer nevarnost posameznikom ni velika, kjer posledice med nizko- in visokokakovostnimi produkti nimajo resnih posledic, kjer produkcija informacij ni draga, kjer so posamezniki sposobni razumeti in uporabiti informacije ter kjer je mogoče nadzorovati točnost podanih informacij, ne da bi pri tem nastali nerazumni stroški (Baldwin in Cave, 1999, str. 49–50).

5. Zakonodaja o pravicah in dolžnostih

Namesto strategije pravil in nadzora za akterje lahko zakonodaja določa pravice posameznikom, ki bi bili podvrženi škodljivim dejanjem ali posledicam, in jim omogoča možnost civilne tožbe zoper povzročitelja škode. V ekonomskem smislu je taka strategija

učinkovita, kadar je izogibanje škodnim dejavnikom za povzročitelje cenejša, kot bi bilo povračilo škode po civilnem deliktu. Pri tem je treba upoštevati, da tožba za posameznika pomeni strošek in da marsikje niso omogočene možnosti skupinskih tožb, ki za povzročitelja pomenijo večjo ekonomsko izpostavljenost. Težava so tudi zavarovanja odgovornosti, ki odvrnilni učinek dodatno omejujejo (Baldwin in Cave, 1999, str. 51–53).

Proces regulacije sestavljajo tri faze: sprejem zakonodaje oz. pravil, ustvarjanje nadzornih organov in pravil ter uveljavljanje teh pravil med osebami ali organizacijami, na katere želimo vplivati ali jih nadzorovati. Zadnja faza, uveljavljanje pravil oziroma nadzor, je ključna za uspeh celotnega procesa regulacije, saj pravila brez uveljavljanja lahko ostanejo le črka na papirju, prav tako pa premočno ali neprimerno uveljavljanje spodkoplje celoten sistem regulacije. Cilj izvrševanja pravil je doseganje skladnosti s pravili, pri čemer imajo regulatorji poleg pregona oziroma sankcioniranja kršiteljev na voljo tudi neformalna sredstva, kot so izobraževanje, svetovanje, prepričevanje in pogajanja. V primeru slednjih je najbolj poudarjena komponenta doseganja skladnosti z zakonom, pri prvem načinu izvrševanja pravil pa je pomembnejše doseganje odvrnilnega učinka in kaznovanja. Procesi kaznovanja so za regulatorja dražji in vključujejo večjo porabo virov kot svetovalno in izobraževalno ravnanje. Poleg tega so pogosto togi in zato lahko postanejo neučinkoviti. Avtorji tako predlagajo kombinacijo različnih načinov izvrševanja zakonodaje, in sicer glede na težo dejanj, ponavljajočih kršitev, resnosti posledic ali odgovornosti kršiteljev. Pri postavljanju pravil pa je treba upoštevati omejitve zgoraj pojasnjenih pristopov: za kaznovanje morajo biti natančnejša, poleg tega se odpre tudi vprašanje ustvarjalne skladnosti in previsoke ali prenizke vključenosti zaradi slabo določenih pravil (Baldwin in Cave, 1999, str. 96–106).

Vprašanje je tudi, kdaj regulator poseže v dogajanje – s preventivnim delovanjem, posegom v primeru določenih dejanj ali v primeru nekaterih škodljivih posledic dejanj, pri čemer je včasih težko določiti, kakšno škodo je posamezno dejanje povzročilo, tudi v primeru posegov v osebnostne pravice in zasebnost. V primeru nekaterih dejanj so lahko tako sankcije nižje, saj škoda še ni nastala, po nastali škodi pa so sankcije višje. Med sankcije pa ne spada le pregon kaznivih dejanj oziroma prekrškov, ampak tudi administrativne sankcije, katerih del je lahko naložitev poprave določenih nepravilnosti, odprave škodljive dejavnosti itd. Denarne globe lahko gospodarski subjekti štejejo za svoje poslovne stroške in jih celo prevalijo na potrošnike

ali zaposlene, zato so popravljalna dejanja zelo pomemben del sankcioniranja (Baldwin in Cave, 1999, str. 96–106).

Pri odločanju o strategiji regulacije je potreben realističen premislek o učinkovitostih posamezne strategije, ki v resničnosti nikoli ne deluje brez napak in pomanjkljivosti. Primerjave strategije pravil in nadzora z drugimi, manj restriktivnimi strategijami v smislu izvajanja in nadzora morajo upoštevati različne vidike. Čeprav je lahko drag in zapleten nadzor pomanjkljivost, je mogoče tudi nadzor oblikovati prožneje in učinkoviteje. Poleg tega tudi preostale strategije na neki točki vključujejo nadzor nad pravili, le da pravila ne določajo materialnih pogojev, ampak obrobno posegajo v dejavnost in določajo, kdo prejme spodbudo, kdo in kako mora razkriti informacije itd. Prav tako se je treba zavedati, da lahko običajno za eno področje aktivnosti soobstaja več regulacijskih strategij, ki vsaka deluje s svojega vidika –osnove za izvajanje dejavnosti lahko urejajo pravila, hkrati pa obstajajo tudi spodbude in v nekaterih vidikih samoregulacija. Morda obstajajo določbe glede razkritja informacij, hkrati pa so ponudniki izpostavljeni tudi civilnim tožbam. Ključno pri takih prepletih regulacijskih strategij pa je, kako oceniti učinkovitost regulacije (Baldwin in Cave, 1999, str. 56–57).

Za odločitev, ali je sistem regulacije dober, sprejemljiv ali morda potreben reforme, ni dovolj le ocena, ali prinaša ekonomsko korist, ampak kot menita Baldwin and Cave (1999), da je situacijo treba presoditi po petih merilih: zakonodajnega mandata, odgovornosti in nadzora, procesnih varoval, strokovnosti in učinkovitosti. Regulacija izpolnjuje prvo merilo, če je podprta z odločitvijo zakonodajalca, ki izraža voljo ljudstva, in če regulator izpolnjuje mandat, ki mu je bil podeljen. Tukaj so težava nejasno opredeljeni mandati regulatorjev, ki so lahko podvrženi različnim razlagam. Odgovornost regulatorja javnosti in nadzor s strani demokratičnih institucij sta nujna, če želimo govoriti o dobri regulaciji, prav tako procesna varovala – regulator mora zagotavljati postopke, ki so pošteni, dostopni in transparentni. Enaka obravnava in konsistentnost odločanja ter možnost sodelovanja javnosti in drugih zainteresiranih strank v postopkih pred regulatorjem so ključni s tega vidika. Težava nastane npr. pri tehtanju učinkovitega izvajanja mandata in obširnih procesnih varoval, ki vplivajo na hitrost in ekonomičnost postopkov. Izvajanje posameznih funkcij regulacije zahteva strokovno znanje in presojo, še zlasti kadar je treba tehtati med nasprotujočimi interesi ali v situaciji nepopolnih informacij. V takem primeru zanašanje na strokovnost regulatorja nadomesti utemeljevanje, hkrati pa se lahko pojavijo dvomi v dejansko strokovnost, saj

javnost običajno ni usposobljena za preverjanje pravilnosti odločitev. Zadnje merilo je učinkovitost regulatorja, kar pomeni, da naj bi svoj mandat izvajal z najmanjšimi možnimi sredstvi in je pri produkciji učinkovit. Učinkovitost je v praksi težko meriti zaradi nejasno opredeljenih mandatov, ker ni primerljivih podatkov o delovanju drugih strategij regulacije. Učinkovitost pomeni tudi, da regulacija vodi k rezultatom, ki so učinkoviti, kar pa ne zadeva nujno ekonomskih kazalcev, ampak lahko tudi družbene cilje in neekonomske cilje. Zato je presojanje regulacije predvsem glede na njeno ekonomsko učinkovitost (analiza stroškov in koristi) lahko zelo problematično. Presojanje vseh meril lahko pripelje do vprašanj tehtanja med njimi in kompromisov. Kakšni kompromisi med merili še pomenijo dobro regulacijo, pa je na koncu običajno vprašanje osebnih političnih prepričanj in svetovnonazorskih pogledov na svet, čeprav velik del razprave zaznamuje stopnja, do katere je mogoče izboljšati eno od meril, ne da bi posegli v druge. V praksi je tako regulacijo mogoče izboljšati s premišljenimi izboljšavami vsakega od meril (Baldwin in Cave, 1999, str. 76–85).

Akademskih prispevkov na temo celostne regulacije vedenjskega oglaševanja, ki bi upoštevali splet in preplet različnih možnih strategij, ni, saj se raziskovalci ukvarjajo predvsem z izboljšavami na pravnem področju (kot npr. Zuiderveen Borgesius, 2014). Eno ključnih vprašanj za regulacijo vedenjskega oglaševanja je vprašanje nadzora posameznika nad obdelavo njegovih osebnih podatkov. Varovanje pravic uporabnikov na spletu je namreč ključno za njihovo zaupanje v ponudnike storitve, saj bo le zaupanje vodilo v večjo uporabo storitev elektronske družbe (Burnik, 2011a). Pri tem pa privolitev zaradi svojih izkazanih slabosti ni vedno najoptimalnejše orodje možnosti nadzora. V tem kontekstu je zelo pomembno tudi izobraževanje in opolnomočenje uporabnikov (McDonald in Cranor, 2009).

Zuiderveen Borgesius (2014) v svoji raziskavi obravnava vprašanje, kako izboljšati varovanje zasebnosti posameznikov v kontekstu vedenjskega oglaševanja (v okviru prostora EU in zakonodaje v EU), ne da bi nesorazmerno omejili panogo in ugotavlja, da bi bilo treba izboljšati (1) ukrepe za opolnomočenje posameznikov in (2) ukrepe za varovanje posameznikov ter oba pristopa kombinirati. Trenutno regulacija temelji na pravnih pristopih za opolnomočenje, ki pa niso dovolj uspešni, zato bi moral zakonodajalec več pozornosti nameniti pravilom, ki varujejo – torej omejujejo in prepovedujejo nekatere prakse. Med ukrepi za opolnomočenje posameznikov vidi strožji nadzor nad določbami o preglednosti obdelave osebnih podatkov, o obveščanju posameznikov – da se zmanjša informacijska

asimetrija na tem področju, ter zahteve po obvestilih v jasnem in dostopnem jeziku. Pravila bi morala jasneje določati, kakšna mora biti privolitev in zahtevati, da gre pri tem za opt-in in ne opt-out. Prav tako zagovarja, da bi pravila glede zasebnosti v elektronskih komunikacijah morala zahtevati privolitev za vedenjsko oglaševanje in ne za tehnologije za sledenje, ki so v ozadju. Priporoča upoštevanje razvoja standarda »ne-sledi«. Za izboljšanje varovanja posameznikov bi moral biti nadzor nad zakonodajo o varstvu osebnih podatkov učinkovitejši, zakonodaja sama pa izboljšana. Med elemente, ki bi izboljšali učinkovitost nadzora, prišteva večje sankcije, ki bi jih imeli možnost izrekati nadzorni organi, ter možnosti kolektivnih tožb posameznikov zoper kršitelje. Omenja tudi nujnost izboljšav na področju nadzora nad podjetji iz tretjih držav, ki izvajajo vedenjsko oglaševanje na EU trgu. Zakonodaja bi morala biti stroga in jasneje določati načelo najmanjšega obsega podatkov; če upravljavec ne more zagotavljati izvajanja načela preglednosti, bi morala zakonodaja jasno določati, da je taka obdelava podatkov nezakonita. Tukaj izrecno omenja spletne dražbe uporabniških profilov v realnem času. Zakonodaja bi morala dosledno urejati vse ponudnike komunikacijskih storitev (trenutno za ponudnike dostopa – telekome veljajo strožja pravila). Predlaga posebno specialno zakonodajo, ki bi veljala za vedenjsko oglaševanje in bi zajemala vse faze tega procesa: zbiranje podatkov, hrambo podatkov, analize, razkrivanje podatkov in uporabo za vedenjsko oglaševanje. Predlaga tudi prepoved »zidov« in različnih možnosti vzemi ali pusti, ki jih upravljavci spletnih strani uporabljajo kot mehanizem za privolitev, ter prepoved, da vedenjsko oglaševanje izvajajo javni RTV-servisi in upravljavci, financirani z javnimi sredstvi (Zuiderveen Borgesius, 2014, str. 412–423). Na tej točki velja opomba, da prenovljeni okvir za varstvo osebnih podatkov, sprejet leta 2016, marsikaterega od teh predlogov že vsebuje.

Glede na zapisane izzive in dileme pa se zdi, da zgolj urejanje z zakonodajo in čedalje podrobnejšimi pravili ni prava pot, ampak bi bila kombinacija različnih orodij regulacije za iskanje ravnotežja med interesi učinkovitejša, prav tako sodelovanje regulatorjev in panoge pri iskanju tehničnih standardov. Glede tega je bistvena povezava zakonodaje s samoregulacijo in regulacijo s kodo (tehničnimi standardi), opolnomočenje in izobraževanje javnosti ter preskok od določanja pravil k etiki in družbeni odgovornosti izvajalcev vedenjskega oglaševanja.

3.3.4 Pristop družbene odgovornosti

V iskanje okvirov za prihodnje urejanje elektronskega komuniciranja in novih tehnologij, ki vsebujejo komponente nadzora in posega v zasebnost posameznikov pa se v zadnjem času čedalje bolj vpleta pristop družbene odgovornosti (King, 2012). Pollach (2011) je umestil informacijsko zasebnost v okvir družbene odgovornosti podjetij, in sicer kot etično odgovornost, ker zgolj zakonodaja na področju ne zajema vseh vidikov obdelave podatkov. Meni, da bi tak pogled lahko pripomogel k iskanju ravnotežja med željo uporabnikov po zasebnosti in med interesi podjetij po uresničitvi poslovnih ciljev (Pollach, 2011).

Izkušnje kažejo, da zgolj poseg v obliki zunanje regulacije pri sodobnih tehnologijah za varstvo interesov in pravic posameznikov ne zadošča. Pravni okviri vedno zaostajajo za silovitim razvojem tehnologije, ki prinaša vedno nove etične izzive. Samoregulacija ima tudi slabe plati. Zato je v teoretskih pristopih čedalje večji poudarek na različnih orodjih, s katerimi lahko posamezen subjekt oceni potencialne negativne vplive konkretne tehnologije in skuša kot družbeno odgovoren te negativne vplive zmanjšati oziroma obvladati; to so npr. koncept vgrajene zasebnosti (angl. *privacy by design*) ali ocene vplivov na zasebnost oz. etične standarde (angl. *privacy/ethical impact assessment*) (Carsten Stahl, 2011; Wright in de Hert, 2012).

Družbena odgovornost organizacij ni povezana le z odgovornostjo podjetij, da uporabijo svoje vire za večanje profita, ob tem pa ostajajo znotraj določenih pravil ravnanja, ampak zajema širši nabor odgovornosti: ekonomsko in pravno (ki sta zahtevani), etično (ki je pričakovana) in filantropsko (ki je zaželena) (Ferrell in drugi, 2000, v Chen, 2009, str. 523). Pomemben je politični vidik družbene odgovornosti podjetij, ki opredeljuje vlogo ponudnikov spletnih storitev z vidika zagotavljanja političnih pravic. Bauer (2009) denimo delovanje največjih spletnih akterjev preučuje v vidika njihovih odgovornosti v smislu koncepta državljanstva. Preučuje tudi tematike civilnih, družbenih in političnih pravic, ki jih spletni akterji po eni strani omogočajo, po drugi pa lahko tudi zavirajo (Bauer, 2009). Zavedanje glede posledic, ki jih ima delovanje podjetij ali organizacij na družbo, je zelo pomembno, še zlasti v okviru tehnološkega napredka in inovacij, ki imajo lahko daljnosežne posledice na delovanje in zgradbo družbe. Akterji v sistemu vedenjskega oglaševanja bi se morali truditi odkrivati in

razumeti negativne posledice svojih praks na družbo in družbene procese ter ravnati odgovorno, v najširšem pomenu družbene odgovornosti.

Kot argumentira Rogers (2003) z vidika difuzije inovacij, so posledice spremembe, ki se zgodijo na ravni posameznikov ali družbenega sistema kot rezultat sprejema ali zavračanja inovacij. Difuzija inovacij v družbo namreč lahko povzroči nepričakovane negativne posledice, ki se razkrijejo šele po dolgem času, ko uporaba inovacije že preide v splošno rabo.[41] Ker so raziskave uvedbe neke inovacije običajno usmerjene v preučevanje pozitivnih oziroma neposrednejših posledic inovacij, daljnosežne posledice, ki se poleg vsega lahko pokažejo v neki drugi strukturi v družbi ali sistemu, niso v središču pozornosti. Prav tako je daljnosežne posledice težko raziskovati brez večletne ali desetletne kvalitativne raziskave, posledice je težko meriti in jih zaradi njihove kulturne pogojenosti včasih tudi težko zaznati zunanjemu raziskovalcu. Kot poudarja Rogers (2003), so lahko posledice pričakovane ali nepričakovane, zaželene ali nezaželene in posredne ali neposredne. Kot primer navaja tehnološke inovacije, povezane z razvojem interneta, ki ima za nekatere pozitivne, za druge pa negativne posledice v smislu digitalnega razkoraka. Pri uvajanju inovacij je običajno zaželeno doseganje dinamičnega ravnotežja (angl. *dinamic equilibrium*), pri katerem se spremembe uvajajo s hitrostjo, s katero lahko družba sledi tem spremembam in se jim prilagaja, ne da bi pri tem nastajale škodljive posledice. Dejstvo je namreč, da uvajanje inovacij poveča socialne razlike med zgodnjimi in poznejšimi uporabniki inovacij. Inovacije, še zlasti kadar zahtevajo nekaj sredstev, v razslojeni družbi povečajo neenakost. Ob uvajanju inovacij je tako potrebna posebna skrb z vidika manjšanja razkoraka v družbi, npr. prek informiranja šibkejših, z urejanjem dostopa do inovacije za šibkejše. Na primeru digitalnega razkoraka lahko vidimo pomembnost urejanja dostopa do spleta šibkejšim in v regijah v razvoju ter delovanja na področju tehnološke in medijske pismenosti (Rogers, 2003, str. 541, 542), vse to pa je še kako relevantno za področje vedenjskega oglaševanja, na katerem je zasebnostna ločnica dejstvo, nepoznavanje posledic osebne prilagoditve vsebin pa ima številne negativne posledice za demokratično ureditev (glej npr. Taddeo in Floridi, 2014).

Chen (2009) področje družbene odgovornosti organizacij obravnava z vidika teorij družbenih omrežij, saj so prav omrežja in njihova širitev eden bistvenih vidikov poslovanja organizacij.

[41] Med primeri, ki jih avtor navaja, je npr. uvedba snežnih vozil, ki so sicer olajšala življenja plemenu na Finskem, vendar se je hkrati zaradi motorizacije dolgoročno popolnoma spremenila njihova družbena struktura, saj so opustili gojenje jelenov, ki so jih prej uporabljali tako za transport kot tudi za prehrano in trgovanje. Inovacija na področju transporta je tako pomenila neželene posledice v drugih sistemih družbe.

Analiza spletnih družbenih omrežij kaže, kako so akterji v omrežju neposredno in posredno povezani, in se ne omejuje na razmerja med le dvema stranema. Razmerja med akterji ter njihov položaj v omrežju vplivata na njihove pravne in družbene odgovornosti (Chen, 2009, str. 524). Eden pomembnih vidikov vpletenosti organizacij v spletna družbena omrežja je, da so odgovorne za posledice svojih dejanj, pa tudi za posledice dejanj drugih, nad katerimi imajo določeno moč (Amaeshi in drugi, 2008). Moč in vpliv akterja v omrežju pa izvira tako iz strukture omrežja kot tudi z akterjevega položaja v omrežju. Chen (2009) je tako glede na značilnosti spletnih družbenih omrežij (kakšni so odnosi med akterji, kakšno vlogo v omrežju zaseda en akter, kakšno je povezovanje v podskupine, kakšno je omrežje kot tako) opredelil vplive na posredno in neposredno odgovornost. Večjo odgovornost tako nosijo akterji, ki zasedajo položaje z več moči. Ponudniki virov so odgovorni za posledice teh virov. Dejanja akterjev, ki imajo v omrežju osrednji položaj, bolj vplivajo na druge. Člani neke skupine imajo večji vpliv drug na drugega kot na nečlane ipd. Skladno z močjo in vplivom akterja v omrežju bi morali razumeti tudi njegovo odgovornost. Tako Chen omenja primer Googla in Facebooka, ki zasedata osrednja položaja v omrežju, saj njune storitve vsak dan uporablja ogromno uporabnikov. Ti ponudniki se zaradi svoje osrednje vloge in vloge povezovanja med drugimi člani (omogočanja njihove komunikacije) tudi zavedajo marsikaterih dejanj drugih akterjev v omrežju in imajo lahko določeno odgovornost tudi s tega vidika (Chen, 2009).

Taddeo in Floridi (2016) sta analizirala moralne odgovornosti ponudnikov spletnih storitev, za katere menita, da imajo v informacijskih družbah nedvomno osrednjo vlogo. Hkrati pa še ni konsenza, katera načela naj bi oblikovala njihove moralne odgovornosti, ki segajo onkraj skladnosti s trenutnimi pravnimi omejitvami (Taddeo in Floridi, 2016, str. 1575). Osredinjata se na moralne odgovornosti ponudnikov spletni storitev pri upravljanju z vsebinami, ki so na voljo na spletu, in sicer na tri široke teme z etičnimi posledicami. V okviru teme organizacije in upravljanja dostopa do informacij (popačenje informacij) poudarjata kontroverznost osebne prilagoditve informacij, saj so njene posledice za družbene procese, povezane z demokratičnim diskurzom in omejevanjem možnosti izpostavljenosti različnim mnenjem, virom, kulturnim okoljem ter izkušnjam, lahko obsežne, čeprav lahko osebna prilagoditev pripomore k učinkovitejšemu filtriranju informacij, bistvenih za posameznika. Cenzuriranje in svoboda govora, druga široka etična tema, zajema preprečevanje dostopa do škodljivih vsebin, ki ga izvajajo ponudniki storitev (nezakonite vsebine, npr. otroška pornografija, sovražni govor in druge vsebine, ki so škodljive posameznikom ali družbi). Po drugi strani pa

se lahko omejevanje vsebin izvaja tudi kot del zasledovanja političnih agend. Za vsebine, ki jih objavljajo uporabniki, ponudniki storitev pravno načeloma niso odgovorni, vendar se hkrati pričakuje, da spremljajo in filtrirajo vsebine, ki krožijo na spletu. Zasebnost uporabnikov je tretja etična tematika, v okviru katere Taddeo in Floridi (2016) ugotavljata, da ima sicer lahko prostovoljno deljenje podatkov na spletu široke negativne posledice za zasebnost posameznikov, saj se podatki lahko uporabijo za povsem drugačne namene od originalnih in so posamezniki podvrženi stalnemu nadzoru. Ponudniki storitev, še zlasti spletna družbena omrežja, so tako odgovorni za razvrednotenje zasebnosti, saj usmerjajo uporabnike, da še več delijo. Etično odgovornost bi pokazali, če bi ponujali storitve in ukrepe, s katerimi bi posamezniki imeli kar največji nadzor nad svojimi podatki oziroma bi že v oblikovanju svojih storitev upoštevali ukrepe za čim manjšo obdelavo podatkov (Taddeo in Floridi, 2016, str. 1579–1597).

Da je ponudnike spletnih družbenih omrežij nujno obravnavati z vidika njihovih moralnih odgovornosti, ugotavlja tudi Light (2010), saj je le tako mogoče razkriti kompleksna etična vprašanja in posledice njiho uporabe. Hkrati prispevkov z etičnega področja ni v izobilju, saj je veliko pomanjkanje raziskovanja njihovih moralnih vrednot. Zavajanje, razžalitve in podobni pojavi so del etično spornih praks, prisotnih v okviru družbenih omrežij. S tehničnega vidika je lahko tehnologija zasnovana tako, da prinese družbi čim večjo korist, lahko pa je v središču predvsem uporabnost storitve za uporabnike, brez premisleka o neželenih posledicah tehnologije (Light, 2010). Tak je običajno pogled razvijalcev storitev, ki omejujejo le, kaj uporabniki lahko ali česa ne smejo početi na spletnem družbenem omrežju, oziroma jih predvsem zanima reševanje trenutnih problemov, nimajo pa veliko interesa za globlje probleme (Light, 2010; Wakunuma in Carsten Stahl, 2014). Tehnologija naj bi bila sama po sebi nevtralna, in kot taka nezmožna biti nosilec moralnih odgovornosti. Tak pogled ne omogoča odkrivanja širših etičnih posledic in pomeni tudi težavo z vidika uvajanja odgovornih inovacij v okoljih, ki jih vodi imperativ dobičkonosnosti. Zato je potreben premislek o robustnejšem vnosu vsebin etike in odgovornih inovacij v izobraževanje o informacijskih sistemih (Wakunuma in Carsten Stahl, 2014, str. 393).

Če sklenemo, pristop družbene odgovornosti prispeva pomemben kamen v mozaik teoretskega razumevanja vedenjskega oglaševanja, predvsem prek tukaj poudarjenih konceptov moralne odgovornosti ponudnikov in izvajalcev takega oglaševanja, da razmišljajo o posledicah, ki jih imajo njihove prakse na širšo družbo in pravice posameznikov, onkraj

področja učinkovitejšega trženja storitev in izdelkov s pomočjo osebno prilagojenih pristopov. Ključno je, da bi se izvajalci vedenjskega oglaševanja morali negativnih posledic zavedati, jih pričakovati ter delovati moralno odgovorno. Pomemben je tudi premislek o tem, da bi kot družba morali aktivneje pristopiti k vzpostavljanju dinamičnega ravnotežja ob inovacijah na področju strojnega učenja in umetne inteligence, ki sta čedalje pogosteje uporabljena v okviru vedenjskega oglaševanja, in preprečiti večanje razslojevanja v družbi zaradi diskriminatornih odločitev tehnologije.

3.4 Postavitev celostnega teoretskega okvira

Razsežnosti problematike vedenjskega oglaševanja so številne. Dotikajo se vprašanja učinkovitosti in koristnosti vedenjskega oglaševanja z vidika ponudnikov in porabnikov, vprašanja glede vpliva vedenjskega oglaševanja na vsakdanje življenje posameznikov, njihove pravice in družbene procese ter vprašanja regulacije zasebnosti pri vedenjskem oglaševanju. Poleg tega lahko vedenjsko oglaševanje, njegove implikacije in regulacijo raziskujemo na mikro, meso in makro ravni, ki vključuje implikacije za posameznike, oglaševalski ekositem in širšo politično, ekonomsko in družbeno dinamiko (po Frynas in Stephens 2014, 485). Problematika vedenjskega oglaševanja kot smo jo predstavili v našem pregledu literature, je zelo komplesna in v veliki meri presega okvir tržnega komuniciranja, znotraj katerega se vedejsko oglaševanje razvija. Okvir tržnega komuniciranja je za razumevanje vedenjskega oglaševanja teoretsko nepopoln. Kot smo ugotovili, k vedenjskemu oglaševanju pristopa na funkcionalističen oz. utilitarističen način, pri čemer ponuja omejen pogled na družbeno (in ekonomsko) vlogo vedenjskega oglaševanja v sodobni digitalni družbi. Zato smo s pomočjo zgornjega pregleda literature pripravili sintezo pristopov, ki bi osvetlili različne dimenzije vedenjskega oglaševanja. S pomočjo multi-teoretskega pristopa smo poskusili oblikovati konceptualni okvir, s katerim bi bilo mogoče raziskovati razsežnosti vedenjskega oglaševanja in razumeti fenomen na celostni način. Bistvenega pomena se nam je zdelo vključiti uvide študij, ki se posvečajo vlogi medijev v vsakdanjem življenju posameznikov, politične ekonomije komuniciranja, vedenjske ekonomije, teorij informacijske zasebnosti ter normativne teorije in pristop družbene odgovornosti (Tabela 3.1).

Tabela 3.1: Multi-teoretski konceptualni okvir za razumevanje ključnih dilem in vprašanj glede vedenjskega oglaševanja in njegove regulacije

Ključne dileme/vprašanja	Teoretski pristop in avtorji	Odgovori, ki jih pristop ponuja.
Kako učinkovito je VO v primerjavi z drugimi oblikami digitalnega oglaševanja?	**Teorije tržnega komuniciranja** (npr. Ha, 1996; Schneider in drugi, 1984; Seitz in Zorn, 2016; Kang, 2011; Stallworth, 2010; Goldfarb in Tucker, 2010b; Beales, 2010; Picker, 2009; Busch, 2016; Chen in Stallaert, 2014; Aksu in drugi, 2018)	VO je učinkovito, ker je za posameznika relevantno in se nanaša na njegove specifične interese v določenem času ter ga lahko nagovori kontekstu primerno, čemur prispeva napredek na področju avtomatiziranega oglaševanja v realnem času in širitev uporabe na naprave v internetu stvari. Pretvorba v nakupno vedenje naj bi bila zato večja, čeprav niso prednosti za vse subjekte na trgu enake. Največ pridobijo glavni ponudniki sistemov takega oglaševanja.
Kaj VO pomeni za uporabnike? Koliko uporabniki lahko uveljavljajo svoje pravice?	**Študije s fokusom na občinstvu in medijih v vsakdanjem življenju** (npr. Silverstone, 1999; Livingstone, 2002; Lievrouw in Livingstone, 2006a; Couldry, 2009; Zittrain in Palfrey, 2008; Benkler, 2001; Turkle, 2008, Luthar, 2010; Luthar in Črnič Oblak, 2015; Hepp, 2010)	Sodobne komunikacijske tehnologije in mediji so vpeti v vsakodnevno življenje posameznikov, procesi mediatizacije so vseprisotni. Pomemben za razumevanje pristop družbenega oblikovanja informacijsko-komunikacijskih tehnologij. Medijska potrošnja se spreminja (večja interaktivnost in »množenje« osebnih medijev v vsakdanjem življenju), prav tako razmerja med občinstvom in mediji. Uporabniki novih medijev lahko izbirajo načine uporabe, lahko so hkrati tudi ustvarjalec vsebine. Po eni strani to pomeni opolnomočenje posameznikov, po drugi ustvarja digitalne ločnice. Občinstvo v novih medijih naj bi bilo bolj avtonomno, aktivno, vendar je predvsem pri globalno najbolj priljubljenih storitvah to utvara, saj so izbire posameznika tam zelo omejene, čemur lahko prištejemo tudi negativne posege v njegove pravice.
Kaj VO pomeni v okviru razvoja panoge za uporabnike in druge deležnike?	**Politična ekonomija komuniciranja** (npr. McDonald in Cranor, 2009; Mansell, 2004; Mosco, 1996, 2009, 2016; McQuail, 2002; Grant, 2006; Mosco, 2016; Bakardjieva, 2013; Baym, 2013; Crain, 2016; Van Dijck in Poell, 2013; amon Prodnik, 2013)	Odkriva politično ekonomske moči, ki vladajo na trgu novih medijev in ponudnikov naprednih storitev vedenjskega oglaševanja. Ponudnike komunikacijskih storitev obravnava kot predvsem komercialne organizacije in poudarja koncept poblagovljenih občinstev. Ti pridejo v okviru digitalnega oglaševanja še posebej do izraza, saj oglaševalci dejansko kupujejo občinstva, pri najbolj sofisticiranem vedenjskem oglaševanju pa celo posamezne osebe, njihove profile. Izpostavlja vprašanja uspešnih ponudnikov spletnih storitev (iskalniki, spletna družbena omrežja itd.) kot vratarjev do informacij na spletu, pri čemer poudarja njihove komercialne cilje. Odkriva vprašanja konkurence, razmerja moči na trgu ponudnikov elektronskih komunikacij, razmerja moči med ponudniki, uporabniki, regulatorji in drugimi deležniki.
Koliko je VO invazivno in posega v pravice uporabnika (do zasebnosti)? Kako učinkoviti so pristopi za varovanje zasebnosti?	**Teorije informacijske zasebnosti** (npr. McDonald in Cranor, 2009; Woo, 2006; Westin, 1967; Perri, 1998; Rule, 2007; Floridi, 2006; Solove, 2002, 2006; Nissnbaum, 2010; Martin, 2015)	Poudarjajo bistvo in zgodovinski razvoj pravice do zasebnosti, pomen pravice do zasebnosti in varstva osebnih podatkov v sodobnem svetu elektronskih komunikacij in v okviru vedenjskega oglaševanja. Prav tako poudarja negativne plati vedenjskega oglaševanja v smislu izgube zasebnosti, uporabe podatkov za druge, nepovezane namene, možnosti diskriminacije, širjenje družbe nadzora ter nujnosti regulacije za omejitev teh negativnih posledic.

	Vedenjska ekonomija (npr. Acquisti in drugi, 2013; Acquisti in Grossklags 2017)	Pojasnjuje paradoks zasebnosti: zakaj posamezniki cenijo zasebnost, vendar je pri svojem ravnanju v elektronskem komuniciranju ne ubranijo. Ne spreminjajo nastavitev, ki omogočajo deljenje svojih podatkov, ne izrabijo možnosti nadzora nad svojimi podatki in zasebnostjo, za majhne nagrade in prednosti pa so pripravljeni deliti intimne podrobnosti o svojem življenju. Razlogi za to so predsodki, ki jih imamo ljudje – da smo nagnjeni k ohranjanju *statusa quo*, kratkovidni in nas zapelje uokvirjanje v besedilu.
Kako vedenjsko oglaševanje posega v demokratične procese v družbi? **Kakšne so značilnosti in pomanjkljivosti veljavne regulacije VO v EU in ZDA?**	**Normativna teorija** (npr. Poster, 1995; Dahlgren, 2005; Bennet, 2003; Benkler 2006; Goldsmith in Wu, 2006; Baldwin and Cave, 1999; Zittrain, 2008; Castells, 2000; Silverstone, 2004; Goodman, Tambini in drugi 2017)	Poudarja vlogo medijev v družbi in demokratičnih procesih ter utemeljuje državno poseganje. Sprašuje se o javnem mnenju in medijih kot orodju za nadzor oblasti ter poudarja komercializacijo medijev in javni interes. Družba nadzora, digitalne ločnice in medijska pismenost so tematike, ki pomembno vplivajo na vprašanja regulacije medijev in komunikacijskih tehnologij. Pojasnjuje vlogo različnih načinov regulacije, zakonodaje, samoregulacije in drugih.
Kako VO urejati v prihodnje?	**Pristop družbene odgovornosti** (npr. King, 2012; Pollach, 2011; Carsten Stahl, 2011; Wright in de Hert, 2012; Rogers, 2003; Chen, 2009)	Informacijsko zasebnost umesti med družbeno odgovornost podjetij, procese vedenjskega oglaševanja pa osvetli z vidika etike, moralne odgovornosti za širše družbene posledice in iskanje ravnotežja med interesi podjetij in uporabnikov, trajnostnega razvoja in odgovornosti subjektov na trgu. S tega vidika je pomembna vloga novih orodij regulacije (vgrajevanje zasebnosti v tehnične rešitve, večja odgovornost podjetij itd.).

3.5 Raziskovalna vprašanja

Za ekosistem elektronskega komuniciranja so značilne za uporabnika brezplačne vsebine, ki jih izdajatelji financirajo z oglaševalskimi prihodki, zaradi česar oglaševanje neposredno vpliva na vsebino in kakovost storitev v elektronskem komuniciranju (LSE, 2009b). Ta funkcionalističnost dominantnega pristopa tržnega komuniciranja pri razumevanju vedenjskega oglaševanja se osredotoča predvsem na delovanje, koristi in učinkovitost tovrstnega oglaševanja, pri čemer poenostavljeno predpostavlja, da personalizacija nujno prinaša koristi za vse vpletene deležnike. Empirični del pričujoče disertacije želi nasloviti to pomanjkljivost in utrditi zavedanje o kompleksnosti vedenjskega oglaševanja ter njegove učinkovitosti za različne deležnike, ki vključuje tudi vprašanja o poseganju v zasebnost posameznikov, varovanja informacijske zasebnosti in (samo)regulacije. Na podlagi zapisanega in na podlagi pregleda literature ter zastavljenega konceptualnega okvira, v disertaciji odpiramo tri sklope raziskovalnih vprašanj za empirično raziskovanje, ki so predstavljeni in utemeljeni v nadaljevanju. Pristop tržnega komuniciranja predpostavlja, da naj bi bilo vedenjsko oglaševanje zaradi personalizacije bolj učinkovito (Goldfarb in Tucker, 2010a; Tucker, 2011), saj se uporabniki pozitivno odzivajo na zanje relevantne oglase (IAB Europe, 2010b). Rast digitalne oglaševalske industrije in z njo povezanih storitev naj bi pozitivno vplivala na konkurenčnost gospodarstev (WFA, 2010). V tem okviru nas bo zanimalo, kako učinkovito je dejansko vedenjsko oglaševanje in kaj razvoj tehnologij osebne prilagoditve oglasnih vsebin pomeni v okviru razvoja panoge vedenjskega oglaševanja in različnih platform, kakšne so posledice za založnike, oglaševalske mreže, ponudnike dostopa do interneta, manjša podjetja, velike multinacionalne korporacije, uporabnike in preostale deležnike (npr. organe pregona). Zanimali nas bodo predvsem pozitivni vidiki razvoja tehnologij za ciljanje v kontekstu različnih deležnikov, kar pa ne pomeni, da bo raziskovanje gradilo na idejah tehnološkega determinizma, kjer se družbeni napredek dojema kot posledica razvoja tehnologije. Prvo ključno raziskovalno vprašanje je:

1. Koliko je izvajanje vedenjskega oglaševanja na različnih platformah elektronskega komuniciranja učinkovito, kaj razvoj tehnologij vedenjskega oglaševanja pomeni v okviru razvoja relevantne panoge in kakšne so posledice za preostale deležnike?

Vpliv na zasebnost uporabnikov je eden bistvenih pomislekov pri izvajanju vedenjskega oglaševanja (npr. Tucker, 2011); pomembna so vprašanja privolitve uporabnikov v sledenje, transparentnosti oglaševanja, nadaljnje uporabe zbranih podatkov (Bohm, 2008; WP29, 2010a) in izobraževanja uporabnikov Uporabniki se namreč najpogosteje ne zavedajo vedenjskega oglaševanja in svojih pravic. Velike so razlike med tistimi, ki se problematike zasebnosti zavedajo, in tistimi, ki tega znanja nimajo (Woo, 2006). Ker uporabniki ne znajo uveljaviti svojih pravic do zavrnitve sledenja, samoregulacija tega področja ni učinkovita (McDonald in Cranor, 2009). Tudi mehanizem privolitve ni splošno zagotovilo za varovanje pravic uporabnikov, saj je to pogosto le navidezno prostovoljna privolitev (Woo, 2006, str. 958). V tem okviru nas zanima, na katerih temeljih je zasebnost posameznikov varovana v EU in ZDA, kakšne so razlike v pristopih obeh vodilnih sil na tem področju, kakšna je vloga zakonodaje, samoregulacije, koregulacije, regulacije s programsko kodo in kako uspešni so pristopi za varovanje pravic uporabnikov. Drugo raziskovalno vprašanje je sledeče:

2. Koliko je vedenjsko oglaševanje invazivno in posega v pravice uporabnikov elektronskih komunikacijskih tehnologij ter koliko so trenutni pristopi k varovanju informacijske zasebnosti uporabnikov uspešni?

Na pristope k regulaciji vedenjskega oglaševanja vplivajo značilnosti trgov elektronskih komunikacij in odnosi med različnimi deležniki. Trgi elektronskih komunikacij so zaznamovani s koncentracijo moči v rokah peščice multinacionalnih korporacij (Van Couvering, 2003; Noam, 2009; Pariser, 2011). Pomembna razsežnost je konkurenčnost trgov v razmerju med ZDA in EU ter deloma sodelovanje med tema silama (Goldsmith in Wu, 2006). Kje in kako je dojeto ravnotežje med interesi panoge vedenjskega oglaševanja in posameznikov ter kako se to ravnotežje spreminja? Ali je samoregulacija v kontekstu hitro razvijajoče panoge dovolj, ali pa je potrebna strožja zakonodaja (Boucher Ferguson, 2008), je eno od bistvenih vprašanj. Zelo pomembno je izobraževanje uporabnikov (McDonald in Cranor, 2009), razvoj morebitnih shem za certificiranje, pa je kljub pomanjkljivostim pogosto poudarjena tema (Pollach, 2011, str. 90). Koliko so že uporabljeni pristopi regulacije učinkoviti glede na merila dobre regulacije (Baldwin in Cave, 1999) in ali bi lahko za regulacijo uporabili tudi še nepreizkušene strategije? V tem okviru je zadnje, toda ključno raziskovalno vprašanje sledeče:

3. Kakšen naj bo okvir za regulacijo vedenjskega oglaševanja v prihodnosti, ob upoštevanju dejavnikov konkurence in sodelovanja med EU in ZDA, značilnosti trgov elektronskih komunikacij in odnosov med regulatorji, panogo vedenjskega oglaševanja in preostalimi deležniki? Kakšna naj bo vloga zakonodaje, samoregulacije, regulacije s kodo, zasebnosti prijaznih tehnologij,[42] certificiranja, izobraževanja, ocen vplivov in koncepta vgrajene zasebnosti?

[42] Angl. *Privacy Enhancing Technologies (PETs)*.

4 EMPIRIČNO RAZISKOVANJE VEDENJSKEGA OGLAŠEVANJA: METODOLOGIJA RAZISKAVE

Empirični del študije v nadaljevanju obsega poglobljen vpogled v predmet raziskovanja. Na raziskovalna vprašanja namreč odgovarja z uporabo kombinacije več metod (angl. *multimethod approach*). Hkrati sta uporabljeni dve kvalitativni metodi, dokumentarna analiza in ekspertni intervjuji, pri čemer ena od metod prevladuje, druga pa rezultate dopolnjuje (angl. *QUAL+qual*) (glej npr. Morse, 2003, str. 197; Hesse Biber, Rodrigues in Frost, 2015, str. 11). Problematiko skušamo pojasniti z več zornih kotov, pri čemer nam lahko pomagata izbrani metodi, saj omogočata povezovanje ugotovitev, njihovo dopolnjevanje in preverjanje.

Ekosistem vedenjskega oglaševanja in njegove regulacije je raziskan s podrobno dokumentarno analizo (analizo vsebine dokumentov regulatornega okvira v EU in ZDA, tj. zakonodaje, samoregulacije in standardizacijskih pristopov) ter z ekspertnimi, delno strukturiranimi intervjuji. Pri tem na ravni posameznega raziskovalnega vprašanja ena od metod običajno prevladuje, druga pa jo dopolnjuje. Prvo raziskovalno vprašanje obsega poznavanje panoge vedenjskega oglaševanja in njegove učinkovitosti. Prevladujoča metoda za pridobivanje podatkov so ekspertni intervjuji, dopolnjujoča pa dokumentarna analiza. Drugo raziskovalno vprašanje zajema negativne učinke na pravice posameznikov in njihove možnosti za obrambo ter veljavni regulatorni okvir za vedenjsko oglaševanje. Prevladujoča metoda je dokumentarna analiza, ugotovitve intervjujev pa rezultate bistveno dopolnjujejo. Tretje raziskovalno vprašanje sprašuje o prihodnjem okviru regulacije vedenjskega oglaševanja. Bistven prispevek tu prinašajo intervjuji, dopolnilno vlogo pa ima dokumentarna analiza. Empirična raziskava tako polno izrablja potencial kombiniranja metod, pri katerem je, kot poudarja Bazeley (2012), analiza vedno inherentno neurejena in večinoma eksperimentalna ter zaznamovana z inovativnimi načini kombiniranja metod za delo s podatki. Pri tem pa je nepogrešljiv dejavnik prožnost, pragmatičnost pri raziskovalnem načrtu in ustvarjalnost raziskovalca, da polno izrabi potencial kombiniranja podatkov za odgovore na raziskovalna vprašanja (Bazeley, 2012, str. 825).

Uporaba kombinacije različnih raziskovalnih metod gradi verodostojnost ugotovitev ter zmanjšuje pristranskost ugotovitev, ki bi bile utemeljene na le enem viru podatkov ali eni metodi raziskovanja (Patton, 1990). Analiza dokumentov je pogosto uporabljena v

kombinaciji z drugimi metodami pridobivanja podatkov (Denzin, 1970, str. 291), pri čemer prek uporabe različnih metod in virov podatkov raziskovalec išče povezave in podpira svoje ugotovitve. Dokumentarna analiza se tako lahko povezuje z drugimi viri podatkov, npr. intervjuji ali osebno udeležbo (Yin, 1994). V primeru pričujoče študije je kombinacija metod raziskave nujna, tako v smislu pridobivanja kvalitetnih podatkov kot tudi v smislu validacije podatkov in ugotovitev. Kombiniranje kvalitativnih metod, ki smo ga za raziskovalni načrt izbrali, običajno pomeni dva ločena vira podatkov in ločeno analizo podatkov, pri čemer pa se rezultati nato dopolnjujejo (Hesse Biber, Rodrigues in Frost, 2015, str. 11). Kombinacija metode analize dokumentov in ekspertnih intervjujev omogoča večjo verodostojnost rezultatov, saj so lahko navedbe intervjuvancev vedno soočene z ugotovitvami dokumentarne analize oziroma so lahko kritično ovrednotene glede na prejšnje ugotovitve. Na drugi strani pa ugotovitve intervjujev lahko postavijo ugotovitve dokumentarne analize v novo luč, odstirajo nove razsežnosti problematike in nove poglede na problematiko, npr. v primeru razlag zakonskih določb, ki so lahko na različnih ravneh različne.

V tem poglavju sledi podrobnejši opis metodologije, uporabljene za empirično raziskovanje vedenjskega oglaševanja. Pojasnjeni so postopki vzorčenja, zbiranja podatkov in analize dokumentov. Opisani so postopki vzorčenja pri ekspertnih intervjujih, njihova vsebinska zasnova in načini obdelave ter analize. Predstavljeni so tudi profili strokovnjakov, s katerimi so bili opravljeni intervjuji. Rezultati raziskave so zaradi obsežnosti predstavljeni v samostojnih poglavjih. Peto poglavje tako zajema rezultate dokumentarne analize, ki pojasnjuje regulatorni okvir za vedenjsko oglaševanje v EU in ZDA, v šestem poglavju pa so predstavljene ugotovitve analize ekspertnih intervjujev. Slednje so mestoma dopolnjene z ugotovitvami dokumentarne analize, predvsem, kadar bi zgolj navajanje ugotovitev intervjujev kazalo netočne ugotovitve, kar pripomore k validaciji rezultatov intervjujev. Kot opozarja Dexter (1970/2006, str. 27), je namreč metodo take vrste intervjuja zaradi veljavnosti rezultatov primerno kombinirati. Poglavje se sklene s sintezo primerjave ugotovitev dokumentarne analize in analize intervjujev, ki tabelarično prikaže, kako se ugotovitve glede na tri raziskovalna vprašanja povezujejo, kje se dopolnjujejo in podpirajo ter kje ugotovitve različnih metod raziskovanja odstopajo oziroma si nasprotujejo.

4.1 Analiza dokumentov

Hitro spreminjajoče regulatorno okolje raziskujemo s pomočjo analize regulatornega okvira za vedenjsko oglaševanje v EU in ZDA, torej s kritično analizo vsebine dokumentov zakonodajnega okvira in uveljavljene zakonodaje (ter nadzora), samoregulacijskih pristopov in standardizacijskih aktivnosti na tem področju. Analiziramo relevantne pravne akte (veljavne in predloge), smernice in mnenja pristojnih institucij, pravila samoregulacije, prispevke na področju certificiranja in standardizacije, tudi relevantne akademske prispevke – predvsem raziskovalcev s področja prava in tehnologije, zasebnosti in varstva osebnih podatkov. Glede tega nas predvsem zanima odgovor na drugo raziskovalno vprašanje, tj. koliko so trenutni pristopi k varovanju informacijske zasebnosti uporabnikov uspešni. Gradimo tudi znanje o ozadju in kontekstu za odgovor na tretje raziskovalno vprašanje, tj. kakšen naj bo okvir za regulacijo vedenjskega oglaševanja v prihodnosti.

V analizi obravnavamo le pravni okvir za varovanje zasebnosti in varstvo osebnih podatkov, čeprav, kot izhaja iz predhodnih poglavij, vedenjsko oglaševanje ne pomeni le posledic za posameznikovo pravico do zasebnosti in varstva osebnih podatkov, ampak je vpliv širši in se razteza tudi na druge pravice in interese (pravico do obveščenosti in pravico enake obravnave) ter demokratične procese (svobodne volitve, medijska pluralnost). S to študijo pa ni mogoče v dopustnem časovnem in prostorskem okviru globlje raziskati vseh posledic in pravnega okvira na vseh teh področjih.

Glede na to, da je temeljni proces vedenjskega oglaševanja za vse najrazličnejše namene nujno povezan z obdelavo osebnih podatkov posameznikov, je upoštevanje pravnega okvira na tem področju vsekakor bistvena predispozicija razumevanja omejitev. Prav tako je bila tudi večina posegov nadzornih organov doslej oprta le na to pravno področje. Disertacija tako ponudi celosten uvid v to pravno področje ob opozorilu, da je področje vedenjskega oglaševanja vsaj deloma (glede na različne namene, za katere se izvaja) urejeno tudi v okviru potrošniškega prava, nanj pa vpliva tudi pravo varstva konkurence, pravo urejanja volilnih procesov in financiranja političnih kampanj, pravni okvir glede pravice do obveščenosti, javnih RTV servisov ipd.

Metoda analize dokumentov pomeni proces pregleda in ocenjevanja raznovrstnih dokumentov ter njihove razlage. Raziskovalec s tem procesom izlušči pomen, gradi razumevanje dokumentov in razvija empirično znanje (Corbin in Strauss, 2008). Dokumenti lahko nastopajo v najrazličnejših oblikah, tiskani in elektronski, raziskovalcu pa lahko pomagajo odkrivati pomene in vpoglede, pomembne za raziskovalni problem (Marriam, 1988, str. 118). Naša študija obsega analizo velikega števila različnih dokumentov, predvsem povezanih z vprašanjem trenutnega okvira regulacije vedenjskega oglaševanja ter njegove učinkovitosti, in sicer glede na sistematizacijo orodij regulacije, ki izhaja iz teoretskega okvira (po Baldwin in Cave, 1999). Dokumenti obsegajo pravne vire, poročila, mnenja in stališča različnih deležnikov do vprašanja regulacije vedenjskega oglaševanja, raziskave o stališčih uporabnikov, študije, standardizacijske dokumente in akademske prispevke.

Analiza dokumentov je lahko uporabljena za več namenov: lahko gradi kontekst in ozadje raziskave, lahko implicira vprašanja za raziskavo, npr. nova vprašanja za izvedbo intervjujev. Lahko nastopa v vlogi dodatnega vira informacij, poleg primarne metode zbiranja podatkov. Na podlagi dokumentarne analize je mogoče slediti spremembam in razvoju posameznega pojava in verificirati ugotovitve na podlagi drugih metod analize (Bowen, 2009, str. 29–30). V naši raziskavi je dokumentarna analiza uporabljena tako za razumevanje konteksta regulatornega okvira za vedenjsko oglaševanje kot tudi za validacijo in preverjanje ugotovitev na podlagi ekspertnih intervjujev. Dokumentarna analiza je potekala preko celotnega procesa empiričnega raziskovanja, saj na to temo novi relevantni dokumenti nenehno nastajajo, že veljavni pa se dopolnjujejo in razvijajo (od zakonodaje do drugih dokumentov). Tako je bila dokumentarna analiza uporabljena tudi kot vir za oblikovanje novih vprašanj za intervjuje in kot dodaten vir informacij, tudi med izvedbo intervjujev. Ker gre za pojav v razvoju, pa je bila analiza dokumentov posebej uporabna tudi z vidika sledenja spremembam regulacije in pristopov k njej.

Bistveno je, da dokumenti ne morejo preprosto nadomestiti drugih virov podatkov, prav tako jih ni mogoče razumeti kot enoznačne dokaze – vedno je namreč potreben premislek o kontekstu, v katerem so nastali, in namenu, za katerega so bili ustvarjeni (Atkinson in Coffey, 1997, str. 47). To je še zlasti razvidno pri uporabi različnih poročil, mnenj in stališč organizacij in regulatorjev, ki smo jih obravnavali v naši raziskavi. Ti dokumenti odražajo konsenz le določene skupine deležnikov glede vprašanj vedenjskega oglaševanja in njegove

regulacije, morda celo le v zamejenem obdobju ali na geografskem območju. Zato je analiza vsebine teh dokumentov vedno povezana z razumevanjem konteksta, v katerem je dokument nastal, in njegovega namena. Kot poudarja Yin (1994, str. 80), je ena od pomanjkljivosti analize dokumentov lahko pristranskost pri njihovem izboru. Zato smo si v raziskavi prizadevali zajeti dokumentacijo glede regulacije vedenjskega oglaševanja iz različnih virov, ki izražajo mnenja in stališča različnih deležnikov.

4.1.1 Proces analize dokumentov

Proces analize dokumentov vključuje njihovo iskanje, izbor, oceno in sintezo podatkov, ki so na voljo v dokumentih. Podatki iz dokumentov so prek analize vsebine organizirani glede na tematike, kategorije in primere (Labuschagne, 2003). Kot poudarja Bowen (2009), analiza dokumentov v več ponovitvah vključuje analizo vsebine in tematsko analizo. Pri analizi vsebine dokumentov raziskovalec identificira relevantne in pomembne dele besedila ali drugih podatkov ter jih loči od nerelevantnih. S tematsko analizo pa izlušči tematike, ki postanejo kategorije za analizo. Pri tem lahko uporablja vnaprej določeno kodiranje in kategorizacijo, in sicer glede na raziskovalna vprašanja, zlasti če analiza dokumentov dopolnjuje druge metode. Za analize intervjujev je tako npr. uporabljeno enako kodiranje kot za analizo dokumentov (Bowen, 2009, str. 32–33). Temeljita in sistematična analiza dokumentov je bila uporabljena za pridobivanje podatkov o ozadju regulacije vedenjskega oglaševanja in za validacijo ugotovitev ekspertnih intervjujev. Na podlagi analize dokumentov, ki je potekala vzporedno s procesi intervjujev ter analizo podatkov, pridobljenih z intervjuji, so bila oblikovana tudi dodatna vprašanja za intervjuvance, njihovi odgovori pa kontekstualizirani in ugotovitve validirane.

V smislu grajenja verodostojnosti in validacije ugotovitev je pomembna opredelitev dokumentov, ki so uporabljeni za analizo, ter postopki njihove analize. Ključna vprašanja zadevajo morebitno parcialnost dokumentov, kontekst, v katerem so nastali, ciljno javnost, vire, na katerih dokument temelji, informacije o avtorju, metodah priprave (Bowen, 2009, str. 33–34). V številnih primerih so analizirani dokumenti izražali le stališče ene skupine do vprašanja raziskave. Tu so bile posebej pomembne dolgoletne izkušnje raziskovalke na področju raziskave, ki so omogočale intuitivno filtriranje podatkov glede na njihovo

pomembnost in relevanco ter pripisovanje teže dokumentom glede na njihov kontekst nastanka in avtorstvo.

4.1.2 Vzorčenje dokumentov in analizirani podatki

Pregled dokumentov je potekal na podlagi vnaprej določenih kod in kategorij, predvsem z namenom odgovora na drugo raziskovalno vprašanje, tj. kakšen je trenuten okvir za regulacijo vedenjskega oglaševanja in kako učinkovito zagotavlja varovanje pravic posameznikov. V dokumentih smo iskali teme, povezane z raziskovalnim vprašanjem, kot so izhajale iz pregleda literature in teoretskega okvira, npr.: vedenjsko oglaševanje, ciljanje, spletno sledenje, pravice posameznikov, varstvo osebnih podatkov, privolitev, pravne podlage, zakoniti interes, profiliranje, piškotki, standard »ne sledi« itd.

Analiza dokumentov je bila opravljena po sklopih, primarno glede na operacionalizacijo tem znotraj drugega raziskovalnega vprašanja, ki je sledila opredelitvam teoretskega okvira glede regulatornih orodij in strategij, in sicer:

- zakonodajni okvir za varovanje zasebnosti in varstva osebnih podatkov v EU,
- zakonodajni okvir za varovanje zasebnosti in varstva osebnih podatkov v ZDA,
- samoregulacija in
- standardizacija (standard »ne sledi«).

Znotraj posamezne teme je bilo analiziranih veliko raznolikih dokumentov (Tabela 4), pri čemer se je analiza razlikovala tudi glede na naravo izbranih dokumentov (npr. zakonodaja in pravni akti, praksa sodišč in nadzornih organov, dokumenti s stališči deležnikov in poročila, akademski prispevki, standardizacijski dokumenti itd.). Značilnosti dokumentov v vzorcu so namreč različne, analiza zakonodajnih besedil in pravnih dokumentov se razlikuje od analize vsebine akademskih prispevkov ali novinarskih prispevkov, pa tudi od analize standardizacijskih dokumentov, ki so tehnične narave.

Dokumenti se razlikujejo glede na svojo verodostojnost, vezanost na kontekst in avtorja, kar je treba upoštevati pri zagotavljanju veljavnosti ugotovitev. Glede tega sta za grajenje verodostojnosti ugotovitev posebej pomembna navzkrižno preverjanje ugotovljenih dejstev iz različnih dokumentarnih virov v okviru triangulacije virov ter kritična ocena glede na njihov

kontekst nastanka in namen. Ugotovitve pregleda zakonodajnih aktov in pravnih virov so bile soočene z ugotovitvami, ki izhajajo iz sodne prakse in prakse nadzornih organov ter z ugotovitvami akademskih prispevkov na tem področju. Analiza standardizacijskih dokumentov in dokumentov samoregulacije je bila prav tako soočena z akademskimi prispevki, analizo zakonodajnega okvira ter dokumenti različnih deležnikov. Znotraj vsake od kategorij dokumentov smo v luči iskanja odgovora na raziskovalno vprašanje iskali izpostavljene tematike, podatke smo primerjali, jih pregledovali in organizirali glede na koncepte, ki so se pojavljali. Rezultati analize dokumentov so predstavljeni glede na zgoraj navedeno operacionalizacijo ključnih tem, ki pomenijo glavna, trenutno uporabljena orodja za regulacijo vedenjskega oglaševanja.

Tabela 4.1: Vzorčenje dokumentov, ki so bili uporabljeni za analizo, in analizirani podatki

Izbrani dokumenti	**Analizirani podatki**
1. Pravni viri: – zakonodajo: relevantne direktive in uredbe EU, nacionalna zakonodaja, zakoni v ZDA; – mnenja WP29, EDPB, EDPS, Evropske komisije, nadzornih organov za varstvo osebnih podatkov, FTC, ENISA itd.; – odločitve sodišč (SEU, ESČP, nacionalnih sodišč), nadzornih organov in regulatorjev.	Podatki o zakonodajni ureditvi področja vedenjskega oglaševanja, predvsem na področju varovanja zasebnosti in osebnih podatkov. Podatki o razlagah zakonodajne ureditve in sodni oz. nadzorni praksi na tem področju.
2. Poročila, mnenja in stališča različnih deležnikov do vprašanja regulacije vedenjskega oglaševanja (oglaševalska združenja, nevladne organizacije na področju varovanja zasebnosti in tehnologije ipd.)	Podatki o kontekstu in ozadju regulacije vedenjskega oglaševanja, podatki o stališčih in opredelitvah različnih deležnikov do teh vprašanj, o vplivu zakonodajnih rešitev na panožne prakse in na varovanje pravic posameznikov.
3. Raziskave o implementaciji zakonodaje (npr. dokumenti Evropske komisije).	Podatki o učinkovitosti in pomanjkljivostih zakonodajne ureditve na področju varovanja zasebnosti in vedenjskega oglaševanja.
4. Samoregulacijski kodeksi, certifikacijski mehanizmi (npr. samoregulacijski kodeks IAB, certifikacijski mehanizmi)	Podatki o ureditvi področja vedenjskega oglaševanja na spletu in mobilnih napravah na ravni samoregulacije in certificiranja.
5. Standardizacijski dokumenti	Podatki o tehnični zasnovi standarda »ne sledi« ter politikah njegove izvedbe, podatki o standardih za implementacijo tehničnih rešitev iz kodeksa IAB ter standardi ISO.
6. Raziskave o stališčih uporabnikov	Podatki o praksah in stališčih uporabnikov elektronskih komunikacijskih storitev do sledenja njihovim aktivnostim, osebno prilagojenih

	vsebin, oglaševanja, orodjih za nadzor nad zasebnostjo, blokiranju oglasov ipd.
7. Akademski prispevki s pravnega področja	Podatki o kritičnem pregledu zakonodajnih rešitev na področju vedenjskega oglaševanja in varovanja zasebnosti uporabnikov elektronskih komunikacijskih storitev, o pregledu praks na tem področju ter o predlaganih rešitvah za prihodnost.
8. Novinarski prispevki	Podatki o novostih na področju regulatornega okvira za vedenjsko oglaševanje v ZDA in EU, predlaganih rešitvah, komentarji novinarjev, specializiranih za področje raziskave, ipd.

4.2 Ekspertni intervjuji

Za preučevanje pojava vedenjskega oglaševanja in njegove regulacije je bila uporabljena tudi kvalitativna metoda intervjujev. Intervju je posebna oblika pogovora, ki omogoča prost raziskovalni pristop in zbiranje bogatejšega gradiva za analizo (Kvale, 2007, str. 3). Njihov namen je iskanje odgovorov na vsa tri postavljena raziskovalna vprašanja, glede možnosti prihodnjega urejanja področja pa še zlasti na zadnje. Glede na to, da na raziskovalnem področju ni ustaljenih praks razumevanja pojava vedenjskega oglaševanja in da je zaradi hitrega tehnološkega razvoja področje večinoma spreminjajoče, prav tako pa tudi regulatorni odzivi nanj, so intervjuji z različnimi strokovnjaki s tega področja učinkovita metoda zbiranja podatkov, ki jih z drugimi kvantitativnimi metodami ali dokumentarno analizo ni mogoče dobiti. Veliko znanja in poznavanja tematike je namreč le na ravni vedenja posameznih strokovnjakov in njihovega udejstvovanja v strokovnih združenjih ali skupinah na ravni EU in ZDA, ne pa tudi v pisni obliki, dostopni javnosti, saj gre za trenutno zelo aktualna politična in regulatorna vprašanja. Pri tem pa nas je zanimal predvsem opis mnenj in stališč, ki jih imajo strokovnjaki različnih področij glede pojava vedenjskega oglaševanja, ne pa posploševanje ugotovitev. Rezultati intervjujev so tudi orodje za validacijo ugotovitev metode analize dokumentov, saj intervjuji spraševalcu omogočajo postavljanje dodatnih vprašanj in tako pridobivanje nepričakovanih informacij (Berger, 1998). Ker gre za področje, prežeto z nenehnimi velikimi pravnimi in tehnološkimi spremembami, je vrednost pridobljenih podatkov o mnenjih in stališčih do tematike predvsem v opisu trenutne situacije in razumevanju praks, posploševanje pa je v takih razmerah pravzaprav nemogoče.

Kot poudarja Dexter (1970/2006), je pri ekspertnih oziroma »elitnih« intervjujih, pri katerih so spraševanci osebe, ki imajo glede na raziskovalno vprašanje poseben, eliten položaj in znanje, potrebno dobro predhodno poznavanje problematike. Ker nas pri tem tipu intervjuja zanima predvsem mnenje spraševanca, ki ga prav zato ne omejujemo s popolnoma vnaprej oblikovanimi vprašanji in svojimi stališči, mora imeti spraševalec ustrezno znanje, da lahko presodi veljavnost odgovorov. Raziskovalec lahko veljavnost zagotavlja tudi tako, da vnaprej izbere spraševance različnih pogledov, ki bodo uravnotežili mnenja drug drugega. Kvale (2017, str. 11) poudarja, da mora raziskovalec intervjuvanca opogumljati k izražanju svojih izkušenj in občutij, tako da izvablja specifične situacije in dogodke na konkretni ravni, in ne na abstraktni, pri čemer je pomembna ustvarjalnost, odprtost, radovednost in kritičnost, pa tudi empatija, saj se pri delno strukturiranih intervjujih raziskovalec nenehno prilagaja trenutni situaciji. Zelo je pomembna tudi lastna predstavitev raziskovalca (Fontana in Frey, 1994, str. 371 in 367). Med slabosti uporabe intervjujev moramo upoštevati poznavanje različnih jezikov in zmožnosti razumevanja ter interpretacije odgovorov, kar se je v pričujoči raziskavi pokazalo kot zelo pomembno, saj je bila večina intervjujev izvedena z mednarodnimi strokovnjaki v angleškem jeziku. Pomembno je, da raziskovalec, ki na koncu analizira in interpretira rezultate, dobro pozna jezik, v katerem so potekali intervjuji. Raziskovalka, ki je izvedla intervjuje, je strokovnjakinja s področja vedenjskega oglaševanja in varstva osebnih podatkov, kot tudi izkušena v uporabi angleškega jezika. To je omogočilo potrebno kritičnost pri izvedbi, pri postavljanju podvprašanj in konkretizacij situacij, glede katerih so bila iskana mnenja intervjuvancev, ter prav tako pri sprejemanju in odzivanju na njihove odgovore. Intervjuji so tako lahko potekali v smislu enakovredne razprave o mnenjih in stališčih.

4.2.1 Vsebinska zasnova intervjujev

Pri delno strukturiranih intervjujih je bistven načrt intervjuja, ki obsega glavne teme in vprašanja, pri tem pa vrstni red in formulacija nista natančno določena. Načrt pomeni predvsem orientacijo raziskovalcu. Interpretacija tako poteka že med intervjujem, prav tako pa tudi poskus verifikacije intervjuja (Kvale, 2017, str. 80–81). Načrt intervjuja je sledil sklopom, kot so bili opredeljeni v raziskovalnih vprašanjih, za vsako od raziskovalnih vprašanj so bila določena številna podvprašanja, pri čemer je bilo od ozadja in specifičnega znanja intervjuvanca odvisno, katera podvprašanja bodo uporabljena. Strokovnjaki s

tehničnim ozadjem so tako podali več pojasnil na vprašanja tehničnega ozadja, pri tistih, ki so se ukvarjali s specifičnim primerom izvajalca vedenjskega oglaševanja (npr. Facebook), je intervju skušal zajeti čim več podatkov o tem primeru. V splošnem pa so bili vsi strokovnjaki soočeni z vprašanji iz vseh treh sklopov tematik.

Prvi sklop je zadeval vlogo vedenjskega oglaševanja v panogi in družbi ter njegove prednosti. Bistvene so bile razlike med prednostmi in slabostmi za manjše in večje akterje na trgu. Drugi sklop vprašanj se je nanašal predvsem na vpliv vedenjskega oglaševanja na pravice uporabnikov do zasebnosti in varstva osebnih podatkov, pa tudi do enake obravnave in nediskriminacije ter druge potrošniške pravice. Tretji sklop vprašanj se je nanašal na regulatorni okvir za vedenjsko oglaševanje: veljavni in predlagane rešitve za prihodnost, ki bi lahko bolje dosegale ravnotežje med vpletenimi interesi panoge vedenjskega oglaševanja in varovanja pravic posameznikov.[43] Večina intervjujev je bila na koncu dogovorjena prek e-pošte. Intervjuvanci so vnaprej prejeli kratek seznam ključnih tem za pogovor. Na začetku intervjuja so bile teme še enkrat očrtane in tako začrtane načelne meje raziskovalnih vprašanj, konkretizirane glede na specifične izkušnje intervjuvanca, bodisi iz njegovih oz. njenih objavljenih del oz. prispevkov ali izkušenj, ki jih imajo.

4.2.2 Vzorčenje, postopek zbiranja in analize podatkov

Intervjuvanci so bili deloma izbrani znotraj širše strokovne in socialne mreže raziskovalke, deloma pa so predloge za dodatne intervjuvance podali strokovnjaki, s katerimi so bili opravljeni intervjuji oz. pridobljeni z drugimi neformalnimi stiki raziskovalke. Glavno merilo za izbiro je bilo velika angažiranost ter v večini primerov tudi mednarodni ugled posameznega eksperta pri tematiki vedenjskega oglaševanja. Respondenti iz panoge vedenjskega oglaševanja so bili izvajalci take vrste oglaševanja (bodisi oglaševalci ali založniki) ali so predstavljali interesna združenja, ki so vključena tudi v procese vplivanja na regulacijo. Vključeni so bili strokovnjaki, ki so na tem področju izvajali lastne raziskave ali jih še izvajajo (kar je posebej pomembno učinkovalo na validacijo naših rezultatov), strokovnjaki, ki so prispevali ali prispevajo h ključnih skupinam in smernicam, dokumentom in zakonodaje s tega področja, ter ugledni in priznani strokovnjaki s širšega področja varovanja zasebnosti, tako s strani institucij kot tudi nevladnih organizacij. V metodološkem

[43] Glej Prilogo J.

smislu je šlo tako za naključni vzorec, pridobljen na način snežne kepe, kjer so raziskovalko respondenti iz njene mreže seznanili z nadaljnjimi respondenti iz njihove širše mreže.

Izbor takega načina vzorčenja je bil pogojen s cilji raziskave, saj so nas zanimali odgovori predstavnikov različnih deležnikov problematike vedenjskega oglaševanja, strokovnjakov za to tematiko v evropskem in svetovnem merilu – torej ne le pogledi panoge vedenjskega oglaševanja oziroma izvajalcev vedenjskega oglaševanja na različnih tehnoloških platformah, ampak tudi stališča regulatorjev tega področja. Ker sta omenjena pogleda na problematiko lahko binarno nasprotna, sta bili vključeni še dve skupini deležnikov, katerih izražena mnenja se lahko gibajo tudi med obema skrajnima stališčema, čeprav se včasih popolnoma približajo eni ali drugi strani: svetovalne organizacije in pravne pisarne ter raziskovalci in teoretiki oz. nevladne organizacije. Taka struktura respondentov je sledila pregledu literature in študijam primerov ter zakonodaje, kjer so bile identificirane različne skupine, aktivne pri podajanju mnenj in komentarjev glede tematike vedenjskega oglaševanja in vključene v zakonodajne procese ter procese vplivanja na regulacijo tega področja. Z izborom večjega števila deležnikov je bilo mogoče rezultate intervjujev validirati že med njihovim izvajanjem, tako znotraj posameznega intervjuja kot tudi znotraj pogleda ene od skupin deležnikov s primerjavo z drugimi respondenti iz drugih skupin deležnikov. Podatki, pridobljeni z intervjuji, so bili uporabljeni za validiranje podatkov, pridobljenih z metodo analize dokumentov, in tudi obratno – rezultati intervjujev so bili vedno validirani z rezultati dokumentarne analize.

Izvedenih je bilo 19 intervjujev, štiri oz. pet v vsaki od štirih skupin deležnikov. Vsi intervjuvanci so si lahko izbrali čas izvedbe intervjuja, pri čemer je bila večina (12) izvedenih prek telefonskega klica ali spletnega konferenčnega klica, predvsem zato, ker strokovnjaki niso iz Slovenije, ampak iz drugih evropskih držav (Francija, Nizozemska, Belgija, Velika Britanija, Norveška, Danska, Združene države Amerike, Španija itd.). 10 intervjujev je bilo izvedenih v živo, z nekaterimi strokovnjaki v njihovih poslovnih prostorih, z drugimi na neodvisnih lokacijah. Intervjuji so potekali od januarja 2017 do julija 2017. Ključni dejavnik pri odločanju o načinu izvedbe je bila dosegljivost in preference eksperta, katerega odgovori so bili iskani.

Vsem intervjuvancem so bili pojasnjeni cilji in nameni raziskave, kako bodo podatki, pridobljeni z intervjuji, uporabljeni, da je disertacija javno objavljena, vendar njihovi osebni podatki v njej ne bodo razkriti, ampak bodo anonimizirani in bodo med rezultati predstavljeni le izseki iz pogovorov. Identiteta respondentov pa bo znana le raziskovalki in osebam, ki v procesu nastanka disertacije in zagovora sodelujejo na ravni fakultete in Univerze v Ljubljani. V predstavitvi profilov respondentov, ki pričajo o njihovi strokovnosti in edinstvenem strokovnem položaju za odgovore na raziskovalna vprašanja, so bili uporabljeni dodatni ukrepi za zagotovitev anonimizacije, saj bi lahko bili eksperti prepoznani tudi po svojih značilnih stališčih – tako so vsi predstavljeni v moški slovnični obliki, prav tako so bile zakrite države, iz katerih prihajajo, in zelo splošno opisana organizacija, s katero so povezani.

Vsem respondentom, ki s tem niso bili seznanjeni, je bila zaradi spoštovanja etičnih standardov v raziskovanju in transparentnosti vnaprej razkrita zaposlitev raziskovalke pri nadzornem organu za varstvo osebnih podatkov. Predvsem pri respondentih iz panoge vedenjskega oglaševanja in svetovalnih organizacijah se je to pokazalo kot pomembno, saj so svoje odgovore lahko prilagodili temu kontekstu. Pri rezultatih teh intervjujev je bila posebna pozornost namenjena validaciji s pomočjo dokumentarne analize in drugih intervjujev. Vsi respondenti so se strinjali, da je intervju zvočno posnet. Intervjuji so trajali okvirno eno uro, odvisno od časa, ki ga je imel na voljo strokovnjak. Že na začetku intervjuja je bil dogovorjen časovni okvir, da je bilo mogoče tudi v primeru krajših intervjujev pridobiti informacije iz vseh sklopov okvirnega vprašalnika. Posnetki so bili za hrambo ustrezno označeni.

Pomembno pri intervjujih je bilo ohranjanje specifike sproščenega pogovora in ne zadržane drže raziskovalca pri zaprtih intervjujih, ki le postavlja vprašanja in ne podaja lastnega mnenja o raziskovalni tematiki (Fontana in Frey, 1994, str. 364). Raziskovalka, ki je izvedla intervjuje je odgovarjala tudi na vprašanja respondentov, pojasnjevala smeri, v katere teče raziskava, in z navezavami na nekatere konkretne primere praks ter dogodkov pojasnjevala svoja vprašanja. Prizadevala si je ohraniti empatičnost in odprtost do stališč intervjuvancev, s ciljem globljega razumevanja njihovih pojasnil in mnenj. Tako so pridobljeni podatki kakovostnejši in bogatejši.

Za analizo intervjujev je bil najprej narejen magnetogram celotnih pogovorov, v angleškem oz. slovenskem jeziku. Pri obdelavi podatkov (iz magnetogramov) je bilo uporabljenih več

tehnik, ki so se med sabo intuitivno mešale in dopolnjevale: ustvarjanje profilov, kodiranje in združevanje v kategorije. Za vsakega od intervjuvancev je bil uvodoma izdelan profil s kratkim očrtom njegovih ključnih stališč. Podatki so bili analizirani glede na osrednje teme, ki se pojavljajo pri vsakem od treh glavnih raziskovalnih vprašanj. Pri tem so bili klasificirani oziroma kodirani podatki iz magnetogramov glede na teme, kot kategorije predvidene že vnaprej (izhajajoč iz raziskovalnih vprašanj in seznama podvprašanj, ki so bila uporabljena pri izvedbi intervjujev), prav tako pa smo bili pozorni na nove teme in koncepte, ki niso bili predvideni vnaprej, pa so vzniknile med intervjuji, oziroma včasih le v enem intervjuju s specifičnim ekspertom.

V predstavitvi rezultatov analize intervjujev (6. poglavje) so navedene ugotovitve glede na identificirane teme. Za namen interpretacije rezultatov so primerjana različna stališča strokovnjakov glede posamezne teme ali predstavljene podobnosti med stališči. Pri tem so navedbe intervjuvancev povzete in interpretirane v kontekstu raziskovalnih vprašanj, mestoma pa so dodani tudi ilustrativni primeri nekaterih izjav, in sicer v izvornem jeziku (bodisi v slovenskem, bodisi v angleškem). Izseki izjav, predstavljenih v tem poglavju, so le ilustrativni. Izjave so za namen predstavitve ugotovitev povzete v besedilu, pri navedkih, ki dodatno ilustrirajo ugotovitve, pa je ohranjen zapis v izvornem jeziku (tudi, kadar gre za angleški jezik). Na ta način je ohranjen izvirni pomen izrečenega, z vsemi specifikami, govornimi posebnostmi in tonom odgovorov.

4.2.3 Profili strokovnjakov

V vzorcu 19 intervjuvancev so zajeti respondenti glede na vsako od štirih skupin deležnikov, katerih mnenja, stališča in znanja glede vedenjskega oglaševanja so nas zanimala: panoga vedenjskega oglaševanja, pri kateri sta nas zanimala tako panožna plat kot tudi plat izdajateljev oziroma medijev, svetovalne organizacije, ki običajno iščejo kompromise bližje panožnim interesom, regulatorji in zagovorniki zasebnosti, ki so prišli iz nevladnega sektorja in iz vrst teoretikov. Pri tem sta prvi dve skupini običajno, čeprav ne vedno, izražali podobnejša stališča (bližje komercialnim interesom) in prav tako drugi dve (bližje interesom zaščite posameznikovih pravic). V vsaki od teh dveh skupin je bilo približno enako število respondentov (skupno devet oziroma deset).

Večina respondentov je bila iz drugih evropskih držav (deset) ter po eden iz ZDA in Norveške. Sedem respondentov je bilo iz Slovenije. Razpršenost vzorca na predstavnike iz različnih držav je raziskavi zagotovila potrebno globino in širino, saj je vedenjsko oglaševanje čezmejno vprašanje ter praksa in bi jo bilo nesmiselno preučevati zgolj z vidika ene države, še zlasti ker v raziskavi iščemo odgovore na izzive regulacije tega vprašanja, ki morajo biti nujno čezmejna. Čeprav je spol respondentov za raziskavo samo precej nepomemben, saj so bile za izbiro posameznega strokovnjaka bistvene njegove specifične izkušnje in znanje, je bil vzorec precej uravnotežen s 13 respondenti in šest respondentkami, kar najverjetneje ustreza večjemu številu moških, ki načeloma zasedajo položaje strokovnjakov, ki so nas zanimali v raziskavi. Vsi respondenti so bili starejši od 30 let, kar prav tako ustreza merilom visoke usposobljenosti in mednarodnih izkušenj s to tematiko.

Respondenti so vodilni strokovnjaki iz svojih organizacij, bodisi direktorji in vodje organizacij ter združenj ali gospodarskih družb, bodisi zelo izkušeni eksperti na vodilnih položajih na področju zasebnosti ali spletnega oglaševanja. Med strokovnjaki so bili bistveni eksperti nadzornih organov, ki poglobljeno obravnavajo področje vedenjskega oglaševanja in varstva osebnih podatkov, teoretiki, ki so trenutno vodilni v EU pri raziskavah s tega področja, ter predstavniki nevladnih organizacij in neodvisni raziskovalci s specifičnimi znanji in izkušnjami s tega področja. Eno od meril izbora je bilo tudi sodelovanje izbranih ekspertov pri nekaterih ključnih dokumentih, ki so bili uporabljeni v dokumentarni analizi, npr. poročilih o delovanju panoge vedenjskega oglaševanja ali poročilih nadzornih organov, pri nastanku standardizacijskih dokumentov ali zakonodaje in izvajanja zakonodaje. Tudi tako je študija kombinacijo metod in virov uporabila za krepitev verodostojnosti ugotovitev in za možnosti podpore ugotovitvam dokumentarne analize s pomočjo intervjujev. Spodnja tabela prikazuje respondente glede na deležniško skupino, ki ji pripadajo. Njihove identitete so anonimizirane, namesto imen pa so poimenovani z oštevilčenim generičnim imenom skupine, njihov položaj v organizaciji pa je predstavljen opisno. Za opis je uporabljen moški spol, čeprav so respondenti različnih spolov, tudi zaradi večje zanesljivosti anonimiziranja (Tabela 4.2).

Tabela 4.2: Opis intervjuvancev glede na njihove izkušnje in pripadnost skupini deležnikov

Poudarek na panožnih interesih		**Poudarek na varovanju posameznika**	
PANOGA (OGLAŠEVALCI in MEDIJI)	**SVETOVALCI**	**REGULATORJI**	**ZAGOVORNIKI ZASEBNOSTI**
Oglaševalec 1 Ponudnik storitev programatičnega oglaševanja Strokovnjak za programatično oglaševanje	**Svetovalec 1** Svetovalno podjetje s področja regulacije Strokovnjak za oglaševanje in regulacijo	**Regulator 1** Nadzorni organ za varstvo osebnih podatkov Strokovnjak za standard »ne sledi«	**Zagovornik 1** Univerza Strokovnjak za spletno oglaševanje in varovanje zasebnosti
Oglaševalec 2 Mednarodna oglaševalska organizacija Strokovnjak za oglaševanje in zakonodajo	**Svetovalec 2** Svetovalno podjetje Strokovnjak za skladnost na področju varstva osebnih podatkov	**Regulator 2** Nadzorni organ za varstvo osebnih podatkov Strokovnjak za vedenjsko oglaševanje	**Zagovornik 2** Nevladna organizacija Strokovnjak za zasebnost in nove medije
Oglaševalec 3 Mednarodna spletna oglaševalska korporacija Strokovnjak za spletno oglaševanje, zasebnost in zakonodajo	**Svetovalec 3** Svetovalna organizacija Strokovnjak na področju varstva osebnih podatkov	**Regulator 3** Nadzorni organ za varstvo osebnih podatkov Strokovnjak za programatično oglaševanje	**Zagovornik 3** Nevladna organizacija Strokovnjak za področje zasebnosti in spletnega oglaševanja
Medij 1 in Medij 2[44] Spletni medij Strokovnjaka za programatično oglaševanje	**Svetovalec 4** Mednarodni think tank in svetovalna organizacija Strokovnjak na področju varstva osebnih podatkov	**Regulator 4** Nadzorni organ za varstvo osebnih podatkov Strokovnjak za spletna družbena omrežja	**Zagovornik 4** Nevladna organizacija Strokovnjak za podatkovno etiko
Medij 3 Spletni medij Strokovnjak za informacijske tehnologije in zasebnost			**Zagovornik 5** Univerza Strokovnjak za pravo varovanja zasebnosti

[44] Intervju je bil opravljen z dvema osebama hkrati.

5 ANALIZA OKVIRA REGULACIJE VEDENJSKEGA OGLAŠEVANJA

To poglavje predstavlja ugotovitve dokumentarne analize veljavnega regulatornega okvira za vedenjsko oglaševanje v EU in ZDA. Kritično so analizirani zakonodajni okvir in njegovo uveljavljanje (ter nadzor), samoregulacijski pristopi in standardizacijske dejavnosti na tem področju, predvsem tiste, povezane s pravno ureditvijo zasebnosti in varstva osebnih podatkov. V dokumentarni analizi regulatornega okvira regulacijo razumemo, kot jo opredeljuje Lessig (2006, str. 122–125), in raziščemo razsežnosti pravnih pravil ter drugih pravil (npr. zajetih v samoregulacijskih mehanizmih). Analiziramo tudi t. i. regulacijo s kodo. V okviru vedenjskega oglaševanja je najpomembnejši regulatorni mehanizem razvoj in uvedba standarda ne sledi. Sledimo tudi konceptualizaciji orodij regulacije, kot jo ponujata Baldwin in Cave (1999, str. 34–62), kjer je za naše raziskovalno področje pomembno razlikovanje med zakonodajo in samoregulacijo. V analizi se omejimo na zakonodajo in pravila s področja varstva zasebnosti in osebnih podatkov, saj večina regulatornih mehanizmov za področje vedenjskega oglaševanja trenutno izhaja iz tega področja. Treba pa je omeniti, da v zadnjem času tudi na drugih področjih nastajajo ali se spreminjajo pravila za omejevanje škodljivih posledic vedenjskega oglaševanja.[45] V nadaljevanju je najprej predstavljen zakonodajni okvir za vedenjsko oglaševanje v EU, nato pa zakonodajni okvir v ZDA. Sledi analiza ureditve na področju samoregulacije: kodeksov in certifikacijskih elementov ter področja standardizacije. Podrobno je analiziran standard ne sledi.

5.1 Pravni okvir za varovanje zasebnosti in varstva osebnih podatkov v EU

Varstvo osebnih podatkov ima v EU status temeljne pravice. V številnih državah članicah EU je kot temeljna pravica varovana na ustavni ravni. Pravni okvir za vedenjsko oglaševanje v EU sestavljata zlasti dva akta s področja varstva osebnih podatkov oz. zasebnosti v elektronskih komunikacijah: Direktiva 2002/58/ES (Direktiva o zasebnosti in elektronskih komunikacijah oziroma ePD),[46] prenesena v nacionalne zakonodaje držav članic.[47] Ta je

[45] V EU je bila marca 2019 denimo sprejeta Uredba 2019/493, ki opredeljuje postopek preverjanja v zvezi s kršitvami pravil o varstvu osebnih podatkov v okviru volitev v Evropski parlament, in sicer kot odziv na ugotovitve glede manipulacije volivcev s političnim mikro ciljanjem.

[46] Direktiva je bila leta 2009 spremenjena (z Direktivo 2009/136/EC) zaradi posegov v zasebnost uporabnikov s pomočjo piškotkov in drugih tehnologij (npr. spletni svetilniki, odtis naprave ali brskalnika) na spletnih straneh. Nova, strožja pravila glede piškotkov so se začela izvajati leta 2013.

trenutno v postopku prenove in naj bi jo v kratkem nasledila Uredba o Zasebnosti v elektronskih komunikacijah. Drugi bistveni akt je Uredba 2016/679, ki je maja 2018 nasledila Direktivo 95/46/ES o varstvu osebnih podatkov[48]. Prenovo pravnega okvira za varstvo osebnih podatkov lahko pripišemo predvsem bliskovitemu razvoju sodobnih komunikacijskih tehnologij in njihovemu čedalje večjemu vplivu na zasebnost posameznika (npr. pri aktivnostih profiliranja, vedenjskega oglaševanja in pravice do pozabe v elektronskih komunikacijah), pri katerem določbe Direktive 95/46/ES niso več omogočale učinkovitega varstva pravic posameznikov (EC, 2010).

Ker je zakonodaja, ki je bistvena za področje vedenjskega oglaševanja, razmeroma nova, je na tem področju še veliko nedorečenega in odprtega za razlago, še zlasti ker je Direktiva o zasebnosti v elektronskih komunikacijah trenutno v postopku obsežnih sprememb, tudi zaradi škodljivih praks na področju vedenjskega oglaševanja. V dokumentarni analizi smo se v delu zakonodajnega okvira v EU zlasti naslonili na mnenja in razlage pristojnih organov ter institucij, zlasti Delovne skupine iz člena 29[49] in njenega naslednika, Evropskega odbora za varstvo podatkov. Čeprav se nekateri dokumenti nanašajo na razlago določb Direktive 95/46/ES, so za analizo nepogrešljivi, saj so v delu, v katerem določbe z Uredbo (EU) 2016/679 niso bile spremenjene, še vedno veljavni, pri spremenjenih določbah pa nakazujejo na to, kako se bodo razlagale nove določbe Uredbe (EU) 2016/679. Analiza zajema zakonodajo, ki velja v času pisanja te naloge,[50] na koncu pa so predstavljeni in kritično ovrednoteni tudi ključni poudarki osnutka Uredbe o zasebnosti v elektronskih komunikacijah in njegovih sprememb.

5.1.1 Direktiva o zasebnosti in elektronskih komunikacijah

Direktiva 2002/58/ES o zasebnosti in elektronskih komunikacijah ureja vprašanja zasebnosti pri uporabi elektronskih komunikacij in med drugim nalaga ponudnikom javno dostopnih elektronskih storitev zagotavljanje zaupnosti komunikacij, opredeljuje namene, za katere smejo ti uporabljati prometne in lokacijske podatke uporabnikov elektronskih komunikacij,

[47] v Sloveniji denimo v Zakon o elektronskih komunikacijah
[48] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov je veljala od leta 1995 in je bila bolj ali manj harmonizirano prenesena v pravne sisteme držav članic EU.
[49] Gre za svetovalno telo Evropske komisije, sestavljeno iz nacionalnih organov za varstvo osebnih podatkov, ki je delovalo na podlagi Direktive 95/46/ES in se je ob uveljavitvi Uredbe (EU) 2016/679 preoblikovalo v Evropski odbor za varstvo podatkov.
[50] Julij 2019.

kako se izdajajo imeniki, pod kakšnimi pogoji se elektronska pošta, SMS in MMS sporočila ter druge storitve elektronskih komunikacij smejo uporabljati za namen pošiljanja neželenih sporočil in kakšna so pravila glede uporabe piškotkov in podobnih tehnologij.

Za področje vedenjskega oglaševanja je bistvena določba o piškotkih in podobnih tehnologijah, ki omogočajo dostop do uporabnikove naprave in podatkov. Tretji odstavek 5. člena Direktive 2002/58/ES določa, da se piškotki in podobne tehnologije[51] za shranjevanje podatkov ali pridobitev dostopa do podatkov, shranjenih v terminalski opremi uporabnika, lahko uporabljajo, če je bil ta o tem ustrezno obveščen in je v to privolil. Določene so izjeme, pri katerih vnaprejšnja privolitev ni potrebna, in sicer če se piškotek uporablja »izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja«; ali je »nujno potreben, da ponudnik zagotovi storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahtevata« (npr. piškotki za pravilen pretok zahtev, piškotki, povezani z vnosi uporabnika, piškotki za avtentikacijo uporabnika, piškotki, ki so potrebni zaradi varnosti in zavarovanja, piškotki, ki omogočajo predvajanje multimedijskih vsebin, piškotki za prilagoditev nastavitev uporabnikovim željam, tudi piškotki vtičnikov spletnih družbenih omrežij pri uporabnikih, ki so prijavljeni v omrežje) (WP29, 2012). Kjer ni mogoče govoriti o eni od izjem, opisnih zgoraj, je za piškotek treba pridobiti soglasje uporabnika, kar naj bi veljalo tudi za (1) piškotke vtičnikov spletnih družbenih omrežij (npr. vtičnik Všeč mi je), s katerimi lahko ponudnik spletnega družbenega omrežja posamezniku sledi prek različnih spletnih strani, ki imajo integriran tak vtičnik. Brez privolitve posameznika ponudniki spletnih družbenih omrežij ne smejo obdelovati podatkov posameznikov, ki niso člani omrežja. Vtičniki spletnih družbenih omrežij torej ne bi smeli privzeto uporabljati piškotkov tretjih strank na straneh, prikazanih nečlanom (WP29, 2012, str. 9). Predhodno soglasje je nujno tudi v primeru (2) oglaševalskih piškotkov. Te lahko naloži obiskano spletno mesto (angl. *first party*) ali pa prihajajo s strani tretjih (oglaševalske mreže, partnerske spletne strani, ponudniki storitev – angl. *third party*). To so npr. piškotki, katerih namen je omejevanje števila prikazovanja oglasov (angl. *frequency capping*), zaznavanje prevar pri klikanju (angl. *click fraud*), raziskave in marketinške analize, izboljšave produkta glede na podatke o uporabi, piškotki za razlikovanje cen glede na profil uporabnika in prilagajanje vsebine glede na profil (IP, 2013, str. 10). Ti piškotki so še posebno invazivni za zasebnost posameznika, kadar jih naloži tretja stranka, ki lahko spremlja aktivnost uporabnika prek različnih spletnih strani, npr. oglaševalska mreža (WP29, 2012, str. 10).

[51] To velja tudi npr. za vohunsko in zlonamerno programsko opremo.

Podobne namene je mogoče brez uporabe piškotkov doseči tudi s sledenjem uporabniku na podlagi unikatnega »odtisa« njegove naprave. Tako sledenje je uporabniku običajno nevidno, na njegovo napravo pa se ne shranijo datoteke, ki bi jih bilo mogoče preprosto izbrisati ali z njimi upravljati. Spletni sledilci tako pridobljene podatke o uporabnikih pogosto kombinirajo s podatki o uporabniških identifikacijskih oznakah, ki so bili ukradeni spletnim družbenim omrežjem z vdori in izrabo ranljivosti njihovih varnostnih sistemov (Electronic Frontier Foundation, 2016). Za sledenje s pomočjo odtisa naprave veljajo enaka pravila, saj gre tudi tukaj za pridobivanja podatkov iz uporabnikove opreme (WP29, 2014c).[52] Če so za namen vedenjskega oglaševanja uporabljeni t. i. prometni podatki, ki jih obdeluje in beleži operater elektronskih storitev (npr. v primeru digitalne televizije, kjer se beležijo podatki o tem, kdaj je kdo gledal kateri program, kako dolgo itd.), je treba upoštevati omejitve Direktive 2002/58/ES v 6. členu, ki to dopušča na podlagi privolitve posameznika. Direktiva 2002/58/ES o zasebnosti in elektronskih komunikacijah je specialni akt in v tem smislu tretji odstavek 5. člena in 6. člen določata pravno podlago za obdelavo osebnih podatkov – privolitev posameznika. Glede preostalih vprašanj, ki zadevajo varstvo osebnih podatkov, Direktiva 2002/58/ES splošno napotuje na ureditev v Direktivi 95/46/ES[53](WP29, 2010a, str. 10), določba o piškotkih pa tudi sama izrecno napotuje na jasno in izčrpno obveščanje uporabnika o namenih obdelave podatkov v skladu z Direktivo 95/46/ES oziroma njeno naslednico, Uredbo 2016/679.

5.1.2 Splošna uredba o varstvu osebnih podatkov

Uredba 2016/679 osebne podatke opredeljuje široko, tako da zajema tudi različne identifikatorje, ki posameznika določijo na spletu in v elektronskem komuniciranju. Osebni podatek pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom. Določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot so ime, identifikacijska številka, podatki o lokaciji in spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko,

[52] Podrobneje o določbah Direktive 2002/58/ES v Prilogi K.
[53] Deseta uvodna izjava Direktive 2002/58/ES o zasebnosti in elektronskih komunikacijah denimo določa, da se Direktiva za varstvo osebnih podatkov uporablja za »vse zadeve v zvezi z varstvom temeljnih pravic in svoboščin, ki niso izrecno zajete v določbah te direktive, vključno z obveznostmi upravljavca in pravicami posameznikov«. Prav tako 95. člen Uredbe 2016/679 določa, da ne uvaja dodatnih obveznosti za fizične ali pravne osebe v zvezi z obdelavo, povezano z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v EU v povezavi z zadevami, za katere veljajo posebne obveznosti z istim ciljem iz Direktive 2002/58/ES.

genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika (1. točka 4. člena). Uvodna izjava 30 Uredbe 2016/679 posebej opredeljuje, da so posamezniki lahko povezani s spletnimi identifikatorji, ki jih zagotovijo njihove naprave, aplikacije, orodja in protokoli, kot so naslovi internetnega protokola in identifikatorji piškotkov, ali drugi identifikatorji, kot so oznake za radiofrekvenčno identifikacijo.

Uredba 2016/679 prav tako široko opredeljuje, kaj vse je obdelava osebnih podatkov, ki spada v njen okvir. Obdelava tako pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje (drugi odstavek 4. člena Uredbe 2016/679). Eden od temeljev varstva osebnih podatkov v EU je zakonitost obdelave, ki jo določa prvi odstavek 5. člena Uredbe 2016/679. Člen 6 nadalje določa šest pravnih podlag za zakonito obdelavo osebnih podatkov:

1. posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
2. obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;
3. obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca;
4. obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;
5. obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu;
6. obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.[54]

[54] Več pojasnil o Uredbi 2016/679 je na voljo v Prilogi L.

Bistveni del vedenjskega oglaševanja je profiliranje uporabnika, ki nato od oglaševalca prejme le oglase, povezane z njegovimi interesi, vedenjem in brskalnimi navadami. Izdelava profila lahko vključuje sledenje uporabnikom prek različnih spletnih strani in beleženje njihovih interesov in preferenc ter analizo zbranih podatkov in predvidevanje njegovih preferenc. Povezovanje osebnih podatkov v profile pa močno posega v pravice posameznika do varstva osebnih podatkov, še zlasti zato, ker pogosto poteka brez vednosti posameznikov, sploh na spletu. Ker posamezniki niso obveščeni o profiliranju, svojih pravic glede varstva osebnih podatkov tudi ne morejo uveljavljati (WP29, 2013, str. 2). Z razvojem informacijskih tehnologij je profiliranje postalo zelo problematično, saj je mogoče posameznikom slediti prek različnih naprav, beležiti njihove lokacije s pomočjo pametnih telefonov ter vse te podatke brez vednosti posameznika uporabljati za različne namene, od razlikovanja cen do razlikovanja ponudbe glede na profile posameznikov.[55]

Uredba 2016/679 je kot prvi pravno zavezujoč akt v EU izrecno opredelila in omejila profiliranje. V 4. členu tako »oblikovanje profilov« opredeljuje kot

> »vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika.«

Strožje pogoje določa 22. člen Uredbe 2016/679 za posebne primere, in sicer da ima posameznik, na katerega se nanašajo osebni podatki, pravico, da zanj ne velja odločitev, ki je utemeljena (1.) zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov, (2.) ki ima pravne učinke v zvezi z njim ali na nanj podobno znatno vpliva. Primeri pravnih učinkov so npr. odpoved pogodbe, pridobitev ali zavrnitev določene podpore, ki jo opredeljuje zakon – npr. otroški dodatek, zavrnitev vstopa v državo ali državljanstva (WP29, 2017a, str. 21). Primeri učinkov, ki podobno bistveno vplivajo na posameznika, pa so posledica odločitve, ki pomembno zadevajo okoliščine, vedenje ali izbire, na voljo posamezniku, ki imajo daljši ali stalen vpliv na posameznika ali vodijo v izključitev ali diskriminacijo, npr. odločitev o kreditu, o dostopu do zdravstvenih storitev, o možnosti zaposlitve, o dostopu do izobrazbe, npr. sprejemu na univerzo (WP29, 2017a, str. 22). Taka obdelava podatkov in odločanje za

[55] Svet Evrope je tako leta 2010 sprejel *Priporočilo glede avtomatske obdelave osebnih podatkov v kontekstu profiliranja* v katerem profiliranje prepozna kot aktivnost, ki lahko koristi posameznikom, gospodarstvu ter družbi, saj omogoča boljšo delitev trga, pa tudi analizo tveganj in zlorab. Vendar pa lahko raba profiliranja brez ustreznih omejitev in varoval resno škoduje dostojanstvu ljudi, tako da jim nepravično oteži dostop do posameznih stvari ali storitev.

posameznika pomeni tudi največje tveganje, zato so pogoji zanjo strožji. Primeri so samodejna zavrnitev spletne prošnje za posojilo ali prakse zaposlovanja prek spleta brez človekovega posredovanja oziroma »oblikovanje profilov«, na podlagi katerih se ocenjuje in predvideva uspešnost pri delu, ekonomski položaj, zdravje, osebni okus ali interesi, zanesljivost ali vedenje, lokacija ali gibanje (Uredba 2016/679, uvodno pojasnilo št. 71).

Glede na drugi odstavek 22. člena Uredbe 2016/679 je tako odločanje dopustno, če je:
(a) nujno za sklenitev ali izvajanje pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem podatkov; v tem primeru mora upravljavec podatkov izvesti ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, vsaj pravice do osebnega posredovanja upravljavca, do izražanja lastnega stališča in izpodbijanja odločitve;
(b) dovoljeno v pravu EU ali pravu države članice, ki velja za upravljavca in določa tudi ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki; izrecno je tu omenjeno spremljanje in preprečevanje zlorab in davčnih utaj ter zagotavljanje varnosti in zanesljivosti storitve, ki jo zagotavlja upravljavec (glej Uredba 2016/679, uvodno pojasnilo št. 71);
(c) utemeljeno z izrecno privolitvijo posameznika, na katerega se nanašajo osebni podatki. Tudi v tem primeru mora upravljavec podatkov izvesti ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, vsaj pravice do osebnega posredovanja upravljavca, do izražanja lastnega stališča in izpodbijanja odločitve.

Točki a in c omenjata ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznikov. Ti bi morali zajemati vsaj način, s katerim lahko posameznik, na katerega se nanašajo osebni podatki, pridobi osebno posredovanje, izrazi svoje mnenje in ugovarja odločitvi (WP29, 2017a, str. 28). Uredba v tem smislu določa, da bi moral upravljavec za pošteno in pregledno obdelavo osebnih podatkov uporabiti ustrezne matematične ali statistične postopke za oblikovanje profilov, izvajati tehnične in organizacijske ukrepe, s katerimi bi na ustrezen način zagotovil popravo dejavnikov, ki povzročijo netočnost osebnih podatkov, in tveganje napak čim bolj zmanjšal ter zavarovati osebne podatke tako, da se upoštevajo morebitne nevarnosti, povezane z interesi in pravicami posameznika, ter da se preprečijo diskriminatorne posledice za posameznike na podlagi rasnega ali etničnega

porekla, političnega mnenja, vere ali prepričanja, članstva v sindikatu, genetskega ali zdravstvenega stanja ali spolne usmerjenosti. Oblikovanje profilov in avtomatizirane odločitve smejo temeljiti na teh občutljivih osebnih podatkih le pod posebnimi pogoji (Uredba 2016/679, uvodno pojasnilo št. 71).

Iz tega izhaja, da je profiliranje in/ali avtomatizirano odločanje mogoče zakonito izvajati ob upoštevanju določbe Uredbe 2016/679 s temeljem v eni od pravnih podlag, ki jih ta določa v 6. členu, ter ob spoštovanju vseh drugih relevantnih omejitev glede pravic posameznikov, ukrepov za zavarovanje in odgovornost upravljavcev itd. Le za zgolj avtomatizirano obdelavo, vključno z oblikovanjem profilov, ki ima pravne učinke v zvezi s posameznikom ali nanj podobno znatno vpliva, pa veljajo strožje omejitve, in sicer mora biti taka obdelava nujna za izvajanje pogodbe ali določena v zakonu ali utemeljena z izrecno privolitvijo posameznika. Tukaj ne pride v poštev obdelava na podlagi zakonitega interesa upravljavca ali tretje osebe (WP29, 2017a, str. 9). V primeru obdelave občutljivih osebnih podatkov ali če v postopku profiliranja nastanejo občutljivi podatki (npr. možnost napovedi spolne usmerjenosti glede na set »običajnih« podatkov, npr. lokacij posameznika), mora upravljavec izkazati, da ima za to pravno podlago, kot jo določa 9. člen Uredbe 2016/679, ki predpisuje omejitve za obdelavo občutljivih osebnih podatkov (WP29, 2017a, str. 15).

Upravljavec mora prav tako upoštevati določbe glede ustreznega obveščanja, po katerih mora biti posameznik seznanjen z dejstvom, da je obdelava namenjena (a) oblikovanju profilov in (b) sprejemanju odločitev na podlagi ustvarjenega profila. Nujno je izvajanje pravic posameznikov, in sicer: pravice do dostopa (15. člen Uredbe 2016/679), ki se nanaša na pravico do pridobitve podrobnosti o vseh osebnih podatkih, uporabljenih za oblikovanje profilov, vključno z vrstami podatkov, ki se uporabljajo za oblikovanje profila; pravice do popravka po 16. členu (posamezniki lahko izpodbijajo točnost uporabljenih podatkov in katero koli skupino ali kategorijo, ki je bila uporabljena zanje, zagotovljena jim je tudi pravica do dopolnitve osebnih podatkov z dodatnimi informacijami), pravice do izbrisa po 17. členu (ki se uporablja za »vhodne osebne podatke« za oblikovanje profila in »izhodne podatke« – sam profil ali »ocena«, dodeljena osebi) in pravice do omejitve obdelave (18. člen) (WP29, 2017a, str. 17–19). Člen 21 določa pravico do ugovora, na katero mora upravljavec posameznika izrecno opozoriti ter jo predstaviti jasno in ločeno od drugih informacij (četrti odstavek 21. člena). Posameznik lahko ugovarja obdelavi (vključno z oblikovanjem profilov)

iz razlogov, povezanih z njegovim posebnim položajem. Ko posameznik, na katerega se nanašajo osebni podatki, uveljavlja to pravico, mora upravljavec postopek oblikovanja profilov prekiniti (ali preprečiti njegov začetek), razen če lahko dokaže obstoj nujnih in zakonitih razlogov, ki prevladajo nad interesi, pravicami in svoboščinami posameznika, na katerega se osebni podatki nanašajo (WP29, 2017a, str. 19). Za primere zgolj avtomatiziranega odločanja na podlagi profila, ki vpliva na posameznikove pravice ali druge znatne vplive Uredba 2016/679 predpisuje obveščanje posameznika o tem, da se izvaja taka dejavnost; o razlogih zanjo ter o pomenu in predvidenih posledicah obdelave. Zagotovljene informacije pa bi morale biti za posameznika, na katerega se nanašajo osebni podatki, dovolj razumljive, da lahko razume razloge za odločitev (WP29, 2017a, str. 26).[56]

5.1.3 Pravni okvir in vedenjsko oglaševanje: pravne podlage

V nadaljevanju opisani pravni okvir uporabimo na primeru vedenjskega oglaševanja. Opredeljene so glavne omejitve in dolžnosti za različne akterje v ekosistemu vedenjskega oglaševanja, predvsem v zvezi z zakonitostjo obdelave osebnih podatkov – pravnimi podlagami. Zaradi omejenega obsega študije ni mogoče podrobno predstaviti vseh vidikov pravnega okvira, ki si tudi sami zase zaslužijo podrobnejšo obravnavo (npr. izvajanje pravic posameznika, izvedba presoj vpliva na zasebnost pa dolžnost vgrajenega varstva osebnih podatkov, zavarovanja podatkov itd). Zato je treba opomniti, da so to področja, na katerih so potrebne nadaljnje raziskave.

Metode vedenjskega oglaševanja, ki vključujejo uporabo piškotkov ali drugih podobnih tehnologij, običajno pomenijo obdelavo osebnih podatkov, kot jo določa Uredba 2016/679, saj gre za obdelavo uporabnikovih naslovov IP oz. enoličnih identifikatorjev (bodisi piškotka ali naprave). Enolični identifikator pa omogoča spremljanje uporabnika posamezne naprave tudi, kadar ima ta dodeljen dinamični naslov IP. Tako je mogoče uporabnika določiti in poiskati (angl. *single out*), čeprav morda ni znano njegovo ime (WP29, 2010a, str. 10). Poleg tega se podatki, zbrani v okviru vedenjskega oglaševanja, nanašajo na lastnosti in vedenje posamezne osebe, oglaševalec pa jih uporabi prav z namenom vplivanja na to osebo. Včasih se ti podatki dodatno povezujejo z drugimi informacijami, ki jih posreduje uporabnik, npr. pri registraciji, na podlagi katerih je mogoče posameznika neposredno identificirati (WP29,

[56] Več o profiliranju v Prilogi M.

2010a, str. 10). Spletni identifikatorji so bili v razpravah o vedenjskem oglaševanju vedno predmet diskusije – naj jih štejemo za osebne podatke ali ne. Spletna panoga identifikatorje uporablja za analizo aktivnosti uporabnikov na spletu, izboljšave svojih iskalnih storitev, prilagojeno oglaševanje in profiliranje, vendar jih pogosto opredeli kot podatke, ki posameznika ne določujejo (angl. *unidentifiable information*) v smislu imena in priimka, kot anonimne ali psevdonimne podatke, zaradi česar naj zanje ne bi veljala pravila o varstvu osebnih podatkov. Hkrati pa je na podlagi identifikatorja mogoče točno določenemu posamezniku poslati določen oglas, kar pomeni, da je ta posameznik določljiv in ga je mogoče razlikovati od drugih (Burnik, 2016a).

Uredba 2016/679 je na področje prinesla nekaj jasnosti, saj kot osebne podatke izrecno navaja tudi spletne identifikatorje, identifikatorje naprav, ID piškotkov, oznake RFID in IP-naslove (Uredba 2016/679, uvodna izjava št. 24). Identifikatorji piškotkov in naprav, ki so najpogosteje uporabljeni za vedenjsko oglaševanje, torej jasno spadajo med osebne podatke, za obdelavo katerih morajo imeti upravljavci ustrezno pravno podlago, morajo obveščati posameznike in upoštevati preostala pravila varstva osebnih podatkov. Uredba 2016/679 opredeljuje tudi psevdonimne podatke, pri čemer je psevdonimizacija obdelava, pri kateri osebnih podatkov ni več mogoče povezati z določljivim posameznikom brez dodatnih informacij, ki so hranjene posebej, in je s tehničnimi ukrepi preprečeno povezovanje. Upravljavec torej hrani le npr. številsko oznako za posameznika, ne pa tudi podatkov, s katerimi je posameznika mogoče neposredno prepoznati, npr. imena in priimka. Kljub temu so psevdonimni podatki osebni podatki, za katere naj bi veljala enaka pravila varstva.[57]

Uredba 2016/679 določa šest pravnih podlag, ki omogočajo zakonito obdelavo osebnih podatkov: posameznikovo privolitev, pravno obvezo upravljavca, nujnost za izvajanje pogodbe, vitalne interese posameznika, izvajanje naloge v javnem interesu ali izvajanje pooblastila ter zakoniti interes upravljavca osebnih podatkov. V določenih primerih dopušča le obdelavo osebnih podatkov na podlagi izrecne privolitve posameznika, npr. kadar gre za občutljive osebne podatke ali nekatere vrste profiliranja. Hkrati tudi Direktiva 2002/58/ES o zasebnosti in elektronski komunikacijah kot specialni pravni akt za aktivnosti dostopa in pridobivanja podatkov z uporabnikove naprave določa privolitev posameznika kot edino pravno podlago. Privolitev je tako trenutno primarna pravna podlaga za izvajanje vedenjskega

[57] Za razpravo o pojmu psevdonimnih podatkov glej prilogo N.

oglaševanja oziroma vsaj za tiste dele obdelave osebnih podatkov, ki zajemajo dostop do posameznikove naprave oz. ki bi zajemale profiliranje, ki močno posega v posameznikove pravice. V nadaljevanju najprej podrobneje obravnavamo razprave glede privolitve kot pravne podlage za vedenjsko oglaševanje in nato razpravljamo o drugih pravnih podlagah, na katere bi se izvajalci vedenjskega oglaševanja lahko zanašali, s poudarkom na zakonitem interesu. V analizi zaradi omejenega obsega disertacije ne obravnavamo podrobneje pravne podlage pogodbe, ki je prav tako pogosto uporabljena na področju spletnih storitev. Pomembno je poudariti, da je to nedvomno tema, ki si zasluži nadaljnje poglobljene obravnave v prihodnosti. Kot nakazujejo najnovejši dokumenti, pa vedenjskega oglaševanja običajno ne moremo šteti kot nujnega za izvajanje pogodbe o spletnih storitvah (EDPB, 2019).

a) Veljavna privolitev posameznika

Privolitev v piškotke ali podobne tehnologije po Direktivi 2002/58/ES

Po uveljavitvi pravil o piškotkih so upravljavci spletnih strani na različne načine pristopili k iskanju privolitev svojih uporabnikov. Nekatere od praktičnih rešitev so bile npr. takoj vidna obvestila, da spletna stran uporablja piškotke, s povezavo na več informacij o njihovi uporabi, obvestila, da se z uporabo spletne strani uporabnik strinja z namestitvijo piškotkov, informacije o tem, kako lahko uporabnik izrazi svoje preference glede piškotkov, mehanizmi, s katerimi lahko uporabnik izrazi strinjanje z vsemi piškotki oziroma nekatere zavrne, možnosti, da uporabnik naknadno spremeni svoje prejšnje nastavitve glede piškotkov (WP29, 2013, str. 2). Poleg tega so se v različnih državah članicah EU oblikovala različna mnenja glede veljavnosti t. i. implicitne (domnevane) privolitve, po kateri je posameznik v praksi le seznanjen s piškotki, ne vključuje pa njegovega aktivnega dejanja za potrditev.

Kot odziv na to je Delovna skupina iz člena 29 v mnenju pojasnila, da naj bi bila veljavna privolitev v piškotke predvsem nedvoumna, kar v praksi pomeni:

1. uporabnik mora biti o piškotkih jasno in vidno obveščen na vstopni spletni strani. Obveščen mora biti o različnih namenih uporabe piškotkov ter o piškotkih tretjih strank, če je to relevantno. Na voljo mu mora biti tudi podrobnejši seznam vseh piškotkov. Uporabnik mora biti obveščen tudi o tem, kako lahko poda privolitev oz. zavrne piškotke (IP, 2013; WP29, 2013);

2. piškotki ne smejo biti naloženi, preden uporabnik vanje ne privoli. Izjema so piškotki, ki so izvzeti, torej nujno potrebni, da spletna stran deluje ali da uporabnik dobi storitev, ki jo je izrecno zahteval (WP29, 2013);
3. uporabnik lahko v piškotke privoli le z aktivnim dejanjem. To je lahko klik na gumb, povezavo ali okence, lahko pa je tudi katero koli drugo aktivno vedenje uporabnika, iz katerega je mogoče nedvoumno sklepati, da pomeni privolitev. Uporabnik mora biti jasno obveščen, kakšno njegovo aktivno vedenje bo za upravljavca spletne strani pomenilo privolitev (IP, 2013). Orodja za pridobivanje soglasja lahko vključujejo pasice, pojavljajoča okenca itd. pa tudi nastavitve brskalnika, vendar le, če je upravljavec spletne strani prepričan, da je bil uporabnik jasno obveščen o piškotkih in je aktivno izbral ustrezne nastavitve brskalnika. Če uporabnik ostane le na vstopni spletni strani, ne da bi aktivno izvedel kako dejanje, tega ni mogoče šteti za soglasje (WP29, 2013, str. 4);
4. uporabnik mora imeti možnost svobodne izbire. Izbira mora biti mogoča pri privolitvi v piškotke, ki niso potrebni v zvezi z zagotavljanjem same storitve, ki jo spletna stran ponuja, in ponujajo le dodatne prednosti upravljavcu spletne strani. Spletne strani naj bi se izogibale rešitvam, pri katerih uporabnik lahko privoli le v vse piškotke, ne glede na to, ali so za zagotavljanje storitve res potrebni, ter ponudile uporabnikom možnost izbire pri različnih kategorijah piškotkov (sploh spletne strani organizacij iz javnega sektorja). Predvsem je možnost izbire treba ponuditi pri sledilnih piškotkih, ki pomenijo največji poseg v zasebnost posameznikov (IP, 2013; WP29, 2013).

Ali kot ustrezno orodje za pridobivanje privolitve lahko štejemo nastavitve v brskalniku, ki onemogočajo piškotke tretjih strani? Direktiva 2002/58/ES o zasebnosti v elektronskih komunikacijah v uvodni izjavi 66 dopušča, da uporabnik lahko poda svojo privolitev tudi prek ustreznih nastavitev brskalnika ali druge programske opreme »v primeru, da je to tehnično izvedljivo in učinkovito ter v skladu z ustreznimi določbami Direktive 95/46/ES«. Da bi nastavitve v brskalniku lahko šteli za ustrezne za podajo veljavnega soglasja, bi morale te privzeto zavračati piškotke tretjih strank in od posameznika zahtevati, da sprejme namestitev piškotkov konkretnega spletnega mesta in nadaljnji prenos podatkov, ki jih vsebujejo piškotki posameznih spletnih mest. Če bi brskalnik vnaprej določal, da se posameznik strinja z vsemi piškotki, taka »splošna privolitev« ne bi odražala dejanskih želja posameznika, saj privolitev

ne bi bila dana pred konkretno obdelavo podatkov, prav tako pa bi težko sklepali glede veljavnosti privolitve – posameznik je lahko namreč le obdržal nastavitve brskalnika tretje osebe in soglasja ni izrazil sam (WP29, 2010a, str. 15).

Ali veljavna privolitev zagotavlja možnosti za odjavo (angl. *opt-out*)? Posebna spletna mesta ali storitve, kjer posameznik lahko označi, od katerih ponudnikov ne želi prejemati prilagojenih oglasov (npr. youronlinechoices), načeloma ne zagotavljajo vnaprejšnjega soglasja, kot ga zahteva Direktiva 2002/58/ES o zasebnosti v elektronskih komunikacijah, temveč naknadno zavrnitev, ki temelji na domnevi, da se je uporabnik z neaktivnostjo strinjal z namestitvijo piškotkov. V praksi zelo malo ljudi uporabi možnost odjave, in to ne zato, ker bi se po predhodnem obveščanju odločili, da bodo sprejeli vedenjsko oglaševanje, temveč zato, ker se ne zavedajo, da so s tem, da niso uporabili možnosti odjave, pravzaprav dali soglasje (WP29, 2010a, str. 16).

Privolitev po Uredbi 2016/679

Uredba 2016/679 privolitev opredeljuje kot svobodno, posebno, informirano in nedvoumno izjavo volje posameznika (Uredba 2016/679, osma točka 4. člena). Neaktivnost ali molk posameznika nista dovolj, prav tako ne predoznačena polja za strinjanje, zgolj nadaljevanje uporabe storitve ali polja *opt-out* (WP29, 2017b, str. 6). Veljavno privolitev lahko posameznik izrazi npr. s potegom po pametnem telefonu, mahanjem pred kamero, obračanjem pametnega telefona, če je uporabniku jasno predstavljeno, da bo to pomenilo privolitev. Na drugi strani zgolj premik navzdol po spletni strani ni dovolj nedvoumno dejanje, da bi ga bilo mogoče razumeti kot soglasje (WP29, 2017b, str. 17). Prav tako mora imeti posameznik vedno možnost preklica svojega soglasja. Preklic mu mora biti omogočen podobno preprosto, kot je podal privolitev.

Privolitev v obdelavo občutljivih osebnih podatkov ter v zgolj avtomatizirano odločanje in profiliranje z znatnimi posledicami za posameznika mora biti tudi izrecna. Privolitev ne more biti pravna podlaga za obdelavo osebnih podatkov, kadar obstaja pomembno nesorazmerje moči med upravljavcem in posameznikom, npr. ko gre za obdelavo osebnih podatkov s strani javnega sektorja (četrti odstavek 7. člena in uvodna določba 34) (Burnik, 2016a). Privolitev je ustrezna podlaga le, če ima posameznik dejansko izbiro med sprejetjem in zavrnitvijo pogojev ali jih lahko zavrne brez škode. Novost je tudi zahteva Uredbe 2016/679, da je privolitev

dokazljiva, kar pomeni, da jo mora biti upravljavec sposoben izkazati, da je pridobil veljavno privolitev za določene namene (WP29, 2017, str. 3).

Privolitev posameznik lahko poda z uporabo tehničnih nastavitev ali jo drugače jasno izrazi. Da bi nastavitve v brskalniku pomenile veljavno privolitev, bi morale omogočati npr. granularnost glede različnih predvidenih namenov ter zagotavljati informacije o nazivu upravljavcev osebnih podatkov. Prav tako bi morala biti privolitev dana, preden upravljavec začne obdelovati osebne podatke (WP29, 2017b, str. 16).

Privolitev kot pravna podlaga za profiliranje

Čeprav Uredba 2016/679 prinaša pomembno novost v smislu opredelitve profiliranja in avtomatiziranega odločanja ter pogojev zanje, bistvenih vprašanj glede vedenjskega oglaševanja ne reši, ampak vprašanje pravne podlage pravzaprav zaplete. Za začetno točko vedenjskega oglaševanja, torej pridobivanje podatkov iz naprave uporabnika oz. sledenje je glede na Direktivo 2002/58/ES potrebna privolitev posameznika, za nadaljnjo rabo teh podatkov za namen ustvarjanja profila in avtomatiziranega odločanja pa so na voljo različne možnosti pravnih podlag, tudi nujnost za izvajanje pogodbe ali zakoniti interes posameznika. Pri tem zakoniti interes v zvezi z neposrednim trženjem navaja tudi uvodna izjava 47 Uredbe 2016/679, kar nedvomno kaže na to, da Uredba 2016/679 za kanček bolj odpira vrata vedenjskemu oglaševanju brez temelja v posameznikovi privolitvi.

Le če gre za zgolj avtomatizirano odločanje na podlagi profila, ki ima pravne ali druge, podobno znatne posledice za posameznika, je potrebna izrecna privolitev posameznika ali pa mora biti taka obdelava bodisi nujna za izvajanje pogodbe, določena v zakonu (Uredba 2016/679, 22. člen). Tukaj ne pride v poštev obdelava na podlagi zakonitega interesa upravljavca ali tretje osebe. Kot pojasnjuje WP29 (2017a), običajno vedenjsko oglaševanje nima takih učinkov na posameznika, da bi ga morali obravnavati pod strožjimi pogoji iz 22. člena Uredbe 2016/679, če gre na primer za oglas za spletno modno trgovino, ki temelji na preprostem demografskem profilu: »ženske v regiji Bruselj, stare od 25 do 35 let, ki se verjetno zanimajo za modo in nekatera oblačila« (WP29, 2017a, str. 23). V takem primeru so upravljavcu na volje vse pravne podlage iz Uredbe 2016/679. Za presojo, ali ima vedenjsko oglaševanje znatne učinke, in je zanj potrebna izrecna privolitev (ali podlaga v nujnosti za

izvajanje pogodbe ali določenosti v zakonu), bi bilo treba upoštevati okoliščine posameznega primera in sicer:

- vsiljiv postopek oblikovanja profilov, vključno s sledenjem posameznikov po različnih spletiščih, napravah in storitvah;
- pričakovanja in želje posameznikov;
- način objave oglasa ali
- izrabljanje poznavanja ranljivosti posameznikov: čeprav morda obdelava podatkov na posameznika vpliva le neznatno, lahko močno vpliva na nekoga iz ranljivejše skupine – npr. oglaševanje posojil z visokimi obrestmi tistim, ki naj bi bili v finančnih težavah (WP29, 2017a, str. 23).

Avtomatizirano sprejemanje odločitev, katerega rezultat je različno zaračunavanje cen na podlagi osebnih podatkov ali osebnih značilnosti, bi lahko znatno vplivalo tudi, če bi nedopustno visoke cene nekomu na primer dejansko onemogočale dostop do posameznega blaga ali storitev (WP29, 2017a, str. 23). Če bi na področju političnega mikro ciljanja osebno prilagojena sporočila na volivca učinkovala tako, da bi ne bi volili ali bi volili na določen, impliciran način, bi lahko tako profiliranje na posameznika močno vplivalo (Evropska komisija, 2018b, str. 8).

Je pa Uredba 2006/678 jasna, ko govori o informiranju posameznikov. Treba jih bo namreč jasno obvestiti o profiliranju in o tem, kakšne bodo zanje posledice. Uvaja tudi novosti in jasnejša pravila na področju pravic posameznikov, ki so podvrženi profiliranju – npr. pravico, da lahko posameznik taki obdelavi osebnih podatkov kadarkoli ugovarja, če je ta povezana z neposrednim trženjem. Z drugim odstavkom 21. člena posamezniku daje tudi *brezpogojno* pravico, da ugovarja obdelavi svojih osebnih podatkov za neposredno trženje, vključno z oblikovanjem profilov, če je povezano s takim neposrednim trženjem. To pomeni, da tehtanje interesov ni potrebno in da mora upravljavec upoštevati želje posameznika, ne da bi dvomil o razlogih za ugovor. V uvodni izjavi 70 Uredbe 2016/679 je poleg navedbe dodatnih podrobnosti o tej pravici navedeno, da se lahko pravica uveljavlja kadar koli in brezplačno (WP29, 2017a, str. 20).

b) Legitimini interes kot alternativna pravna podlaga za vedenjsko oglaševanje

O legitimnem interesu (v slovenskem prevodu Uredbe 2016/679 se uporablja izraz zakoniti interes) kot pravni podlagi za obdelavo osebnih podatkov ni na voljo veliko virov, v nasprotju s številnimi prispevki o (veljavnosti) in (ne)učinkovitosti privolitve. Kritiki poudarjajo, da je zakoniti interes nekakšna pravna luknja, saj je v primerjavi z drugimi pravnimi podlagami, ki so natančneje formulirane, prilagodljiv glede na konkretno situacijo. Zakoniti interes se v praksi pogosto razlaga kot izjema od preostalih pravnih podlag ter privolitev kot najpomembnejša (Kamara in deHert, 2018, str. 5). Kljub temu pa upravljavci osebnih podatkov v praksi pogosto temeljijo svoje aktivnosti obdelave na tej podlagi, npr. pri neposrednem trženju in oglaševanju, merjenju občinstev, obdelavi osebnih podatkov znotraj skupine povezanih podjetij za administrativne namene, za namene varnosti omrežja, preprečevanje zlorab in preiskave zlorab itd. (CIPL, 2017, str. 23–27).

Pravna podlaga zakonitega interesa je povezana s tehtanjem med interesi upravljavca in interesi posameznika v konkretni situaciji, hkrati pa ni na voljo veliko smernic, kako to tehtanje izvesti, niti tega ne določa zakonodaja. Delovna skupina iz člena 29 v svojem mnenju o zakonitem interesu poudarja, da primerna uporaba in izvedba tehtanja interesov lahko prepreči zlorabo in napačno rabo drugih pravnih podlag, npr. prevelikega zanašanja na privolitev ali nujnosti za izvajanje pogodbe. Pojasnjuje, da je treba na interese gledati široko – morajo biti v skladu s pravom EU, vendar pa morajo biti natančno opredeljeni in dovolj jasno določeni, da se izvede tehtanje. Obdelava podatkov mora biti nujna za doseganje takega interesa – merilo nujnosti pomeni, da interesa ni mogoče zasledovati brez določene obdelave osebnih podatkov.

Interesi posameznikov so opredeljeni še širše, saj jih ne omejuje izraz »zakoniti«, temveč katerikoli interesi relevantni v okviru varstva osebnih podatkov (WP29, 2014a, str. 49). Tehtanje interesov naj bi potekalo v dveh fazah:

- v prvi fazi je treba upoštevati (1) naravo in vir upravičenega interesa upravljavca in ali je obdelava osebnih podatkov nujna za ta namen ter (2) vpliv na posameznike. Pri tem je treba upoštevati vse ukrepe, ki jih upravljavec upošteva za doseganje skladnosti s pravili varstva osebnih podatkov – npr. omenjen nabor osebnih podatkov in ustrezno obveščanje. Po tehtanju se ustvari preliminaren zaključek (angl. *provisional balance*),

ali interesi upravljavca pretehtajo nad interesi posameznika. Če zaključek ni jasen, se opravi nadaljnje tehtanje;

- v drugi fazi upravljavec presodi, ali lahko uvede še dodatne ukrepe, ki segajo onkraj zakonskih zahtev, da bi bili interesi posameznikov bolje zaščiteni (npr. preprost način za zavrnitev obdelave osebnih podatkov) (WP29, 2014a, str. 50).

Dejavniki, ki jih je koristno upoštevati pri tehtanju so:

- narava in vir zakonitega interesa, npr. ali je obdelava podatkov potrebna za izvajanje temeljne pravice ali je drugače v javnem interesu ali uživa družbeno, kulturno ali pravno priznavanje s strani družbe;
- vpliv na posameznika:
    - narava podatkov (občutljivi ali ne, iz javnih virov ali ne ipd.),
    - narava obdelave podatkov (ali so javno objavljeni ali dostopni širokemu krogu ljudi, ali gre za veliko podatkov, ali so namenjeni kombiniranju z drugimi podatki – kot npr. pri komercialnem profiliranju ali profiliranju za namen organov pregona),
    - razumna pričakovanja posameznika, sploh glede uporabe in razkritja podatkov v relevantnem kontekstu,
    - status upravljavca in posameznika, odnosi moči med njima ali če je posameznik otrok ali pripada ranljivi skupini;
- dodatna varovala za preprečevanje čezmernega posega v pravice posameznika:
    - omejen nabor osebnih podatkov ali izbris takoj po uporabi,
    - ukrepi za zavarovanje – ločevanje podatkov (angl. *functional separation*),
    - raba anonimizacijskih tehnik, agregacije podatkov, PETs, vgrajene zasebnosti in presoj vplivov na zasebnost,
    - povečana preglednost, brezpogojna pravica do zavrnitve obdelave, prenosljivost podatkov in drugi ukrepi za opolnomočenje posameznikov. WP29 poudarja pomen odgovornosti upravljavcev, da potek tehtanja dokumentirajo in zagotovijo vidnost informacij o tehtanju in o tem, zakaj in kako njihov interes prevlada nad interesi posameznikov (WP29, 2014a, str. 50–51).

Uredba 2016/679 upravljavcu ali tretji osebi, ki obdelavo osebnih podatkov utemelji na zakonitem interesu, nalaga dodatne obveznosti obveščanja posameznikov o tem, da obdelava temelji na zakonitem interesu, in kakšen ta interes je (13. in 14. člen). Posamezniki imajo glede na 21. člen Uredbe 2016/679 tudi pravico ugovora zoper tako obdelavo. Upravljavec ali tretja oseba morata nato prenehati obdelovati osebne podatke, razen če izkažeta nujne razloge za obdelavo (Kamara in deHert, 2018, str. 19). Uredba 2016/679 postavlja tudi omejitev za uporabo temelja zakonitega interesa, ko gre za obdelavo osebnih podatkov otrok in obdelavo s strani javnega sektorja (točka f prvega odstavka 6. člena).

Potek tehtanja je Delovna skupina iz člena 29 opredelila v več korakih:

1. presoja o najprimernejši pravni podlagi za obdelavo;
2. opredelitev interesa upravljavca kot upravičenega, zakonitega;
3. ugotovitev, ali je konkretna obdelava osebnih podatkov nujna za doseganje zasledovanega interesa;
4. preliminarna odločitev, ali interes upravljavca pretehtajo temeljne pravice ali interesi posameznikov:
    - kakšni so upravljavčevi interesi (temeljna pravica, drug interes),
    - ocena posledic, ki bi jih upravljavec ali družba utrpela, če obdelave ne bi bilo,
    - upoštevanje narave podatkov, statusa posameznika in upravljavca in njunih pozicij moči,
    - načini obdelave podatkov (obsežno, rudarjenje podatkov, profiliranje, razkritje javnosti),
    - opredelitev, na kakšne pravice posameznika bi lahko obdelava vplivala,
    - upoštevanje razumnih pričakovanj posameznika,
    - ocena vplivov na posameznika in primerjava s pozitivnimi posledicami obdelave;
5. končno tehtanje interesov na podlagi dodatnih varoval;
6. izkazovanje skladnosti in zagotavljanje preglednosti:
    - dokumentiranje korakov tehtanja, informiranje posameznikov o tem, zakaj naj bi interes upravljavca prevladal, hramba evidenc za primer nadzora;
7. zagotavljanje pravice do zavrnitve obdelave podatkov (WP29, 2014a, str. 55–56).

Kamara in deHert (2018) predlagata vsebinsko podoben, vendar krajši model za formalizacijo izvedbe tehtanja v treh korakih:

- 1. korak

Upravljavec ali tretja oseba mora imeti za konkretno obdelavo osebnih podatkov legitimen interes – ni nujno, da je opredeljen v zakonu, vendar pa ne sme biti v nasprotju z zakonom (npr. komercialni interes).

- 2. korak

Presoja nujnosti – obdelava osebnih podatkov mora biti nujna glede na cilje, ki jih zasleduje upravljavec. To pomeni, da cilji ne morejo biti doseženi na način, ki ne bi vključeval take obdelave osebnih podatkov.

- 3. korak

Tehtanje med nasprotnimi interesi upravljavca in posameznika mora biti izvedeno v vsaki konkretni situaciji obdelave osebnih podatkov, da se ugotovi, ali pravice posameznika pretehtajo interese upravljavca ali tretje osebe. Pri tehtanju je treba upoštevati več elementov, ki lahko pretehtajo v eno ali drugo stran:

- kakšni so osebni podatki? Občutljivi, javno dostopni itd.;
- status in moč obeh strani, upravljavca ali tretje stranke in posameznika (delodajalec je npr. močnejša stranka; ponudnik storitev z monopolnim položajem je močnejša stranka);
- vir legitimnega interesa: če legitimni interes temelji na zakonodaji (npr. svoboda izražanja), je močnejši, kot če gre le za komercialni interes pridobivanja kupcev prek vedenjskega oglaševanja;
- namen obdelave;
- vpliv obdelave na interese, pravice in svoboščine posameznika: vpliv pomeni pozitivne učinke in tudi tveganja. Za izvedbo analize tveganja obstajajo različna orodja, ki jih lahko upravljavec uporabi,[58] kompleksnejša je ocena pozitivnih učinkov, saj je lahko zelo subjektivna;
- ukrepi za zmanjšanje negativnih vplivov, kot je npr. uporaba zasebnosti prijaznih tehnologih (PETs) in anonimizacijskih tehnik – ob upoštevanju učinka takih ukrepov je jasna celotna slika negativnih vidikov za interese in pravice posameznika, treba pa je upoštevati, da je teža ukrepov odvisna od njihove dejanske izvedbe in učinkovitosti;

[58] Privacy Risk Assessment Methodology. ISO 31000 on risk management ISO/IEC 27005 which is specific to information security risk management.

- razumna pričakovanja posameznika: upravljavec mora presoditi, ali posameznik lahko razumno pričakuje obdelavo osebnih podatkov v času in kontekstu ter za določen namen (npr. če posameznik naroči produkt v spletni trgovini, lahko razumno pričakuje, da se bodo za ta namen obdelovali podatki, ki so za to neizogibno potrebni). Tu so ključne informacije, ki so posamezniku dostopne pred zbiranjem njegovih podatkov (jasne, pravočasne in pregledne), njegovo strinjanje pa je implicirano (Kamara in deHert, 2018, str. 11–17).

V primeru korektno izvedenega tehtanja, ki vključuje uporabo varoval za posameznika za zmanjšanje posega v njegove pravice, ter ob pogojih upoštevanja načela odgovornosti po Uredbi 2016/679 je lahko pravna podlaga zakonitega interesa pomenljiva in ne pravna praznina, ki je zlahka izrabljena.

Kamara in deHert v okviru svojega modela tehtanja interesov podata tudi premislek o pravni podlagi zakonitega interesa za obdelave v okviru profiliranja in velikega podatkovja. Mnenja o tem se krešejo; nekateri vidijo potencial podlage zakonitega interesa v okviru neposrednega trženja, izrecno pa je to poudaril tudi evropski zakonodajalec v uvodni izjavi 47 Uredbe 2016/679. Drugi poudarjajo, da za vedenjsko oglaševanje legitimen interes ne more biti primerna pravna podlaga, in napotujejo na izboljšanje privolitve (npr. Zuiderveen Borgesius, 2015). Strinjanje o tej temi je težko pričakovati. Avtorja zaključujeta, da kljub težavam, povezanim s privolitvijo, za vse primere profiliranja na podlagi velikega podatkovja pravna podlaga zakonitega interesa ni primerna, že zaradi problematičnosti drugih načel obdelave, kot sta omejitev in določitev namenov obdelave (Kamara in deHert, 2018, str. 28–29). Delovna skupina iz člena 29 je poudarila nekaj konkretnih primerov zakonitih interesov, pri čemer pa je opozorila, da bi jih ob tehtanju lahko pretehtale pravice posameznikov. Med njimi je navedla tudi: konvencionalno neposredno trženje in druge oblike trženja ali oglaševanja, ne-komercialna sporočila za namen političnih kampanj in človekoljubnih organizacij ter obdelave za namen raziskav trga. Podala je tudi nekaj konkretiziranih primerov praks neposrednega trženja, od preprostega neposrednega trženja strankam po pošti pa do subjektov, ki analizirajo velike količine podatkov o posameznikih in njihovih dejavnostih (lahko tudi občutljive), jih profilirajo in jim nato prikazujejo oglase. V vseh primerih je treba opraviti preliminarno presojo o tem, ali bi bilo kot podlago za tako dejavnost mogoče uporabiti temelj legitimnega interesa upravljavca. Pri tem je Delovna skupina iz člena 29 pojasnila, da imajo

upravljavci lahko zakoniti interes, da spoznajo preference svojih strank, da jim lahko ponudijo osebno prilagojene storitve, ki jih posamezniki želijo. Zato je zakoniti interes lahko primerna pravna podlaga za te dejavnosti, če obstaja mehanizem za zavrnitev take obdelave (WP29, 2014a, str. 25–26). V takem primeru npr. računalniška trgovina pri prodaji izdelkov od kupcev pridobi njihove kontaktne podatke za obveščanje o svojih podobnih produktih po pošti. Prav tako jih o novi ponudbi obvešča po e-pošti, pri čemer imajo posamezniki možnost zavrnitve prejemanja e-poštnih sporočil. V takem primeru je bil posameznik ustrezno obveščen, lahko kot kupec razumno pričakuje oglaševanje in ima možnost ugovarjanja. Prav tako ni posebnega vliva na njegovo pravico do zasebnosti, saj ne gre za izdelavo profilov. Zakoniti interes bi bila primerna podlaga (WP29, 2014a, str. 59). Še en omenjen primer je dostava pic, kjer ponudnik kontaktne podatke stranke uporabi za to, da ji po navadni pošti pošlje kupone za popust, na spletni strani pa omogoča odjavo od neposrednega trženja. Ker pri tehtanju ni zaznati posebnega posega v interese posameznika, interes ponudnika pic prevlada (WP29, 2014a, str. 31).

Taka argumentacija pa ne velja za neposredno trženje, ki vključuje prakse nadzora spletnih dejavnosti in dejavnosti v realnosti, kombiniranje velikih količin podatkov iz različnih virov, ki so bili zbrani za druge namene, v drugih kontekstih, in ustvarjanje ter trgovanje s kompleksnimi profili posameznikov, brez njihovega vedenja in možnosti, da temu ugovarjajo, in brez privolitve. Ker tako profiliranje pomeni velik poseg v zasebnost, ta interes pretehta nad upravljavčevim (WP29, 2014a, str. 25–26). Delovna skupina iz člena 29 je kot primer poudarila že omenjenega ponudnika dostave pic, ki si beleži zgodovino naročil stranke ter podatke kombinira z zgodovino nakupov v supermarketu, katerega lastnik je isto podjetje. Beleži se njena zgodovina brskanja in lokacije. Ciljana sporočila stranka prejema *online* in *offline,* po e-pošti in na spletnih straneh. Oglase prejema na lokacijah, za katere ponudnik predvideva, da bo tam bolj nagnjena k nakupu. Ko se preseli v sosesko z manjšo kupno močjo, ne prejema več promocijskih popustov. Na koncu ponudnik proda njene podatke zavarovalnici, ki ji zaradi slabih prehranjevalnih navad zviša premijo. Ta primer vključuje obširno spremljanje posameznice prek različnih kanalov, kombiniranje podatkov, profiliranje, diskriminacijo itd. ter s tem večji poseg v njene interese, kot bi bile njene koristi in interes upravljavca (WP29, 2014a, str. 32). Delovna skupina iz člena 29 omenja tudi spletno lekarno, ki beleži podatke o nakupih, tudi tistih na recept. Analizira jih in kombinira z demografskimi podatki o kupcih. Podatkom so dodani podatki o spletnih aktivnostih posameznikov. Zgradi

profile glede na zdravje in dobro počutje, ki vključujejo tudi predvidevanja glede nosečnosti, kroničnih bolezni itd. ter s pomočjo teh informacij trži po e-pošti zdravila, ki jih prodaja brez recepta. Ker gre za obširno profiliranje, ki vključuje občutljive osebne podatke iz različnih virov, in napovedovanje s pomočjo algoritmov, pravna podlaga zakonitega interesa ni primerna (WP29, 2014a, str. 59).

Na primeru neposrednega trženja Delovna skupina iz člena 29 pojasnjuje razlike med položaji, ko je primerna podlaga za obdelavo osebnih podatkov privolitev, in med tistimi, v katerih je lahko podlaga zakoniti interes, ob čemer je uporabniku kot dodatno varovalo ponujena možnost naknadne zavrnitve. Za bolj intruzivne prakse neposrednega trženja v elektronskih komunikacijah naj bi mejo postavila že Direktiva 2002/58/ES, ki za neželena sporočila (angl. *spam*) ter piškotke in podobne tehnologije zahteva privolitev posameznika. Ne pokrivajo pa te določbe vseh praks neposrednega trženja in tako še vedno obstajajo nejasnosti glede uporabe pravnih podlag. Delovna skupina iz člena 29 meni, da bi morale biti prakse sledenja in profiliranja, vedenjskega oglaševanja, preprodaje podatkov, oglaševanja glede na lokacijo ali raziskave trga, ki temeljijo na sledenju, utemeljene na privolitvi posameznikov (WP29, 2014a, str. 47).

Glede tega je treba pripomniti, da so primeri, ki jih Delovna skupina iz člena 29 navaja, sicer nazorni, pa vendar ne dovolj povedni za odločanje, ali neko neposredno trženje lahko temelji na podlagi zakonitega interesa. Vsebujejo namreč prakse, ki jih lahko označimo le za skrajni točki neposrednega trženja – primeri, ki so navedeni kot neintruzivni, vključujejo preprosto pošiljanje pošte ali e-pošte kupcu svojih storitev, kar že zakonodaja (na področju e-pošte Direktiva 2002/58/ES, 13. člen) dovoljuje brez privolitve. Na drugi strani navajajo kot alternativo prej omenjenemu neintruzivnemu modelu le zelo intenzivno spremljanje vedenja posameznikov prek različnih platform, analizo, napovedi in diskriminacijo, po možnosti še glede na občutljive osebne podatke, prodajo podatkov in njihovo kombiniranje, za katerega je jasno, da težko pretehta poseg v pravice posameznika. Tako obširne prakse pravzaprav niti niso tako pogoste, saj zahtevajo tehnične zmogljivosti, ki jih nima veliko subjektov na trgu. Trženjska realnost je povsod vmes, morda subjekti uporabljajo le eno ali dve aktivnosti, ki bi jih Delovna skupina iz člena 29 označila kot intruzivne, ne pa celotnega sklopa takih praks. Morda spletni časopis sodeluje le z eno oglaševalsko mrežo za vedenjsko oglaševanje, ustrezno obvešča bralce o tem in jim ponuja realno možnost, da to zavrnejo. Morda

neposredno trženje temelji na profilu, ki ga je neki ponudnik izdelal iz neobčutljivih podatkov, ki so mu jih posamezniki sami posredovali. Primerov vmesnih praks je veliko, kar odpira vprašanja, kako zakoniti interes pretehtati v situacijah, ki niso skrajno intruzivne, vendarle pa posegajo v posameznikov zasebnost.

V enem zadnjih mnenj je Delovna skupina iz člena 29 nekoliko jasneje omenila možnost, da je podlaga zakonitega interesa lahko uporabljena tudi v okviru vedenjskega oglaševanja. Da bi bilo to utemeljeno na zakonitem interesu, bi moral upravljavec s tehtanjem presoditi, ali nad njegovimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki.

> »Pomembno je zlasti naslednje:
> - stopnja podrobnosti profila (posameznik, na katerega se nanašajo osebni podatki, katerega profil je oblikovan v okviru splošno opisane kohorte, kot je 'ljudje, ki se zanimajo za angleško literaturo', ali segmentiran in ciljno določen na podrobni ravni);
> - celovitost profila (ali profil opisuje le majhen vidik posameznika, na katerega se nanašajo osebni podatki, ali prikazuje celovitejšo sliko);
> - vpliv oblikovanja profilov (učinki na posameznika, na katerega se nanašajo osebni podatki) in
> - zaščitni ukrepi, namenjeni zagotavljanju poštenosti, nediskriminacije in točnosti pri postopku oblikovanja profilov.« (WP29, 2017a, str. 15).

Delovna skupina iz člena 29 konkretno meni, da bi

> »upravljavci težko upravičili uporabo zakonitih interesov kot zakonito podlago za vsiljive prakse oblikovanja profilov in sledenja za namene trženja ali oglaševanja, na primer tiste, ki vključujejo sledenje posameznikov na več spletiščih, lokacijah, napravah in pri storitvah ali posredovanju podatkov. Upravljavec bi moral pri ocenjevanju veljavnosti obdelave v skladu s členom 6(1)(f) upoštevati tudi prihodnjo uporabo ali kombinacijo profilov.« (WP29, 2017a, str. 15).

Zakoniti interes tudi ne more biti podlaga v primerih, ko obdelava lahko znatno vpliva na nekatere skupine v družbi, kot so manjšine ali ranljivi odrasli (da je nekdo npr. redno cilj oglasov za posojila z visokimi obrestmi, se lahko odloči za tako posojilo ter se tako še bolj zadolži). Avtomatizirano sprejemanje odločitev, katerega rezultat je različno zaračunavanje cen na podlagi osebnih podatkov ali osebnih značilnosti, bi lahko znatno vplivalo tudi, če bi nedopustno visoke cene nekomu na primer dejansko onemogočale dostop do določenega blaga ali storitev (WP29, 2017a, str. 15).

5.1.4 Obveščanje o vedenjskem oglaševanju

Ustrezna obveščenost je bistveni pogoj veljavnega soglasja posameznika oz. uporabe katere koli pravne podlage za obdelavo osebnih podatkov. Težava pri vedenjskem oglaševanju je, da uporabniki na splošno slabo poznajo in slabo razumejo tehnologije, ki so uporabljene za vedenjsko oglaševanje, oz. morda sploh ne vedo, da so podvrženi takemu oglaševanju na spletu. Obveščanje mora biti izvedeno skladno z Uredbo 2016/679, kot to določa tretji odstavek 5. člena o Direktive 2002/58/ES o zasebnosti v elektronskih komunikacijah, in sicer morajo biti informacije:

(1) jedrnate, pregledne, razumljive in lahko dostopne (člen 12(1))
To pomeni, da so jasno ločene od drugih informacij, ki niso povezane z zasebnostjo, kot so pogodbene določbe ali splošni pogoji uporabe. Priporočljiva je uporaba večdelnih (angl. layered) izjav, kjer lahko posameznik takoj dostopa do tistih informacij, ki ga zanimajo. Razumljive morajo biti povprečnemu članu ciljne skupine, ki jim je obvestilo namenjeno. Zlasti pri tehnično zapletenih ali nepričakovanih obdelavah podatkov bi morali upravljavci posebej in nedvoumno navesti tudi najpomembnejše posledice, ki jih bo obdelava imela za posameznike. Lahko dostopno pa se nanaša na to, da bi moralo biti posamezniku nemudoma jasno, kako dostopati do informacij, in ne da jih je prisiljen iskati (npr. s povezavo, jasno oznako ali v obliki odgovora na vprašanje, kontekstnih pojavnih oknih ali v interaktivnem digitalnem kontekstu s pogovornim programom itd.) (WP29, 2017c, str. 6–8). Delovna skupina iz člena 29 je poudarila tudi t. i. *push and pull* sporočila, ki posamezniku olajšajo dostopnost, tj. ažurna (angl. *right on time*) obvestila, ki so npr. na oglasu ali ob aktivnosti obdelave osebnih podatkov ter nadzorne plošče za zasebnost (angl. *privacy dashboard*), kjer posameznik lahko sam pridobiva informacije, ki jih želi (WP29, 2017c, str. 22).

(2) Uporabiti je treba jasen in preprost jezik (posebej pri obveščanju otrok (člen 12(1));
Izogniti se je treba zapletenim stavčnim in jezikovnim strukturam. Informacije bi morale biti konkretne in dokončne. Informacije naj ne bi bile abstraktne ali dvoumne ali dopuščati možnost drugačne razlage. Jasni morajo biti zlasti nameni obdelave osebnih podatkov in pravna podlaga zanjo. Informacije ne bi smele biti v čezmerno pravniškem, tehničnem ali strokovnem jeziku ali izrazju. Delovna skupina iz člena 29 kot primer slabe prakse navaja: »Vaše osebne podatke lahko uporabimo za zagotavljanje prilagojenih storitev,« saj ni jasno,

kaj »prilagoditev« vključuje (WP29, 2017c, str. 9–10). Poudarila je tudi nekaj primernih obvestil – npr. za področje osebno prilagojenega oglaševanja:

> »Hranili bomo podatke o tem, na katere članke na spletnem mestu ste kliknili in jih uporabili za ciljno oglaševanje na tem spletnem mestu, tako da bodo oglasi ustrezali vašim interesom, ki jim bomo ugotovili na podlagi člankov, ki jih preberete.«

Tukaj je jasno, kaj osebna prilagoditev vključuje in kako se ugotavljajo interesi, pripisani posamezniku. In drug primer:

> »Podatke o vaših pretekih nakupih bomo hranili in uporabili podrobnosti o izdelkih, ki ste jih kupili, za oblikovanje priporočil za druge izdelke, ki vas bodo po našem mnenju prav tako zanimali.«

Jasno je, kakšne vrste podatkov se bodo obdelovale, da bo posameznik predmet ciljno usmerjenih oglasov za izdelke in da bodo njegovi podatki uporabljeni za omogočanje tega (WP29, 2017c, str. 9–10). Člen 13 Uredbe 2016/679 določa vsebino obvestila, kadar so podatki zbrani neposredno od posameznika, 14. člen pa vsebino, ko podatki niso zbrani neposredno od posameznika. Za vedenjsko oglaševanje sta relevantna oba scenarija, saj lahko podatke o posamezniku zbira upravljavec neposredno, lahko pa jih tudi pridobi od drugega subjekta, npr. preprodajalca podatkov, in jih priključi svojim informacijam.[59]

V okviru uporabe piškotkov in podobnih tehnologij to pomeni, da bi morali biti posamezniki obveščeni o tem, kdo obdeluje njihove podatke, in o namenih obdelave, o tem, da bo piškotek ponudniku oglaševanja omogočal zbiranje podatkov o obiskovanju drugih spletnih mest, oglasih, ki so bili prikazani, oglasih, ki jih je uporabnik kliknil, času itd. Obstajati bi morala preprosta razlaga o uporabi piškotka za ustvarjanje profilov za namene prilagojenega oglaševanja (WP29, 2010a, str. 18–19). Osnovne informacije bi morale biti podane neposredno na zaslonu na interaktiven, opazen in razumljiv način in ne skrite v splošnih pogojih in/ali izjavah o zasebnosti. Potencial je lahko tudi v razvoju različnih ikon v ali ob oglasih, ki kažejo na prisotnost vedenjskega oglaševanja. Tako bi bili uporabniki vedno obveščeni o tem, da vedenjsko oglaševanje poteka, hkrati pa bi jih simbol opominjal tudi na to, da lahko svoje soglasje kadar koli umaknejo (WP29, 2010a, str. 19).

[59] Podrobnejše informacije o elementih obvestila so v prilogi O.

5.1.5 Odgovornosti različnih akterjev v ekosistemu vedenjskega oglaševanja

Odgovornosti različnih akterjev v ekosistemu vedenjskega oglaševanja določata tako Direktiva 2002/58/ES kot tudi Uredba 2016/679, ki opredeljujeta, kdo so akterji, ki nosijo glavnino obveznosti – tj. pridobivanje privolitve posameznika in obveščanje. Direktiva 2002/58/ES glavnino obveznosti pripisuje subjektom, ki nalagajo piškotke in/ali pridobivajo podatke iz terminalske opreme posameznika, na katerega se nanašajo podatki oziroma v primeru drugih določb operaterjem elektronskih komunikacij (Direktiva 2002/58/ES, člen 5(3)). Obveznosti z vidika varstva osebnih podatkov pa primarno zadevajo upravljavca osebnih podatkov, tj. subjekt, ki v konkretnem primeru in okoliščinah določa namene in sredstva obdelave podatkov (Uredba 2016/679, člen 4(7)).

Kot kaže dokumentarna analiza, na tem področju ni ustaljenih praks in se pravne razlage še razvijajo, predvsem glede vprašanj delitev odgovornosti pri spletnem vedenjskem oglaševanju, ki vključuje uporabo piškotkov in podobnih tehnologij, kjer v grobem nastopajo tri vrste subjektov: izdajatelji spletnih strani oz. ponudniki storitev, aplikacij (posamezniki njihovo spletno stran obiščejo oz. uporabljajo storitev), oglaševalske mreže oz. drugi specializirani ponudniki oglaševalskih storitev (ti sodelujejo pri prikazu oglasa na spletni strani ali prek storitve izdajatelja) in oglaševalci (njihov oglas je s pomočjo oglaševalski mrež prikazan na strani izdajatelja). Vsi ti subjekti imajo teoretično možnost nastavljanja piškotkov oz. drugih tehnologij na posameznikovo napravo in možnost obdelave njegovih podatkov (piškotkov prvih oziroma tretjih strank, več v poglavju 2). Prav tako vsi lahko obdelujejo osebne podatke posameznikov, vendar ni nujno, da imajo dostop do enakih podatkov. Od konkretnega položaja je torej odvisno, kateri subjekti so v vlogi upravljavcev osebnih podatkov. Hkrati pa nimajo vsi ti subjekti neposrednega stika s posameznikom, tako da bi mu lahko prikazali obvestilo o obdelavi osebnih podatkov in od njega ustrezno pridobili privolitev. Zato je na tem področju precej vprašanj: mora privolitve za oglaševanje, ki ga izvajajo partnerske oglaševalske mreže, pridobiti izvirna spletna stran, ki jo je obiskal posameznik, ali je na oglaševalskih mrežah in drugih subjektih tega tipa odgovornost, da obveščajo posameznike in pridobivajo privolitve?

Po eni strani imajo oglaševalske mreže in drugi ponudniki oglaševalskih storitev popoln nadzor nad nameni in načini obdelave osebnih podatkov, saj »najemajo« prostor na spletnih

mestih izdajateljev za objavo oglasov, nastavljajo in berejo podatke, povezane s piškotki, ter morebitne druge podatke, ki bi jih lahko razkril brskalnik. Zbrane podatke o brskalnih navadah internetnih uporabnikov uporabijo za oblikovanje profilov in posredovanje oglasov na podlagi profila. V tem smislu imajo vlogo upravljavca osebnih podatkov (WP29, 2010a, str. 11). Izdajatelji dajejo v najem prostor na svojih spletnih mestih, na katerega lahko oglaševalske mreže postavijo oglase. Spletna mesta nastavijo tako, da je brskalnik uporabnika samodejno preusmerjen na spletno stran ponudnika oglaševalske mreže (ki nato pošlje piškotek in posreduje prilagojene oglase). Ponudniku oglaševalske storitve lahko posredujejo tudi dodatne osebne podatke o svojih obiskovalcih in so tako soodgovorni za tiste obdelave osebnih podatkov, ki so pod njihovim nadzorom (WP29, 2010a, str. 11–12). V tem smislu Delovna skupina iz člena 29 meni, da morajo izdajatelji skupaj z oglaševalskimi mrežami poiskati ustrezne načine za izpolnjevanje obveznosti upravljavca in zagotavljanje pravic posameznikov, na katere se nanašajo osebni podatki. Izdajatelji bi se morali zavedati, da s sklenitvijo pogodbe z oglaševalskimi mrežami, s čimer osebne podatke svojih obiskovalcev dajo na voljo ponudnikom oglaševalskih mrež, prevzemajo del odgovornosti do svojih obiskovalcev (WP29, 2010a, str. 12–13). Na koncu so tukaj še *oglaševalci*, ki podatke posameznika lahko prejmejo, ko ta klikne na prikazan oglas. Oglaševalec je tako lahko neodvisen upravljavec podatkov za ta del obdelave podatkov (WP29, 2010a, str. 13).

Z razvojem programatičnega oglaševanja se spreminjajo tudi odnosi v ekosistemu vedenjskega oglaševanja in vnovič odpirajo premisleki o tem, kakšne so dolžnosti spletnih strani izdajateljev, ki uporabljajo oglaševalske storitve tretjih strank. Francoski nadzorni organ za varstvo osebnih podatkov v tem smislu razlikuje med dvema možnostma, predvsem glede na to, za čigav namen se obdelujejo posameznikovi podatki:

1. upravljavec spletne strani (izdajatelj) uporablja piškotke s svoje spletne strani ali dovoli tretjim stranem da nalagajo piškotke prek njegove spletne strani, pri čemer obdelava osebnih podatkov poteka izključno za njegove lastne namene, ne za namene tretjih strani.

V tem primeru je izdajatelj spletne strani v vlogi upravljavca osebnih podatkov, katerega dolžnost je pridobivanje predhodnega soglasja za piškotke, pa tudi omogočanje načina za zavrnitev piškotkov. Če uporablja storitev tretjih strani, vendar za izpolnjevanje svojih lastnih namenov, so te lahko pogodbeni obdelovalci osebnih podatkov, pri čemer jih mora

pogodbeno zavezati, da podatkov ne smejo obdelovati za druge namene. Tak scenarij je značilen za naslednje storitve:

- spletne trgovine, pri katerih oglaševalski vmesniki ali agencije uporabnikom servirajo piškotke za namen vnovičnega ciljanja (angl. *retargeting*) (za pošiljanje ciljnega oglasa uporabnikom, ki so spletno trgovino že obiskali in si npr. ogledali določen produkt),
- spletne strani, ki uporabljajo orodja za merjenje in analizo občinstev, ki temeljijo na piškotkih; bodisi lastna, bodisi orodja tretjih strank,
- spletne strani, ki uporabljajo piškotke za merjenje dobičkonosnosti oglasnega prostora, ki ga imajo na voljo (da lahko maksimirajo prihodke, urejajo zaračunavanje) (Orion, 2017);

2. osebne podatke, ki so bili zbrani s pomočjo piškotka tretje stranke, obdeluje ta tretja stranka in ne upravljavec spletne strani.

V tem primeru upravljavec spletne strani nima nadzora nad tem, kako in za katere namene se obdelujejo podatki, zbrani s pomočjo piškotkov tretjih strank. Ima pa neposreden odnos s tretjo stranjo, ki na naprave uporabnikov nalaga piškotke. Ta tretja stran lahko sklepa nadaljnje dogovore z nadaljnjimi tretjimi stranmi, ki bodo na naprave uporabnikov shranjevale piškotke, s katerimi upravljavec spletne strani ni več neposredno povezan. Tretja stran ima nadzor nad nameni obdelave osebnih podatkov, ali jih bo uporabila za svoje potrebe ali izvajala analize ali profiliranje za svoje stranke in partnerje. Tukaj gre za:

- storitve profiliranja spletnih uporabnikov prek različnih spletnih strani z namenom segmentiranja in prodaje teh informacij tretjim strankam,
- platforme za draženje uporabniških profilov v realnem času, ki oglaševalcem prodajo pravico, da objavijo oglas na določenem mestu,
- tretje strani, ki delajo v imenu oglaševalca (npr. *Demand Side Platforms*), ki podajajo ponudbe za oglaševalski prostor in uporabljajo informacije, povezane z oglaševalskim prostorom za prilagoditev svojega ciljanja.

Take tretje strani je treba obravnavati kot upravljavce osebnih podatkov, izdajatelji spletnih strani pa so v tem primeru v vlogi pogodbenih obdelovalcev, saj delujejo v imenu in glede na pooblastila upravljavcev osebnih podatkov. Ti bi morali poskrbeti, da imajo s spletnimi stranmi sklenjene ustrezne pogodbe, in tako zagotoviti, da so bile od uporabnikov spletne

strani zbrane ustrezne privolitve in da imajo na voljo preprost način, da oporekajo piškotkom. Spletne strani se običajno znajdejo v obeh vlogah hkrati – deloma kot upravljavci osebnih podatkov in deloma kot pogodbeni obdelovalci – odvisno od primera (Orion, 2017).

Hkrati to področje želi razjasniti tudi nova Uredba o zasebnosti in elektronskih komunikacijah (več v poglavju 5.1.7), po kateri naj bi privolitev moral pridobiti tisti, ki dostopa do naprave – naloži piškotek oz. pridobi informacije z uporabnikove naprave, torej ponudnik storitve ali oglaševalske mreže. Ti lahko zaprosijo tudi drugo stran (izdajatelja), da pridobi privolitev zanje. Taka privolitev velja tudi za nadaljnja branja piškotka na strani, ki jo je obiskal uporabnik (predlog Uredbe o zasebnosti in elektronskih komunikacijah, 2017, uvodna izjava 20). Taka ureditev smiselno sledi francoskemu modelu,po katerem je tretja stran dolžna urediti pridobivanje soglasja, tudi če zato pooblasti dejansko obiskano spletno stran.

Drugo pomembno vprašanje je, kdo v ekosistemu vedenjskega oglaševanja bi moral zagotoviti te informacije – bi jih moral zagotoviti izdajatelj, ponudnik oglaševalske mreže oz. oglaševalske storitve ali oba? Dokumentarna analiza kaže, da je tukaj poudarek na sodelovanju ponudnikov oglaševalskih mrež (in storitev) ter izdajateljev (WP29, 2010a, str. 19). Izdajatelji bi morali posameznikom, na katere se nanašajo podatki, zagotoviti informacije o obdelavi podatkov, do katere pride zaradi preusmeritve brskalnika na njihovi strani, in tudi o namenih, za katere bodo podatke pozneje uporabljali ponudniki oglaševalskih mrež. To je še toliko pomembneje, ker je ponudnik oglaševalske mreže za posameznika, na katerega se nanašajo podatki, načeloma neviden. Interakcija uporabnika poteka le z obiskanim spletnim mestom izdajatelja. Zato je z uporabnikovega stališča bolj naravno, če obvestilo prejme od spletnega mesta izdajatelja, tako da ta npr. zagotovi prostor za obvestilo oglaševalske mreže (WP29, 2010a, str. 20). Kadar oglaševalski partnerji obdelujejo podatke na podlagi piškotkov za svoje namene, pa je odgovornost za točnost informacij na njih, upravljavec spletne strani pa mora uporabnika obvestiti o tem, da uporablja tudi piškotke tretjih strani (Orion, 2017).

5.1.6 Nacionalne razlike in nadzor nad področjem vedenjskega oglaševanja

Nadzor na področju vedenjskega oglaševanja predvsem zajema vprašanje skladnosti s pravili o piškotkih in podobnih tehnologijah iz Direktive 2002/58/ES o zasebnosti in elektronski

komunikacijah ter spoštovanjem pravil varstva osebnih podatkov[60] in tako predvsem usmerjen na vprašanja privolitve posameznikov ter na tehnične načine njene izpeljave. Pregled praks uporabe piškotkov v različnih državah članicah EU in aktivnosti nadzornih organov kaže, da je na vzorcu skoraj 500 spletnih strani skoraj 70 odstotkov piškotkov tretjih strank in le 30 odstotkov piškotkov spletnih strani, ki so bile dejansko obiskane. Le 25 ponudnikov storitev (tretjih strank) naloži več kot polovico vseh piškotkov, med njimi prevladujejo Google, Yahoo (Right Media), AOL (Advertising.com), Amazon (A9), Dstillery in Twitter. Google AdSense, AdWords in Doubleclick so prisotni na več kot polovici spletnih strani v Evropi. Največ piškotkov se naložili ob obisku medijskih spletnih strani in najmanj na spletnih straneh javnega sektorja. Pasica z obvestilom o piškotkih je najbolj priljubljen način za obveščanje obiskovalcev spletnih strani o piškotkih. Številne spletne strani nimajo ustreznih informacij o piškotkih. Le 16 odstotkov spletnih strani uporabnikom ponuja možnost zavrnitve piškotkov in upravljanja z njimi – večina navaja možnosti, ki jih ponujajo brskalniki ali samoregulacijska shema (WP29, 2015b).

Kljub mnenjem in smernicam, v katerih Delovna skupina iz člena 29 pojasnjuje razmeroma nejasno določbo o piškotkih in podobnih tehnologijah, da bi se uskladila praksa nadzornih organov v EU, so na območju držav članic EU vzniknile različne razlage pravil. Na Nizozemskem je bil leta 2015 celo spremenjen zakon, ki je dodal izjemo za analitične piškotke, ki je Direktiva 2002/58/ES ne pozna. Pravila o piškotkih so tako le delno učinkovita zaradi nejasnosti v smislu obsega piškotkov in tehnologij, ki naj bi bil po eni strani preširok (in vključuje tudi piškotke, ki za zasebnost posameznika nimajo posebnega tveganja), po drugi strani pa preozek, saj ni popolnoma jasno, koliko vključuje drugačne tehnologije sledenja (npr. z odtisom naprave, sledenje prek različnih brezžičnih tehnologij), omejene preglednosti in učinkovitosti mehanizmov za podajo soglasja in tudi težave z vidika nadzora (Evropska komisija, 2017, str. 134–135).

Problematična je tudi preglednost mehanizmov za podajanje soglasja, saj posamezniki nimajo možnosti za upravljanje in za zavrnitev soglasja ter načini izražanja soglasja, pri katerih uporabnikom ni jasno, da privolitev pomeni, da bodo podvrženi obširnemu sledenju in profiliranju, tudi zaradi preobremenjenosti z informacijami in kompleksnostjo (Evropska komisija, 2017, str. 137). V praksi so imeli nadzorni organi različna stališča do t. i. implicitne

[60] Več o pristojnosti nadzornih organov EU v primeru čezmejnih podjetij v prilogi P.

(domnevne) privolitve, ki se je v praksi kazala zgolj kot obvestilo o piškotkih, ni pa posameznik imel možnosti aktivne interakcije in zavrnitve. Različna so bila mnenja, v katerih primerih piškotkov je tak način privolitve (za katerega je bilo tudi sicer tudi pod ohlapnejšimi določbami Direktive 2002/58/ES o varstvu osebnih podatkov sporno, ali je veljaven) lahko veljaven. Posledično so v državah članicah, ki so zahtevale izrecnejše načine podajanja privolitve, vzniknili t. i. zidovi piškotkov, kjer je ponudnik spletne strani dostop do vsebine začel pogojevati z izrecnim strinjanjem z vsemi piškotki. Razprava, ali je taka praksa dopustna, še vedno poteka. Analiza prenosa Direktive 2002/58/ES kaže, da je bil ta na nacionalnih ravneh razdrobljen, kar vpliva tudi na stroške, ki so jih imeli subjekti z zagotavljanjem skladnosti, saj ni nujno, da so bile enake tehnološke rešitve skladne s pravili v državah članicah EU. Posebej pri pravilih o piškotkih, ki niso dosegla svojega namena, ti stroški niso upravičeni (Evropska komisija, 2017, str. 19–20).

Poleg nejasnosti določbe, ki dopušča različne razlage, je za to področje značilen tudi neusklajen nadzor v različnih državah članicah EU. Eden od razlogov za neučinkovit nadzor je tudi v tem, da Direktiva 2002/58/ES državam članicam dopušča, da same določijo organ, ki je pristojen za nadzor na tem področju. V praksi je to pomenilo, da so določbo o piškotkih nadzorovali tako organi za varstvo osebnih podatkov kot tudi nacionalni regulatorji za področje telekomunikacijskih družb, ponekod tudi regulator za področje trga, kar vsekakor ni pripomoglo k harmonizirani uporabi pravil. Dodatni razlog, poudarjen v analizi Direktive 2002/58/ES, je bilo pomanjkanje smernic glede čezmejnih primerov, ki so pri piškotkih realnost, ter dejstvo, da vsi različni organi niso imeli neke skupne referenčne skupine za sodelovanje na ravni EU (Evropska komisija, 2017, str. 195).

5.1.7 Uredba o zasebnosti in elektronskih komunikacijah

Po sprejetju in uveljavitvi Uredbe 2016/679 je stekel postopek sprememb Direktive 2002/58/ES. Tako je bil v začetku leta 2017 objavljen prvi predlog Uredbe o zasebnosti in elektronskih komunikacijah[61] (oziroma ePR), ki je vseboval strožja in jasnejša določila glede zasebnosti uporabnikov pri uporabi elektronskih komunikacij. Pravila naj bi po novem morali

[61] Predlog 2017/0003 (COD) Uredba evropskega parlamenta in sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah)

spoštovati tudi ponudniki komunikacijskih storitev, kot so storitve hipnega sporočanja, npr. Skype, Whatsapp itd. in deloma tudi ponudniki storitev v okviru interneta stvari, ki jih prej veljaven režim, usmerjen predvsem na ponudnike telekomunikacijskih omrežij, ni zajemal. Pravila vključujejo omejitve za obdelavo vsebine komunikacij in tudi za obdelavo metapodatkov (to so t. i. prometni podatki – npr. telefonska števila, naslov IP, časi komunikacij, lokacije itd.). Spremenjena je določba o piškotkih – ker je prej veljavna povzročila poplavo zahtev za privolitev, se novo pravilo bolj naslanja na privolitev prek nastavitev v brskalniku, dodana je nova izjema za analitične piškotke za štetje obiskovalcev. Zajete so tudi določbe glede neželenih sporočil (angl. *spam*). Nadzor nad uredbo naj bi zaradi bolj usklajenega nadzora vsaj deloma prevzeli organi za varstvo osebnih podatkov, ki nadzorujejo tudi uporabo Uredbe 2016/679. Predlog ePR je konec leta 2017 dopolnila pristojna komisija Evropskega parlamenta, ki je nekatere določbe še zaostrila. Tako je npr. predlagala, da ne bi bili dovoljeni t. i. zidovi piškotkov, pri katerih dostop do vsebine uporabnikom ni dovoljen, če se ne strinjajo z vsemi piškotki (Evropski parlament, 2017). Nadaljnji postopek je vodil predlog ePR v usklajevanje do sveta EU – do vlad držav članic, ki v okviru predsedovanja EU osnutek predvsem rahljajo ter glede na pritiske in predloge držav članic ustvarjajo kompromisni predlog (Council of the European Union, 2019). V nadaljevanju sledi očrt nekaterih ključnih področij in njihovih sprememb prek različnih zakonodajnih predlogov.

Obseg storitev, ki jih bo urejala omenjena uredba, je veliko širši, s tem pa za področje vedenjskega oglaševanja postane relevantnih tudi več določb. Vedenjsko oglaševanje je mogoče izvajati na podlagi sledenja uporabnikovi napravi, bodisi po spletu, s pomočjo piškotkov in podobnih tehnologij, bodisi glede na fizične lokacije, kjer se oseba giblje. Vhodni podatki za izdelavo posameznikovega profila so lahko vezani na njegove aktivnosti na spletu ali pri uporabi mobilnih aplikacij, lahko pa so to tudi metapodatki, ki jih obdeluje ponudnik storitve, bodisi ponudnik dostopa do interneta ali ponudnik platforme za hipno sporočanje, lahko tudi ponudnik storitve v okviru naprav, povezanih v internet stvari. Za izvajanje storitve namreč običajno vsi obdelujejo metapodatke (kdo je komuniciral s kom, kdaj, s katere lokacije ipd.), ki jih je mogoče dalje izkoriščati tudi onkraj prvotnega namena zagotavljanja storitve in zaračunavanja. Predlog uredbe opredeljuje različne podlage, na katerih je dopustno obdelovati take podatke: če je to nujno zaradi urejanja in optimizacije omrežja in ni mogoče na anonimiziranih podatkih, če je nujno zaradi zaračunavanja ali

izvajanja pogodbe z naročnikom, če je končni uporabnik podal soglasje za enega ali več določenih namenov, če je nujno za zavarovanje vitalnega interesa fizične osebe v primeru sile, če je potrebno za statistične namene ali znanstvene raziskave (z dodatnimi omejitvami in sklicem na Uredbo 2016/679) (Council of the European Union, 2019). Omejitve za obdelavo metapodatkov so bile zajete že v Direktivi 2002/58/ES, in sicer s pojmom »prometni podatki«. Ker pa je Direktiva 2002/58/ES v tem delu veljala le za telekomunikacijske družbe, torej ponudnike dostopa do elektronskih komunikacij, je omejevanje obdelave prometnih podatkov npr. za namen vedenjskega oglaševanja na podlagi privolitve uporabnika zadevalo le majhen krog subjektov (Direktiva 2002/58/ES, člen 6). S spremenjenim obsegom subjektov, ki zapadejo pod določbe uredbe, bodo ta pravila zadevala tudi večji krog ponudnikov storitev, od katerih mnogi temeljijo svoj poslovni model prav na monetizaciji s pomočjo ciljanega oglaševanja, saj je osnovna komunikacijska storitev uporabniku običajno na voljo brezplačno. Pravna podlaga za vedenjsko oglaševanje na podlagi metapodatkov naj bi tako bila glede na (trenutni) 6(b). člen ePR privolitev uporabnika, hkrati pa ePR uvaja še novost – nadaljnjo obdelavo podatkov za namene, drugačne od tistih, za katere so bili zbrani. ePR določa pogoje, kdaj je taka obdelava za drugotne namene in ne na podlagi privolitve ali zakonske določbe možna, in napotuje upravljavca na izvedbo presoje kompatibilnosti namenov, poleg tega pa bi morali biti podatki psevdonimizirani in ne uporabljeni za profiliranje posameznikov. Upravljavec bi moral izvesti presojo vplivov na zasebnost in se posvetovati z nadzornim organom ter posameznika obvestiti o pravici, da ugovarja taki obdelavi. Kritika označuje uvedbo možnosti za nadaljnjo obdelavo metapodatkov brez privolitve posameznika na podlagi tehtanja, ki ga izvede ponudnik storitve, za nekakšno pravno praznino, podobno podlagi zakonitega interesa v Uredbi 2016/679, ki ponuja možnosti izkoriščanja podatkov (Lund, 2018).

Za vedenjsko oglaševanje, ki temelji na piškotkih ali podobnih tehnologijah, so bistvene določbe o piškotkih, pa tudi o pogojevanju dostopa do storitve in zasebnosti prijaznih začetnih storitvah. Določba o piškotkih vsebuje več izjem, pri katerih za piškotke ni potrebno soglasje: če so potrebni za pošiljanje komunikacije, potrebni za izvajanje storitve, ki jo je zahteval uporabnik, če so uporabljeni za štetje obiskovalcev in štetje izvaja obiskana spletna stvar ali njen pogodbeni obdelovalec, če so potrebni za varnostne namene ter preprečevanje zlorab in (pod določenimi pogoji) če so potrebni za samodejne posodobitve. Zadnji kompromisni predlog gre v nasprotno smer kot predlog Evropskega parlamenta in dovoljuje zidove, pri

katerih je uporabnik prisiljen, da se za brezplačne dostop do vsebine strinja s piškotki, tudi če niso potrebni za izvajanje storitve (običajno so to piškotki za vedenjsko oglaševanje), če spletna stran ponuja tudi drugačen dostop do vsebine, brez strinjanja s piškotki, npr. naročnino na spletno publikacijo 2002/58/ES (Council of the European Union, 2019, člen 8). Lund (2018) opozarja, da to pomeni, da osebni podatki postanejo komodificirani in z njimi uporabniki lahko trgujejo ter da je ePR glede tega v neskladju z Uredbo 2016/679, ki določa, da osebni podatki ne smejo predstavljati nasprotne izpolnitve v pogodbenem smislu (Uredba 2016/679, četrti odstavek 7. člena) (Lund, 2018). Kompromisni predlog prav tako popolnoma opušča dolžnost za brskalnike in aplikacije, da ponujajo možnost blokiranja piškotkov in drugih sledilnih tehnologij tretjih strani ter da z možnostmi nastavitev seznanijo uporabnike takoj ob namestitvi (Council of the European Union, 2019, člen 10).[62]

Nadzorni organi za varstvo osebnih podatkov in zagovorniki zasebnosti poudarjajo, da bi morala biti pravila strožja oziroma čim bolj določna, da ne bi obstajale pravne praznine glede določenih praks sledenja posameznikom prek različnih naprav in izkoriščanja njihovih podatkov. WP29 se je tako v več mnenjih izrekla glede situacij, v katerih so uporabniki prisiljeni v strinjanje z vsemi piškotki (t. i. *cookie walls*), tudi invazivnimi sledilnimi in bi morali biti po njihovem mnenju v ePR izrecno prepovedani, to je:

- sledenje na spletnih straneh, aplikacijah ali lokacijah, ki razkrivajo občutljive podatke o posameznikih, ne glede na to, ali jih razkrijejo sami ali pa so izpeljani iz drugih podatkov;
- sledenje s strani neidentificiranih tretjih strani za nedoločene namene, kot pri praksah *real time bidding*;
- sledenje na spletnih straneh, ki so financirane z javnimi sredstvi;
- vedno, ko gre za neenake položaje moči – če ni enakovredne alternative ali če je posameznik prisiljen v privolitev na podlagi pogodbe za uporabo storitve;
- če je ena privolitev podana hkrati za več namenov – privolitev mora biti posebna, granularna (WP29, 2016, str. 16–17).

Taki zidovi piškotkov bi morali biti prepovedani, saj prisilijo uporabnike v strinjanje s sledenjem, če želijo dostop do storitve (WP29, 2017d, str. 4). WP29 priporoča, da se za namen pridobivanja privolitev spodbuja uporaba tehničnih standardov, kot je npr. standard ne sledi, in da za upravljavce velja obveznost, da morajo take nastavitve uporabnikov spoštovati

[62] Črtan 10. člen in uvodne izjave od 22 do 24.

(WP29, 2016, str. 16–17) ter da morajo ponudniki naprav in programske opreme privzeto omogočati zasebnosti prijazne nastavitve, ki jih lahko uporabnik spremeni med namestitvijo (WP29, 2017d, str. 4).

Delovna skupina iz člena 29 se je tudi izrecno izrekla proti možnostim, da bi bila lahko obdelava metapodatkov utemeljena na pravni podlagi zakonitega interesa ali nujnosti za izvajanje pogodbe, ampak zaradi občutljivosti meta podatkov vztraja, da mora obdelava temeljiti na strogih omejitvah v zakonu ali v privolitvi uporabnika, ter poudarja, da so v besedilu že zajete dopustne obdelave, npr. za varnost in statistične namene (WP29, 2018).

Kritike ePR poudarjajo, da so predlagana pravila prestroga in toga in da bodo pomenila ogromno finančno izgubo, nekateri napovedujejo tudi do 30-odstoten padec prihodkov v digitalni industriji (Palladino, 2018). Posebej močno naj bi prizadele spletne novice, spletno oglaševanje in računalništvo v oblaku, saj njihovi poslovni modeli temeljijo na obširni obdelavi podatkov in bodo zahteve po soglasjih zanje zelo omejujoče. ePR naj bi zajemala preveč različnih ponudnikov storitev, od spletnih aplikacij pa do interneta stvari, katerih obdelava podatkov bi drugače spadala v okvir Uredbe 2016/679 in ne strožjih specialnih pravil pod ePR. Preveliko poudarjanje koncepta privolitve naj bi vodilo v še večjo brezvoljnost soglašanja. Kritiki namreč poudarjajo, da bi morale biti vključene tudi druge pravne podlage, ki jih predpisuje Uredba 2016/679, npr. zakoniti interes (Fazlioglu, 2018). Argumenti gredo tudi v smer, da ePR pravzaprav ne ponuja več, kot že zagotavlja Uredba 2016/679, in da sploh ni potrebe po natančnejši določitvi pravil za sektor elektronskega komuniciranja, saj bi v tem primeru za področje vedenjskega oglaševanja veljale vse pravne podlage, tudi zakoniti interes, in ne bi več obstajala omejitev le na privolitev posameznika in druge izjeme, pod katerimi so lahko naloženi piškotki in druge podobne tehnologije (Brinkhof Advocaten, 2018, str. 30). Digitalna oglaševalska panoga tudi poudarja, da bi morala ePR dopuščati, da je dostop do storitve pogojen z informirano privolitvijo posameznika v obdelavo osebnih podatkov za namen oglaševanja, ki sicer ni tehnično nujna za izvajanje storitve, je pa nujna za model monetizacije take storitve. Svari tudi pred privzetim blokiranjem sledenja s strani brskalnikov, ki naj bi povzročilo še večji naval zahtev za soglasje, saj bi vsaka spletna stran zase zahtevala izjemo (IAB, 2017, str. 1). Različne koalicije izvajajo pritiske na javnost, vlade držav članic in lobirajo v Bruslju za mehčanje določb (Singer, 2018), kar že kaže učinke, kot izhaja iz zadnjega dostopnega besedila ePR.

Če povzamemo, čeprav se v kontekstu zakonodajnih omejitev vedenjskega oglaševanja v EU poudarja privolitev posameznika kot ključno varovalo za uporabnike in zahteva za ponudnike storitev, vedno obstajajo bodisi razlage, da je privolitev lahko tudi implicirana (s spremembami Uredbe 2016/679 je taka argumentacija sicer postala zelo otežena), bodisi so določene izjeme od zahteve po aktivni privolitvi, ob katerih se bijejo bitke glede njihovega obsega – kateri nameni, katere storitve in kateri piškotki bi lahko spadali v varni pristan takih izjem in ne bi bili podvrženi zahtevam za privolitev posameznika. Kot kaže razvoj ePR in razlage Uredbe 2016/679, bodo še naprej potekale razprave o tem:

- kateri piškotki oz. kakšno sledenje je lahko potrebno za izvajanje storitve, ki jo je zahteval uporabnik (pri čemer je trenutno izpuščena besedna zveza nujno potrebno) – je to lahko tudi oglaševanje, brez katerega marsikateri medij argumentirano ne more ponujati storitve?
- katere spletne strani lahko uporabnikom pogojujejo dostop do vsebine s privolitvijo v piškotke – pri čemer se ne upošteva opredelitve privolitve v Uredbi 2016/679, saj mora biti ta svobodna in ne izsiljena;
- katera obdelava metapodatkov je lahko potrebna v okviru izvajanja pogodbe oz. dopustna kot nadaljnja obdelava, ne glede na namene, za katere so bili prvotno zbrani podatki – je to lahko tudi oglaševanje?
- v primeru katerih obdelav podatkov se lahko izvajalec zanaša na pravno podlago zakonitega interesa?

V praksi to pomeni, da izvajalci vedenjskega oglaševanja poslujejo na trgu s precej pravne negotovosti, kljub strogim razlagam pravil v mnenjih nadzornih organov. Če temu prištejemo še pomanjkljiv nadzor nad nejasnimi pravili, ne čudi posledica, da kljub (na papirju) strogim pravilom na trgu sledenja in vedenjskega oglaševanja pravzaprav ni omejevanja in lahko že leta spremljamo veliko rast in širjenje praks, ki poleg pozitivnih plati osebne prilagoditve pomenijo tudi velika tveganja za pravice posameznikov.

V Evropi področje vedenjskega oglaševanja ureja precej zakonodaje, ki pa je prepuščena različnim razlagam, nadzor je razpršen, po državah različen in zato neučinkovit. Podjetja se pravilom prilagajajo malo tu in malo tam, svojega poslovnega modela, ki je srž problema posegov v pravice posameznikov, pa ne spreminjajo. Finančne sankcije se zdijo zanje prej strošek, kot pa resna motivacija za spremembo najspornejših praks. Za resnejši učinek bi moral biti nadzor poenoten po vsej EU, za kar pa je potrebna politična volja. Zakonodaja to

večinoma že omogoča in dopušča, pravne in politične volje za omejevanje podatkovnih panog, kot jasno kaže slika stanja v tej panogi, (še) ni.

5.2 Pravni okvir za varovanje osebnih podatkov v Združenih državah Amerike

Pravni okvir za varovanje osebnih podatkov v Združenih državah Amerike (ZDA) pogosto opisujejo kot krpanko (Cunningham, 2015), saj splošne zakonodaje o varovanju osebnih podatkov ni, temveč različni zakoni urejajo varovanje osebnih podatkov v različnih sektorjih in panogah, in sicer na zvezni ravni in na ravni zveznih držav (Sotto in Simpson, 2014, str. 208), hkrati pa je treba še upoštevati kodekse samoregulacije in navodila izvršne oblasti (angl. *executive order*). Organizacije, ki uporabljajo, hranijo ali prenašajo osebne podatke, morajo tako upoštevati zakonodajo na različnih ravneh, ki med seboj pogosto ni usklajena. Pravica do varstva osebnih podatkov in zasebnosti ni razumljena kot temeljna človekova pravica (Cunningham, 2015), ampak je načeloma obravnavana z vidika pravic potrošnika.

5.2.1 Sektorske omejitve za obdelavo osebnih podatkov

Zakonodaja lahko nekatere prakse varovanja osebnih podatkov predpisuje na ravni zveznih držav. Skoraj vse imajo tako zakone, ki v primeru incidentov, pri katerih so razkriti osebni podatki, nalagajo organizacijam, da o tem obvestijo posameznike (Burnik, 2012, str. 127–128). Poseben primer je Kalifornija, katere zakonodajalec je v zadnjih letih sprejel več zakonov, ki varstvo osebnih podatkov obravnavajo na splošni ravni in ne le sektorsko. Zakonodaja na zvezni ravni, ki obravnava osebne podatke, pa je vezana predvsem na sektorje, ki zgodovinsko gledano obdelujejo občutljivejše osebne podatke (Cunningham, 2015). Kot poudarja Bennet (1997), je splošni pristop k varovanju zasebnosti v ZDA reaktiven in ne proaktiven (angl. *anticipatory*), ter razdrobljen in ne celosten (Bennet, 1997, str. 7, v: Crain, 2016, str. 5). Zakoni so pogosto zelo ozko usmerjeni in zadevajo samo specifične primere uporabe osebnih podatkov, npr. uporabo osebnih podatkov za namen izdelave kreditne ocene potrošnika, obdelavo osebnih podatkov otrok na spletu, obdelavo zdravstvenih podatkov, obdelavo podatkov, ki jih obdelujejo izposojevalnice videov, itd.[63]

[63] Več v prilogi R.

ZDA nimajo posebnega splošnega zakona, ki bi urejal obdelavo osebnih podatkov, zato se opredelitev osebnega podatka oz. podatka, ki posameznika določi (angl. *personally identifiable information* – PII) v različnih zakonih razlikuje. V kontekstu nekaterih zakonov so to predvsem ime in priimek, številka socialnega zavarovanja, številka vozniškega dovoljenja ali bančnega računa. V odločitvah FTC pa je pojem osebnih podatkov širši. Nekateri zakoni se uporabljajo le za elektronske podatke, drugi pa v primeru katerih koli medijev, ki hranijo podatke (Sotto in Simpson, 2014, str. 209; Cunningham, 2015). Zakonodaja v ZDA ne pozna enotnega pojma občutljivih osebnih podatkov, ki bi bili podvrženi višjim standardom. So pa organizacije glede na zakone, ki urejajo poročanje o incidentih v zvezi z osebnimi podatki, če hranijo posameznikovo ime in priimek ter tudi številko socialnega zavarovanja, številko vozniškega dovoljenja ali bančnega računa, zavezane, da prizadetim posameznikom poročajo o morebitnih incidentih, pri katerih bi bili njihovi osebni podatki razkriti nepooblaščenim osebam (Sotto in Simpson, 2014, str. 209).

Zakonodaja v ZDA ne razlikuje med upravljavci osebnih podatkov in pogodbenimi obdelovalci, ampak se obveznosti razlikujejo glede na to, ali je entiteta »lastnik osebnih podatkov« ali »ponudnik storitev«. Zakonodaja, ki določa obveznost poročanja o varnostnih incidentih, ki vodijo v razkritja osebnih podatkov, tako zavezuje lastnike osebnih podatkov, ponudnik storitev pa mora zaznan incident le poročati lastniku osebnih podatkov (Sotto in Simpson, 2014, str. 209). Subjekti, ki obdelujejo osebne podatke, niso omejeni s pravnimi podlagami. Lahko pa posamezni zakoni posredno omejujejo obdelavo. Primer je kalifornijski zakon o zaščiti zasebnosti na spletu, po katerem morajo organizacije, ki na spletu pridobivajo osebne podatke, objaviti obvestilo, katere osebne podatke zbirajo in kako jih uporabljajo. Če podatke želijo uporabiti na drugačne načine, kot so navedli v obvestilu, morajo posameznike o tem obvestiti in pridobiti njihovo soglasje. V nasprotnem primeru bi tako prakso lahko šteli za zavajajočo poslovno prakso glede na zvezno zakonodajo o nepošteni konkurenci (Sotto in Simpson, 2014, str. 209). Možnosti, ki jih imajo posamezniki glede obdelave svojih osebnih podatkov za drugačne namene od prvotnih, so prav tako omejene le na posameznih področjih. Na področju poročil o potrošnikih za namen ocene kreditne sposobnosti imajo posamezniki npr. pravico, da oporekajo nadaljnjemu deljenju svojih podatkov in uporabi zbranih podatkov za namen neposrednega trženja. Zakonodaja v ZDA načeloma ne pozna omejitev nadaljnje uporabe osebnih podatkov za druge namene, vendar pa imajo organizacije obdelavo osebnih podatkov načeloma opisano v izjavah o zasebnosti. Če bi podatke obdelovale za namene, ki

niso opisani in za to ne bi pridobile soglasja posameznikov, bi tako dejanje načeloma pomenilo zavajajočo poslovno prakso glede na zvezne in državne zakone (Sotto in Simpson, 2014, str. 211).

Na zvezni ravni obveščanje posameznikov o obdelavi osebnih podatkov zapovedujejo le že omenjeni področni zakoni, ne pa tudi splošna zakonodaja, ki bi veljala za vse organizacije. Zakon o varovanju zasebnosti otrok na spletu (*Children's Online Privacy Protection Act* – COPPA) na primer obvezuje ponudnike storitev na spletu, ki so usmerjeni k otrokom, mlajšim od 13 let, in ki vede zbirajo njihove osebne podatke, da na svoji spletni strani objavijo izčrpno obvestilo o varovanju zasebnosti, ki mora vključevati informacije o tem, kateri osebni podatki se obdelujejo, kako bodo uporabljeni ter kdaj so lahko razkriti tretjim osebam, in glede možnosti staršev, da pregledajo informacije, zbrane od otroka, ter zahtevajo prenehanje nadaljnjega zbiranja. V večini primerov mora organizacija, ki zbere podatke od otroka, o tem neposredno obvestiti tudi starše in od njih pridobiti soglasje (Sotto in Simpson, 2014, str. 210). Zakon o prenosljivosti zdravstvenega zavarovanja in odgovornosti (*Health Insurance Portability and Accountability Act* – HIPAA) pa zahteva, da organizacije, ki posedujejo zdravstvene podatke, posameznika obvestijo o varovanju zasebnosti. Zakon določa dopustne rabe in primere posredovanja zdravstvenih informacij, pravice posameznika in kako jih lahko uveljavlja, obveznosti organizacije glede zdravstvenih podatkov in obveznost posredovanja kontaktnih informacij za posameznike, ki bi se želeli pritožiti (Sotto in Simpson, 2014, str. 210).

Na tem področju piškotkov in podobnih tehnologij, še zlasti v kontekstu vedenjskega oglaševanja, so v zadnjem času vzniknile številne pobude za formalno regulacijo in predlagani številni zakoni, vendar nobeden ni bil sprejet. Tudi FTC je izdala že številna priporočila glede vedenjskega oglaševanja, panoga pa se je odzvala s kodeksi samoregulacije. FTC je prav tako obravnavala že številne primere, povezane z uporabo piškotkov, vendar so očitane nepravilnosti vezane na splošno določbo o nepoštenih in zavajajočih praksah (Sotto in Simpson, 2014, str. 214).

5.2.2 Nadzor na področju varovanja osebnih podatkov

Nadzor nad spoštovanjem zakonodaje glede varstva osebnih podatkov v ZDA izvajajo zvezni nadzorni organi in nadzorni organi zveznih držav, v številnih državah pa lahko posamezniki svoje pravice uveljavljajo v pravdnih postopkih (zasebne tožbe, lahko tudi skupinske) zoper organizacije, ki naj bi kršile zakonodajo. Na ravni ZDA ni enotnega regulatorja ali nadzornega organa, ki bi bdel nad spoštovanjem zakonodaje glede varstva osebnih podatkov. Na zvezni ravni je nadzorni organ odvisen od področja. Na področju finančnih storitev je to Urad za varovanje potrošnikov na finančnem področju (*Consumer Financial Protection Bureau*), na področju zdravstvenih podatkov je to *Department of Health and Human Services*. Onkraj specifičnih reguliranih področij na zvezni ravni nad področjem varstva osebnih podatkov bdi Zvezna komisija za trgovino (*Federal Trade Commission* – FTC). Zakon o FTC splošno pokriva varstvo potrošnikov in prepoveduje »nepoštena ali zavajajoča dejanja in prakse pri poslovanju ali ki zadevajo poslovanje« (5. razdelek Zakona o FTC). To je glavno orodje FTC pri izvajanju nadzora na področju varstva zasebnosti. Na tej podlagi je FTC zoper številna podjetja vodila postopke nadzora zaradi različnih dejanj v zvezi z obdelavo osebnih podatkov, ki naj bi bila »zavajajoča« ali »nepoštena«. Ti nadzorni postopki so se običajno končali z dogovorom, ki je podjetju prepovedoval nadaljevanje spornega početja, in pogosto zahteval dopustitev revizije svojega delovanja enkrat na dve leti, za obdobje do 20 let. V primeru kršitve takega dogovora ima FTC možnost, da organizacijo oglobi. Na zvezni ravni imajo možnost izvajanja nadzora zaradi nepoštenih ali zavajajočih poslovnih praks in kršitev zakonodaje zveznih držav tudi državni tožilci (Sotto in Simpson, 2014, str. 208).

FTC naj bi v zadnjih letih razširila svojo razlago prepovedi zavajajočih praks ne le na napačne izjave podjetij, ampak tudi na pomanjkljive izjave, torej na primere, ko podjetje ne poda informacij o potencialno spornih praksah, ki bi lahko vplivale na zasebnost. Tako naj bi spodbujala odgovornost podjetij za svoje delovanje na področju zasebnosti in ustvarjala transparenten trg za osebne podatke, saj morajo imeti posamezniki moč, da na podlagi informacij ocenijo različne vidike varstva svoje zasebnosti in nadzora nad informacijami o sebi. Kljub nizkemu pragu za začetek nadzornega postopka, ki je torej omejen predvsem na to, da podjetja posameznikom ne smejo lagati, pa nekateri v FTC menijo, da bi se morala FTC zaradi zavajanja zoper podjetje odzvati le, če bi prej ugotovila tudi obstoj škode za potrošnika zaradi te konkretne prakse podjetja, pri čemer bi morala biti taka škoda konkretna in vidna.

Prav tako naj bi pred začetkom postopka zaradi zavajanja preučili pozitivne plati obdelave osebnih podatkov, torej izvedli analizo stroškov in koristi, tako kot v primerih zoper domnevno nepoštene poslovne prakse. Zagovorniki zasebnosti svarijo, da bi taka razlaga pomenila nižanje standardov varstva potrošnikov, saj je prizadetost posameznika zaradi npr. razkritja podatkov lahko subjektivna in je ne bi smela presojati FTC, temveč bi morala poskrbeti, da so posamezniki dobro seznanjeni s praksami obdelave osebnih podatkov in se lahko sami informirano odločijo, kaj posamezna praksa za njih pomeni (Brookman, 2015).

Samoregulacija

Poleg zakonodaje na precej področjih obstaja tudi samoregulacija, ob čemer posamezna panoga izdela nezavezujoče smernice ali dobre prakse. Samoregulacija naj bi bila najboljši način za zagotavljanje zasebnosti uporabnikov spleta, ne da bi z zakonodajnimi ukrepi dušili razvoj panoge. Samoregulacija prevladuje predvsem na področju neposrednega trženja. Združenje za neposredno trženje (*Direct Marketing Association*) na primer od članov zahteva, da na vidnem mestu objavijo obvestilo potrošnikom o svojih praksah zbiranja informacij. Prav tako obstajajo zasebne certifikacijske sheme, kot je npr. TRUSTe, neprofitna pobuda, ki jo financirajo npr. Microsoft, Compaq, IBM in AT&T ter ki izdaja certifikate – značke organizacijam, ki delujejo v skladu s svojimi izjavami o zasebnosti (Cunningham, 2015).

Relevantna praksa FTC na področju vedenjskega oglaševanja

Regulator je kljub formalnim omejitvam pri ukrepanju zoper subjekte, ki kršijo zasebnost in varstvo osebnih podatkov uporabnikov elektronskih komunikacij, na področju praks vedenjskega oglaševanja že izdal številne odločitve oziroma se s kršitelji glede na postopkovna pravila pogodil – jim pri tem naložil ukrepe, ki jih morajo izvesti, in denarno kazen, ki jo morajo poravnati, npr.:

- oglaševalski mreži za mobilne platforme InMobi (leta 2016), ki je sledila stotinam milijonom lokacij uporabnikov (tudi otrok) brez njihove privolitve, oziroma ob zavajajočem pojasnilu, da upoštevajo nastavitve glede deljenja lokacije, ki so jo uporabniki nastavili na napravi (FTC, 2016a);
- podjetju Turn (2016), ki je sledilo milijonom potrošnikov na spletu in prek mobilnih aplikacij, čeprav so imeli v brskalniku vklopljene nastavitve omejevanja ali blokiranja piškotkov tretjih strank (FTC, 2016b);

- podjetju Compete (2012), ki ponuja analitične storitve s pomočjo sledenja uporabnikom na spletu. Podjetje milijonom uporabnikov ni ustrezno razkrilo, kakšen obseg osebnih podatkov se pri tem obdeluje (FTC, 2012);
- podjetju Nomi (2015), ki trgovcem ponuja storitev sledenja posameznikom v njihovih trgovinah, s pomočjo sledenja njihovim mobilnim napravam, in sicer za izdelavo analitičnih poročil o vzorcih gibanja. Čeprav je podjetje trdilo, da je *opt out* omogočen na njihovi spletni strani in v trgovinah, v slednjih to ni bilo mogoče – to je bil tudi razlog za ukrep regulatorja (FTC, 2015);
- podjetju Vizio (2015), ki je prek pametnih televizijskih sprejemnikov zbiral podatke o gledanosti milijonov uporabnikov in jih prodajalo oglaševalcem ter tretjim stranem brez soglasja (Fair, 2017).

Zanimiva je tudi poravnava z Googlom na področju konkurenčnega prava. Google se je med drugim moral strinjati, da tekmecev ne bo omejeval pri dostopu do nekaterih patentov, kritičnih za izdelavo pametnih telefonov in tabličnih naprav ter igralnih konzol in da bo oglaševalcem nudil več prožnosti za hkratno urejanje oglaševalskih kampanj na platformi AdWords in konkurenčnih platformah (FTC, 2013).

5.2.3 Razvoj zakonodaje, ki bi poenotila pravila o varstvu osebnih podatkov

Zadnja leta so zaznamovana z različnimi pobudami in poročili (tudi regulatorja FTC) o nezadovoljivih razmerah na področju varstva zasebnosti uporabnikov spleta v ZDA ter zgodbami o razkritjih osebnih podatkov posameznikov zaradi vdora v sisteme velikih ponudnikov storitev (Sotto in Simpson, 2014) in neprimernem ravnanju s podatki uporabnikov. Razprave so dosegle vrh ob zadnjem škandalu s Facebookom in Cambridge Analytico, ki je nakazal, kako velik je potencial uporabniških podatkov, celo pri vplivu na predsedniške volitve (Confessore, 2018).

V ZDA je bilo v zadnjem desetletju pripravljenih več predlogov zakonodaje, ki bi na zvezni ravni enotno urejala vprašanja varstva osebnih podatkov, predvsem uporabnikov spletnih storitev, vendar so vse spodletele (Cunningham, 2015; Singer, 2016), med zadnjimi je bil predlog administracije takratnega ameriškega predsednika Baracka Obame *Consumer Data Privacy Bill* (Singer, 2015). Razlogi so predvsem pomanjkanje politične volje za strožjo

regulacijo cvetoče podatkovne panoge ter politična in finančna moč najuspešnejših igralcev – vedno so blizu visoke politike in poskrbijo za svoje interese (Confessore, 2018; Glaser, 2018). Kot kažejo ugotovitve v primeru Cambridge Analytice, pa je tudi visoka politika zelo zainteresirana za sodelovanje s podatkovnimi veljaki, saj ji to v politični tekmi prinaša otipljive prednosti (Cadwalladr, 2017).

Ne glede na neuspehe na zvezni ravni so posamezne zvezne države začele sprejemati lastne zakonodaje, ki bolj ali manj strogo urejajo dele vprašanj zasebnosti uporabnikov spleta, vendar pa je uspeh take zakonodaje predvsem vezan na ozemlje posamezne države. Ena najambicioznejših zveznih držav je Kalifornija, ki je denimo sprejela zakonodajo, ki daje mladoletnim na voljo pravico do pozabe. Starši in mladi imajo pravico zahtevati izbris osebnih podatkov, ki jih o njih obdelujejo tretje stranke (Cunningham, 2015, str. 425). Junija 2018 je sprejela tudi eno najstrožjih in najbolj celostnih zakonodaj o zasebnosti uporabnikov digitalnih storitev v ZDA, in sicer Zakon o zasebnosti kalifornijskih potrošnikov (*California Consumer Privacy Act* – CCPA), ki je nastal po močnih pritiskih aktivista za zasebnost (Alastair Mactaggart), ki mu je uspelo mobilizirati strokovnjake za zasebnost, javnost in politične sile v Kaliforniji ter se upreti velikim tehnološkim podjetjem in doseči sprejem tega zakona (Confessore, 2018).

Kalifornijski zakon o zasebnosti potrošnikov deloma sledi vzoru Uredbe 2016/679, vendar velja le za tiste upravljavce osebnih podatkov, ki obdelujejo podatke velikega števila posameznikov, tj. prodajajo podatke najmanj 50.000 potrošnikov, oziroma imajo dovolj visoke letne prihodke (najmanj 25 milijonov ameriških dolarjev), delujejo v Kaliforniji in so profitne narave. Opredelitev osebnega podatka je široka in vključuje tudi podatke, ki so posameznikom pripisani in izpeljani iz osnovnih podatkov. Zakon daje potrošnikom (1.) možnost zahtevati od podjetij pojasnilo, kateri njihovi podatki se obdelujejo in prodajajo, (2.) pravico, da od podjetij zahtevajo prenehanje prodajanja njihovih podatkov; hkrati tudi (3.) ustvarja strožje standarde za varstvo osebnih podatkov. Ključne pravice potrošnikov po CCPA so (1.) pravica do obveščenosti o tem, kateri podatki se obdelujejo, (2) pravica do izbrisa podatkov, (3) pravica zavrnitve prodaje podatkov in (4) pravica dostopa do enake storitve za enako ceno (z nekaterimi omejitvami). Sankcije so predvsem vezane na incidente razkritja osebnih podatkov potrošnikov in na neupoštevanje njihovih zahtev. Zakon ne

predpisuje dolžnosti pridobivanja soglasja od potrošnikov, temveč prinaša strožje omejitve za deljenje podatkov za komercialne namene (Rowntree, 2018).

Komentarji sicer poudarjajo, da z zakonom nihče ni popolnoma zadovoljen, panoga meni, da je prestrog, zagovorniki zasebnosti, da nima dovolj omejitev. Veljati bo začel leta 2020, do takrat pa še obstajajo možnosti dopolnil (Rowntree, 2018; Confessore, 2018). V luči Uredbe 2016/679, ki je začela veljati maja 2018 in ki naj bi se ji prilagodila tudi podjetja iz ZDA, ki poslujejo na trgu EU, ter kalifornijske zakonodaje, so se znova obudila prizadevanja tudi na zvezni ravni. Administracija predsednika Donalda Trumpa je namreč poleti 2018 sporočila, da začenja pogovore z deležniki glede skupnih temeljnih načel za varovanje zasebnosti potrošnikov, ki bodo primerno uravnotežila interese potrošnikov in napredek (Shepardson, 2018). Oglaševalska panoga je spremenila argumente iz »proti regulaciji« h »kakšna naj bo« in pojavljajo se že proaktivni predlogi za okvir prihodnje regulacije (Google, 2018). Kritiki poudarjajo, da je te predloge in izjave treba obravnavati z vidika izogibanja strogim zahtevam kalifornijskega zakona in Uredbe 2016/679 tako, da bi zvezna zakonodaja določala nižje standarde (Glaser, 2018).

Če povzamemo, se pravni okvir za varstvo osebnih podatkov in zasebnosti posameznikov v vedenjskem oglaševanju v ZDA zelo razlikuje od evropskega. Zakonodaja v ZDA ne pozna posebnih omejitev za obdelavo osebnih podatkov na zvezni ravni, se pa čedalje bolj razvija na ravni posameznih zveznih držav, najbolj ambiciozno trenutno v Kaliforniji. Na zvezni ravni je obdelava osebnih podatkov regulirana le sektorsko, npr. podatki za ustvarjanje ocen kreditne sposobnosti, podatki otrok, zdravstveni podatki itd. Najpomembnejši regulator je FTC – ki je tudi zelo proaktiven v smislu objave mnenj in stališč, ki zadevajo področja vedenjskega oglaševanja (npr. o preprodajalcih podatkov, sledenju prek različnih naprav, pametnih televizijskih sprejemnikov itd.). Na tem področju ima omejena pooblastila za nadzor, in sicer le glede zavajajočih in nepoštenih praks, kar presoja predvsem z vidika informacij, ki jih podjetja zagotovijo javnosti, prek politik zasebnosti, saj vsebinskih omejitev glede obdelave podatkov ameriški pravni sistem ne pozna. Kljub temu je že več podjetjem izrekel ukrepe zaradi obširnih praks sledenja potrošnikom na različnih napravah, vendar pa so ti ukrepi zadevali zlasti boljše obveščanje o praksah sledenja, niso pa omejili sledenja samega. Zadnji škandali v zvezi z vdori v podatke nekaterih največjih spletnih ponudnikov storitev (npr. Facebook – več v poglavju 2) ter vpletanja v ameriške predsedniške volitve so znižali

zaupanje potrošnikov v ponudnike digitalnih storitev in trenutno se kažejo novi poskusi oblikovanja enotnih standardov za varovanje zasebnosti potrošnikov na ravni celotnih ZDA.

5.3 Samoregulacija

Da je zakonodaja potrebna, ne pa zadostna za urejanje področja zasebnosti, menita Bennett in Mulligan (2012), ki napotujeta na druge instrumente, s katerimi je mogoče vplivati na tem področju, kot so kodeksi, ocene vplivov na zasebnost, standardi glede zasebnosti, pečati zasebnosti in drugi instrumenti, ki so v oporo in podporo zakonodaji (Bennett in Mulligan, 2012). Razlogi za odmikanje od izključne strategije pravil in nadzora na področju varstva osebnih podatkov k samoregulacijskim orodjem so v učinkovitosti samoregulacije pri tehnološko specifičnih vprašanjih in ukrepih, ki jih zakonodaja težko določi, deloma zato, ker je zakonodajni postopek dolg in bi specifične tehnološke rešitve v nekaj letih že zastarale, deloma pa tudi zaradi specialističnih znanj, ki jih ima za razvijanje tehnoloških rešitev predvsem zadevna panoga. Zakonodaja na področju varstva osebnih podatkov je tehnološko nevtralna, prav zato pa ji umanjka natančnejših specifikacij, kako zagotoviti skladnost z nekaterimi določbami, npr. kakšno je učinkovito zavarovanje osebnih podatkov (Kamara, 2017). Različni avtorji poudarjajo pomen in koristi koregulacije, kjer je strategija pravil in nadzora dopolnjena oz. soobstaja s samoregulacijskimi ukrepi, pri čemer zakonodaja določa temeljna pravila ter opredeljuje nadzor, samoregulacijski mehanizmi pa poskrbijo za izvedbeni del določanja specifičnih pravil za skladnost z določbami, posebej ko gre za tehnična vprašanja (Baldwin in Cave, 1999; Kamara, 2017; Weber, 2010). Tudi Uredba 2016/679 po novem spodbuja uporabo kodeksov, certifikacijskih mehanizmov, ocen vpliva na varstvo osebnih podatkov in tehničnih standardov za doseganje skladnosti s pravili in preglednost (Uredba 2016/679, členi 40, 42, 43, 20 in 25).

5.3.1 Samoregulacijski kodeksi

Začetki samoregulacije na področju vedenjskega oglaševanja segajo v leto 2010, ko je bil v ZDA predstavljen prvi kodeks, ki ga je pripravila koalicija marketinških združenj.[64] Kodeks je nastal kot odziv na pobudo regulatorja FTC in Network Advertising Initiative (NAI), ki sta se na čedalje večje skrbi glede varstva posameznikov na spletu odzvala z osnutkom samoregulacijskega kodeksa, v katerem sta pozvala oglaševalsko panogo k opredelitvi načel, ki bi jih pri vedenjskem oglaševanju morala spoštovati (FTC, 2007; NAI, 2008).

Načela za izvajanje vedenjskega oglaševanja, poudarjena v kodeksu in pripadajočem vodniku za implementacijo, naj bi poskrbela za varstvo osebnih podatkov potrošnikov, vendar hkrati ohranila inovativno oglaševanje, ki podpira velik del brezplačne vsebine na spletu in omogoča dostavo relevantnih oglasov:

1. *načelo izobraževanja* spodbuja organizacije k izobraževanju posameznikov in podjetij o vedenjskem oglaševanju;
2. *načelo preglednosti* zahteva jasna in lahko dostopna pojasnila o zbiranju podatkov;
3. *načelo uporabnikovega nadzora* uporabnikom prinaša razširjene možnosti nadzora nad tem, ali se podatki zbirajo in uporabljajo za vedenjsko oglaševanje. Izbiro lahko izvedejo z obiskom povezave, ki je objavljena na mestu, kjer se podatki zbirajo. Ponudniki dostopa do omrežja bi morali pridobiti privolitev, preden izvajajo vedenjsko oglaševanje, in izvesti deidentifikacijo podatkov, uporabljenih za tak namen;
4. *načelo zavarovanja podatkov* in omejenega roka hrambe takih podatkov;
5. *načelo materialnih sprememb* načel pomeni, da bi morali potrošniki privoliti, preden pride pri obdelavi njihovih podatkov do materialnih sprememb;
6. *načelo občutljivih podatkov* se nanaša na podatke otrok, in napotuje na privolitev staršev, če so podatki otrok uporabljani za vedenjsko oglaševanje;
7. *načelo odgovornosti* napotuje na razvoj programov za upoštevanje teh načel, vključno s programi za nadzor in poročanje nespoštovanja nadzornim organom (American Association of Advertising Agencies, Association of National Advertisers, Direct

[64] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, Council of Better Business Bureaus.

Marketing Association, Interactive Advertising Bureau, Council of Better Business Bureaus, 2010a in b).

Kljub omejeni učinkovitosti kodeksa pri varovanju pravic potrošnikov so tudi pozneje v ZDA prevladovale zamisli in pobude, ki bi boljše varstvo potrošnikov uresničevale na temelju samoregulativnih ukrepov, ki pa bi morda imeli zunanji nadzor. FTC se je tako osredinila na tehnični mehanizem ne sledi in vgrajevanje zasebnosti prijaznih rešitev ter praks (FTC, 2010), zvezno Ministrstvo za trgovino pa je kot rešitev predlagalo obširno uresničevanje načel poštenih informacij – *Fair Information Practice Principles*, vendar ne v smislu zakonodajnih obveznosti, temveč bi poseben oddelek pomagal pri razvijanju prostovoljnih kodeksov v postopku z več deležniki. Prožnejša samoregulacija naj bi bila boljša za izzive prihodnosti, pri tem pa naj bi bilo najpomembneje izobraževati potrošnike, da se bodo lahko sami odločili, kakšno ciljanje je zanje sprejemljivo (Department of Commerce, 2010b). Nevladni sektor se je na tak proces odzval, češ da bi šlo za političen proces, ki bi vodil le k splošnim načelom, ki jih je težko udejanjiti, ter da je splošna težava prostovoljnih kodeksov pomanjkljiv nadzor (Tien, 2010). Prav tako je vprašljivo, koliko je lahko učinkovito izobraževanje potrošnikov, zlasti ob tehnično zahtevnih invazivnih praksah sledenja in vedenjskega oglaševanja. Kot izhaja iz poglavja 5.2, v ZDA politične volje za sprejem celostnejših pravil, morda celo zvezne zakonodaje, ki bi bolje varovala interese potrošnikov, še ni.

V EU je bila leta 2009 kot odgovor na izzive vedenjskega oglaševanja in sledenja sprejeta strožja zakonodaja, ki je zahtevala privolitev v piškotke in podobne tehnologije. Evropska oglaševalska panoga je izrazila nestrinjanje s tako strogimi pravili, ki naj ne bi upoštevala, da potrošniki podpirajo vedenjsko oglaševanje in menjavo vrednosti, saj lahko zato brezplačno dostopajo do visokokakovostnih vsebin. Stroga zakonodaja naj bi pomenila velike izgube za panogo, ki bi negativno vplivale na rast digitalne ekonomije in ogrozile doseganje ciljev Digitalne agende, zato je panoga podprla urejanje s samoregulacijo (WFA, 2010; IAB Europe, 2010a; EACA, 2010), podobno tisti v ZDA, ki naj zagotavljala dobre rezultate (GPA, 2010). Da je samoregulacija lahko primerna in realistična rešitev, ki bi okrepila zaupanje posameznikov, vendar ne bi hkrati tudi škodovala napredku digitalne panoge, je poudarila tudi takratna evropska komisarka, odgovorna za digitalno agendo, in panogo pozvala k razvoju kodeksa, ki pa bi moral biti skladen z evropskimi pravili, temeljiti na preglednosti,

privolitvi, uporabniku prijaznih rešitvah, če je mogoče, na ravni brskalnikov, in učinkovitem nadzoru (Kroes, 2010).

Leta 2011 je bila javnosti predstavljana samoregulacijska rešitev *European Advertising Standards Alliance (EASA) Best Practice Recommendation on Online Behavioural Advertising*.[65] Temelj kodeksa je učinkovito obveščanje posameznikov, tudi prek posebne spletne strani http://www.youronlinechoices.com/, ki deluje v vseh uradnih jezikih EU in poleg informacij o vedenjskem oglaševanju posameznikom zagotavlja tudi možnost zavrnitve obdelave osebnih podatkov za namen vedenjskega oglaševanja v celoti ali pa zavrnitve takih praks le posameznih ponudnikov, oglaševalskih mrež ipd. Vključeno je pojasnilo, da zavrnitev vedenjskega oglaševanja ne pomeni, da ni obdelave podatkov posameznika, ampak le, da bo prejemal oglase, ki mu ne bodo prilagojeni (EASA 2011).

V državah članicah EU lahko ustreznost samoregulacijskih kodeksov potrdijo nadzorni organi za varstvo osebnih podatkov (Uredba 2016/679, člena 40 in 41), v času veljavnosti prejšnje direktive pa je ustreznost kodeksov potrjevala Delovna skupina iz člena 29, kot v primeru kodeksa FEDMA za neposredno trženje (FEDMA, 2010). Kodeksa EASA/IAB delovna skupina ni prejela v uraden postopek ocene, je pa na lastno pobudo z vidika zagotavljanja poštenih informacij javnosti in da bi se izognili potencialnemu zavajanju panoge, da skladnost s kodeksom pomeni skladnost z zakonodajo, objavila mnenje o nekaterih ključnih vidikih predlaganega samoregulacijskega okvira. Tako je opozorila, da spoštovanje določb kodeksa EASA/IAB in sodelovanje pri spletni strani www.youronlinechoices.eu ne pomeni skladnosti z Direktivo 2002/58/ES o zasebnosti in elektronskih komunikacijah. Kodeks naj bi ustvarjal napačen vtis, da lahko uporabnik izbere možnost, da mu subjekti med brskanjem po spletu ne sledijo. To je lahko negativno tako za posameznike kot tudi za panogo, ki je lahko zavedena, da spoštovanje kodeksa pomeni tudi spoštovanja zakonskih zahtev. Delovna skupina iz člena 29 je v svojem mnenju tudi poudarila načine, kako bi lahko rešitve, ki so bile predlagane v kodeksu za naknadno zavrnitev, lahko preprosto prilagodili in jih uporabili za pridobivanje predhodne privolitve glede uporabe piškotkov in podobne tehnologije. Tako bi kodeks lahko omogočal skladnost s pravili Direktive 2002/58/ES. Dodatno je poudarila, da možnosti obveščanja, ki jih kodeks predvideva in temeljijo predvsem na ikoni ob oglasu, na katero

[65] EASA je evropska oglaševalska samoregulacijska zveza, ki združuje lokalne organe samoregulacije iz držav članic (tudi Slovensko oglaševalsko zbornico) ter panožna združenja, med njimi IAB (*Interactive Advertising Bureau*).

lahko klikne uporabnik, ki želi več informacij, same po sebi niso dovolj informativne, saj jih uporabniki glede na trenutno stanje na trgu ne bodo prepoznali (WP29, 2011).

Kodeks je bil leta 2016 posodobljen. Njegovi avtorji poudarjajo, da naj bi bil pristop tehnološko nevtralen in je zato primeren za vse naprave, ki se povezujejo na splet, ne le za spletno vedenjsko oglaševanje, kot ga uporabnik prejema pri klasičnem brskanju na računalniku, ampak tudi za mobilne naprave. Bistvo pristopa je standardizacija obveščanja posameznikov glede vedenjskega oglaševanja pri digitalnem oglaševanju (tudi video) na spletu in pri mobilnih aplikacijah. Ti mehanizmi naj bi uporabniku prav tako omogočili preprost pritožbeni postopek glede neskladnega ravnanja. Priporočila se nanašajo na vedenjsko oglaševanje, vendar izključujejo aktivnosti, ki jih spletne strani ali ponudnik aplikacij izvajajo le znotraj svoje domene ali aplikacije, dostavo oglasov ali statistike oglaševanja in kontekstualno oglaševanje. Namenjen je izvajalcem vedenjskega oglaševanja, ki so tretje stranke (EASA, 2016).

Priporočila dobrih praks za vedenjsko oglaševanje EASA opredeljujejo glavna načela (obvestilo, uporabnikova izbira, razčlenjenost glede na občutljive podatke, skladnost in nadzor, pregled),[66] ki izhajajo iz vključenega podrobnejšega okvira IAB za vedenjsko oglaševanje. Del priporočil so tudi načela IAB za vedenjsko oglaševanje v mobilnem okolju ter tehnične specifikacije za izvedbo rešitev, podrobnejše smernice glede nadzora nad skladnostjo s pravili in navodila glede samocertificiranja skladnosti (EASA, 2016).

Ob zadnji reviziji okvira leta 2016 je bil dodan še del za uporabo v mobilnem okolju. Pametni telefoni in tablične naprave so oglaševalski panogi omogočili, da s potrošniki komunicira na nove načine, s čedalje bolj prilagojenimi in ustreznimi sporočili. V središču tega razvoja so podatki, ki poganjajo inovacije in oglaševalski panogi omogočajo, da še naprej ustvarja digitalne vsebine, storitve in aplikacije, ki so uporabnikom na voljo brezplačno. Oglaševalska panoga mora zato s podatki z mobilnih naprav ravnati odgovorno, kar predvsem pomeni preglednost oglaševalskih praks. Za mobilno okolje je posebej značilno, da so naprave »vedno vklopljene«, prenosljive in z dostopom do mobilnega interneta skoraj kjerkoli, ekrani so majhni in uporabnik običajno izvaja nadzor z dotiki ekrana – zato so tudi pričakovanja glede uporabnosti drugačna. Tudi nekatere tehnologije za dostavo oglasov se razlikujejo od

[66] Podrobneje v Prilogi S.

običajnega računalniškega okolja. V zvezi s tem opredelitve posebej pojasnjujejo izraze *cross-app* podatki (podatki o različnih aplikacijah, zbrani z uporabnikove naprave za namen vedenjskega oglaševanja), podatki o lokaciji naprave (lahko vključujejo podatke, pridobljene iz baznih postaj, WiFi, GPS ali podatke na podlagi Bluetooth tehnologije), podatki uporabnika naprave (npr. koledar, imenik, fotografije, videi, dnevniki klicev, sporočil – podatki ki niso ustvarjeni s strani ponudnika aplikacije). Načela so posebej prilagojena tem specifikam in npr. določajo, da mora biti obvestilu o uporabi teh specifičnih vrst podatkov na voljo tudi pred namestitvijo aplikacije in v aplikaciji (EASA, 2016, str. 22–27).

Težava kodeksa je, da ne zagotavlja osnovne skladnosti z novimi pravili v zakonodaji, ki zahtevajo predhodno soglasje za obdelavo osebnih podatkov za namen vedenjskega oglaševanja. Prav tako mehanizem za nadzor nad skladnostjo ne predvideva nobenega zunanjega posega. Samoregulacijski okvir pa ponuja izboljšave na področju ozaveščanja posameznikov o vedenjskem oglaševanju in jim daje možnost, da tako obdelavo podatkov zavrnejo (Burnik, 2011a, str. 298–299). Kritike letijo na kodeks tudi z vidika dopolnitev in skladnosti v kontekstu določb Uredbe 2016/679. Čeprav kodeks vsebuje zagotovila, da imajo izdajatelji nadzor nad tem, kdo so njihovi partnerji in za koga pridobijo privolitev svojih uporabnikov, Ryan (2018) opozarja, da dokumenti IAB kažejo, da se *ad tech* panoga, ki je kodeksu zavezana, lahko prosto odloča, da deli podatke, ki jih je pridobila na izdajateljevi spleti strani, s tretjimi strankami. Ko podatki pridejo v sistem RTB (*real time bidding*), ni več nadzora nad njimi, saj kodeks določa, da se ponudniki oglaševalskih storitev lahko odločijo, da osebnih podatkov ne posredujejo tistim nadaljnjim ponudnikom, ki nimajo soglasja posameznikov, vendar pa to ni nujno. Z ekonomskega vidika pa je podjetjem pomembno, da podatke delijo s čim širšim krogom nadaljnjih ponudnikov in preprodajalcev podatkov. Izdajatelji, ki zaupajo ponudnikom storitev, ki zatrjujejo skladnost z IAB kodeksom, se izpostavijo tveganju deljenja podatkov o svojih obiskovalcev s tisoči *ad tech* podjetij. IAB prav tako priporoča, da izdajatelji pridobijo vse privolitve – za uporabo podatkov za svoje namene in za namene tretjih strani – enotno, hkrati pa Uredba 2016/679 zahteva granularnost privolitve za različne namene (Ryan, 2018).

Kot poudarjata Baldwin in Cave (1999), so prednosti samoregulacije zlasti v njeni strokovnosti in učinkovitosti. Samoregulacijski organi, ki jih sestavljajo pripadniki panoge, imajo visoko raven strokovnega znanja, pravila, ki jih postavijo, pa so teoretično bolj

uresničljiva. To pripomore k učinkovitosti take regulacije, saj je prožnejša kot zakonodaja. Na drugi strani pa ima samoregulacija težave na področju odgovornosti in pravičnosti postopkov. Ker panoga regulira samo sebe, težko govorimo o pravi odgovornosti (saj je ta le do same sebe), razen če ima kak element zunanjega nadzora, npr. zunanje potrjevanje pravil s strani drugih organov, nadzor nadzornih organov, sodna presoja ali mehanizem za obravnavo pritožb. Priporočljivo je tudi, da vključuje predstavnike potrošnikov in drugih deležnikov ter primerne sankcije za nespoštovanje. Ker običajno zavezuje le pristopnike, je lahko na trgu veliko subjektov, ki jih pravila ne vežejo (Baldwin and Cave, 1999).

Samoregulacija se v okolju interneta pogosto poudarja kot učinkovita, ker je prožna in tako lažje prilagodljiva hitremu napredku tehnologij in praks. Tudi na širšem področju oglaševanja ima samoregulacija pomembno vlogo. Vprašanje pa je, ali je lahko kot primarno orodje regulacije učinkovita tudi na področju vedenjskega oglaševanja. Ta panoga se namreč razvija zelo hitro, standardi pa še niso jasni. Ker je samoregulacija po inerciji ujeta v panožne interese, je v takih okoliščinah težko pričakovati, da se bo panoga učinkovito samoomejevala in si predpisovala pravila, ki jo bodo zelo omejila. Tudi koncentracija moči na trgu ponudnikov digitalnega oglaševanja je dejavnik, zaradi katerega samoregulaciji umanjka verodostojnost (Burnik, 2011a, str. 301–302). Kot izhaja iz zgodnjih izkušenj urejanja področja vedenjskega oglaševanja s pomočjo samoregulacije v ZDA in tudi v EU, ta ne varuje učinkovito pravic uporabnikov elektronskih komunikacij, saj postavlja prenizke standarde in ne zahteva uporabnikove privolitve v sledenje (Burnik, 2011a, str. 304).

Predstavljen kodeks za vedenjsko oglaševanje je, kot so poudarili nadzorni organi, sicer dobrodošlo orodje za krepitev zavedanja in obveščanja o praksah vedenjskega oglaševanja, ne ponuja pa skladnosti z evropsko zakonodajo, v smislu zagotavljanja vnaprejšnje privolitve uporabnikov v vedenjsko oglaševanje, kar je njegova glavna pomanjkljivost (WP29, 2011). Prispevek kodeksa lahko opazimo tudi pri urejanju vedenjskega oglaševanja na mobilnih napravah, kjer so prakse raznolike, tehnologija pa se šele razvija. Zakonodaja se razvija dalj časa, na ravni samoregulacije pa je postavljanje pravil hitrejše. Tudi tukaj pa velja pomislek glede skladnosti z različno zakonodajo, ki ureja uporabo mobilnih naprav, ki je določbe kodeksa ne zagotavljajo, saj le za omejene primere podatkov zahtevajo pridobitev izrecne privolitve, npr. pri obdelavi občutljivih osebnih podatkov.

Po drugi strani zakonodaja v Evropi kljub svoji podrobnosti in dorečenosti nikakor ne more urejati vseh podrobnosti praks vedenjskega oglaševanja, in bi imel v prihodnosti samoregulacijski mehanizem lahko vlogo pri enotnejšem določanju tehničnih načinov in standardov za pridobivanje soglasja in obveščanje, seveda ob jasnejšem upoštevanju minimalnih zakonskih zahtev. Glede na to, da mnenja o tem, ali je za vse vedenjsko oglaševanje res potrebna privolitev, in glede na pritiske ob spremembah zakonodaje, da bi ta dovoljevala tudi drugačne pravne podlage, lahko kodeks EASA/IAB pridobi na veljavi tudi v obliki, ki ne temelji na pridobivanju vnaprejšnje privolitve. Prav tako bi kodeks lahko pripomogel na področjih, ki jih zakonodaja najbrž ne bo urejala – npr. pri pobudah za boljše obveščanje ali tehničnih standardih za enovito obveščanje.

Za učinkovito regulacijo področja vedenjskega oglaševanja bi bila tako koristna kombinacija pristopov zakonodaje in samoregulacije, v katerih zakonodaja določi enotne standarde, normo, samoregulacija pa izpolnjuje vlogo natančnejše določitve pristopov za skladnost s pravili, ki lahko zagotovijo boljše varstvo (Burnik, 2011a, str. 304).

5.3.1 Certificiranje in standardizacija

Certificiranje, pečati in znaki lahko podjetjem in organizacijam pomagajo tako pri doseganju skladnosti, v konkretnem primeru z zakonodajo s področja varstva osebnih podatkov in zasebnosti, kot tudi pri izkazovanju te skladnosti pred nadzornim organom v primeru nadzora. Njihova vloga je tudi v zagotavljanju preglednosti. Posamezniki lahko tako hitro presodijo, ali posamezen produkt ali storitev zagotavlja ustrezno raven varovanja njihovih pravic (ENISA, 2017, str. 5). Zato je certificiranje kot oblika samoregulacije, poleg drugih orodij odgovornosti upravljavcev osebnih podatkov (presoje vplivov na zasebnost, načelo vgrajene zasebnosti), lahko zelo koristno orodje tudi pri regulaciji vedenjskega oglaševanja (Burnik, 2011a, str. 303).

Certificiranje je proces, v katerem zaupanja vredna tretja stranka, ki ima potrebna znanja in sposobnosti (certifikacijsko telo) pregleda in oceni prakse posameznega podjetja ali organizacije in presodi, ali so skladne z vnaprej določenimi pravili in standardi. Ti lahko izhajajo iz zakonodaje (npr. certificiranje glede na določbe Uredbe 2016/679) ali pa izhajajo

iz drugačnega normativnega dokumenta, npr. mednarodnega standarda (kot so npr. standardi ISO). Če podjetje ali organizacija izpolnjuje zahteve, prejme potrdilo o skladnosti – certifikat. Običajno lahko nato uporablja ob svojih komunikacijah ali predstavitvah znak, pečat, ikono ali podobno vizualno orodje, ki označuje to skladnost. Certificiranje je lahko obvezno in ga zahteva zakonodaja ali pa prostovoljno, kot v primeru certificiranja na področju varstva osebnih podatkov (ENISA, 2017, str. 5).

Kot ugotavljata Burnik in Kamara (2017) na področju varovanja zasebnosti in osebnih podatkov, obstaja kar nekaj certifikacijskih pobud, ki so namenjene tako produktom kot tudi storitvam in procesom. Nekatere temeljijo na družini standardov ISO (npr. standard za računalništvo v oblaku ali za zavarovanje osebnih podatkov),[67] druge pa so vezane na izpolnjevanje zahtev, ki izhajajo iz zakonodaje, npr. EuroPrise ali certificiranje, ki ga izvaja francoski nadzorni organ za varstvo osebnih podatkov (za digitalne sefe, za tečaje s področja varstva osebnih podatkov in revizijske postopke). Razlikujejo se v postopku certificiranja pa tudi v pocertifikacijskih dejavnostih (npr. preverjanje skladnosti s certifikatom) (ENISA, 2017, str. 16–21, 32–43). Certificiranje je lahko zelo primerno v položajih, v katerih gre za izpolnjevanje zahtev tehničnih standardov, kjer je za oceno skladnosti potrebno specialistično znanje, ki ga certifikacijsko telo in njegovi laboratoriji imajo. Certificiranje pogosto pomeni tudi upoštevanje nekih višjih standardov, kot jih zahteva zakonodaja, in izkazuje angažiranost subjekta za njihovo doseganje. Poleg tega je to običajno plačljiv proces in zahteva precejšen vložek podjetja ali organizacije.

Certificiranje lahko zmanjša breme nadzornih organov in olajša nadzor ter hkrati poveča skladnost na trgu, če je del certifikacijskega mehanizma tudi ustrezen nadzor nad skladnostjo s certifikatom (Rodrigues in drugi, 2013, str. 12). Uredba 2016/679 certificiranje izrecno določa in za določene namene omogoča v 42. in 43. členu.[68] Certifikati na področju varovanja osebnih podatkov omogočajo posameznikom, da se hitreje seznanijo s politikami obdelave osebnih podatkov posameznega ponudnika, njegovimi praksami in spoštovanjem pravil. Nekatere sheme so celostno usmerjene (npr. že omenjeni EuroPrise, ki preverja skladnost z zakonodajo), druge pa so utemeljene na panožnih standardih, ki so lahko precej nizki (Rodrigues in drugi, 2013, str. 13).

[67] Npr. ISO/IEC 27001.
[68] Za podrobno analizo certificiranj v okviru Uredbe 2016/679 glej analizo Burnik in Kamara v ENISA, 2017.

Na področju vedenjskega oglaševanja trenutno ni specifične certifikacije, ki bi pokrila celotno dejavnost in ki bi bila na voljo vsem izvajalcem, vsaj ne v smislu neodvisnega preverjanja skladnosti s strani usposobljene tretje stranke. Deloma je certificiranje vpeto v že omenjen samoregulacijski kodeks EASA/IAB. Priporočila za dobre prakse predvidevajo samocertificiranje subjektov, ki smejo uporabljati ikono za označevanje vedenjskega oglaševanja, da ravnajo skladno s priporočili in zunanje preverjanje skladnosti s strani pooblaščenega revizorja (EASA 2016, 32). Pomanjkljivost te rešitve je, kot je bilo že poudarjeno, da trenutno v EU ne izpolnjuje minimalnih zakonskih zahtev. Izvajalci vedenjskega oglaševanja lahko za izkazovanje dobre prakse na posameznem področju, npr. pri zavarovanju osebnih podatkov, uporabijo tudi katerega od standardov ISO. Prav tako bi se lahko certificirali v okviru pečata EuroPrise.

Ker so prednosti certificiranja povezane tudi z njegovo učinkovitostjo na zelo specifičnih področjih, na katerih je potrebno specialistično, tudi tehnično znanje, certificiranje na področju vedenjskega oglaševanja vsekakor ponuja veliko možnosti, vendar le v primeru upoštevanja minimalnih zakonskih zahtev in če je shema za certificiranje vredna zaupanja, transparentna in utemeljena na zunanji neodvisni oceni skladnosti z ustreznim, prav tako zaupanja vrednim, standardom.

Priložnost za boljšo regulacijo vedenjskega oglaševanja ponujajo tudi tehnični standardi kot eno od orodij samoregulacije oz. koregulacije, ki podrobneje predpišejo način izpolnjevanja neke konkretne zakonske določbe v določenem kontekstu, sektorju ali panogi. Uredba 2016/679 denimo odpira različne tematike, pri katerih ni tehnično določenega načina, kako zagotoviti skladnost z določbami – med njimi glede vgrajene zasebnosti, pa tudi v primeru pravice posameznika do obveščenosti[69] in v primeru certifikacijskih mehanizmov.[70] To pomanjkanje določenosti tehničnih rešitev lahko pomagajo zapolniti tehnični standardi – normativni dokumenti, ki jih po določenem transparentnem postopku sprejme panoga za posamezna ozka področja. Postopek sprejema standarda je hitrejši in prožnejši ter omogoča vključitev specifičnih tehničnih znanj. Med najbolj znanimi lahko omenimo mednarodne standarde ISO (npr. za zavarovanje podatkov), v Evropi pa deluje tudi Evropsko standardizacijsko telo, ki sprejema evropske standarde (EN) in podobne normativne

[69] Uvodna izjava 60 omenja možnosti standardiziranih ikon za obveščanje.
[70] Deveti odstavek 43. člena omenja tehnične standarde za certifikacijske mehanizme.

dokumente dobre prakse.[71] Standardi so lahko tudi nacionalni in tako veljajo le v posamezni državi članici (npr. standardi nemške organizacije za standardizacijo DIN). Kot poudarja Kamara (2017), skladnost s standardi lahko olajša izvajanje nadzora (Kamara, 2017). Na področju vedenjskega oglaševanja je trenutno najbolj relevantna standardizacijska pobuda konzorcija W3C, ki že skoraj desetletje dela na standardu ne sledi. Ta bi se lahko razvil v primarno orodje za posameznikovo izbiro in nadzor nad obdelavo njegovih osebnih podatkov na spletu. Naslednje poglavje podrobneje predstavlja pomen standarda, proces njegovega ustvarjanja in posledice za ekosistem vedenjskega oglaševanja.

5.4 Standard ne sledi

Kot odziv na vseprisotno sledenje na spletu so nastala številna orodja, s katerimi uporabnik lahko npr. preprečuje prikazovanje oglasov (angl. *ad blockers*) oziroma si vzpostavi t. i. seznam za zaščito pred sledenjem (angl. *tracking protection lists*).[72] Obetajoče orodje naj bi bil tudi mehanizem ne sledi (angl. *Do Not Track* – DNT), ki naj bi uporabnikom dal možnost, da v svojem brskalniku izberejo možnost oddajanja signala ne sledi in bi tak signal prenesli vsaki spletni strani, ki jo obiščejo, ta pa bi morala signal spoštovati in podatkov o uporabniku ne zbirati in obdelovati (Electronic Frontier Foundation, 2016). Koncept ne sledi naj bi bil kombinacija tehničnega standarda in pripadajočih politik, poveznih z zakonodajo, ki bi nadzornim organom podelila pristojnosti za usmerjen nadzor (Jeschke, 2011).

Pobuda za razvoj mehanizma ne sledi prihaja iz ZDA. Ameriški regulator FTC jo je podprl že leta 2010, tudi kot odziv na čedalje bolj perečo problematiko sledenja na spletu, glede katerega uporabniki v ZDA nimajo primernega orodja za omejevanje, hkrati pa jim ameriška zakonodaja ni ponujala varstva v smislu, da bi sledilci morali pridobiti soglasje za sledenje.[73] Zamisel o standardu ne sledi se je zdela obetajoča za zagotavljanje možnosti naknadne zavrnitve sledenja, saj, kot je v svojih dokumentih poudarila FTC, uporabniki morajo imeti možnost izbire glede sledenja za namen prikazovanja osebno prilagojenih oglasov. FTC je

[71] Npr. CEN Workshop Agreement. Podrobneje o tem instrumentu v Golyardi in drugi (2017) in Tomšič in drugi (2017).
[72] Seznam vsebuje ažurno množico ponudnikov sledenja na spletu, uporabnik pa s prijavo svojega brskalnika na tak seznam blokira vzpostavljanje povezave med brskalnikom in ponudniki na seznamu, razen če uporabnik dejansko klikne na povezavo, ki vodi do enega od ponudnikov (npr. na njegov oglas). Glej npr. Microsoft's Internet Explorer 9 Tracking Protection Lists (Electronic Frontier Foundation, 2010).
[73] Da je sledenje postalo vroča tematika, je poskrbel odmevi eksperiment časopisne hiše Wall Street Journal, ki je objavila reportažo o sledilcih na spletu in razkrila globine ter obširnost sledenja za trženjske namene (The Wall Street Journal, 2016).

oglaševalski panogi priporočila razvoj mehanizma ne sledi, ki bi deloval na ravni brskalnika in bi uporabniku omogočil preprosto uveljavljanje svoje izbire, kot nasprotje temu, da mora svoje nestrinjanje s sledenjem izražati na ravni ponudnikov ali sektorjev (FTC, 2010). Leta 2012 je zamisel podprla tudi ameriška vlada (Brookman, 2014).

Standard ne sledi je leta 2011 začela razvijati Skupina za zaščito proti sledenju (angl. *Tracking Protection Working Group*) znotraj konzorcija W3C. W3C je organ, v katerem na prostovoljni ravni sodelujejo različni panožni deležniki iz in zagovorniki temeljnih načel ter pravic na spletu in razvijajo standarde, pomembne za delovanje spleta, ki nimajo pravne veljavnosti, ampak so prostovoljni. Postopek razvijanja standarda, ki je prepuščen panogi in zainteresiranim deležnikom brez vpletanja vlade ali regulatorja ter zakonodajnega nadzora naj bi pomenil, da bo nastali standard postal širše uveljavljen in bo v panogi spoštovan. Samoregulacija spleta in interneta s standardizacijo naj bi bila po mnenju nekaterih boljša alternativa kot regulatorni posegi nadnacionalnih teles, kot so Združeni narodi ali Mednarodna telekomunikacijska zveza, ali nacionalnih regulatorjev ali vladni posegi, saj naj bi standardi pomenili širok konsenz, ki temelji na vključevanju široke skupine deležnikov (Centre for Digital Technology, 2012). Po drugi strani pa kritiki poudarjajo, da imajo v skupini večino največji ponudniki spletnih storitev, kot so Adobe, Apple, Facebook, Google in Yahoo, tako da sprejeti standardi odražajo predvsem njihove interese (Campbell, 2014).

Razvoj standarda ne sledi je bil zelo težak in počasen. Temeljil naj bi na konsenzu znotraj široke skupine, kmalu pa se je izkazalo, da v skupini tako različnih deležnikov (oglaševalska panoga, iskalniki, drugi ponudniki storitev na spletu, zagovorniki zasebnosti, raziskovalci itd.) ni mogoče doseči strinjanja glede nekaterih ključnih tem o političnem vprašanju pomena in dopustnosti sledenja, kjer so panožna stališča diametralno nasprotna od stališč zagovornikov zasebnosti (Tene, 2013). Vprašanja so zadevala zasebnosti (ne)prijazne privzete nastavitve, dopustne namene sledenja itd. Skupino so nekateri med razvojem standarda zapustili, nekateri iskalniki so začeli signal ne sledi sprva podpirati pa so si pozneje premislili,[74] hkrati pa ga tisti na drugi strani (založniki itd.) niso upoštevali. Prav pred koncem procesa je skupino konzorcija W3C za zaščito proti sledenju zapustil tudi pomemben panožni deležnik, Digital

[74] Internet Explorer ponudnika Microsoft je kot prvi oznanil, da bo v brskalniku privzeto vklopljena možnost ne sledi, zaradi razprave v W3C, da privzeta nastavitev ne odraža volje uporabnika, pa je nastavitev pozneje spremenil.

Advertising Alliance (DAA), ki združuje številne predstavnike digitalnega oglaševalskega posla v ZDA (Tene, 2013).

Kritiki postopka oblikovanja standarda ne sledi poudarjajo, da iskanje soglasja pri tako različnih stališčih pomeni rešitev, s katero na koncu ni nihče zadovoljen. V primeru previsokih meril panoga standarda ne bo upoštevala, saj je prostovoljen, v primeru prenizkih meril pa ne sledi zvodeni in bi za posameznike pomenil le majhno dodano vrednost. Prav tako so v dolgem postopku oblikovanja standarda vzniknile različne druge pobude orodij zoper sledenje, ki niso jasno povezane s standardom ne sledi, in sicer na ravneh zveznih držav ZDA in še posebej na ravni zakonodaje v EU, kjer so med letoma 2012 in 2016 potekala pogajanja glede nove Splošne uredbe o varstvu osebnih podatkov (Tene, 2013).

Kritiki tudi poudarjajo, da prepuščanje regulacije sledenja na spletu organizaciji, kot je W3C, v kateri ima glavno vlogo panoga, pomeni, da bo končni rezultat po godu največjih igralcev, ne pa v korist uporabnikov spleta, in da je prava pot zakonsko reguliranje, pri čemer bi moral posredovati tudi regulator FTC, ki je bil v postopku ustvarjanja standarda ne sledi v ozadju in ne na čelu razprave o koristih uporabnikov. Cambell (2014) je argument podkrepil z dejstvom, da naj bi standard ne sledi omejeval le tretje strani, ne pa tudi tistih, ki jih uporabnik dejansko obišče. Največji ponudniki storitev na spletu in hkrati največji sledilci pa so po svoji naravi oboje, prva in tretja stranka, kar pomeni, da bo lahko npr. Google svojim uporabnikom še vedno sledil in svojo prednost nato unovčil na trgu tretjih strank, ker ima kot oglaševalska mreža, ponudnik analitike itd. pomembno vlogo. Standard ne sledi naj bi tako resno omejil le manjše ponudnike v vlogi tretjih strani (Cambell, 2014).

5.4.1 Standard ne sledi danes

Postopek oblikovanja standarda ne sledi je obsegal več osnutkov, ki jih je pripravljala skupina deležnikov in so bili na voljo javnosti za komentarje. Standard obsega dva dokumenta: tehnično specifikacijo signala ne sledi (W3C, 2015, 2017, 2019a) in dokument z okvirom politik, kako glede signala ravnati (W3C 2016, 2019b). Dokumenta opisujeta tehnične nastavitve za oddajanje signala ne sledi ter delovanje druge strani, ki prejme signal. Oba sta prostovoljna, prav tako pa ni na voljo tehničnih mehanizmov za preverjanje skladnosti.

a) Tehnična specifikacija signala ne sledi

Tehnična specifikacija signala ne sledi ne omejuje zbiranja podatkov strani, ki jo je uporabnik dejansko obiskal (angl. 1st party), temveč le tretjim stranem. Spletni trgovci bi znotraj svojega spletnega mesta lahko sledili uporabnikom in beležili njihove navade, spletni mediji šteli prebrane članke itd. in svojim uporabnikom priporočali vsebine glede na njihovo vedenje (Brookman, 2014). Signal ne sledi pa bi morale upoštevati tretje strani, npr. pri praksi ponovnega ciljanja (angl. retargeting), kjer spletna stran zbira podatke o svojih uporabnikih znotraj svoje spletne strani, da jih lahko znova doseže na drugih spletnih straneh. Prav tako bi morale signal spoštovati oglaševalske mreže, ki sledijo uporabnikom prek različnih spletnih strani in ustvarjajo profile, ter pri sledenju, ki ga izvajajo predvsem spletna družbena omrežja, tako da na druge spletne strani vključijo svoje vtičnike (npr. Facebookov »Všeč mi je« vtičnik) ter tako spremljajo uporabnika tudi zunaj svojega omrežja, po vseh straneh, ki vključujejo vtičnik (Davies, 2015).

Bistveni poudarek je na tem, da mora signal ne sledi izražati uporabnikovo voljo in torej ne sme biti prednastavljen s strani brskalnika, ponudnika storitev, organizacije ali omrežnih mehanizmov zunaj nadzora uporabnika. Dokument primeroma navaja, kako bi uporabnik lahko izrazil svojo odločitev, npr. s klikom na potrditveno polje v svojem brskalniku, namestitvijo dodatka, ki je namenjen izražanju izbire glede sledenja, s spremembo nastavitev zasebnosti, ki bi vključevale tudi možnost signala ne sledi. Brskalnik bi lahko ponudil izbiro glede sledenja med zagonom, npr. pri prvi uporabi po tem, ko je v brskalniku omogočena možnost izbire signala ne sledi. Prav tako bi uporabnik lahko imel možnost, da sam izbere posodobitev brskalnika in tako vključi signal ne sledi. Tehnična specifikacija poudarja, da če uporabnik sam ne izrazi izbire, preference glede sledenja ne smejo biti poslane. Če uporabnik svoje volje glede sledenja ni izrazil, mora oddajati signal »nenastavljeno« (angl. *unset*). Prejemniki tega signala pa se lahko nato odločijo, kakor se jim zdi najbolj primerno glede na konkretnega uporabnika in njegovih okoliščin ter na zakonodajo, ki jih veže. Lahko se zanašajo tudi na morebitne izražene preference iz drugih virov (morda je uporabnik privolil v sledenje pri določeni strani, morda je registriran itd.) (W3C, 2019).

Dokument predvideva, da morajo strežniki, ki bodo prejeli uporabnikov signal ne sledi, oddati odziv, s katerim opredelijo, ali in kako bodo spoštovali signal. Strežnik lahko npr. odgovori z N, kar pomeni, da ne zbira podatkov o uporabniku. C pomeni, da menijo, da imajo

uporabnikovo soglasje in da mu lahko sledijo ne glede na signal ne sledi. Strežnik lahko odgovori z vrednostjo P – potencialno soglasje, kar pomeni, da trenutno ne ve, ali ima posameznikovo privolitev, vendar pridobljenih podatkov ne bo delil, preden ne ugotovi, ali obstaja posameznikova privolitev, in da bo, če privolitve ne najde v 48 urah, zbrane podatke izbrisal ali jih za stalno deidentificiral. To naj bi bilo namenjeno sistemom za merjenje občinstva (analitiki), kjer je ugotavljanje, ali obstaja posameznikova privolitev nepraktična ali povezana s tem, da morajo spletne strani, ki uporabljajo take storitve, ugotoviti, ali imajo privolitev. Odziv z D pa pomeni, da signala ne sledi ne bodo upoštevali. V tem primeru bi moral strežnik zagotoviti povezavo na informacije, v katerih natančno opredeli, zakaj uporabnikove nastavitve ne bo upošteval (W3C, 2019). Tiste strežnike, ki signala ne sledi upoštevali, bi na koncu lahko brskalnik tehnično omejil, tako da sledenje ne bi bilo mogoče (Brookman, 2014; Rose, 2015).

Tehnična specifikacija opredeljuje, da se lahko standard uporablja tudi kot mehanizem za pridobivanje privolitve (kot odziv na evropsko zakonodajo), pri čemer bi lahko ponudniki vsebin uporabnikom, ki oddajajo signal ne sledi, ponudili možnost, da bi lahko svojo odločitev za kontekst obiskane spletne strani in potencialno tudi njene zaupanja vredne partnerje spremenili ter tako dodali izjemo (W3C, 2019). Dodana vrednost standarda je tudi, da uporabnik lahko, še preden se mu naloži zahtevana spletna stran, preveri, ali upošteva signal ne sledi (angl. *preflight check*) (W3C, 2019). W3C je podaljšal mandat skupini, ki dela na standardu, za dodatne aktivnosti izkazovanja, da standard omogoča pridobivanje privolitve skladno z zakonodajo EU. O'Neill ugotavlja, da ima standard ne sledi kot orodje za izražanje uporabnikove izbire absolutno prednost pred drugimi rešitvami, ki temeljijo na piškotkih (npr. shema IAB, pojasnjena v poglavju 5.3.1), saj je signal na ravni brskalnika precej zanesljivejši kot piškotki, s katerimi se označuje uporabnikovo izbiro, saj so ti lahko izbrisani, blokirani itd. (O'Neill, 2018).

b) Dokument z okvirom politik, kako glede signala ravnati

Eden bistvenih poudarkov dokumenta je opredelitev sledenja, ki zajema zbiranje podatkov o aktivnostih posameznega uporabnika v različnih okoljih in hrambo, uporabo ali deljenje podatkov, izpeljanih iz te aktivnosti zunaj okolja, v katerem je nastala, pri čemer je okolje zbirka virov, ki jih obvladuje ista stranka ali jih skupno obvladuje več strank (W3C, 2016). Iz opredelitve izhaja, da signal ne sledi zajema tako zbiranje podatkov o uporabnikih kot tudi

njihovo uporabo zunaj konteksta, v katerem so bili zbrani. Ali bo signal ne sledi zajemal zbiranje podatkov ali pa le njihovo uporabo za namen oglaševanja ipd., je bila ena od prvih dilem pri razvoju (Kamara in Kosta, 2016, str. 13), vendarle pa je, kot kaže, na koncu prevladal argument, da je omejeno že samo zbiranje podatkov (kar je tudi eden ključnih pogojev za potencialno uporabo signala v okviru evropske zakonodaje).

Bistveni poudarek dokumenta sprejemljivih politik sledenja je, da tretje stranke (kot so npr. oglaševalske mreže) ne smejo slediti uporabniku, ki oddaja signal ne sledi, razen če:

- so od uporabnika pridobile soglasje;
- zbirajo podatke za enega od dopustnih rab, tj. za namen omejevanja števila prikazovanja oglasov, zaračunavanja in revizije, zavarovanja ali zaščite pred programskimi napakami (angl. *debugging*);
- so podatki deidentificirani, kar pomeni, da obstaja visoka raven zaupanja, da posameznik na podlagi podatkov ali kombinacije z drugimi hranjenimi in dostopnimi informacijami ne more biti neposredno ali posredno prepoznaven (npr. s povezovanjem z identifikatorjem ali napravo). Dokument ponuja tudi širšo razlago pojma deidentifikacije (W3C, 2016);
- panožni predlogi, da bi bilo dopustno tudi sledenje za namen izboljševanja storitve, analitike ter profiliranja za trženjske raziskave in bi bilo omejeno le prikazovanje oglasov, ne pa tudi zbiranje podatkov, ni bilo sprejeto (Rose, 2015).

Čeprav vsi večji brskalniki že omogočajo nastavitev ne sledi, je trenutno število tistih ponudnikov, ki ta signal dejansko upoštevajo, majhno in ne vključuje največjih spetnih ponudnikov, kot sta npr. Google in Yahoo. Zuiderveen Borgesius in McDonald (2015) sta analizirala politike varovanja zasebnosti nekaterih največjih ponudnikov v ZDA (Facebook, Google, Amazon, YouTube, Wikipedija, eBay, Twitter, Netflix, LinkedIn, Bing itd.) in ugotovila, da glede spoštovanja signala ne sledi bodisi ne ponujajo nobenih informacij bodisi pojasnjujejo, da ga ne upoštevajo, saj naj še ne bi bil dokončan, naj ne bi obstajala skupna razlaga njegove veljave ipd. (Zuiderveen Borgesius in McDonald, 2015).

Majhno število tistih, ki signal ne sledi spoštujejo, nekateri pripisujejo dejstvu, da ni predpisanega načina, na katerega mora ponudnik storitve oz. spletna stran zahtevi po prekinitvi sledenja zadostiti, temveč se lahko vsak odloči v skladu s svojimi tehnološkimi

možnostmi in preferencami. Zahtevo ne sledi lahko spletna stran spoštuje tako, da si zahtevka uporabnika ne beleži v svojih dnevnikih, lahko pa tudi izklopi osebno prilagojeno priporočanje vsebin za take uporabnike (Packer, 2015).

Spoštovanja signala ne sledi v praksi ni veliko, je pa na drugi strani opazen velik porast orodij za blokiranje oglasov (protireklamnih vtičnikov), kar kaže na to, da bo dokončni standard ne sledi morda prišel prepozno (Rose, 2015; Davies, 2015; Packer, 2015). Kot trdi Packer (2015), bi moralo biti spoštovanje signala ne sledi v interesu panoge, saj so druge metode omejevanja sledenja, kot so razdrobljene možnosti odjave pri različnih ponudnikih, protireklamni vtičniki in potencialna zakonodaja, podobna evropski, še bolj omejujoče (Packer, 2015). Standard ne sledi omejuje le sledenje, dopušča pa prikazovanje oglasov (Brookman, 2014).

Potrošniška organizacija Consumer Watchdog iz ZDA je sredi leta 2015 od Zvezne komisije za komunikacije (*Federal Communications Commission* – FCC) zahtevala, da začne od ponudnikov spletnih storitev (ki jih po svoji terminologiji poimenuje *edge providers*), kot so npr. Google, Facebook, YouTube, Pandora, Netflix in LinkedIn, zahtevati, da spoštujejo signal ne sledi, ki ga oddajajo uporabniki. FCC pa je zahtevo zavrnila z obrazložitvijo, da ti ponudniki ne spadajo med ponudnike dostopa do interneta, na katere naj bi se nanašala strožja pravila glede varovanja zasebnosti (Brodkin, 2015).

Veliki pomanjkljivosti standarda ne sledi sta prav njegova prostovoljnost in pravno nezavezujoč status, saj na panožni ravni še ni čutiti pravega interesa za njegovo uvedbo, hkrati pa obstajajo le redki primeri zunanje prisile k spoštovanju signala in možnosti za sankcioniranje neupoštevanja. Prvi korak je bil leta 2013 narejen v Kaliforniji, kjer je bil sprejet zakon o Zaščiti zasebnosti na spletu,[75] ki od ponudnikov storitev in spletnih strani zahteva, da v svojih politikah zasebnosti jasno opredelijo, kako ravnajo, če prejmejo signal ne sledi. Ne zahteva torej upoštevanja signala, temveč le opredelitev, ali signal upoštevajo (Kamara in Kosta, 2016). Da bi standard ne sledi postal učinkovito orodje za obrambo pravic uporabnikov na spletu, je glede na razvoj in pomanjkanje interesa po njegovi uvedbi potreben razvoj v smeri zakonodaje, ki bi ponudnike spletnih storitev prisilil k omogočanju možnosti izbire in bi sankcioniral ravnanja, ki ne spoštujejo uporabnikovega signala ne sledi. Prav tako

[75] *The California Online Privacy Protection Act* (CalOPPA).

pa bi glede tega morali upoštevati tudi raznolikost nacionalnih zakonodaj in omejitve ozemeljske veljavnosti prava ter nadzornih organov. Zuiderveen Borgesius in McDonald (2015) glede ozemeljske veljavnosti prava navajata, da naj bi omenjeni kalifornijski zakon, ki zahteva razkritje praks upoštevanja signala ne sledi, *de facto* veljal na vsem ozemlju ZDA, čeprav je zavezujoč le v Kaliforniji, saj naj bi varoval državljane Kalifornije, pri čemer sedež ponudnika storitve, do katere dostopajo (npr. iz druge zvezne države v ZDA), ni pomemben. Ker je za ponudnike storitev precej preprosteje, da upoštevajo signale ne sledi vseh uporabnikov, kot pa z geolociranjem iskati le tiste iz Kalifornije, naj bi kalifornijski zakon praktično omejeval vse ponudnike iz ZDA (Zuiderveen Borgesius in McDonald, 2015, str. 19–20).

Uporabnost standarda v okviru EU, kjer velja strožja zakonodaja glede sledenja, ki zahteva vnaprejšnjo privolitev, in ne le možnost naknadne zavrnitve, je bila pomembna tema od začetka njegovega razvoja. Kako z eno rešitvijo omogočiti skladnost v obeh kontekstih, je bil velik izziv, na koncu rešen tako, da je odgovornost na strani, ki prejme signal ne sledi ali informacijo, da uporabnik ni izrazil svoje preference. Če mora spoštovati zakonodajo EU, uporabniku, če ni izrazil svoje volje, ne sme slediti. Če je na območju ZDA, takemu uporabniku lahko sledi, saj mu mora ponuditi le možnost naknadne zavrnitve (Zuiderveen Borgesius in McDonald, 2015, str. 18). Zuiderveen Borgesius in McDonald (2015) sta prepričana, da standard ne sledi načeloma zagotavlja vse potrebne komponente za implementacije, skladne s pravom EU. Hkrati sta pojasnila, kako bil lahko ta obravnavala zahteve ne sledi, da bi bila skladna z zakonodajo EU. Lahko bi razlikovala uporabnike iz EU, pri katerih ne bi smela izvajati sledenja, če ti ne bi imeli vklopljene možnosti sledi (DNT: 0), ter uporabnike zunaj EU, ki bi jim lahko sledila, razen če bi imeli vklopljeno možnost ne sledi (DNT: 1). Uporabnikom, ki jim ne bi smela slediti, bi lahko ponudila možnost, da soglašajo s sledenjem, lahko bi jim ponudila možnost, da plačajo, če ne želijo sledenja, ali pa bi jim zavrnila ogled spletne strani, če se ne bi strinjali s sledenjem (zadnja možnost je sicer glede na zakonodajo EU sporna) (Zuiderveen Borgesius in McDonald, 2015, str. 35–36). Nadgrajena oblika standarda ne sledi, ki ga je razvila nevladna organizacija Electronic Frontier Foundation in je združena z dodatki Privacy Badger ali Disconnect, ki samodejno blokirajo sledenje, ki ni skladno z uporabnikovim signalom ne sledi, naj bi npr. najverjetneje zagotavljala skladnost s pravom EU (Zuiderveen Borgesius in McDonald, 2015, str. 19–31). Tudi iz zadnjega mnenja Delovne skupine iz člena 29 izhaja za(upanje) v obete standarda ne

sledi oz. takega tehničnega mehanizma na ravni nastavitev v brskalniku, saj poziva tudi panogo – upravljavce spletnih strani, da signal ne sledi upoštevajo in spoštujejo (WP29, 2016, str. 17).

5.4.2 Standard ne sledi kot orodje za regulacijo vedenjskega oglaševanja

Kamara in Kosta (2016) idejo standardizacije izražanja uporabnikove volje glede sledenja pozdravljata, saj naj bi bili po teoriji standardi tehnične specifikacije o dobrih praksah in učinkovite rešitve za postavljen cilj. V tem smislu bi bil mehanizem ne sledi preprosto in učinkovito orodje za to, da uporabnik izrazi svojo željo, in za prejemnika, ki se mora na željo odzvati. Standardizirana rešitev zagotavlja konsistentno izvedbo in razlago, kar je pri čezmejni naravi sledenja na spletu nujno. Razvoj standardov v telesih, kot je W3C, je odprt in transparenten ter s tem pridobi legitimnost, saj ne preferira strani, temveč išče soglasje in vključuje strani z nasprotnimi argumenti. Standardizacija je prav tako pomembna z vidika uporabniške izkušnje (Kamara in Kosta, 2016, str. 8). Ker pa je upoštevanje standarda prostovoljno, je njegova uspešnost na koncu odvisna od podpore ključnih akterjev v postopku nastajanja in tudi pozneje (Zuiderveen Borgesius in McDonald, 2015).

V primeru standarda ne sledi, ki ga je razvila W3C in omogoča prilagajanje različnim politikam v različnih okoljih ter odgovornost za spoštovanje želje uporabnika v celoti prelaga na prejemnika signala, lahko vidimo, da bo njegova uspešnost najverjetneje odvisna od zakonodajnih ukrepov – bodisi, da bodo ti zahtevali upoštevanje signala ne sledi, ali pa bodo zahtevali razkritje, kako spletne strani standard upoštevajo. Ker standard sam ne omejuje sledenja, je odgovornost za skladno ravnanje povsem na prejemniku signala ne sledi, panoga sama pa še ni pokazala interesa, da se k upoštevanju standarda zaveže. To pomeni, da bi bila za delovanje potrebna zunanja spodbuda ali prisila, najverjetneje v obliki zakonodaje, ki bi določala tudi sankcioniranje nespoštovanja in pristojnosti nadzornih organov.

Na drugi strani pa bi lahko učinkovito varovanje posameznikovih pravic (tudi skladno s strožjo zakonodajo EU) zagotavljal tudi standard sam, brez prevalitve odgovornosti za (ne)spoštovanje popolnoma na stran prejemnikov signala ne sledi, če bi bila nastavitev v brskalniku ne sledi povezana z dodatki, ki tehnično blokirajo sledenje s strani tistih spletnih

strani, ki ne delujejo skladno s standardom in torej nimajo privolitve uporabnika v sledenje (kot v primeru signala ne sledi EFF z dodatki v brskalniku), ugotavljata Zuiderveen Borgesius in McDonald (2015). Tak, strožji standard, ki bi tehnično že sam omejil sledenje, bi lahko učinkovito deloval tudi brez ali pa le z minimalno podporo oz. prisilo zakonodaje in zunanjega nadzora nad prejemniki signala ne sledi. Težava pa je, da bo tak strožji standard glede na proces ustvarjanja signala ne sledi težko dobil podporo panoge in na prostovoljni ravni dosegel veliko sprejetost, saj panogi bolj ustreza nedorečeno stanje, v katerem lahko ob odsotnosti jasnih pravil precej nemoteno izvaja sledenje. Strožji standard bi lahko pridobil veljavo v EU, kjer so upravljavci zavezani strožji zakonodaji, v ZDA pa je težko pričakovati, da bo prostovoljni standard panogo zavezal k restriktivnejšemu sledenju, saj v ozadju ni zakonodaje in sankcij.

5.5 Sklepno o regulatornem okviru za vedenjsko oglaševanje

Regulatorni okvir za vedenjsko oglaševanje je trenutno pester, neenoten v zahtevah in zato neučinkovit. Kljub različnim pobudam za regulacijo, ki bi bolje varovala uporabnike elektronskih komunikacij oz. zmanjšala negativne posledice obširnega sledenja in netransparentnega obdelovanja podatkov uporabnikov za družbo, so dejavnosti vedenjskega oglaševanja na trgu skoraj nedotaknjene, novi pristopi pa se nemoteno razvijajo. To lahko pripišemo tako nejasnim pravilom kot tudi zelo pomanjkljivemu nadzoru.

Regulatorni okvir v EU temelji na razmeroma strogi zakonodaji varstva osebnih podatkov in zasebnosti v elektronskih komunikacijah, ki pa kljub osnovnemu imperativu privolitve posameznika v vedenjsko oglaševanje v večini primerov ponuja ravno dovolj izjem in olajšav, da so te lahko bolj ali manj legitimno uporabljene in uporabniku ni ponujena možnost izbire glede vedenjskega oglaševanja, ali pa je privolitev pridobljena na način, ki pušča dvome glede njene veljavnosti (implicitno, s pogojevanjem itd.). Tudi ob spremembah zakonodaje se kažejo pritiski k mehčanju določb in k razumevanju, da je vedenjsko oglaševanje lahko upravičeno v okviru ponujanja storitve, ki je za uporabnika brezplačna, inovativna itd. Samoregulacija je utemeljena na panožnem kodeksu, ki pa ne zagotavlja skladnosti z minimalnimi zakonskimi zahtevami, kar je njegova glavna pomanjkljivost.

Na drugi strani ZDA prepuščajo urejanje vedenjskega oglaševanja prav takemu kodeksu, saj nimajo koherentne zakonodaje za varovanje pravic uporabnikov v elektronskih komunikacijah. Pravni okvir v ZDA je namreč razdrobljen in temelji predvsem na zahtevi, da podjetja svoje prakse ravnanja s podatki razkrijejo, ni pa posebnih omejitev glede praks obdelave. Če svoje zaveze kršijo, lahko to sankcionira regulator, FTC, kot nepošteno ali zavajajočo prakso. Ker ni posebnih pravnih omejitev glede dopustnih ravnanj in odgovornosti subjektov, ki podatke obdelujejo, so prakse vedenjskega oglaševanja skoraj neomejene. Rezultat je cvetoča panoga vedenjskega oglaševanja, ki za zdaj posluje brez omembe vrednih omejitev, z nekaterimi izjemami uspešnih nadzornih akcij.

Certificiranje in standardizacija sta področji, na katerih se kaže napredek, vendar le, če bosta celostno vpeti v splet regulacijskih strategij in če bo temeljne norme ter možnosti sankcioniranja in nadzora zagotavljala zakonodaja. Zdi se, da bo dolgoletno delo na standardu ne sledi prineslo rezultate: standard je načeloma razvit in pripravljen za uporabo, tudi z vidika skladnosti z zahtevami zakonodaje EU, vendar pa se panoga še vedno obotavlja pri njegovi uresničitvi, kar jasno kaže na to, da se mora zgoditi zunanja spodbuda – bodisi v smislu zakonodaje, ki bo zahtevala uresničitev in spoštovanje, bodisi bo ta spodbuda ekonomska in bo tako ne sledi za izvajalce vedenjskega oglaševanja manjše zlo kot pa npr. protireklamni vtičniki.

Regulacija širšega področja varstva osebnih podatkov se počasi nagiba v smer prepoznavanja koristi spleta različnih regulatornih orodij, med njimi usklajevanja zakonodaje in samoregulacijskih pobud. To bi bilo treba upoštevati tudi na področju vedenjskega oglaševanja. Zakonodajo, ki omogoča različne razlage (v tehnično zahtevnem okolju), bi lahko koristno dopolnjevala in specificirala samoregulacijska orodja, kodeksi, standardi in certificiranje – seveda pod pogojem, da upoštevajo temelje, ki jih ta določa.

Vedenjsko oglaševanje nima le negativnih posledic za zasebnost posameznikov in varstvo njihovih osebnih podatkov, ampak gre tudi za druge interese. Je bistvo monetizacije »brezplačnih« storitev, programske opreme, lahko tudi izdelkov, kar zagotovo prinaša prednosti v smislu družbenega napredka, inovacij in zastopanosti socialno ranljivejših skupin v informacijsko-komunikacijski sferi, vendar hkrati negativne posledice v smislu vseprisotnega nadzora in diskriminacije, tudi negativnega vpliva na politične in demokratične

procese. Glede tega je posebej pomembno vprašanje medijev in njihove odvisnosti od vedenjskega oglaševanja ter alternativnih možnosti financiranja za izvajanje vloge »četrte veje oblasti«. S tem je povezano vprašanje kakovosti vsebin in tudi vloge javnih RTV servisov, ki ostanejo eden redkih branikov »neodvisne« produkcije vsebin. Glavni izvajalci vedenjskega oglaševanja imajo pravzaprav monopolne položaje, kar zbuja nadaljnja vprašanja koristi in izzivov za širšo družbo.

Pričakovati, da bodo vse ali večino teh posledic na različnih družbenih ravneh in sistemih rešila pravila s področja varovanja zasebnosti in varstva osebnih podatkov ali osredinjenost na vprašanje privolitve ali ne, je utvara, saj zadevajo le najbolj instrumentalni del te dejavnosti – obdelave osebnih podatkov –, posledice vedenjskega oglaševanja pa segajo na področje pravil za varstvo konkurence, davčnih pravil, medijskih pravil itd. Prav tako so visoka pričakovanja za nadzorne organe s področja varstva osebnih podatkov, ki bi morali biti s svojimi omejenimi viri in pooblastili sposobni poznavanja vsega tega širšega konteksta, da bi lahko verodostojno in samozavestno tehtali med različnimi zadevnimi interesi. Nerealistično je pričakovati, da bodo lahko branik pred praksami, ki presegajo okvire varovanja temeljne pravice do zasebnosti in varstva osebnih podatkov.

Profiliranje, strojno učenje, diskriminacija in posegi v samo bistvo demokratičnega procesa so posledice vedenjskega oglaševanja, ki pravzaprav presegajo tudi današnje regulatorne okvire. Slednji namreč pogosto le stežka uokvirjajo nove prakse, ki jih omogoča skokovit razvoj tehnologije. Zato je morda rešitev, poleg izboljšanja regulatornih okvirov, smiselno iskati na področju etike, družbene odgovornosti in vizije trajnostnega razvoja družbe.

6 UGOTOVITVE ANALIZE INTERVJUJEV

V nadaljevanju so predstavljene ugotovitve analize intervjujev[76], in sicer po sklopih glede na raziskovalna vprašanja in tematike, ki se pojavljajo znotraj njih. Ponekod so ugotovitve dopolnjene z ugotovitvami dokumentarne analize, predvsem, kadar bi zgolj navajanje ugotovitev intervjujev kazalo nepopolno sliko in ugotovitve dokumentarne analize nastopajo v vlogi preverjanja informacij in zagotavljanja točnosti ugotovitev intervjujev. Prav tako so ugotovitve, kjer je to potrebno za doseganje jasnosti besedila, postavljene v kontekst, ki izhaja iz poglavja o pregledu literature in primerov izvajalcev vedenjskega oglaševanja. V empiričnem raziskovanju smo uporabili različni kvalitativni metodi, ki sta se med seboj dopolnjevali v smislu pridobivanja informacij, hkrati pa služili kot sredstvo za preverjanje relevantnosti in točnosti zaključkov – z intervjuji so bili tako preverjeni začetni zaključki iz analize dokumentarnih virov in zakonodaje, ter obratno, analiza dokumentov je služila kot pomembno sredstvo preverjanja navedb intervjuvancev in kritične refleksije glede njihovih zaključkov o prihodnji regulaciji vedenjskega oglaševanja. Poglavje se sklene s sintezo primerjave ugotovitev dokumentarne analize in analize intervjujev, ki tabelarično prikaže, kako se ugotovitve glede na tri raziskovalna vprašanja povezujejo, kje se dopolnjujejo in podpirajo ter kje ugotovitve različnih metod raziskovanja odstopajo oziroma si nasprotujejo.

Prvi del zajema vedenjsko oglaševanje v kontekstu razvijajočih sodobnih tehnologij in novih poslovnih modelov, predstavljene so prednosti in izzivi za različne deležnike tega ekosistema, Ponuja odgovor na prvo raziskovalno vprašanje. V drugem delu so predstavljeni pogledi glede tega, kako vedenjsko oglaševanje vpliva na pravice uporabnikov spleta in sodobne tehnologije. Obravnavano je tudi vprašanje mehanizmov, ki so uporabniku na voljo, da zaščiti te svoje pravice. Tretji del zajema vprašanja veljavne regulacije tega področja in koliko je učinkovit v varstvu pravic posameznikov. Drugi in tretji del skupaj ponujata odgovor na drugo raziskovalno vprašanje. Četrti del zajema vprašanja prihodnje regulacije, in kako bi ta lahko bila učinkovitejša ter torej ponuja odgovor na tretje raziskovalno vprašanje.

[76] Zvočni posnetki vseh intervjujev so v obliki surovih podatkov na voljo pri avtorici. Izseki izjav, predstavljenih v tem poglavju, so le ilustrativni. Izjave so za namen predstavitve ugotovitev povzete v besedilu, pri navedkih, ki dodatno ilustrirajo ugotovitve, pa je ohranjen zapis v izvornem jeziku (tudi, kadar gre za angleški jezik). Na ta način je ohranjen izvirni pomen izrečenega, z vsemi specifikami, govornimi posebnostmi in tonom odgovorov.

6.1 Vedenjsko oglaševanje v kontekstu razvijajočih sodobnih tehnologij in novih poslovnih modelov: prednosti in izzivi za deležnike

Prvi sklop ugotovitev in razprave zajema vedenjsko oglaševanje v kontekstu razvijajočih sodobnih tehnologij in novih poslovnih modelov. Raziskali smo prednosti in izzive za različne deležnike: oglaševalce, oglaševalske agencije in podjetja z dejavnostjo posredovanja spletnih oglasov (t. i. *ad tech* panogo), za založnike (zlasti medije) in za uporabnike elektronskih komunikacij. Največkrat omenjena prednost vedenjskega oglaševanja v intervjujih je manjša izguba oglaševalskih sredstev za ne-relevantna občinstva, saj je mogoče zelo natančno ciljanje na posameznike s specifičnimi lastnostmi, interesi, zgodovino in prikazovanje zanje pomembnih vsebin. Učinkovitost oglasov in porabe oglaševalskih sredstev ter merljivost so bile posebej poudarjene prednosti avtomatiziranih programatičnih oglaševalskih sistemov, kjer je jasno, kolikšna so bila sredstva za oglaševanje, koliko je bilo prikazov oglasa ter s tem povezano je jasneje tudi, kje je oglaševalski denar izgubljen: »Da se da vržt stran samo še tretjino denarja, ali pa samo še četrtino.« (Medij 3, osebni intervju, 2017, 11. julij). Eden glavnih argumentov za vedenjsko oglaševanje je omogočanje brezplačnih vsebin in inovativnih storitev, npr. zavarovanj za uporabnike zelo dragih koles ali posebnih pasem psov, ki običajno svojega imetja ne bi mogli zavarovati. Če zavarovalnica ugotovi, da obstaja trg za take produkte, lahko produkt ponudi in tako pridobijo vsi akterji (Svetovalec 4, osebni intervju, 2017, 14. marec).

6.1.1 Oglaševalci

Z vidika oglaševalca vedenjsko oglaševanje pomeni večjo učinkovitost, tako v smislu boljšega doseganja ciljnih občinstev kot tudi v smislu višje konverzije v nakupno vedenje. Oglas bo videlo večje število ljudi, ki so potencialno v položaju, da jih ponudba zanima. Zato je tudi večja možnost transformacije tega v nakupno vedenje. Še posebej je to pomebno za nišne oglaševalce.

> From an advertiser perspective, targeting promises to be more efficient for start and more effective. More efficient because you end up actually having a larger percentage of your ads being seen by people which are potentially in the position of considering your offer. More effective because the likelihood of transforming that through connection into purchase is higher. (Oglaševalec 2, osebni intervju, 2017, 7. februar)

Temu je treba dodati prednosti, ki jih omogoča povezovanje različnih uporabnikovih naprav in razvoj v okviru interneta stvari, kot izhaja iz pregleda literature: posameznika je mogoče z oglasi doseči na različnih platformah, v kontekstu, ki je za to primeren, in na primerni lokaciji. Zmožnosti vse bolj sofisticiranih analiz podatkov posameznikov, pridobljenih iz različnih naprav, in nato povezanih, pa se pokažejo v oglasih, ki so relevantni glede na stanje, vedenje in prepričanja posameznika ter se tako povečajo možnosti, da se bo na oglase odzval z zaželenim vedenjem (glej npr. Busch, 2016; Aksu in drugi, 2018).

Zato se oglaševalci čedalje bolj zavedajo pomena in vrednosti podatkov svojih uporabnikov ter so zainteresirani za to, da so podatki v njihovem lastništvu. Kot pojasnjuje Oglaševalec 2, oglaševalci razumejo, da jim bodo podatki na dolgi rok omogočali ciljano oglaševanje in pri tem so najbolj pomembni t. i. *first party* podatki – tisti, ki jih zberejo oglaševalci sami (Oglaševalec 2, osebni intervju, 2017, 7. februar). Oglaševalci si v svojih odnosih z agencijami tudi vse pogosteje prizadevajo poskrbeti, da obdržijo nadzor nad uporabo osebnih podatkov svojih strank, tudi iz strahu, da bi v primeru menjave agencije izgubili dostop do njih ali bi jih agencija uporabila pri storitvah za njihove konkurente (Oglaševalec 2, osebni intervju, 2017, 7. februar).

Ker so za spletno oglaševanje značilne tudi goljufije in zlorabe (npr. ustvarjanje neveljavnega spletnega prometa),[77] se oglaševalci skušajo zaščititi na različne načine – npr. s sklepanjem neposrednih dogovorov s pogodbenimi oglaševalskimi partnerji ali z omejevanjem namenov, za katere lahko agencije uporabljajo njihove podatke (Oglaševalec 2, osebni intervju, 7. februar). Na voljo so jim tudi specializirane revizije za področje zakupa oglasnega prostora (Svetovalec 1, osebni intervju, 2017, 23. januar).

6.1.2 *Ad tech* panoga

Sodobna spletna oglaševalska panoga oz. *ad tech* panoga vključuje veliko podjetij, ki sodelujejo pri dostavi oglasa. Ta opravljajo specializirane naloge in analize podatkov, izdelujejo profile, primerjajo profile posameznikov pri različnih podjetjih in trgujejo s podatki posameznikov, na katere je mogoče ciljati z oglasi. Za nekatere je ciljanje in grajenje

[77] Plačilo oglaševalca je običajno vezano na število obiskovalcev ali število prikazov oglasa, to pa je mogoče izrabiti in ustvarjati obiske ter tako goljufati (Zagovornik 1, osebni intervju, 2017, 26. januar).

seznamov za personalizirano ciljanje oglasov primarna naloga (Oglaševalec 3, osebni intervju, 2017, 27. januar). Kot izhaja iz pregleda literature, jih lahko razvrstimo v nekaj glavnih kategorij – od platform za izmenjavo oglasov, do podjetij, specializiranih za avtomatizacijo oddaje oglasnega prostora in specializiranih za dostavo oglasov glede na prej določene preference oglaševalcev pa do različnih ponudnikov analize podatkov in metrike (Busch, 2016, str. 9).

Učinkovitost oglasov in porabe oglaševalskih sredstev ter merljivost sta bili posebej poudarjeni prednosti avtomatiziranih programatičnih oglaševalskih sistemov: »Na oko 10x. Če izvedem programatično kampanjo, če gledam človek/ure, koliko časa se za nekaj porabi, dobim samo pri organizaciji in izvedbi 10x ceneje. Kakšen je učinek? Ti brez programatika sploh ne moreš ciljati« (Medij 2, osebni intervju, 2017, 13. januar). Ad tech panoga je v porastu, po nekaterih pričakovanjih bo pravzaprav vse digitalno oglaševanje v naslednjih nekaj letih postreženo programatično, kar se kaže na rasti panožnih prihodkov, pa tudi v skoraj monopolnih položajih najuspešnejših ponudnikov Facebooka in Googla, ki skupaj pokrivata tudi do 80 odstotkov trga (eMarketer, 2017; Engelhardt in Narayanan, 2016). Prednosti *ad tech* panoge so tudi v razvijajočih se možnostih oglaševanja prek interneta stvari in mobilnih naprav, ki povezujejo aktivnosti potrošnikov na spletu in v realnem življenju (Busch, 2016; Seitz in Zorn, 2016).

Hkrati pa je trg ponudnikov programatičnega oglaševanja zelo nepregleden oz. sistem »črne skrinje« (Datatilsynet, 2015, str. 10). V verigi izvajalcev se izgubljajo sredstva, (podjetja zaračunavajo provizije), prisotne so tudi goljufije in nepoštene prakse (npr. sledenje uporabnikom po odtisu naprave, ki ga ni mogoče zaznati[78], mnogi klienti ne razumejo, katera podjetja v verigi vse sodelujejo pri izvajanju oglaševanja (Oglaševalec 2, osebni intervju, 2017, 7. februar). Nepregleden je tudi tok podatkov posameznikov. Založnik najame enega oglaševalskega partnerja, ta pa dostop do podatkov o uporabnikovem obisku posamezne spletne strani omogoči svojim nadaljnjim pogodbenim partnerjem, običajno za to, da izdela tabelo za primerjavo piškotkov različnih ponudnikov ali pa za namen draženja profilov v realnem času (angl. *real time bidding*) (Oglaševalec 3, osebni intervju, 2017, 27. januar).

[78] Oglaševalec 3 (osebni intervju, 2017, 27. januar) omenja primer podjetja Turn.

Zaradi porasta blokiranja oglasov so založniki pozornejši, komu dovolijo dostop do podatkov o strankah, saj to pomeni slabšo uporabniško izkušnjo, slabše zavarovanje podatkov in splošne negativne občutke posameznikov do teh praks (Oglaševalec 3, osebni intervju, 2017, 27. januar). Zaradi velikega števila ponudnikov in nepreglednosti *ad tech* panoge nekateri napovedujejo konsolidacijo na tem trgu (Oglaševalec 3, osebni intervju, 2017, 27. januar; Regulator 2, osebni intervju, 2017, 31. marec).

6.1.3 Založniki

Možnost ciljanja na specifične stranke ima za založnike otipljivo vrednost v smislu prodaje oglasnega prostora. Nekateri založniki zelo dobro vedo, kdo so njihove stranke in znajo prodati njihove profile klientom (Oglaševalec 2, osebni intervju, 2017, 7. februar). Založniki, ki imajo vsebino, ki odseva nakupne namene potrošnika (npr. podatki o tem, kaj so posamezniki na spletni strani iskali), ne potrebujejo veliko podatkov o potrošniku, da lahko učinkovito ciljajo oglase. Vrednost zanje ustvarja kontekst, vsebina in podatki o potrošnikih pa so morda le dodaten vir prihodkov (Oglaševalec 3, osebni intervju, 2017, 27. januar). Založniki, katerih vsebina pa se ne prodaja sama (npr. imeniki, spletna stran o človekovih pravicah itd.), lahko unovčijo podatke uporabnikov, katerih podatke imajo. Tako lahko tudi 50 odstotkov prihodkov založnika predstavljajo podatki o uporabnikih spletne strani, uporabljeni za namen oglaševanja (Oglaševalec 3, osebni intervju, 2017, 27. januar). Poudarjeno je bilo, da ima za manjše, posebej nišne založnike, prednost programatično oglaševanje. Oglaševalec 2 izpostavlja, da lahko veliko bolj učinkovito monetizirajo svoje občinstvo (Oglaševalec 2, osebni intervju, 2017, 7. februar). Medij 2 pa pojasni, da malim izdajateljem lahko zagotavlja minimalen prihodek, potreben za njihovo delovanje in tehnične stroške (Medij 2, osebni intervju, 2017, 13. januar).

Negativni vidik avtomatizacije oglaševanja ter velikega števila akterjev, ki sodelujejo v delčkih transakcij je, da založniki pogosto poznajo le tistega oglaševalskega posrednika (angl. *supply side platform*), s katerim neposredno sodelujejo, ne pa tudi množice podjetij v verigi, s katerim slednji sodeluje pri analizi podatkov, draženju profilov in dostavi oglasa (Medij 1, osebni intervju, 2017, 13. januar). To ima negativne posledice v smislu varnosti uporabnikov in uporabniške izkušnje (Oglaševalec 3, osebni intervju, 2017, 27. januar), saj založnik nima nadzora nad tem, kdo vstopa v njegove procese obdelave podatkov in na neki način »krade«

podatke njegovih strank (Regulator 3, osebni intervju, 2017, 15. februar). Po drugi strani pa Regulator 3 pojasnjuje, da mediji na Norveškem želijo bolj nadzorovati podatke svojih uporabnikov in zato imeti na svojih spletnih straneh manj sledilcev, kar pomeni večjo preglednost. Njihov cilj je nadzor nad podatki in zato so tudi njihove rešitve lahko bolj zasebnosti prijazne (Regulator 3, osebni intervju, 2017, 15. februar).

Poudarjeno je bilo, da morda založniki slabo preučijo pogodbena določila ponudnikov programatičnih oglaševalskih storitev (Oglaševalec 3, osebni intervju, 2017, 27. januar). Za veliko založnikov je značilna predvsem skrb glede tega, po kakšni ceni prodajajo svoj oglasni prostor in ali so oglasi pravilno prikazani. Medij 1 pojasni, da jih s stroškovnega vidika zanima, kakšna je celotna veriga oglaševalskih izvajalcev, da bi videli, koliko sredstev se v verigi izgubi (Medij 1, osebni intervju, 2017, 13. januar). Poudarjena je bila tudi izguba nadzora založnika nad tem, ali je poleg njegove vsebine morda prikazan kontekstu neprimeren oglas (npr. za vrv ob članku o samomorih). Medij 1 pojasni, da obstajajo seznami prepovedanih vsebin, kot je npr. prikazovanje oglasov za alkohol ali tobačne izdelke, seksualne vsebine, ki so privzeto vključeni. Založnik mora posebej odobriti, če želi dopustiti oglaševanje te vrste vsebin na svoji spletni strani (Medij 1, osebni intervju, 2017, 13. januar).

Mediji

Mediji oziroma njihove spletne edicije so eden ključnih deležnikov iz vrste založnikov pri vprašanjih uporabe vedenjskega oglaševanja na spletu. Ker lahko spletne izdaje uporabniki običajno spremljajo brezplačno, imajo težave s financiranjem. Medij 3 poudarja problematiko konkurence spletnih medijev z drugimi ponudniki storitev in vsebin na spletu (npr. spletna družbena omrežja): »Internetna podjetja so imela popolnoma free ride, ona so kar naenkrat pobrala vse prihodke medijem, pobrale veliko vsebin medijem, pobrale veliko pozornosti medijem, in hkrati so se uspele izogniti praktično vse odgovornosti, ki jih mediji imajo« (Medij 3, osebni intervju, 2017, 11. julij). Poslovni model medijev pojasni skozi prizmo podatkovne panoge in jih primerja s spletnim prodajalcem Amazon, ki se je razvil tako, da je razumel, da je predvsem podatkovno podjetje in ne toliko trgovec: »Na neki ravni lahko danes deliš posle na tiste, ki razumejo podatkovne baze in na tiste, ki jih ne. In mediji so tipični primer industrije, ki tega ne razume« (Medij 3, osebni intervju, 2017, 11. julij).

Zagate s financiranjem mediji rešujejo z oglaševanjem, najpogosteje vedenjskim ter tako podatke svojih bralcev delijo z oglaševalci in podjetji, ki sodelujejo pri bolj ali manj avtomatiziranem prikazovanju spletnih oglasov. Najpogostejši taki omrežji sta Google in Facebook. Trenutno mediji uporabljajo različne načine, da uporabnike »prisilijo« v strinjanje z vedenjskim oglaševanjem, bodisi uporabljajo t. i. zidove, kjer brez strinjanja ni mogoč dostop do vsebine, rešitve prijave (angl. *log-in*), kjer ta ni dostopna uporabnikom, ki niso registrirani in se niso strinjali z vedenjskim oglaševanjem (Regulator 3, osebni intervju, 2017, 15. februar), ali pa uporabnike zgolj obvestijo o vedenjskem oglaševanju. Regulator 3 pojasnjuje, da na Norveškem npr. obstaja dominantni založnik, ki upravlja z vsemi večjimi nacionalnimi in regionalnimi časniki. Želeli so ustvariti enoten nacionalen sistem prijave, s katerim bi zajeli večino uporabnikov in bi bili tako konkurenca Googlu in Facebooku. Podatki posameznikov bi se tako delili le na nacionalni ravni. Niso pa s tem načrtom uspeli (Regulator 3, osebni intervju, 2017, 15. februar).

Sicer je vprašanje, koliko je nujno posegati prav po vedenjskem oglaševanju, saj ugotovitve intervjujev kažejo, da mediji več prihodka dobijo od neposrednih dogovorov z oglaševalci kot od oglasnega prostora, ki ga oddajajo prek programatičnega zakupa. Kot pojasnjuje Medij 1, se lahko spletni medij prilagaja oglaševalcu, lahko zanj ustvarja plačano vsebino, kar je bolj učinkovito (Medij 1, osebni intervju, 2017, 13. januar). Argument nujnosti vedenjskega oglaševanja za obstoj spletnega medija je tako relativiziran, saj je vsaj v primeru konkretnega spletnega medija doprinos na podlagi vedenjskega oglaševanja majhen.

Kritika tudi poudarja, da ni nujno, da se uporabniki medijev teh transakcij s podatki zavedajo in da vedenjsko oglaševanje škoduje njihovi zasebnosti, zato bi morali mediji uporabnikom ponuditi vsebino, tudi če se ne strinjajo z vedenjskim oglaševanjem. (Regulator 3, osebni intervju, 2017, 15. februar). Regulator 3 meni, da uporabniki na tak način za časopis plačajo dvakrat, enkrat ko ga kupijo in še enkrat z osebnimi podatki, ko ga spremljajo na spletu (Regulator 3, osebni intervju, 2017, 15. februar).

Rešitve finančne zagate medijev bi lahko bile v naročninah kot alternativnemu viru financiranja, pa tudi v sredstvih, ki bi jih lahko za svoje delovanje mediji pridobili od države, saj so eden postulatov delujoče demokracije. Zagovornik 4 tako poudarja, dobro novinarstvo ne more biti financirano le z oglasi, pač pa potrebuje tudi naročnine. Izpostavi primere

spletnih medijev iz ZDA, ki imajo oglaševalski poslovni model in so osredotočeni le na zbiranje klikov, delitev in objavo čudnih zgodb. To ni poglobljeno, resno novinarstvo, ki ga potrebuje demokracija (Zagovornik 4, osebni intervju, 2017, 8. februar). Optimizacija vsebin glede na zanimanje bralcev, kar bi širilo njihov krog in prihodke medijev, kot poudarja Medij 3, vodi v tabloidizacijo in slabšo kvaliteto vsebin: »*3B: bombs boobs and bizzare*« (Medij 3, osebni intervju, 2017, 11. julij), kar negativno vpliva na položaj medijev v demokratični družbi.

Zadnje raziskave sicer kažejo spodbudne trende financiranja spletnih medijev z naročninami: čeprav digitalno oglaševanje ostaja glavni vir financiranja, se izdajatelji medijev čedalje bolj zavedajo, da to za produkcijo kakovostnega novinarstva ni dovolj in pritiskajo na bralce k neposrednim plačilom – bodisi na ravni posameznih člankov, članarin, naročnin ali donacij. Dvig naročnin je še zlasti zaznaven na Norveškem, Švedskem in Finskem, kjer deluje majhno število izdajateljev medijev in so zelo pogosti različni »plačilni zidovi«. Avtorji dodajajo, da gre sicer za bogate države, ki imajo bogato tradicijo naročnin na časopise in kjer jezikovna ovira preprečuje vstop tuje konkurence na medijski trg in da obstaja tudi veliko držav, v katerih so novice še vedno na voljo brezplačno (Reuters Institute, 2018). Glede tega pa je zagotovo na mestu pomislek, da bi uvedba naročnin vodila v več zasebnosti za tiste, ki si stroške za potrošnjo medijev lahko privoščijo, in manj zasebnosti za ranljivejše (Regulator 4, osebni intervju, 2017, 16. februar).

Vprašanje poslovnih modelov medijev ima posledice za demokratične procese in Regulator 1 ugotavlja, da te tematike ni primerno reducirati le na vprašanje posega v zasebnost in privolitve v vedenjsko oglaševanje, saj imajo mediji v demokraciji vlogo kot neodvisni nadzorniki. Tako je zelo problematično, če družba kot taka ni pripravljena plačati za izvajanje tega nadzora (Regulator 1, osebni intervju, 2017, 15. februar). Regulator 1 zaključuje, da ključna problematika vedenjskega oglaševanja v medijih ni toliko privolitev uporabnikov v sledenje, kot je ustrezno urejanje pogodbene obdelave teh podatkov, in dodaja, da osebno nima tako veliko težav z dejstvom, da je oglaševanje ciljno oziroma osebno prilagojeno, se mu pa zdi problematično, če so podatki uporabljeni za drugačne namene, ne le za ciljanje oglasov (Regulator 1, osebni intervju, 2017, 15. februar).

6.1.4 Uporabniki: od prednosti osebne prilagoditve vsebin do sredstev za blokiranje oglasov

Z vidika uporabnika so prednosti vedenjskega oglaševanja predvsem boljše storitve in bolj relevantne vsebine:

> V tem trenutku je več dobrega za userje, če se te tracka, dobijo prilagojene oglase, ne dobivajo slik iz nekega resorta iz Tajske, 14 dni po tem ko so že doma, to ti gre res na jetra, tisti ki imajo to dobro zrihtat. Vsaj približno so oglasi v kontekstu. (Medij 2, osebni intervju, 2017, 13. januar).

Kadar temeljijo na veljavnih in ne zastarelih podatkih, so prilagojene vsebine boljše, bolj relevantne glede na strasti posameznika, njegovo življenje, kje živi, njegova hotenja, verovanja. Možnost, da se bodo potrošniki na oglase dobro odzvali, je tako večja (Oglaševalec 2, osebni intervju, 2017, 7. februar). Zato si številni uporabniki želijo osebno prilagojenih vsebin. Zagovornik 4 izpostavlja tudi veljavnost in točnost podatkov: ko vedenjsko oglaševanje izvaja podjetje (npr. supermarket), ki ima veliko podatkov o posamezniku, o njegovih nakupih, je to lahko posamezniku v pomoč, saj temelji na veljavnih podatkih. Ko pa gre za podatke, ki se jih uporablja pri ciljanju preko različnih spletnih strani, ti niso nujno točni in natančni. Zato meni, da je vedenjsko oglaševanje lahko dobro, kadar se izvaja omejeno in pametno. V nasprotnem primeru pa gre posameznikom na živce in ruši njihovo zaupanje (Zagovornik 4, osebni intervju, 2017, 8. februar).

Predvsem sogovorniki zunaj panoge vedenjskega oglaševanja poudarjajo tudi, da so prakse sledenja kljub prednostim za uporabnike lahko preveč invazivne, sploh če ciljanje izvajajo tretje strani prek različnih platform. Zagovornik 4 izpostavlja, da je strašljivo, ko te oglasi zalezujejo preko interneta, še posebej, ker pogosto niso relevantni zate ali si pravkar tisto, kar je oglaševano, že kupil (Zagovornik 4, osebni intervju, 2017, 8. februar).

Raziskave stališč uporabnikov elektronskih komunikacij kažejo različno sliko – kažejo, da se posamezniki ne zavedajo, kaj se dogaja na področju oglaševanja, v nekaterih raziskavah vedenjskega oglaševanja večina posameznikov ne želi, vendar se počutijo, da nimajo izbire (Regulator 3, osebni intervju, 2017, 15. februar). V drugih raziskavah (predvsem tistih, ki jih je naročila panoga vedenjskega oglaševanja), ga večina podpira. Razlog lahko iščemo v različno sugestibilnih formulacijah vprašanj in pomanjkanju razumevanja tematike na strani uporabnikov.

> I just don't think people have good understanding of what's happening and I think that when you ask them a question, It's very hard to ask a question even for unbiased, that does not solicit a certain kind of response. So when the advertising industry asks the people: do you like adds about products you're not interested and do you like products that are interesting to you – well I'm obviously interested in the products that are interesting to me. A civil society asks: do you want people profiling you for the purpose of trying to get you to buy things. It's very hard to formulate these questions. (Oglaševalec 3, osebni intervju, 2017, 27. januar).

Zato Oglaševalec 3 meni, da je bolj relevanten kazalnik volje uporabnikov v njihovih aktivnostih, ko so soočeni z izbiro glede svojih možnosti. Zdi se mu, da v zadnjih letih večina ljudi sprejema, da je posredovanje podatkov potrebno, če želijo uporabljati neko storitev (Oglaševalec 3, osebni intervju, 2017, 27. januar).

Na drugi strani pa Oglaševalec 2 pojasnjuje, da oglaševalci razumejo potencial, ki ga ima zanje poznavanje svojega občinstva (da je to vredno več kot fizična lastnina podjetja), in da razumejo, da je interese potrošnikov treba varovati, saj v nasprotnem primeru ti izgubijo zaupanje v posamezno blagovno znamko. Zato so zainteresirani, da so podatki potrošnikov zbrani na način, ki jim je sprejemljiv. Meni tudi, da bi morali deljenje svojih podatkov potrošniki razumeti v kontekstu menjave vrednosti in razumeti prednosti tega.

> You know, brand owners have at stake their reputation with consumers. So this is why we're very keen to make sure that when data has been collected, it has been collected in a manner with which people are comfortable. And we also check the idea that, if you want to collect data from people, it needs to happen in a value exchange. The people need to see a benefit to that. It can't be just a one-way street. (Oglaševalec 2, osebni intervju, 2017, 7. februar)

Ne glede na izražena mnenja in zagotovila sogovornikov iz panoge (vedenjskega) oglaševanja pa je nesporno dejstvo, da uporabniki čedalje pogosteje uporabljajo protireklamne vtičnike, tehnologije, ki bodisi zaustavijo le prikazovanje oglasov bodisi prekinejo celotno komunikacijo uporabnika z oglaševalskimi strežniki – torej prekinejo tudi zbiranje podatkov o uporabnikih, na podlagi katerih so nato postreženi oglasi.

6.2 Vedenjsko oglaševanje in vpliv na pravice uporabnikov elektronskih komunikacij

V drugem sklopu smo najprej obravnavali negativni vpliv, ki ga ima vedenjsko oglaševanje na uporabnike elektronskih komunikacij, in sicer izzive za zasebnost in varstvo osebnih podatkov, ujetosti v mehurčke, diskriminacijo in izzive, ki jih prinaša mikro ciljanje za politične namene za pravico do obveščenosti in do svobodnih volitev. Dalje smo raziskali,

kakšne mehanizme imajo posamezniki na voljo za obrambo svojih pravic (predvsem zasebnosti prijazne tehnologije), ali in kako jih uporabljajo, in ali so učinkoviti.

6.2.1 Izzivi vedenjskega oglaševanja za posameznike in družbene procese

Oglaševalec 3 poudarja, da elektronskih komunikacijskih storitev pravzaprav ni mogoče uporabljati, ne da bi pri tem prihajalo do obdelave uporabnikovih podatkov za najrazličnejše namene, od zagotavljanja varnosti do merjenja. Eden od namenov pa je lahko tudi vedenjsko oglaševanje. Zato se mu zdi zavajajoče ponujati možnost brez sledenja, saj se bo to vseeno zgodilo:

> One of the false choices is: I don't want to be tracked at all, because collection of this data happen. There's no real ways to currently use the internet in a way that does not have this data collection occurring, at least for purposes like anti-fraud, security, measurement, analytics. […] Few people understand that tracking data is processed, collected for many different purposes, only one of them is targeting (Oglaševalec 3, osebni intervju, 2017, 27. januar).

Na spletu in mobilnih napravah je sledenje mogoče na različne načine – s piškotki in drugimi tehnologijami, ki se naložijo na uporabnikovo napravo (svetilniki, piksli). Le peščica največjih sledilcev, spletnih velikanov (Google in Facebook), sledi skoraj vsem uporabnikom spleta (Engelhardt in Narayanan, 2016) in mobilnim napravam. Čedalje pogosteje je sledenje s sistemi prijave, ki jih ponujajo npr. Google, Facebook, različni mediji. Regulator 3 ob tem opomni, da ko se posameznik prijavi, je lahko stalno vpisan v storitev in je mogoče slediti vsakemu njegovemu premiku, čeprav se tega morda ne zaveda (Regulator 3, osebni intervju, 2017, 15. februar). Facebook ponuja svojo rešitev prijave tudi tretjim spletnim stranem, in sicer brezplačno ter tako prejme veliko podatkov o uporabnikih od tretjih strani (Evropska komisija, 2018a, str. 78–89). Čedalje pogostejše je tudi sledenje in na podlagi odtisa naprave. Nekateri poudarjajo, da so take prakse razlog, da ljudje čedalje pogosteje uporabljajo protireklamne vtičnike (Oglaševalec 3, osebni intervju, 2017, 27. januar).

Možnosti obdelave najrazličnejših podatkov, od demografskih pa do podatkov o vedenju in stališčih, občutljivih osebnih podatkov in lokacij se nezadržno širijo, predvsem ob upoštevanju razmaha uporabe mobilnih naprav in naprav, povezanih v internet stvari (WP29, 2014). Z evropskega vidika vsa ta podjetja obdelujejo osebne podatke; ne glede na obstoj pravne prakse in zakonskih določb o tem, kaj je osebni podatek, ter mnenj pristojnih organov, pa lahko v panogi najdemo tudi drugačna mnenja – da ponudniki digitalnih oglaševalskih

storitev (DSPji in SSPji) ne obdelujejo osebnih podatkov ter da ni tveganja za zasebnost uporabnika, saj podjetij točno določen posameznik niti ne zanima niti podatkov ne morejo povezati z imenom in priimkom, če nimajo npr. sistema prijave ali se uporabniki ne prijavijo sami:

> Mi, ponudniki tehnologije, DSPji, SSPji, vsa ta fama, ki smo deležni največje gonje birokratov, smo nedolžne ovčke, v primerjavi s Facebookom. [M]i nimamo nobenih osebnih podatkov, nikamor se ne logiraš. Mi zbiramo samo ID in na osnovi njega želimo izbirati potencialnega kupca. […] Ampak tu not ni nobenih imen in priimkov. […] Imaš pa Facebook, ki pa dejansko ve, kdo so te ljudje in kaj delajo. (Oglaševalec 1, osebni intervju, 2017, 16. januar)

Poudarjena so bila različna tveganja, ki jih prakse vedenjskega oglaševanja in s tem povezanega sledenja in profiliranja prinašajo za posameznike:

1. Zasebnost, uporaba podatkov za druge namene in družba nadzora

Sledenje posameznikovim aktivnostim za namen oglaševanja ima negativne posledice za njegovo zasebnost. Sledenje ima nedvomno ekonomske prednosti za korporacije, a Zagovornik 3 opozarja, da je težko videti koristi za državljane (Zagovornik 3, osebni intervju, 2017, 16. februar). Uporabniki s sledenjem niso seznanjeni in ne razumejo, kako se podatki o tem, kaj počnejo na spletu, uporabljajo, čeprav so danes že zelo pogosta obvestila o piškotkih, ki pa realno ne dosežejo večje obveščenosti posameznikov, saj posamezniki najpogosteje nimajo druge izbire, kot da se strinjajo, še posebej, kadar je privolitev privzeto podana (Zagovornik 3, osebni intervju, 2017, 16. februar). Poleg tega sledenje za namen vedenjskega oglaševanja poteka tudi na drugih napravah v okviru interneta stvari, kjer se lahko podatki različnih senzorjev v napravah prav tako uporabijo za izdelavo profilov in nato vedenjsko oglaševanje (npr. podatki o teku iz tekaške zapestnice, na podlagi katerih oglašuje proizvajalec izotoničnih napitkov):

> Recimo internet of things, ko ga gledaš, to je nazi Germany […] Pravijo, ni slabe tehnologije. Ja, je slaba tehnologija. Oziroma programiranje, ki ima v svojem bistvu vdelane neke škodljive mehanizme, ki jih noben ne zna izklopit […] Programerji, ki to delajo, pa ne vejo oz. ne razmišljajo o posledicah, pa se jim zdi brez veze. (Zagovornik 2, osebni intervju, 2017, 11. januar)

Dodatno raven problematiki doda uporaba že zbranih podatkov o posamezniku za druge namene, drugačne od prvotnih, npr. za državno varnost, zavarovalništvo, bančne ocene kreditne sposobnosti (»*all data is credit data*«), ter pojavnost vseprisotnega nadzora z ogromnimi zbirkami podatkov:

> Dokler to segmentiranje in obdelava podatkov posameznika poteka v enem zaprtem loncu, kjer je to vezano na marketing, na potrošniške navade. A misliš, da je nemogoče […] da v prihodnosti res pridemo do tega strahovitega efekta velikega brata, ko bodo vsi naši podatki na enem mestu, […]. Tisti, ki bo imel oblast nad to enormno bazo podatkov o posamezniku, bo imel strahovito moč. (Svetovalec 3, osebni intervju, 2017, 13. januar)

2. Diskriminacija, profiliranje, algoritmi in umetna inteligenca

Nove možnosti analiz podatkov, ki temeljijo na umetni inteligenci, strojnem učenju in algoritmih, omogočajo pridobivanje zelo specifičnih podatkov prek sklepanja iz neobčutljivih podatkov ali celo na videz neosebnih podatkov in nadaljnjem profiliranju posameznikov, ki zaradi prikritosti takih postopkov ne morejo učinkovito posredovati (Demos, 2018, str. 1–7). Profiliranje kot del procesa vedenjskega oglaševanja zbuja vprašanja glede diskriminacije uporabnikov na podlagi njihovih ranljivosti, npr. socialnega statusa, rase in nacionalne pripadnosti, spolne usmerjenosti ipd., sploh v okoljih, v katerih zakonodaja ne postavlja posebnih omejitev za obdelavo teh podatkov za namen trženja, npr. v ZDA (Zuiderveen Borgesius, 2014; FTC, 2014; Demos, 2018; idr.). Profiliranje za namen cenovne diskriminacije je posebej uporabno v zavarovalniškem sektorju in bančništvu:

> […] mi bomo razvili sistem, po katerem bomo ugotavljali, kateri vozniki so bolj agresivni, in prišli smo do zaključka, da so vozniki rdečih avtomobilov bolj agresivni. A lahko mi ponudimo višjo ceno zavarovanja voznikom, ki vozijo rdeče avte?« (Svetovalec 3, osebni intervju, 2017, 13. januar). »In tukaj, tukaj, pa vsak potrošnik po moje razume, da to kar se v ozadju dogaja, ko sistem predvidi, koliko si ti res nujno eno stvar želiš, ali pa da jo nujno potrebuješ […] in potem glede na to tvojo stisko ne nazadnje lahko tudi […] ti viša ceno. (Svetovalec 3, osebni intervju, 2017, 13. januar)

Problematično je profiliranje na podlagi napačnih ali netočnih vhodnih podatkov, ki lahko za posameznika pomeni veliko težavo, če je zaradi rezultata profiliranja diskriminiran, mu je omejen dostop do dobrin ali podobno (Svetovalec 3, osebni intervju, 2017, 13. januar). Glede tega so bistvena vprašanja transparentnosti pri uporabi algoritmov in avtomatiziranega odločanja ter posameznikove možnosti vpliva na avtomatizirane odločitve. Posameznik namreč pogosto ne ve, da je bil profiliran, niti na kakšnih podatkih je profil utemeljen ter tudi nima možnosti, da bi lahko zahteval popravek podatkov ali izbris (Zagovornik 2, osebni intervju, 2017, 11. januar; Svetovalec 3, osebni intervju, 2017, 13. januar). V Franciji so denimo sprejeli zakonodajo, ki javnemu sektorju nalaga določeno transparentnost pri uporabi algoritmov in avtomatiziranega odločanja, ki zajema tudi etično plat problematike, ne le vprašanja varstva osebnih podatkov (Regulator 2, osebni intervju, 2017, 31. marec). Zahteve po razkritju delovanja algoritma pa pogosto trčijo ob argument varovanja intelektualne lastnine.

3. Ožanje izbire (t. i. filtre bubbles)

Ena od posledic profiliranja je tudi oženje izbire, ki je posamezniku na voljo, saj profil vedno temelji na zgodovinskih podatkih ter predvidevanju, kaj bo posameznika zanimalo v prihodnosti:

> Profiliranje, ki ga piškotki seveda omogočajo, oži našo izbiro – a res jaz hočem, da sistem namesto mene odloča, da če jaz ne vem – jem samo čokolade Milka, da mi Lindtovih recimo sploh ne bo več ponudil in bo sistem namesto mene sprejel neko odločitev. […] [N]a kratek rok je mogoče še zate v redu, da se sistem namesto tebe odloča, na dolgi rok pa po moje ne, zato ker bo tvoje polje izbire tako ozko, pa na dolgi rok boš ti prikrajšan za določene stvari, no, mogoče je to bolj pravi izraz. (Svetovalec 3, osebni intervju, 2017, 13. januar)

V tem procesu so lahko vhodni podatki neoptimalni in tako ne kažejo resničnih interesov posameznika (lahko so netočni, zastareli, vezani le na posamezen kontekst), lahko je napaka tudi v postopku predvidevanja, ker algoritem ni optimalno predvidel prihodnjih interesov posameznika. Posledica vsega tega je ujetost posameznika v t. i. *filtre bubbles*, *echo chambers* ipd., v katerih so mu vedno znova ponujene enake stvari, kot so ga zanimale v preteklosti, ni pa mu na voljo vsebina, ki bi ga zanimala na novo, kreativno, hipno. Velika razlika je tudi v kontekstu uporabe podatkov:

> Problem vseh teh optimizacij je samo to, da bolj ko optimiziraš, bolj postaneš slep za karkoli izven tega. Kar pomeni, vsi ti modeli so kronično nezanesljivi pri napovedovanju nepredvidljivih dogodkov. […] [S]tvar, ki jo sedaj zelo veliko preučujejo, učinek teh echo chambersov in filter bubblov. […] Imamo le zgodovinske podatke in zdaj reči, če imaš ti močan historičen vzorec, če bi kdo kvantificiral 20 let tvojega življenja, lahko z določeno gotovostjo določene stvari napoveduje, ne pa vseh. Je tudi stvar industrije, jaz si predstavljam, da za enega zavarovalniškega analitika, pa recimo da smo v enem bloku, smo ena familija pa druga familija […]. Oni so bolj katoliški, hodijo k maši, so taki bolj poštirkana familija, mi pa malo manj recimo. Kar pomeni, volimo čisto druge politike, hodimo gledat druge filme, na eni ravni smo si ful različni […]. Z vidika enega zavarovalniškega agenta, ki nam prodaja določene oblike zavarovanj, smo mi tako rekoč identični. Za enega političnega analitika pa ne. (Medij 3, osebni intervju, 2017, 11. julij)

4. Pravica do informiranosti in pravica do svobodnih volitev

Napredek v podatkovnem trženju sežejo tudi na politično področje. Volitve namreč postajajo čedalje bolj podprte s podatkovnimi storitvami, ki jih za politične stranke izvajajo specializirana podjetja in analitiki podatkov, ter so usmerjena v sofisticirano segmentacijo volivcev in vedenjsko ciljanje političnih sporočil – t. i. mikro ciljanje. Politične kampanje kombinirajo svoje podatke o volivcih in njihovem vedenju s komercialnimi podatki, pridobljenimi od ponudnikov teh storitev na trgu, da lahko zgradijo natančnejše profile volivcev (EDPS, 2018; Goodman in drugi, 2017; COE, 2017). Regulator 1 meni, da je taka uporaba in zloraba spletnih oglaševalskih sistemov za politično trženje veliko večji problem

kot vedenjsko oglaševanje običajnih produktov, saj so podatki uporabnikov uporabljeni za manipulacijo državljanov, za napovedovanje njihovih političnih stališč in nagnjenj ter za to, da je mogoče vplivati na izide volitev v korist posameznega kandidata.

> But still, there are bigger problems in the world not just advertising. What the risk of having a behavioural advertising network or ecosystem could be for a functioning democracy. […] This is more about in this history of fake news and alternative facts and the role of journalists and the mechanism, the infrastructure of targeted advertising that you can easily abuse and misuse to manipulate public opinion in order to influence outcomes of who's going to be in the leadership of the democracy. (Regulator 1, osebni intervju, 2017, 15. februar).

Taka praksa odpira širša vprašanja kot le zasebnost in Svetovalec 4 poudarja, da tega ne sprejema (Svetovalec 4, osebni intervju, 2017, 14. marec). Korporacije imajo tako veliko moč, ki je lahko zlorabljena za manipulacijo volivcev, da volijo določenega kandidata, čeprav lahko prinaša tudi določene prednosti, npr. boljše informiranje posameznikov (Zagovornik 3, osebni intervju, 2017, 16. februar). V izrabi vedenjskega oglaševanja na področju politične promocije Regulator 4 vidi različna tveganja, glede tega, kako posamezniki izrabljajo dostop do informacij, kako to vpliva na njihovo intelektualno zasebnosti in kako iščejo informacije na spletu, glede raznolikosti stališč, izraženih na spletu in glede tega, kako so posamezniki dejansko vpeti v politični proces in kako se izrazijo na volitvah; na tnalu je veliko več kot le zasebnost (Regulator 4, osebni intervju, 2017, 16. februar).

Poleg tega ni lahko razlikovati med podatki, ki so politično občutljivi, in tistimi, ki to niso, ter za rešitev problematike le zahtevati dodatna varovala za občutljive podatke. Iz zelo »navadnih« podatkov o osebi je mogoče sklepati o njenih političnih prepričanjih oz. osebnostnih potezah, zaradi katerih bo te posameznike lažje prepričevati, kot izhaja iz primera Cambridge Analytica. Izražena je bila kritika, da je v primeru Cambridge Analytica/Facebook odpovedal tudi sistem nadzora, čeprav je to veliko analitično podjetje, pa so vseeno njihove aktivnosti dolgo potekale neopažene (Svetovalec 4, osebni intervju, 2017, 14. marec). Nadzorni organi so od razkritja te zgodbe sicer sprožili že veliko postopkov na različnih ravneh – tudi prek sodelovanja s pristojnimi organi v tretjih državah (ICO, 2018, str. a, b).

6.2.2 Mehanizmi za zaščito uporabnikov pred vedenjskim oglaševanjem in sledenjem

Posamezniki imajo na voljo široke možnosti za varovanje svoje zasebnosti pri vedenjskem oglaševanju. Obstajajo nastavitve v aplikacijah, ki preprečujejo zbiranje podatkov (npr.

mehanizmi za soglasje glede uporabe piškotkov na spletnih straneh), preprečujejo deljenje podatkov z uporabo zasebnega brskanja (prek nastavitev v brskalniku), lahko preprečujejo obdelavo podatkov za vedenjsko oglaševanje (prek sistema samoregulacije) (Evropska komisija, 2017; IAB, 2016; idr.).

Ugotovitve empiričnega dela kažejo, da so mehanizmi, pri katerih ima posameznik možnost, da se izrazi glede svojih preferenc o zasebnosti, precej neučinkoviti, saj se posamezniki za to le redko odločijo: »Problem je v tem, da uporabniki tega dejansko ne razumejo, vsi klikamo samo 'v redu', ker te nekaj moti in to je to. Ne dosega svojega namena« (Medij 1, osebni intervju, 2017, 13. januar). Eden od izdajateljev je uporabnikom na obvestilu o piškotkih ponudil možnost, da zavrnejo piškotke za napredne oglaševalske funkcije, pa vendar je to možnost izrabilo zelo malo posameznikov, preostali so kliknili na polje »strinjam se« in tako soglašali z vsemi piškotki. Osipa tako niti ni bilo: »Ne, sploh ne. Sploh nimamo dejansko izmerjenega. Vem, da to stran, kjer lahko izbiraš, […] gledal sem leto nazaj, ne vem, če je bilo 200 obiskov v enem mesecu.« (Medij 1, osebni intervju, 2017, 13. januar).

Med razlogi za to je bilo poudarjeno, da je na slabo tehnično podkovanega posameznika preloženo preveliko breme obrambe svojih pravic, pri čemer pogosto niti ne ve, da se njegovi podatki obdelujejo, zakaj se obdelujejo in kakšne so posledice take obdelave, da večina brezplačnih storitev na spletu dejansko temelji na prihodkih, povezanih z obdelavo podatkov uporabnikov in da sledenju skoraj ni mogoče ubežati (Regulator 4, osebni intervju, 2017, 16. februar).

Za današnje generacije uporabnikov spleta naj bi bilo tudi značilno, da poseg v zasebnost dojemajo bolj v fizičnem smislu (Zagovornik 1, osebni intervju, 2017, 26. januar) in da svojo dejavnost na spletu dojemajo drugače od dejavnosti v »realnem« življenju, ki ima otipljive posledic: »[D]ejstvo je, ko uporabljaš te zadeve, nimaš občutka, da je to del tega sveta, in se ti zdi, da je to oddaljeno, ne samo geografsko, ampak tudi na neki način ideološko, da to je nekje drugje. Ni tukaj. To, kar delaš na internetu, ni to, kar delaš offline, v normalnem svetu« (Zagovornik 2, osebni intervju, 2017, 11. januar). Drugi razlog je slabo delovanje teh mehanizmov (Zagovornik 5, osebni intervju, 2017, 13. marec) oziroma nespoštovanje preferenc uporabnika s strani oglaševalske panoge (Oglaševalec 3, osebni intervju, 2017, 27. januar). Zato posebej regulatorji in sogovorniki iz nevladnega sektorja menijo, da uporabniki

ne morejo učinkovito izrabljati možnosti in tehnologij, ki so jim na voljo, da bi preprečili ali zmanjšali posege v svoje pravice (npr. z uporabo zasebnosti prijaznih tehnologij – PETs, zavrnitev piškotkov): Zagovornik 3 poudari, da niti sam, kljub temu, da se s tem področjem ukvarja, ne ve točno, kaj se dogaja z njegovimi podatki, ko mora sprejeti določene piškotke ali druge sledilne tehnologije. Kdo dobi podatke, kdo jih uporablja in za kakšen namen. Ne ve, ali so o njem sprejete odločitve, brez da bi bil o tem obveščen (Zagovornik 3, osebni intervju, 2017, 16. februar).

Eden od zanimivih argumentov je tudi, da celotna panoga tehnoloških rešitev sloni na podmeni preprostosti uporabe za uporabnika in da ta ni več navajen odločanja v posameznih korakih nastavitev oziroma ni več navajen, da ima v procesih možnosti izbire (Zagovornik 2, osebni intervju, 2017, 11. januar). Dodatna težava je vezanost procesov na nekega ponudnika (angl. *lock-in*), ki je prav tako ovira za prehod na uporabo zasebnosti prijaznih storitev (Zagovornik 2, osebni intervju, 2017, 11. januar).

Blokiranje oglasov s pomočjo protireklamnih vtičnikov je ena najpogosteje uporabljanih tehnologij za varovanje zasebnosti. Prepreči namreč tok podatkov od uporabnika do oglaševalskih strežnikov, kar je učinkovito, ko gre za sledenje s piškotki, manj pa pri sledenju po drugih identifikatorjih (Regulator 3, osebni intervju, 2017, 15. februar; Oglaševalec 3, osebni intervju, 2017, 27. januar). Oglaševalec 3 pojasnjuje, da se glede na nekatere raziskave uporabniki za protireklamne vtičnike odločajo iz različnih vzgibov, med drugim zaradi zavarovanja (30%), slabe uporabniške izkušnje (29%), zaradi počasnejšega nalaganja strani (16%), zaradi prevelikega števila oglasov (14%) in tudi zaradi zasebnosti (6%). Poudari, da ga uporablja zaradi slabe uporabniške izkušnje, tudi na svoji službeni napravi, saj se mu zdijo nekatere spletne strani neznosne zaradi oglasov (Oglaševalec 3, osebni intervju, 2017, 27. januar).

Ad tech panogo čedalje večja raba protireklamnih vtičnikov zelo skrbi – predvsem založnike (Medij 1, osebni intervju, 2017, 13. januar). Glavnina uporabnikov protireklamnih vtičnikov so napredni uporabniki spleta, kar je za založnike težava (Medij 1, osebni intervju, 2017, 13. januar). Oglaševalec 3 pojasnjuje ekonomiko protireklamnih vtičnikov. Oglaševalcev njihova uporaba ne prizadene tako zelo, saj prikazovanje oglasov ljudem, ki uporabljajo protireklamne vtičnike razumejo kot prikazovanje oglasov manj relevantnim potrošnikom. Udarec pomenijo

predvsem za založnike, ki nenadoma beležijo 25% padec prihodkov. V Evropi tudi 40% pri nekaterih publikacijah; lahko tudi 40%, 50%, 60% upad, če so njihova ciljna skupina poznavalci tehnologije. To za njih pomeni paniko (Oglaševalec 3, osebni intervju, 2017, 27. januar).

Zato se založniki ozirajo po načinih za obid protireklamnih vtičnikov. Tehnični načini obida so učinkoviti le, če vplivajo na uporabnikov nadzor nad brskalnikom (Oglaševalec 3, osebni intervju, 2017, 27. januar), hkrati pa gre za tesno tekmo med sposobnostmi protireklamnih vtičnikov in načini založnikov za spopadanje z njimi (Regulator 4, osebni intervju, 2017, 16. februar), saj tudi protireklamni vtičniki postajajo bolj sofisticirani in lahko preprečijo založniku, da prepozna, da jih uporabnik uporablja. Poudarjeno je bilo, da bi založniki ravnali odgovorneje, če bi uporabnikom predstavili, da gre za menjavo vrednosti in da morajo izklopiti protireklamni vtičnik, če želijo brezplačno dostopati do vsebin na spletni strani. Prav tako že potekajo panožne pobude, da bi oglasi delovali bolje in manj moteče (Oglaševalec 3, osebni intervju, 2017, 27. januar).

Poleg blokiranja oglasov prihajajo v uporabo tudi sredstva, s katerimi uporabnik lahko vpliva na to, kakšne podatke zmore nekdo zbrati o njem, tako da v dostopne podatke vnaša šum, napačne podatke, ki popačijo sliko o posamezniku. Profil uporabnika tako ni več točen, s čimer se je mogoče izogniti ujetosti v mehurček vedno iste ponudbe (angl. *data obfuscation, randomization*) (Medij 3, osebni intervju, 2017, 11. julij). Oziroma lahko uporabnik izboljša kakovost podatkov, ki so na voljo o njem tako, da posreduje dodatne informacije in tako izboljša svoj profil. Zagovornik 4 omeni projekt, ki nastaja v sodelovanju z bankami in zavarovalnicami, da bi posamezniki imeli več nadzora nad svojimi podatki, z orodji, s katerimi bi lahko optimizirali podatke o svojem zdravju ali financah (Zagovornik 4, osebni intervju, 2017, 8. februar).

Iz realnosti »plačevanja« za digitalne storitve z osebnimi podatki izhajajo zamisli o kvantificiranju vrednosti osebnih podatkov kot neke vrste »plačilnega« sredstva (Zagovornik 1, osebni intervju, 2017, 26. januar). Na podlagi določene vrednosti osebnega podatka naj bi posameznik imel moč, da se pogaja s ponudnikom storitve. Eden od sogovornikov je poudaril orodje za določitev vrednosti podatkov[79] v obliki vtičnika, ki na podlagi brskanja uporabnika

[79] EU Projekt TYPES – data valuation tool

določa, koliko so njegovi podatki o brskanju vredni Facebooku. Meni, da bi z uporabo vtičnika posamezniki lahko bolje razumeli, da (1) vsak klik pomeni zaslužek za nekoga, torej imajo osebni podatki ekonomsko vrednost in da (2) je trg digitalnega oglaševanja zelo kompleksen, zato osebni podatki nimajo fiksne cene, ampak je vrednost odvisna od tega, koliko je nekdo v nekem trenutku zanje pripravljen plačati (Zagovornik 1, osebni intervju, 2017, 26. januar). S pomočjo takega vtičnika naj bi bil uporabnik informiran in opolnomočen glede menjalne vrednosti svojih podatkov (Zagovornik 4, osebni intervju, 2017, 8. februar).

Kljub prednostim, ki jih zasebnosti prijazne tehnologije prinašajo, in funkcionalnostim, ki jih omogočajo, te običajno ne dosežejo širšega občinstva. Sogovorniki med razlogi za to poudarjajo tudi praktične vidike težavnosti namestitve in uporabe za povprečnega uporabnika, ki ni tehnično podkovan. Za običajnega uporabnika naj bi bile primerne predvsem rešitve, ki zahtevajo »en klik« (Zagovornik 1, osebni intervju, 2017, 26. januar). Regulator 2 kot težavo izpostavlja tudi kakovost delovanja oziroma nezadostno preprečevanje sledenja in oglaševanja ter vprašanje ekonomske koristi za izvajalce spletnega sledenja in oglaševanja, ki bi uporabljali zasebnosti prijazne rešitve (npr. *privacy preserving re-targeting system*). Te so lahko drage za implementacijo in če ni dovolj uporabnikov, ki bi jih uporabljali, ponudniki ne najdejo ekonomskega argumenta za implementacijo. Če jih ne uporabljajo tekmeci, je prav tako problem, saj to pomeni slabost. Če ni nadzora, izvajalci vedenjskega oglaševanja prav tako nimajo prave motivacije za implementacijo zasebnosti prijaznih rešitev (Regulator 2, osebni intervju, 2017, 31. marec). Pogosto zasebnosti prijazne tehnologije prihajajo iz akademskih in raziskovalnih krogov, ki pa imajo neredko težave z rednim financiranjem in tako s prehodom v vsakdanjo rabo v panogi (Zagovornik 1, osebni intervju, 2017, 26. januar).

6.3 Razvoj in trenutne razmere na področju regulacije vedenjskega oglaševanja

Tretji sklop ugotovitev iz ekspertnih intervjujev zajema razvoj in trenutne razmere na področju regulacije vedenjskega oglaševanja. Dokumentarna analiza regulatornega okvira je pokazala, da je ta trenutno pester, neenoten v zahtevah in zato precej neučinkovit. To lahko pripišemo tako nejasnim pravilom kot tudi zelo pomanjkljivemu nadzoru in čezmejnosti oglaševalskih aktivnosti, ki nadzor otežuje: »[M]islimo, da je na globalnem trgu Evropa silver bullet. Ni. Moraš upoštevati še Kitajsko, Rusijo, Ameriko« (Zagovornik 2, osebni intervju, 2017, 11. januar). Mednarodna regulacija interneta je zelo kompleksna: »Tukaj nastane en

velik problem o tem, kako v mednarodnem pravnem okolju regulirati internet. *Global law of the net* ne obstaja« (Svetovalec 3, osebni intervju, 2017, 13. januar). Interesi različnih držav pa so pri regulaciji različni, kar se kaže tudi v praksi (npr. pri možnostih implementacije standarda ne sledi): »[O]*pt-out* v ZDA, v EU bomo šli na *opt-in*, pa bodo *browserji* to omogočali glede na jurisdikcijo. In smo se tudi takrat začeli pogovarjati o tem, ali bomo mi res dobili dva interneta« (Svetovalec 3, osebni intervju, 2017, 13. januar).

6.3.1 Varovanje zasebnosti v ZDA in v EU: varstvo osebnih podatkov kot temeljna človekova pravica ali kot potrošniška pravica

V EU je pravica do zasebnosti in varstva osebnih podatkov varovana kot temeljna človekova pravica, v ZDA pa varovanje osebnih podatkov spada v okvir varovanja potrošnikovih pravic (npr. Cunningham, 2015; Zuiderveen Borgesius, 2014; itd.), kjer so pomembni koncepti izogibanja zavajanja potrošnikov in nepoštenih praks: Oglaševalec 3 meni, da je tak koncept dober. Načela poštenosti v odnosih med korporacijami in posamezniki ter izogibanja škodovanju potrošnikom so vključena v vso federalno zakonodajo in to naj bi bil dober temelj (Oglaševalec 3, osebni intervju, 2017, 27. januar).

Težava je v omejenih možnostih nadzora, ki jih ima ameriški nadzorni organ Zvezna komisija za trgovino (*Federal Trade Commission* – FTC). To pa je posledica omejene politične volje za strožji nadzor na področju hitro razvijajočih tehnoloških storitev, ki poganjajo ekonomijo ZDA. (Confessore, 2018; Glaser, 2018; Singer, 2016). FTC mora nadzor nad vprašanji zasebnosti graditi iz temeljev pravil za varovanje potrošnikov, saj je glavna motivacija večine kongresa, da omogočajo poslovnemu svetu delovanje brez posebnih pravnih ovir (Oglaševalec 3, osebni intervju, 2017, 27. januar). Je pa na tem področju v ZDA zelo močan pritisk nevladnih organizacij (Zagovornik 2, osebni intervju, 2017, 11. januar). Kljub temu analiza pravnega okvira kaže, da je regulator obravnaval že precejšnje število primerov podjetij s področja vedenjskega oglaševanja in jim naložil kazni ter ukrepe (FTC. 2012; FTC, 2015; FTC, 2016; itd.), vendar pa ukrepi predvsem zadevajo boljše obveščanje o praksah sledenja, ne omejijo pa sledenja samega.

Po drugi strani ima tudi sistem, kot ga poznamo v EU, torej varovanje zasebnosti in osebnih podatkov kot temeljno človekovo pravico, pomanjkljivosti. Varstvo osebnih podatkov kot

temeljno pravico naj bi bilo čedalje težje vzdrževati in udejanjati, saj so podatki preprosto povsod. Vse naše dejavnosti temeljijo na obdelavi osebnih podatkov in njihovo varovanje prav v vseh situacijah, tudi tam, kjer ni posebnega tveganja za škodo posamezniku, je omejujoče. Svetovalec 4 poudarja, da v imamo v EU različne temeljne pravice, ne le pravico do varstva osebnih podatkov, pač pa tudi pravico do ekonomske aktivnosti, do življenja, varovanja zdravja, pravico do svobode govora in da je usklajevanje teh pravic zelo težka naloga (Svetovalec 4, osebni intervju, 2017, 14. marec).

Razlike med regulacijo vedenjskega oglaševanja v ZDA in EU se kažejo v temeljnih konceptih regulacije. V ZDA je poudarek na tem, da je posameznik obveščen o obdelavi podatkov, potem pa je odgovornost za varstvo pravice na njem samem, v EU pa že zakonodaja predpisuje, kaj podjetja smejo in česa ne smejo početi s podatki. Zagovornik 4 verjame, da okvir v ZDA preveč nalaga posamezniku, saj ta težko razume delovanje tehnologij in ga lahko zavedejo bleščeče obljube gospodarske rasti. Meni, da ZDA favorizirajo monopole velikih podatkov, medtem ko je v EU večji poudarek na pravicah, ki jih imajo posamezniki glede svojih podatkov. Poudari, da podjetja iz ZDA uničujejo zaupanje v digitalne storitve (Zagovornik 4, osebni intervju, 2017, 8. februar).

6.3.2 Razvoj regulacije glede vedenjskega oglaševanja v ZDA in EU

Zakonodaja za varstvo osebnih podatkov in varovanje zasebnosti v ZDA in EU

Ameriška zakonodaja na zvezni ravni vsebuje le malo pravil glede varovanja osebnih podatkov uporabnikov elektronskih komunikacij, razen tega, da imajo podjetja objavljene politike zasebnosti in še to pri manjših pogosto umanjka. Samoregulacija dodaja obveznost objave določenih informacij. Nadzor, če podjetja ravnajo v skladu s svojimi obvestili, izvaja regulator (Oglaševalec 3, osebni intervju, 2017, 27. januar).

V ZDA že več let spodletijo vsi poskusi za sprejetje enotne zvezne zakonodaje, ki bi varovala uporabnike elektronskih komunikacij. Razlog za to je v politični volji desnice in levice za spodbude in ne za omejevanje ponudnikov storitev digitalnih tehnologij, ki imajo globalno prevlado.

> I don’t think the American political system is designed anymore to make fundamental changes to the relationship between commercial businesses and people. I think that the American political system, both right and left is essentially run for – by different competing economic interests. […] I don’t believe them as evil, they’re not. They’re just relentless pursuers of their business interests. […] There’s very little political ability to make those kinds of changes because there’s too many people who would be upset by them. (Oglaševalec 3, osebni intervju, 2017, 27. januar)

Poudarjeno je bilo, da so spletni velikani zelo ranljivi, saj svojega poslovnega modela ne morejo veliko spreminjati, ne da bi jim zelo škodilo, če se veliko držav odloči za strogo regulacijo:

> [Č]e se iz takih ali drugačnih razlogov dosti držav odloči za eno tako dosti neugodno regulacijo, ki ne bi bilo le samo, plačaj dve milijardi, ni panike, ampak tisto, it na toliko in toliko procentov tega, dokler ne spremeniš prakse, na spremenit prakso so pa izredno ranljivi. Ne morejo si privoščiti zelo spreminjati te prakse. (Medij 3, osebni intervju, 2017, 11. julij)

Omenjen je bil kontekst drugih monopolov v zgodovini, kjer so monopolisti sami na neki točki želeli regulacijo:

> [K]o so tudi te železniški in naftni ameriški baroni prej ali pa kasneje šli v kongres, pa rekli 'now please regulate us', […] ko bodo ratali zrela industrija, ali pa tudi ko bodo oni zaslutili, da lahko njih ogrozijo podobne prakse, s katerimi so oni akumulirali kapital, bodo hoteli postavit pravila. (Medij 3, osebni intervju, 2017, 11. julij)

V Evropi je sistem varovanja pravic uporabnikov elektronskih komunikacij pri spletnem sledenju in vedenjskem oglaševanju v EU utemeljen na zakonodaji, Direktivi 2002/58/ES, ki zahteva privolitve v piškotke. Ta določba naj bi bila le delno učinkovita (Evropska komisija, 2017, str. 134–137), kar potrjujejo tudi eksperti: »Zdaj [je] tako, da je volk sit in koza cela […] [D]al smo nekaj gor in gremo naprej, zadaj pa se vse sorte dogaja« (Svetovalec 1, osebni intervju, 2017, 23. januar). Poudarjeno je bilo, da sistemi dejansko ne delujejo, kot bi morali: »Noben nima to zrihtano. […] Večina nima.« (Medij 2, osebni intervju, 2017, 13. januar).

Panoga je že ob sprejemu takih pravil imela velike pomisleke, da bodo zahteve po soglasju v uporabo piškotkov uničile svet svobodnega interneta: »A so bili strahovi 100 % upravičeni ali ne, […] so pač neki učinki bili, ampak na dolgi rok […] to so šoki ob uvedbi novosti. Če bi gledali trendno linijo, nekih večjih pretresov dejansko ni bilo« (Svetovalec 1, osebni intervju, 2017, 23. januar). Da je zakonodaja na tem področju, ki se hitro tehnološko spreminja, zastarela, že ko je sprejeta, je še eden od pomislekov (Svetovalec 1, osebni intervju, 2017, 23. januar). Poudarjeno je bilo, da »dejansko sistemi ne delujejo, kot bi morali« (Oglaševalec, 3, osebni intervju, 2017str. 10) ter problematika neprijetne uporabniške izkušnje, ker je »treba

klikat na vsaki spletni strani sprejmem piškotke/ne sprejmem piškotke – piškotkov« (Svetovalec 3, osebni intervju, 2017, 13. januar). Uporabniki niso seznanjeni s temi praksami, da bi lahko pomenljivo udejanjali svojo možnost podaje privolitve. Ker so piškotki le ena od tehnologij sledenja, je taka regulacija neučinkovita:

> Ko je prišla ven *cookie* direktiva, sem rekel, to ne more delovati zaradi dveh zadev, eno je zato, ker so bili že takrat *cookiji* irelevantna tehnologija, in B, do tistega trenutka ljudje niso vedeli, da to obstaja. Ne samo, da si ljudem povedal, da obstaja, ampak si v isti sapi rekel, da je to *bad*. […] V določenih primerih to nima nobenega smisla, samo ljudje se sekirajo, al jim gre nekaj na živce, imajo negativne občutke od tega, nobene koristi. […] [C]*ookiji* niso vse, pa so šli na *tracking* preko IP-ja oz. prek nekih teh *behavioural* pa tega. […] [T]o je, kot da bi čoln imel pet lukenj, ti pa bi mašil največjo. Saj nekaj pomaga, ampak tam so še štiri luknje. (Zagovornik 2, osebni intervju, 2017, 11. januar)

Nadzor nad pravili o piškotkih je bil v državah članicah zelo različen, prav tako rešitve, ki so vzniknile. Posebej priljubljeni so postali »zidovi« (angl. *cookie walls*), pri katerih se je uporabnik moral strinjati z uporabo vseh piškotkov, tudi tistih za vedenjsko oglaševanje, preden je lahko nadaljeval do vsebine. Številni nadzorni organi so se sicer izrekli proti takim rešitvam (Zagovornik 5, osebni intervju, 2017, 13. marec), vendar Regulator 1 izpostavlja, da je še vedno vprašanje, ali jih je dejansko mogoče prepovedati in prisiliti ponudnike, da vsebino ponujajo vsem uporabnikom, saj gre za tržno gospodarstvo in ta argument pretehta nad argumentom varovanja zasebnosti. Kot lahko prodajalec na tržnici sam odloči, ali želi nekomu prodati jabolka ali pomaranče ali pa ga bo usmeril h konkurenci (Regulator 1, osebni intervju, 2017, 15. februar).

Zakonodaja v EU je sicer najbrž dosegla večjo obveščenost uporabnikov o tem, da piškotki obstajajo, ali je dejansko zmanjšala sledenje oziroma ponudila uporabnikom možnost odločanja, pa je zelo vprašljivo (Svetovalec 3, osebni intervju, 2017, 13. januar).

Samoregulacija

Samoregulacija na področju vedenjskega oglaševanja zajema predvsem kodeks *Interactive Advertising Bureau*, kot izhaja iz dokumentarne analize (poglavje 5. 3. 1). Ugotovitve kažejo dvom v učinkovitost te rešitve, saj ne preprečuje zbiranja podatkov o posamezniku, pač pa le prikazovanje oglasov. Poleg tega je spletno stran težko najti in je uporabniki ne poznajo dobro (Regulator 3, osebni intervju, 2017, 15. februar).

Zagovorniki pa menijo, da je samoregulacijski kodeks ustrezen način urejanja področja vedenjskega oglaševanja, saj deluje na informiranju posameznikov glede praks sledenja zgodovini brskanja uporabnika po spletu in jim ponuja možnost, da tako oglaševanje zavrnejo. Oglaševalec 2 pojasnjuje, da posameznik lahko klikne na ikono na oglasu in tam je pojasnilo, da je bil oglas prikazan, glede na zgodovino brskanja. Potem lahko posameznik preveri še več informacij o tem, kateri podatki se zbirajo in kako. Nato se lahko odloči, ali take oglase želi ali ne. To naj bi bila sorazmerna rešitev za obveščanje posameznikov in omogočanje zavrnitve oglasov (Oglaševalec 2, osebni intervju, 2017, 7. februar).

Ker kodeks nikoli ni vseboval zahteve po tem, da se vedenjsko oglaševanje izvaja šele po privolitvi posameznika, v EU ni dosegel posebne veljave, ampak so se nadzorni organi izrekli, da upoštevanje kodeksa samo po sebi ne zagotavlja skladnosti z zakonodajo (WP29, 2011).

Samoregulacija kot primarna strategija urejanja vedenjskega oglaševanja ima dvomljivo učinkovitost, če ni izpostavljena tako notranjemu kot tudi zunanjemu nadzoru (Svetovalec 2, osebni intervju, 2017, 25. januar). Nekateri so samoregulacijo opredelili kot zadnji panožni branik pred zunanjo regulacijo. Učinkovita je, če so zunanje grozeče sankcije zaradi tega manjše: »Saj samoregulacija nikjer ne deluje zares. […] To je čisti damage control. […] Ne bit naivna tukaj. Medijska samoregulacija, resna, se je razvila samo v okoljih, kjer je to pravna praksa privedla« (Medij 3, osebni intervju, 2017, 11. julij).

Standardizacija – ne sledi

V zadnjih letih je bilo precej prizadevanja na področju samoregulacije vedenjskega oglaševanja vloženega na področju vzpostavljanja tehničnih standardov, ki bi omogočili uporabnikov nadzor nad obdelavo podatkov na ravni brskalnika in ne na ravni vsake posamezne spletne strani, kot to zapoveduje veljavna zakonodaja. Predvsem s stališča dobre uporabnikove izkušnje in izogibanja t. i. brezvoljnosti privolitev je bila rešitev na ravni tehničnega standarda, ki bi ga implementirali brskalniki, bolj zaželena že od nastanka zakonodaje o piškotkih. Privolitev v piškotke na posameznih straneh ni bila nikoli videna kot optimalna rešitev, ampak se je kot boljša rešitev kazal standard ne sledi, ki ga pripravlja konzorcij W3C (Svetovalec 3, osebni intervju, 2017, 13. januar).

Med prednostmi standarda ne sledi so bile poudarjene naslednje točke:

- privolitev je lahko avtomatizirana in podana prek mehanizma na ravni brskalnika – ta proces je za uporabnika manj moteč, po tej poti pa ima prav tako možnost preklicati svoje soglasje in je o vsem ustrezno obveščen (Regulator 1, osebni intervju, 2017, 15. februar).
- brskalnik bi tako nastopal kot instrument, ki dela v imenu uporabnika in bi glede na izražene preference uporabnika (npr. kateri sledilci mu lahko sledijo in kateri ne) sprejemal te odločitve v odnosih s posameznimi spletnimi stranmi, s katerimi se uporabnik ne bi več pogajal neposredno, prav tako mu ne bi bilo treba uveljavljati svojih pravic nasproti posameznih strani, ampak bi to storil prek brskalnika. Tako bi lažje izražal svoj namen in prevzel nadzor nad svojimi podatki ter lažje uveljavljal svoje pravice (Regulator , osebni intervju, 2017, str. 7);
- dodana vrednost standarda je v tem, da je še pred obiskom spletne strani, še preden je naložena vsebina, mogoče videti, kdo so sledilci na tej strani, s kom se delijo podatki, ne tako kot trenutno, pri obvestilih o piškotkih, ko se obvestilo prikaže hkrati s tem, ko se piškotki že naložijo in uporabnik nima možnosti videti podatkov o sledilcih vnaprej *(*angl. *pre-flight)*. Ker so podatki vidni, lahko brskalnik skladno z vnaprej določenimi pooblastili in dovoljenji uporabnika presodi, ali je posamezna spletna stran skladna z željami uporabnika (Regulator 1, osebni intervju, 2017, 15. februar);
- uporabnikov signal ne sledi bo prejela vsaka stranka v procesu sledenja, ne le prva stran, ki jo dejansko obišče. Tako ne bo več mogoče izogibanje odgovornosti tretjih strani, ki trenutno lahko trdijo, da niso odgovorne za pridobivanje soglasja, ampak so za to odgovorne prve strani. Tudi v okviru zakonodaje ZDA bodo obstajale možnosti, da se take zavajajoče prakse tretjih strani sankcionira (Regulator 2, osebni intervju, 2017, 31. marec).

Poudarjeni so bili naslednji izzivi za standard ne sledi:

- večina uporabnikov ne bi nikoli spremenila privzete možnosti ne sledi na ravni brskalnika in aktivno izbrala možnost, da želi deljenje podatkov s tretjimi strankami, saj na ravni brskalnika še ne pride do izmenjave vrednosti – da bi uporabnik videl vrednost v tem, da dovoli deljenje svojih podatkov v zameno za storitev ali vsebino. Posledično tretje stranke, katerih poslovni model je vezan na obdelavo podatkov, ne bi mogel več delovati (Oglaševalec 2, osebni intervju, 2017, 7. februar);

- v praksi bo uporabnik kljub odločitvi ne sledi v brskalniku stalno prejemal prošnje za izjeme od obiskanih spletnih strani (Oglaševalec 2, osebni intervju, 2017, 7. februar);
- poplava vprašanj za privolitev bo povzročila, da bodo uporabniki obupani spremenili nastavitve v brskalniku, da se izognejo nadaljnjim zahtevam in slabi izkušnji brskanja (Regulator 4, osebni intervju, 2017, 16. februar);
- enkratna privolitev v sledenje za nedefinirane namene morda glede na evropski pravni okvir ne bo ustrezna rešitev(Svetovalec 2, osebni intervju, 2017, 25. januar);
- privzete nastavitve ne sledi na ravni brskalnika bodo pomenile velik udarec za digitalni ekosistem v Evropi, ki je zelo pomemben za gospodarski napredek Evrope, trenutna razprava pa se po mnenju Oglaševalca 2 preveč osredinja le na vidik zasebnosti (Oglaševalec 2, osebni intervju, 2017, 7. februar);
- vprašanje, kaj ne sledi sploh pomeni – dejansko preprečevanje sledenja uporabniku za različne namene ali le preprečevanje sledenja za namen vedenjskega oglaševanja (angl. *do not target*). Oglaševalec 3 poudarja, da tehnologija, ki preprečuje sledenje obstaja, in to so protireklamni vtičniki, medtem ko standard ne sledi ne preprečuje sledenja (Oglaševalec 3, osebni intervju, 2017, 27. januar);
- ker je to tehnična rešitev, je možno tudi, da bo panoga iznašla tehnično rešitev za zaobid upoštevanja omejitev v brskalniku in tukaj bo moral nastopiti nadzor (Regulator 2, osebni intervju, 2017, 31. marec).

6.3.3 Regulacija vedenjskega oglaševanja v širšem političnem kontekstu konkurenčnosti držav

Razvoj regulacije s področja varovanja pravic uporabnikov elektronskih komunikacij pri vedenjskem oglaševanju nikakor ne poteka v praznem prostoru, omejenem le na vprašanja zasebnosti uporabnikov in prava človekovih pravic, ter tehtanjem z ekonomskimi interesi ponudnikov storitev, ki vedenjsko oglaševanje izrabljajo za povečanje svojih prihodkov. Ključen je širši kontekst geopolitičnih odnosov med gospodarstvi tehnološko razvitih držav, ki narekuje, kakšno podjetniško okolje naj države ustvarjajo, da bodo čim bolj konkurenčne, tudi za ceno posegov v pravice uporabnikov elektronskih komunikacij. Dopuščanje posegov v zasebnost uporabnikov in razvoj tehnologije, ki na tem temelji, je del širšega spleta politik, s ciljem konkurenčnosti poslovnega okolja:

> Če bi hoteli zaščitene carine, ali pa Kitajci ne morete več izvažati, dokler ne morate izdati certifikata, da ne uporabljate kemikalij, da imate minimalno plačo, da ne izkoriščate otroškega dela, mislim, se da. Ampak ima svojo ceno in podraži stvar. Ta internetna ekonomija je izven tega navideznega zastonjkarstva, ki deluje na ogromnem *scaleu* . [obsegu, op. avtorja] in na užitkarstvu. (Medij 3, osebni intervju, 2017, 11. julij)

Spodbujanje razvoja visokotehnoloških storitev je vsekakor ena od zapovedi za gospodarsko rast in državam je v interesu, da so visokotehnološka podjetja in spletni velikani ustanovljeni na njihovem ozemlju (Zagovornik 1, osebni intervju, 2017, 26. januar).

Pravila, ki varujejo uporabnike, so zunaj EU precej bolj sproščena, kar pomeni prednost za podjetja, ki so ustanovljena v teh pravnih sistemih, ter oviro za podjetja, ki so ustanovljena v EU in poslujejo v EU:

> To je primer dopinga. Ko se enkrat v nekem športu zgodi, da brez dopinga ne moreš biti konkurenčen, je problem. […] Seveda, ker Američani in Kitajci igrajo po čisto drugih pravilih. Evropska podjetja pravijo, da jih naša regulacija dela nekonkurenčne. Ampak je pa spet nekaj drugega, je pa res da Evropa ima mehanizme, da zadeve zaostri, če bi hoteli. Ampak dostikrat jim ni bilo v interesu, poceni kitajski uvozi so dolgo časa v Evropi dvigovali standard nižjega in srednjega razreda in omogočali delodajalcem, da so pritiskali na sindikate. (Medij 3, osebni intervju, 2017, 11. julij)

Zato nekateri menijo, da bi morala EU bolj spodbujati evropske ponudnike, ki se trudijo vzdrževati raven storitev, ki ne posega v pravice posameznikov (Zagovornik 4, osebni intervju, 2017, 8. februar).

Strožja regulacija le v Evropi v spletnem svetu tudi s tehničnega vidika nima smisla, saj internet ne pozna meja v klasičnem smislu in se je zelo preprosto odločiti za ponudnike storitev iz držav, v katerih ni tako stroge regulacije, kot je v EU. Kot poudarja Zagovornik 4, nadzor le nad Evropskimi podjetji nima smisla, če hkrati ni nadzora nad velikimi multinacionalkami, ki prevladujejo na trgu, kot so Google, Facebook in Amazon (Zagovornik 4, osebni intervju, 2017, 8. februar). Na premike v tej smeri kažejo tudi zadnje odločitve Evropske komisije v zvezi z Googlom in njegovim operacijskim sistemom Android, kjer je Evropska komisija Googlu postavila velike zahteve v zvezi z njegovim monopolnim položajem in mu izrekla sankcijo v višini 4,34 milijarde evrov (Warren, 2018).

6.4 Boljša regulacija vedenjskega oglaševanja v prihodnosti

V četrtem sklopu je bila obravnavana tematika boljše regulacije vedenjskega oglaševanja v prihodnosti. Motivi za vzpostavitev boljše regulacije vedenjskega oglaševanja so povezani z različnimi negativnimi učinki na posameznike – uporabnike elektronskih komunikacij, kar pa ima nadaljnje negativne učinke za družbo. Baldwin in Cave (1999) med običajne razloge za regulacijo posameznega področja uvrščata situacije, v katerih neregulirani trg ne deluje v skladu z določenim javnim interesom. Negativne eksternalije v smislu izgube pravice do zasebnosti v informacijsko-komunikacijski družbi, diskriminacije in posega v politične pravice ter številne negativne posledice prepuščanja odločanja tehnologiji in algoritmom so glavna motivacija za regulacijo tega področja:

> Nekako vedno, ko razmišljam o pravici do zasebnosti in pravici do varstva osebnih podatkov, nočem izgubiti vojne. [...] ko bomo rekli, tehnologija nam je ušla iz rok. […] Ampak mislim da future to be [prihodnos, op. avtorja]je ta artificial intelligence [umetna inteligenca, op. avtorja], ki bo znala sama razmišljat, in upam, da bo pravo tu še vedno znalo postaviti meje ljudem, ki to tehnologijo gradijo, da se bodo zavedali, kaj se lahko zgodi, ko tehnologija razmišlja namesto nas in mi več vpliva ne bomo imeli […] In mislim, da bo treba tudi bolj razmišljati v to smer, kje bomo tej tehnologiji mi ljudje postavili meje, mislim, da je treba postaviti meje tam, kjer ne smemo dopustiti, da bo tehnologija razmišljala namesto nas. (Svetovalec 3, osebni intervju, 2017, 13. januar)

Motiv za regulacijo je tudi varovanje uporabnikov elektronskih komunikacij kot žrtev oziroma omogočanje, da lahko uveljavljajo svoje pravice:

> [Z]ame recimo je bistvo regulacije, da ti omogoča uveljavljati pravice. […] Če jaz iz kakršnega koli razloga želim zase udejanjiti pravico do zasebnosti in biti nediskriminiran zaradi tega, mi mora regulator to omogočiti. […] Država izobraziti, regulator pa udejanjiti. To je po moje to. Da jaz lahko udejanjim pravice, ki so mi z ustavo in zakoni zagotovljene, in da nisem pri tem diskriminiran. Jaz nimam možnosti udejanjiti pravice do zasebnosti. […] Mislim, da bi to moralo biti to, k čemur naj bi regulacija sledila. (Medij 3, osebni intervju, 2017, 11. julij)

Med možnostmi, kako bi lahko področje vedenjskega oglaševanja v prihodnosti regulirali bolje, so bile poudarjene marsikatere od zgoraj navedenih strategij (Baldwin in Cave, 1999, str. 34–62), ne le zakonodaja in samoregulacija. Ugotovitve pa kažejo predvsem, da je ključen splet različnih strategij in orodij ter zavedanje o problematiki med različnimi deležniki, ki morajo biti aktivno vpeti v iskanje boljših rešitev in strategij.

V nadaljevanju so predstavljene ugotovitve analize intervjujev glede na ključni ugotovitvi:

- za boljšo regulacijo področja je potreben splet strategij in orodij ter delovanje na področju vseh deležnikov, ne le izboljšave zakonodaje na tem področju;

- boljša regulacija v EU zahteva tudi izboljšave na področju zakonodaje o varovanju zasebnosti in osebnih podatkov (glede konceptov privolitve in zakonitega interesa, obveščanja in orodij za večjo odgovornost subjektov, ki izvajajo vedenjsko oglaševanje).

6.4.1 Splet strategij za boljšo regulacijo vedenjskega oglaševanja

a) Strategija pravil in nadzora

Prihodnja regulacija vedenjskega oglaševanja bi morala biti utemeljena v zakonodaji, ki zagotavlja ustrezno ravnotežje med vsemi interesi, ter na učinkovitem nadzoru, torej na strategiji pravil in nadzora: »Ti seveda rabiš zakonodajo, vsaj v nekem bazičnem pomenu rabiš neko referenco, nekaj, na kar se lahko sklicuješ« (Zagovornik 2, osebni intervju, 2017, 11. januar). Zgolj samoregulacija področja brez zaslombe v zakonodaji ni pogosto videna kot prava pot naprej. Temeljni koncepti pravil, ki so bili poudarjeni, so določbe glede privolitve v sledenje in informiranje, ki mora biti pomenljivo, posameznik pa ne sme biti prisiljen v privolitev (npr. v vse piškotke) (Zagovornik 3, osebni intervju, 2017, 16. februar). Izpostavljen je bil pomen zasebnosti prijaznih začetnih nastavitev, ki bi jih moral predpisati zakonodajalec, bodisi za raven aplikacij ali za raven brskalnika (Zagovornik 5, osebni intervju, 2017, 13. marec).

Dileme glede reguliranja z zakonodajo

Pri strategiji regulacije z zakonodajo se (predvsem glede na izkušnje v EU) odpira več dilem, ki bi jih morala prihodnja ureditev upoštevati in rešiti – v EU v konkretnem primeru razvoja ePR, ki bo področje vedenjskega oglaševanja najbolj ključno urejal in pri vprašanjih razlage relevantnih določb Uredbe 2016/679 v praksi, v ZDA pa pri oblikovanju nove zvezne zakonodaje:

- prestroga zakonodaja oziroma previsoki standardi, ki jih subjekti na trgu zato ne upoštevajo – poudarjeno je bilo, da mora zakonodaja upoštevati vidike malih podjetij in da mora biti panoga vključena v odločanje o standardih (Svetovalec 4, osebni intervju, 2017, 14. marec). Podjetja bodo vedno našla pot, da obidejo stroge določbe, saj imajo primarno ekonomske cilje (Zagovornik 2, osebni intervju, 2017, 11. januar).

Poudarjene so bile posledice stroge zakonodaje, ki da bo onemogočila zagonska podjetja, ki se financirajo z oglaševanjem. Več kot 9 od 10 zagonskih podjetij se zanaša na monetizacijo preko oglaševanja. Nova pravila jim bodo, po mnenju Oglaševalca 2, zelo otežila delovanje (Oglaševalec 2, osebni intervju, 2017, 7. februar);

- nepoznavanje zakonodaje oziroma pomen izobraževanja in dviga zavedanja o pravilih ter komunikaciji o dobrih in slabih praksah. Pomanjkljivosti v znanju in vedenju o tematiki regulacije so tako na strani pripravljavcev zakonov kot tudi pristojnih organov in panožnih združenj, ki bi vsak morali opraviti svojo nalogo pri ozaveščanju o novih zakonskih določbah (Svetovalec 1, osebni intervju, 2017, 23. januar).

Eksperti so Poudarili tudi nekatera aktualna vsebinska vprašanja, ki lahko kažejo nove poti za določanje pravil v prihodnje – bodisi v okviru določb zakonodaje bodisi razlag zakonodaje:

- koliko bi bilo smiselno vedenjsko oglaševanje regulirati glede na koncept lastništva podatkov, predvsem je to slišati ob razpravah glede interneta stvari, kjer vsakovrstne naprave obdelujejo mnoge podatke o delovanju uporabnika naprave? Poudarjeno je bilo, da tak pristop vodi v poblagovljenje osebnih podatkov in človekove pravice do zasebnosti, ki ima številne posledice za pravice posameznika, tudi z vidika varovanja pravic intelektualne lastnine in poslovnih skrivnosti, ki bi jih lahko »lastniki« podatkov zatrjevali (Zagovornik 3, osebni intervju, 2017, 16. februar);
- ali bi morali vedenjsko oglaševanje v nekaterih primerih prepovedati (npr. kadar temelji na občutljivih osebnih podatkih in je posledica lahko diskriminacija)? S sodobnimi tehnično izpopolnjenimi metodami je iz na videz običajnih osebnih podatkov, ki niso sami po sebi občutljivi, mogoče sklepati na občutljive, na npr. spolno usmerjenost posameznika (npr. iz lokacij, kjer se nahaja), njegovo rasno poreklo (iz podatka o najljubši hrani ipd.), zato je težko potegniti mejo, katere podatke strožje varovati. Vprašljiva je tudi privolitev posameznika, ki ne glede na vse legitimira tudi obdelavo občutljivih osebnih podatkov (Zagovornik 4, osebni intervju, 2017, 8. februar);
- postavlja se tudi vprašanje, ali bi bilo smiselno omejiti le nekatere namene, za katere se v okviru vedenjskega oglaševanja uporabljajo podatki. Ne da bi razlikovali med občutljivimi in običajnimi osebnimi podatki, ampak da bi omejitve veljale za določene namene, za katere se uporabljajo osebni podatki ali vsebine; namene, ki pomenijo

tveganje za posameznika ali za ranljivejše družbene skupine (kot npr. otroke), po vzoru oglaševanja v starih medijih, glede katerih obstajajo omejitve za oglaševanje nekaterih produktov (npr. tobačni izdelki, spolne vsebine), za zavajajoče prakse (npr. produktno umeščanje) ali oglaševanje ranljivejšim (otrokom), omejitve glede politične propagande in pravila oglaševanja v času volitev (Svetovalec 4, osebni intervju, 2017, 14. marec);

- kako urejati uporabo vedenjskega oglaševanja za namen promocije političnih idej in kandidatov (Svetovalec, 4, osebni intervju, 2017, str. 7).

Izvajanje zakonodaje in nadzor

Ugotovitve intervjujev kažejo, da je za prihodnjo boljšo regulacijo vedenjskega oglaševanja pri strategiji pravil bistven učinkovitejši nadzor (Svetovalec 2, osebni intervju, 2017, 25. januar), saj »ni za pričakovati, da bodo ljudje spoštovali zakone, ki grejo direktno njim na škodo, ali pa podjetja, ki jim gre direktno njim na škodo in jim motijo poslovne modele, brez tega, da bi se nečesa bali« (Zagovornik 2, osebni intervju, 2017, 11. januar).

> [V] pravu je tako, če napiše zakon, […] in nima kaznovalnih določb, nima enforcementa [nadzora, op. avtorja], je pač v naravi ljudi, da hvatajo krivine, če enforcementa ne boš mel, je čisto brezveze, da nekaj napišeš, neko zapoved v zakon. Potem smo na morali, etiki, standardih, to je *soft law* [nezavezujoče pravo, op. avtorja]. Pri človekovih pravicah se mi zdi, ne vidim, da bi s *soft lawom* lahko dosegel implementacijo neke filozofije reguliranja temeljnih človekovih pravic. (Svetovalec 3, osebni intervju, 2017, 13. januar)

Sogovorniki so pogosto poudarili, da je grožnja z nadzorom in (visokimi) sankcijami sicer res motivacija za organizacije in podjetja, da prilagodijo svoje prakse v skladu s pravili, vendar pa to ni edina spodbuda. Na motivacijo delujejo tudi in predvsem naslednji dejavniki, ki bi jih v prihodnjem okviru regulacije vedenjskega oglaševanja morali upoštevati oziroma bolje vplesti v celoten sistem urejanja:

- ekonomske posledice ali prednosti za izvajalce vedenjskega oglaševanja, bodisi v smislu večjega zaslužka bodisi manjših stroškov zaradi plačevanja sankcij (Zagovornik 3, osebni intervju, 2017, 16. februar). Zato eden od nadzornih organov pri tehnoloških temah sodeluje z inštitutom za znanost in tehnologijo, ki med drugim razvija tudi zasebnosti prijazna orodja za vedenjsko oglaševanje in pri tem upošteva tudi ekonomsko plat – da lahko še vedno pridobivajo prihodke z oglaševanjem (Regulator 2, osebni intervju, 2017, 31. marec). Zasebnosti prijazne rešitve so lahko drage za implementacijo, in če ni dovolj uporabnikov, ki bi jih uporabljali, ponudniki

ne najdejo ekonomskega argumenta za implementacijo (Regulator 2, osebni intervju, 2017, 31. marec);

- konkurenčna prednost, ki bi jo imel subjekt zaradi skladnosti s pravili – trenutno zasebnosti prijazne prakse za izvajalce vedenjskega oglaševanja prej pomenijo slabost (Regulator 4, osebni intervju, 2017, 16. februar);
- izboljšanje ugleda, npr. s poudarjanjem dobrih praks (subjekti, ki spoštujejo pravila, bi lahko imeli nekatere ugodnosti, bi bili vključeni npr. na seznamih zanesljivih partnerjev, na seznamih protireklamnih vtičnikov ipd.) (Svetovalec 2, osebni intervju, 2017, 25. januar).
- strategija poimenskega sramotenja (angl. *name and shame*) s strani nadzornih organov (Oglaševalec 1, osebni intervju, 2017, 16. januar).
- In tudi znotraj panoge, da npr. oglaševalec (torej plačnik oglasa, ne nujno založnik) izpostavi podjetja, s katerimi ni dobro sodelovati (veliko moč za spremembe v tem ekosistemu imajo namreč prav veliki oglaševalci, ki bi se jim oglaševalski posredniki morali ukloniti, če bi si želeli zagotoviti zaslužek), in posledična izguba zaupanja potrošnikov (Regulator 2, osebni intervju, 2017, 31. marec).
- čezmejna doslednost pravil in nadzora: skladnost s pravili v eni državi članici EU bi morala omogočati skladno delovanje v drugi (Regulator 2, osebni intervju, 2017, 31. marec);
- grajenje dolgotrajnih odnosov zaupanja s potrošniki in ustvarjanja trajnostnega razvoja in okolja za prihodnost. Grajenje zaupanja s potrošniki bi morala biti bistvena spodbuda za subjekte na trgu (Zagovornik 4, osebni intervju, 2017, 10).

Ugotovitve tudi kažejo, da za strategijo pravil bistven »pameten« nadzor, osredinjen na tiste subjekte, katerih dejanja pomenijo tveganje za uporabnike spleta in ne birokratsko breme. Svetovalec 4 kot primer velikega tveganja izpostavlja zadeve glede političnega oglaševanja in mikro-ciljanja, poleg tega pa poudarja, da bi morali imeti nadzorni organi več resursov, tudi človeških in da bi morali bolje selekcionirati, kam usmerijo nadzor (Svetovalec 4, osebni intervju, 2017, 14. marec).

Nadzor področja vedenjskega oglaševanja je težaven. Oglaševalska panoga se je 20 let razvijala v smeri zbiranja podatkov in ponudbe brezplačnih storitev, zato je sprememba tega vzorca težavna. Eno bistvenih vprašanj, ki mora biti v smislu prihodnje regulacije rešeno, je

vprašanje, zoper koga usmeriti nadzor – zoper najuspešnejše igralce na trgu, ki imajo večje zmožnosti pravnega oporekanja in iskanja tehničnih obidov ali zoper manjše, pri katerih je nadzor sicer lažji, vendar z manjšim učinkom. Vprašanje je tudi, ali se osrediniti le na posebej škodljive (Regulator 3, osebni intervju, 2017, 15. februar).

Pri nadzoru nad spletnim sledenjem in vedenjskim oglaševanjem se pojavljajo konkretne dileme, in sicer zoper koga usmeriti nadzor, saj v ekosistemu deluje veliko različnih akterjev, najbolj poudarjeno pa je vprašanje odgovornosti prvih spletnih strani (ki jih uporabnik dejansko obišče), vendar mu ne sledijo, in tretjih spletnih strani (običajno sledilcev), ki prek prve spletne strani na uporabnikovo napravo namestijo sledilno tehnologijo. Prevladujoče mnenje je, da bi moral biti nadzor usmerjen zoper prvo stran, ki mora biti sposobna ustrezno obveščati uporabnike, saj sama dopusti na svojo stran sledilce tretjih strani in morajo prevzeti odgovornost, čeprav se zdi včasih nepošteno, tudi z vidika tega, da nima največje ekonomske koristi ona, ampak tretje strani (Regulator 3, osebni intervju, 2017, 15. februar). Čeprav je nadzor nad prvo stranjo težak, ker ta dejansko nima vpliva na to, kaj tretje strani počnejo s podatki, pa so prve strani vendarle tiste, ki dostop do svoje strani omogočijo. Zato bi moral biti nadzor usmerjen k pogodbenim dogovorom, ki jih prve strani sklepajo s tretjimi (Regulator 3, osebni intervju, 2017, 15. februar).

Učinkovit nadzor je povezan s položajem nadzornega organa in z viri, ki so mu na voljo, tako v smislu kadrovskih kot tudi finančnih (Svetovalec 2, osebni intervju, 2017, 25. januar). Pomemben vidik so tudi pristojnosti, ki so mu zaupane. Nadzorni organ mora imeti namreč možnosti določenih samostojnih ravnanj zoper svoje nadzorovance. Če ne more prepovedati obdelave podatkov sam, ampak mora to doseči v sodnem postopku, je njegova moč okrnjena (Regulator 4, osebni intervju, 2017, 16. februar). Nadzor na področju vedenjskega oglaševanja je tehnično zahteven, nadzorni organi pa pregovorno podhranjeni tehničnega kadra. Svetovalec 2 poudari, da v praksi pravzaprav potrebujejo hekerje, da lahko razumejo vse tehnične plati ozadja panoge (Svetovalec 2, osebni intervju, 2017, 25. januar). Podhranjenost nadzornih organov je po mnenju nekaterih eden glavnih problemov v kontekstu vedenjskega oglaševanja (Zagovornik 3, osebni intervju, 2017, 16. februar). V prihodnje bi torej morali nadzornim organom na ravni pravil in predvsem v praksi (tudi s stališča financiranja) zagotoviti ustrezna pooblastila, ustrezne možnosti pridobivanja in uporabe znanj

tehničnih strokovnjakov na področju spletnega sledenja pa tudi ekonomskih in marketinških znanj, ki osvetljujejo področje vedenjskega oglaševanja.

V tem smislu je bila poudarjena tudi potreba po orodjih, ki bi nadzornim organom olajšala izvajanje nadzora. Omenjena so bila orodja, s katerimi bi uporabniki lahko opozarjali na težave s sledilci, v smislu vtičnika za brskalnik ali podobno. Tako bi nadzorni organi dobili več informacij o tem, kaj se v praksi dogaja in bi lahko bolje izvajali nadzor (Regulator 2, osebni intervju, 2017, 31. marec). Regulator 1 (osebni intervju, 2017, 15. februar) pa je omenil orodja, s katerimi bi bilo mogoče hitro prepoznati, ali je posamezen piškotek sledilni ali ne.

Po drugi strani pa je bilo poudarjeno tudi, da se razmere glede tehničnega znanja in virov pri nadzornih organih za varstvo osebnih podatkov izboljšujejo, tudi na račun formalnega in neformalnega sodelovanja med strokovnjaki iz različnih držav (Regulator 2, osebni intervju, 2017, 31. marec). Formalno sodelovanje med nadzornimi organi za varstvo osebnih podatkov sicer zapoveduje Uredba 2016/679 (v 7. poglavju). Pomembno je tudi sodelovanje z drugimi nadzornimi organi, npr. na področju varstva potrošnikov, ki se spopadajo s podobnimi vprašanji. Regulator 3 omeni, da imajo redne sestanke in seminarje z nadzornim organom za varstvo potrošnikov, s fokusom na zakonodaji in sodelovanju pri nadzoru (Regulator 3, osebni intervju, 2017, 15. februar).

Poudarjeno je bilo, da se lahko v iskanju rešitve za podhranjeni nadzor ozremo tudi k javno-zasebnemu partnerstvu, npr. s certifikacijskimi telesi ali revizijskimi organizacijami, ki imajo zelo specifična znanja revidiranja različnih subjektov in praks (Zagovornik 5, osebni intervju, 2017, 13. marec). Omenjeno je bilo tudi, da ni rešitev nujno v številčnejšem nadzoru, ampak v doslednem izvajanju načel vgrajene zasebnosti in upoštevanju ustreznih tehničnih standardov. V tem primeru bi bile storitve in rešitve privzeto vgrajene zasebnosti prijazne, standardne rešitve pa bi preprečevale zlorabe podatkov in bi nadzor posegel le na področje večjih tveganj (Zagovornik 3, osebni intervju, 2017, 16. februar).

Ugotovitve kažejo, da so za prihodnjo regulacijo pomembne tudi mehkejše tehnike, kot je poudarjanje dobrih praks in njihova promocija, kar dviguje raven skladnosti s pravili v celotni panogi. Hkrati pa Svetovalec 4 poudarja, da to včasih ni dovolj, pač pa je potreben nadzor.

> [Y]ou don't achieve compliance by just passing enforcement. You achieve compliance by co-regulatory mechanism, by engaging with your regulators, by trying to understand, collaborate, exchange views. By showcasing what do the best examples look like. Incentivizing good behaviour, so when companies do something well, promote that, show it, talk about it. Because actually, companies are very glad when they do that. Then they do better, then they do more. […] [T]hat's how extra smart regulators would behave. Now, it doesn't always work, sometimes you need this enforcement. (Svetovalec 4, osebni intervju, 2017, 14. marec)

Ima pa promocija dobrih praks tudi pomanjkljivost. Hitro se lahko izkaže, da so se npr. spremenile tehnične podrobnosti ali da ponudnik dobrih praks ne upošteva več, nadzorni organ pa je potem odgovoren (Regulator 2, osebni intervju, 2017, 31. marec). V tem smislu je pomembna tudi krepitev odgovornosti podjetij in organizacij, ki se ukvarjajo z vedenjskim oglaševanjem, da spoštujejo pravila, tako da vplivamo na njihovo motiviranost za ravnanje v skladu s pravili ter na dvig zavedanja o problematiki na vseh ravneh (Svetovalec 2, osebni intervju, 2017, 25. januar).

Ker so aktivnosti vedenjskega oglaševanja čezmejne, izvajalci pogosto prihajajo iz različnih držav članic EU ter tretjih držav, najpogosteje ZDA, uporabniki elektronskih komunikacij, ki so podvrženi sledenju in profiliranju, pa so prav tako v različnih državah, praktično ni mogoče govoriti o prihodnjem nadzoru, ki ne bi bil čezmejen (Svetovalec 2, osebni intervju, 2017, 25. januar). V praksi se pojavljajo številna vprašanja glede čezmejne veljavnosti predpisov ter glede učinkovitosti čezmejnega nadzora. Prenovljen evropski okvir za varstvo osebnih podatkov ima izrazito čezmejno noto – pristojnosti evropskih nadzornih organov se namreč razteza tudi v tretje države, če subjekti iz njih npr. spremljajo vedenje posameznikov v EU, kar je pri vedenjskem oglaševanju zelo pogosta praksa. Vprašanje pa je, kot poudarja Zagovornik 3, koliko bodo ti subjekti zunaj EU delovali skladno z zakonodajo EU ob pomanjkljivih možnostih, ki jih imajo evropski nadzorni organi za izvajanje svojih pristojnosti zunaj meja Evrope (Zagovornik 3, osebni intervju, 2017, 16. februar).

Učinkovit in skladen čezmejni nadzor je tako ena bistvenih predpostavk prihodnje regulacije vedenjskega oglaševanja, hkrati pa izkušnje kažejo, da se nadzorni organi glede aktivnosti med seboj precej razlikujejo*:* »In pri globalnem kotlu imaš spet ta problem, da imaš en *law enforcement* [organ nadzora, op. avtorja], ki je agilen, priden, ki dela, in enega, ki sedi v pisarni s fikusom in ne naredi nič« (Svetovalec 3, osebni intervju, 2017, 13. januar). Že znotraj EU, v različnih državah članicah, se lahko razlaga pravil in akcije nadzornih organov med seboj precej razlikujejo (Oglaševalec 3, osebni intervju, 2017, 27. januar), kar vpliva na

to, v katerih država članicah EU spletna podjetja ustanovijo svoje evropske sedeže in se s tem podvržejo zakonodaji tiste države članice: »[Č]e vse države članice ne bodo vsaj približno enakovredno implementirale, imaš vedno tako, da se biznis seli tam, kjer je zadeva za njih bolj ugodna […] [T]udi FB je zelo natančno pogledal, zakaj se je usedel na Irsko, ne ker je le evropska Silicijeva dolina […] Ampak mislim, da so zelo pogledali, kje bodo najlažje prišli čez z vidika nadzora« (Svetovalec 3, osebni intervju, 2017, 13. januar). Za učinkovitejšo regulacijo in nadzor nad pravili je tako bistveno poenotenje nadzornih organov glede najpomembnejših tem, da nasproti spornim praksam vedenjskega oglaševanja nastopijo z enim glasom in ni več mogoče izbiranje najugodnejšega okolja (angl. *forum shopping*), saj podjetja ustanovijo svoje sedeže tam, kjer je nadzorni organ najbolj blag. Bistveno je dobro formalno in neformalno sodelovanje, tudi z nadzornimi organi iz različnih področij.

Opolnomočenje uporabnikov elektronskih komunikacij

Ne glede na to, kako protekcionistična so pravila, ki omejujejo izvajalce vedenjskega oglaševanja, in kakšne pravne podlage jim omogoča zakonodaja ter kako aktivna vloga je v sistemu regulacije predvidena za uporabnike elektronskih komunikacij, ostaja dejstvo, da gre pri regulaciji vedenjskega oglaševanja za iskanje ravnotežja med pravicami in interesi posameznikov in panožnih praks. Zato je nujno, da so posamezniki opolnomočeni in zmožni uveljavljanja svojih pravic. Pravzaprav vsi štejejo izobraževanje kot enega od temeljev za boljše reguliranje področja vedenjskega oglaševanja. Tako bi posamezniki lahko učinkoviteje uveljavljali svoje pravice, ki jim jih daje zakonodaja oziroma, uporabljali druga orodja, kot so certificiranje, standardizacija itd.

Sogovorniki v tem kontekstu poudarjajo dvigovanje zavedanja o škodljivih praksah oglaševanja na spletu ter o pravicah in vzvodih, ki so posameznikom na voljo. Nekateri poudarjajo odgovornost posameznika, da se pouči o zasebnosti na spletu: »Ampak moja odgovornost je, da bom svoje otroke naučil, kako in kaj naj delajo. Če bom imel odprt profil na Facebooku, pa objavljal fotke, da pijančujem, da najemam prostitutke, da sem agresiven, kako sem enega sam pretepel, pa bom potem šel na razgovor za službo. Vsak danes pogugla« (Oglaševalec 1, osebni intervju, 2017, 16. januar).

Drugi stavijo na kampanje za krepitev zavedanja kot dober prvi korak k boljšemu poznavanju problematike spletnega sledenja in oglaševanja ter vpliva na zasebnost (Svetovalec 1, osebni

intervju, 2017, 23. januar). Vendar ostaja dejstvo, da posamezniki kljub različnim predavanjem in treningom v praksi s svojimi osebnimi podatki pogosto ravnajo neodgovorno:

> Dva dni so ljudem pumpali osem ur na dan vse o zaščiti, o data leakih [razkritjih podatkov, op. avtorja], o cloud servicih [oblačnih ponudnikih, op. avtorja], o telefonih, o PGP, o vsem. Dva dni, 16 ur si imel samo to, nič drugega. In potem so ta tretji dan, preden je folk prišel ta tretji dan v službo, so po parkirišču raztresli neke USB ključe. In vse ključe so ljudje pobrali, neke no name, no brand [brez znamke, navedbe lastnika, op. avtorja], nič. Tam je neki na tleh ležalo. In so jih vsi pobrali in so jih vtaknili v komp [računalnik, op. avtorja] v firmi. Ko so imeli dva dni, en dan prej, učenje o tem, kako tega ne delat, kako je to narobe, kako je to uno, kako je to tretje. (Zagovornik 2, osebni intervju, 2017, 11. januar)

Poudarjajo pomen praktičnega treninga ter institucionaliziranega izobraževanja o temeljnih pravicah v kontekstu tehnološko razvitega vsakdana, Zagovornik 2 poudarja, da ni dovolj le dvigovanje zavedanja, pač pa predlaga tudi delavnice in aktivistične pozive k boljši regulaciji, da problem napadeš z različnih zornih kotov in spodbudiš razmišljanje (Zagovornik 2, osebni intervju, 2017, 11. januar). »Tako kot bi morala biti državljanska vzgoja in slovenščina, tako bi morala biti *privacy* [zasebnost, op. avtorja] del slovenščine, neka podsekcija literature. Da ti pride to v kri« (Zagovornik 2, osebni intervju, 2017, 11. januar). Tudi v smislu vključevanja vsebin varstva podatkov in zasebnosti ter digitalne pismenosti v šolske učne načrte (Svetovalec 2, osebni intervju, 2017, 25. januar). Nadzorni organi pa bi lahko pripomogli k oblikovanju in izboljšanju izobraževalnih gradiv (Regulator 4, osebni intervju, 2017, 16. februar).

Ker so specifična tehnična znanja hitro zastarela, bi moralo izobraževanje stremeti k znanju o temeljnih pravicah ter na kritičnih vidikih prevlade velikih korporacij v digitalnem okolju, ne le na izobraževanju o družbenih medijih in podobnih trenutno priljubljenih storitvah (Zagovornik 5, osebni intervju, 2017, 13. marec; Regulator 2, osebni intervju, 2017, 31. Marec, Regulator 3, osebni intervju, 2017, 15. februar). Veliko vlogo pri opolnomočenju imajo zasebnosti prijazne tehnologije (angl. *PETs*), ki so bile podrobneje obravnavane v prejšnjem poglavju.

b) Druge strategije in področja regulacije

Med drugimi strategijami regulacije so za področje vedenjskega oglaševanja pomembne samoregulacija (na podlagi kodeksa in tudi možnosti na področju standardizacije in certificiranja), eksperti pa so poudarili tudi pravni okvir za vzpostavljanje konkurence na trgu in davčna pravila ter premik k etiki in družbeni odgovornosti podjetij.

Samoregulacija

Ugotovitve študije kažejo, da so orodja samoregulacije zelo pomemben del spleta regulatornih strategij in bi bile lahko plodneje uporabljene tudi na področju vedenjskega oglaševanja. Posebej ob upoštevanju smeri, v katere se zakonodaja v EU trenutno razvija, in na možnosti, da izrecno soglasje ne bo več edina možna podlaga za sledenje uporabnikom in vedenjsko oglaševanje, ki pomenijo, da bi obstoječi kodeks samoregulacije lahko pridobil na teži in uporabnosti kot orodje regulacije.

Kodeksi samoregulacije so lahko zelo učinkovito orodje regulacije, saj lahko določajo višje standarde oziroma take standarde, ki jih panoga dejansko spoštuje. Kaže pa tudi na slabosti samoregulacije, če nima ustreznih postopkov nadzora nad kršitelji. Zato je poudarjena korist koregulacije, pri kateri zakonodaja določa osnovne temelje in pogoje nadzora, podrobnejša merila pa predpiše samoregulacija. Kot kažejo ugotovitve ekspertnih intervjujev, tako možnost zagovarjajo tudi nekateri strokovnjaki (Svetovalec 2, osebni intervju, 2017, 25. januar; Svetovalec 4, osebni intervju, 2017, 14. marec). V kontekstu prihodnje regulacije vedenjskega oglaševanja to pomeni, da bi bilo treba kodeks uskladiti z minimalnimi zahtevami zakonodaje v EU predvsem glede pravnih podlag, kakršne bodo za vedenjsko oglaševanje določene z Uredbo 2016/679 in nastajajočo ePR. V delu specifičnih tehničnih zahtev in poenotenja informiranja pa bi kodeks lahko pripomogel z določbami, ki so veliko bolj specifične od zakonodaje, zlasti v okviru mobilnega oglaševanja in interneta stvari. Uredba 2016/679 ponuja tudi možnosti validacije kodeksa s strani nadzornih organov. Neusklajenost kodeksa in zakonodaje glede temeljnih zahtev je najslabša pot, saj veča pravno negotovost na trgu izvajalcev vedenjskega oglaševanja ter omogoča zavajanje vseh relevantnih deležnikov – od posameznikov do izdajateljev spletnih strani.

Eksperti so tudi poudarili, da je trenutno v *ad tech* panogi težko doseči strinjanje glede zahtev za vedenjsko oglaševanje in je zato težko kmalu pričakovati kodeks, ki bi bil celosten in bi bil učinkovito samostojno orodje za regulacijo tega področja. Svetovalec 4 izpostavi, da je kodeks za neposredno trženje nastajal 7 let in je moral biti odobren s strani Delovne skupine po členu 29. Bolj realno se mu zdi, da bi bila samoregulacija dodatek osnovnim pravilom, morda le na tistih področjih, na katerih je mogoče pobudo prepustiti panogi, ki se bo zmožna strinjati, in je pričakovati boljše rezultate kot pri zunanji regulaciji (npr. ikone) (Svetovalec 4, osebni intervju, 2017, 14. marec).

Tudi standardizacija in certificiranje lahko veliko pripomoreta k boljšemu urejanju področja vedenjskega oglaševanja, vendar v primeru EU le z usklajenim delovanjem z zakonodajo, predvsem Uredbo 2016/679. Odprte so možnosti za nastanek specifičnih certifikacijskih shem za vedenjsko oglaševanje, morda le na ozkem področju interneta stvari, mobilnega okolja, ali pa za posebne namene, v posameznem sektorju (npr. pri političnem komuniciranju), lahko bi se nanašale le na specifične elemente dejavnosti – obveščanje, ikone in znake ali specifične faze obdelave podatkov – npr. profiliranje. Ob pogoju upoštevanja določb zakonodaje in zmožnostih nadzora bi taki mehanizmi pomenili izboljšave za področje urejanja vedenjskega oglaševanja. Enako velja za področje standardizacije, na katerem že potekajo aktivnosti na ozkem področju vgrajene zasebnosti, pa tudi na področju spletnega sledenja, vhodne točke v proces vedenjskega oglaševanja na spletu. Zelo pomembno bo torej, kako se bodo do standarda ne sledi in njegove ustreznosti kot orodja za podajo soglasja opredelili evropski nadzorni organi za varstvo osebnih podatkov, zdaj združeni v Evropski svet za varstvo osebnih podatkov, ki imajo zgodovinsko različne poglede na tematiko (Regulator 1, osebni intervju, 2017, 15. februar).

Rezultati študije kažejo, da brez zunanje prisile v obliki zakonodaje, ki bi zahtevala implementacijo in spoštovanje uporabnikovih nastavitev vedenjskooglaševalska panoga ne bo proaktivna pri uporabi in spoštovanju standarda (Regulator 1, osebni intervju, 2017, 15. februar). Pri tehnični rešitvi, kot je standard ne sledi, ki ga načeloma vedenjskooglaševalska panoga uporablja prostovoljno, mora biti v ozadju zunanji nadzor oziroma pravila, ki zapovedujejo njegovo rabo in spoštovanje, saj panoga nima interesa po samoomejevanju, če ni zunanjega pritiska, hkrati pa tehnično nima ovir za sledenje. Podjetja so tako zaprošena naj ne zbirajo podatkov, ki jih lahko enostavno zbirajo (Zagovornik 5, osebni intervju, 2017, 13. marec). Uredba 2016/679 je v tem smislu napredek, saj jasneje določa, kakšna mora biti privolitev, in dopušča, da je lahko dana s pomočjo nastavitev v brskalniku, pomembno pa je, da to področje urejeno tudi v ePR. Eden od argumentov za neodzivnost vedenjskooglaševalske panoge je tudi, da je vložila sredstva v razvoj in uporabo mehanizmov za soglasje v piškotke in želi najprej izrabiti te rešitve. Zato na ravni konzorcija W3C potekajo razprave, kako tehnično prilagoditi standard ne sledi, da bo deloval vzporedno z mehanizmi za privolitev in bodo te tehnične rešitve med seboj interoperabilne (Regulator 1, osebni intervju, 2017, 15. februar). Interoperabilnost različnih rešitev za zagotavljanje

zakonitosti sledenja na spletu je torej še en ključni element učinkovitejše regulacije vedenjskega oglaševanja v prihodnosti.

Problematično področje je tudi nadzor, ki je za učinkovito regulacijo nujen. Tehnično je namreč na tem področju zelo zahteven, še posebej kadar sledenje ni izvedeno s piškotki, ampak npr. glede na odtis naprave. Na terminalni opremi uporabnika tega ni mogoče zaznati, na strani podjetja pa bi morali v nadzoru pregledovati programsko opremo in kode, kar je težko in Oglaševalec 3 meni, da lahko tudi izguba časa (Oglaševalec 3, osebni intervju, 2017, 27. januar). Vprašljivi so viri in znanje nadzornih organov za izvajanje takega nadzora, saj ne zajema le tistega, kar je vidno na uporabnikovi napravi, ampak preglede sistemov v zaledju. Regulator 4 izpostavlja, da bodo nadzorni organi morali najti orodja za take preglede sistemov in poudarja, da se bo izkazala pomembnost odgovornosti podjetij in digitalne pismenosti nadzornih organov, tako v smislu najemanja tehnično kvalificiranega kadra, kot v smislu zagotavljanja, da njihovo znanje sledi razvoju sledilnih praks (Regulator 4, osebni intervju, 2017, 16. februar). Za prihodnje boljše urejanje področja tako tudi na področju standardizacije veljajo premisleki o boljšem nadzoru, ki zajema močne nadzorne organe s primernimi pooblastili in specifičnim tehničnim znanjem za to področje oziroma partnerstvo s specializiranimi ustanovami, ki imajo tehnično znanje na tem področju.

Pravila na davčnem področju

Med drugimi strategijami regulacije so sogovorniki poudarili tudi možnosti z vidika pravil na davčnem področju. Na davčnem področju bi po eni strani lahko subjektom naložili davčne obremenitve za uporabo zasebnosti škodljivih praks ali olajšave za dobro delovanje, po drugi strani pa bi z večjo preglednostjo, oziroma dolžnostmi razkritja lahko bolje ocenili, kakšno količino osebnih podatkov posamezen subjekt obdeluje, in premislili, kako to vezati na njegove davčne obveznosti.

Obdavčitev glede na število uporabnikov je bila omenjena kot ena od možnosti regulacije, s katero bi pritisnili na največje ponudnike:

> »[Č]e pogledaš top 5 najbolj downloadanih [nalaganih, op. avtorja] aplikacij zastonj, sta mislim da Facebook pa Google, to je to. […] Toliko davka, če ga boš znal pobrati, kot boš pobral od Facebooka pa Googla, lahko rečeš ostalim, da jim ni treba plačevati. Pa lahko rečeš, glej davek velja, če imaš več kot, ne vem, pa naložiš neki prelom, ki ga noben ne doseže od spodaj gor, Google pa Facebook pa ga presegata že sto let in si zmagal« (Zagovornik 2, osebni intervju, 2017, 11. januar).

Mogoče je, da bi spletni velikani ta davek precej lahko plačali in bi ga razumeli le kot strošek, praks pa ne bi spremenili; zato bi zbrana sredstva lahko porabili na drugih področjih, npr. za izobraževanje (Zagovornik 2, osebni intervju, 2017, 11. januar). Možnost je tudi obdavčitev transakcij z osebnimi podatki, kjer se določi vrednost posameznemu osebnemu podatku, kar bi najbrž prisililo tudi k premisleku o tem, katere podatke subjekti na trgu vedenjskega oglaševanja dejansko potrebujejo (Zagovornik 2, osebni intervju, 2017, 11. januar).

Podoben primer je vtičnik, ki posamezniku na podlagi njegovega brskanja po spletu pove, kakšno vrednost je s tem brskanjem ustvaril omrežju Facebook oz. koliko je Facebook na podlagi njegovih podatkov o brskanju zaslužil. S pomočjo takega vtičnika bi lahko ugotovili število posameznikov, katerih podatke obdeluje iz različnih držav ter koliko je z njihovimi podatki pridobil. S predpostavko, da so osebni podatki teh posameznikov premoženje določene države, katere državljani so, bi lahko razkrili, da podjetje obdeluje podatke več milijonov državljanov in na njihovi podlagi ustvarja neko vrednost oz. dobiček, hkrati pa morda v tej državni niti ne plačuje davkov niti ne odpira delovnih mest ipd. (Zagovornik 1, osebni intervju, 2017, 26. januar).

Najnovejši razvoj na področju davčne zakonodaje v EU kaže tudi premike na tem področju. Leta 2018 je bil objavljen predlog reforme o obdavčenju digitalnih storitev, ki bi dopuščal obdavčitev tudi v državi, v kateri ponudnik digitalnih storitev ni fizično prisoten, pa ima v tisti državi več kot 100.000 uporabnikov ali več kot 3.000 sklenjenih poslovnih pogodb za digitalne storitve. Kot pojasnjuje Evropska komisija, je namen reforme prav v obdavčitvi aktivnosti, kjer v ustvarjanju vrednosti večinoma sodelujejo uporabniki (njihovi podatki in vsebine) in ki jih je težko zajeti z danes veljavnimi pravili (prihodki, ustvarjeni s prodajo spletnega oglaševalskega prostora; prihodki, ustvarjeni s storitvami, ki omogočajo interakcijo med uporabniki; prihodki, ustvarjeni s prodajo vsebin, ki jih priskrbijo uporabniki) (Evropska komisija, 2018c).

Pravila za varovanje konkurence

Čedalje bolj se poudarja tudi vidik regulacije z namenom varstva konkurence. Nekateri spletni velikani (kot npr. Google) so namreč postali zelo podobni ponudnikom kritičnih storitev in infrastrukture ter zasedajo praktično monopolne položaje. Zagovornik 1 tako izpostavlja, da je situacija kompleksna, ker uporabniki praktično ne morejo ne-uporabljati Google storitev, saj na trgu pogosto ni konkurenčne ponudbe. Meni, da bi morala tu nastopiti regulacija, kot v primeru telekomov, naftnih derivatov, itd., saj ni prav dopuščati dvema podjetjema, da upravljata z vsemi naravnimi viri in jima tako podrediti celo državo (Zagovornik 1, osebni intervju, 2017, 26. januar). Argumenti torej so, da bi morali obravnavati ta podjetja kot ponudnike kritične infrastrukture ali storitev. Če Google neha ponujati svoje storitve, so posledice lahko globalno hude, ne bo mogoče komunicirati, iskati informacij, uporabljati zemljevidov. Nihče ne bi smel biti tako močan, meni Zagovornik 1 (Zagovornik 1, osebni intervju, 2017, 26. januar).

Na premike v tej smeri kažejo tudi nedavne odločitve Evropske komisije v zvezi z dejavnostmi Googla, ki kršijo evropska protimonopolna pravila. Leta 2017 je tako izrekla kazen zaradi iskalnika, ki je med zadetki dajal prednost Googlovim storitve za nakupovanje, in leta 2018 rekordno sankcijo v višini 4,34 milijarde evrov zaradi povezovanja iskalnika v androidni operacijski sistem. Evropska komisija obravnava še primer omejevanja konkurence na področju digitalnega oglaševanja s pomočjo Googlove storitve AdWords.

Omenjena je bila potreba, da bi ponudniki storitev na spletu in v elektronskih komunikacijah morali določeno raven storitve ponujati brez prisile uporabnikov v sledenje oz. prakse, ki škodujejo njihovim pravicam. Ker je uporaba elektronskih komunikacij v sodobnem svetu nujna za poslovanje, uveljavljanje svojih pravic in bivanje, bi ponudnike morali razumeti v okviru konceptov univerzalne storitve oz. kritične infrastrukture ter jih regulirati podobno kot druge ponudnike temeljnih dobrin, npr. transporta, goriv, radijskega spektra itd. oz., kot poudarjata Baldwin in Cave (1999), z razlogom zagotavljanja dostopnosti in neprekinjenosti storitev: »Treba bi bilo narediti, da bi regulator moral reči, da bi vse te zadeve morale nuditi osnovno storitev, ki je dostopna vsem, na podobni ravni, kot recimo trgovina« (Medij 3, osebni intervju, 2017, 11. julij).

Regulacija na področjih, ki zagotavljajo pravico do obveščenosti in svobodne volitve

Glede negativnih posledic vedenjskega oglaševanja na področju politične komunikacije so možnosti regulacije tudi:

- na področju pravil o avdiovizualnih medijskih storitvah (ki jih ureja Direktiva 2010/13/EU o avdiovizualnih medijskih storitvah) ter na področju nacionalnih zakonodaj glede nepristranosti pri poročanju s strani javnih RTV-servisov, pa glede volilnega molka in glede časovnih okvirov, namenjenih posameznim kandidatom. Podobne zahteve bi lahko veljale tudi za netradicionalne medije. EDPS poudarja, da bi lahko obstajala tudi pravila o transparentnosti algoritmičnega predvidevanja;
- volilna zakonodaja je še eno od področij, ki lahko pripomore k večji preglednosti političnega ciljanja, predvsem prek jasnih podatkov o financiranju kampanj in o sredstvih, namenjenih posameznim podatkovnim storitvam;
- pravo varovanja potrošnikov opolnomoči potrošnike v situacijah, v katerih so šibkejša stranka, kar je nedvomno res tudi v odnosu do sodobnih ponudnikov spletnih storitev. Direktiva o nepoštenih poslovnih praksah prepoveduje zavajajoče, agresivne ali drugače nepoštene poslovne prakse, in sicer ne velja za politično komunikacijo, pa vendar so nepoštene prakse na področju komercialnega in nekomercialnega vedenjskega ciljanja zelo podobne (EDPS 2018, str. 16–17).

Etičnost poslovanja in družbena odgovornost organizacij

Čedalje večje je zavedanje, da marsikatera dilema vedenjskega oglaševanja in sledenja na spletu presega okvire, ki jih določa zakonodaja, bodisi o zasebnosti bodisi na drugih področjih, od davčnega do konkurenčnega, pa na področju okoljskih vplivov, zaradi velikih količin energije, ki jo zahteva vzdrževanje ogromnih podatkovnih centrov in procesiranja podatkov. Zato prihajajo v ospredje tudi ideje o etičnem delovanju, o podatkovni etiki, programerski etiki, družbeno odgovornem delovanju organizacij, ki poudarjajo zmanjšanje škodljivega vpliva na družbo in okolje kot strateško usmeritev, ki zagotavlja trajnostne rešitve za prihodnost. V panogi digitalnega oglaševanja take usmeritve še niso pogoste, »tako da, pogrešam […] neko strateško razmišljanje, strateško poslovno razumevanje okolja, širšega okolja, v katerem posluješ, ne samo danes, ampak če želiš poslovati tudi jutri, pojutrišnjem, čez tri ali pa pet let, moraš to malo drugače gledat« (Svetovalec 1, osebni intervju, 2017, 23. januar). Nekatera podjetja pa vendarle že gradijo dobre prakse v tem smislu in delujejo na družbeni odgovornosti Zagovornik 4 (osebni intervju, 2017, 8. februar) omeni podjetje Lego.

Zaradi kompleksnosti področja profiliranja, umetne inteligence in strojnega učenja je tukaj čedalje več klicev k etičnim pristopom, saj zakonodajni okviri niso več dovolj. Široka javna razprava v Franciji je denimo opredelila šest predlogov glede prihodnjih politik urejanja uporabe umetne inteligence: izobraževanje vseh udeleženih v algoritmični verigi (ustvarjalci, profesionalci, državljani) o etiki, prizadevanje po razumljivosti algoritemskih sistemov, tako da se okrepijo pravice posameznikov in mediacija z njimi, izboljšanje algoritemskih sistemov v interesu posameznikove svobode, vzpostavitev nacionalne platforme za revizijo algoritmov, spodbujanje raziskav o etični umetni inteligenci, okrepitev poslovne etike (CNIL, 2018).

Večkrat je bilo tudi omenjeno, da bodo trenutni poslovni modeli spletnih velikanov in *ad tech* panoge težko hkrati zagotovili varovanje pravic uporabnikov in etično delovanje, saj je izraba podatkov uporabnikov del osrčja teh poslovnih modelov, manj podatkov zaradi boljšega varovanja interesov uporabnikov pa pomeni slabše delovanje storitve, nižje prihodke itd. Zato se sogovorniki v iskanju rešitev ozirajo po novih poslovnih modelih, ki bi te pravice in interese bolje pretehtali. V razvoj novih poslovnih modelov bodo *ad tech* panogo morda prisilile tudi zlorabe, ki se trenutno dogajajo v njej. Regulator 4 omeni goljufije s kliki in neveljavnim prometom, zaradi katerih bo morda prišlo do razvoja drugačnih modelov ciljanja, ki bodo oglaševalcem koristni, vendar ne bodo temeljili na ekstenzivnem profiliranju posameznikov v daljših časovnih obdobjih (Regulator 4, osebni intervju, 2017, 16. februar).

Nekateri menijo, da je rešitev v poslovnem modelu, ki bi omogočal izmenjavo vrednosti in bi posameznik lahko na neki način trgoval s svojimi podatki oziroma bi zanje dobil primerno plačilo ali ugodnost, hkrati pa bi obstajale varovalke glede tega, kakšne podatke je mogoče prodati oziroma izmenjevati za druge vrednosti (Zagovornik 1, osebni intervju, 2017, 26. januar).

> [P]otem pa mi ti zaračunavaj, mi ponudi to storitev za 5 €, daj mi opcijo. Ponudniki Facebook za 5 € na mesec, pa si brez trackinga [sledenja, op. avtorja]. Ali pa mi daj tracking, ampak nekaj v zameno. Mislim, da se bodo te stvari [morale] še malo postavljat. Se bodo začele, ko se bodo ljudje malo bolj začeli zavedati vrednosti teh podatkov, kar pomeni, da če ti jaz nekaj dam, sem tudi do nečesa upravičen. (Medij 3, osebni intervju, 2017, 11. julij)

Tudi strožja regulacija je lahko razlog za inovacijo in razvoj zasebnosti prijaznejših poslovnih modelov, pojasni Oglaševalec 1 in se naveže na orodje, ki so ga razvili kot odziv na strožjo zakonodajo o piškotkih, zato da lahko njihove stranke še vedno uporabljajo analitične storitve

tretjih partnerjev, a se pred posredovanjem podatki uporabnikov anonimizirajo (Oglaševalec 1, osebni intervju, 2017, 16. januar).

Povezovanje in prepletanje strategij regulacije

Ena ključnih ugotovitev naše študije je, da morajo biti uporabljene strategije regulacije ustrezno prepletene in skladne ter uporabljene v primernih kontekstih. Za boljšo regulacijo vedenjskega oglaševanja tako niso dovolj le izboljšave v smislu strožje zakonodaje, kot jih predlagajo raziskovalci (npr. Zuiderveen Borgesius, 2014), ampak je potreben splet regulacijskih strategij in usklajeno ravnanje različnih deležnikov.

Povezovanje različnih strategij in pristopov poudarjajo različni sogovorniki, bodisi kombinacijo regulacije, izobraževanja in poslovnih modelov (Regulator 4, osebni intervju, 2017, 16. februar), bodisi privzeto zasebnost in izobraževanje o delovanju tehnologije in algoritmov (Zagovornik 3, osebni intervju, 2017, 16. februar). Vse več je tudi omembe etike in družbene odgovornosti podjetij, ki izvajajo sledenje in vedenjsko oglaševanje (Zagovornik 4, osebni intervju, 2017, 8. februar). Zagovornik 2 poudarja pomembnost usklajene akcije različnih akterjev, panoge in države, izobraževanja in zakonodaje (Zagovornik 2, osebni intervju, 2017, 11. januar).

Nujno je tudi povezovanje različnih deležnikov (posamezniki, podjetja in regulatorji oz. država). Zagovornik 4 poudarja, da mora potrošnik deloma poskrbeti zase, vlada mora poskrbeti za dobre zakone, čeprav je večina zakonov reaktivnih in ima posameznik le možnost kompenzacije za že storjeno škodo (kot je v ZDA). Podjetja pa morajo poskrbeti za varovanje podatkovne zasebnosti, tako kot to delajo na področju varovanja okolja, da so družbeno odgovorni za skrb nad podatki.

> We have the consumer which is partly responsible to take care of herself. We have the government which is partly responsible of making good laws but I think that most laws will be reactive in a way that the damage will be done and then you can get the compensation just like what is happening in the US. Then the third responsible part is companies who should take on data privacy in the same way as a lot of them have taken on the environment. That it is a part of being socially responsible to take care of our data (Zagovornik 4, osebni intervju, 2017, 8. februar).

6.4.2 Izboljšave na področju EU zakonodaje o varovanju zasebnosti in osebnih podatkov in njenega izvajanja

V nadaljevanju sledi predstavitev rezultatov intervjujev glede drugega glavnega zaključka pri vprašanju, kako bolje regulirati vedenjsko oglaševanje v prihodnosti, tj. da so v EU potrebne tudi izboljšave na področju zakonodaje o varovanju zasebnosti in osebnih podatkov, ki se nanašajo na razlage Uredbe 2016/679 in na nastajajočo ePR. Obravnavane so nekatere ključne teme: privolitev v vedenjsko oglaševanje ter alternativna podlaga zakonitega interesa, ki jo v ospredje potiska predvsem oglaševalska panoga, preglednosti in obveščanja o vedenjskem oglaševanju ter orodij za večjo odgovornost subjektov, ki izvajajo vedenjsko oglaševanje.

Privolitev kot temeljni mehanizem

Privolitev uporabnika v sledenje oziroma obdelavo osebnih podatkov za namen vedenjskega oglaševanja je trenutno v EU razumljena kot najboljši mehanizem za opolnomočenje posameznika, mehanizem, ki mu daje nadzor nad lastnimi osebnimi podatki. Čeprav je privolitev v pravnem okviru za varovanje osebnih podatkov le ena od šestih pravnih podlag, pravni okvir za varovanje zasebnosti v elektronskih komunikacijah temu zgledu ne sledi, ampak privolitev postavi za temeljno, najpogosteje edino pravno podlago za obdelavo osebnih podatkov uporabnikov elektronskih komunikacij. Da je privolitev najboljše orodje za opolnomočenje uporabnika, da ima nadzor nad svojo zasebnostjo pri uporabi elektronskih komunikacij, je prevladujoče mnenje zakonodajalca v EU (tudi zato, ker lahko vedno pride do obdelave občutljivih osebnih podatkov). Zagovornik 5 sicer poudari, da ga ta argument ne prepriča (Zagovornik 5, osebni intervju, 2017, 13. marec).

Kot je pokazala analiza pravnega okvira v EU pa, čeprav se v kontekstu zakonodajnih omejitev vedenjskega oglaševanja v EU poudarja privolitev posameznika kot bistveno varovalo za uporabnike in zahteva za ponudnike storitev, vedno obstajajo bodisi razlage, da je privolitev lahko tudi implicirana (s spremembami Uredbe 2016/679 je taka argumentacija sicer postala zelo otežena), bodisi so določene izjeme od zahteve po aktivni privolitvi, ob katerih se bijejo bitke glede njihovega obsega – kateri nameni, katere storitve in kateri piškotki bi lahko spadali v varni pristan takih izjem in ne bi bili podvrženi zahtevam za privolitev posameznika. Kot kaže razvoj ePR in razlage Uredbe 2016/679, bo razprava še naprej potekala o tem, kateri piškotki oz. kakšno sledenje je lahko potrebno za izvajanje

storitve, ki jo je zahteval uporabnik (pri čemer je trenutno izpuščena beseda nujno potrebno) – je to lahko tudi oglaševanje, brez katerega marsikateri medij argumentirano ne more ponujati storitve? Katere spletne strani lahko uporabnikom pogojujejo dostop do vsebine s privolitvijo v piškotke – pri čemer se ne upošteva opredelitve privolitve v Uredbi 2016/679– ta mora biti namreč svobodna in ne izsiljena. Katera obdelava metapodatkov je lahko potrebna v okviru izvajanja pogodbe oziroma dopustna kot nadaljnja obdelava, ne glede na namene, za katere so bili prvotno zbrani podatki – je to lahko tudi oglaševanje? V primeru katerih obdelav podatkov se lahko izvajalec zanaša na pravno podlago zakonitega interesa?

Ker se v kontekstu regulacije spletnega sledenja in piškotkov privolitev doslej ni izkazala kot učinkovito orodje, se razprave obračajo tudi k drugim pravnim podlagam, ki bi bile lahko učinkovitejše v varovanju posameznika (Zagovornik 5, osebni intervju, 2017, 13. marec).

Rezultati kažejo na številne dileme glede privolitve, njene veljavnosti in varstva, ki ga zagotavlja, ki bi morale biti upoštevane in rešene za boljši okvir regulacije v prihodnosti:

- privolitev je v praksi spekter različnih možnih tehničnih izvedb in ne enoznačna razlika med *opt in* in *opt out* (Oglaševalec 3, osebni intervju, 2017, 27. januar). Uredba 2016/679 zdaj sicer podrobneje določa, kaj privolitev je in kakšna mora biti, da je veljavna (strinjanje s splošnimi pogoji to ni), pa vendar so na tehnični ravni raznoliki pristopi;
- v svetu sodobnih tehnologij, v katerem poteka obdelava osebnih podatkov na skoraj vsakem koraku, Svetovalec 4 poudarja, da lahko govorimo le o utvari privolitve in o utvari nadzora, saj uporabniki brezvoljno privolijo v vse (t. i. privolitvena brezvoljnost ali angl. *consent fatigue*), ne berejo obvestil, jih ne razumejo in zato s privolitvijo sploh niso zaščiteni (Svetovalec 4, osebni intervju, 2017, 14. marec);
- ozreti bi se morali po drugih pravnih podlagah, kot je zakoniti interes, in varstvo posameznikovih pravic bi bilo učinkovitejše (Svetovalec 4, osebni intervju, 2017, 14. marec; tudi Oglaševalec 3, osebni intervju, 2017, 27. januar);
- privolitev ni podana svobodno; najpogosteje uporabnik nima možnosti nestrinjanja s pogoji uporabe storitve in obdelavo osebnih podatkov, čeprav je ta nesorazmerna, če mora ali želi uporabljati določene storitve:

> Mene pri privolitvah nekaj moti. Spet ena taka temeljna definicija pravic, da ideja pravic je nična, če je ni mogoče uveljaviti. Mislim, da je tu ta varianta, da imaš pravico se strinjat ali pa ne s pogoji uporabe, je dosti hipotetična […] Vedno več je poklicev, ko ne moreš ne biti na družabnih omrežjih, kar pomeni da nimaš možnosti se

nestrinjati s pogoji uporabe ali pa protestno se to iti, ker nisi zaposljiv ali pa ne moreš opravljati svojega dela (Medij 3, osebni intervju, 2017, 11. julij);

- veljavnost privolitve je odvisna od posameznikovega razumevanja situacije, česar pa v sodobnem, tehnološko razvitem svetu ne moremo pričakovati (Svetovalec 4, osebni intervju, 2017, 14. marec). Pomanjkljivo razumevanje se nanaša tako na omejene sposobnosti povprečnega uporabnika elektronskih komunikacij, da razume delovanje tehnično kompleksnega sveta spleta in spletnega oglaševanja, kot tudi na pomanjkljive informacije, ki jih ponudniki storitev o obdelavi osebnih podatkov navajajo (Zagovornik 3, osebni intervju, 2017, 16. februar). Privolitev lahko učinkovito deluje le v okolju, ki je na vseh ravneh preglednejše in zdravo (Zagovornik 3, osebni intervju, 2017, 16. februar);
- posamezniki redko spreminjajo privzete nastavitve in tako pogosto ne izrabijo možnosti za do zasebnosti prijaznejše delovanje spletnih storitev. Zagovornik 4 meni, da smo preleni, da bi izkoristili možnosti zavrnitve, ki jih imamo (Zagovornik 4, osebni intervju, 2017, 8. februar);
- problematika mladoletnih in otrok, v imenu katerih naj bi veljavno soglašali starši, kar pa je na spletu težko preverjati, kot tudi starost otrok (Svetovalec 4, osebni intervju, 2017, 14. marec).

Koncept privolitve uporabnika, na katerem temelji pravzaprav vsa regulacija vedenjskega oglaševanja danes v EU, ima resne pomanjkljivosti, zaradi česar uporabniki elektronskih komunikacij niso varovani pred invazivnimi praksami sledenja in profiliranja, čeprav to področje ureja zakonodaja. Kljub temu ostaja orodje, v katerem zakonodajalec, pa tudi druge družbene skupine, vidijo največ potenciala za opolnomočenje uporabnika elektronskih komunikacij (WP29, 2017; Evropska komisija, 2018a; itd.).

Intervjuji s strokovnjaki so pokazali tudi nekaj ključnih poudarkov o tem, kakšno mesto bi morala zavzemati privolitev v prihodnji regulaciji vedenjskega oglaševanja, da bo veljavna in bo uporabnika dejansko opolnomočila:

- večji poudarek bi moral biti na tehnoloških rešitvah in standardih za podajo privolitve, ki bi zagotavljali enotnejše implementacije mehanizmov v praksi in bi pripomogel k preglednosti in jasnosti (Zagovornik 5, osebni intervju, 2017, 13. marec);

- boljše obveščanje uporabnikov in delovanje na izmenjavi vrednosti: Uredba 2016/679 sicer predpisuje vsebino, o čem mora biti posameznik obveščen, sogovorniki pa poudarjajo še dodatne kontekstualne dejavnike, ki bi pripomogli k veljavnosti privolitve, in sicer da je posameznik za privolitev vprašan v pravem trenutku in to ne poseže negativno v njegovo aktivnost (Oglaševalec 2, osebni intervju, 2017, 7. februar). Pojasnilo o tem, za kakšno menjavo vrednosti gre v konkretnem primeru, bi pripomoglo k jasnosti situacije (Oglaševalec 2, osebni intervju, 2017, 7. februar). Plastenje informacij je nadaljnji predlog – naprej bistvene in nato podrobnejše;
- privolitev mora uporabnik podati aktivno in ne pasivno, kot pojasnjuje že Uredba 2016/679 (Svetovalec 4, osebni intervju, 2017, 14. marec, Oglaševalec 3, osebni intervju, 2017, 27. januar);
- pomen dobre uporabnikove izkušnje: treba je iskati možnosti, ki bodo za uporabnika elektronskih komunikacij najmanj moteče (Oglaševalec 2, osebni intervju, 20177. februar);
- privolitev le v situacijah, v katerih ima posameznik dejansko možnost odločanja in zavrniti neko obdelavo osebnih podatkov, ne da bi bila posledica tega škoda za ponudnika storitev. Če je mehanizem privolitve uporabljen prevečkrat, zvodeni. Svetovalec 4 poudarja, da je uporabniku nemogoče operirati z vsemi zahtevami za privolitev podjetij in javnega sektorja. Mogoče je bil to učinkovit mehanizem 40 let nazaj, ko ni bilo toliko primerov privolitev, ampak danes to nikakor ne deluje več. Meni, da bi morala privolitev biti uporabljena v pomembnejših primerih, pri obdelavi občutljivih osebnih podatkov (Svetovalec 4, osebni intervju, 2017, 14. marec);
- omejitev zanašanja na privolitev le v situacijah, ki pomenijo tveganje za posameznika, saj je privolitev lahko učinkovito orodje le, če je uporabljena dovolj redko, v le nekaterih situacijah, da ostane pomenljiva in ne pride do t. i. privolitvene utrujenosti, ki se kaže v tem, da uporabniki le brezvoljno klikajo »Strinjam se« (Regulator 2, osebni intervju, 2017, 31. marec).
- Rešitev je lahko, da uporabnik npr. poda le privolitev v nekatere namene na ravni brskalnika (npr. spletno analitiko) in je zaprošen za vnovično privolitev le, ko gre za drugačne namene (npr. vedenjsko oglaševanje). Tako privolitev ne zvodeni zaradi svoje pogostosti. Spletni mediji bi tako lahko izrabili pozitivne ekonomske plati sledenja in vedenjskega oglaševanja ter hkrati spoštovali želje uporabnikov. Če bi posameznik podal privolitev nekemu spletnemu mediju, da mu sledijo tudi tretje strani

(angl. *third party trackers*), bi ta privolitev veljala le za sledenje znotraj te prve spletne strani in ne za ves splet, kjer se tretje strani tudi nahajajo (Regulator 2, osebni intervju, 2017, 31. marec).

Zakoniti interes kot podlaga za vedenjsko oglaševanje

Ker privolitev na področju vedenjskega oglaševanja ne dosega svojega cilja, se odpirajo razprave o alternativah. Sogovorniki poudarjajo, da imajo različne pravne podlage različne namene in so primerne za različne kontekste. Posamezna ozka skupina obdelav, ki pomeni tveganje za posameznika, je lahko prepovedana z zakonom, sledi ji področje, ki je lahko prepuščeno prosti presoji posameznika in njegovi privolitvi, ter še eno področje, kjer posamezniki razumejo, da je obdelava osebnih podatkov del aktivnosti ali posla in bi lahko obdelava potekala na podlagi zakonitega interesa posameznika (Oglaševalec 3, osebni intervju, 2017, 27. januar).

Poleg poudarjanja drugih pravnih podlag sogovorniki omenjajo tudi druga orodja, ki jih omogoča zakonodaja in bi lahko pripomogla k boljšemu varstvu posameznikov, pa hkrati na oglaševalsko panogo ne bi tako negativno vplivala, npr. upoštevanje načela odgovornosti, izvedba ocen tveganja in obveščanje. Varovanje posameznikov je učinkovitejše, če morajo organizacije preučiti, kakšno tveganje pomeni obdelava osebnih podatkov in kakšni so negativni učinki ter podatke skladno s tem varovati ter posameznika ustrezno seznanjati z obdelavo osebnih podatkov (Svetovalec 4, osebni intervju, 2017, 14. marec).

Nekateri zagovarjajo strožje omejitve, ki naj jih predpiše zakon in so tako onkraj posameznikove odločitve (Zagovornik 5, osebni intervju, 2017, 13. marec). Kritiki tak pristop označujejo za paternalističen in neučinkovit na dolgi rok (Oglaševalec 3, osebni intervju, 2017, 27. januar).

Čedalje veljavnejši pa postaja argument, da bi podjetja lahko vedenjsko oglaševanje izvajala na podlagi svojega zakonitega interesa, ki pretehta nad pravicami posameznikov, zlasti zato ker je veliko podatkov posameznikov že zbranih za prvotno drugačne namene – elektronske komunikacijske storitve je pravzaprav nemogoče uporabljati brez sledenja in beleženja podatkov o uporabi – in so za vedenjsko oglaševanje uporabljeni naknadno, kar načenja vprašanja primernih podlag za nadaljnjo obdelavo. V tem okviru se razprave obračajo tudi k

zakonitemu interesu (Regulator 1, osebni intervju, 2017, 15. februar). Vedenjsko oglaševanje je pogosto del poslovnega modela spletne storitve ali aplikacije, ki je uporabniku na voljo brezplačno, oziroma je prilagojena za njegovo uporabo – osebno prilagojena. Od tega ima posameznik lahko večjo korist, kot je zanj negativnih posledic v smislu posega v zasebnost, poleg tega uporabniki tako raven storitev sami želijo. V vedenjskem oglaševanju, ki ne temelji na občutljivih podatkih in ne posega v pravice posameznika, ne diskriminira, nekateri intervjuvanci ne vidijo škode za posameznika, razen tega, da ga včasih razburjajo (Svetovalec 4; osebni intervju, 2017, 14. marec; tudi Regulator 1, osebni intervju, 2017, 15. februar). Svetovalec 4 poudari, da moramo biti v takih primerih realistični. Če želimo brezplačne storitve, se tako financirajo. Če je nekomu npr. všeč *The Guardian* [časnik iz Združenega Kraljestva, op. avtorja], lahko plača 5 funtov za aplikacijo, ampak on se za to ni odločil, saj se mu njihovo oglaševanje in sledenje za ta namen ne zdi poseben poseg (Svetovalec 4, osebni intervju, 2017, 14. marec).

V nekaterih situacijah je težko zatrjevati zakoniti interes, saj je poseg v posameznikove pravice prevelik in pretehta zakonite interese podjetja ali organizacije, npr. tam, kjer prihaja do diskriminacije, posebej na podlagi občutljivih podatkov in pri ranljivih skupinah. Omenjeno je bilo, da bi ob zaostrovanju pogojev za obdelavo podatkov v *ad tech* panogi številna podjetja ostala brez pogojev za obstoj, saj se ne bi mogla financirati iz oglaševanja, kar govori v korist njihovemu legitimnemu interesu za obdelavo podatkov posmeznikov (Svetovalec 4, osebni intervju, 2017, 14. marec; Svetovalec 2, osebni intervju, 2017, 25. januar).

Pravna podlaga zakonitega interesa za obdelavo osebnih podatkov pomeni, da mora podjetje biti sposobno bolje utemeljiti, kako je njegov poslovni model odvisen od podatkov, in izvesti tehtanje med interesi ter sprejeti varovala, ki omejijo morebitne posege v pravice posameznikov – npr. prek ustreznega obveščanja, omogočanja izvajanja pravic posameznikov, omogočanja možnosti zavrnitve obdelave osebnih podatkov ipd. Svetovalec 4 poudarja, da mora biti to utemeljevanje vedno opravljeno glede na konkretno situacijo. Če ni mogoče utemeljiti, da je poseg v pravice posameznika pretehtan, bi morali iskati privolitev posameznika. Izpostavi, da je tudi oglaševanje lahko v zakonitem interesu podjetja, če ne škodi pravicam posameznika, a se hkrati strinja, da obstaja tudi oglaševanje, ki v pravice posega. Uporaba pravne podlage zakonitega interesa naj bi bila za posameznike boljša kot

vztrajanje pri nujnosti privolitve, saj morajo subjekti pretehtati svoje odločitve in upoštevati tako njihove interese, kot tudi interese in pravice posameznikov (Svetovalec 4, osebni intervju, 2017, 14. marec). Poudarjeno je pa bilo, da so bistvena dodatna varovala, ki bi jih moral določiti zakonodajalec, saj gre za področje, na katerem so možne zlorabe Hkrati pa se moramo zavedati tudi nevarnosti slabe zakonodaje oz. velikih vplivov na zakonodajalca, lobiranja, ki ga je v tem sektorju ogromno, še posebej ob razvoju Uredbe 2016/679 in ePR (Zagovornik 3, osebni intervju, 2017, 16. februar).

Na praktični ravni so bili omenjeni tudi naslednji premisleki o uporabi legitimnega interesa kot pravne podlage:

- če bi za prve strani veljal blažji režim za lastno sledenje, bi imele možnost več zaslužiti in s tem bi imele tudi večji nadzor nad svojimi podatki. Tako bi prve stranke imele več možnosti in motivacije za pogajanje glede pogodbenih razmerij s tretjimi stranmi (Regulator 2, osebni intervju, 2017, 31. marec);
- prva stran, torej tista, ki jo uporabnik obišče, ima vsaj deloma zagotovo možnosti zatrjevati zakoniti interes za sledenje in oglaševanje, tretje strani pa to težko trdijo. Pri prvi strani uporabnik ve, kdo obdeluje podatke, tudi če ni vprašan za soglasje, pri tretjih straneh pa tega ne ve in je pri zatrjevanju zakonitega interesa velika težava že obveščanje uporabnikov o obdelavi (Regulator 2, osebni intervju, 2017, 31. marec);
- težko bi bilo določiti, kakšne tehnične ukrepe bi morale sprejeti spletne strani, da bi lahko izpolnile merila zakonitega interesa po tehtanju pravic uporabnikov. Te tehnične ukrepe in rešitve bi nadzorni organ tehnično težko nadzoroval, kar bi pomenilo, da nobeden ne bi spoštoval takih omejitev (Regulator 2, osebni intervju, 2017, 31. marec). Koncept odgovornosti, po katerem mora biti upravljavec podatkov sposoben izkazati, da deluje skladno, in imeti primerno dokumentacijo, sam po sebi ni rešitev za vprašanje težavnosti nadzora nad tehničnimi rešitvami za omejevanje sledenja. Možnost za boljši nadzor so usposobljene tretje stranke – revizorji (npr. certificiranje);
- zmeda za uporabnike, če bi za slednje nekatera podjetja potrebovala privolitev, druga pa ne, s čimer bi prišlo do paradoksa, da bi nezanesljiva podjetja lahko sledila na podlagi privolitve (z vsemi slabostmi), zanesljiva pa brez privolitve, na podlagi zakonitega interesa (Regulator 2, osebni intervju, 2017, 31. marec);
- pravno podlago v zakonitem interesu je mogoče hitro zlorabiti; tak pristop k regulaciji je tvegan (Zagovornik 3, osebni intervju, 2017, 16. februar).

Preglednost, obveščanje

Preglednost obdelave osebnih podatkov oziroma obveščanje posameznikov o njej ter omogočanje izvrševanja posameznikovih pravic je eden bistvenih temeljev za zakonito obdelavo osebnih podatkov uporabnikov elektronskih komunikacij, ne glede na to, ali ta temelji na njihovi privolitvi ali pa se pomaknemo k razumevanju, da je vedenjsko oglaševanje lahko v zakonitem interesu podjetij in organizacij, posameznik pa ga ima morda pravico naknadno zavrniti. Boljše obveščanje je lahko konkurenčna prednost za podjetja. Obveščanje o obdelavi osebnih podatkov mora vključevati podatke o tem, kdo je upravljavec podatkov, za kakšen namen se ti obdelujejo in koliko časa hranijo ter komu se morda posredujejo. Novi okvir za varstvo osebnih podatkov temu med drugim dodaja še informacije o pravicah, ki jih imajo posamezniki na voljo glede svojih podatkov, pa podrobnosti o morebitnem profiliranju in možnostih, ki so posamezniku na voljo v zvezi z vplivanjem na avtomatsko sprejete odločitve. Trenutne razmere so klavrne, saj posamezniki obvestil niti ne berejo niti jih ne razumejo.

Če posamezniki niso pošteno in ustrezno obveščeni o tem, kaj se dogaja z njihovimi podatki, to vpliva na zmanjšanje zaupanja, ki ga imajo v ponudnike digitalnih storitev in na koncu vodi k blokiranju oglasov, kar je za oglaševalsko panogo najslabša možnost, zato bi morala delovati v smeri večje preglednosti in boljšega obveščanja. (Svetovaelc 4, osebni intervju, 2017, 14. marec). Obveščati bi morali pomenljivo, o ključnih stvareh:

- posamezniki hočejo predvsem vedeti o praksah, ki jih ne pričakujejo (npr. če se bo izvajalo profiliranje, če bodo podatki posredovani tretjim), ne toliko o obdelavah podatkov, ki so normalne, zato da se npr. obdela določeno spletno naročilo. Svetovalec 4 to poimenuje pomenljiva preglednosti (angl. *meaningful transparency*) (Svetovalec 4, osebni intervju, 2017, 14. marec);
- v različnih kontekstih delimo različne podatke, na športni spletni strani npr. drugačne kot na spletni strani, povezani z zdravstvenimi težavami. Za uporabnike v slednji situaciji je lahko bolj kritično obveščanje o tem, kateri podatki se delijo, kot o tem, točno katere tretje stranke bodo podatke prejele, tudi zato, ker večina uporabnikov pozna le nekaj največjih sledilcev – tretjih strank –, kot je npr. Facebook, v oglaševalski panogi pa je tudi veliko malih podjetij, ki niso širše poznana (Regulator 2, osebni intervju, 2017, 31. marec);

- pri praksah, ki bolj posežejo v pravice posameznika (npr. *fingerprinting*), se je treba bolj potruditi pri obveščanju in ne zgolj navajati pavšalnih izjav. (Oglaševalec 3, osebni intervju, 2017, 27. januar);
- o tem, katere pravice imajo posamezniki glede svojih podatkov (Svetovalec 4, osebni intervju, 2017, 14. marec);
- obveščati bi morali v jasnejšem, dostopnem jeziku, ne v pravniškem jeziku, nerazumljivem običajnemu uporabniku, predstaviti informacije v plasteh, preprosto. Namen obveščanja uporabnika ni izogibanje pravni odgovornosti, ki zahteva pravniški jezik, ampak razlaga praks obdelave podatkov, ki jo bo povprečen uporabnik sposoben razumeti (Svetovalec 2, osebni intervju, 2017, 25. januar):

  > Vedno se je treba postaviti v kožo povprečnega uporabnika. […] [P]ovprečen gledalec BBC-ja, njegov povprečen besedni zaklad je 1.400, 1.200 besed […] tako malo […] In moramo s preprostimi besedami najbolj zakomplicirano stvar znati razložiti. To je umetnost dobrega javnega nastopanja. Po tem principu, kako bomo zdaj povprečnemu uporabniku razložili programatično oglaševanje […] [Ž]e sami oglaševalci imajo znotraj podjetja težave to razumeti. (Svetovalec 1, osebni intervju, 2017, 23. januar)

- najpomembnejše informacije bi morale biti podane na kratko, uporabnik pa bi imel nato možnost klikniti na daljša pojasnila. Obvestilo bi moralo doseči uporabnika v primernem času in kontekstu (npr. »Zakaj mi je prikazan ta oglas?« in je uporabnik obveščen v času in kontekstu, ki ga sam želi) (Oglaševalec 3, osebni intervju, 2017, 27. januar). Obvestilo hkrati ne sme biti zavajajoče.

Pomembno je vprašanje odgovornosti za obveščanje v ekosistemu vedenjskega oglaševanja. Načeloma o obdelavi osebnih podatkov in tudi o piškotkih obvešča tisti, ki podatke obdeluje oz. piškotek postreže, kar pa je v spletnem svetu oteženo. Večino sledenja in nameščanja piškotkov ter zalednih operacij dajanja spletnih oglasov izvajajo t. i. tretje stranke – torej ne spletne strani, ki jih uporabnik dejansko obišče. Na neki medijski spletni strani je lahko tudi več deset zalednih sledilcev, ki do uporabnika nimajo samostojne povezave, le prek prve strani. Zato je v praksi prevladalo mnenje, da o tretjih straneh obvešča prva, obiskana spletna stran, saj ima možnost vpliva na to, katere sledilce bo na svojem spletnem mestu dopustila. Hkrati pa ne more vplivati na to, kako tretji obdelujejo podatke, ali so njihove informacije o obdelavi podatkov resnične ipd. Sogovorniki tako poudarjajo, da bi odgovornost za obveščanje uporabnikov morala nositi celotna veriga ponudnikov v ekosistemu spletnega oglaševanja, torej prva stran v sodelovanju s tretjimi stranmi, čeprav je na tem področju v

praksi še mnogo dilem (Regulator 3, osebni intervju, 2017, 15. februar; Regulator 2, osebni intervju, 2017, 31. marec).

Kot je pokazala analiza pravnega okvira, se pristopi do odgovornosti v praksi nadzornih organov lahko razlikujejo (CNIL, 2017; WP29, 2011), kot kaže razvoj ePR in analiza zadnjega dostopnega besedila, pa naj bi bile tretje strani samostojno odgovorne za pridobivanje soglasja in za obveščanje – lahko pa prvo stran pooblastijo, da to pridobi zanje.

Odgovornost subjektov, ki izvajajo vedenjsko oglaševanje

Odgovornost upravljavcev podatkov (angl. *accountability*) je eden od novih pojmov prenovljenega okvira za varstvo osebnih podatkov v Evropi ter se nanaša na to, da morajo biti organizacije in podjetja odgovorni pri obdelavi osebnih podatkov in tudi sposobni izkazati nadzornemu organu in javnosti, da spoštujejo pravila. Poudarek je tudi na ustreznem vodenju dokumentacije, ki izkazuje odgovorno delovanje upravljavca (Zagovornik 5, osebni intervju, 2017, 13. marec). Odgovornost ima tudi vlogo pri zmanjševanja tveganja za izpostavljenost nadzoru s strani nadzornega organa (Svetovalec 2, osebni intervju, 2017, 25. januar). Kljub pozitivnim stranem spodbujanja in zapovedovanja odgovornosti upravljavcev osebnih podatkov pa je na mestu ugotovitev, da je to le sredstvo uveljavljanja pravil – bistvena so namreč dobra pravila (Regulator 4, osebni intervju, 2017, 16. februar).

Koncepta vgrajene zasebnosti in izvajanja ocen tveganja za zasebnost (angl. *privacy by design/default* in *PIA*) sta ena ključnih novosti v okviru večje odgovornosti podjetij in organizacij ter jih usmerjata k temu, da že na začetku presodijo, kakšen vpliv ima obdelava osebnih podatkov na posameznika, ter da si prizadevajo sprejeti ukrepe, ki bi posege omejili, oziroma da snujejo svoje storitve tako, da je zasebnost vgrajena v delovanje sistemov. Nova orodja odgovornosti so lahko tudi dobro orodje za grajenje odnosa s strankami ter dvigovanje konkurenčne prednosti na račun boljšega varovanja podatkov strank (Svetovalec 3, osebni intervju, 2017, 13. januar). Poudarjen je bil tudi pomen uradnih oseb za varstvo osebnih podatkov (še eno novo orodje odgovornosti) ter zagotavljanja skladnosti in komunikacije z operativnimi strukturami v organizaciji, ki dejansko vedo, kaj in kako se s podatki dogaja (Svetovalec 2, osebni intervju, 2017, 25. januar).

Razvoj ePR in izvajanje Uredbe 2016/679

ePR naj bi določala strožje pogoje za vsakršno sledenje uporabnikom, ne glede na kanal ali tip naprave (tudi za sledenje prek naprav, povezanih v internet stvari). V začetnem osnutku je bila temelj le privolitev uporabnika naprave, zadnji osnutek pa že dopušča tudi nekatere obdelave osebnih podatkov na alternativnih podlagah, podobnih zakonitemu interesu, kar upošteva prizadevanja oglaševalske panoge, da bi pokazala na prednosti, ki jih ima tehtanje med različnimi interesi in varovanjem uporabnikov, ter po uskladitvi določb ePR z Uredbo 2016/679, ki prav tako pozna različne pravne podlage za obdelavo osebnih podatkov, ki se uporabljajo glede na kontekst. Odpira se vprašanje, koliko naj že zakonodaja opredeli različne omejitve za sledenje in koliko je to odločanje lahko prepuščeno uporabniku, glede na njegovo omejeno tehnično poznavanje kompleksne problematike – naj bo zakonodaja strožja ali naj dopušča možnost za presojo posameznih primerov in okoliščin glede na tveganja za posameznika (Regulator 4, osebni intervju, 2017, 16. februar).

Negativna posledica nedoločne zakonodaje je preveč prostora za razlago prvil in s tem raznolike prakse »skladnosti« na trgu EU. Nadzor nad to uredbo naj bi vsaj deloma prevzeli nadzorni organi za varstvo osebnih podatkov, ki nadzorujejo tudi izvajanje Uredbe 2016/679, kar odpira vprašanja učinkovitosti, virov in tehničnih sposobnosti. ePR se nanaša na širok spekter naprav in obdelav osebnih podatkov ter ga bo zato težko upoštevati in nadzorovati. Kot poudarja Svetovalec 4 se nanaša na vse, lahko se nanaša na našo celotno spletno digitalno eksistenco (Svetovalec 4, osebni intervju, 2017, 14. marec). Vprašanje je tudi, kakšen je odnos med Uredbo 2016/679in ePR. ePR je sicer specialni predpis in njene določbe prevladajo v okviru sektorja elektronskih komunikacij, vendar je ta, kot pojasni Svetovalec 4, tako širok, da se ePR pravzaprav lahko nanaša na vse elektronsko komuniciranje, tudi na komunikacijo naprava-naprava (Svetovalec 4, osebni intervju, 2017, 14. marec).

ePR bo tako veljala za ogromno obdelav podatkov v elektronskih komunikacijah, nekateri pa opozarjajo, da v njej ni glavnih naprednih premislekov iz Uredbe 2016/679, ki so osredinjeni na obdelave, ki za posameznika pomenijo tveganje. Ni podlage zakonitega interesa, zelo malo je izjem, ni pristopa ocene tveganja. Svetovalec 4 zato meni, da bo Uredba 2016/670 praktično odveč, če bo veljala le še za npr. podatke zaposlenih. Čeprav se strinja, da ni popolna, pa vseeno vsebuje nekatere dobre elemente, kot je certificiranje, kodeksi, pristop ocene tveganja, odgovornosti upravljavcev in preglednosti (Svetovalec 4, osebni intervju, 2017, 14. marec).

Izražena je bila bojazen, da kombinacija ePR in Uredbe 2016/679 pomeni odpiranje vrat nejasnim pravilom, saj po eni strani poudarja pomen privolitve in po drugi dopušča uporabo podatkov za druge namene (Regulator 1, osebni intervju, 2017, 15. februar). Hkrati ePR širi nabor tistih, katerih podatki so varovani – ne le podatki fizičnih oseb, ampak podatki vseh naročnikov in uporabnikov storitev, ki so lahko tudi pravne osebe, kar prinaša velike spremembe in dileme glede izvajanja takih pravil, saj podatki podjetja niso osebni podatki in običajno niso varovani kot taki (Svetovalec 4, osebni intervju, 2017, 14. marec).

Ali bo posodobljena ePR dejansko prinesla več preglednosti na trgu sledenja za namen vedenjskega oglaševanja, ki v praksi trenutno deluje, kot da omejitev v zakonodaji ne bi bilo, je veliko vprašanje. Veliko je tudi pritiskov lobistov na Evropsko komisijo, ki pripravlja ePR. Zagovornik 3 izpostavlja bojazen, da bo ta pred sprejemom postala le bleda senca zamišljenih ukrepov za boljše varstvo posameznikovih pravic. Ker močne omejitve v smislu privolitve uporabnika in prepovedi nekaterih praks obdelave osebnih podatkov vplivajo neposredno na poslovne modele uspešnih ponudnikov spletnih storitev, je na njihovi strani močan interes, da preprečijo sprejem stroga zakonodaje in skušajo vplivati na zakonodajalca, da sprejme ukrepe, ki zanje niso tako omejujoči. Pričakuje še velike bitke na tem področju.

> I don't want to get it even more watered down. I want it to be strengthened and that these abusive online tracking […] and online surveillance is blocked so we can have a real, safe online life. And that the businesses can develop in an environment of trust and that we are not profiled and being sold to third parties. […] I think the commission is really trying to make a good instrument out of it but there are many lobby groups which are still very influential which seem – it feel that they lost in the GDPR and they want to regain that in the ePrivacy. I do not expect it because one, that's my job to make it a good ePrivacy provision but I expect a big battle. (Zagovornik 3, osebni intervju, 2017, 16. februar)

6.5 Sinteza ugotovitev dokumentarne analize in analize intervjujev

Sinteza ugotovitev dokumentarne analize in analize intervjujev v tabeli 6.1 prikaže, kako se ugotovitve glede na tri raziskovalna vprašanja povezujejo, kje se dopolnjujejo in podpirajo ter kje ugotovitve različnih metod raziskovanja odstopajo oziroma si nasprotujejo. Metoda dokumentarne analize je bila deloma uporabljena za identifikacijo ključnih tem, glede na katere je potekalo intervjuvanje in poznejša analiza rezultatov, predvsem na področju vprašanja trenutnega stanja regulacije in prihodnje regulacije vedenjskega oglaševanja. Deloma pa je služila preverjanju in dopolnjevanju rezultatov, ki izhajajo iz ekspertnih intervjujev. Na drugi strani so intervjuji služili kot primarna metoda pri vprašanjih delovanja

oglaševalske panoge, učinkovitosti vedenjskega oglaševanja in kot bistveni vir pri vprašanju prihodnje regulacije tega področja. Ekspertni intervjuji so bili prav tako v vlogi preverjanja veljavnosti zaključkov dokumentarne analize in razumevanja trenutnega stanja regulacije na tem področju.

Tabela 6.1: Sinteza primerjave ugotovitev dokumentarne analize in analize intervjujev

1. raziskovalno vprašanje	**Dokumentarna analiza**	**Analiza intervjujev**
Učinkovitost VO, prednosti in izzivi za deležnike v industriji (oglaševalci, *ad tech*, založniki)	Ugotovitve obeh metod se dopolnjujejo in si v splošnem ne nasprotujejo, saj ponujajo odgovor na raziskovalno vprašanje z različnih vidikov – pravnega in z vidika delovanja panoge v praksi.	
	Opredeljuje deležnike v ekosistemu vedenjskega oglaševanja (oglaševalci, *ad tech*, založniki, mediji) in njihove vloge ter odgovornosti predvsem s stališča urejenosti v pravu.	Analiza intervjujev ugotovitve dopolnjuje z odgovori na vprašanja delovanja panoge vedenjskega oglaševanja in njene organiziranosti ter ponuja specifične odgovore na vprašanja glede učinkovitosti vedenjskega oglaševanja pri različnih deležnikih.
	Dokumentarna analiza konkretizira izzive varovanja podatkov posameznikov in ponuja odgovore na konkretna pravna vprašanja varovanja osebnih podatkov v verigi izvajalcev vedenjskega (programatičnega) oglaševanja.	Poudarja panožne izzive v smislu varovanja podatkov posameznikov, njenih strank, kadar imajo dostop do njih oglaševalski partnerji, *ad tech*.
Prednosti in izzivi za posameznike oz. uporabnike	Ugotovitve obeh metod se dopolnjujejo in podpirajo; v delu, ko gre za poudarjanje izzivov, ki jih vedenjsko oglaševanje prinaša posameznikom, si ne nasprotujejo. Razlikujejo pa se ugotovitve v delu prednosti, ki jih vedenjsko oglaševanje prinaša posameznikom – te izhajajo predvsem iz ugotovitev intervjujev.	
	Ugotovitve konkretizirajo pravna vprašanja, povezana s posegi v posameznikove pravice in poudarjajo izzive, ki jih vedenjsko oglaševanje prinaša posameznikom.	Ugotovitve kažejo na prednosti in slabosti vedenjskega oglaševanja za posameznike

2. raziskovalno vprašanje	**Dokumentarna analiza**	**Analiza intervjujev**
Izzivi VO za posameznike in družbene procese	Ugotovitve obeh metod se dopolnjujejo in podpirajo, saj ponujajo odgovor na raziskovalno vprašanje z različnih vidikov – pravnega in z vidika praktičnih posledic VO na življenje posameznika in družbene oz. demokratične procese.	
	Dokumentarna analiza podrobno opredeljuje pravne okvire za varovanje pravice do zasebnosti pri vedenjskem oglaševanju in odkriva njihove pomanjkljivosti.	Analiza intervjujev opredeljuje štiri kategorije izzivov (za zasebnost posameznika, diskriminacijo, oženje izbire in izzive za demokratične procese).

Mehanizmi za zaščito posameznikov pred negativnimi posledicami VO	Ugotovitve obeh metod se dopolnjujejo; obe metodi sta uporabljeni kot način verifikacije ugotovitev. Ugotovitve si deloma nasprotujejo pri vprašanju samoregulacije in standarda ne sledi.	
	Podrobno opredeljuje načine varovanja pravice do zasebnosti pri vedenjskem oglaševanju v pravu EU in ZDA.	Opredeljujejo različna tehnična orodja za varovanje zasebnosti, možnosti privolitve v piškotke, protireklamne vtičnike, zasebnosti prijazne tehnologije, kritično glede učinkovitosti teh orodij.
Varovanje pravice do informacijske zasebnosti kot jo zagotavlja vejavni regulatorni okvir v EU in ZDA, v širšem političnem kontekstu konkurenčnosti med državami	Ugotovitve obeh metod se dopolnjujejo; s pomočjo dokumentarne analize so verificirane ugotovitve intervjujev in obratno. Med regulacijo v ZDA in EU so pomembne konceptualne razlike. Širši politični kontekst zahteva nastanek regulacije. Deloma se ugotovitve razlikujejo. Intervjuji kritično osvetlijo vidik (ne)učinkovitosti pravnih možnosti.	
	Pojasni okvir regulacije VO v EU in ZDA, koncepte privolitve posameznika v pravu, podrobno opredeljuje samoregulacijo in standardizacijo na tem področju.	Ugotovitve kažejo na širše izzive pri standardizaciji, kritično glede učinkovitosti samoregulacije. Poudarjajo neučinkovitost pravnih rešitev.

3. raziskovalno vprašanje	**Dokumentarna analiza**	**Analiza intervjujev**
Splet strategij za boljšo regulacijo VO	Dokumentarna analiza v tem sklopu je predvsem prispevala nabor in opredelitev strategij za regulacijo, rezultati intervjujev pa kažejo na konkretne rešitve znotraj nabora strategij. Ugotovitve se tako medsebojno dopolnjujejo.	
	Splet strategij vključuje: pravila in nadzor (zakonodajo, izboljšave na področju izvajanja in nadzora, opolnomočenje in izobraževanje posameznikov) in druge strategije (samoregulacija, pravila na davčnem področju, področju varovanja konkurence, pravice do obveščenosti in svobodnih volitev, etika in družbena odgovornost)	Konkretne ugotovitve znotraj nabora strategij.
Izboljšave zakonodaje v EU	Ugotovitve dokumentarne analize in intervjujev se dopolnjujejo. Razlikujejo se glede vprašanj pravnih podlag, ki bi v prihodnje lahko pomenile boljše varstvo pravic posameznikov. Ugotovitve intervjujev odkrivajo podrobnejše rešitve na področju pravnih podlag, obveščanja in mehanizmov odgovornosti.	
	Ugotovitve kažejo na pomembnost koncepta privolitve za regulacijo VO in njegovo prevlado. Opredeljujejo pravne zahteve glede obveščanja in orodij odgovornosti.	Ugotovitve kažejo, da je privolitev neučinkovit mehanizem in da bi morale po eni strani obstajati strožje omejitve v zakonu, po drugi strani pa blažje omejitve glede na koncept zakonitega interesa. Konkretizirajo vprašanja boljšega obveščanja in orodij odgovornosti.

7 DISKUSIJA UGOTOVITEV GLEDE NA TEORETSKI OKVIR IN ODGOVORI NA RAZISKOVALNA VPRAŠANJA

7.1 Diskusija ugotovitev glede na teoretski okvir

V nadaljevanju so ključne ugotovitve empirične raziskave postavljene v kontekst konceptualnega teoretičnega okvira. Diskusija zajema vidike teorij tržnega komuniciranja o oglaševalski navlaki, selektivni zaznavi in učinkovitosti vedenjskega oglaševanja, vidike študij medijske potrošnje in občinstev, ki poudarjajo procese mediatizacije, vseprisotnost in interaktivnost novih medijev, njihovo kombiniranje v medijske repertoarje (Luthar in Oblak Črnič, 2015), vidike aktivnega občinstva in po drugi strani občinstva, ki je ujeto v prakse vedenjska oglaševanja, tudi zaradi vidikov pismenosti in informacijskih ločnic. Diskusija zajema teorije zasebnosti in njenega pomena v kontekstu življenjskih situacij posameznika ter drugih pravic, procese komodifikacije, ki so značilni za vedenjsko oglaševanje, in politično ekonomskih struktur, ki določajo odnose moči v svetu novih medijev. V konceptualni okvir povežemo vprašanja regulacije vedenjskega oglaševanja – njeno trenutno stanje in možne izboljšave v prihodnosti.

Ekosistem vedenjskega oglaševanja z vidika koncepta oglaševalske navlake, selektivne zaznave in s tem povezane učinkovitosti

Empirične ugotovitve nakazujejo, da je bistvo učinkovitosti vedenjskega oglaševanja v njegovi relevantnosti in privlačnosti za posameznika. Ker je oglaševanje prilagojeno njegovim predvidenim interesom, je večja možnost, da se bo nanj želeno odzval. Z vidika t. i. oglaševalske navlake (Ha, 1996, v: Ha in McCann, 2008, str. 570) in velikih količin neuredniških vsebin v medijih ter omejene zmožnosti za predelavo informacij, ki jo imamo potrošniki (Schneider in drugi, 1984) je za oglaševalca bistveno, da mu uspe pritegniti selektivno pozornost posameznika na svojo vsebino (Smith in Buchholz, 1991). Model verjetne vpletenosti tukaj kot bistveno komponento poudari vpletenost v oglaševani produkt (Ha, 1999, v: Ha in McCann, 2008, str. 574). Prilagajanje oglasov posameznikovim zaznanim in pričakovanim potrebam ter željam je tako bistveni element učinkovitejšega oglaševanja. Z večanjem natančnosti profila posameznika pa se izboljša tudi prilagajanje. Večja učinkovitost

oglaševanja, ki posamezniku po eno strani olajša življenje in mu prihrani vire, pa je v tem primeru nedvomno povezana z večanjem posega v njegovo zasebnost.

Ugotovitve raziskave ne kažejo enotnih učinkov vedenjskega oglaševanja na ključne igralce v sistemu. Po eni strani ima pomembne prednosti zaradi učinkovitega ciljanja (npr. Seitz in Zorn, 2016), po drugi strani pa ni nujno, da je za vse subjekte boljša izbira kot običajno digitalno oglaševanje, ki ni utemeljeno na profilih posameznikov. Oglaševalci so pri uporabi sistemov avtomatiziranega oglaševanja izpostavljeni večjim možnostim zlorabe podatkov o njihovih strankah, čeprav naj bi posebej nišnim oglaševalcem natančnejša specifikacija občinstva koristila. Slednje se sklada z ugotovitvami Chena in Stallaerta (2014), ki ugotavljata, da so manjši oglaševalci z vedenjskim oglaševanjem načeloma v boljšem položaju, saj pridobijo le tiste uporabnike, na katere ciljajo. Prevladujoči oglaševalci pa z vedenjskim oglaševanjem ne pridobijo, kadar imajo pomembno konkurenčno prednost pred tekmeci, saj bi s tradicionalnim oglaševanjem imeli na voljo večjo skupino uporabnikov in bi še vedno pridobili pomembne prihodke (Chen in Stallaert, 2014).

Iz ugotovitev izhajajo nedvomne prednosti za *ad tech* panogo, ki ponuja storitve vedenjskega oglaševanja in povezanih podatkovnih storitev in katere finančni izkazi so odlični, zlasti kadar oglaševalske storitve ponujajo tisti ponudniki, ki kot osnovno storitev ponujajo drugo vrsto dejavnosti (spletno družbeno omrežje, iskalnik itd.), zaradi katere imajo dostop do velikega števila uporabnikov, ki jim lahko strežejo oglase. Pri izdajateljih je slika prednosti in izzivov zopet mešana. Po eni strani vedenjsko oglaševanje omogoča pridobivanje širšega nabora sredstev, ki ga izdajatelji lahko namenijo ustvarjanju vsebine – torej bogati raznolikost ponudbe –, po drugi strani pa nima vedno prednosti pred klasičnim oglaševanjem, pri katerem posamezen oglaševalec neposredno zakupi prostor. Intervjuji z eksperti kažejo, da programatično oglaševanje prinaša prihodke predvsem v kontekstu vsebine, ki se težko trži sama, v smislu, da predstavlja kontekst oglasu (npr. imeniške spletne strani), ter tudi za majhne izdajatelje, ki nimajo možnosti neposrednih pogajanj z oglaševalci, lahko pa si z uporabo programatičnih sistemov velikih ponudnikov (npr. Google in Facebook) zagotovijo vsaj pokritje svojih stroškov poslovanja. Programatičen zakup naj bi prav tako nižal ceno oglasnemu prostoru, zato ima prednost na spletni strani razmeroma velikega medija neposredno oglaševanje. Chen in Stallaert (2014) pa denimo ugotavljata, da imajo z vedenjskim oglaševanjem boljši položaj veliki založniki, kjer za isti oglasni prostor tekmuje

več oglaševalcev, ki so med seboj primerljivi, in so uporabniki heterogeni. Za majhne izdajatelje, ki nimajo veliko povpraševanja po svojem oglasnem prostoru, pa naj bi bilo tradicionalno oglaševanje boljša izbira. Ugotovitve torej niso enoznačne, kar lahko najverjetneje deloma pripišemo napredku tehnik in ponudbe vedenjskega oglaševanja v letih od objave te raziskave, ki je najverjetneje spremenila tudi ekonomske kazalce, poleg tega pa so tudi spletne strani velikih založnikov heterogene, tako po številu kot tudi tipu oglaševalcev in uporabnikov, kar po vsej verjetnosti vpliva tudi na izplen, ki bi ga lahko imeli od vedenjskega oglaševanja. Naša študija prav tako ni primerljivo merila ekonomske učinkovitosti vedenjskega oglaševanja, ampak ugotovitve izhajajo iz konkretnih izkušenj nekaj ekspertov. V vsakem primeru iz neskladja izhaja vsaj to, da ekonomski učinki za izdajatelje in oglaševalce niso nujno enoznačni, ampak so odvisni od konkretne situacije in strategije, *ad tech* panoga, ki storitve vedenjskega oglaševanja ponuja, pa v skupnem nedvomno napreduje in se razvija. Na strani ponudnikov vsebine se pojavljajo tudi že pozivi, da vzame oglaševanje na podlagi podatkov uporabnikov nazaj v svoje roke in ne financira izdatno *ad tech* panoge, brez otipljivih prednosti tega zase in z veliki tveganji glede odgovornosti za kršitev varstva osebnih podatkov uporabnikov (Ryan, 2018).

Študije občinstva in medijske potrošnje: nemoč posameznika in njegov aktivni upor

Pri iskanju razumevanja vedenjskega oglaševanja skozi optiko teorij medijske potrošnje in študij občinstva naletimo na prenekatere pojme in teorije, ki nam pomagajo razumeti nekatere razsežnosti pojava vedenjskega oglaševanja, predvsem glede njegove vseprisotnosti in vtkanosti v vse pore družbenega življenja ter glede vloge, ki jo imajo uporabniki elektronskih storitev, novih medijev, oziroma ljudje, ki smo jih včasih poznali pod imenom občinstvo (Rosen, 2006). Ugotovitve študije kažejo, da po eni strani občinstvo v svojem vsakdanu pravzaprav nima možnosti ubežati elektronskim komunikacijskim storitvam in s tem vedenjskemu oglaševanju, ter so v tem smislu precej nemočno prepuščeni njegovim posledicam. Te so lahko pozitivne, saj posameznikom in družbi olajšajo marsikatere procese (optimizacija delovanja, prihranek časa in energije pri predelavi informacij, ipd., pa tudi izrazito negativne, v smislu izgube zasebnosti, družbe vseprisotnega nadzora in oteženega izvajanja drugih temeljnih pravic. Po drugi strani pa lahko opazujmo aktivno občinstvo, ki se temu sistemu upira, npr. z uporabo protireklamnih vtičnikov, digitalnim odklopom (angl. *digital detox*) itd.

Študije medijske potrošnje in občinstev nam odkrivajo, da je vedenjsko oglaševanje samo po sebi vseprisotno, kot je vseprisotna narava novih medijev, še toliko bolj zaradi kombiniranja medijev, ki jih dan za dnem uporablja posameznik v svojem medijskem repertoarju (Luthar in Oblak Črnič, 2015) in njihove udomačitve (Silverstone, 1994), ki posameznika pušča ranljivo odprtega interesom različnih panog, ki izrabljajo tržni potencial informacij o njem. Mediatizacije tako ne opazujemo le na ravni vtkanosti medijev in komunikacij v različne pore družbenega življenja, ampak tudi na ravni vedenjskega oglaševanja, saj je posameznik opodatkovljen (Cheney Lippold, 2017) v vseh situacijah svojega družbenega udejstvovanja (zasebnega, institucionalnega, poslovnega itd.) in mediatizacija pomeni tudi vključenost vedenjskega oglaševanja na vse te ravni njegovega družbenega obstoja.

Procesi mediatizacije in vseprisotnosti novih medijev (Lievrouw in Livingstone, 2006a) ter povezan koncept vedno vključene oz. povezane družbe (Turkle, 2008) so zelo aktualni v kontekstu ugotovitev študije. S širitvami dejavnosti vedenjskega oglaševanja na različne zaslone, na naprave interneta stvari ter s povezovanjem podatkov o aktivnosti *online* in *offline* lahko resnično govorimo o vseprisotnem oglaševanju in posamezniku, ki je vedno vključen – vedno na voljo za prikaz relevantnega oglasa glede na njegov trenutni kontekst ter vedno obkrožen s podatkovnimi točkami, ki hranijo njegov profil. V tem smislu oglaševanje postane dejansko vtkano v vsakodnevne aktivnosti posameznika in ne le omejeno na zaslone in čas, ki ga preživi za njimi. Kot poudarja Hepp (2010), mediatizacija zajema tako časovni vidik, kjer je vse več tehnoloških medijev uporabniku dostopnih neprekinjeno in povsod (Hepp, 2010, str. 39–43).

Tehnološki napredek pri možnostih sofisticiranih analiz velikih količin podatkov o posameznikih in zmožnostih ciljanja v oglaševanju prinaša prenekatere izzive za posameznike in družbo. Kot poudarja že McQuail (2005), številni posamezniki nimajo možnosti, znanja ali želje po aktivni udeležbi v okolju novih medijev, tudi vsebine se zapirajo (McQuail, 2005, str. 138–139), čeprav morda ne toliko s strani urednikov kot s strani algoritmov, ki sprejemajo odločitve na podlagi dobičkonosnosti, uporabniki pa se tem postopkom in posegom ne znajo ali ne zmorejo izogniti (Cheney Lippold, 2017). Rezultati študije kažejo, da sta največja ponudnika oglaševalskih storitev prisotna na 80 odstotkov vseh spletnih strani ter z oglasi servisirata do 70 odstotkov vsega trga. To jasno nakazuje, da nekaterim praksam ni mogoče ubežati, tudi če bi posameznik to želel, saj mora v vsakdanjem življenju uporabljati številne

storitve elektronskih komunikacij, ki pa skoraj vse vključujejo obdelavo podatkov za oglaševanje (npr. e-pošta, spletna družbena omrežja in novičarske spletne strani). Velja pa seveda omejitev – učinkovitost osebno prilagojenih vsebin je daleč od stoodstotne, čeprav je morda veliko višja od običajnih vsebin. Potrjujejo se ugotovitve, da sodobne elektronske storitve pomenijo izziv za zasebnost zaradi (1) »brezplačnega« poslovnega modela, ki se financira z analizo podatkov o uporabnikih ter (2) da številni realno nimajo druge možnosti, kot da priljubljene storitve uporabljajo, saj tam poteka njihovo družbeno udejstvovanje (Lueders, 2013, str. 459).

Aktivno občinstvo, ki se upira in izrablja možnosti izbire

Vedenjsko oglaševanje omogoča raznolikost vsebine in storitev, ki je na voljo posameznikom (tudi ranljivejšim skupinam, za katere ob plačljivih modelih uporabe ne bi bilo nujno poskrbljeno), ter boljše, relevantnejše skupine, prihranek virov za iskanje storitev ter produktov ipd. Uporabniki razmeroma svobodno odločijo, ali jih bo informacija iz osebno prilagojenega oglasa posrkala vase ali jo bodo delili in se o njej pogovorili z bližnjimi, o ponujenem poiskali več informacij na drugih mestih in tako sami preverili, kako primerna ali ugodna je, ali pa bodo morda stvar ignorirali. Uporabniki imajo na spletu široko izbiro storitev, ki jih lahko uporabijo, in med njimi lahko izbirajo ponudnike glede na različne potrebe, preference, ali želje, tudi po merilu varovanja zasebnosti in izpostavljenosti oglaševanju na podlagi profiliranja. Težava se pokaže pri tistih storitvah, ki so tako globalno uporabljene, da pravzaprav nimajo več tekmecev, npr. najbolj priljubljeno družabno omrežje Facebook. Uporabnik se tukaj mora strinjati s pogoji uporabe, ki vključujejo vedenjsko oglaševanje, saj je v nasprotnem primeru izključen iz (za mnoge) pomembnega dela komunikacijske in družbene dnevne aktivnosti. Težavna je tudi vseprisotnost spletnih storitev, ki smo jih vse bolj primorani uporabljati v vsakdanjem komuniciranju in opravljanju dnevnih obveznosti (npr. e-pošta in spletne trgovine) (Livingstone, 2006). Njihovi uporabi se zelo težko izognemo in tako nimamo izbire, kadar ponudnik take storitve izvaja vedenjsko oglaševanje in ne ponuja možnosti izbire. V primeru tako široko uporabljanih zelo hierarhičnih storitev, kot so storitve Googla in Facebooka, zagotovo lahko iščemo tudi vzporednice s starimi mediji in njihovimi odnosi z občinstvom.

Glede na koncept družbenega oblikovanja informacijsko-komunikacijskih tehnologij bi lahko trdili, da posamezniki deloma sooblikujejo področje oglaševanja in izrabijo svoje možnosti

nadzora, vendar pa je prav tako treba poudariti, da v resničnosti te možnosti bodisi nimajo bodisi je ne uveljavijo, kot poudarjajo različni avtorji (Daryl Slack in MacGregor Wise, 2006; Lievrow in Livingstone, 2006b, str. 21). Iz študije izhaja porast uporabe protireklamnih vtičnikov, ki kaže, da posamezniki deloma jemljejo v svoje roke nadzor nad deljenjem svojih podatkov za namen vedenjskega oglaševanja in s tem sooblikujejo načine, na katere lahko oglaševanje poteka, nekateri izrbijo tudi svoje možnosti pri obvestilih o piškotkih in uporabijo samoregulacijske možnosti, da se odrečejo ciljnim oglasom. Rezultati študije kažejo tudi konkretne pobude na področju iskanja nadzora nad podatki in algoritemsko regulacijo, tako da se namenoma v podatke dodaja šum (Cheney Lippold, 2017; Brunton in Nissenbaum, 2016). Pa vendar celotna slika kaže, da je te akcije razmeroma malo, da obstajajo velike ovire v poznavanju tehnološko kompleksnega okolja, v razumevanju posledic, ki jih ima neprekinjeno sledenje in analiziranje podatkov uporabnikov za njihove pravice, ter v dejanskih možnostih odločanja, ki jih zelo omejeno ponujajo ponudniki elektronskih storitev. Temu lahko prištejemo še vtkanost sodobnih komunikacijskih orodij v vsakdan običajnega posameznika in dejstvo, da je na nekatere storitve priklenjen, saj bi mu menjava povzročila nesorazmerne stroške (finančne in nefinančne), če na trgu primeren primerljiv produkti sploh je (kar je v prevladi Googla in Facebooka vprašljivo).

Digitalna pismenost in ločnica, informacijska asimetrija ter predsodki, ki vodijo posameznike v njihovih odločitvah

Tukaj so zelo aktualna vprašanja digitalne pismenosti, ki zajema vprašanje dostopa do medijev, enakosti in znanja, kulture in participacije, na katerih temeljijo zmožnosti ocenjevanja in presojanja vsebine (Livingstone, 2004) oziroma »zasebnostne ločnice« (angl. *privacy divide*), med tistimi, ki vprašanja zasebnosti razumejo, in tistimi, ki jih ne (Woo, 2006, str. 958). Brunton in Nissenbaum (2016) vprašanje neenakosti (asimetrije), razumeta v smislu razlike med tistimi, ki so, in tistimi, ki niso informirani (angl. *information haves and have-nots*), pri čemer razlikujeta med neenakostjo v moči, ki običajno izhaja iz dejstva, da posamezniki običajno nimajo moči odločanja o tem, kaj se bo dogajalo z njihovimi osebnimi podatki ali kako bo njihova uporaba vplivala nanje, ter neenakostjo v znanju, ki je posledica dejstva, da večina ljudi ignorira ali v najboljšem primeru le slabo zaznava zbiranje, agregiranje, analizo in deljenje svojih podatkov. Glede tega poudarjata perečo problematiko velikega podatkovja, kjer posameznikom niso znani nameni nadaljnje obdelave takih podatkov, niti načini njihove analize ali predvidevanj (Brunton and Nissenbaum, 2016).

Rezultati študije te ugotovitve potrjujejo in njihovo pomembnost še dodatno podkrepijo – selitev vedenjskega oglaševanja na področje sledenja prek različnih naprav in v internetu stvari, uporaba profiliranja in strojnega učenja, ki vodi v diskriminacijo, ter uporaba teh tehnik na področju političnega komuniciranja razgaljajo visoko stopnjo informacijske asimetrije, saj je zmožnost posameznikov razumeti tako kompleksne obdelave podatkov čedalje manjša, vse večja pa je prikritost teh procesov in zmožnosti manipulacije posameznikov, tudi na političnem področju. Z vstopom vedenjskega oglaševanja tudi na področje interneta stvari in političnega komuniciranja so še jasneje vidne možnosti nenehnega nadzora nad posameznikom, ki omogoča diskriminacijo in posege v njegove temeljne politične pravice, manipulacijo in zapiranje vsebine, ki je posameznikom na voljo. Posameznik postaja čedalje bolj ujet v svoje pretekle interese in izgublja možnost spontanega odkrivanja novih znanj in novih nepričakovanih informacij (Pariser, 2011; Woo, 2006, str. 957).

Ugotovitve študije po drugi strani kažejo tudi drugo plat – pasivnost posameznikov pri ravnanju v korist svojim pravicam, tudi kadar jim je ta možnost ponujena. Zakonodajni okvir za varovanje osebnih podatkov v EU temelji na tem, da ima posameznik možnost odločitve v svojih rokah, saj naj bi bil v teoriji zmožen podaje privolitve, čeprav posamezniki najpogosteje le klikamo na najlažje možnosti »se strinjam«, da bi čim prej prišli do storitve, ki jo želimo. Tako ravnanje pomaga pojasniti vedenjska ekonomija (Acquisti in drugi, 2013), ki pojasnjuje, da na posameznika pri odločanju vplivajo številni predsodki, kot je npr. predsodek *statusa quo* (angl. *status quo bias*), ki se nanaša na to, da smo ljudje nagnjeni k obdržanju privzetih možnosti in ne izvajamo sprememb, predsodek kratkovidnosti (angl. *myopia bias*) pa se nanaša na to, da ljudje stremimo k čimprejšnji nagradi in nismo pozorni na prihodnje stroške in posledice neke naše odločitve (Zuiderveen Borgesius, 2014, str. 298). Poleg tega je veliko odvisno od načina, kako so predstavljene informacije – ohlapnejši jezik, izbira prijaznejših izrazov, izpostavljene informacije o zasebnosti, čeprav pomanjkljive, vključevanje ikon, ki naj bi pomenile varovanje podatkov, čeprav dejansko to ni nujno, itd. so možnosti, ki uporabnika zlahka zavedejo v prepričanje, da je poskrbel za svojo zasebnost (Zuiderveen Borgesius, 2014, str. 292).

Vedenjsko oglaševanje in zasebnost: njena instrumentalna vrednost in pomen konteksta

Kot poudarja Solove (2006), pravico do zasebnosti običajno dojemamo kot prvi pogoj svobode posameznika do lastne misli, izražanja, združevanja, ustvarjanja in politične volje (Solove, 2006, str. 3). Avtor hkrati zagovarja njeno instrumentalno vrednost in ne kot vrednost oz. vrednoto samo po sebi, saj predvsem omogoča druge cilje oz. namene. Zato je bistveno ovrednotiti zasebnost v konkretni situaciji, saj ima pri različnih dejavnostih različen pomen (Solove, 2002, str. 1143–1155). Študija potrjuje to tezo – nemogoče je pavšalno odgovoriti na vprašanje vedenjskega oglaševanja in škode za zasebnost posameznika. V konkretnih situacijah uporabe vedenjskega oglaševanja s strani različnih ponudnikov elektronskih storitev smo zato analizirali posledice, ki jih ima za pravice posameznikov in družbene procese, ter ugotovili, da je pravica posameznika do zasebnosti in informacijske zasebnosti, v katero posega, tista podstat, ki je instrumentalna za izvrševanje drugih pravic – do obveščenosti, enake obravnave, svobodnih in pravičnih volitev.

Obdelava velike količine podatkov posameznikov za namen vedenjskega oglaševanja in predvsem sklepanja, ki jih omogočajo napredne zmožnosti umetne inteligence in strojnega učenja so posebej problematični na področju diskriminacije posameznikov glede na njihove socialne razmere, politično prepričanje, zdravstveno stanje in spolno usmerjenost, ki jim lahko prepreči dostop do informacij in storitev, jih s tem zapira v mehurček in tako veča družbeno razslojenost in segregacijo ter poustvarja in multiplicira stereotipe.

Drugi zelo kritičen kontekst je uporaba vedenjskega oglaševanja v okviru političnega komuniciranja, čeprav avtorji navajajo prednosti v smislu večjih možnosti, da politična sporočila dosežejo skupine volivcev, ki jih je težko doseči (npr. mladi), na platformah, ki so jim bliže (npr. spletni družbeni mediji), in glede tematik, ki so jim bolj v interesu in jih bodo mobilizirale, s tem pa lahko pozitivno vpliva na večjo obveščenost volivcev o tematikah, ki so relevantne, in zmanjša odtujenost od političnega procesa ter volilno abstinenco (Zuiderveen Borgesius in drugi, 2018, str. 85–86). Ker politična sporočila temeljijo na osebnih podatkih, na natančno opredeljenem profilu posameznika, mu je tako dostopnih manj različnih mnenj, kar se kaže v ideološki polarizaciji in prepričljivosti lažnih zgodb pa tudi v potencialih manipulacije – politika lahko volivcem prikazuje sporočila, ki jih angažirajo zaradi čustvene povezanosti z aktualnimi temami, kot so npr. ksenofobija, migracije, spolna usmerjenost in pravica do splava. Na udaru je medijska pluralnost in pravica do obveščenosti, saj ponudniki

spletnih storitev čedalje bolj prevzemajo vlogo glavnih informatorjev v družbi, hkrati pa jih ne vežejo novinarski standardi enakovredne zastopanosti stališč (Martens in drugi, 2018, str. 16). Prav tako pa so s tem ogroženi temeljni demokratični procesi svobodnih, poštenih in preglednih volitev (Goodman in drugi, 2017; COE, 2017), saj so posamezniki na podlagi posega v svojo zasebnost in analize njihovih podatkov lahko predmet manipulacije za doseganje vpliva na izid volitev.

Ugotovitve študije nakazujejo na situacije, v katerih vedenjsko oglaševanje negativno posega v zasebnost posameznikov, saj jim onemogoča izvrševanje drugih interesov in pravic. Pokazale pa so tudi, da obstajajo konteksti, v katerih ta poseg ni kritičen in lahko posameznikom (glede na njihov profil) relevantnejše informacije in vsebine koristijo, zmanjšajo njihov trud in porabo virov za pridobivanje informacij, povečajo krog storitev, ki so jim na voljo brezplačno, in omogočijo ustvarjalno izražanje ter inovativnost in komunikacije, s katerimi lahko gradijo in utrjujejo svoje družbene odnose. Predvsem so to konteksti, v katerih ni poudarka na obdelavi občutljivih podatkov o posameznikih, v situacijah, ki jih sami dojemajo kot občutljive, in bi lahko vodile v neželeno diskriminacijo ali politično manipulacijo. Glede tega se lahko naslonimo tudi na ugotovitve Nissenbaumove (2010), ki je opredelila koncept moralno primernega toka osebnih podatkov, pri katerem so norme, ki omejujejo tok, kontekstualno opredeljene, in je omenila zdravnika, ki posameznikove osebne podatke lahko zakonito posreduje drugemu specialistu, hkrati pa bi posredovanje tržnikom ali delodajalcu brez pacientovega soglasja pomenilo kršitev norm (Nissenbaum, 2010, str. 24). V primeru vedenjskega oglaševanja vidimo, da je v nekaterih kontekstih lahko zaželeno in koristno, hkrati pa obdelava enakih podatkov posameznika v kontekstu političnega prepričevanja pomeni popolnoma drugačen poseg v posameznikove interese.

Upoštevanje specifičnega konteksta bi moral biti eden od temeljev pravice do informacijske zasebnosti (Nissenbaum, 2015) oziroma, kot je bilo že poudarjeno: vedenjsko oglaševanje kot orodje za politično trženje odpira popolnoma drugačne razsežnosti spornosti takih praks v smislu vpliva na demokratične procese. Prav tako uporaba zdravstvenih podatkov za namen trženja prehranskih dopolnil, ki so lahko nekakovostna in škodijo posameznikovi (pravilno ali ne) pripisani domnevni diagnozi. Razumevanje pravila spoštovanja konteksta mora biti torej precej ozko usmerjeno na določene družbene situacije, da lahko z njim razločimo med

škodljivimi in manj škodljivimi praksami za zasebnost in druge človekove pravice. V smislu posledic za prihodnjo regulacijo nam to kaže tudi na pomembnost premika k večji odgovornosti subjektov, ki izvajajo vedenjsko oglaševanje – ti bi morali biti v konkretni situaciji sposobni opredeliti, kakšna so morebiti pričakovanja glede zasebnosti in drugih pravic, v katere lahko s svojimi praksami posežejo, kot to opredeljuje Martin (2015) v svoji konceptualizaciji družbene pogodbe.

Komodifikacija posameznikov in politična ekonomija vedenjskega oglaševanja, ki oblikuje ozadje regulacije

Politična ekonomija poudarja, da mediji delujejo na dvojnem trgu, svoje produkte ponujajo občinstvu, hkrati pa producirajo občinstva in jih ponujajo oglaševalcem (Smythe, v: Mosco, 1996, str. 148–149). Občinstvo postane poblagovljeno. V okviru programatičnega oglaševanja in panoge preprodajalcev podatkov se ti koncepti nedvomno potrjujejo – na ravni dražb uporabniških profilov je vsak posameznik prodan najboljšemu ponudniku za najboljšo ceno in, kot kažejo ekonomski podatki, ta trg nezadržno raste – trgovanje z občinstvom, podatkovna panoga je ena najbolj dobičkonosnih v zgodovini. Kot trdi Craine (2016), se s podatki posameznika trguje in preprodaja, hkrati pa so produkt in gorivo celotne nove panoge. Naše ugotovitve potrjujejo ugotovitve drugih avtorjev glede procesa kvantifikacije in predstave našega življenja v obliki podatkov – ne le tistih, ki jih posamezniki delimo o sebi, ampak tudi metapodatkov, ki jih zajema ponudnih elektronskih storitev, oz. »opodatkovljenja« (Van Dijck in Poell, 2013, str. 3–6), ki po eni strani deluje posameznikom v korist, po drugi strani pa vodilni igralci na trgu vedenjskega oglaševanja svoje uporabnike predvsem vodijo in jih izrabljajo, ti pa tega v večini niti ne opazijo. Naše ugotovitve glede tveganj, ki jih vedenjsko oglaševanje prinaša demokratičnim družbenim procesom, kadar se izvaja v polju političnega prepričevanja ali na podlagi podatkov, ki ljudi opredeljujejo v ranljivih situacijah, lahko opremo na razpravo o algoritemski kulturi in podatkovnem jazu, kot ga opredeljuje Cheney-Lippold (2017). Ta pokaže, kako algoritmi ustvarjajo naš današnji jaz in vplivajo na naše vedenje, in nam pomaga razumeti, kako ciljanje političnih sporočil prek spletnih družbenih omrežij, kadar vključimo sofisticirane načine analize bogatih podatkov o posamezniku, ki jih nadzoruje ponudnik spletnega družbenega omrežja, lahko pomeni zelo konkretne posledice v smislu porazdelitve moči v družbi.

Na pristope k regulaciji vedenjskega oglaševanja poleg dilem v zvezi z varovanjem pravic posameznikov močno vplivajo značilnosti trgov elektronskih komunikacij in odnosi med

različnimi deležniki. Trgi elektronskih komunikacij so namreč zaznamovani s koncentracijo moči v rokah peščice multinacionalnih korporacij (Van Couvering, 2003; Noam, 2009; Pariser, 2011). Pomembna razsežnost je tudi konkurenčnost trgov v razmerju med ZDA in EU ter deloma sodelovanje med tema silama (Goldsmith in Wu, 2006). Kot jasno kažejo ugotovitve študije, je posebej v ZDA vidna moč korporacij, ki cvetijo v podatkovni industriji – vedno so blizu oblastem in se tako branijo pred strožjimi posegi v osnovno dejavnost, ki poganja njihov razvoj – obdelavo podatkov posameznikov (Confessore, 2018). To je vidno tudi v EU, saj so ob zadnjih spremembah zakonodaje (Uredba 2016/679in ePR) pritiski panožnih lobistov po nekaterih komentarjih presegli tiste na okoljskem področju (Singer, 2018; Burnik, 2016a). Vprašanje konkurenčnosti visokotehnoloških podjetij v EU v razmerju do ZDA, ki ima bolj sproščena pravila glede varovanja pravic posameznikov, je tema, ki se ob spremembah zakonodaje stalno pojavlja (IAB, 2017). Kot kaže literatura, ima velika moč v rokah le nekaj igralcev, ki ključno zaznamujejo današnje področje vedenjskega oglaševanja (najbolj Facebook in Google), tudi veliko negativnih posledic v smislu zapiranja vsebin, ki so posameznikom dostopne, oziroma še bolj kritično – v potencialih manipulacije, ki sega tudi na področje političnega diskurza in demokratičnih procesov.

Pomembna je tudi refleksija konceptualizacije osebnih podatkov v smislu njihove ekonomske vrednosti, ki se čedalje pogosteje pojavlja na različnih ravneh razprave o regulaciji vedenjskega oglaševanja: v pristopih regulacije glede na lastništvo podatkov, v ekonomskih in drugih ugodnostih, ki naj bi jih v zameno za osebne podatke ponudili ponudniki storitev, v rešitvah (celo na ravni razvoja ePR), da svojo storitev ponudijo bodisi brezplačno, na podlagi obdelave osebnih podatkov, bodisi odplačno. Taka konceptualizacija implicira redukcijo pomena osebnih podatkov in zasebnosti na njeno ekonomsko vrednost, kar je z vidika teoretskih pristopov pravzaprav preživet pogled, povezan z lastniško pravico nad svojimi podatki (Westin, 1967, str. 324), ki ne zajema celostnega pomena pravice do zasebnosti kot temeljne človekove pravice, ki omogoča udejanjanje drugih interesov posameznika v posameznih kontekstih (Solove, 2006). Tak vidik utrjuje procese komodifikacije osebnih podatkov in občinstev (Crane, 2016), saj so podatki, lahko tudi zelo intimne podrobnosti o posameznikovem življenju, ki dopuščajo diskriminacijo in družbeno segregacijo ter vzdrževanje neenakosti, opredeljeni le z vidika materialne koristi. Potrjujejo se kritični pogledi na zasebnostno ločnico, kjer bodo pravico do zasebnosti bolj uživali bogatejši in tisti, ki imajo več znanja o upravljanju s svojimi podatki, socialno šibkejši in tisti z manj znanja ter

priložnostmi pa bodo podvrženi obširnim obdelavam njihovih osebnih podatkov, ki lahko vodijo v še večje razslojevanje in diskriminacijo. Opredelitev ekonomske vrednosti osebnega podatka je lahko tudi sredstvo za dvigovanje preglednosti, v smislu zavedanja posameznikov, da obdelava podatkov prinaša ekonomsko korist ponudnikom storitev, in kakšna ta korist je. V tem smislu pa jo lahko razumemo kot sredstvo za odkrivanje procesov komodifikacije, ki lahko koristi tudi regulaciji (kot kaže primer izračuna števila uporabnikov, ki je lahko kazalec za davčne obveznosti).

Zakaj in kako regulirati vedenjsko oglaševanje

Ugotovitve študije kažejo, da vedenjsko oglaševanje nima le negativnih posledic za zasebnost posameznikov in varstvo njihovih osebnih podatkov, ampak so lahko prizadeti tudi drugi interesi. Je bistvo monetizacije »brezplačnih« storitev, programske opreme, lahko tudi izdelkov, kar zagotovo prinaša prednosti v smislu napredka družbe, inovacij in zastopanosti socialno ranljivejših skupin v informacijsko-komunikacijski sferi, toda hkrati tudi negativne posledice v smislu vseprisotnega nadzora in diskriminacije ter celo negativnega vpliva na politične in demokratične procese. Glede tega je zlasti pomembno vprašanje medijev in njihove odvisnosti od vedenjskega oglaševanja ter alternativnih možnosti financiranja za izvajanje vloge četrte veje oblasti. S tem je povezano vprašanje kakovosti vsebin in tudi vloge javnih RTV servisov, ki ostanejo eden redkih branikov »neodvisne« produkcije vsebin. Glavni izvajalci vedenjskega oglaševanja imajo skoraj monopolne položaje, kar zbuja nadaljnja vprašanja koristi in izzivov za širšo družbo.

Iz tega lahko izluščimo številne razloge za regulacijo vedenjskega oglaševanja, kot jih opredeljujeta Baldwin in Cave (1999): Google in Facebook sta vsak na svojem ozkem segmentu trga zagotovo vsaj blizu monopolistom. Za njune produkte namreč ni primerljive zamenjave, poleg tega pa so uporabniki »zaklenjeni« na njihove storitve, tudi zaradi ekonomije obsega, ki njune storitve dela še učinkovitejše. Čeprav so njune storitve brezplačne in težko govorimo o višanju cene, ki bi ga monopolni položaj povzročal, se viša cena v smislu količine podatkov, ki jih uporabnik mora predati za uporabo njunih storitev in dovoljenj za njihovo analizo in nadaljnjo uporabo. Negativni zunanji učinki vključujejo poseg v temeljne pravice posameznikov, uporabnikov storitev, do zasebnosti in nediskriminacije ter v demokratične procese. Prav tako je za trg vedenjskega oglaševanja značilna visoka stopnja informacijske asimetrije – nezadovoljivega informiranja uporabnikov spleta. Po eni strani

zato, ker uporabniki pogosto nimajo znanja ali orodij za preverjanje, kaj se dogaja z njihovimi podatki in kaj to pomeni za njih, po drugi strani pa bi večje informiranje posameznikov o potencialnih škodnih vplivih posredovanja njihovih podatkov lahko poseglo v osnovni poslovni model izvajalcev vedenjskega oglaševanja. Več posameznikov, ki bi se sledenju odreklo, bi pomenilo manjše prihodke oz. slabše zmožnosti analize podatkov. Internet je postal dobrina, ki je dejansko pomembna za javno dobro, še zlasti z vidika informatizacije storitev javne uprave, bančništva itd., kjer nezmožnost svobodne uporabe spleta lahko onemogoči posameznikovo zmožnost vsakodnevnega delovanja. Ker so posamezniki tudi za opravljanje dnevnih opravkov prisiljeni uporabljati internet, je dejstvo, da so pri tem tudi izpostavljeni komercialnemu sledenju in v zadnjem obdobju tudi sledenju za namene politične komunikacije, tudi razlog za regulacijo v smislu dostopnosti storitve in javnega dobrega. Prav tako lahko v odnosu velikih ponudnikov, kot sta Google in Facebook, in uporabnikov vidimo odnos neenakih moči, kjer so uporabniki pogosto prisiljeni v strinjanje s splošnimi pogoji, hkrati pa ne morejo uporabljati primerljive druge storitve. Dolgoročni učinki obširnega beleženja aktivnosti uporabnikov ter prilagajanja oglasov in vsebin njihovim predvidenim interesom pa sproža velika vprašanja o koristi tega za prihodnost uporabnikov, v smislu družbe nadzora, diskriminacije in ujetosti v »mehurčke« preteklih interesov, pravice do informiranosti in svobodnih volilnih procesov, kar je zagotovo lahko razlog za regulacijo v smislu motiva načrtovanja za ohranjanje dobrobiti naslednjih generacij.

Ugotovitve študije kažejo možnosti regulacije vedenjskega oglaševanja na različnih ravneh, predvsem v okviru zakonodaje in pravil, ki jih panoga vzpostavi sama (samoregulacija) (po Baldwin in Cave, 1999, str. 34–62) ter na ravni regulacije s kodo (po Lessig 2006, str. 122–125) oz. tehnične standardizacije. V okviru vedenjskega oglaševanja je najpomembnejši regulatorni mehanizem razvoj in uvedba standarda ne sledi. Naše ugotovitve v kontekstu pojma regulacija s kodo kažejo, da je koda kot način regulacije čedalje primernejša na področju vedenjskega oglaševanja. Koda tu označuje tehnične rešitve, tehnično arhitekturo storitev elektronskih komunikacijskih sredstev, ki omejuje, kaj lahko akterji z njo počno. V teoriji naj bi bila taka regulacija učinkovitejša kot preplet pravil in organov, ki pravila nadzorujejo, saj razen tehnološke ovire ni potreben neki zunanji okvir nadzora nad spoštovanjem pravila. Želje in potrebe po regulaciji s pomočjo tehničnih standardov se kažejo tako na ravni razvoja zakonodaje in pravil (predvsem v EU), kjer Uredba 2016/679 spodbuja nastanek zasebnosti prijaznih rešitev in konfiguracij tehničnih sistemov (t. i. vgrajena in

privzeta zasebnost), ter še posebej na ozkem področju regulacije vedenjskega oglaševanja s standardom ne sledi. Ta naj bi v eni potezi rešil mučna vprašanja različnih zahtev pravil v EU in ZDA glede sledenja na spletu (ali je potrebna vnaprejšnja privolitev ali ne) in vprašanja nadzora. Razvoj standarda pa kaže, kako zelo pomembna so tudi v okviru regulacije s kodo povsem običajna vprašanja regulacije, in sicer ali bodo pravila v zakonodaji določala, da mora panoga standard spoštovati; kakšne izjeme sledenja dopušča standard; tehnična rešitev, ki jo oblikuje industrija sama; kdo jo pri tem omejuje in kdo bo izvajal nadzor nad nespoštovanjem standarda. Naše ugotovitve kažejo, da sama po sebi regulacija s kodo v obliki standarda ne sledi nikakor ne kaže potenciala za velik preskok in da je za boljšo regulacijo področja vedenjskega oglaševanja potrebna kombinacija regulacije s pravili v zakonodaji, samoregulacije in regulacije s kodo. Poleg tega pa je nujno krepiti nadzor nad pravili in opolnomočiti posameznike.

Kritična refleksija trenutnega okvira regulacije vedenjskega oglaševanja

Ugotovitve študije kažejo, da je stanje regulacije vedenjskega oglaševanja danes raznoliko. Analiza trenutnega regulatornega okvira v EU in ZDA je pokazala, da je ta pester, neenoten v zahtevah in zato precej neučinkovit v premagovanju negativnih vidikov vedenjskega oglaševanja za pravice posameznikov. Pomembni so tudi elementi samoregulacije, predvsem v ZDA, kjer je na panožnem kodeksu utemeljena večina podrobnejših pravil za vedenjsko oglaševanje, manj pa v EU, kjer podoben kodeks ne dosega minimalnih zahtev zakonodaje. Odpirajo se možnosti na področju certificiranja in standardizacije: standard ne sledi je skoraj dokončan, viri pa se vlagajo tudi v standardizacijo področja vgrajene zasebnosti. Raznolike pristope k regulaciji, ki so tudi različno učinkoviti in bolj ali manj primerni za kontekst hitro spreminjajočih razmer pri sodobnih elektronskih komunikacijskih storitvah, lahko zasledimo tudi v teoretičnih temeljih (Baldwin in Cave, 1999; Lessig, 2006; Braman, 2013). Za namen celostne analize slike regulacije se bomo v nadaljevanju oprli na tipizacijo strategij regulacije, kot jo ponujata Baldwin in Cave (1999, str. 34–62) in vključuje: pravila in nadzor, samoregulacijo, spodbude, ukrepe za vzpostavljanje trga (konkurenčno pravo, franšize in licence, reguliranje s pogodbami, dovoljenja, s katerimi je mogoče trgovati), dolžnost razkritja, neposredno vpletanje, zakonodajo o pravicah in obligacijah, javna nadomestila in socialno zavarovanje. Ugotovitve kažejo, da na področju vedenjskega oglaševanja trenutno prevladuje strategija pravil in nadzora (predvsem v EU) ter samoregulacije, pa tudi dolžnosti razkritja (predvsem v ZDA) ter zakonodaja o pravicah in dolžnostih.

Bistvo strategije pravil in nadzora so jasna pravila in sankcije za kršitve pravil, ki jih določa zakonodaja in uveljavljajo regulatorji, ki naj bi imeli določeno moč. Med slabosti je postavljanje kompleksnih pravil in težnja k prenormiranju tega področja. Postavljanje dobrih standardov je težavno in drago, ta strategija je toga in draga za izvajanje (Baldwin in Cave, 1999, str. 39–41). Evropska zakonodaja na področju vedenjskega oglaševanja glede na ugotovitve analize pravnega okvirja izkazuje kar nekaj pomanjkljivosti. Pravila, ki jih določa, so kompleksna, nejasna in dopuščajo različne razlage. Ker je bila zakonodaja s področja varovanja zasebnosti in osebnih podatkov pred kratkim posodobljena (Uredba 2016/679), oziroma še bo posodobljena (ePR), je veliko nejasnosti glede pomena, sicer na papirju razmeroma strogih določb glede njihove uporabe v konkretnih situacijah. Za področje vedenjskega oglaševanja so značilne tudi različne razlage nadzornih organov, kako tehnično zadovoljiti zahtevo po pridobivanju privolitve, kakšne obdelave podatkov lahko temeljijo na zakonitem interesu posameznika in kakšne so potrebne za izvajanje pogodbe. Kot kaže razvoj zakonodaje, se pravila, ki urejajo vedenjsko oglaševanje, postavljajo in spreminjajo že desetletje, kar kaže na to, da je postavljanje dobrih standardov na ravni zakonodaje težavno, postopki so togi in dolgotrajni, zakonodaja ki ureja tehnologijo, pa zato v nevarnosti, da hitro zastara. Nadzorni organi v EU so v državah članicah različno močni in imajo tudi različna pooblastila.

Veljavni samoregulacijski kodeks na področju vedenjskega oglaševanja ni učinkovit pri omejevanju negativnih učinkov na posameznike, saj temelji na podmeni, da morajo posamezniki naknadno zavrniti vedenjsko oglaševanje, če ga ne želijo. Ker posamezniki to področje slabo poznajo in razumejo, te možnosti ne izrabijo. V EU tak pristop ne zagotavlja minimalnega standarda za skladnost s pravili, ki je vnaprejšnja privolitev posameznika. Te ugotovitve kažejo negativne strani samoregulacije, ki jih poudarjata Baldwin in Cave (1999), in sicer predvsem ujetost v panožne interese, saj bi njim škodovalo večje število posameznikov, ki bi nasprotovalo vedenjskemu oglaševanju, zato pravila določajo nižji standard, naknadno zavrnitev – saj jo posamezniki zaradi neznanja redko uveljavijo. Kot kažejo ugotovitve vedenjske ekonomije (Zuiderveen Borgesius, 2014), pa smo posamezniki nagnjeni tudi k temu, da ne spreminjamo začetnih nastavitev in da stremimo k takojšnji zadovoljitvi želja, ne glede na prihodnje posledice (Zuiderveen Borgesius, 2014, str. 298). Vidimo tudi, da je samoregulacijski okvir v ZDA in tudi v EU nastal zato, da bi preprečil

strožjo regulacijo z zakonodajo – v ZDA tak pristop še vedno deluje, v EU pa je obstoj pravil za varstvo osebnih podatkov in varovanje zasebnosti v elektronskih komunikacijah že pred samoregulacijskim kodeksom določil minimalni standard predhodne privolitve posameznikov, česar kodeks ne dosega in zato nima posebne veljave.

Za področje vedenjskega oglaševanja v ZDA je značilna strategija dolžnosti razkritja informacij – oblika regulacije, ki ne posega v produkcijski proces, v produkt, ceno in porazdelitev produkta sam po sebi, ampak prepoveduje le posredovanje nepopolnih ali zavajajočih informacij o produktu, oziroma zapoveduje posredovanje določenih informacij. Razkritje informacij naj bi potrošniku (pa tudi državljanu oz. volivcu) omogočilo, da sam sprejme odločitev glede produkta in sprejemljivosti njegove proizvodnje (Baldwin in Cave, 1999, str. 49–50). Izvajalci vedenjskega oglaševanja so dožni razkriti svoje prakse in so za navedbe odgovorni pred regulatorjem FTC, niso pa omejeni v svojih praksah ravnanja z osebnimi podatki. Študija kaže, da ta strategija ni učinkovita v obrambi pred negativnimi posledicami vedenjskega oglaševanja za posameznika, po ugotovitvah Baldwina in Cavea (1999), da ta strategija ni učinkovita, kadar je nevarnost posameznikom velika in kjer niso sposobni razumeti in uporabiti informacije ter kjer ni mogoče nadzorovati točnosti podanih informacij, ne da bi pri tem nastali nerazumni stroški (Baldwin in Cave, 1999, str. 49–50).

Boljša regulacija vedenjskega oglaševanja v prihodnosti: koregulacija, nadzor in izobraževanje ter preskok na področje etike in družbene odgovornosti

Za boljšo regulacijo področja vedenjskega oglaševanja je potreben splet strategij in orodij ter delovanje na področju vseh deležnikov, ne le izboljšave zakonodaje na tem področju. Prva bistvena ugotovitev v tem kontekstu je, da bi ustrezen splet strategij pomenila koregulacija, preplet zakonodaje, ki bi dala ustrezno podlago za varovanje temeljnih pravic in interesov posameznikov, ter samoregulacije, ki bi jo dopolnila s podrobnejšimi pravili. Vloga zakonodaje v tem spletu je ključna, saj izkušnje dosedanje regulacije in pregled literature kaže, da je na področju varovanja temeljnih pravic in interesov posameznikov ter demokratične družbe potreba po določitvi vsaj osnovnih pravil na ravni zakonodaje, ki lahko v demokratični družbi bolj zagotavlja ustrezno tehtanje med interesi in se bolj, čeprav ne popolnoma, izogiba ujetosti v panožne interese. Kako stroga bi morala biti pravila? Dovolj, da učinkovito ubranijo interese, ki so lahko prizadeti, vendar po nepotrebnem ne obremenijo panoge, ustvarjalnosti, inovacije in napredka. Predvsem pa ne tako stroga, da jih subjekti že v

naprej ne bi upoštevali. Ali relevantna zakonodaja v EU tem merilom sledi, je, glede na ugotovitve študije, vprašljivo.

Vprašanje podrobnejših pravil glede vedenjskega oglaševanja, tehničnih izvedb zakonsko skladnih rešitev, posebnih omejitev in pravil za specifična področja, obveščanja ipd. je lahko prepuščeno samoregulacijskim strategijam – ki so prožnejše, strokovnejše in postavljajo učinkovitejše standarde, če seveda izpolnjujejo določene pogoje, npr. glede članstva v organih samoregulacije, preglednih postopkov sprejema pravil ipd. Področje varovanja zasebnosti in osebnih podatkov ter drugih pravic in interesov je v sodobnem tehnološko razvitem svetu težavno, saj nove tehnologije pomenijo nove izzive za pravice, ki jim zakonodaja sama težko sledi. Ob sprejemu je slednja lahko namreč že zastarela oziroma hitro postane neustrezna in zavrti se nov cikel sprememb, ki vodijo v pravno negotovost na trgu. Zato je na tem področju velik, še precej neizrabljen potencial samoregulacije (s kodeksi, certificiranjem in tehničnimi standardi), regulacije s kodo, ki bi lahko pomenljivo dopolnila osnovna pravila v zakonodaji, ob predpostavki, da ne bi bilo neskladja z določbami zakonodaje in bi bil določen učinkovit nadzor (ti elementi v trenutnem okviru niso zadovoljeni). Uredba 2016/679 že ponuja nastavke na tem področju, saj vključuje določbe o potrjevanju kodeksov, certifikacijskih mehanizmov in omenja tehnične standarde za izpolnjevanje določb. Bistveno bi bilo tudi, da bi bili samoregulacijski mehanizmi vsaj osnovno usklajeni in ne bi prihajalo do pravne negotovosti. Vlogo pri tem imajo zagotovo nadzorni organi in zakonodajalec, predvsem relevantni direktorati Evropske komisije.

Druga bistvena ugotovitev je, da niti najboljši splet pravil v okviru koregulacije ne more biti učinkovit brez ustreznega nadzora. Pravila tako ostanejo le črka na papirju, kar lahko opazujemo na ravni doslejšnjega razvoja zakonodaje EU o vedenjskem oglaševanju. Sicer podrobna stroga pravila namreč niso upoštevana, saj je nadzor tako pomanjkljiv, da subjekti na trgu ravnajo skoraj brez omejitev. Pomanjkljiv je zaradi različnih dejavnikov: zaradi nejasnih pravil, ki dopuščajo različne razlage, zaradi neenakih moči in pristojnosti nadzornih organov, zaradi pomanjkljivih pooblastil in težav pri čezmejnem uveljavljanju pravil, tudi zaradi podhranjenosti nadzornih organov z viri in s specifičnim znanjem (tehnološkim, ekonomskim, marketinškim), ki je potrebno za kompetentni nadzor na področju sodobnega vedenjskega oglaševanja. V kontekstu nadzora nad zakonodajo je profil pravnika

najverjetneje prevladujoč, potrebno znanje pa presega okvire prava in mora biti multidisciplinarno.

Nikakor pa koregulacija na področju vedenjskega oglaševanja ne more delovati učinkovito brez širokega izobraževanja in opolnomočenja posameznikov, katerih pravice in interesi so prizadeti. Ne glede na to, kako protekcionistična so pravila, ostaja dejstvo, da je določena raven odločanja pri vprašanjih vedenjskega oglaševanja vedno v rokah posameznikov, ki morajo biti bodisi sposobni odločiti o tem, ali dovolijo uporabo svojih podatkov za posamezen oglaševalski namen, bodisi biti dovolj usposobljeni, da poznajo možnosti, kako to prekiniti, če tako želijo. Tretja bistvena ugotovitev v tem okviru je torej, da posamezniki niso dovolj obveščeni in izobraženi za uveljavljanje svojih pravic na področju vedenjskega oglaševanja in da bi moralo biti precej več virov (tako finančnih kot tudi drugih) na različnih ravneh (od šolstva dalje) usmerjenih v izobraževanje in opolnomočenje, če bi želeli, da so kakršna koli pravila in strategije regulacije s temeljnim poudarkom na pravicah posameznika učinkovite.

Četrta bistvena ugotovitev je, da vedenjsko oglaševanje nima le negativnih posledic za zasebnost posameznikov in varstvo njihovih osebnih podatkov, ampak gre tudi za druge interese in negativne posledice v smislu vseprisotnega nadzora in diskriminacije, pa tudi negativnega vpliva na politične in demokratične procese. Pričakovati, da bodo vse ali večino teh posledic na različnih družbenih ravneh in sistemih rešila pravila s področja varovanja zasebnosti in varstva osebnih podatkov, ali osredotočenost na vprašanje privolitve ali ne, je utvara, saj zadevajo le najbolj instrumentalen del te dejavnosti – obdelave osebnih podatkov, posledice vedenjskega oglaševanja pa segajo na področje pravil ohranjanja konkurence, davčnih pravil, medijskih pravil, volilnih pravil itd.

Profiliranje, strojno učenje, diskriminacija in posegi v samo bistvo demokratičnega procesa so posledice vedenjskega oglaševanja, ki pravzaprav presegajo tudi današnje različne regulatorne okvire. Ti namreč pogosto le stežka uokvirjajo nove in nove prakse, ki jih omogoča skokovit napredek v razvoju tehnologije. Zato je rešitev, poleg v skladnem izboljšanju različnih relevantnih regulatornih okvirov, smiselno iskati na področju etike, družbene odgovornosti in vizije trajnostnega razvoja družbe, kot zagovarja Pollach (2011), ki je informacijsko zasebnost

umestil v okvir družbene odgovornosti podjetij, kot etično odgovornost, ker zgolj zakonodaja na tem področju ne zajema vseh vidikov obdelave podatkov.

Ugotovitve te študije so skladne s teoretskimi temelji. Baldwin in Cave (1999) navajata, da za eno področje aktivnosti lahko soobstaja več regulacijskih strategij, ki vsaka deluje s svojega vidika – osnove za izvajanje dejavnosti lahko urejajo pravila, hkrati pa obstajajo tudi spodbude in v nekaterih vidikih samoregulacija. Morda obstajajo določbe glede razkritja informacij, hkrati pa so ponudniki izpostavljeni tudi civilnim tožbam. (Baldwin in Cave, 1999, str. 56–57). V primeru vedenjskega oglaševanja študija kaže, da bi bil primeren splet različnih strategij, ki jih navajata. Tako temelje za varovanje pravic posameznikov določa zakonodaja, ki med drugim določa tudi dolžnosti razkritja informacija, določene specifične vidike bi pokrila samoregulacija in v njenem okviru regulacija s kodo (po Lessig, 2016) in tehnični standardi (ne sledi). Hkrati na širše področje izvajanja dejavnosti vplivajo tudi davčna pravila (torej spodbude in obveznosti), pravila za varovanje konkurence, medijska in volilna pravila. Ključno pri takih prepletih regulacijskih strategij pa je, kako oceniti učinkovitost regulacije.

Za odločitev, ali je sistem regulacije dober, je treba situacijo oceniti z vidika petih elementov: zakonodajnega mandata, odgovornosti in nadzora, procesnih varoval, strokovnosti in učinkovitosti. Regulacija izpolnjuje prvo merilo, če je podprta z odločitvijo zakonodajalca, ki izraža voljo ljudstva, in če regulator izpolnjuje mandat, ki mu je bil podeljen. Težava glede tega so nejasno opredeljeni mandati regulatorjev, ki so lahko podvrženi različnim razlagam. Odgovornost regulatorja javnosti in nadzor s strani demokratičnih institucij sta nujna, če želimo govoriti o dobri regulacij, prav tako procesna varovala – regulator mora zagotavljati postopke, ki so pošteni, dostopni in transparentni. Enaka obravnava in doslednost odločanja ter možnost sodelovanja javnosti in drugih zainteresiranih strank v postopkih pred regulatorjem so s tega vidika bistveni. Težava nastane npr. pri tehtanju učinkovitega izvajanja mandata in obširnih procesnih varoval, ki vplivajo na hitrost in ekonomičnost postopkov (Baldwin in Cave, 1999, str. 76–85). Kot je bilo pojasnjeno zgoraj, ima predlagani splet regulacijskih strategij vse možnosti, da izpolni navedena merila, saj upošteva, da so temelji določeni v zakonodaji, ki izražajo voljo ljudstva, vključno s pristojnostmi in dolžnostnimi nadzornih organov ter procesnimi varovali.

Izvajanje funkcij regulacije zahteva strokovno znanje in presojo, še zlasti kadar je treba tehtati med nasprotujočimi interesi ali v situaciji nepopolnih informacij. Zadnje merilo je učinkovitost regulatorja, kar pomeni, da naj bi svoj mandat izvajal z najmanjšimi možnimi sredstvi in je pri produkciji učinkovit. Učinkovitost pomeni tudi, da regulacija vodi k rezultatom, ki so učinkoviti, kar pa ne zadeva nujno ekonomskih kazalcev, ampak lahko tudi družbene cilje in neekonomske cilje (Baldwin in Cave, 1999, str. 76–85). Strokovno znanje je na tako kompleksnem področju, ki zahteva multidisciplinarno znanje in profile, lahko problematično, to pa vpliva tudi na učinkovitost regulatorja pri zasledovanju ekonomskih in družbenih ciljev. Zato je glede tega upoštevana možnost, da natančnejša pravila določijo orodja samoregulacije, ki lahko zagotovijo potrebno strokovnost in učinkovitost, če so seveda upoštevani premisleki o dobri samoregulaciji.

Kot izhaja iz ugotovitev študije in kot poudarjata tudi Baldwin in Cave (1999), je za uspeh celotnega procesa regulacije bistvena faza uveljavljanja pravil oziroma nadzor, saj lahko pravila brez uveljavljanja ostanejo le črka na papirju, hkrati pa tudi premočno ali neustrezno uveljavljanje spodkoplje celoten sistem regulacije. Regulatorji imajo poleg sankcioniranja kršiteljev na voljo tudi neformalna sredstva, kot so izobraževanje, svetovanje, prepričevanje in pogajanja. V primeru slednjih je najbolj poudarjena komponenta promocije skladnosti z zakonom, pri prvem načinu izvrševanja pravil pa je pomembnejše doseganje odvrnilnega učinka in kaznovanja (Baldwin in Cave, 1999, str. 96–106). Ugotovitve študije kažejo, da sta na področju regulacije vedenjskega oglaševanja pomembni obe veji – nadzor nad skladnostjo in izobraževanje, svetovanje – tako subjektom na trgu, ki izvajajo vedenjsko oglaševanje (saj, kot kažejo rezultati, grožnja s kaznijo ni edina motivacija za doseganje skladnosti, ampak je treba upoštevati tudi mehkejše metode izpostavljanja dobrih in slabih praks, ugodnosti, grajenja ugleda ipd.), kot tudi posameznikom glede uveljavljanja njihovih pravic. Se pa tudi na tem področju kaže, da so kazni nadzornih organov pogosto le poslovni stroški največjih spletnih velikanov in da ne vplivajo na to, da bi spremenili svoje prakse obdelave osebnih podatkov, zato so popravljalna dejanja zelo pomemben del sankcioniranja (Baldwin in Cave, 1999, str. 96–106).

Izboljšave na področju zakonodaje EU o varovanju zasebnosti in osebnih podatkov

Boljša regulacija v EU zahteva tudi vsebinske izboljšave na področju zakonodaje o varovanju zasebnosti in osebnih podatkov, predvsem glede konceptov privolitve in alternativnih pravnih podlag (zakonitega interesa), omejitev najspornejših praks v zakonodaji, obveščanja in orodij za večjo odgovornost subjektov, ki izvajajo vedenjsko oglaševanje. Zuiderveen Borgesius (2014) v svoji raziskavi ugotavlja, da za vedenjsko oglaševanje, glede na tveganja, ki jih prinaša za varstvo osebnih podatkov posameznikov, pravna podlaga zakonitega interesa redko pride v poštev, ker so posledice za posameznika lahko resne in je težko trditi, da ne pretehtajo interesa upravljavca podatkov. Privolitev posameznika je tako v EU bistvena predpostavka za zakonito izvajanje vedenjskega oglaševanja, čeprav, kot ugotavlja, je s privolitvijo v praksi veliko težav tudi zaradi njene sporne veljavnosti, če posameznik ni ustrezno obveščen oziroma ne razume kompleksnih procesov v ozadju vedenjskega oglaševanja (Zuiderveen Borgesius, 2014, str. 405–406). Naše ugotovitve to delno potrjujejo – predvsem v delu, da je privolitev v praksi problematična in da niti dodatna varovala iz Uredbe 2016/679 najbrž ne bodo zagotovila, da bodo privolitve pridobljene veljavno. V svojih ugotovitvah upoštevamo, da morajo biti standardi v zakonodaji določeni realistično, če ne jih je težko spoštovati (Baldwin in Cave, 1999), kar se kaže na področju zahteve po privolitvi v piškotke in podobne tehnologije v zakonodaji EU, kjer prevladuje ustvarjalna skladnost s pravili, ki vedenjskega oglaševanja in njegovih posledic pravzaprav ne omejuje. To pomeni, da so po eni strani pravila prestroga (za prakse, ki nimajo znatnega negativnega učinka na posameznike) in po drugi strani preblaga, saj privolitev (čeprav pridobljena na sporno veljaven način) legitimira tudi vedenjsko oglaševanje za namene, ki izrazito negativno učinkujejo na posameznika in družbene procese.

Naše ugotovitve kažejo, da bi morale za najbolj tvegane prakse vedenjskega oglaševanja obstajati omejitve v zakonu. Na to področje gotovo spada vedenjsko oglaševanje v okviru političnega komuniciranja, pa tudi komercialno vedenjsko oglaševanje, kadar omogoča zelo specifično diskriminiranje na podlagi občutljivih podatkov o posamezniku, ki ima zanj znatne negativne posledice v smislu reproduciranja družbene neenakosti, ali kadar vključuje podrobno stalno spremljanje posameznika prek različnih platform. Glede na trenutno ureditev v zakonodaji EU je tudi take prakse mogoče legitimirati s privolitvijo posameznika, čeprav je veljavno privolitev na tem področju zelo težko doseči zaradi pomanjkljivega znanja in razumevanja posameznikov. Prepovedi bi morale biti vsebinsko naravnane na posamezne

sporne namene in posledice vedenjskega oglaševanja ter ne vezane na tehnologije sledenja ali obdelave podatkov, ki so temelj tega. Lahko bi bile zajete v področni zakonodaji, ki ureja npr. volilne procese. Dejstvo pa je, da lahko k takim prepovedim vodi le družbeni konsenz o tem, kakšna družba želimo biti in kako to doseči z omejenim vplivom tehnologije na pravice in interese posameznikov.

Privolitev posameznika, ki je trenutno v okviru zakonodaje EU primarna pravna podlaga za vedenjsko oglaševanje, je le utvara privolitve in je najpogosteje uporabljena za to, da legitimira obdelavo nesorazmerno velikega nabora podatkov. Posamezniki ne razumejo tehnično kompleksne obdelave podatkov, posebej na področju umetne inteligence in programatičnega oglaševanja, in so o tem slabo obveščeni, le redko spreminjajo privzete nastavitve. Glede na to rezultati raziskave nakazujejo, da bi morala imeti privolitev v prihodnosti bolj omejeno vlogo. Da ostane pomenljiva, bi morala biti uporabljena manjkrat, v primerih, ki pomenijo večje tveganje za posameznika pa vendar v situacijah, kjer ima posameznik dejansko možnost odločanja in zavrniti neko obdelavo osebnih podatkov. Večji poudarek bi moral biti na enotnih tehnoloških rešitvah in standardih (standard ne sledi je ena od možnosti). Precej bi moralo biti izboljšano obveščanje posameznikov. Proces privolitve ne bi smel biti moteč za uporabnika in bi ga moral pritegniti v pravem času in kontekstu, da bi lahko prepoznal, za kakšno menjavo vrednosti gre.

Več premisleka bi bilo potrebnega o drugih pravnih podlagah, predvsem zakonitem interesu. Vedenjsko oglaševanje je pogosto del poslovnega modela spletne storitve ali aplikacije, ki je uporabniku na voljo brezplačno oziroma je prilagojena za njegovo uporabo – osebno prilagojena. Od tega ima posameznik lahko večjo korist, kot je zanj negativnih posledic v smislu posega v zasebnost, poleg tega uporabniki pogosto tako raven storitev tudi sami želijo. V vedenjskem oglaševanju, ki ne temelji na občutljivih podatkih in ne posega v pravice posameznika, nekateri ne vidijo škode za posameznika in menijo, da bi lahko temeljilo tudi na legitimnem interesu upravljavca, ki bi izvedel tehtanje in sprejel primerne varovalke. Tu so možnosti za prve strani, ki bi lahko uživale blažji režim pravil za lastno sledenje, večje ekonomske prednosti in tako boljše pogajalske možnosti v razmerju do *ad tech* panoge. Pri slednji je težava obveščanje, saj ga v vsakem primeru težko zagotovijo in se tako težko zanašajo na podlago zakonitega interesa. V nekaterih situacijah je težko zatrjevati zakoniti interes, saj je poseg v posameznikove pravice prevelik in pretehta zakonite interese podjetja

ali organizacije, npr. kjer prihaja do diskriminacije, posebej na podlagi občutljivih podatkov in pri ranljivih skupinah, na področju političnega komuniciranja.

Pomembna ugotovitev študije glede pravnih podlag za izvajanje vedenjskega oglaševanja je, da sta tako privolitev kot tudi zakoniti interes v teoriji trdni pravni podlagi, ki opolnomočita posameznika, oziroma upravljavcu nalagata obveznosti, da ne zbira nesorazmerne količine podatkov, in jo lahko posameznik zavrne oziroma izvede tehtanje interesov in poskrbi za ustrezne varovalke. V praksi pa sta obe pravni podlagi pogosto uporabljeni tako, da obstaja velik dvom v veljavnost in zakonitost. Razlike so tudi v možnostih nadzora. Pridobivanje privolitev je mogoče pri nadzoru lažje izkazati, tehtanje interesov in varovalke pa težje. V tem okviru disertacija ponuja poskus operacionalizacije meril za uporabo zakonitega interesa v modelu operacionalizacije procesa tehtanja zakonitega interesa za primer vedenjskega oglaševanja, kot orodje za odločanje, ali bi bil lahko primerna podlaga v konkretnem primeru izvajanja vedenjskega oglaševanja (če seveda zakon ne predpisuje določene podlage ali omejitve za določen primer, kot trenutno ePD predpisuje privolitev za piškotke). Če bi se ta podlaga uporabljala tudi za vedenjsko oglaševanje je v izogib tveganjem za pravice posameznikov ob samovoljni uporabi zakonitega interesa treba imeti merila, ki bodo omogočila pravno dorečenost (pravna besedila namreč ne ponujajo razlage, kako izvesti tehtanje, niti ne praksa ESČP); kot poudarjata Kamara in deHert (2018) in na koncu tudi usklajenost pri nadzoru – ta je namreč v primeru uporabe te podlage še bolj zahteven, saj zahteva presojo tehtanja, kar npr. pomeni tudi poznavanje zapletene *ad tech* panoge, njenih motivov in ekonomskih modelov, zaradi katerih bi lahko upravljavci zatrjevali nujnost izvajanja vedenjskega oglaševanja. Ne zahteva le znanj s področja varstva osebnih podatkov, ampak tudi kompleksna tehnična znanja, ki omogočajo pregled zalednih podatkov in dnevnikov izvajalcev vedenjskega oglaševanja. V nasprotnem primeru se vpeljava zakonitega interesa kot pravne podlage za vedenjsko oglaševanje lahko izkaže za pravno praznino oziroma blanketno pravno podlago za sledenje uporabnikom in invazivne prakse profiliranja ter oglaševanja.

Vedenjsko oglaševanje nima vedno enako velikih posledic za posameznika in družbo. Veliko je namreč odvisno od tega, kdo ga izvaja, kakšen obseg podatkov se v njem upošteva, kakšna so predvidevanja na podlagi teh podatkov, kakšne so posledice in kakšni nameni oglaševanja ter kakšen je kontekst (Nissenbaum, 2010). Zato je pomembna naša ugotovitev, da privolitev

ni vedno najoptimalnejša pravna podlaga za vedenjsko oglaševanje, ampak bi lahko druge pravne podlage bile učinkovitejše v tehtanju interesov. Kadar ni znatnega posega v pravice posameznikov bi to lahko bil zakoniti interes, pri namenih, ki najbolj škodujejo pravicam posameznikov in demokratični družbi, pa so potrebne vsebinske omejitve za vedenjsko oglaševanje, npr. v področni zakonodaji. Ena od ugotovitev je tudi, da morajo biti določbe zakonov skladne – kar bi bilo treba upoštevati pri razvoju ePR – neskladje v določbah bo nujno vodilo v pravno negotovost, ki bo na škodo interesom posameznikov.

Zuiderveen Borgesius (2014) glede izboljšanja varovanja zasebnosti posameznikov v kontekstu vedenjskega oglaševanja (v okviru prostora EU in zakonodaje v EU) ugotavlja, da bi bilo treba izboljšati (1) ukrepe za opolnomočenje posameznikov in (2) ukrepe za varovanje posameznikov ter oba pristopa kombinirati. Med ukrepi za opolnomočenje posameznikov prišteva strožji nadzor nad določbami o preglednosti obdelave osebnih podatkov in o obveščanju posameznikov, s čimer bi zmanjšali informacijsko asimetrijo na tem področju, ter zahteve po obvestilih v jasnem in dostopnem jeziku. Pravila bi morala jasneje določati, kakšna mora biti privolitev, in zahtevati, da gre za *opt in* in ne *opt out*. Prav tako zagovarja, da bi pravila glede zasebnosti v elektronskih komunikacijah morala zahtevati privolitev za vedenjsko oglaševanje in ne za tehnologije za sledenje, ki so v ozadju. Priporoča upoštevanje razvoja standarda ne sledi (Zuiderveen Borgesius, 2014, str. 412–423). Naše ugotovitve to deloma potrjujejo, predvsem glede nujnosti, da zakonodaja predpiše načine obveščanja, ki bodo učinkovitejši, in izvajanje nadzora nad tem. Kot je bilo že večkrat poudarjeno, pa ta dva elementa nikakor nista dovolj za to, da posamezniki dejansko razumejo procese obdelave podatkov in njihove posledice ter so zmožni uveljavljati svoje pravice in veljavno soglašati. Če je zakonodaja utemeljena na tem, da mora imeti posameznik nadzor nad svojimi podatki, bi moralo biti precej bolj poudarjeno izobraževanje posameznikov, da bodo sploh sposobni in zainteresirani tak nadzor izvajati. Tako – z izobraževanjem (formalnim in neformalnim) – je vpliv na zmanjšanje informacijske asimetrije večji. Študija tudi ugotavlja, da mora biti formulacija glede privolitve in promocija tehničnih standardov za njeno izvedbo karseda jasna.

Rezultati študije kažejo, da je glede obveščanja ključno, da posamezniki obvestilo razumejo in da jih to doseže v primernem času, ne da so nanizane vse obvezne vsebine glede na Uredbo 2016/679, razumevanje posameznika pa je puščeno ob strani. Obvestilo mora biti v jasnejšem,

dostopnem jeziku, ne v pravniškem jeziku, nerazumljivem običajnemu uporabniku, informacije pa morajo biti predstavljene v plasteh, preprosto. Ključni poudarki obvestila bi morali biti na praksah, ki jih posamezniki ne pričakujejo, ne toliko o obdelavah podatkov, ki so normalne, in o obdelavah, ki pomenijo večje tveganje (npr. *fingerprinting*). V različnih kontekstih delimo različne podatke, na športni spletni strani npr. drugačne kot na spletni strani, povezani z zdravstvenimi težavami za uporabnike v tej situaciji je lahko bolj kritično obveščanje o tem, kateri podatki se delijo, kot o tem, točno katere tretje stranke bodo podatke prejele, tudi zato, ker večina uporabnikov pozna le nekaj največjih sledilcev – tretjih strank – kot je npr. Facebook, v panogi pa je veliko malih podjetij, ki niso širše znana. Bistveno je tudi obveščanje o pravicah, ki jih imajo posamezniki.

Bistvene ugotovitve študije glede novih orodij odgovornosti upravljavcev podatkov, tj. upoštevanje načela vgrajene zasebnosti in izvajanje predhodnih ocen vplivov na zasebnost, kažejo, da so ta orodja zelo pomembna v okviru regulacije vedenjskega oglaševanja, saj usmerjata upravljavce podatkov k temu, da že v začetku presodijo, kakšen vpliv ima obdelava osebnih podatkov na posameznika, ter da skušajo sprejeti ukrepe, ki bi posege omejili oziroma da snujejo svoje storitve tako, da je zasebnost vgrajena v delovanje sistemov. Nova orodja odgovornosti so lahko tudi dobro orodje za grajenje odnosa s strankami ter dvigovanje konkurenčne prednosti na račun boljšega varovanja podatkov strank. Vendar pa je na mestu ugotovitev, da je to le sredstvo uveljavljanja pravil – ključna so dobra pravila.

Zuiderveen Borgesius (2014) tudi ugotavlja, da bi morala biti zakonodaja stroga in bi morala jasneje določati načelo najmanjšega obsega podatkov. Če upravljavec ne more zagotavljati izvajanja načela preglednosti, bi morala zakonodaja jasno določati, da je taka obdelava podatkov nezakonita. Glede tega izrecno omenja spletne dražbe uporabniških profilov v realnem času. Predlaga posebno zakonodajo, ki bi veljala za vedenjsko oglaševanje in bi vključevala vse faze tega procesa: zbiranje podatkov, hrambo podatkov, analize, razkrivanje podatkov in uporabo za vedenjsko oglaševanje. Predlaga tudi prepoved »zidov« in različnih možnosti vzemi ali pusti, ki jih upravljavci spletnih strani uporabljajo kot mehanizem za privolitev, ter prepoved, da vedenjsko oglaševanje izvajajo javni RTV servisi in upravljavci, financirani z javnimi sredstvi (Zuiderveen Borgesius, 2014, str. 412–423). Glede na naše ugotovitve ti predlogi ne bi nujno poskrbeli za boljše varstvo posameznikov ob izogibanju pretiranih omejitev za panogo. Dejstvo, da neizvajanje načela preglednosti vnaprej pomeni

nezakonito obdelavo osebnih podatkov, ni nujno vedno točno. Vprašanje je, kakšno je ustrezno obveščanje – je to le zagotovitev, da je skladno z določbami Uredbe 2016/679, ali bi moralo biti vprašanje postavljeno drugače – ali je obveščanje tako, da zagotavlja, da posamezniki informacije razumejo? Ugotovitve naše študije npr. kažejo, da so posameznikom lahko bolj pomenljive informacije o tem, katere svoje podatke delijo s sledilci, kot to, kdo natančno ti sledilci so, saj večine njih niti ne poznajo. Tudi ugotovitev, da so spletne dražbe uporabniških profilov v realnem času zaradi pomanjkljivega obveščanja nezakonite in bi morali biti zidovi prepovedani, upošteva posledic, ki jih ima obdelava podatkov za posameznika, subjekte na trgu, medije in družbo. Kot je bilo pojasnjeno zgoraj, je veliko odvisno od konteksta – kdo izvaja te aktivnosti, s kakšnimi nameni in kako. Različne pravne podlage ponujajo možnost boljšega urejanja področja kot pa zgolj legitimacija teh praks s privolitvijo oziroma prepovedmi posameznih tehničnih rešitev ali načinov obdelave podatkov. Na tem področju so zelo uporabno orodje presoje vplivov na zasebnost, s katerimi lahko upravljavec primerno pretehta situacijo in izbere ustrezno pravno podlago in zaščitne ukrepe. Omejitve bi se morale nanašati na kontekste, kjer je uporaba takih tehnologij in takih praks obdelave osebnih podatkov sporna zaradi znatnih posledic, ki jih ima za posameznika, kot je npr. ugotovitev, da vedenjskega oglaševanja ne bi smeli izvajati javni RTV servisi in upravljavci, financirani z javnimi sredstvi, saj se ne financirajo z oglaševanjem.

7.2 Odgovori na raziskovalna vprašanja

7.2.1 Odgovor na prvo raziskovalno vprašanje

Koliko je izvajanje vedenjskega oglaševanja na različnih platformah elektronskega komuniciranja učinkovito, kaj razvoj tehnologij vedenjskega oglaševanja pomeni v okviru razvoja relevantne panoge in kakšne so posledice za preostale deležnike?

Vedenjsko oglaševanje je učinkovito, ker posameznika nagovarja osebno prilagojeno in je utemeljeno na analizi podatkov posameznika. Ker posameznik vsebine na spletu zaznava selektivno, ima oglaševanje, ki mu pokaže le zanj relevantne vsebine, večjo možnost premagati negativni učinek oglaševalske navlake. Podatki posameznikov so gorivo današnjih najuspešnejših panog in poslovnih modelov. Možnosti obdelave najrazličnejših podatkov, od

demografskih pa do podatkov o vedenju in stališčih, občutljivih osebnih podatkov in lokacij se nezadržno širijo, prav tako se razvijajo sofisticirane tehnike analize podatkov, njihovo kombiniranje in povezovanje prek različnih naprav. Nove možnosti analiz podatkov, ki temeljijo na umetni inteligenci, strojnem učenju in algoritmih, omogočajo pridobivanje zelo specifičnih podatkov prek sklepanja iz neobčutljivih podatkov ali celo na videz neosebnih podatkov in nadaljnje profiliranje posameznikov. Za učinkovitost vedenjskega oglaševanja je pomembno tudi stalno izpopolnjevanje možnosti natančnega ciljanja oglaševanja, kjer je posamezniku mogoče prikazovati oglase na različnih napravah in v različnih okoljih. Kot odgovor na te težnje je zrasel nov sektor podjetij, ki delujejo na področju zbiranja, analize in posredovanja podatkov, kot so preprodajalci podatkov, pa tudi različni oglaševalski posredniki – *ad tech* panoga. V smislu ekonomske učinkovitosti vedenjskega oglaševanja pa je pomembno tudi, da se oglaševanje na spletu in mobilnih napravah čedalje bolj avtomatizira in temelji na sistemih za dražbo uporabniških profilov v realnem času.

Največkrat omenjena prednost vedenjskega oglaševanja je manjša izguba oglaševalskih sredstev za nerelevantna občinstva, saj je mogoče zelo natančno ciljanje na posameznike s specifičnimi lastnostmi, interesi, zgodovino in prikazovanje njim relevantnih vsebin. Eden glavnih argumentov za vedenjsko oglaševanje je omogočanje brezplačnih vsebin in inovativnih storitev. Temu je treba dodati prednosti, ki jih omogoča povezovanje različnih uporabnikovih naprav in razvoj v okviru interneta stvari. Posameznika je mogoče z oglasi doseči na različnih platformah, v kontekstu, ki je za to primeren in na primerni lokaciji. Rezultat zmožnosti čedalje bolj sofisticiranih analiz podatkov posameznikov, pridobljenih iz različnih naprav in nato povezanih, pa je prikazovanje oglasov, ki so relevantni glede na stanje, vedenje in prepričanja posameznika in se tako povečajo možnosti, da se bo nanje ozdval z zaželenim vedenjem.

Ugotovitve študije ne kažejo enotnih učinkov vedenjskega oglaševanja na ključne igralce v sistemu. Po eni strani ima pomembne prednosti zaradi učinkovitega ciljanja, kar poveča možnosti nakupnega vedenja, po drugi strani pa ni nujno, da je za vse subjekte boljša izbira kot običajno digitalno oglaševanje, ki ni utemeljeno na tako natančnih profilih posameznikov.

Iz ugotovitev izhajajo nedvomne prednosti za *ad tech* panogo, ki ponuja storitve vedenjskega oglaševanja, in povezanih podatkovnih storitev (programatično oglaševanje) – od platform za

izmenjavo oglasov, podjetij, specializiranih za avtomatizacijo oddaje oglasnega prostora in specializiranih za dostavo oglasov glede na vnaprej določene preference oglaševalcev pa do različnih ponudnikov podatkovne analize in metrike. Finančni vidiki te panoge so odlični, še zlasti takrat, kadar oglaševalske storitve ponujajo tisti ponudniki, ki kot osnovno storitev ponujajo drugo vrsto dejavnosti (družbeno omrežje, iskalnik itd.), zaradi katere imajo dostop do veliko uporabnikov, ki jim lahko strežejo oglase in katerih podatke lahko analizirajo, kar se kaže tudi v skoraj monopolnih položajih najuspešnejših ponudnikov Facebooka in Googla, ki skupaj pokrivata tudi do 80 odstotkov trga. Prednosti *ad tech* panoge so tudi v razvijajočih se možnostih oglaševanja prek interneta stvari in mobilnih naprav, ki povezujejo aktivnosti potrošnikov na spletu in v realnem življenju. Običajen uporabnik v vsakdanjem življenju uporablja številne storitve elektronskih komunikacij, skoraj vse pa vključujejo obdelavo podatkov za oglaševanje (npr. e-pošta, spletno družbeno omrežje, iskalnik, zemljevidi, druge aplikacije, operacijski sistem Android, ki je v večini vseh pametnih telefonov na trgu, itd.). S širitvami dejavnosti vedenjskega oglaševanja na različne zaslone, na naprave interneta stvari, resnično lahko bolj kot kadarkoli v zgodovini govorimo o vseprisotnem oglaševanju in posamezniku, ki je vedno vključen – vedno na voljo za prikaz relevantnega oglasa glede na njegov trenutni kontekst, ter vedno obkrožen s podatkovnimi točkami, ki hranijo njegov profil. V tem smislu oglaševanje postane dejansko vtkano v vsakodnevne aktivnosti posameznika, kot poudarja koncept mediatizacije, in ne le omejeno na zaslone in čas, ki ga preživi za njimi. Hkrati pa je trg ponudnikov programatičnega oglaševanja zelo nepregleden. V verigi izvajalcev se izgubljajo sredstva (podjetja zaračunavajo provizije), prisotne pa so tudi goljufije in nepoštene prakse. Nepregleden je tudi tok podatkov posameznikov – zato programatično oglaševanje imenujejo tudi črna skrinja, saj je vpogled v njegovo delovanje skoraj nemogoč.

Oglaševalci so pri uporabi sistemov avtomatiziranega oglaševanja izpostavljeni večjim možnostim zlorabe podatkov o njihovih strankah, čeprav naj bi posebej nišnim oglaševalcem natančnejša specifikacija občinstva koristila. Druge raziskave kažejo, da prevladujoči oglaševalci z vedenjskim oglaševanjem ne pridobijo nujno, kadar imajo pomembno konkurenčno prednost pred tekmeci, saj bi s tradicionalnim oglaševanjem imeli na voljo večjo skupino uporabnikov in bi še vedno pridobili pomembne prihodke (Chen in Stallaert, 2014). Učinkovitost oglasov in porabe oglaševalskih sredstev ter merljivost so posebej izpostavljene prednosti avtomatiziranih programatičnih oglaševalskih sistemov.

Pri izdajateljih je slika prednosti in izzivov zopet mešana. Po eni strani vedenjsko oglaševanje omogoča pridobivanje širšega nabora sredstev, ki ga izdajatelji lahko namenijo ustvarjanju vsebine – torej bogati raznolikost ponudbe, po drugi strani pa nima vedno prednosti pred klasičnim oglaševanjem, kjer posamezen oglaševalec neposredno zakupi prostor. Ugotovitve kažejo, da programatično oglaševanje učinkoviteje prinaša prihodke v kontekstu vsebine, ki se težko trži sama, v smislu, da ne predstavlja konteksta oglasu (npr. imeniške spletne strani) ter tudi majhnim izdajateljem, ki nimajo možnosti neposrednih pogajanj z oglaševalci, lahko pa si z uporabo programatičnih sistemov velikih ponudnikov (Google in Facebook) zagotovijo vsaj pokritje svojih stroškov poslovanja. Programatičen zakup naj bi prav tako nižal ceno oglasnemu prostoru, zato ima prednost na spletni strani razmeroma velikega medija neposredno oglaševanje. Druge raziskave kažejo tudi, da imajo z vedenjskim oglaševanjem boljši položaj veliki založniki, kjer za isti oglasni prostor tekmuje več oglaševalcev, ki so med seboj primerljivi, in so uporabniki heterogeni (Chen in Stallaert, 2014). Ugotovitve torej niso enotne, iz česar izhaja vsaj to, da ekonomski učinki za izdajatelje in oglaševalce niso nujno enoznačni, ampak so odvisni od konkretne situacije in strategije izdajatelja. Na strani ponudnikov vsebine se pojavljajo tudi že pozivi, da prične sama izkoriščati potencial podatkov in ne financira izdatno *ad tech* panoge, brez otipljivih prednosti tega zase in z velikimi tveganji glede odgovornosti za kršitev varstva osebnih podatkov uporabnikov (Ryan 2018).

Mediji oziroma njihove spletne edicije so eden ključnih deležnikov med založniki pri vprašanjih uporabe vedenjskega oglaševanja na spletu. Ker lahko uporabniki spletne izdaje običajno spremljajo brezplačno, imajo težave s financiranjem, kar mediji rešujejo z oglaševanjem, tudi vedenjskim, ter tako podatke svojih bralcev delijo z oglaševalci in podjetji, ki sodelujejo pri bolj ali manj avtomatiziranem prikazovanju spletnih oglasov. Kritika z vidika politične ekonomije glede tega poudarja poblagovljenost (komodifikacijo) občinstva. Na ravni dražb uporabniških profilov je vsak posameznik prodan najboljšemu ponudniku za najboljšo ceno in kot kažejo ekonomski podatki, je podatkovna panoga ena najbolj dobičkonosnih v zgodovini. Trenutno mediji uporabljajo različne načine, da uporabnike »prisilijo« v strinjanje z vedenjskim oglaševanjem, bodisi uporabljajo t. i. zidove, kjer brez strinjanja ni mogoč dostop do vsebine, rešitve prijave (angl. *log in*), kjer ta ni dostopna uporabnikom, ki niso registrirani in se niso strinjali z vedenjskim oglaševanjem, ali pa uporabnike o vedenjskem

oglaševanju zgolj obvestijo. Vprašanje sicer je, koliko je nujno posegati prav po vedenjskem oglaševanju, saj ugotovitve ne kažejo, da je to najučinkovitejša možnost v vseh kontekstih. Nekateri vidijo rešitve finančne zagate medijev v naročninah kot alternativnemu viru financiranja, pa tudi v sredstvih, ki bi jih lahko za svoje delovanje mediji pridobili od države. Zadnje raziskave sicer kažejo spodbudna gibanja na področju financiranja spletnih medijev z naročninami. Zagotovo pa je tukaj na mestu pomislek, da naročnine kot alternativni model vedenjskemu oglaševanju vodijo v več zasebnosti za tiste, ki si stroške lahko privoščijo, in manj za tiste, ki si jih ne morejo.

Slika prednosti in izzivov za uporabnike elektronskih komunikacij je podobno mešana – na eni strani vedenjsko oglaševanje omogoča raznolikost vsebine in storitev, ki so jim na voljo (tudi ranljivejšim skupinam, za katere ob plačljivih modelih uporabe ne bi bilo nujno poskrbljeno). ter boljše, bolj relevantne skupine, prihranek virov pri iskanju storitev in produktov. Po drugi strani pa je vedenjsko oglaševanje najpogosteje prikrito, posamezniki tehničnega ozadja in posledic ne razumejo, kar prinaša številne izzive za pravice posameznikov. Nesporno pa je dejstvo, da uporabniki čedalje pogosteje uporabljajo protireklamne vtičnike, tehnologije, ki bodisi zaustavijo prikazovanje oglasov bodisi prekinejo tudi zbiranje podatkov o uporabnikih.

7.2.2 Odgovor na drugo raziskovalno vprašanje

Koliko je vedenjsko oglaševanje invazivno in posega v pravice uporabnikov elektronskih komunikacijskih tehnologij ter koliko so trenutni pristopi k varovanju informacijske zasebnosti uporabnikov uspešni?

Posegi v pravice in interese posameznikov ter demokratične družbene procese

Ugotovitve disertacije kažejo, da je nemogoče pavšalno odgovoriti na vprašanje, ali vedenjsko oglaševanje negativno posega v pravice posameznikov, ampak je treba odgovor iskati v konkretnih situacijah in namenih uporabe. Disertacija je tako obravnavala situacije, v katerih vedenjsko oglaševanje posega v zasebnost posameznikov v negativnem smislu, saj jim onemogoča izvrševanje drugih interesov in pravic. Pokazala pa je tudi, da obstajajo konteksti,

v katerih ta poseg ni kritičen in lahko posameznikom (glede na njihov profil) relevantnejše informacije in vsebine koristijo, zmanjšajo njihov trud in vire, potrebne za pridobivanje informacij, povečajo krog storitev, ki so jim na voljo brezplačno, in omogočajo ustvarjalno izražanje ter inovativnost komunikacij, s katerimi lahko gradijo in utrjujejo svoje družbene odnose. Predvsem so to konteksti, v katerih ni poudarka na obdelavi občutljivih podatkov o posameznikih, v situacijah, ki jih sami dojemajo kot občutljive in ki bi lahko vodile v neželeno diskriminacijo ali politično manipulacijo. Tveganja, ki jih vedenjsko oglaševanje prinaša, so glede na ugotovitve naslednja:

a) Zasebnost, uporaba osebnih podatkov za druge namene in družba nadzora

Sledenje posameznikovim aktivnostim in obdelava njihovih najrazličnejših podatkov (od demografskih pa do podatkov o vedenju in stališčih, občutljivih osebnih podatkov in lokacij) za namen oglaševanja ima negativne posledice za njegovo zasebnost. Uporabniki najpogosteje ne razumejo, kako se podatki o tem, kaj počnejo na spletu, in o njihovi uporabi naprav interneta stvari uporabljajo (npr. podatki o teku iz tekaške zapestnice, na podlagi katerih oglašuje proizvajalec izotoničnih napitkov). Dodatno raven problematiki doda uporaba že zbranih podatkov o posamezniku za druge namene, drugačne od prvotnih, npr. za državno varnost, zavarovalništvo, bančne ocene kreditne sposobnosti (angl. *all data is credit data*), t. i. *function creep* ter pojavnost vseprisotnega nadzora z ogromnimi zbirkami podatkov. Pravica posameznika do zasebnosti in informacijske zasebnosti, v katero vedenjsko oglaševanje bolj ali manj posega, je tista podstat, ki je instrumentalna za izvrševanje drugih pravic – do obveščenosti, enake obravnave ter do svobodnih in pravičnih volitev.

b) Diskriminacija, profiliranje, algoritmi in umetna inteligenca

Nove možnosti analiz podatkov, ki so utemeljene na umetni inteligenci, strojnem učenju in algoritmih, omogočajo pridobivanje zelo specifičnih podatkov prek sklepanja iz neobčutljivih podatkov ali celo na videz neosebnih podatkov, in nato omogočajo razkritja in sklepanja o zelo intimnih situacijah. Tako profiliranje vzbuja vprašanja glede diskriminacije uporabnikov na podlagi njihovih ranljivosti, npr. socialnega statusa, rase in nacionalne pripadnosti, spolne usmerjenosti ipd., posameznikom lahko prepreči dostop do informacij in storitev, jih s tem zapira v mehurček in tako povečuje družbeno razslojenost in segregacijo ter poustvarja in multiplicira stereotipe. Profiliranje za namen cenovne diskriminacije je posebej uporabno v

zavarovalniškem sektorju in bančništvu. Problematično je profiliranje na podlagi napačnih ali netočnih vhodnih podatkov, ki lahko za posameznika pomeni veliko težavo, če je zaradi rezultata profiliranja diskriminiran, mu je omejen dostop do dobrin ali podobno. Tu so ključna vprašanja transparentnosti pri uporabi algoritmov in avtomatiziranega odločanja ter posameznikove možnosti vpliva na avtomatizirane odločitve. Posameznik namreč pogosto ne ve, da je bil profiliran, niti na kakšnih podatkih je profil utemeljen, in tudi nima možnosti zahtevati popravek podatkov ali njihov izbris.

c) Ožanje izbire (t. i. filtre bubbles)

Ena od posledic profiliranja je tudi oženje izbire, ki je posamezniku na voljo, saj profil vedno izhaja iz zgodovinskih podatkov ter predvidevanja, kaj bo posameznika zanimalo v prihodnosti. V tem procesu so lahko neoptimalni vhodni podatki in ne kažejo resničnih interesov posameznika (lahko so netočni, zastareli, vezani le na posamezen kontekst), lahko je napaka tudi v procesu predvidevanja, ker algoritem ni optimalno predvidel prihodnjih interesov posameznika. Rezultat vsega tega je ujetost posameznika v t. i. *filtre bubbles, echo chambers* ipd., kjer so mu vedno znova ponujene enake stvari, kot so ga zanimale v preteklosti, ni pa mu na voljo vsebina, ki bi ga zanimala na novo, ustvarjalno, hipno.

č) Pravica do informiranosti in pravica do svobodnih volitev

Večja težava kot vedenjsko oglaševanje običajnih produktov in storitev je uporaba in zloraba spletnih oglaševalskih sistemov za politično trženje, kjer so podatki uporabnikov uporabljeni za predvidevanje njihovih političnih stališč in nagnjenj ter lahko tudi za to, da je mogoče vplivati na izide volitev v korist posameznega kandidata. Prednosti takih praks so večje možnosti, da politična sporočila dosežejo skupine volivcev, ki jih je težko doseči (npr. mladi), na platformah, ki so jim bliže (npr. spletni družbeni mediji), in glede tematik, ki so jim bolj v interesu in jih bodo mobilizirale. S tem pa lahko pozitivno vpliva na večjo obveščenost volivcev o tematikah, ki so relevantne, in zmanjša odtujenost od političnega procesa ter volilno abstinenco. Ker pa politična sporočila temeljijo na osebnih podatkih, na natančno opredeljenem profilu posameznika, mu je tako dostopnih manj različnih mnenj, kar se kaže v ideološki polarizaciji in prepričljivosti lažnih zgodb pa tudi v potencialih manipulacije. To ogroža medijsko pluralnost in pravico do obveščenosti, saj ponudniki spletnih storitev čedalje bolj prevzemajo vlogo glavnih informatorjev v družbi, hkrati pa jih ne vežejo novinarski

standardi enakovredne zastopanosti stališč. Prav tako pa so s tem ogroženi temeljni demokratični procesi svobodnih, poštenih in preglednih volitev, saj so posamezniki na podlagi posega v svojo zasebnost in analize njihovih podatkov lahko predmet manipulacije za dosego vpliva na izid volitev.

Koliko so trenutni pristopi k varovanju informacijske zasebnosti v kontekstu vedenjskega oglaševanja uspešni?

a) Mehanizmi za zaščito uporabnikov pred vedenjskim oglaševanjem in sledenjem

Posamezniki imajo na voljo spekter različnih možnosti za varovanje svoje zasebnosti pri vedenjskem oglaševanju. Obstajajo nastavitve v aplikacijah, ki preprečujejo zbiranje podatkov (npr. mehanizmi za soglasje v piškotke na spletnih straneh), preprečujejo deljenje podatkov z uporabo zasebnega brskanja (prek nastavitev v brskalniku) ali lahko preprečujejo obdelavo podatkov za vedenjsko oglaševanje (prek sistema samoregulacije). Posameznikom so na voljo tudi različne zasebnosti prijazne tehnologije (PETs). Blokiranje oglasov s protireklamnimi vtičniki je ena najpogosteje uporabljanih tehnologij za varovanje zasebnosti. Uporabniki se za protireklamne vtičnike odločajo iz različnih vzgibov, med drugim zaradi slabe uporabniške izkušnje, predvsem na mobilnih napravah.

Ugotovitve kažejo, da so ti mehanizmi, pri katerih je na posamezniku odgovornost, da se izrazi glede svojih preferenc o zasebnosti oziroma udejanja svoje pravice, razmeroma neučinkoviti, saj posamezniki le redko izrabijo to svojo izbiro. Med razlogi za to je bilo poudarjeno, da je na slabo tehnično podkovanega posameznika preloženo preveliko breme obrambe svojih pravic, pri čemer pogosto niti ne ve, da se njegovi podatki obdelujejo ter zakaj in kakšne so posledice te obdelave, da večina brezplačnih storitev na spletu dejansko temelji na prihodkih, povezanih z obdelavo podatkov uporabnikov in da sledenju skoraj ni mogoče ubežati. Drugi razlog je slabo delovanje teh mehanizmov oziroma nespoštovanje preferenc uporabnika s strani oglaševalske panoge. Ena od zanimivih ugotovitev je tudi, da celotna panoga tehnoloških rešitev sloni na podmeni preprostosti uporabe za uporabnika, tako da ta ni več navajen odločanja v posameznih korakih nastavitev oziroma ni več navajen, da ima v procesih možnosti izbire. Dodatna težava je vezanost procesov na nekega ponudnika (t. i. *lock-in*), ki je prav tako ovira za prehod na uporabo zasebnosti prijaznih storitev. Za

oglaševalsko panogo je prav tako značilno pomanjkanje interesa za ponudbo zasebnosti prijaznih rešitev, saj so lahko drage za implementacijo in lahko pomenijo konkurenčno slabost. Tu so zelo aktualna vprašanja digitalne pismenosti, ki zajema vprašanje dostopa do medijev, enakosti in znanja, kulture in participacije, na katerih temeljijo zmožnosti ocenjevanja in presojanja vsebine oziroma »zasebnostne ločnice« med tistimi, ki vprašanja zasebnosti razumejo, in tistimi, ki jih ne.

Vedenjska ekonomija tudi pojasnjuje, da na posameznika pri izvajanju nadzora nad svojo zasebnostjo vplivajo številni predsodki, kot je npr. predsodek *statusa quo* (angl. *status quo bias*). Slednji opisuje nagnjenje ljudi, da obdržimo privzete možnosti in ne izvajamo sprememb. Predsodek kratkovidnosti (angl. *myopia bias*) pa se nanaša na to, da ljudje stremimo k čimprejšnji nagradi in nismo pozorni na prihodnje stroške in posledice neke naše odločitve. Poleg tega je veliko odvisno od načina, kako so predstavljene informacije in uporabnika zlahka zavedejo v prepričanje, da varuje svojo zasebnost, pa je v resnici ne.

b) Varovanje pravice do informacijske zasebnosti, kot ga zagotavlja trenutni okvir regulacije

Ker vedenjsko oglaševanje v precej kontekstih negativno vpliva na pravice uporabnikov elektronskih komunikacij, je na tem področju kar nekaj regulacije. Analiza trenutnega regulatornega okvira v EU in ZDA je pokazala, da je ta pester, neenoten v zahtevah in zato precej neučinkovit v premagovanju negativnih vidikov vedenjskega oglaševanja za pravice posameznikov. Dejstvo je, da so spletne aktivnosti pri vedenjskem oglaševanju čezmejne, zato je pri sodbah glede učinkovitosti regulacije treba upoštevati mednarodni kontekst pravil, ki ga urejajo.

V EU je pravica do zasebnosti in varstva osebnih podatkov varovana kot temeljna človekova pravica, v ZDA pa varovanje osebnih podatkov spada v okvir varovanja potrošnikovih pravic. Razlike med regulacijo vedenjskega oglaševanja v ZDA in EU se kažejo v temeljnih konceptih regulacije. V ZDA je poudarek na tem, da je posameznik obveščen o obdelavi podatkov, potem pa je odgovornost za varstvo pravice na njem samem, v EU pa že zakonodaja predpisuje, kaj podjetja smejo in česa ne smejo početi s podatki.

Zakonodaja v ZDA ima temelje za varovanje zasebnosti uporabnikov elektronskih storitev v konceptih izogibanja zavajanja potrošnikov. Težava je v omejenih možnostih nadzora, ki jih ima ameriški nadzorni organ Zvezna komisija za trgovino (*Federal Trade Commission* – FTC). To pa je posledica omejene politične volje za strožji nadzor na področju hitro razvijajočih tehnoloških storitev, ki poganjajo ekonomijo ZDA. Je pa na tem področju v ZDA zelo močan pritisk nevladnih organizacij. Kljub temu je regulator obravnaval že precej primerov podjetij s področja vedenjskega oglaševanja ter jim naložil kazni in ukrepe, vendar pa ukrepi predvsem zadevajo boljše obveščanje o praksah sledenja, ne omejijo pa sledenja samega. Po drugi strani ima tudi sistem, kot ga poznamo v EU, pomanjkljivosti. Varstvo osebnih podatkov kot temeljno človekovo pravico naj bi bilo čedalje težje vzdrževati in udejanjati zaradi vseprisotnosti obdelav osebnih podatkov. Vse naše dejavnosti temeljijo na obdelavi osebnih podatkov in njihovo varovanje prav v vseh situacijah; tudi v tistih, v katerih ni posebnega tveganja za škodo posamezniku, naj bi bilo po nepotrebnem omejujoče za napredek panoge.

V ZDA že več let spodletijo vsi poskusi za sprejetje enotne zvezne zakonodaje, ki bi varovala uporabnike elektronskih komunikacij. Spletni velikani svojega poslovnega modela ne morejo veliko spreminjati, ne da bi jim zelo škodilo, če se veliko držav odloči za strogo regulacijo. Leta 2018 je bila v Kaliforniji sprejeta zakonodaja, ki prvič na ravni ene zvezne države v ZDA ureja varstvo potrošnikov pri uporabi informacijskih storitev enotno in horizontalno. Na zvezni ravni panoga zdaj proaktivno podaja svoje predloge, kritiki pa poudarjajo, da je to treba videti v luči izogibanja strogim zahtevam kalifornijskega zakona in Uredbe 2016/679 tako, da bi zvezna zakonodaja določala nižje standarde.

V Evropi je sistem varovanja pravic uporabnikov elektronskih komunikacij pri spletnem sledenju in vedenjskem oglaševanju utemeljen na zakonodaji, in sicer Direktivi 2002/58/ES o zasebnosti v elektronskih komunikacijah (ki jo bo v bližnji prihodnosti nadomestila Uredba o zasebnosti in elektronskih komunikacijah) in Uredbi 2016/679 o varstvu osebnih podatkov. Posebnost reguliranja z evropskimi direktivami je prenos določb v nacionalne zakonodaje držav članic EU, pri katerih je pogosto prišlo do zelo različnih prenosov in razlag določb. Posledica te raznolikosti je pravna negotovost za subjekte na trgu, saj se ni mogoče zanesti na to, da skladnost s pravili v eni članici EU pomeni tudi skladnost v drugi.

Direktiva 2002/58/ES omejuje sledenje s pomočjo piškotkov in podobnih tehnologij ter zahteva vnaprejšnje soglasje uporabnika spleta. Posledica so raznovrstna obvestila oziroma mehanizmi za podajo privolitve v piškotke, ki jih uporabljajo spletne strani v Evropi. Določba o piškotkih je le delno učinkovita zaradi nejasnosti v smislu obsega piškotkov in tehnologij, ki naj bi bil po eni strani preširok (in vključuje tudi piškotke, ki za zasebnost posameznika nimajo posebnega tveganja), po drugi strani pa preozek, saj ni jasno, koliko vključuje drugačne tehnologije sledenja (npr. z odtisom naprave, Wi-Fi sledenje, Bluetooth sledenje), omejene preglednosti in učinkovitosti mehanizmov za podajo soglasja, saj ti posamezniki nimajo možnosti za upravljanje in za zavrnitev soglasja, kot tudi težav z vidika nadzora (Evropska komisija, 2017, str. 134–135).

Evropska zakonodaja na področju vedenjskega oglaševanja glede na ugotovitve analize pravnega okvirja izkazuje kar nekaj pomanjkljivosti. Pravila, ki jih določa, so kompleksna, nejasna in dopuščajo različne razlage, kako tehnično izpolniti zahtevo po pridobivanju privolitve, kakšne obdelave podatkov lahko temeljijo na zakonitem interesu posameznika in kakšne so potrebne za izvajanje pogodbe. Kot kaže razvoj zakonodaje, se pravila, ki urejajo vedenjsko oglaševanje, postavljajo in spreminjajo že desetletje, kar kaže na to, da je postavljanje dobrih standardov na ravni zakonodaje težavno, postopki so togi in dolgotrajni, zakonodaja ki ureja tehnologijo, pa zato v nevarnosti, da hitro zastara. Nadzorni organi v državah članicah imajo različno močne položaje in tudi različna pooblastila.

Zakonodaja v EU je sicer najbrž dosegla večjo obveščenost uporabnikov o tem, da piškotki obstajajo, ali je dejansko zmanjšala sledenje, oziroma ponudila uporabnikom možnost odločanja, pa je zelo vprašljivo. Kot je pokazala analiza regulatornega okvira v EU, ta temelji na razmeroma strogi zakonodaji varstva osebnih podatkov in zasebnosti v elektronskih komunikacijah, ki pa kljub osnovni zapovedi privolitve posameznika v vedenjsko oglaševanje v večini primerov ponuja ravno dovolj izjem in olajšav, da so te lahko bolj ali manj legitimno uporabljene in uporabniku ni ponujena možnost izbire glede vedenjskega oglaševanja ali pa je privolitev pridobljena na način, ki pušča dvome glede njene veljavnosti (implicitno, s pogojevanjem itd.). V praksi to pomeni, da izvajalci vedenjskega oglaševanja poslujejo na trgu, kjer je precej pravne negotovosti, čeprav na ravni mnenj nadzornih organov obstajajo stroge razlage pravil. Če temu prištejemo še pomanjkljiv nadzor nad nejasnimi pravili, ne čudi posledica, da v EU kljub (na papirju) strogim pravilom na trgu sledenja in vedenjskega

oglaševanja pravzaprav ni omejevanja in lahko že leta spremljamo veliko rast in širjenje praks, ki poleg pozitivnih plati osebne prilagoditve pomenijo tudi velika tveganja za pravice posameznikov.

Samoregulacija na področju vedenjskega oglaševanja predvsem zajema kodeks Interactive Advertising Bureauja v povezavi z DAA v ZDA in EASA v EU. Kodeks vpelje spletno mesto youronlinechoices, na katerem lahko posamezniki izrazijo svoje naknadne zavrnitve posameznim akterjem spletnega sledenja, ter ikono ob oglasih, kjer lahko posameznik dobi več informacij o tem, zakaj mu je prikazan oglas in kje se lahko od prejemanja odjavi. Spletna rešitev youronlinechoices po mnenju kritikov naj ne bi bila učinkovita. Ker kodeks nikoli ni vseboval zahteve po tem, da se vedenjsko oglaševanje izvaja šele po privolitvi posameznika, v EU ni dosegel posebne veljave. Samoregulacija kot primarna strategija urejanja vedenjskega oglaševanja ima dvomljivo učinkovitost, če ni izpostavljena zunanjemu nadzoru. Učinkovita je, če so zunanje grozeče sankcije zaradi tega manjše. Ugotovitve tudi kažejo, da sta certificiranje in standardizacija področji, ki obljubljata napredek pri varovanju interesov posameznikov, vendar le, če bosta celostno vpeti v splet regulacijskih strategij in bo temeljne norme ter možnosti sankcioniranja in nadzora zagotavljala zakonodaja. Zdi se, da bo dolgoletno delo na standardu ne sledi obrodilo sadove: standard je načeloma razvit in pripravljen za uporabo, avtorji imajo pripravljajo morebitne prilagoditve z vidika zahtev zakonodaje EU, vendar pa se panoga še vedno obotavlja pri njegovi vpeljavi. Zato je jasno, da mora priti do zunanje spodbude – bodisi v obliki zakonodaje, ki bo zahtevala implementacijo in spoštovanje, bodisi bo ta spodbuda ekonomska, in bo ne sledi za izvajalce vedenjskega oglaševanja manjše zlo, kot so npr. protireklamni vtičniki.

Prednosti standarda ne sledi so v tem, da je privolitev lahko avtomatizirana in podana prek mehanizma na ravni brskalnika. Ta proces je za uporabnika manj moteč, po tej poti pa ima prav tako možnost preklicati svoje soglasje in je o vsem ustrezno obveščen. Dodana vrednost standarda je v tem, da je še pred obiskom spletne strani, še preden je naložena vsebina, mogoče videti, kdo so sledilci na tej strani in s kom se delijo podatki. Izzivi za standard ne sledi so povezani s tem, da večina uporabnikov ne bi nikoli spremenila privzete možnosti ne sledi na ravni brskalnika in aktivno izbrala možnost, da želi deljenje podatkov s tretjimi strankami, te pa posledično ne bi več mogle delovati in bo to pomenilo velik udarec za digitalni ekosistem v Evropi, ki je zelo pomemben za gospodarski napredek Evrope, kot

zatrjuje predvsem oglaševalska panoga. Ker je to tehnična rešitev, je možno tudi, da bo panoga iznašla tehnično rešitev, da upoštevanje omejitev v brskalniku zaobide in tu bo moral nastopiti nadzor.

Razvoj regulacije s področja varovanja pravic uporabnikov elektronskih komunikacij pri vedenjskem oglaševanju nikakor ne poteka v praznem prostoru, omejenem le na vprašanja zasebnosti uporabnikov in prava človekovih pravic ter tehtanjem z ekonomskimi interesi ponudnikov storitev, ki vedenjsko oglaševanje izrabljajo za povečanje svojih prihodkov. Ključen je širši kontekst geopolitičnih odnosov med gospodarstvi tehnološko razvitih držav, ki narekuje, kakšno podjetniško okolje naj države ustvarjajo, da bodo čim bolj konkurenčne, tudi za ceno posegov v pravice uporabnikov elektronskih komunikacij. Pravila, ki varujejo uporabnike, so zunaj EU precej bolj sproščena, kar pomeni prednost za podjetja, ki so ustanovljena v teh pravnih sistemih, ter oviro za tista, ki so ustanovljena v EU in poslujejo v EU. Zato nekateri menijo, da bi morala EU bolj spodbujati evropske ponudnike, ki se trudijo vzdrževati raven storitev, ki ne posega v pravice posameznikov. Nadzor le nad evropskimi podjetji ni smiseln, če hkrati ni nadzora nad velikimi multinacionalkami, ki prevladujejo na trgu, kot so Google, Facebook in Amazon. Na premike v tej smeri kažejo tudi odločitve v zvezi z Googlom in njegovim operacijskim sistemom Android iz leta 2018, v katerih je Evropska komisija postavila Googlu velike zahteve v zvezi z njegovim monopolnim položajnem in mu izrekla sankcijo v višini 4,34 milijarde evrov (Warren, 2018).

7.2.3 Odgovor na tretje raziskovalno vprašanje

Kakšen naj bo okvir za regulacijo vedenjskega oglaševanja v prihodnosti, ob upoštevanju dejavnikov konkurence in sodelovanja med EU in ZDA, značilnosti trgov elektronskih komunikacij in odnosov med regulatorji, panogo in preostalimi deležniki? Kakšna naj bo vloga zakonodaje, samoregulacije, regulacije s kodo, zasebnosti prijaznih tehnologij, certificiranja, izobraževanja, ocen vplivov in koncepta vgrajene zasebnosti?

1. Za boljšo regulacijo področja vedenjskega oglaševanja je potreben splet strategij in orodij ter delovanje na področju vseh deležnikov, ne le izboljšave zakonodaje na tem področju.

Prva ključna ugotovitev v tem kontekstu je, da bi ustrezen splet strategij lahko bila koregulacija, preplet zakonodaje, ki bi dala ustrezno podlago za varovanje temeljnih pravic in interesov posameznikov ter samoregulacije, ki bi jo dopolnila s podrobnejšimi pravili. Prav tako naj bi zakonodaja določala kaznovalne elemente oziroma elemente nadzora, tudi pristojnosti in moči nadzornih organov, brez česar strategija pravil ne more učinkovati. Pravila ne bi smela biti tako stroga, da jih subjekti *a priori* ne bi upoštevali, saj bi bili sicer zakonodajni trud in procesi zaman, interesi posameznikov pa kljub zagotovilom v zakonodaji niso varovani. Na tem področju je bistvena tudi mednarodna razsežnost – če pravila niso vsaj deloma skladna čezmejno, stanje negotovosti in nespoštovanja na trgu ostaja, kar lahko opazujemo v trenutnih razmerah med ohlapnimi pravili v ZDA in strožjimi v EU. Vprašljivo je, koliko lahko to situacijo popravi zunajozemeljski domet nove zakonodaje EU, saj je v praksi nadzor in izvrševanje sankcij izrečenim subjektom zunaj EU zelo zapleten. Poenotenje oziroma skladno razumevanje problematike, z besedami EDPS »enotno diagnosticiranje« problema, bi moralo biti udejanjeno na ravni sodelovanja med EU in ZDA.

Vprašanje podrobnejših pravil glede vedenjskega oglaševanja, tehničnih izvedb zakonsko skladnih rešitev, posebnih omejitev in pravil za specifična področja, obveščanja ipd. je lahko prepuščeno samoregulacijskim strategijam, ki so prožnejše, bolj strokovne, postavljajo učinkovitejše standarde, če seveda izpolnjujejo določene pogoje, npr. glede članstva v organih samoregulacije ali preglednih postopkov sprejema pravil. Področje varovanja zasebnosti in osebnih podatkov ter drugih pravic in interesov je v sodobnem tehnološko razvitem svetu težavno, saj vedno nove tehnologije pomenijo vedno nove izzive za pravice, ki jim zakonodaja sama težko sledi. Ob sprejemu je namreč ta lahko že zastarela oziroma hitro postane neustrezna in zavrti se nov krog sprememb, ki zopet vodijo v pravno negotovost na trgu. Zato je na tem področju velik, še precej neizrabljen potencial samoregulacije – s kodeksi, certificiranjem in tehničnimi standardi – regulacije s kodo, ki bi lahko pomenljivo dopolnila osnovna pravila v zakonodaji, ob predpostavki, da ne bi bilo neskladja z določbami zakonodaje in bi bil določen učinkovit nadzor (ti elementi v trenutnem okviru niso zadovoljeni). Uredba 2016/679 že ponuja nastavke na tem področju, saj vključuje določbe o

potrjevanju kodeksov, certifikacijskih mehanizmov in omenja tehnične standarde za izpolnjevanje določb. Prav tako bi bilo pomembno, da bi bili samoregulacijski mehanizmi vsaj osnovno usklajeni in da ne bi prihajalo do pravne negotovosti. Vlogo pri tem imajo zagotovo nadzorni organi in zakonodajalec, predvsem relevantni direktorati Evropske komisije.

Druga bistvena ugotovitev je, da niti najboljši splet pravil v okviru koregulacije ne more biti učinkovit brez ustreznega nadzora. Pravila tako ostanejo le črka na papirju, kar lahko opazimo pri dozdajšnjem razvoju zakonodaje EU o vedenjskem oglaševanju. Sicer podrobna in stroga pravila niso upoštevana, saj je nadzor pomanjkljiv, subjekti na trgu pa ravnajo skoraj brez omejitev. Pomanjkljiv je zaradi različnih dejavnikov: zaradi nejasnih pravil, ki dopuščajo različne razlage, zaradi neenakih moči in pristojnosti nadzornih organov, zaradi pomanjkljivih pooblastil in težav pri čezmejnem uveljavljanju pravil, tudi zaradi podhranjenosti nadzornih organov v smislu resursov in specifičnega znanja (tehnološkega, ekonomskega, marketinškega), ki je potrebno za kompetentni nadzor na področju sodobnega vedenjskega oglaševanja. Se pa tudi na tem področju kaže, da so kazni nadzornih organov pogosto le poslovni stroški največjih spletnih velikanov in da ne vplivajo na to, da bi spremenili svoje prakse obdelave osebnih podatkov, zato so popravljalna dejanja zelo pomemben del sankcioniranja.

Tretja bistvena ugotovitev v tem okviru torej je, da posamezniki niso dovolj obveščeni in izobraženi za uveljavljanje svojih pravic na področju vedenjskega oglaševanja in da bi moralo biti precej več virov (tako finančnih kot tudi drugih) na različnih ravneh (od šolstva dalje) usmerjenih v izobraževanje in opolnomočenje, če bi želeli, da so kakršna koli pravila in strategije regulacije s temeljnim poudarkom na posameznikovih pravicah učinkovite. Ne glede na to, kako protekcionistična so pravila, ostaja dejstvo, da je določena raven odločanja pri vprašanjih vedenjskega oglaševanja vedno v rokah posameznikov, ki morajo biti bodisi sposobni odločiti o tem, ali dovolijo uporabo svojih podatkov za posamezen oglaševalski namen, bodisi biti dovolj usposobljeni, da poznajo možnosti, kako to prekiniti, če tako želijo.

Četrta bistvena ugotovitev pa je, da vedenjsko oglaševanje nima le negativnih posledic za zasebnost posameznikov in varstvo njihovih osebnih podatkov, ampak so prizadeti tudi drugi interesi in negativne posledice v smislu vseprisotnega nadzora in diskriminacije, pa tudi

negativnega vpliva na politične in demokratične procese. Pričakovati, da bodo vse ali večino teh posledic na različnih družbenih ravneh in sistemih rešila pravila s področja varovanja zasebnosti in varstva osebnih podatkov, ali osredinjenost na vprašanje privolitve ali ne, je utvara, saj zadevajo le najbolj instrumentalen del te dejavnosti – obdelavo osebnih podatkov. Posledice vedenjskega oglaševanja pa segajo tudi na področja pravil varstva konkurence, davčnih pravil, medijskih pravil, volilnih pravil itd. Profiliranje, strojno učenje, diskriminacija in posegi v samo bistvo demokratičnega procesa so posledice vedenjskega oglaševanja, ki pravzaprav presegajo tudi današnje različne regulatorne okvire. Ti namreč pogosto le stežka uokvirjajo nove in nove prakse, ki jih omogoča skokovit napredek v razvoju tehnologije. Zato je rešitev, poleg v skladnem izboljšanju različnih relevantnih regulatornih okvirov, smiselno iskati na področju etike, družbene odgovornosti in vizije trajnostnega razvoja družbe.

V zaključku je pomembna še refleksija konceptualizacije osebnih podatkov v smislu njihove ekonomske vrednosti, ki se čedalje pogosteje pojavlja na različnih ravneh razprave o regulaciji vedenjskega oglaševanja, celo na ravni razvoja zakonodaje: v pristopih regulacije glede na lastništvo podatkov oziroma poudarjanje ekonomskih in drugih ugodnosti, ki naj bi jih posameznikom v zameno za svoje osebne podatke ponudili ponudniki storitev. Taka konceptualizacija krči pomen osebnih podatkov in zasebnosti na njeno ekonomsko vrednost in zasebnosti ne šteje kot tiste, ki omogoča udejanjanje drugih temeljnih pravic posameznika. Tu lahko govorimo o komodifikaciji osebnih podatkov in občinstev, ki spodbuja diskriminacijo in družbeno segregacijo, zasebnostno ločnico, kjer bodo imeli več pravic do zasebnosti bogatejši in bolj izobraženi, socialno in izobrazbeno šibkejši pa bodo podvrženi obdelavam osebnih podatkov, ki vodijo v še večje razslojevanje.

2. Boljša regulacija v EU zahteva tudi vsebinske izboljšave na področju zakonodaje o varovanju zasebnosti in osebnih podatkov, predvsem glede konceptov privolitve in alternativnih pravnih podlag (zakonitega interesa), omejitev najspornejših praks v zakonodaji, obveščanja in orodij za večjo odgovornost subjektov, ki izvajajo vedenjsko oglaševanje.

a) Omejitve v zakonu za najbolj tvegane prakse vedenjskega oglaševanja

Ugotovitve študije kažejo, da so nekatere prakse vedenjskega oglaševanja zelo sporne in močno posegajo v različne pravice posameznikov ter demokratične procese, zlasti zaradi svoje prikritosti in dejstva, da je, ne glede na trud pri obveščanju posameznikov, tehnično zapleten kontekst obdelave podatkov v okviru umetne inteligence, profiliranja in predvidevanja ter posledic teh obdelav v smislu diskriminacije težko razumeti. Zmožnosti beleženja posameznikovih aktivnosti prek velikega števila različnih naprav, pravzaprav 24 ur na dan in na vseh lokacijah pomeni veliko tveganje v smislu družbe nadzora, kraje podatkov in njihove uporabe za druge, nepovezane namene, ki lahko posamezniku škodijo. Na to področje gotovo spada vedenjsko oglaševanje v okviru političnega komuniciranja, pa tudi komercialno vedenjsko oglaševanje, kadar omogoča zelo specifično diskriminiranje na podlagi občutljivih podatkov o posamezniku, ki ima zanj znatne negativne posledice v smislu reproduciranja družbene neenakosti, ali kadar vključuje podrobno stalno spremljanje posameznika prek različnih platform. Glede na veljavno ureditev v zakonodaji EU je tudi take prakse mogoče legitimirati s privolitvijo posameznika – ki sicer mora biti izrecna, kadar gre za obdelavo občutljivih osebnih podatkov, in mora biti v skladu z določbo o profiliranju, ki dodatno zahteva uporabo varoval za zaščito interesov posameznikov. Kot kažejo ugotovitve študije, je veljavno privolitev na tem področju zelo težko doseči, predvsem zaradi pomanjkljivega znanja in razumevanja posameznikov, zato bi moral biti glede teh situacij, ki pomenijo največji poseg v pravice posameznikov in škodo demokratičnim procesom, opravljen premislek o vključitvi specifičnih prepovedi in omejitev v zakonodaji in ne le o omejevanju s pomočjo zahteve po privolitvi. Prepovedi bi morale biti vsebinsko naravnane na nekatere sporne namene in posledice vedenjskega oglaševanja ter ne vezane na tehnologije sledenja ali obdelave podatkov, ki so temelj tega. Lahko bi bile zajete v področni zakonodaji, ki ureja npr. volilne procese. Dejstvo pa je, da lahko k takim prepovedim vodi le družbeni konsenz o tem, kakšna družba želimo biti in kako to doseči z omejenim vplivom tehnologije na pravice in interese posameznikov.

b) Privolitev posameznika kot podlaga za vedenjsko oglaševanje

Ugotovitve študije kažejo, da je za privolitev v svetu vedenjskega oglaševanja značilno, da obstaja veliko različnih tehničnih izvedb, da je uporabljena v preveč situacijah, posamezniki samo brezvoljno klikajo »se strinjam« in gre zato le za utvaro privolitve, da posamezniki pogosto nimajo možnosti zavrniti privolitve, če želijo dostop do storitve (ni svobodna), in da

je uporabljena za to, da legitimira obdelavo nesorazmerno velikega nabora podatkov, da posamezniki ne razumejo tehnično kompleksne obdelave podatkov in so o tem slabo obveščeni, da le redko spreminjajo privzete nastavitve. Večina privolitev v svetu vedenjskega oglaševanja je dvomljive veljavnosti in posamezniki dejansko niso opolnomočeni z možnostjo nadzora nad svojimi podatki.

Rezultati študije nakazujejo, da bi morala biti vloga privolitve v regulaciji vedenjskega oglaševanja bolj omejena in da bi bili interesi posameznikov in oglaševalske panoge bolje pretehtani ob uporabi različnih pravnih podlag. Da bi privolitev posameznikom dejansko omogočala nadzor nad obdelavo svojih podatkov, bi morali upoštevati naslednje elemente:

- večji poudarek bi moral biti na enotnih tehnoloških rešitvah in standardih (standard ne sledi je ena od možnosti);
- posamezniki bi morali biti bolje obveščeni, kot je pojasnjeno v naslednji točki;
- da ostane pomenljiva, bi morala biti uporabljena manjkrat, v primerih, ki pomenijo večje tveganje za posameznika in v katerih ima posameznik dejansko možnost odločanja ter zavrniti neko obdelavo osebnih podatkov;
- proces privolitve ne bi smel biti moteč za uporabnika in bi ga moral pritegniti v pravem času in kontekstu, da bi lahko prepoznal, za kakšno menjavo vrednosti gre.

c) Zakoniti interes kot pravna podlaga za vedenjsko oglaševanje

Čedalje veljavnejši je argument, da bi lahko podjetja vedenjsko oglaševanje izvajala na podlagi svojega zakonitega interesa, ki pretehta nad pravicami posameznikov. To dopušča tudi Uredba 2016/679 (razen v delu piškotkov, kjer trenutno še prevlada zahteva po privolitvi). Vedenjsko oglaševanje je pogosto del poslovnega modela spletne storitve ali aplikacije, ki je uporabniku na voljo brezplačno, oziroma je prilagojena za njegovo uporabo – osebno prilagojena. Od tega ima lahko posameznik večjo korist, kot je zanj negativnih posledic v smislu posega v zasebnost, poleg tega uporabniki pogosto tako raven storitev sami želijo. V vedenjskem oglaševanju, ki ni utemeljeno na občutljivih podatkih in ne posega v pravice posameznika, mnogi strokovnjaki, s katerimi so bili opravljeni intervjuji, ne vidijo škode za posameznika in menijo, da bi lahko temeljilo tudi na legitimnem interesu upravljavca, ki bi izvedel tehtanje in sprejel ustrezne varovalke. Tukaj so možnosti za prve strani, ki bi lahko uživale blažji režim pravil za lastno sledenje, večje ekonomske prednosti in tako boljše pogajalske možnosti v razmerju do *ad tech* panoge. V nekaterih situacijah je na

drugi strani težko zatrjevati zakoniti interes, saj je poseg v posameznikove pravice prevelik in pretehta zakonite interese podjetja ali organizacije, npr. kjer prihaja do diskriminacije, posebej na podlagi občutljivih podatkov in pri ranljivih skupinah, na področju političnega komuniciranja. Izzivi so na področju tehničnih ukrepov, ki bi jih morale sprejeti spletne strani, da bi lahko izpolnile merila zakonitega interesa po tehtanju pravic uporabnikov in nadzoru nad njimi.

Tako privolitev kot tudi zakoniti interes sta v teoriji trdni pravni podlagi, ki opolnomočita posameznika oziroma upravljavcu nalagata obveznosti, da ne zbira nesorazmerne količine podatkov, in jo lahko posameznik zavrne oz. izvede tehtanje interesov ter poskrbi za ustrezne varovalke. V praksi pa sta obe pravni podlagi pogosto uporabljeni tako, da vzbujata velik dvom v veljavnost in zakonitost. Razlike so tudi v možnostih nadzora. Pridobivanje privolitev je mogoče lažje izkazati v nadzoru, tehtanje interesov in varovalk pa težje. V tem okviru disertacija ponuja poskus operacionalizacije meril za uporabo zakonitega interesa v modelu operacionalizacije procesa tehtanja zakonitega interesa za primer vedenjskega oglaševanja kot orodje za pomoč pri odločanju, ali bi bil lahko ustrezna podlaga v konkretnem primeru izvajanja vedenjskega oglaševanja (če seveda zakon za posamezen primer ne predpisuje določene podlage ali omejitve, kot jo trenutno ePD predpisuje glede privolitev za piškotke). Da bi se izognili tveganjem za pravice posameznikov ob samovoljni uporabi zakonitega interesa, je namreč treba imeti merila, ki bodo omogočila pravno dorečenost in na koncu tudi usklajenost pri nadzoru – ta je namreč zahteva presojo tehtanja, kar npr. pomeni tudi poznavanje zapletene *ad tech* panoge, njenih motivov in ekonomskih modelov, zaradi katerih bi lahko upravljavci zatrjevali nujnost izvajanja vedenjskega oglaševanja. Ne zahteva le znanj s področja varstva osebnih podatkov, temveč tudi kompleksna tehnična znanja, ki omogočajo pregled zalednih podatkov in dnevnikov izvajalcev vedenjskega oglaševanja. V nasprotnem primeru se vpeljava zakonitega interesa kot pravne podlage za vedenjsko oglaševanje lahko izkaže za pravno praznino oziroma blanketno pravno podlago za sledenje uporabnikom in invazivne prakse profiliranja ter oglaševanja.

č) Obveščanje

Rezultati študije kažejo, da je glede obveščanja bistveno, da posamezniki obvestilo razumejo in jih doseže v primernem času, ne da so nanizane vse obvezne vsebine glede na Uredbo 2016/679, razumevanje posameznika pa je puščeno ob strani. Obvestilo mora biti v jasnejšem,

dostopnem jeziku in mora predstaviti informacije v plasteh, preprosto. Ključni poudarki obvestila bi morali biti na praksah, ki jih posamezniki ne pričakujejo glede na kontekst in ki pomenijo večje tveganje. Ključno je tudi obveščanje o pravicah, ki jih imajo posamezniki. Obveščanje, katerega rezultat je, da posamezniki informacije razumejo, tako ni nujno le odraz skladnosti obveščanja z Uredbo (EU) 2016/679. Prav tako ni ustrezno obveščanje dovolj, da posamezniki dejansko razumejo procese obdelave podatkov in njihove posledice ter so zmožni uveljavljati svoje pravice in veljavno soglašati. Če zakonodaja temelji na tem, da mora imeti posameznik nadzor nad svojimi podatki, bi moralo biti bolj poudarjeno izobraževanje posameznikov, da bodo sploh sposobni in zainteresirani tak nadzor izvajati.

d) Ocene vplivov na zasebnost in vgrajena zasebnost

Bistvene ugotovitve študije glede novih orodij odgovornosti upravljavcev podatkov, tj. upoštevanje načela vgrajene zasebnosti in izvajanje predhodnih ocen vplivov na zasebnost, kažejo, da so ta orodja zelo pomembna v okviru regulacij vedenjskega oglaševanja, saj usmerjata upravljavce podatkov k temu, da že na začetku presodijo, kako obdelava osebnih podatkov vpliva na posameznika, ter da si prizadevajo sprejeti ukrepe, ki bi posege omejili, oziroma da snujejo svoje storitve tako, da je zasebnost vgrajena v delovanje sistemov. Nova orodja odgovornosti so lahko tudi dobro izhodišče za grajenje odnosa s strankami ter krepitev konkurenčne prednosti na račun boljšega varovanja podatkov strank.

V svojih ugotovitvah upoštevamo, da morajo biti standardi v zakonodaji določeni realistično, saj jih je sicer težko spoštovati, kar se kaže na področju zahteve po privolitvi v piškotke in podobne tehnologije v zakonodaji EU, kjer prevladuje ustvarjalna skladnost s pravili, ki vedenjskega oglaševanja in njegovih posledic pravzaprav ne omejuje. Slednje pomeni, da so po eni strani pravila prestroga – za prakse, ki nimajo znatnega negativnega učinka na posameznike, in po drugi strani preblaga, saj privolitev (čeprav pridobljena na sporno veljaven način) legitimira tudi vedenjsko oglaševanje za namene, ki na posameznika in družbene procese učinkujejo zelo negativno. Zato študija kaže, da bi nekatere sporne prakse morale biti jasno prepovedane, v nekaterih primerih vedenjskega oglaševanja pa bi pravna podlaga zakonitega interesa zagotavljala boljše tehtanje med interesi. Vedenjsko oglaševanje nima vedno enako znatnih posledic za posameznika in družbo, saj je veliko odvisno od tega, kdo ga izvaja, kakšen obseg podatkov se v njem upošteva, kakšna so predvidevanja na podlagi teh podatkov, kakšne so posledice in kakšni nameni oglaševanja itd. V zaključku pa je

nujno poudariti, da morajo biti določbe različne zakonodaje skladne – kar bi bilo treba upoštevati pri razvoju ePR – neskladje v določbah bo nujno vodilo v pravno negotovost, ki bo škodilo interesom posameznikov.

7.3 Operacionalizacija modela tehtanja zakonitega interesa za primer vedenjskega oglaševanja

Ena od ugotovitev disertacije je, da boljša regulacija področja v EU zahteva tudi vsebinske izboljšave na področju zakonodaje o varovanju zasebnosti in osebnih podatkov, predvsem glede konceptov privolitve in alternativnih pravnih podlag, tudi podlage zakonitega interesa. Podlago zakonitega interesa dopušča tudi Uredba 2016/679 (razen v delu piškotkov, kjer trenutno še prevlada zahteva po privolitvi) in zahteva, da upravljavec izvede tehtanje pravic in interesov ter sprejme ustrezna varovala za varovanje pravic posameznikov. V tabeli 7.1 je predstavljen poskus operacionalizacije procesa tehtanja zakonitega interesa za primer vedenjskega oglaševanja. Model je oblikovan kot orodje za pomoč pri odločanju, ali bi bil lahko primerna podlaga v konkretnem primeru izvajanja vedenjskega oglaševanja (če seveda zakon ne predpisuje določene podlage ali omejitve za določen primer, kot trenutno ePD predpisuje privolitev za piškotke).

Tabela 7.1: Poskus operacionalizacije modela tehtanja zakonitega interesa za primer vedenjskega oglaševanja

1. korak – Ali ima upravljavec zakoniti interes?

Splošna merila za tehtanje[80]	*Operacionalizacija meril za področje vedenjskega oglaševanja*
Obstoj legitimnega interesa za obdelavo osebnih podatkov (ne nujno opredeljen v zakonu), ki ni v nasprotju z zakonom (npr. komercialni interes).	Komercialni interes po izvajanju vedenjskega oglaševanja je legitimen, če se storitev dejansko financira iz oglaševalskih sredstev (primeri javne uprave, drugih spletnih strani, ki se ne financirajo z oglaševanjem).

2. korak – Ali je konkretna obdelava podatkov nujna za prav ta interes?

Presoja nujnosti – obdelava osebnih podatkov mora biti neizogibno potrebna; cilji, ki jih zasleduje upravljavec, ne morejo biti doseženi na način, ki ne bi vključeval take obdelave osebnih podatkov.	Ali je nujno uporabiti prav obdelavo osebnih podatkov, kot jo zahteva vedenjsko oglaševanje, in zakaj? Ali je vedenjsko oglaševanje najučinkovitejše za financiranje konkretne storitve (kar ne velja nujno za vse kontekste in razmere, saj imajo mediji lahko večino oglaševalskih prihodkov iz nevedenjskih oblik oglaševanja). Pri tem bi bilo treba preveriti, kolikšen je dejansko prispevek vedenjskega oglaševanja in ali je resnično ključen za financiranje storitve.

3. korak – Tehtanje med nasprotnimi interesi upravljavca in posameznika

Mora biti izveden v vsaki konkretni situaciji obdelave osebnih podatkov, da se ugotovi ali pravice posameznika pretehtajo interese upravljavca ali tretje osebe. Pri tehtanju je treba upoštevati naslednje dejavnike:

Narava in vir zakonitega interesa, npr. ali je obdelava potrebna za izvajanje temeljne pravice ali je drugače v javnem interesu ali je uživa družbeno, kulturno ali pravno priznavanje s strani družbe. Če je temelj legitimnega interesa v zakonodaji (npr. svoboda izražanja), je močnejši, kot če gre le za komercialni interes pridobivanja kupcev prek vedenjskega oglaševanja. Ocena posledic, ki bi jih upravljavec ali družba utrpela, če obdelave ne bi bilo.	Sicer komercialni interes, bodisi pridobivanje strank prek vedenjskega oglaševanja bodisi monetizacija storitve, ki je uporabniku na voljo brezplačno, vendar to pomeni tudi prednosti v smislu brezplačnih informacij, storitev, inovacij, skrbi za nišne populacije, ki so jim na voljo osebno prilagojene storitve. Prihranek virov.
Vpliv obdelave na interese, pravice in svoboščine posameznika: pomeni pozitivne učinke in tudi tveganja. Za izvedbo analize tveganja obstajajo različna orodja, ki jih lahko upravljavec uporabi,[81] ocena pozitivnih učinkov je lahko kompleksnejša, saj je lahko zelo subjektivna.	Pozitivno: Uporabniki želijo in pričakujejo osebno prilagojene storitve, ker so učinkovitejše, jim olajšajo delo, iskanje informacij in komuniciranje. Pričakujejo tudi brezplačne storitve oz. niso pripravljeni plačevati za storitve, ki so v bližnji zgodovini temeljile na brezplačnem modelu. Raznolikost storitev bogati vsakdan in olajša življenje ter ustvarja družbeni napredek – tudi pri ranljivih skupinah, ki si ne bi mogle privoščiti odplačnih poslovnih modelov, invalidi, ki ne bi imeli prilagojenih storitev, ipd. Novičarski mediji ponujajo vsem dostopne informacije, kar ima vlogo v demokratičnem procesu. Negativno: vpliv na zasebnost in varstvo osebnih podatkov, diskriminacija, ujetost v mehurček, izkrivljanje demokratičnih procesov, pravica do informiranosti in svobodnih volitev.
- narava podatkov (občutljivi ali ne, iz javnih virov ali ne ipd), količina podatkov;	Če gre za občutljive osebne podatke, za izpeljane občutljive osebne podatke (npr. politična prepričanja in mikro ciljanje, zdravstveni podatki), bo vedenjsko oglaševanje težko temeljilo na zakonitem interesu, prav tako oglaševanje glede na obdelavo podatkov o lokaciji.

[80] Splošna merila so povzeta po Kamara in deHert (2018) ter WP29 (2014a).
[81] Privacy Risk Assessment Methodology. ISO 31000 on risk management ISO/IEC 27005 which is specific to information security risk management.

- narava in namen obdelave podatkov (ali so javno objavljeni ali dostopni velikemu številu ljudi, ali gre za veliko količino podatkov, ali so namenjeni kombiniranju z drugimi podatki – kot npr. pri komercialnem profiliranju ali profiliranju za namen organov pregona);	Zakoniti interes bo težko zatrjevati v primeru vedenjskega oglaševanja, ki vključuje: - sledenje posameznikom na več spletiščih, lokacijah, napravah in pri storitvah, - povezovanje teh podatkov, kombiniranje podatkov iz različnih virov, - prikazovanje oglasov na različnih napravah, (zasledovanje posameznika z oglasi) tudi tam, kjer jih glede na kontekst posameznik ne pričakuje in lahko pomenijo poseg v njegovo zasebnost, - diskriminacijo glede na občutljive podatke ali ranljive skupine, zavrnjene možnosti. Pri zatrjevanju zakonitega interesa pri profiliranju je pomembno upoštevati: - stopnjo podrobnosti profila (posameznik, na katerega se nanašajo osebni podatki, katerega profil je oblikovan v okviru splošno opisane kohorte, kot je „ljudje, ki se zanimajo za angleško literaturo“, ali segmentiran in ciljno določen na podrobni ravni), - celovitost profila (ali profil opisuje le majhen vidik posameznika, na katerega se nanašajo osebni podatki, ali prikazuje celovitejšo sliko), - vpliv oblikovanja profilov (učinki na posameznika, na katerega se nanašajo osebni podatki – upoštevati je treba tudi potencialna tveganja za prihodnjo uporabo ali kombinacijo profilov), - zaščitni ukrepi, namenjeni zagotavljanju poštenosti, nediskriminacije in točnosti pri postopku oblikovanja profilov – da je dobra napoved, da so možnosti človeške intervencije.
- razumna pričakovanja posameznika, sploh glede uporabe in razkritja podatkov v relevantnem kontekstu (npr. če posameznik naroči produkt v spletni trgovini, lahko razumno pričakuje, da se bodo za ta namen obdelovali podatki, ki so za to neizogibno potrebni). Tukaj so ključne informacije, ki so posamezniku dostopne pred zbiranjem njegovih podatkov (jasne, pravočasne in pregledne), njegovo strinjanje pa je implicirano;	Primer – vedenjsko oglaševanje na napravah, na katerih to ni razumno pričakovano – npr. pametni televizijski sprejemniki, tudi internet stvari, posebej za starejše, ranljivejše skupine.
- status upravljavca in posameznika, odnosi moči med njima (delodajalec je npr. močnejša stranka; ponudnik storitev, ki ima monopolni položaj, je močnejša stranka) ali če je posameznik otrok ali pripada ranljivi skupini;	Če posameznik nima na voljo drugih alternativnih možnosti in je prisiljen uporabljati določene storitve (lahko tudi zaradi tehnološke zaklenjenosti oziroma vpetosti) in s tem tudi obdelave osebnih podatkov.
Dodatna varovala, da se prepreči čezmeren poseg v pravice posameznika: ob upoštevanju učinka takih ukrepov je jasna celotna slika negativnih vidikov za interese in pravice posameznika, treba pa je upoštevati, da je teža ukrepov odvisna od njihovega dejanskega uresničevanja in učinkovitosti.	- omejen nabor osebnih podatkov ali izbris takoj po uporabi; - ukrepi za zavarovanje – ločevanje podatkov (angl. *functional separation*); - raba anonimizacijskih tehnik, agregacije podatkov, PETs, vgrajene zasebnosti in presoja vplivov na zasebnost.
Povečana preglednost, brezpogojna pravica do zavrnitve obdelave, prenosljivost podatkov in drugi ukrepi za opolnomočenje posameznikov. Odgovornost upravljavcev, da potek tehtanja dokumentirajo in zagotovijo vidnost informacij o tehtanju in o tem, zakaj in kako njihov interes prevlada nad interesi posameznikov.	Če upravljavec zagotavlja povečano preglednost in ustrezno izvaja pravico do zavrnitve obdelave ter druge ukrepe za opolnomočenje posameznikov, to govori v korist omejevanja posega v pravice posameznikov. Pomembno je, da tehtanje zakonitega interesa dokumentira.

7.4 Sinteza odgovorov na raziskovalna vprašanja

Tabela 7.2 prikazuje sintezo odgovorov na raziskovalna vprašanja, na jasen in pregleden način, ki bralcu olajša razumevanje. Prikazuje tudi povezavo s teoretskimi pristopi, ki služijo pojasnjevanju relevantnih tematik.

Tabela 7.2: Sinteza odgovorov na raziskovalna vprašanja

1. raziskovalno vprašanje **Koliko je izvajanje vedenjskega oglaševanja na različnih platformah elektronskega komuniciranja učinkovito, kaj razvoj tehnologij vedenjskega oglaševanja pomeni v okviru razvoja relevantne industrije in kakšne so posledice za preostale deležnike?**		**Teoretski okvir**
Kako učinkovito je vedenjsko oglaševanje?	Posameznika nagovarja osebno prilagojeno, temelji na analizi njegovih podatkov in sklepanjih na njegove interese; premaguje oglaševalsko navlako in omejitve selektivne zaznave; Stalno se izboljšujejo možnosti natančnega ciljanja oglaševanja (prikaz oglasa na različnih napravah in v različnih okoljih, kontekstih).	*Teorije tržnega komuniciranja, vsakdanja raba medijev, politična ekonomija komuniciranja*
Kaj razvoj VO pomeni v okviru razvoja relevantne panoge in kakšne so posledice za preostale deležnike?	Nov sektor podjetij, ki delujejo na področju zbiranja, analize in posredovanja podatkov: preprodajalci podatkov in različni oglaševalski posredniki – *ad tech* panoga. Učinki vedenjskega oglaševanja na ključne igralce v ekosistemu niso enotni, ni nujno, da je boljša izbira kot običajno digitalno oglaševanje, ki ne temelji na tako natančnih profilih posameznikov: – nedvomne koristi za *ad tech* panogo (eksponentna rast sektorja), – za izdajatelje, medije in oglaševalce je slika učinkov mešana, vedenjsko oglaševanje ni nujno učinkovitejša izbira.	
Prednosti in izzivi za uporabnike elektronskih komunikacij	Vedenjsko oglaševanje omogoča raznolikost in kakovost vsebine ter storitev (tudi ranljivejšim skupinam, za katere ob plačljivih modelih uporabe ne bi bilo nujno poskrbljeno), prihranek virov pri iskanju storitev in produktov, filtriranje informacij, posameznikom omogoča ustvarjalno izražanje ter inovativnost in komunikacije, s katerimi lahko gradijo in utrjujejo svoje družbene odnose. Najpogosteje je prikrito, posamezniki tehničnega ozadja in posledic ne razumejo – poseg v zasebnost, lahko onemogoča tudi izvrševanje drugih interesov in pravic.	*Teorije informacijske zasebnosti, vedenjska ekonomija*
2. raziskovalno vprašanje **Koliko je vedenjsko oglaševanje invazivno in posega v pravice uporabnikov elektronskih komunikacijskih tehnologij ter koliko so trenutni pristopi k varovanju informacijske zasebnosti uporabnikov uspešni?**		
a) Posegi v pravice posameznikov	Specifična tveganja, ki jih vedenjsko oglaševanje prinaša posameznikom: – zasebnost, uporaba osebnih podatkov za druge namene in družba nadzora, – diskriminacija, profiliranje, algoritmi in umetna inteligenca, – oženje izbire (t. i. *filtre bubbles*), – pravica do informiranosti in pravica do svobodnih volitev. V nekaterih kontekstih poseg v pravice posameznikov ni kritičen in je korist večja (predvsem kadar ni poudarka na obdelavi občutljivih podatkov o posameznikih, občutljivih situacijah, ki bi lahko vodile v neželeno	*vsakdanja raba medijev, teorije informacijske zasebnosti, vedenjska ekonomija, normativna teorija*

	diskriminacijo ali politično manipulacijo).	
b) Kako lahko posameznik sam varuje svojo zasebnost? ** Zakaj posamezniki redko izrabijo možnost izbire zasebnosti prijaznejših rešitev?*	Mehanizmi, pri katerih je na posamezniku odgovornost, da se izrazi glede svojih preferenc o zasebnosti, so razmeroma neučinkoviti (posamezniki se le redko odločijo za to izbiro): – zaradi slabe tehnične podkovanosti in seznanjenosti s tem, da se podatki obdelujejo, in kakšne so posledice, da večina brezplačnih storitev temelji na monetizaciji podatkov posameznikov (problematika digitalne pismenosti, enakosti dostopa do medijev in informacij, zasebnostne ločnice), – ker na posameznika vplivajo številni predsodki (nagnjenje k obdržanju privzetih možnosti, stremimo k čimprejšnji nagradi in nismo pozorni na prihodnje posledice neke naše odločitve), – zaradi neučinkovitega delovanja orodij za varovanje zasebnosti oz. nespoštovanja nastavitev uporabnika s strani panoge.	*Teorije informacijske zasebnosti, vedenjska ekonomija, vsakdanja raba medijev*
c) Varovanje pravice do informacijske zasebnosti, kot ga zagotavlja trenutni okvir regulacije	Regulatorni okvir v EU in ZDA je pester, neenoten v zahtevah in zato precej neučinkovit v premagovanju negativnih vidikov vedenjskega oglaševanja za pravice posameznikov. Bistven je širši kontekst geopolitičnih odnosov med gospodarstvi tehnološko razvitih držav, ki narekuje, kakšno podjetniško okolje naj države ustvarjajo, da bodo čim bolj konkurenčne, tudi za ceno posegov v pravice uporabnikov elektronskih komunikacij.	*Teorije informacijske zasebnosti, normativne teorije*
Zakonodajni okvir	Regulacija v ZDA ne temelji na zakonodaji o varstvu osebnih podatkov, ampak predvsem na regulacijskem kodeksu za vedenjsko oglaševanje, ki temelji na pristopu *opt-out*. Regulator za varovanje potrošnikov izvaja nadzor nad praksami vedenjskega oglaševanja z vidika zavajajočih obvestil podjetij. V Evropi okvir regulacije določa predvsem zakonodaja, pravila so kompleksna, nejasna in dopuščajo različne razlage, kako tehnično zadovoljiti zahtevo po pridobivanju privolitve. Nadzorni organi v državah članicah EU imajo različno močne položaje in tudi različna pooblastila.	
Samoregulacija	Kodeks Interactive Advertising Bureauja v povezavi z DAA v ZDA in EASA v EU (spletno mesto youronlinechoices, na katerem lahko posamezniki izrazijo svoje naknadne zavrnitve posameznim akterjem spletnega sledenja, in ikona ob oglasih, kjer lahko posameznik dobi več informacij o tem, zakaj mu je prikazan oglas in kje se lahko od prejemanja odjavi).	
Standardizacija	Standard ne sledi je načeloma razvit in pripravljen za uporabo, panoga pa se obotavlja pri njegovi uveljavitvi, kar kaže na nujnost zunanje spodbude – bodisi v smislu zakonodaje bodisi ekonomskih spodbud.	

3. raziskovalno vprašanje
Kakšen naj bo okvir za regulacijo vedenjskega oglaševanja v prihodnosti, ob upoštevanju dejavnikov konkurence in sodelovanja med EU in ZDA, značilnosti trgov elektronskih komunikacij in odnosov med regulatorji, panogo ter preostalimi deležniki? Kakšna naj bo vloga zakonodaje, samoregulacije, regulacije s kodo, zasebnosti prijaznih tehnologij, certificiranja, izobraževanja, ocen vplivov in koncepta vgrajene zasebnosti?

Za boljšo regulacijo področja vedenjskega oglaševanja je potreben splet strategij in orodij ter delovanje na področju vseh deležnikov, ne le izboljšave zakonodaje na tem področju.	1. Koregulacija: – zakonodaja določa ustrezno podlago za varovanje temeljnih pravic in interesov posameznikov, kaznovalne elemente oziroma elemente nadzora in tudi pristojnosti in moči nadzornih organov, – samoregulacija (kodeksi, certificiranje in tehničnimi standardi) dopolni s podrobnejšimi pravili, tehničnimi izvedbami zakonsko skladnih rešitev, posebnimi omejitvami in pravili za specifična področja, obveščanje. Mora biti skladna z zahtevami zakonodaje. 2. Nujnost izboljšav na področju nadzora. 3. Vlaganje v izobraževanje in opolnomočenje posameznikov, da so lahko pravila in strategije regulacije s temeljnim poudarkom na pravicah posameznika učinkovite. 4. Posledice vedenjskega oglaševanja segajo na področje pravil za varstvo konkurence, davčnih pravil, medijskih pravil, volilnih pravil itd., ne le pravil na področju varstva osebnih podatkov. 5. Konceptualizacije osebnih podatkov v smislu njihove ekonomske vrednosti – vodi v komodifikacijo osebnih podatkov in občinstev, ki spodbuja diskriminacijo in družbeno segregacijo, zasebnostno ločnico.	*politična ekonomija komuniciranja, vsakdanja raba medijev, normativne teorije, pristop družbene odgovornosti*

Boljša regulacija v EU zahteva tudi vsebinske izboljšave na področju zakonodaje o varovanju zasebnosti in osebnih podatkov, predvsem glede konceptov privolitve in alternativnih pravnih podlag (zakonitega interesa), omejitev najspornejših praks v zakonodaji, obveščanja in orodij za večjo odgovornost subjektov, ki izvajajo vedenjsko oglaševanje.	– Za najbolj tvegane namene vedenjskega oglaševanja bi morale obstajati omejitve v zakonu (npr. v okviru političnega komuniciranja, diskriminiranja, stalnega spremljanja prek različnih platform). – Privolitev bi morala biti omejena na primere, ki pomenijo večje tveganje za pravice posameznika, in je hkrati posameznik zmožen situacijo razumeti in podati veljavno privolitev. Proces pridobivanja privolitve ne bi smel biti moteč. Večji poudarek bi moral biti na enotnih tehnoloških rešitvah in standardih za pridobivanje privolitve (standard ne sledi je ena od možnosti). – V nekaterih primerih bi lahko ustrezno pravno podlago za vedenjsko oglaševanje iskali v zakonitem interesu izvajalca (ni obdelave ali sklepanja na občutljive osebne podatke ter je poseg v zasebnost zanemarljiv. Disertacija zato ponuja model operacionalizacije procesa tehtanja zakonitega interesa za primer vedenjskega oglaševanja. Ključno je tudi boljše obveščanje ter izobraževanje posameznikov, da bodo sposobni in zainteresirani nadzor nad svojimi podatki izvajati. Ključni poudarki obvestila bi morali biti na praksah, ki jih posamezniki ne pričakujejo glede na kontekst in ki pomenijo večje tveganje. Zelo je pomembno upoštevanje načela vgrajene zasebnosti in izvajanje predhodnih ocen vplivov na zasebnost, saj usmerja izvajalce k uvajanju poslovnih modelov, ki omejujejo posege v pravice posameznikov.	*Teorije informacijske zasebnosti, vedenjska ekonomija, normativne teorije, pristop družbene odgovornosti.*

8 ZAKLJUČEK

8.1 Sklepne misli

Disertacija obravnava vedenjsko oglaševanje pri različnih storitvah elektronskih komunikacij, prek različnih naprav in tehnoloških ravni ter odgovarja na vprašanja, kakšne so prednosti, ki jih prinaša različnim deležnikom – oglaševalcem, *ad tech* panogi in založnikom, zlasti medijem ter posameznikom, ki so vedenjskega oglaševanja deležni. Odkriva tudi negativne plati in posledice, ki jih ima za pravice in interese posameznikov, za deležnike v ekosistemu, družbo in demokratične procese. Razišče trenuten okvir regulacije v EU in ZDA, kar zajema zakonodajo, samoregulacijo ter tudi standardizacijske aktivnosti, in predlaga okvir za boljšo regulacijo vedenjskega oglaševanja v prihodnosti – tak, ki bo bolje pretehtal različne interese in bo učinkoviteje omejil negativne posledice s podatkovnimi analizami okrepljenih marketinških strategij. Disertacija vedenjsko oglaševanje razišče s kombinacijo dveh sočasno uporabljenih kvalitativnih metod, katerih cilj je bil celostna obravnava problematike in ne le iskanje parcialnih rešitev.

Vedenjsko oglaševanje je učinkovito, ker posameznika nagovarja osebno prilagojeno – relevantno glede na njegovo stanje, vedenje in prepričanja. Tako se povečajo možnosti, da se bo na oglase odzval z zaželenim (nakupnim) vedenjem. Temelj osebne prilagoditve je zbiranje podatkov o posameznikih, njihova analiza in umeščanje posameznikov v profile, na podlagi katerih je izbran posamezniku primeren oglas. Podatki posameznikov so tako gorivo današnjih najuspešnejših panog in poslovnih modelov, kjer je večina storitev posameznikom sicer na voljo brezplačno, prihodke pa ponudniki storitev pridobivajo z (najpogosteje) vedenjskim oglaševanjem. Učinkovitost vedenjskega oglaševanja se krepi s tehnološkim napredkom na področju možnosti zbiranja podatkov, njihovih obdelav in analiz ter ciljanja oglasov. Zanj je značilno povezovanje in kombiniranje podatkov, zbranih iz različnih *online* in *offline* virov, uporaba umetne inteligence, algoritmov in strojnega učenja za analizo podatkov ter navsezadnje težnje k čedalje večji avtomatizaciji oglaševanja, ki vse bolj temelji na sistemih za dražbo uporabniških profilov v realnem času. Govorimo lahko o vseprisotnem oglaševanju in posamezniku, ki je vedno vključen, oglaševanje je vtkano v vsakodnevne aktivnosti posameznika, kot poudarja koncept mediatizacije, in ne le omejeno na zaslone in čas, ki ga preživi za njimi.

V ekosistemu vedenjskega oglaševanja nastopajo različni akterji in kot kažejo naše ugotovitve, ni nujno, da je za vse subjekte boljša izbira kot tradicionalno oglaševanje, ki ne temelji na osebni prilagoditvi. Prednosti nedvomno prinaša ad tech panogi, ki ponuja storitve vedenjskega oglaševanja in povezanih podatkovnih storitev, še zlasti tistim ponudnikom, ki imajo dostop do podatkov velikega števila uporabnikov svojih »osnovnih storitev« (npr. Facebook in Google). Največja prednost vedenjskega oglaševanja za oglaševalce naj bi bila manjša izguba sredstev za nerelevantna občinstva, predvsem za nišne oglaševalce, boljše ciljanje ter merljivost. So pa pri uporabi sistemov avtomatiziranega oglaševanja izpostavljeni večjim možnostim zlorabe podatkov o njihovih strankah s strani ad tech panoge. Ni nujno, da je zanje vedenjsko oglaševanje boljša možnost od tradicionalnega, še zlasti kadar imajo pomembno konkurenčno prednost pred tekmeci (Chen in Stallaert, 2014). Izdajateljem vedenjsko oglaševanje omogoča več sredstev za ustvarjanje vsebine, še zlasti kadar se ta težko trži sama in pri manjših izdajateljih, ki nimajo možnosti neposrednega pogajanja z oglaševalci. Nekatere raziskave kažejo tudi prednosti vedenjskega oglaševanja pri velikih izdajateljih (Chen in Stallaert 2014). Programatičen zakup naj bi po drugi strani oglasnemu prostoru nižal ceno, poleg tega izdajatelji podatkov svojih strank ne izkoriščajo sami, ampak ekonomske koristi večinoma prepustijo ad tech panogi, tveganja z vidika varstva osebnih podatkov strank pa so večja. Mediji z vedenjskim oglaševanjem pristopajo k reševanju finančnih težav in pogosto omejujejo dostop do vsebine tistim, ki takega oglaševanja ne želijo (z zidovi in rešitvami prijave). Zgornje ugotovitve pa kažejo, da vedenjsko oglaševanje ni nujno najučinkovitejša ekonomska možnost financiranja vsebine (rešitve so tudi na področju naročnin ter financiranja s strani države), še zlasti če tveganjem prištejemo izpostavljenost ranljivejših posameznikov.

Slika prednosti in izzivov za uporabnike elektronskih komunikacij je podobno mešana. Na eni strani vedenjsko oglaševanje omogoča raznolikost vsebine in storitev, ki so jim na voljo (tudi ranljivejšim skupinam, za katere ob plačljivih modelih uporabe ne bi bilo nujno poskrbljeno), ter boljše, bolj relevantne storitve, prihranek virov pri iskanju storitev in produktov ipd. Po drugi strani pa je vedenjsko oglaševanje najpogosteje prikrito, posamezniki tehničnega ozadja in posledic ne razumejo, kar prinaša številne izzive za pravice posameznikov:

- poseg v pravico do zasebnosti in varstva osebnih podatkov ter vseprisotni nadzor komercialnih institucij in sledenje prek različnih naprav *online* in *offline*;

- poseg v pravico do enake obravnave: profiliranje posameznikov lahko vodi v diskriminacijo, ki posameznikom otežuje dostop do informacij in storitev, veča družbeno razslojenost in segregacijo ter poustvarja in multiplicira stereotipe;
- oženje izbire (t. i. *filtre bubbles*), ki je posamezniku na voljo, saj profil vedno temelji na zgodovinskih podatkih ter predvidevanju, kaj bo posameznika zanimalo v prihodnosti, ni pa mu na voljo vsebina, ki bi ga zanimala na novo, ustvarjalno, hipno;
- uporaba in zloraba spletnih oglaševalskih sistemov za politično trženje posega v pravico do informiranosti in pravico do svobodnih volitev.

Posamezniki imajo na voljo spekter različnih možnosti za varovanje svoje zasebnosti pri vedenjskem oglaševanju, vendar jih le redko izrabijo, in sicer zaradi slabe tehnične podkovanosti in slabega razumevanja posledic vedenjskega oglaševanja, tudi zaradi vezanosti na posameznega ponudnika. V zadnjem obdobju je sicer viden porast uporabe protireklamnih vtičnikov, vendar najbrž predvsem zaradi izboljšane izkušnje uporabe storitev brez oglasov. Glede tega so zelo aktualna vprašanja digitalne pismenosti, oziroma »zasebnostne ločnice« med tistimi, ki vprašanja zasebnosti razumejo, in tistimi, ki jih ne. Na posameznika pri izvajanju nadzora nad svojo zasebnostjo prav tako vplivajo številni predsodki, kot je npr. predsodek *statusa quo* in predsodek kratkovidnosti. Ker vedenjsko oglaševanje v precej kontekstih negativno vpliva na pravice uporabnikov elektronskih komunikacij, na tem področju v EU in ZDA obstaja kar nekaj regulacije, vendar je ta neenotna v zahtevah in zato precej neučinkovita. Za razvoj regulacije je bistven širši kontekst geopolitičnih odnosov med gospodarstvi tehnološko razvitih držav, kjer je dopuščanje posegov v zasebnost uporabnikov del širšega spleta politik, s ciljem konkurenčnosti poslovnega okolja.

Pomembna je tudi refleksija konceptualizacije osebnih podatkov v smislu njihove ekonomske vrednosti, ki se čedalje pogosteje pojavlja na različnih ravneh razprave o regulaciji vedenjskega oglaševanja, celo na ravni razvoja zakonodaje: v pristopih regulacije glede na lastništvo podatkov oziroma poudarjanju ekonomskih in drugih ugodnosti, ki naj bi jih posameznikom v zameno za njihove osebne podatke ponudili ponudniki storitev. Taka konceptualizacija reducira pomen osebnih podatkov in zasebnosti na njeno ekonomsko vrednost in zasebnosti ne šteje kot tiste, ki omogoča udejanjanje drugih temeljnih pravic posameznika. Tu lahko govorimo o komodifikaciji osebnih podatkov in občinstev, ki spodbuja diskriminacijo in družbeno segregacijo, zasebnostno ločnico, kjer bodo imeli več

pravic do zasebnosti bogatejši in bolj izobraženi, socialno in izobrazbeno šibkejši pa bodo podvrženi obdelavam njihovih osebnih podatkov, ki vodijo v še večje razslojevanje.

Za boljšo regulacijo področja vedenjskega oglaševanja v prihodnosti je potreben splet strategij in orodij ter usklajeno delovanje globalnih deležnikov, ne le izboljšave zakonodaje na tem področju. Ustrezen splet bi lahko bila koregulacija, preplet zakonodaje, ki bi dala ustrezno podlago za varovanje temeljnih pravic in interesov posameznikov (ter določala kaznovalne elemente oziroma elemente nadzora) in samoregulacije, ki bi jo dopolnila s podrobnejšimi vsebinskimi pravili. Poenotiti bi bilo treba razumevanje problematike vedenjskega oglaševanja med ZDA in EU, saj so dejavnosti čezmejne. Bistveni komponenti za učinkovito koregulacijo sta »pameten« nadzor in okrepitev nadzornih organov ter široko izobraževanje in opolnomočenje posameznikov (od šolske ravni dalje), da bodo sposobni uveljavljati svoje pravice. Ker vedenjsko oglaševanje negativno vpliva tudi na politične pravice in demokratične procese, pravila s področja varovanja zasebnosti in varstva osebnih podatkov ne morejo rešiti problematike celostno. Tukaj imajo pomembno vlogo pravila za varstvo konkurence, davčna pravila, medijska pravila, volilna pravila itd. Poleg skladnega izboljšanja različnih relevantnih regulatornih okvirov je rešitve smiselno iskati tudi na področju etike, družbene odgovornosti in vizije trajnostnega razvoja družbe.

Boljša regulacija v EU zahteva tudi konkretne vsebinske izboljšave na področju zakonodaje o varovanju zasebnosti in osebnih podatkov (tako v smislu razlag Uredbe 2016/679 kot tudi trenutno nastajajoče ePR), predvsem glede različnih pravnih podlag, ki zagotavljajo možnost boljšega urejanja področja, kot pa zgolj legitimacija praks vedenjskega oglaševanja s privolitvijo. Za najbolj tvegane namene vedenjskega oglaševanja[82] bi morale obstajati zakonske omejitve (npr. v okviru političnega komuniciranja, kadar omogoča zelo specifično diskriminiranje, ki ima znatne negativne posledice v smislu reproduciranja družbene neenakosti, ali vključuje stalno spremljanje posameznika prek različnih platform). Privolitev bi morala biti omejena na primere, ki pomenijo večje tveganje za pravice posameznika, in je hkrati posameznik zmožen situacijo razumeti ter podati veljavno privolitev. Proces pridobivanja privolitve ne bi smel biti moteč in bi moral posameznika pritegniti v pravem času in kontekstu, da bi lahko prepoznal, za kakšno menjavo vrednosti gre. Večji poudarek bi

[82] Pri takih vrstah vedenjskega oglaševanja je tudi težko doseči veljavno privolitev zaradi pomanjkljivega znanja in razumevanja posameznikov.

moral biti na enotnih tehnoloških rešitvah in standardih za pridobivanje privolitve (standard ne sledi je ena od možnosti). V nekaterih primerih bi lahko primerno pravno podlago za vedenjsko oglaševanje iskali v zakonitem interesu izvajalca,[83] kadar npr. v procesu ni obdelave ali sklepanja glede občutljivih osebnih podatkov ter je poseg v zasebnost zanemarljiv, ni diskriminacije ali vpliva na politične pravice. Da bi se izognili tveganjem ob samovoljni uporabi tehtanja zakonitega interesa, so potrebna merila, ki bi omogočila pravno dorečenost in usklajenost pri nadzoru – presoji izvedenega tehtanja.[84] Disertacija zato v zaključku ponuja model operacionalizacije procesa tehtanja zakonitega interesa za primer vedenjskega oglaševanja. Bistvene so tudi izboljšave na področju obveščanja o vedenjskem oglaševanju s strani izvajalcev ter izobraževanju posameznikov, da bodo sposobni in zainteresirani nadzor nad svojimi podatki izvajati. Navsezadnje pa je zelo pomembno upoštevanje načela vgrajene zasebnosti in izvajanje predhodnih ocen vplivov na zasebnost, saj usmerja izvajalce k uvajanju poslovnih modelov, ki omejujejo posege v pravice posameznikov.

8.2 Omejitve in nadaljnje raziskovanje

Disertacija obravnava vedenjsko oglaševanje pri različnih storitvah elektronskih komunikacij, preko različnih naprav in tehnoloških ravni in se sprašuje o bodočem okviru regulacije. Konceptualni okvir gradi na kombiniranju različnih teorij, ki vsaka posebej in v kombinaciji prispevajo k boljšemu razumevanju različnih nians in vidikov fenomena. Čeprav naše ugotovitve potrjujejo koristnost omenjenih teoretskih pristopov pri razumevanju fenomena vedenjskega oglaševanja, ima multi-teoretski pristop k raziskovanju tudi svoje omejitve; predvsem z vidika poglobljenosti obravnave fenomena raziskovanja in potencialnih nasprotujočih si pogledov med posameznimi teoretskimi pristopi. Vsekakor bi bilo mogoče v vsakem izmed teoretskih pristopov, ki smo jih uporabili, raziskovati tematiko še globlje in veliko bolj podrobno, npr. glede pogleda uporabnikov, posameznikov, ki se praksam vedenjskega oglaševanja upirajo, in podobno. Ob omejitvah obsega disertacije se pričujoči multi-teoretski okvir osredotoča predvsem na tiste bistvene poudarke znotraj posameznega pristopa, ki nam lahko pomagajo pri razumevanju kompleksnosti vedenjskega oglaševanja, pri

[83] To ima lahko za posameznika večjo korist, kot pa je deležen negativnih posledic v smislu posega v zasebnost. Poleg tega to dopušča tudi Uredba 2016/679 (razen v delu piškotkov, kjer trenutno še prevlada zahteva po privolitvi iz ePD).
[84] To pomeni tudi poznavanje zapletene *ad tech* panoge in ekonomskih modelov ter kompleksna tehnična znanja, ki omogočajo pregled zalednih podatkov in dnevnikov izvajalcev vedenjskega oglaševanja.

tem pa ne predstavlja nujno edine mogoče kombinacije različnih teoretičnih pristopov. Globlje raziskovanje tematike znotraj posameznega teoretskega pristopa in obravnava alternativnih pristopov, ki bi prav tako lahko osvetlili kompleksnost problematike vedenjskega oglaševanja, ostaja priložnost za nadaljnje študije.

Iz ugotovitev disertacije izhajajo neenotne ugotovitve o ekonomski učinkovitosti vedenjskega oglaševanja za različne deležnike, vendar pa velja opozorilo, da študija ni vključevala metod ekonomskih analiz in vsi podatki o učinkovitosti izhajajo iz pregleda literature ter subjektivnih pogledov ekspertov na tem področju. Na tem področju so tako potrebne nadaljnje raziskave, ki bi zagotovile zanesljivejši vpogled v ekonomsko plat vedenjskega oglaševanja in njegovo učinkovitost v različnih kontekstih, in sicer v primerjavi z digitalnim oglaševanjem, ki ne gradi tako široko na analizi podatkov posameznikov in nima tako znatnih negativnih posledic.

Kot je bilo že večkrat poudarjeno je študija usmerjena predvsem na vidike posega v zasebnosti in varstvo osebnih podatkov ter okvir regulacije na tem področju, čeprav se vpliv vedenjskega oglaševanja razteza tudi na druge pravice in interese ter demokratične procese. Okvir pričujoče študije ne dopušča podrobnejše analize vseh teh področij, zato je analiza usmerjena na obdelavo osebnih podatkov posameznikov, ki je temeljni proces vedenjskega oglaševanja za vse najrazličnejše namene. Tudi večina intervencij nadzornih organov je bila do sedaj oprta le na to pravno področje. Disertacija le mestoma omenja relevantne pomisleke tudi z vidika širših posledic. Iz tega izhaja, da si tematika vsekakor zasluži podrobnejšo znanstveno obravnavo tudi z vidika drugih pravic posameznikov, kot so pravica do enake obravnave in nediskriminacije, pravica do obveščenosti in pravica do svobodnih volitev, ter tudi z vidika posega v demokratične procese, medijski pluralizem ter konkurenco na trgu ponudnikov sodobnih elektronskih storitev.

Na področju okvira regulacije za varstvo osebnih podatkov je v zadnjih letih prišlo do številnih sprememb, predvsem v EU, s sprejemom Uredbe 2016/679, ki uvaja številne nove pojme, kot je promocija certificiranja, in samoregulacijske kodekse, pa orodja za večjo odgovornost upravljavcev, kot so ocene vplivov na zasebnost in koncept vgrajene zasebnosti ter nove pravice posameznikov, npr. do pozabe in prenosljivosti osebnih podatkov. Vsaka od teh novosti ima lahko v prihodnosti na področju vedenjskega oglaševanja pomembno vlogo,

vendar jih v okviru te disertacije ni bilo mogoče temeljiteje raziskati. Nadaljnje raziskave na teh področjih so pomembne tudi za prihodnji razvoj zakonodaje v drugih državah, ki jim zakonodajni okvir EU lahko služi kot zgled. Učenje iz dobrih in slabih izkušenj uvedbe teh orodij bi lahko pomembno pripomoglo k boljši ureditvi področja varovanja zasebnosti pri digitalnem oglaševanju.

Zadnja omejitev izhaja iz izbrane metode ekspertnih intervjujev v povezavi s položajem raziskovalke, ki prihajam iz organa za varstvo osebnih podatkov z dolgoletnimi izkušnjami na tem področju. Gradivo, pridobljeno z ekspertnimi intervjuji, nujno vključuje veliko subjektivnih informacij, prav tako je s subjektivnostjo prežeta analiza takih podatkov. Intervjuji so bili primarno uporabljeni za odgovor na vprašanje prihodnje regulacije vedenjskega oglaševanja, ki je nerešeno, tudi politično vprašanje, zato subjektivnost pri odgovorih študijo pravzaprav bogati. Pogovori s strokovnjaki namreč odstrejo marsikatero tančico, ki je dokumentarna analiza ne bi mogla, saj so objavljeni dokumenti pogosto očiščeni spornejših izjav in pisani v diplomatskem tonu, iz katerega je lahko težko razbrati nianse. Kljub temu pa strokovnost raziskovalca, podprta z obsežno in globoko analizo dokumentarnih virov, relevantne zakonodaje in študijami primerov, omogoča, da analiza subjektivnih pogledov na prihodnjo regulacijo pridobi veljavnost in objektivnost.

8.3 Prispevki za prakso

Disertacija v smislu prispevka za prakso ponuja uvide v trenutno stanje in delovanje okvira regulacije vedenjskega oglaševanja ter v posledice za prihodnjo regulacijo, kar je lahko neposredno uporabljivo v okviru pogajanj o nastajajoči ePR in pozneje, na ravni razlag zahtev uredbe, tudi na nacionalni ravni. Enako velja za določbe Uredbe 2016/679 glede vedenjskega oglaševanja. Disertacija ne zagotavlja le pojasnil glede pravnega okvira in razlag, ampak bogato raziskavo vedenjskega oglaševanja v različnih kontekstih, ki jo lahko uporabijo in se z njo informirajo vsi relevantni deležniki na ravni zakonodajalca, nadzornih organov in samoregulacijskih organov pri razvoju regulatornih rešitev in politik urejanja vedenjskega oglaševanja in tudi v praksi pri izvajanju nadzora. Neposreden prispevek za prakso je tudi model operacionalizacije tehtanja zakonitega interesa za področje vedenjskega oglaševanja, ki ga lahko uporabijo upravljavci, izvajalci vedenjskega oglaševanja in tudi nadzorni organi za varstvo osebnih podatkov oziroma pristojni organi, ki razvijajo politike na tem področju.

9 VIRI

1. 20/80 THINKING (2008). *Privacy Impact Assessment*. Dostopno prek http://www.phorm.com/assets/reports/Phorm_PIA_Final.pdf
2. Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM Conference on electronic commerce*, 21–29. EC'04. New York: ACM.
3. Acquisti, A. in Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security Privacy, 3*(1), 26–33.
4. Acquisti, A. (2014). From the Economics of Privacy to the Economics of Big Data. V S. Bender, J. Lane, H. Nissenbaum in V. Stodden (ur.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (str. 76–95). New York: Cambridge University press.
5. Adams, T. (2018, 24. marec). Facebook's week of shame: the Cambridge Analytica fallout. *The Guardian*. Dostopno prek https://www.theguardian.com/technology/2018/mar/24/facebook-week-of-shame-data-breach-observer-revelations-zuckerberg-silence
6. Adblockplus (2019). *About AdblockPlus*. Dostopno preko: https://adblockplus.org/en/about
7. Adorno, T. in Horkheimer M. (1944). *The Culture Industry: Enlightenment as Mass Deception*. Dostopno prek http://www.marxists.org/reference/archive/adorno/1944/culture-industry.htm
8. Ahmad, I. (2019, 2. april). Global Ad Blocking Behavior 2019 [Infographic]. *Social Media Today*. Dostopno prek https://www.socialmediatoday.com/news/global-ad-blocking-behavior-2019-infographic/551716/
9. Aitken, R. (2017). 'All data is credit data': Constituting the unbanked. *Competition and Change 21*(4), 274–300.
10. Aksu, H., Babun, L., Conti, M., Tolomei, G. in Uluagac, A. S. (2018). Advertising in the IoT Era: Vision and Challenges. *IEEE Communications Magazine 56*(11), 138–144. Dostopno prek https://arxiv.org/abs/1802.04102
11. Amaeshi, K. M., Osuji O. K. in Nnodim P. (2008). Corporate Social Responsibility in Supply Chains of Global Brands: A Boundaryless Responsibility? Clarifications, Exceptions and Implications. *Journal of Business Ethics 81*(1), 223–234.

12. American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, Council of Better Business Bureaus (2010). *Self-Regulatory Principles for Online Behavioral Advertising*. Dostopno prek http://www.iab.net/media/file/ven-principles-07-01-09.pdf
13. Amon Prodnik, J. (2013). *Politična ekonomija komuniciranja in strukturne transformacije kapitalizma* (doktorska disertacija). Univerza v Ljubljani, Fakulteta za družbene vede. Dostopno prek http://dk.fdv.uni-lj.si/doktorska_dela/pdfs/dr_amon-prodnik-jernej.PDF
14. Anton, A. I., Earp, J. B. in Young, J. D. (2009). *How Internet users' privacy concerns have evolved since 2002*. Tech. Rep. Computer Science Technical Report TR-2009-16, North Carolina State. Dostopno prek http://theprivacyplace.org/blog/wp-content/uploads/2009/07/tr_2009_16.pdf
15. Anton, A., Earp, J., He, Q., Stufflebeam, W., Bolchini, D. in Jensen, C. (2004). Financial privacy policies and the need for standardization. *IEEE Security & Privacy 2*(2), 36–45.
16. AT Kearney (2010). *A Viable Future Model for the Internet*. Dostopno prek http://www.atkearney.com/images/global/pdf/Viable_Future_Model_for_Internet.pdf
17. Autoriteit Persoonsgegevens (2017). *Conclusions*. Dostopno prek https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_facebook_february_23_2017.pdf
18. Autoriteit Persoonsgegevens (2018). *Facebook changes policy after investigation by Dutch Data Protection Authority*. Dostopno prek https://autoriteitpersoonsgegevens.nl/en/news/facebook-changes-policy-after-investigation-dutch-data-protection-authority
19. Bagdikian, B. H. (2004). *The New Media Monopoly*. 7th ed. Boston: Beacon Press.
20. Baker, J. (2012). *European Watchdog Pushes for Do Not Track Protocol*. Dostopno prek http://www.pcworld.com/article/251373/european_watchdog_pushes_for_do_not_track_protocol.html
21. Baldwin, R. in Cave M. (1999). *Understanding Regulation. Theory, Strategy, and Practice*. New York: Oxford University Press.
22. Battelle, J. (2010). *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*. London: Penguin Books.

23. Baym, N. K. (2011). Social Networks 2.0. V M. Consalvo in C. Ess (ur.), *The Handbook of Internet Studies* (str. 384–405). Chichester: Blackwell Publishing Ltd.
24. Bauer, T. (2014). The reponsibilities of social networking companies. Applying political CSR theoriy to google, Faebook and Twitter. V R. Tench, W. Sun in B. Jones (ur.), *Communicating Corporate Social Responsibility*: Perspectives and Practice (str. 259–282). Bingley: Emerald Group Publishing Limited.
25. BBC (2018, 25. oktober). Facebook fined £500,000 for Cambridge Analytica scandal. *BBC*. Dostopno prek https://www.bbc.com/news/technology-45976300
26. Beales, H. (2010). *The Value of Behavioural Targeting. Network Advertising Initiative*. Dostopno prek http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf
27. Ben L. (2010). Ethics and social networking sites: A disclosive analysis of Facebook. *Information Technology & People*. Dostopno prek https://www.researchgate.net/publication/220437071
28. Benkler, Y. (2001). The battle over the institutional ecosystem in the digital evironment. *Communications of the ACM 44*(2), 84–90.
29. Benkler, Y. (2003). Freedom in the commons: Towards a political economy of information. *Duke Law Journal 52*, 1245–1276.
30. Benkler, Y. (2006). *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press.
31. Benkler, Y. (2011). Networks of Power; Degrees and Freedom. *International Journal of Communication 5*, 721–755.
32. Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press.
33. Bennett, C. in Mulligan, D. K. (2012). *The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy*. Dostopno prek https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2230369
34. Bennett, W. L. (2003). Communicating Global Activism. *Information, Communication & Society 6*(2), 143–168.
35. Berger, A. A. (1998). *Media Research Techniques*. Thousand Oaks, London, New Delhi: Sage Publications.
36. Bettig, R. V. (1997). The enclosure of cyberspace. *Critical Studies in Mass Communication 14*(2), 138–157.

37. Bies, R., Bartunek, J., L. Fort, T. in Mayer, N. Z. (2007). Corporations as Social Change Agents: Individual, Interpersonal, Institutional, and Environmental Dynamics. *Academy of Management Review 32*(3), 788–793.
38. Boerman, S. C., Kruikemeier, S. in Zuiderveen Borgesius, F. J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising 46*(3), 363–376.
39. Bohm, N. (2008). *The Phorm "Webwise" System – A Legal Analysis*. Dostopno prek http://www.fipr.org/080423phormlegal.pdf
40. Boucher Ferguson, R. (2008). *A Battle Is Brewing Over Online Behavioral Advertising*. Dostopno prek: http://www.eweek.com/c/a/Enterprise-Apps/A-Battle-Is-Brewing-Over-Online-Behavioral-Advertising-Market/
41. Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal 9*(2), 27–40.
42. Brinkhof Advokaten (2018). *EPR vis-à-vis GDPR A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation*. Dostopno prek https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-brinkhof_epr_study.pdf
43. Brodkin, J. (2015, 11. junij). Websites can keep ignoring "Do Not Track" requests after FCC ruling. *Ars Technica*. Dostopno prek http://arstechnica.com/business/2015/11/fcc-wont-force-websites-to-honor-do-not-track-requests/
44. Brookman, J. (2014, 24. april). *At Last, Some Progress on Do Not Track* [blog]. Dostopno prek https://cdt.org/blog/at-last-some-progress-on-do-not-track/
45. Brookman, J. (2015, 28. maj). Privacy Harm Is In the Eye of Beholder. *IAPP*. Dostopno prek https://iapp.org/news/a/privacy-harm-is-in-the-eye-of-beholder/
46. Brunton, F. in Nissenbaum, H. (2016). *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge (Massacusets), London: The MIT Press.
47. Burke, D. (2003). *Your TV is watching you*. Dostopno prek http://www.opendemocracy.net/media-digitaltv/article_1019.jsp
48. Burnik, J. (2008). *Tabloidization of online news providers* (magistrska naloga). University of London, London School of Economics, London.
49. Burnik, J. (2011a). Behavioural advertising in electronic communications. V A. Cerrillo-i-Martínez, M. Peguera, I. Peña-López in M. Vilasau Solana (ur.), *Net*

Neutrality and other challenges for the future of the Internet. Proceedings of the 7th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 11.–12. julij 2011. Barcelona: UOC-Huygens.

50. Burnik, J. (2011b). Prihodnost varstva osebnih podakov v Evropski uniji. *Pravna praksa 30*(3), 18–19.
51. Burnik, J. (2012a). Information Society Services and Mandatory Data Breach Notifications: Introduction to Open Issues in the EU Framework. *Journal of Intellectual Property, Information Technology and E-Commerce Law 3*, 126–137.
52. Burnik, J. (2012b). *Ali naj mi bo žal, da nimam nobene Facebook delnice*? Dostopno prek https://metinalista.si/ali-naj-mi-bo-zal-da-nimam-nobene-facebook-delnice/
53. Burnik, J. (2012c). Facebook v evropskem okviru varstva osebnih podatkov. *Pravna praksa 2012*(3), 6–8.
54. Burnik, J. (2013). Vedenjsko oglaševanje v elektronskem komuniciranju: okvir za raziskovanje. *Akademija MM. Volume XIII* (21), 65–79.
55. Burnik, J. (2016a). Kaj Sloveniji prinaša nova uredba o varstvu osebnih podatkov. V *Zbornik 2016 / 2. dnevi prava zasebnosti in svobode izražanja*, Kranjska Gora, 7. in 8. april 2016, Ljubljana: IUS Software, GV Založba, str. 7–13.
56. Burnik, J. in Tomšič, A. (2011). DPI – Pandorina skrinjica interneta. *Pravna praksa 30*(13), 19–21.
57. Burnik, J. in drugi (2016b). The teacher's manual. V G. Furster Gonzales in D. Kloza (ur.), *The European Handbook for Teaching Privacy and Data Protection at Schools* (str. 41–77). Bruselj: EAP.
58. Busch, O. (2016). *Programmatic Advertising: The Successful Transformation to Automated, Data-Driven Marketing in Real-Time*. Switzerland: Springer Internetional Publishing.
59. Cadwalladr, C. (2017, 26. februar). Robert Mercer: The big data billionaire waging war on mainstream media. *The Guardian*. Dostopno prek https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage
60. Cambell, F. B. Jr. (2014, 27. december). The Slow Death of 'Do Not Track'. *The New York Times*. Dostopno prek http://www.nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html?_r=0

61. Carsten Stahl, B. (2008). Ethical Issues of Information and Business. V K. Einar Himma in H. T. Tavani (ur.), *The Handbook of Information and Computer Ethics* (str. 311–336). New York: Wiley and Sons, inc.
62. Carsten Stahl, B. (2011). IT for a Better Future. How to integrate ethics, politics and innovation. V R. von Schomberg (ur.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (str. 18–33). Luxembourg: Publications Office of the European Union.
63. Castells, M. (2001). *The Internet Galaxy: Reflections on the Internet, Business, and Society.* New York: Oxford University Press.
64. Castelluccia, C. (2012). Behavioural Tracking on the Internet: A Technical Perspective. V S. Gutwirth, R. Leenes, P. De Hert in Y. Poullet (ur.), *European Data Protection: In Good Health?* (str. 21–33). Dordrecht, Heidelberg, London, New York: Springer.
65. Castelluccia, C. in Narayanan, A. (2012). Privacy considerations of online behavioural tracking. *ENISA report*. Dostopno prek https://www.enisa.europa.eu/publications/privacy-considerations-of-online-behavioural-tracking
66. Cavoukian, A. (2008). *Privacy and radical pragmatism*. Change the Paradigm. Ontario: Information and Privacy Commissioner of Ontario.
67. Centre for Digital Technology (2012, 3. oktober). *The Bizarre, Belated Assault on Do Not Track* [blog]. Dostopno prek https://cdt.org/blog/the-bizarre-belated-assault-on-do-not-track/
68. Chen, J. in Stallaert, J. (2014). An Economic Analysis of Online Advertising Using Behavioral Targeting. *MIS Quarterly 38*, 429–449.
69. Chen, S. (2009). Corporate Responsibilities in Internet-Enabled Social Networks. *Journal of Business Ethics 90*, 523–536.
70. Cheney-Lippold (2017). *We are data. Algorithms and the Making of Our Digital Selves*. New York: New Your University Press.
71. CIPL Centre for Information Policy Leadership (2017). *GDPR Implementation Project. Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR*. Dostopno prek https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommend

ations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf

72. Clayton, R. (2008). *The Phorm "Webwise" System*. Dostopno prek http://www.cl.cam.ac.uk/~rnc1/080404phorm.pdf.
73. CNIL (2018). *Algorithms and artificial intelligence: CNIL's report on the ethical issues.* Dostopno prek https://www.cnil.fr/en/algorithms-and-artificial-intelligence-cnils-report-ethical-issues
74. COE Council of Europe. (2017). *Study on the use of internet in electoral campaigns, prepared by the committee of experts on media pluralism and transparency of media ownership* (MSI-MED). Dostopno prek https://rm.coe.int/use-of-internet-in-electoral-campaigns-/16807c0e24
75. Confessore, N. (2018, 14. avgust). The Unlikely Activists Who Took On Silicon Valley – and Won. *The New York Times*. Dostopno prek https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html?rref=collection%2Fbyline%2Fnicholas-confessore&action=click&contentCollection=undefined&region=stream&module=stream_unit&version=latest&contentPlacement=10&pgtype=collection
76. Cooper, A. (2010). *The Singular Challenges of ISP Use of Deep Packet Inspection.* Dostopno prek http://www.deeppacketinspection.ca/the-singular-challenges-of-isp-use-of-deep-packet-inspection/
77. Couldry, N. (2009). Does 'the Media' Have a Future? *European Journal of Communication. 24*(4), 437–449.
78. Council of the EU (2019). *Interinstitutional File: 2017/0003(COD)*. Dostopno prek https://data.consilium.europa.eu/doc/document/ST-11291-2019-INIT/en/pdf
79. Crain, M. (2016). *The limits of transparency: Data brokers and commodification*. New Media & Society 20(3).
80. Cunningham, M. (2015). *Complying with international data protection law*. Dostopno prek SSRN: https://ssrn.com/abstract=2706738
81. Dahlgren, P. (2005). The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation. *Political Communication 22*(2), 147–162.
82. Daryl Slack, J. in Macgregor Wise, J. (2006). *Culture + Technology: A Primer*. New York: Peter Lang.

83. Data Protection Authority (2018). *The Belgian Authority publishes new recommendation relating to the processing of personal data by Facebook through cookies, social plug-ins and pixels.* Dostopno prek https://www.dataprotectionauthority.be/news/belgian-privacy-commission-publishes-new-recommendation-relating-processing-personal-data
84. Datatilsynet (2015). *The Great Data Race. How Commercial Utilisation of Personal Data Challenges Privacy*. Report, november 2015. Dostopno prek https://www.datatilsynet.no/globalassets/global/english/engelsk-kommersialisering-endelig.pdf
85. Davies, H. (2015a, 11. december). Ted Cruz using firm that harvested data on millions of unwitting Facebook users. *The Guardian*. Dostopno prek https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data
86. Davies, W. (2015b). *World Wide Web Consortium Unveils Do-Not-Track Standards*. Dostopno prek http://www.mediapost.com/publications/article/253995/world-wide-web-consortium-unveils-do-not-track-sta.html
87. Demos (2018). *The Future of Political Campaigning*. Dostopno prek https://demosuk.wpengine.com/wp-content/uploads/2018/07/The-Future-of-Political-Campaigning.pdf
88. Department of Commerce (2010a). *Notice of Inquiry. Information Privacy and Innovation in the Internet Economy*. Federal Register / Vol. 75, No. 78 / Friday, April 23. Dostopno prek http://www.ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf
89. Department of Commerce, Internet Policy Task Force (2010b). *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework.* Dostopno prek http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.
90. Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. Dostopno prek https://eur-lex.europa.eu/legal-content/sl/TXT/?uri=CELEX%3A31995L0046.
91. Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih

komunikacij. Dostopno prek https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32002L0058&from=EN.

92. Direktiva Evropskega parlamenta in Sveta 2005/29/ES z dne 11. maja 2005 o nepoštenih poslovnih praksah podjetij v razmerju do potrošnikov na notranjem trgu ter o spremembi Direktive Sveta 84/450/EGS, direktiv Evropskega parlamenta in Sveta 97/7/ES, 98/27/ES in 2002/65/ES ter Uredbe (ES) št. 2006/2004 Evropskega parlamenta in Sveta. Dostopno prek https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex%3A32005L0029.
93. Direktiva 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov. Dostopno prek https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32009L0136
94. Direktiva 2010/13/EU Evropskega parlamenta in Sveta z dne 10. marca 2010 o usklajevanju nekaterih zakonov in drugih predpisov držav članic o opravljanju avdiovizualnih medijskih storitev. Dostopno prek https://eur-lex.europa.eu/legal-content/sl/TXT/?uri=CELEX:32010L0013
95. EACA European Association of Communications Agencies (2010). *Europe's data privacy regulators' latest opinion on cookies is out of step with online businesses and their consumers.* Dostopno prek http://www.eaca.be/news/pressdetail.asp?release=253.
96. Earp, J., Anton, A., Aiman-Smith, L. in Stufflebeam, W. (2005, maj). *Examining internet privacy policies within the context of user privacy values*. Engineering Management, IEEE Transactions on 52(2), 227–237.
97. EASA European Advertising Standards Alliance (2011). *Best Practice Recommendation for Online Behavioural Advertising*. Dostopno prek http://www.easa-alliance.org/News/News/page.aspx/46?xf_itemId=131&xf_selectionDatapartId=91
98. EASA European Advertising Standards Alliance (2016). *EASA Best Practice Recommendation onOnline Behavioural Advertising*. Dostopno prek

https://www.edaa.eu/wp-content/uploads/2012/10/EASA-Best-Practice-Recommendation-on-Online-Behavioural-Advertising_1.pdf.

99. EASA European Advertising Standards Alliance (2018). *Online Behavioural Advertising*. Dostopno prek https://www.easa-alliance.org/issues/oba
100. Eckersley, P. (2011). *What Does the "Track" in "Do Not Track" Mean?* Dostopno prek https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean
101. Economist (2018, 22. maj). What Zuckerberg should do. Facebook faces a reputational meltdown. *The Economist*. Dostopno prek https://www.economist.com/leaders/2018/03/22/facebook-faces-a-reputational-meltdown
102. EDPB Evropski odbor za varstvo podatkov (2018). *Statement of the EDPB on the revision of the ePrivacyRegulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications*. Dostopno prek https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf
103. EDPB Evropski odbor za varstvo podatkov (2019). *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*. Dostopno prek https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_en
104. EDPS European Data Protection Supervisor (2016). *Opinion 3/2018 EDPS Opinion on online manipulation and personal data*. Dostopno prek https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
105. Egelman, S., Tsai, J., Faith Cranor, L. in Acquisti, A. (2009). *Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators*. Dostopno prek https://www.researchgate.net/publication/221518894_Timing_Is_everything_The_effects_of_timing_and_placement_of_online_privacy_indicators
106. Eisner, E. W. (1991). *The Enlightened Eye: Qualitative Inquiry and the Enhancement of Educational Practice*. New York, London: Techers College Press.
107. Electronic Frontier Foundation (2010). *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Preliminary Staff Report), Response of the Electronic Frontier Foundation. Dostopno prek https://www.eff.org/files/ftccommentseff.pdf

108. Electronic Frontier Foundation (2016). *Do not track*. Dostopno prek https://www.eff.org/issues/do-not-track
109. eMarketer (2017, 21. september). Google and Facebook Tighten Grip on US Digital Ad Market. *eMarketer*. Dostopno prek https://www.emarketer.com/Article/Google-Facebook-Tighten-Grip-on-US-Digital-Ad-Market/1016494
110. Englehardt, S. in Narayanan, A. (2016). *Online Tracking: A 1-million-site Measurement and Analysis.* Dostopno prek http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf
111. European Privacy Seal. (2010). *Position paper on the impact of the new "Cookie Law" on certifiability of behavioural advertising systems according to EuroPriSe*. Dostopno prek https://www.european-privacy-seal.eu/results/Position-Papers/PDF%20-%20EuroPriSe%20position%20paper%20on%20the%20new%20cookie%20law.pdf
112. ENISA European Union Agency For Network and Information Security (2017). *Recommendations on European Data Protection Certification* (contributing authors: Jelena Burnik and Irene Kamara). Dostopno prek https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification
113. Evans, D. S. (2009). *The Online Advertising Industry: Economics, Evolution, and Privacy*. Dostopno prek http://www.intertic.org/Policy%20Papers/EvansEOAI.pdf
114. Evropska komisija (2009a). *Telecoms: Commission launches case against UK over privacy and personal data protection.* Dostopno prek http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=EN&guiLanguage=en
115. Evropska komisija (2009b). *Telecoms: Commission steps up UK legal action over privacy and personal data protection.* Dostopno prek http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1626
116. Evropska komisija (2010). *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions "A Comprehensive Approach on Data Protection in the European Union".* Dostopno prek http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

117. Evropska Komisija (2015). *Special Eurobarometer 431. Data Protection Report*. Dostopno preko https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf
118. Evropska komisija (2017). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector. FINAL REPORT A study prepared for the European Commission DG Communications Networks, Content & Technology by Dellotite*. Dostopno prek https://ec.europa.eu/digital-single-market/en/news/evaluation-and-review-directive-200258-privacy-and-electronic-communication-sector
119. Evropska komisija (2018a). *Behavioural study on advertising and marketing practices in social media*. Dostopno prek https://ec.europa.eu/info/publications/behavioural-study-advertising-and-marketing-practices-social-media-0_en
120. Evropska komisija (2018b). *Free and Fair elections. Guidance Document. Commission guidance on the application of Union data protection law in the electoral context A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018*. Dostopno prek https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf
121. Evropska komisija (2018c). *Fair Taxation of the Digital Economy*. Dostopno prek https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en
122. Evropski parlament (2017). *Poročilo o predlogu uredbe Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD))*, Odbor za državljanske svoboščine, pravosodje in notranje zadeve, 20. oktober, dostopno prek http://www.europarl.europa.eu/doceo/document/A-8-2017-0324_SL.html?redirect
123. Facebook (2018). *Suspending Cambridge Analytica and SCL Group From Facebook*. Dsotopno prek https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/

124. Fair, L. (2017, 6. februar). *What Vizio was doing behind the TV screen* [blog]. Dostopno prek https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen
125. Fashion ID GmbH & Co. KG vs. Verbraucherzentrale NRW eV. (2019). *C-40/17. SEU*, 29. julij. Dostopno prek http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=sl&mode=lst&dir=&occ=first&part=1&cid=6110368
126. Fazlioglu, M. (2018). *The top five contested issues in the EU's developing ePrivacy Regulation*. Dostopno prek https://iapp.org/news/a/the-top-5-contested-issues-in-the-eus-developing-eprivacy-regulation/
127. Federation of German Consumer Organisations (2018). *Facebook in Breach of German Data Protection Law*. Dostopno prek https://www.vzbv.de/sites/default/files/downloads/2018/02/14/18-02-12_vzbv_pm_facebook-urteil_en.pdf
128. FEDMA Federation Oof European Direct And Interactive Marketing (2010). *European Code Of Practice For The Use Of Personal Data In Direct Marketing Electronic Communications Annex.* Dostopno prek https://www.eesc.europa.eu/sites/default/files/resources/docs/57-markt-2003-fedma-personal-data-in-direct-marketing.pdf
129. Feintuck, M. (2004). *»The Public Interest« In Regulation*. Oxford: Oxford University Press.
130. Fernback, J. in Papacharissi, Z. (2007). Online Privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies. *New media and society 9*(5), 715–734.
131. FIPR Foundation for Information Policy Research (2008). *Open Letter to the Information Commissioner*. Dostopno prek http://www.fipr.org/080317icoletter.html
132. Fischer, L. (2018). *US Programmatic Ad Spending Forecast Update 2018*. Dostopno prek https://www.emarketer.com/content/us-programmatic-ad-spending-forecast-update-2018
133. Fiske, J. (1987). *Television Culture*. London: Methuen.
134. Floridi, L. (1999). Information Ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology 1*, 37–56.

135. Floridi, L. (2006). Four challenges for a theory of informational privacy. *Ethics and Information Technology 8*, 109–119.
136. Fontana, J. (2012). *W3C moves Do Not Track to showdown phase*. Dostopno prek https://www.zdnet.com/article/w3c-moves-do-not-track-to-showdown-phase/
137. Fouad, Y. (2015). *Monitoring of digital television consumption infringes Dutch data protection law*. Dostopno prek http://merlin.obs.coe.int/iris/2015/7/article25.en.html
138. Freudiger, J., Vratonjic, N. in Hubaux, J. P. (2009). *Towards Privacy-Friendly Online Advertising*. Dostopno prek http://w2spconf.com/2009/papers/s2p1.pdf
139. Frynas, J. G. in Stephens, S. (2015). Political CSR: Reviewing Theories. *International Journal of Management Reviews 17*, 483–509.
140. FTC Federal Trade Commission (2007). *FTC Staff Proposes Online Behavioral Advertising Privacy Principles*. Dostopno prek http://www.ftc.gov/opa/2007/12/principles.shtm
141. FTC Federal Trade Commission (2010). *Protecting Consumer Privacy in an Era of Rapid Change, A proposed framework for Business and Policymakers*, Preliminary FTC Staff Report. Dostopno prek http://www.ftc.gov/os/2010/12/101201privacyreport.pdf
142. FTC Federal Trade Commission (2011). *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*. Dostopno prek https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep
143. FTC Federal Trade Commission (2012). *Tracking Software Company Settles FTC Charges That it Deceived Consumers and Failed to Safeguard Sensitive Data it Collected*. Dostopno prek https://www.ftc.gov/news-events/press-releases/2012/10/tracking-software-company-settles-ftc-charges-it-deceived
144. FTC Federal Trade Commission (2013). *Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns In the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search. Landmark Agreements Will Give Competitors Access to Standard-Essential Patents;Advertisers Will Get More Flexibility to Use Rival Search Engines*. Dostopno prek https://www.ftc.gov/news-events/press-releases/2013/01/google-agrees-change-its-business-practices-resolve-ftc
145. FTC Federal Trade Commission (2014). *Data Brokers. A Call for Transparency and Accountability*. Dostopno prek

https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

146. FTC Federal Trade Commission (2015). *Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices. Company Falsely Promised an In-Store Opt Out, Agency Alleges*. Dostopno prek https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers
147. FTC Federal Trade Commission (2016a). *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission. Company Will Pay $950,000 For Tracking Children Without Parental Consent*. Dostopno prek: https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked
148. FTC Federal Trade Commission (2016b). *Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices. Settlement ensures consumers can control targeted ads*. Dostopno prek https://www.ftc.gov/news-events/press-releases/2016/12/digital-advertising-company-settles-ftc-charges-it-deceptively
149. FTC Federal Trade Commission (2017). *Cross Device Tracking. An FTC staff report*. Dostopno prek https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf
150. Galperin, H. (2004). *New Television, Old Politics. The Transition to Digital Television in the United States and Britain*. New York: Cambridge University Press.
151. Glaser, M. (2018). *In search of a Goldilocks solution to online privacy*. Dostopno prek https://digitalcontentnext.org/blog/2018/10/04/in-search-of-a-goldilocks-solution-to-online-privacy/
152. Goldfarb, A. in Tucker, C. (2010). Online Display Advertising: Targeting and obtrusiveness. *Marketing Science 30*, 413–415.
153. Goldsmith, J. L. in Wu, T. (2006). *Who Controls the Internet*. Oxford, New York: Oxford University Press.
154. Golyardi, S., Hortensius, D., Lau Y.Y., Burnik, J. in drugi (2017). *Final Consolidated Exploitation Plan: Deliverable 7.4 for the CRISP project*. CRISP

project. Dostopno prek http://crispproject.eu/wp-content/uploads/2017/07/CRISP_D7.1_Consolidated-WP7-report.pdf.

155. Goodman, E., Labo, S., Moore, M. in Tambini, D. (2017). *The new political campaigning. Media Policy Brief 19*. London: Media Policy Project, London School of Economics and Political Science.
156. Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos (2014). C-131/12, Sodišče Evropske unije, 13. maj. Dostopno prek http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=SL
157. Google (2018). *Framework for Responsible Data Protection Regulation*. Dostopno prek https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf
158. Gorton, W. (2016). Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy. *New Political Science 38*(1), 61–80.
159. GPA Global Privacy Alliance (2010). *Comments of the Global Privacy Alliance on Cookies and Web Beacons.* Dostopno prek http://www.ip-rs.si/fileadmin/user_upload/Pdf/novice/GPA_Comments_on_Cookies_and_Web_Beacons.pdf
160. Grant, J. (2006). OFCOM buys into product placement: consultation on issues related to product placement. *Entertainment Law Review 17*(4), 118–121.
161. Ha, L. in McCann, K. (2008). An integrated model of advertising clutter in offline and online media. *International Journal of Advertising 27*(4), 569–592
162. Habermas, J. (1974). *The public sphere: an encyclopaedia article*. New German Critique 1(3), 49–55.
163. Hall, S. (1974). The television discourse; encoding and decoding. *Education and Culture (Council of Europe) 25*, 8–15.
164. Hall, S. (1974). Media Power: The Double Bind. *Journal of Communication 24*(4), 19–26.
165. Hepp, A. (2010). Researching 'mediatized worlds': Non-media-centric media and communication research as a challenge. V: N. Carpentier, I. T. Trivundza, P. Pruulmann-Vengerfeldt, B. Cammaerts, R. Kilborn, H. Nieminen, T. Olsson in E. Sundin (ur.), *Media and Communication Studies Intersections and Interventions* (str. 37–48). Tartu: University of Tartu Press.

166. Herman, E. S. in Chomsky, N. (1994). *Manufacturing Consent: The Political Economy of the Mass Media*. London: The Random House.
167. Hinduja in Patchin (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of adolescence 31*(1), 125–46.
168. Home Office (2008). *Home Office notice*. Dostopno prek http://cryptome.org/ho-phorm.htm
169. IAB (2017). *IAB Europe position paper: Position on the proposal for an ePrivacy Regulation.* Dostopno prek https://iabeurope.eu/iab-europe-position-paper-position-on-the-proposal-for-an-eprivacy-regulation/
170. IAB Europe Interactive Advertising Bureau Europe (2010a). *Industry unites to reject privacy opinion*. Dostopno prek http://www.iabuk.net/en/1/europeanmediaindustryunitesagainstarticle29opinion.mxs
171. IAB Europe Interactive Advertising Bureau Europe (2010b). *Consumers driving the digital uptake. The economic value of online advertising-based services for consumers*. Dostopno prek http://iabeurope.eu/media/39559/whitepaper%20_consumerdrivingdigitaluptake_final.pdf
172. IAB Europe (2014). *Programmatic Trading. An IAB Europe White Paper*. Dostopno prek https://www.iabeurope.eu/research-thought-leadership/iab-europe-programmatic-trading-white-paper/
173. ICO Information Commissioner's Office (2008). *Phorm – Webwise and Open Internet Exchange*. Dostopno prek http://www.ico.gov.uk/
174. ICO Information Commissioner's Office (2012). *Guidance on the rules on use of cookies and similar technologies*. Dostopno prek http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies
175. ICO Information Commissioner's Office (2016). *2016 GPEN Sweep Internet of Things.* Dostopno prek https://ico.org.uk/media/about-the-ico/disclosure-log/1625142/irq0648379-attachment.pdf
176. ICO Information Commissioner's Office (2016). *Big data, artificial intelligence, machine learning and data protection*. Dostopno prek https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

177. ICO Information Commissioner's Office (2016). *2016 GPEN Sweep Internet of Things.* Dotopno prek https://ico.org.uk/media/about-the-ico/disclosure-log/1625142/irq0648379-attachment.pdf
178. ICO Information Commissioner's Office (2018a). *Investigation into theuse of data analyticsin political campaigns.* A report to Parliament. 6 November 2018. Dostopno prek https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf
179. ICO Information Commissioner's Office (2018b). *Democracy disrupted? Personal information and political influence.* Dostopno prek https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf
180. IP Informacijski pooblaščenec RS (2013). *Kdaj lahko uporabimo piškotke? Smernice Informacijskega pooblaščenca*. Dostopno prek https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_uporabi_piskotkov.pdf.
181. IP Informacijski pooblaščenec RS (2017). *Skupno stališče IP in AKOS glede obdelave podatkov o uporabi storitev digitalne televizijes strani operaterjev*. Dostopno prek https://www.ip-rs.si/fileadmin/user_upload/Pdf/novice/Stalisce_glede_obdelave_podatkov_o_uporabi_storitev_digitalne_televizije.pdf
182. IWGDPT International Working Group on Data Protection in Telecommunications (2010). *Working Paper on the Use of Deep Packet Inspection for Marketing Purposes*. Dostopno prek www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf
183. Jančič, Z. (1999). Etično oglaševanje in samoregulativa. *Teorija in praksa 36*(6), 957–975.
184. Janet (2012). *US Consumer Privacy Bill of Rights*. Dostopno prek http://webmedia.company.ja.net/edlabblogs/regulatory-developments/2012/03/14/us-consumer-privacy-bill-of-rights/
185. Jeschke, R. (2011). *EFF Urges Commerce Department to Embrace 'Do Not Track'*. Dostopno prek https://www.eff.org/deeplinks/2011/02/eff-urges-commerce-department-embrace-do-not-track
186. Kafka, P. in Rani M. (2017). *2017 was the year digital ad spending finally beat TV*. Dostopno prek https://www.vox.com/2017/12/4/16733460/2017-digital-ad-spend-advertising-beat-tv

187. Kamara, I. (2017). *Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'*. European Journal of Law And Technology 8(1). Dostopno prek http://ejlt.org/article/view/545/723
188. Kamara, I. in de Hert, P. (2018). Data protection certification in the EU: Possibilities, actors and building blocks in a reformed landscape. V R. Rodrigues in V. Papakonstantinou (ur.), *Privacy and data protection seals*. TMC Asser Press.
189. Kamara, I. in De Hert, P. (2018, 8. avgust). Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. *Brussels Privacy Hub 4*(12), Dostopno prek SSRN: https://ssrn.com/abstract=3228369
190. Kamara, I. in Kosta, E. (2016). Do Not Track initiatives: regaining the lost user control. *International Data Privacy Law 0*(0), 1–15.
191. Kang, H. (2011). Examining the Audience Commodification of Google. *Open Access Journal for a Global Sustainable Information Society 9*(2), 141–153.
192. Katayev, V. (2015, 23. november). *The Future of Ad Targeting In An IoT World*. Forbes. Dostopno prek https://www.forbes.com/sites/onmarketing/2015/11/23/the-future-of-ad-targeting-in-an-iot-world/#4c5694552e7a
193. Kim, N. Y. (2010). Relevance to the rescue: can "smart ads" reduce negative response to online ad clutter? *Journalism & Mass Communication Quarterly 87*(2), 346–362.
194. King, B. in McDonnell, M.-H. (2012, 1. junij). Good Firms, Good Targets: The Relationship between Corporate Social Responsibility, Reputation, and Activist Targeting. V K. Tsutsui in A. Lim (ur.), *Corporate Social Responsibility in a Globalizing World: Toward Effective Global CSR Frameworks* (v tisku). Dostopno prek SSRN: https://ssrn.com/abstract=2079227
195. King, E. (2012). *Surveillance companies: Real responsibility goes beyond the letter of the law*. Dostopno prek https://www.privacyinternational.org/blog/surveillance-companies-real-responsibility-goes-beyond-the-letter-of-the-law
196. Kohnstamm, J. (2012). *Online tracking: to collect or not to collect, that's the question...*. Dostopno prek http://www.cbpweb.nl/downloads_artikelen/art_2012_kohnstamm_online_tracking.pdf

197. Kovačič, M. (2006). *Nadzor in zasebnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.
198. Kroes, N. (2010). *Towards more confidence and more value for European Digital Citizens. Speech at European Roundtable on the Benefits of Online Advertising for Consumers*. Dostopno prek http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/452
199. Kroes, N. (2012). *Why we need a sound Do-Not-Track standard for privacy online*. Dostopno prek http://blogs.ec.europa.eu/neelie-kroes/donottrack/
200. Lessig, L. (2006). *Code version 2.0*. New York: Basic Books.
201. LIBE Committee on Civil Liberties, Justice and Home Affairs (2012). *Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Dostopno prek http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf
202. Lievrouw, L. A. in Livingstone, S. (2006a). Introduction to the Updated Student Edition. V L. A. Lievrouw in S. Livingstone (ur.), *The Handbook of New Media* (str. 1–15). London: SAGE Publications.
203. Lievrouw, L. A. in Livingstone, S. (2006b). Introduction to the First Edition (2002). V L. A. Lievrouw in S. Livingstone (ur.), *The Handbook of New Media* (str. 15–32). London: Sage Publications.
204. Livingstone, S. (2002). The changing social landscape. V L. A. Lievrouw in S. Livingstone (ur.), *Handbook of new media: social shaping and social consequences of ICTs* (str. 17–21). London: Sage.
205. Livingstone, S. (2004a). Media literacy and the challenge of new information and communication technologies. *Communication Review 1*(7), 3–14.
206. Livingstone, S. (2004b). *The challenge of cjhanging audiences: or, what is the researcher to do in the age of the internet?* Dostopno prek http://eprints.lse.ac.uk/412/.
207. Livingstone, S. (2007). On the material and the symbolic: Silverstone's double articulation of research traditions in new media studies. *New Media & Society 9*(1), 16–24.
208. LSE London School of Economics and Political Science (2009a). *From legitimacy to informed consent: Mapping best practices and identifying risks*. London: LSE.

209. LSE London School of Economics and Political Science (2009b). *Online Advertising, Confronting the Challenges*. London: LSE
210. Lueders, M (2013). Why and How Online Sociability Became Part and Parcel of Teenage Life. V M. Consalvo in C. Ess (ur.), *The Handbook of Internet Studies* (str. 452–470). Chichester: Blackwell Publishing Ltd.
211. Luma (2019). *Display LUMAscape*. Dostopno prek: https://lumapartners.com/content/lumascapes/display-ad-tech-lumascape/.
212. Lund, J. (2018, 26. september). Five reasons to be concerned about the Council ePrivacy draft. *EDRi*. Dostopno prek https://edri.org/five-reasons-to-be-concerned-about-the-council-eprivacy-draft/
213. Luthar, B. (2010). Nove kulturne tehnologije, komodifikacija kulture in študije občinstva. *Teorija in Praksa 47*(1), 59–77.
214. Luthar, B. in Oblak Črnič, T. (2015). Medijski repertoarja in diskurzivne skupnosti. *Teorija in Praksa 52*(1-2), 7–30.
215. Mansell, R. (2004). Political economy, power and new media. *New Media & Society 6*(1), 96–105.
216. Martens, B., Aguiar, L., Gomez-Herrera, E. in Mueller-Langer, F. (2018). *The digital Transformation of News Media And the rise of disinformation and fakenews.* Dostopno prek https://ec.europa.eu/jrc/sites/jrcsh/files/jrc111529.pdf
217. Matz, S. C., Kosinski, M., Nave, G. in Stillwell, D. J. (2017). *Psychological targeting as an effective approach to digital mass persuasion*. Proceedings of the National Academy of Sciences of the United States of America 114(48), 12714–12719. Dostopno prek https://www.pnas.org/content/114/48/12714
218. McDonald, A. M. (2011). *User Perceptions of Online Advertising*. Yale ISP Conference, 25.–26. Marec.
219. McDonald, A. M. in Cranor, L. F. (2010). *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*, TPRC 2010. Dostopno prek http://ssrn.com/abstract=1989092
220. McQuail, D. (2002). *McQuail's Reader in Mass Comminication Theory*. London: Sage Publications Ltd.
221. McStay, A. (2011). *The mood of information. A critique of behavioural advertising*. New York, London: The Continuum International Publishing Group.

222. Isaac, M. in Frenkel, S. (2018, 28. september). Facebook Security Breach Exposes Accounts of 50 Million Users. *The New York Times*. Dostopno prek https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html
223. Milne, G. R. in Culnan, M. J. (2004) Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing 18*(3), 54–61.
224. Mocso, V. (1996). *The political economy of communication*: Rethinking and renewal. London; Thousand Oaks: Sage Publications.
225. Moores, T. (2005). Do consumers understand the role of privacy seals in e-commerce? *Communications of the ACM 48*(3), 86–91.
226. Moriarty, K. (2017, 6. februar). *VIZIO Settlement: Smart TVs should not track your shows without your O.K*. Dostopno prek https://www.consumer.ftc.gov/blog/2017/02/vizio-settlement-smart-tvs-should-not-track-your-shows-without-your-ok
227. Mosco, V. (2004). *The Digital Sublime: Myth, Power, and Cyberspace. Cambridge*, London: The MIT Press.
228. Mosco, V. (2009). *The Political Economy of Communication*. Druga izdaja. Los Angeles, London: Sage.
229. Mosco, V. (2016). *To the Cloud: Big Data in a Turbulent World*. New York: Routledge.
230. Murdock, G. in Golding, P. (1997). For a Political Economy of Mass Communications. V P. Golding in G. Murdock (ur.), *The Political Economy of the Media* (str. 3–32). Cheltenham, Brookfield: Edward Elgar.
231. NAI Network Advertising Initiative (2008). *Self-regulatory Code of Conduct for online Behavioral Advertising*. Dostopno prek http://www.networkadvertising.org/networks/principles.asp
232. Näränen, P. (2003). European Regulation of Digital Television: The Opportunity Lost and Found? V G. Ferrel Lowe in T. Hujanen (ur.), *Broadcasting & Convergence: New Articulations of the Public Service Remit* (str. 57–69). Göteborg: NORDICOM.
233. Narayanan, A. in Reisman, D. (2017). *The Princeton Web Transparency and Accountability Project*. Dostopno prek http://randomwalker.info/publications/webtap-chapter.pdf

234. Nerone, J. C. (2002). Social Responsibility Theory. V D. McQuail (ur.), *McQuail's Reader in Mass Communication Theory* (str. 185–192). Thousand Oaks, London, New Delhi: Sage Publications.

235. Nesdale, S. (2018). *Programmatic Advertising: The Successful Transformation to Automated, Data-Driven Marketing in Real-Time, by Oliver Busch*, dostopno prek https://www.marketingfirst.co.nz/2018/09/programmatic-advertising-the-successful-transformation-to-automated-data-driven-marketing-in-real-time-by-oliver-busch/

236. Nissenbaum, H. (2010). *Privacy in Context*. Stanford: Stanford Law Books.

237. Nissenbaum, H. (2015). Respecting Context to Protect Privacy: Why Meaning Matters. *Science and Engineering Ethics 24*(3), 831–852.

238. Nithyanand, R., Khattak, S., Javed, M., Vallina-Rodriguez, N., Falahrastegar, M., Powles, J. E., De Cristofaro, E., Haddadi, H. in Murdoch, S. J. (2016). *Adblocking and Counter Blocking: A Slice of the Arms Race*, Workshop on Free and Open Communications on the Internet 2016, Austin, Texas. Dostopno prek https://www.usenix.org/conference/foci16/workshop-program/presentation/nithyanand

239. Noam, E. M. (2009). *Media Ownership and Concentration an America*. Oxford: University Press.

240. O'Brien, M. in Anderson, M. (2018, 29. september). Facebook says 50M user accounts affected by security breach. *AP News*. Dostopno prek https://apnews.com/65986276c04449ffb3e795ce0eef29d4

241. OFCOM (2008). *Delivering super-fast broadband in the UK, setting the right policy framework.* Dostopno prek http://stakeholders.ofcom.org.uk/consultations/nga_future_broadband/

242. Office of the Privacy Commissioner of Canada (b. d.). *Deep Packet Inspection. A Collection of Essays from Industry Experts*. Dostopno prek http://dpi.priv.gc.ca/index.php/essays/

243. Ohm, P. (2009). *Broken Promises of Privacy: Responding To The Surprising Failure Of Anonymization*. U of Colorado Law Legal Studies Research Paper No. 9-12. Dostopno prek https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

244. Olejnik, L., Minh-Dung T. in Castelluccia, C. (2014). *Selling off User Privacy at Auction*. Dostopno prek https://www.ndss-symposium.org/ndss2014/programme/selling-privacy-auction/

245. O'Neill, M. (2018, 11. junij). *Do Not Track and the GDPR* [blog]. Dostopno prek https://www.w3.org/blog/2018/06/do-not-track-and-the-gdpr/
246. Orion, J. M. (2017). *Online advertising: after monitoring, CNIL sets out applicable regulations*. Dostopno prek https://koan.law/brussels/en/news/online-advertising-after-monitoring-cnil-sets-out-applicable-regulations
247. OUT-LAW (2008). *The law of Phorm*. Dostopno prek http://www.out-law.com/page-9090
248. Packer, J. (2015). *How Many of Your Users Set "Do Not Track"?* Dostopno prek https://www.quantable.com/analytics/how-many-do-not-track/
249. Palladino, M. (2018). *Proposed ePrivacy Regulation to affect all European industries and cost more than €500 billion in reduced annual turnover*. Dostopno prek https://www.developersalliance.org/press-releases/2018/5/7/proposed-eprivacy-regulation-to-affect-all-european-industries-and-cost-more-than-500-billion-in-reduced-annual-turnover
250. Pariser, E. (2011). *The Filter Bubble*. New York: The Penguin Press.
251. Perri 6 (1998). *The future of privacy. Vol. 1, Private Life and Public Policy*. London: Demos.
252. Person, A. (2010). Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May Be Limiting the Online Experience. *Communications Law Journal 62*(2), 435–464.
253. Petrescu, M. in Korgaonkar, P. (2011). Viral Advertising: Definitional Review and Synthesis. *Journal of Internet Commerce 10*(3), 208–226.
254. Pew Research Center (2016). *Privacy and Information Sharing*. Dostopno prek https://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/
255. Pew Research Center (2015). *Americans' Attitudes About Privacy, Security and Surveillance*. Dostopno prek https://www.pewresearch.org/wp-content/uploads/sites/9/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf
256. Picker, R. C. (2009). *Online Advertising, Identity and Privacy*. U of Chicago Law & Economics, Olin Working Paper No. 475. Dostopno prek https://ssrn.com/abstract=1428065
257. Pollach, I. (2011). Online privacy as a corporate social responsibility: an empirical study. *Business Ethics, A European Review 20*(1), 88–102.

258. Pollach, I. (2007). What's wrong with online privacy policies? *Commun. ACM 50*(9), 103–108.
259. Poster, M. (1995). *CyberDemocracy: Internet and the Public Sphere*. Dostopno prek http://www.hnet.uci.edu/mposter/writings/democ.html
260. Predlog 2017/0003 (COD) Uredba evropskega parlamenta in sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah).Dostopno prek https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A52017PC0010
261. Reitman, R. (2011). *Mozilla Leads the Way on Do Not Track*. Dostopno prek http://www.eff.org/deeplinks/2011/01/mozilla-leads-the-way-on-do-not-track
262. Reuters Institute (2018). *Digital News Report*. Dostopno prek http://www.digitalnewsreport.org/survey/2018/overview-key-findings-2018/
263. Robinson, N. in drugi (2009). *Review of the EU Data Protection Directive*. Dostopno prek http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf
264. Roderick, L. (2014). Discipline and Power in the Digital Age: The Case of the US Consumer Data Broker Industry. *Critical Sociology 40*(5), 729–746.
265. Rodrigues, R., Barnard-Wills, D., Wright, D., De Hert, P. in Papakonstantinou, E. (2013). *EU Privacy seals project. Inventory and analysis of privacy certification schemes, Final Report* Study Deliverable 1.4. Dostopno prek https://publications.jrc.ec.europa.eu/repository/bitstream/JRC85092/lb-na-26190-en-n.pdf
266. Rogers, R. (2004). *Information Politics on the Web*. Cambridge (Mass.): The MIT Press.
267. Rose, K. (2015). *W3C Releases Draft Do-Not-Track Compliance Standards*. Dostopno prek http://www.canadiancybersecuritylaw.com/2015/07/w3c-releases-draft-do-not-track-compliance-standards/.
268. Rosenberg, M. in Frenkel, S. (2018, 18. marec). Facebook's Role in Data Misuse Sets Off Storms on Two Continents. *The New York Times*. Dostopno prek https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html?rref=collection%2Fbyline%2Fmatthew-

rosenberg&action=click&contentCollection=undefined&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection

269. Rowntree, L. (2018). *How the California Consumer Privacy Act Aims to Put an End to the Data Wild West.* Dostopno prek https://www.exchangewire.com/blog/2018/09/04/how-the-california-consumer-privacy-act-aims-to-put-an-end-to-the-data-wild-west/

270. Rule, J. B. (2007). *Privacy in Peril*. Oxford, New York: Oxford University Press.

271. Ryan, J. (2018, 20. marec). *Risks in IAB Europe's proposed consent mechanism* [blog]. Dostopno prek https://pagefair.com/blog/2018/iab-europe-consent-problems/

272. Schmidt, D. C. (2018). *Google Data Collection*. Dostopno prek https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf

273. Schneider, W., Dumas, S. T. in Shiffrin, R. M. (1984). Automatic and Controlled Processing Revisited. *Psychological Review 91*(2), 269-276.

274. Seitz, J. in Zorn, S. (2016). Perspectives of Programmatic Advertising. V Busch, O. (ur.), *Programmatic Advertising: The Successful Transformation to Automated, Data-Driven Marketing in Real-Time*. Switzerland: Springer Internetional Publishing.

275. Shapiro, A. L. (1999). *The Control Revolution: How the Internet in Puttig Individuals in Charge and Changing the World We Know*. New York: Public Affairs.

276. Shepardson, D. (2018, 27. julij). Trump administration working on consumer data privacy policy. *Reuters*. Dostopno prek https://www.reuters.com/article/us-usa-internet-privacy/trump-administration-working-on-consumer-data-privacy-policy-idUSKBN1KH2MK

277. Sherman, E. (2008, 4. september). *Privacy policies are great—for phds*. Dostopno prek http://industry.bnet.com/technology/1000391/privacypolicies-are-great-for-phds/

278. Silverstone, R. (1999). *Why Study the Media?* London: Sage.

279. Singer, N. (2015, 28. februar). White House Proposes Broad Consumer Data Privacy Bill. *The New York Times*. Dostopno prek https://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html?module=inline

280. Singer, N. (2016, 29. februar). Why a Push for Online Privacy Is Bogged Down in Washington. *The New York Times*. Dostopno prek

https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html

281. Singer, N. (2018, 27. maj). The Next Privacy Battle in Europe Is Over This New Law. *The New York Times*. Dostopno prek https://www.nytimes.com/2018/05/27/technology/europe-eprivacy-regulation-battle.html
282. Slefo, G. P. (2017, 26. april). Desktop and Mobile Ad Revenue Surpasses TV for the First Time. *Adage*. Dostopno prek https://adage.com/article/digital/digital-ad-revenue-surpasses-tv-desktop-iab/308808/
283. Soghoian, C. (2011). *The History of the Do Not Track Header*. Dostopno prek http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html
284. Solon, O. in Graham-Harrison, E. (2018, 3. maj). The six weeks that brought Cambridge Analytica down. *The Guardian*. Dostopno prek https://www.theguardian.com/uk-news/2018/may/03/cambridge-analytica-closing-what-happened-trump-brexit
285. Solove, D. J. (2004). *The Digital Person*. New York: NYU Press.
286. Sotto, L. J. in Simpson, A. P. (2014). United States. V R. P. Jay (ur.), *Data Protection & Privacy in 31 jurisdictions worldwide* (str. 208–214). London: Law Business Research Ltd.
287. Stallworth, B. (2010). Future Imperfect: Googling for Principles in Online Behavioral Advertising. *Federal Communications Law Journal 62*(2), 465–490.
288. Statista (2017a). *Daily time spent on social networking by internet users worldwide from 2012 to 2017 (in minutes)*. Dostopno prek https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/
289. Statista (2017b). *Digital Advertising*, dostopno prek https://www.statista.com/outlook/216/102/digital-advertising/europe
290. Chen, S. (2009). Corporate Responsibilities in Internet-Enabled Social Networks. *Journal of Business Ethics 90*(4), 523–536.
291. Storey, G., Dillon Reisman, J. M. in Narayanan, A. (2017). *The Future of Ad Blocking: An Analytical Framework and New Techniques*. Dostopno prek https://arxiv.org/abs/1705.08568
292. Taddeo, M. in Floridi, L. (2016). The Debate on the Moral Responsibilities of Online Service Providers. *Sci Eng Ethics 22*, 1575–1603.

293. Tene, O. in Polonetsky, J. (2012). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property 11*(239). Dostopno prek SSRN: https://ssrn.com/abstract=2149364
294. Tene, O. (2013). *DNT 2.0: What Next for Policymakers?* Dostopno prek https://iapp.org/news/a/dnt-2-0-what-next-for-policymakers/
295. Tidey, A. (2018, 19. oktober). Facebook shareholders call for Zuckerberg to step down as chair. *Euronews.* Dostopno prek https://www.euronews.com/2018/10/19/facebook-shareholders-call-for-zuckerberg-to-step-down-as-chair
296. Tien, L. (2010). *Commerce Department's Online Privacy Report a Positive Step, But Self-Regulation Isn't Enough*. Dostopno prek http://www.eff.org/deeplinks/2010/12/commerce-departments-online-privacy-report
297. The Wall Street Journal (2016, 4. november). What They Know. *The Wall Street Journal*. Dostopno prek: http://blogs.wsj.com/wtk/
298. Tomšič, A., Burnik, J. in drugi (2017). *Consolidated report on enhancing confidence and acceptability of new certification measures. Deliverable D7.1 for the CRISP project*. Dostopno prek http://crispproject.eu/wp-content/uploads/2017/07/CRISP_D7.1_Consolidated-WP7-report.pdf
299. Tran, M.-D., Acs, G. in Castelluccia, C. (2014). *Retargeting Without Tracking.* Dostopno prek https://www.semanticscholar.org/paper/Retargeting-Without-Tracking-Tran-%C3%81cs/affbf3fbaf99667e91c477610e11a601521768ec
300. Tucker, C. (2011). *Social Networks, Personalized Advertising and Privacy Controls*. NET Institute Working Paper No. 10-07; MIT Sloan Research Paper No. 4851-10. Dostopno prek http://ssrn.com/abstract=1694319
301. Turkle, S. (1994). Constructions and Reconstructions of Self in Virtual Reality: Playing in the MUDs. *Mind, Culture, and Activity 1*(3), 158–167.
302. Turkle, S. (2007). Authenticity in the age of digital companions. *Interaction Studies 8*(3), 500–517.
303. Turkle, S. (2008). Always-on/Always-on-you: The Tethered Self. V J. E. Katz (ur.), *Handbook of Mobile Communication Studies* (str. 121–137). Cambridge (Mass.), London: MIT Press.
304. Turow, J., King, J., Hoofnagle, C. J., Bleakley, A. in Hennesy, M. (2009). *Americans reject tailored advertising and three activities that enable it.* Tech. rep., Annenberg

School for Communications, University of Pennsylvania. Dostopno prek http://repository.upenn.edu/asc_papers/137/

305. Tutaj, K. in van Reijmersdal, E. A. (2012). Effects of online advertising format and persuasion knowledge on audience reactions. *Journal of Marketing Communications 18*(1), 5–18.

306. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein vs. Wirtschaftsakademie (sodba). (2018). *C-210/16. SEU*, 5. junij. Dostopno prek http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN

307. Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES. Dostopno prek https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32016R0679

308. Van Alsenoy, B., Verdoodt, V., Heyman, R., Ausloos, J., Wauters, E. in Acar, G. (2015). *From social media service to advertising network – A critical analysis of Facebook's Revised Policies and Terms.* Dostopno prek https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms

309. Van Canneyt in De Smet (2018, 6. marec). Brussels court: Facebook must play by the Belgian privacy and cookie rules. *IAPP*. Dostopno prek https://iapp.org/news/a/brussels-court-facebook-must-play-by-the-belgian-privacy-and-cookie-rules/

310. Van Couvering, E. (2004). *New Media? The Political Economy of Internet Search Engines.* Dostopno prek http://personal.lse.ac.uk/vancouve/IAMCR-CTP_SearchEnginePoliticalEconomy_EVC_2004-07-14.pdf

311. Van Dijck, J. in Poell, T. (2013). Understanding Social Media Logic. *Media and Communication 1*(1), 2–14.

312. Van Noort, G., Smit, E. G. in Voorveld, H. A. M. (2013). The online behavioural advertising icon: Two user studies. V S. Rosengren in M. Dahlen (ur.), *EAA Advances in Advertising Research (Vol. IV The Changing Roles of Advertising)* (str. 365–378). Cutting Edge International Research.

313. W3C (2015). *Tracking Preference Expression (DNT)*, W3C Candidate Recommendation 20 August 2015. Dostopno prek https://www.w3.org/TR/tracking-dnt/
314. W3C (2016). *Tracking Compliance and Scope*, W3C Candidate Recommendation 26 April 2016. Dostopno prek http://www.w3.org/TR/2016/CR-tracking-compliance-20160426/
315. W3C (2017). *Tracking Preference Expression (DNT)*, W3C Candidate Recommendation 20 August 2015. Dostopno prek https://www.w3.org/TR/2017/CR-tracking-dnt-20171019/
316. W3C (2019a). *Tracking Preference Expression (DNT)*. Dostopno prek: https://www.w3.org/TR/tracking-dnt/
317. W3C (2019b). *Tracking Compliance and Scope*. Dostopno prek: https://www.w3.org/TR/tracking-compliance/
318. Wakunuma, K. J. in Stahl, B. C. (2014). Tomorrow's ethics and today's response: An investigation into the ways information systems professionals perceive and address emerging ethical issues. *Inf Syst Front 16*, 383–397.
319. Warren, S. in Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review 4*(5), 193.
320. Warren, T. (2018, 18. julij). Google fined a record $5 billion by the EU for Android antitrust violations. *The Verge*. Dostopno prek https://www.theverge.com/2018/7/18/17580694/google-android-eu-fine-antitrust
321. Weber, R. (2010). Internet of Things – New Security and privacy challenges. *Computer Law & Security Report 01 26*(1), 23–30.
322. Wellman, B. (2011). Studying the Internet through the Ages. V M. Consalvo in C. Ess (ur.), *The Handbook of Internet Studies* (str. 17–23). Chichester: Blackwell Publishing Ltd.
323. Wells, T. (2006). *How and Why Behavioral Advertising Works*. Dostopno prek http://www.seochat.com/c/a/Website-Marketing-Help/How-and-Why-Behavioral-Advertising-Works/
324. Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.
325. WFA (2014). *WFA guide to What Every Advertiser Should Know about Media Markets*. Dostopno prek https://www.wfanet.org/app/uploads/2017/04/programmatic.pdf

326. WFA World Federation of Advertisers (2010). *WFA responds to EU opinion on interest-based advertising.* Dostopno prek http://www.wfanet.org/globalnews.cfm?id=381

327. Woo, J. (2006). The right not to be identified: Privacy and anonymity in the interactive media environment. *New Media Society 8*(6), 949–967.

328. WP29 Delovna skupina iz člena 29 (2010a). *Opinion 2/2010 on online behavioral advertising.* Dostopno prek http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

329. WP29 Delovna skupina iz člena 29 (2010b). *Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing*. Dostopno prek http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp174_en.pdf

330. WP29 Delovna skupina iz člena 29 (2011). *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising.* Dostopno prek https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf

331. WP29 Delovna skupina iz člena 29 (2012). *Opinion 04/2012 on Cookie Consent Exemption.* Dostopno prek http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

332. WP29 Delovna skupina iz člena 29 (2013). *Working Document 02/2013 providing guidance on obtaining consent for cookies.* Dostopno prek https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

333. WP29 Delovna skupina iz člena 29 (2014a). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. Dostopno prek https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

334. WP29 Delovna skupina iz člena 29 (2014b). *Opinion 8/2014on the on Recent Developments on the Internet of Things.* Dostopno prek https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

335. WP29 Delovna skupina iz člena 29 (2014c). *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting.* Dostopno prek

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf

336. WP29 Delovna skupina iz člena 29 (2014d). *Article 29 Data Protection Working Party comments in response to W3C's public consultation on the W3C Last Call Working Draft, 24 April 2014, Tracking Preference Expression (DNT).* Dostopno prek https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf
337. WP29 Delovna skupina iz člena 29 (2015a). *Article 29 Data Protection Working Party comments in response to W3C's public consultation on the W3C Last Call Working Draft, 14 July 2015, Tracking Compliance and Scope.* Dostopno prek https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20151001__letter_of_the_art_29_wp_w3c_compliance.pdf
338. WP29 Delovna skupina iz člena 29 (2015b). *Cookie sweep combined analysis – report.* Dostopno prek https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp229_en.pdf
339. WP29 Delovna skupina iz člena 29 (2015c). *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain.* Dostopno prek https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf
340. WP29 Delovna skupina iz člena 29 (2016). *Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC).* Dostopno prek https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf
341. WP29 Delovna skupina iz člena 29 (2017a). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018.* Dostopno prek https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
342. WP29 Delovna skupina iz člena 29 (2017b). *Guidelines on Consent under Regulation 2016/679 (wp259rev.01).* Dostopno prek https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
343. WP29 Delovna skupina iz člena 29 (2017c). *Guidelines on transparency under Regulation 2016/679. Adopted on 29 November 2017. As last Revised and Adopted on*

11 April 2018. Dostopno prek https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

344. WP29 Delovna skupina iz člena 29 (2017d). *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC).* Dostopno prek https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140
345. WP29 Article 29 Data Protection Working Party (2018). *Press Release "Sorry is not enough": WP29 establishes a Social Media Working Group.* Dostopno prek https://edps.europa.eu/sites/edp/files/publication/18-04-11_wp29_press_release_en.pdf
346. Wright, D. in de Hert, P. (2012). *Privacy Impact Assessment.* Netherlands: Springer.
347. Wu, M., Miller, R. C. in Garfinkel, S. L. (2006). D*o Security Toolbars Actually Prevent Phishing Attacks?* V Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Held in Montreal, ACM Press, str. 601–610.
348. Zenith (2017). *67% of digital display to be sold programmatically by 2019.* Dostopno prek https://www.zenithmedia.com/programmatic-marketing-forecasts/
349. Zittrain, J. (2008). *The Future of the Internet and how to stop it.* New Haven: Yale University Press.
350. Zittrain, J. in Palfrey, J. (2008). Internet Filtering: The Politics and Mechanisms of Control. V R. Deibert, J. Palfrey, R. Rohozinski in J. Zittrain (ur.), *Access Denied. The Practice and Policy of Global Internet Filtering* (str. 29–56). Boston: The MIT Press.
351. Zuiderveen Borgesius, F. (2016). Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new data protection regulation. *Computer Law Security Review 2*, 256–271.
352. Zuiderveen Borgesius, F. in Poort, J. (2017). Online Price Discrimination and EU Data Privacy Law. *Journal of Consumer Policy 40*(3), 347–366.
353. Zuiderveen Borgesius, F. J. in McDonald, A. (2015). *Do Not Track for Europe.* TPRC43: The 43rd Research Conference on Communications, Information and Internet Policy paper. Dostopno prek https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2588086
354. Zuiderveen Borgesius, F. J. (2014). *Improving privacy protection in the area of behavioural targeting* (doktorska disertacija) University of Amsterdam, Amsterdam.

Dostopno prek https://dare.uva.nl/search?identifier=c74bdba6-616c-4cd9-925e-33a5858935e5

PRILOGE

Priloga A: Povezovanje piškotkov

Tehnologija, s katero platforma za izmenjavo oglasov (angl. *ad exchange*) in kupci oglasnega prostora lahko primerjajo informacije o določenem uporabniku, se imenuje »primerjava piškotkov« (angl. *Cookie Matching/Syncing*), kar pomeni, da različni domeni (spletni strani) primerjata svoje piškotke pri določenem posameznem uporabniku. Ker na ta način nastane povezava med profili posameznika pri neodvisnih podjetjih, ima to velik vpliv na zasebnost posameznika. Ko spletna stran posreduje podatke platformi za izmenjavo oglasov, ta zagotovi primerjavo piškotkov s kupci oglasnega prostora, uporabnikovi podatki pa tako postanejo produkt, ki ga platforma draži v realnem času (Olejnik in drugi, 2014, str.1). Nedavna študija je pokazala, da največ svojih piškotkov s tretjimi stranmi primerja Doubleclick. net – Googlova oglaševalska platforma (Engelhardt in Narayanan, 2016, str. 11). Tak način oglaševanja prinaša prednosti v smislu bolj racionalne izrabe oglaševalskih sredstev in večjega prihodka od oddajanja prostora za oglase. Hkrati pa pomeni povečana tveganja za zasebnost in varstvo osebnih podatkov uporabnikov.

Priloga B: Potenciali programatičnega oglaševanja in izzivi za uporabnike elektronskih komunikacij

Oglaševanje z uporabo programatičnih platform je v porastu (Olejnik in drugi, 2014, str. 1). Omogoča povezovanje *offline* in *online* podatkov, poleg tega pa digitalizacija tradicionalnih medijskih kanalov pomeni priložnost za razširitev programatičnega oglaševanja na zunanje medije (jumbo plakati), radio in TV (Roloff 2013, v Busch 2016, str. 13). Busch (2016) zaključuje, da bo avtomatizacija oglaševanja in vse večji poudarek na analizi in izrabi podatkov postala stalnica vsega oglaševanja, ne glede na kanal in da je programatično oglaševanje eden od štirih pomembnih razvojnih mejnikov v trženjskem komuniciranju v zadnjih 20 letih (Busch 2016, str. 12–14). Gonilna sila za rastjo programatičnega oglaševanja je problematika monetizacije mobilnega prometa, potrebe medijev po kombiniranju monetizacije vsebine in podatkov, ki so jim na voljo, ponujajo pa se jim tudi možnosti kombiniranja podatkov iz realnega in virtualnega sveta (Seitz in Zorn 2016, str. 38).

Tudi avtorji s področja marketinga, ki trende razvoja programatičnega oglaševanja spremljajo z veliko mero optimizma in upanja, izpostavljajo, da prinaša tudi izzive. Veliko podatkovje in tehnološki napredek pri avtomatizaciji oglaševanja, sposobnosti predvidevanja v okviru strojnega učenja ter možnosti izrabe novih kanalov (npr. interneta stvari) so povezani s pomisleki glede zasebnosti uporabnikov in s tem povezane uporabe protireklamnih vtičnikov (Seitz in Zorn, 2016, str. 47–49) ter z zlorabami in neprimernimi objavami oglasov. Po nekaterih raziskavah si polovice oglasov, kupljenih preko mrež in platform za izmenjavo oglasov, ni mogoče ogledati, pri čemer so nekateri prikazi goljufija. Težak je tudi nadzor nad primernostjo prikazanega oglasa v kontekstu vsebine, npr. sladkarije ob članku o sladkorni bolezni, kar slabo vpliva na pozicioniranje znamke (Nesdale, 2018).

Odgovor na izzive glede zasebnosti oglaševalska panoga vidi predvsem v samoregulaciji in svari pred preveč restriktivno zakonodajo, ki bi lahko omejila podatkovne tokove, nujno gorivo za razvoj *ad tech* panoge. Prav tako naj bi ponudba resnične vrednosti potrošnikom pripomogla k temu, da bodo razumeli menjavo vrednosti za učinkovite in inovativne storitve in vsebine. Seitz in Zorn (2016) optimistično zaključita, da so negativni pogledi na vprašanje zasebnost obvladljivi in izpostavljata, da navkljub vsemu danes večina pametnih telefonov dovoljuje, da so locirani (uporabniki dovoljujejo oddajanje lokacijskih podatkov) in da

uporabniki očitno pristajajao v deljenje tega podatka pri uporabi aplikacij (Seitz in Zorn, 2016, str. 49). Na tej točki velja pripomniti, da pogosto uporabniki niti ne vedo, da oddajajo svojo lokacijo, niti ne, da jo aplikacije zahtevajo, kaj s tem podatkov dejansko počnejo ali bi lahko počele. Deloma zaradi netransparentnega razkrivanja informacij in deloma zaradi nepoučenosti uporabnikov o delovanju *ad tech* industrije in poslovnih modelih za brezplačnimi storitvami in aplikacijami. Da je ta tok podatkov enostavno dostopen torej ne pomeni, da uporabniki s tem veljavno soglašajo in da so pričakovanja glede zasebnosti v družbi postala nižja, pač pa je tok podaktov dostopen zaradi slabega zavedanja uporabnikov o tveganjih. Prav tako samoregulacijske iniciative na trgu programatičnega oglaševanja še niso pokazale zadovoljivih rezultatov, oziroma so, kot poudarjajo strokovnjaki, celo zavajajoče glede zagotavljanja minimalnih ukrepov za skladnost z zakonodajo (Ryan, 2018).

Da je varovanje zasebnosti in osebnih podatkov potrošnikov večji izziv, kot ga poskuša relativizirati hitro razvijajoča oglaševalska panoga, poudarjajo regulatorji in zagovorniki zasebnosti. Norveški organ za varstvo osebnih podatkov v analizi trga programatičnega oglaševanja oceni, da oglaševalski prihodki nedvomno prispevajo k financiranju mnogih storitev, ki so uporabnikom v korist, hkrati pa je programatično oglaševanje običajno prikrito in netransparentno; običajen uporabnik nikakor ne razume širine podatkovnih tokov, kar prinaša izzive za njegovo zasebnost:

- informacijska asimetrija – potrošniki se ne zavedajo množičnega zbiranja in deljenja podatkov pri uporabi elektronskih naprav. Informacijska asimetrija je oblika napake trga;
- šibkost privolitve – uporabniki interneta želijo hiter in enostaven dostop do storitev, zato avtomatično podajo vsa dovoljenja, za katera so zaprošeni. Omejevanje obdelave osebnih podatkov s privolitvijo ne deluje kot bi moralo. Uporabniki so prepuščeni velikim in močnim igralcem na trgu, ki diktirajo v kaj morajo uporabniki privoliti, da lahko uporabljajo storitve;
- pomanjkanje izbire – potrošniki običajno nimajo druge izbire, kot da potrdijo, da se strinjajo z obdelavo osebnih podatkov. Veljavna privolitev pa bi morala pomeniti resnično izbiro in možnost svobodne zavrnitve;
- pomanjkanje nadzora – avtomatizacija prodaje in prikazovanja oglasov pomeni, da je zelo težko nadzorovati, kdo bo prikazal kakšen oglas in kje, ter kdo bo sledil uporabnikom določene spletne strani. V tem smislu izdajatelji težko zagotovijo

potrebne informacije o obdelavi osebnih podatkov, saj niti sami ne vedo, kdo bo obdeloval podatke njihovih strank;

— manipulacija in prikrita diskriminacija – oglaševalska panoga ve o potrošnikih več kot katerakoli druga, hkrati pa imamo zelo malo uvida v to, kako podjetja iz te panoge obdelujejo podatke. Zaradi tega smo potrošniki lahko izpostavljeni prikriti diskriminaciji in manipulaciji. Avtomatizirano trženje, ki ga poganjajo algoritmi lahko reproducira obstoječe predsodke in stereotipe;

— *function creep* in intenzivni vseprisotni nadzor – podatki, ki jih obdeluje oglaševalska panoga, lahko prihajajo iz najrazličnejših virov, lahko so bili zbrani za čisto drugačne začetne namene. Velike zbirke podatkov so bolj ranljive z vidika napadov in incidentov. *Log in* rešitve, na podlagi katerih je mogoče sledenje uporabnikom preko različnih naprav, pa še dodano širijo možnosti nadzora (Datatilsynet, 2015, str. 39–43).

Norveški nadzorni organ poda več priporočil za boljšo ureditev na trgu programatičnega oglaševanja. Priporočila segajo tudi na področje etike, ki bi zagotovila boljšo preglednost in odprtost oglaševalskega trga ter varovanje pravic posameznikov.

— Priporočila glede zbiranja podatkov: izdajatelji morajo prevzeti odgovornost, ker dopuščajo tretjim strankam, da preko njihove spletne strani sledijo uporabnikom, tako z vidika obveščanja, kot tudi zagotavljanja, da tretje stranke delujejo v skladu z zakonodajo. Vzemi ali pusti mehanizmi bi morali biti prepovedani, če obdelava podatkov ni potrebna za zagotavljanje storitve. Izjave za pridobivanje privolitve bi morale biti izboljšane, primerne digitalnim okoljem.

— Priporočila glede obdelave podatkov: Oglaševalska panoga bi morala upoštevati pravila glede omejitve namenov obdelave podatkov. Podatki bi morali biti po doseženem namenu njihove obdelave izbrisani. Profiliranje na podlagi občutljivih podatkov bi moralo biti prepovedano. Profiliranje na podlagi primerjanja piškotkov ne bi smelo biti dovoljeno. Algoritmi bi morali biti pod stalnim nadzorom. Pri anonimizaciji podatkov bi morale biti izvedene ocene tveganja.

— Priporočila glede boljšega informiranja posameznikov: razvoj avtomatiziranih orodij za preglednost (katere podatke oglaševalski ponudnik sploh obdeluje, kateri podatki so zajeti v profilu posameznika) in za upravljanje s podatki (npr. t. i. *privacy*

dashboards). Enostavnost uporabe alternativnih storitev, ki ne vključujejo sledenja s strani tretjih strank.

— Sodelovanje nadzornih organov za varstvo osebnih podatkov in zaščito potrošnikov, spodbujanje oglaševalske panoge k ustvarjanju kodeksov in sistemov ciljanja oglasov, ki so zasebnosti bolj prijazni, izobraževanje o zasebnosti prijazni izrabi podatkov v trženju na univerzah (trženje, novinarstvo, informacijske tehnologije) (Datatilsynet, 2015, str. 46–49).

Priloga C: Facebook v primežu nadzornih organov in sodišč

Leta 2011 je ameriški regulator (FTC) ugotovil, da Facebook na mnogih področjih ne deluje v skladu z zakonodajo in da je zavajal svoje uporabnike glede nadzora, ki ga imajo nad svojimi lastnimi podatki. Facebook je na primer brez opozorila ali privolitve razkril liste prijateljev uporabnikov. V pogojih uporabe in izjavi o zasebnosti je zavajajoče navajal, da aplikacije ne bodo imele dostopa do več podatkov, kot jih nujno potrebujejo. Zavajal je uporabnike z izjavo, da njihovih podatkov ne deli z oglaševalci, pa to zahteva že sam brezplačni poslovni model Facebooka – storitev je namreč poplačana s strani oglaševalcev, ki jim prinaša natančno določeno občinstvo, itd. Zato sta FTC in Facebook sklenila dogovor, po katerem je slednji zavezan, da svoje prakse prilagodi in 20 let vsaki dve leti dopusti zunanjo revizijo svojih praks glede varovanja zasebnosti uporabnikov. Če Facebook dogovor prekrši, ga lahko doleti denarna kazen (FTC, 2011).

V Evropi je inšpekcijski pregled leta 2012 opravil irski nadzorni organ za varstvo osebnih podatkov[85] po pritožbah pobude *Europe v. Facebook*, ker naj bi Facebook prek gumba »Všeč mi je«, ki je široko prisoten po mnogih spletnih straneh, zbiral podatke o ne-uporabnikih Facebooka brez njihove privolitve. Nadzorni organ je ugotovil, da Facebook na mnogih področjih ne sledi natančno evropskemu pravnemu okvirju. Med naloženimi ukrepi je bila priprava natančnejših pojasnil, kako in kateri podatki se uporabljajo za oglaševanje, omejitve pri sledenju uporabnikov prek gumba »Všeč mi je«, strogo upoštevanje zahteve po predhodni privolitvi v obdelavo osebnih podatkov in omejitve dostopa aplikacij do podatkov uporabnika. Ukrepe naj bi Facebook zadovoljivo izvedel (Burnik, 2012b).

Novi val postopkov se je zgodil v zadnjih treh letih, ko je bilo razkrito ekstenzivno sledenje uporabnikom in ne-uporabnikom Facebooka po nepovezanih spletnih straneh, prakse kombiniranja in povezovanja podatkov iz različnih virov – tudi ne-spletnih in uporabe podatkov, pridobljenih od preprodajalcev podatkov ter slabe prakse obveščanja in uveljavljanja pravic posameznikov (Van Alsnoy in drugi, 2015). Nekaj ključnih spornih točk delovanja omrežja Facebook zadeva:

— privolitev uporabnikov: Facebook pridobi privolitev v vse svoje obdelave osebnih podatkov tako, da se posameznik strinja s splošnimi pogoji uporabe storitev, pri čemer

[85] Ker je leta 2010 Facebook na irskem ustanovil podružnico, je postal zavezan evropskemu pravu glede varstva osebnih podatkov.

ima možnost določnim obdelavam oporekati – npr. izraziti naknadno zavrnitev vedenjskega oglaševanja ali kombiniranja podatkov z zunanjimi partnerji Facebooka.

— Vprašljivo je, do katere mere lahko tako privolitev štejemo kot veljavno, glede na to, da mora biti privolitev svobodna, informirana, pravočasna in aktivna. Privzete nastavitve, s katerimi se mora uporabnik strinjati za uporabo storitve, namreč niso zasebnosti prijazne, pač pa so obdelave v zvezi z oglaševanjem in profiliranjem privzeto vklopljene.

— Kombiniranje in deljenje podatkov: Facebook lahko kombinira podatke iz vedno širšega kroga virov (npr. Instagram, Whatsapp, preprodajalci podatkov) in tako dobi globlji in natančnejši vpogled v profile svojih uporabnikov za namene oglaševanja. Sporno je, ali Facebook za to pridobi veljavno privolitev.

— Sledenje: Facebook sledi svojim uporabnikom in ne-uporabnikom preko piškotkov in morda tudi preko odtisov naprav, in sicer s pomočjo svojega »Všeč mi je« vtičnika, ki je integriran v ogromno število spletnih strani, ter preko spletnih svetilnikov oziroma pikslov, ki jih na svoje spletne strani integrirajo tisti, ki želijo oglaševati na Facebooku posameznikom, ki so bili prej na njihovi spletni strani (piksli so pogosto uporabljeni za ponovno ciljanje – kjer si posameznik ogleduje specifičen produkt, a ga ne kupi in nato prejme na Facebooku oglas za ta ali podoben produkt). Facebook naj bi s sledenjem ne-uporabnikom kršil zakonodajo s področja varstva osebnih podatkov in Direktivo 2002/58/ES, saj za tako sledenje ne pridobi vnaprejšnje privolitve od ne-uporabnikov (Van Alsenoy in drugi, 2015, str. 8–9).

Belgijski nadzorni organ za varstvo osebnih podatkov je na podlagi teh ugotovitev pozval Facebook k prenehanju sledenja preko »Všeč mi je« gumba. Ker se ta ni odzval, se je bitka preselila pred belgijska sodišča, medtem pa je belgijski nadzorni organ izdal priporočilo, kako naj Facebook prilagodi svoje delovanje, da bo skladno z zakonodajo. Facebook je namreč leta 2016 uvedel tudi sledenje posameznikom preko pikslov na tretjih partnerskih straneh. Priporočila so znova zadevala nujnost, da Facebook za sledenje z različnimi tehnologijami pridobi veljavno privolitev, da posameznikov ne zavaja z informacijami, ampak jih ustrezno obvešča ter da omeji svoje prakse sledenja (DPA, 2018).

Vprašanja v sodnih postopkih so zadevala pristojnost belgijskih organov za izvajanje nadzor nad Facebookom (ker je glavni sedež Facebook ustanovil na Irskem) in zakonitost njegove

obdelave osebnih podatkov. V prvi fazi je belgijsko sodišče pritrdilo, da Facebook ne sme slediti ne-uporabnikom preko svojega vtičnika na spletnih straneh brez njihove ustrezne privolitve. Na podlagi pritožbe je naslednja sodna instanca februarja 2018 razsodila, da belgijski organi imajo pristojnost odločanja v primeru Facebook, glede na argumentacijo v t. i. sodbi *Google Spain*[86] ter da Facebook krši pravila o piškotkih tako pri uporabnikih Facebooka kot pri ne-uporabnikih, saj naj ne bi pridobil veljavne privolitve za sledenje. Poleg tega naj bi bila taka obdelava podatkov nepoštena in nesorazmerna. Sodišče z grožnjo denarne kazni od Facebooka zahteva, da preneha uporabljati piškotke, piksle in podobne sledilne tehnologije na svoji in na tretjih domenah, če ne pridobi ustrezne privolitve uporabnikov, ki morajo biti celostno obveščeni (pri tem sodišče meni, da je trenutno obveščanje zavajajoče) ter da sprejme različne ukrepe za omejitev rabo piškotkov in podobnih tehnologij za namene oglaševanja, da bo njihova raba sorazmerna (Van Canneyt in De Smet, 2018).

Istočasno so postopke zoper Facebook koordinirano vodili tudi drugi nadzorni organi za varstvo osebnih podatkov v EU. Francoski organ je Facebooku izrekel sankcijo, ker brez pravne podlage kombinira osebne podatke uporabnikov za namen oglaševanja ter nezakonito sledi uporabnikom spleta na in izven omrežja Facebook, saj uporabniki niso zadostno obveščeni o teh praksah. Nizozemski organ je prav tako ugotovil kršitve zakonodaje glede varstva osebnih podatkov zaradi nezadostnega obveščanja ter zaradi uporabe občutljivih osebnih podatkov posameznikov brez njihovega izrecnega soglasja – podatki o spolnih preferencah so bili uporabljeni za oglaševanje (Autoriteit Persoonsgegevens, str. 2017). Facebook naj bi v odziv na to odpravil obdelavo podatka o spolni usmerjenosti za namen oglaševanja ter izboljšal obveščanje uporabnikov. Nizozemski nadzorni organ pa je pojasnil, da bodo nadaljnji postopki zoper Facebook potekali na evropski ravni in ne več na nacionalnih, kot to zapoveduje Uredba 2016/679 (Autoriteit Persoonsgegevens, 2018). Postopki potekajo tudi v Nemčiji, kjer nemški nadzorni organ iz Hamburga Facebooku oporeka, da uporabnikom ne dovoli rabe psevdonimov, pač pa vztraja pri resničnih imenih. Odločil je, da Facebook ne sme kombinirati podatkov pridobljenih iz WhatsApp storitve. Slednjo odločitev je potrdilo tudi sodišče. Tudi Berlinsko sodišče je pred kratkim razsodilo, da so Facebookovi splošni pogoji v nasprotju s pravili za varovanje potrošnikov: zavajajoča je trditev, da je storitev zastonj, premalo natančne so informacije o obdelavi podatkov,

[86] Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos (AEPD), 2014, C-131/12, Sodišče Evropske unije, C-131/12.

nezakonita je zahteva po razkritju resničnega imena in priimka (Federation of German Consumer Organisations, 2018).

Aprila 2018 je posebno strokovno skupino, namenjeno le vprašanjem družbenih medijev in njihove obdelave podatkov za najrazličnejše namene, predvsem glede oglaševanja in ciljanja, ustanovila Delovna skupina iz člena 29 (WP29, str. 2018). Povod so bila predvsem razkritja glede političnega mikro ciljanja, ki ga je s pomočjo Facebooka izvajala družba Cambridge Analytica in je imelo vpliv na zadnje predsedniške volitve v ZDA in referendum o izstopu Združenega Kraljestva iz EU.

Krog pravnih omejitev in odločitev pristojnih organov okoli Facebooka se torej vztrajno oži, predvsem v Evropi, kjer regulatorji že močno pritiskajo k uvedbi nujnih sprememb. Kaplja čez rob so bili pretresi v zvezi s Cambridge Analytica, pa tudi incident oktobra 2018, ko so hekerji kompromitirali račune skoraj 30 milijonov uporabnikov Facebooka in pridobili dostop do imen, kontaktnih e-naslovov in telefonskih številk. Pri nekaterih tudi do kraja bivanja, rojstnega datuma, zadnjih 10 krajev, kjer so se prijavili in zadnjih 15 iskanj. Pridobili so dostop do zasebnih sporočil. Kot opozarjajo strokovnjaki, bi napadalci te podatke lahko izkoriščali za nadaljnje nelegalne aktivnosti, kot je pridobivanje dostopa do drugih storitev, do spletnega bančništva, itd. Napad je omogočila ranljivost v sistemu Facebooka (O'Brien in Anderson, 2018). Pomembno je dodati, da pritisk ne zajema le regulatorjev na področju varstva osebnih podatkov, pač pa se seli tudi na področje pravil o varovanju potrošnikov, kot kaže poročilo, ki ga je pripravila enota za varstvo potrošnikov Evropske komisije in vsebuje tudi nekatere inovativnejše predloge glede regulacije delovanja spletnih družbenih medijev z vidika pravil o varovanju potrošnikov: npr. glede dolžnosti razkrivanja informacij in glede zavajajočih trditev, da je storitev brezplačna, pa jo v resnici uporabniki plačajo s svojimi podatki ter glede spodbujanja dvigovanja zavedanja in izobraževanja (Evropska komisija, 2018a, str. 84–87).

Priloga D: Trženjski produkti trgovcev s podatki

FTC je v svoji raziskavi marketinške produkte trgovcev s podatki razdelila na tri skupine: (1) neposredno trženje, (2) *online* trženje, ki vključuje trženje na spletu, mobilnih napravah in preko kabelske in satelitske televizije ter (3) trženjska analitika.

Neposredno trženje

Pri neposrednem trženju trgovci s podatki ponujajo klientom bodisi »pripenjanje« podatkov (angl. *data append*) ali sezname za trženje (angl. *marketing lists*). V prvem primeru klient trgovcu s podatki sporoči nekaj podatkov svojih strank (npr. ime in naslov) in si izbere, katere podatke o tej listi svojih strank želi dodatno pridobiti – npr. njihovo telefonsko številko ali nakupne navade. Trgovec s podatki te nove podatke »pripne« h klientovim podatkom zato, da jih ta lahko nato uporabi pri neposredni pošti, telemarketingu in e-mail trženju. Klient lahko priskrbi le telefonske številke, trgovec s podatki pa jih poveže z imeni, priimki in e-naslovi. Lahko pa klient priskrbi listo svojih strank, ki jo trgovec s podatki dopolni z njihovimi značilnostmi (podatki, ki jih trgovec zbral iz drugih virov in podatki, ki jih je sam pripisal – npr. *High End Shopper*, *Cholesterol Focus*). V drugem primeru pa klient izbere karakteristike potrošnikov, ki ga zanimajo, npr. ženske, ki imajo določeno znamko avta, da jim ponudijo določene produkte ali tiste, ki so v denarni stiski, da jim ponudijo posojilo, tiste, ki živijo v določeni regiji in jih zanima kuhanje, itd. Trgovec s podatki sestavi listo potrošnikov, ki ustrezajo kriterijem naročnika, in vključuje npr. ime, priimek, kontaktne podatke, morda tudi starost in prihodek gospodinjstva (FTC, 2014, str. 23–25).

Spletno trženje

Produkti za spletno trženje (na spletu, mobilnih napravah in preko kabelske in satelitske televizije) vključujejo tri tipične storitve:

— Ciljanje registriranim: spletna stran podatke svojih registriranih uporabnikov posreduje trgovcu s podatki, ta pa spletni strani priskrbi podatke o značilnostih teh uporabnikov, npr. njihovih potovalnih željah. Tako lahko spletna stran svojim registriranim uporabnikom prikaže oglase glede na njihove preference, bodisi jim ponudi ponudbe za svoje izdelke, ali pa proda oglasni prostor oglaševalcem, ki jih

zanima tak tip uporabnikov. Na enak način lahko npr. ponudnik kabelske televizije trgovcu s podatki posreduje podatke o svojih naročnikih, in pridobi podatke o njihovih interesih ali značilnostih. Ponudnik kabelske TV se lahko potem odloči, katerim naročnikom bi oddajal oglas za svoje nove španske kanale, lahko pa npr. lokalni potovalni agenciji ponudi, da za njih oddaja oglas točno določenemu segmentu svojih naročnikov.

— Vzajemno ciljanje: v primeru take storitve dve organizaciji ponudita trgovcu s podatki liste svojih uporabnikov, strank, ta pa analizira, ali se eni strani splača oglaševati pri drugi. Spletna stran z opremo za potapljanje želi oglaševati nove maske. Turistična spletna stran ponuja potapljaški spletni strani prostor za njen oglas, vendar potapljaška spletna stran ne ve, ali njeni kupci obiskujejo turistično spletno stran. Spletni strani ne želita deliti baze svojih uporabnikov druga z drugo, zato primerjavo opravi trgovec s podatki in ugotovi, da je 3000 registriranih uporabnikov potapljaške strani tudi registriranih na turistični spletni strani. Zadovoljna s temi obeti se potapljaška spletna stran odloči, da bo oglaševala svoje maske na turistični spletni strani.
— Dodajanje podatkov, pridobljenih izven spleta (angl. *onboarding*): bistvo take vrste storitve je, da trgovec s podatki piškotku doda podatke o posamezniku, pridobljene izven spleta, tako, da je mogoče posamezniku na spletu prikazovati oglase glede na njegove aktivnosti izven spleta. V tem primeru (1) organizacije trgovcu bodisi posredujejo podatke o svojih strankah, zato da jih ta izsledi na spletu in jim tam prikaže primeren oglas ali pa (2) organizacije želijo, da trgovec s podatki najprej identificira posameznike, ki jih vežejo določene značilnosti (npr starost, kraj bivanja, znamka avta) in jih potem poišče še na spletu, kjer jim prikaže oglas (FTC, 2014, str. 25–27).

Ta proces običajno poteka v treh fazah:

— Segmentacija: trgovec s podatki najprej dobi naročilo, da identificira posameznike z določenimi značilnostmi, bodisi iz svojih baz podatkov, bodisi dobi listo posameznikov od naročnika in mora iz te liste izločiti primeren segment, glede na želje naročnika (npr. sofisticirani nakupovalci, ki živijo na določenem območju).
— Povezovanje (angl. *matching*): v tem koraku trgovec s podatki poišče posameznike, ki jih je identificiral v prejšnjem koraku še na spletu. To stori tako, da od spletnih strani, ki imajo registrirane uporabnike (npr. družbena omrežja) pridobi njihove sezname.

Nato svoj seznam primerja s pridobljenimi in poveže posameznike (to naj bi se dogajalo na podlagi unikatnih identifikatorjev in ne imen in priimkov).

— Ciljanje na spletu: v zadnjem koraku je povezanim posameznikom prikazan oglas na spletu. Da to izvede, mora trgovec s podatki na napravo posameznika namestiti piškotek; to stori takrat, ko ga družbeno omrežje obvesti, da se je iskani uporabnik prijavil v omrežje. Piškotek vsebuje tudi informacije, ki jih trgovec s podatki pripel (vendar ne informacij o imenu, e-pošti, itd.). Tako lahko trgovec s podatki oglašuje uporabniku kjerkoli na spletu, dokler ima ta na svoji napravi piškotek. Trgovec s podatki lahko oglašuje sam, ali pa se poveže z oglaševalskimi mrežami, ki imajo zakupljene prostore na spletnih straneh in želijo tam prikazati oglas posamezniku.
— Ena od možnosti je tudi ponovno ciljanje (angl. *retargeting*), kjer želi organizacija svojim določenim strankam ponuditi za njih prilagojeno ponudbo tudi na spletu, oziroma kampanje preko različnih kanalov (angl. *cross-channel*), kjer bi organizacija želela istim posameznikom prikazovati oglase na različnih platformah in po različnih kanalih, npr. na spletu in po e-pošti (FTC, 2014, str. 27–30).

Trženjska analitika

Trgovci s podatki ponujajo tudi analitiko za namene trženja in predvidevanje verjetnega vedenja potrošnikov. Analitični produkti lahko pomagajo natančnejše ciljati v oglaševalskih kampanjah, izboljšati produkte in sporočila in zbrati podatke o stališčih in željah potrošnikov. Trgovec s podatki lahko npr. analizira naročnikove podatke in mu svetuje glede izbire kanala za oglaševanje določenega produkta ali znamke. Prav tako lahko napovejo pričakovane rezultate marketinških strategij – npr. o učinkovitosti oglaševanja na Twitterju. Lahko ponujajo oceno kampanje po njeni izvedbi in pri tem upoštevajo vse mogoče vire informacij, javno dostopne in komercialne, ki jih povezujejo s podatki, ki jih priskrbi naročnik. Npr. koliko strank je videlo določen oglas in nato kupilo izdelek v trgovini. Nekateri tako za potrošnike ustvarjajo ocene, kako verjetno se bodo odzvali na določen trženjski prijem, npr. na oglasno e-pošto, ali kako verjetno je, da imajo vpliv na druge potrošnike – so neke vrste mnenjski voditelji (FTC, 2014, str. 31).

Priloga E: Priporočila glede dobrih praks in bodoče zakonodaje na področju trgovcev s podatki

FTC je glede na različne kategorije produktov, ki jih ponujajo trgovci s podatki, zakonodajalcu izdala priporočila glede bodoče zakonodaje, ki bi v prihodnje morala omejiti njihovo dejavnost. V primeru marketinških produktov bi morala zakonodaja posameznikom omogočiti (1.) dostop do podatkov o njih in (2.) naknadno zavrnitev obdelave osebnih podatkov. Da bi se lahko posamezniki sploh seznanili s temi pravicami, bi morala zakonodaja zahtevati vzpostavitev centraliziranega mehanizma, kot npr. internetnega portala, kjer bi se trgovci s podatki lahko identificirali in objavili orodja za dostop do podatkov in zavrnitev obdelave. Tako bi posamezniki na eni točki lahko izvedeli katere njihove podatke trgovci s podatki obdelujejo in uveljavili svojo voljo do zavrnitve. FTC pa opozarja, da je trgovcev s podatki na trgu veliko in da bi moral biti portal omejen na npr. 50 največjih, da ne bi bili posamezniki soočeni s tako širokim naborom informacij. V tem smislu FTC tudi priporoča, da so posamezniki seznanjeni s svojimi podatki v razumnem obsegu, ki še vedno kaže celostno sliko ter vključuje morebitne občutljive podatke, saj bi v nasprotnem primeru težko razumeli tisoče segmentov, ki jih o posamezniku morda vodi trgovec s podatki. V zvezi z obveščanjem potrošnikov FTC meni, da bi morala zakonodaja zahtevati, da je posameznik obveščen, če trgovec s podatki zbira podatke iz različnih virov in jih dopolnjuje s sklepanjem na določene druge podatke, ter obveščen o virih podatkov in kategorijah podatkov, da lahko v primeru napak podatke popravi pri viru. Ker so trgovci s podatki posamezniku nevidni, FTC predlaga tudi, da bi morale imeti stranke, ki imajo stik neposredno s posamezniki, dolžnost, da ga informirajo, če podatke posredujejo naprej trgovcem (FTC 2014, str. 50–54).

FTC poda tudi priporočila trgovcem s podatki in sicer glede upoštevanja koncepta vgrajene zasebnosti (angl. *privacy by design*), ki naj bi preprečil zbiranje nesorazmernih količin podatkov, s katerimi je posameznik podvržen večjim možnostim za zlorabe, pač pa naj bi trgovci s podatki uničevali podatke, ki niso več relevantni. FTC svari tudi pred obdelavo osebnih podatkov otrok in najstnikov, ki so še posebej ranljivi, ter opozarja trgovce s podatki naj po najboljših močeh zagotovijo, da klienti njihovih podatkov (še posebej občutljivih) ne bi uporabili za nezakonito diskriminacijo oziroma, da podatke dejansko uporabijo za namene, kot so določeni – da npr. marketinških produktov ne uporabijo za namen zavračanja potrošniških kreditov, zavarovanja, itd. Nekateri trgovci s podatki že revidirajo svoje kliente,

da se prepričajo, da s podatki ravnajo skladno s pogodbeno določenimi nameni (FTC 2014, str. 55–56).

V zadnjih letih je bila industrija trgovcev s podatki v ZDA deležna precejšnjega zanimanja s strani regulatornih organov in zakonodajalca v ZDA, predlaganih je bilo več zakonov, ki sicer niso bili sprejeti[87], njihov namen pa je bil povečati preglednost komercialnega nadzora, kar naj bi opolnomočilo posameznike glede obdelave njihovih osebnih podatkov (Crain, 2016, str. 4). Crain (2016) zelo kritično dojema pozive in iniciative ameriškega regulatorja k večji preglednosti industrije trgovcev s podatki, ki naj bi pomenila rešitev dane situacije, v kateri trpijo pravice posameznikov in meni, da v tej industriji prevladuje asimetrija zasebnosti. Avtor se kritično sooči z miselnostjo, da naj bi večja seznanjenost potrošnikov s praksami obdelave njihovih osebnih podatkov pomenila tudi njihovo opolnomočenje, saj lahko z vedenjem o teh praksah nanje vplivajo in tako sami zavarujejo svoje interese, če tako želijo. Informiranje posameznikov naj bi bil eden bistvenih stebrov liberalno demokratičnih vrednot in predpogoj za svobodo odločanja o stvareh, ki zadevajo posameznika. Avtor pa nasprotno zagovarja, da zgolj informiranost v pogojih, v katerih operirajo trgovci s podatki nikakor ni zadostna, saj naleti na nepremostljive strukturalne omejitve v smislu politične ekonomije trgovcev s podatki. Ti namreč ne morejo prepustiti nadzora nad zbranimi podatki, ki so bistvo njihovega poslovnega modela, posameznikom, ne da bi zato morali popolnoma spremeniti svoje načine poslovanja. Crain (2016) meni, da v srcu problematike nesorazmerja moči med posameznikom i trgovci s podatki leži komodifikacija osebnih podatkov, te pa ni mogoče odpraviti ali popraviti s strategijami, ki temeljijo le na boljši informiranosti posameznikov (Crain, 2016, str. 2).

V svojem prispevku analizira odziv enega od trgovcev s podatki na priporočila in pozive FTC po večji transparentnosti ter po omejevanju zbiranja osebnih podatkov in ugotavlja, da po eni strani struktura in načini poslovanja industrije sami po sebi omejujejo njeno preglednost, saj so to podjetja, ki niso v neposrednem stiku s posamezniki. Po drugi strani pa trgovci s podatki uporabijo sporočila o preglednosti v svojih odzivih pri odnosih z javnostmi in tako odganjajo poskuse strožje zunanje regulacije pod krinko spoštovanja svobodne izbire informiranega

87 Consumer Privacy Protection Act (2011, 2015), Commercial Privacy Bill of Rights Act (2011, 2014), in Data Broker Accountability and Transparency Act (2014).

posameznika. Na zunaj tako ustvarjajo videz reforme svojih praks, medtem ko ostajajo razmerja moči pravzaprav nespremenjena (Crain, 2016, str. 2).

Kot odziv na pritiske po strožji regulaciji komercialnega nadzora so mnogi trgovci s podatki sprejeli ukrepe glede seznanjanja posameznikov z njihovimi praksami. Acxiom je leta 2013 npr. uvedel portal About The Data, na katerem lahko posameznik preveri, katere njegove podatke ima podjetje in do določene mere upravlja z njimi. Podatki so razdeljeni po kategorijah in lahko za posameznika razkrijejo tudi do sto delcev podatkov: demografskih, poklicnih, zgodovino nakupov, prihodek, kredit, lastništvo nepremičnin, spletne aktivnosti. Nekatere vrste obdelave lahko uporabnik zavrne. V prvem mesecu naj bi portal obiskalo kar 500.000 obiskovalcev (Watson, 2014, v Crain, 2016, str. 6), vendar Crain prav na primeru tega portala oblikuje svojo kritiko omejitev transparentnosti, zaradi česar ta ne vodi k večji odgovornosti trgovcev s podatki. Najprej izpostavlja, da je celostno informiranost posameznikov nemogoče doseči, saj je to v nasprotju s temeljnim poslovnim modelom trgovcev s podatki, ki temelji na asimetriji zasebnosti. Portal Acxioma tako razkrije uporabniku le do 125 tipov podatkov, ki jih o njem hrani, čeprav izjavlja, da hrani o posamezniku tudi do 3000 vnosov podatkov. Poleg tega ne poda jasnih informacij, od kje je bil določen podatek pridobljen in komu je bil posredovan. Za opise svojih aktivnosti v zvezi s podatki uporablja jezik, ki uporabnika pomirja in poenostavlja vprašanja – npr., »da pomaga pri ustvarjanju bolj relevantnega oglaševanja, da vas oglaševalci ne bombardirajo z oglasi za kolo, če ste Ferrari fan.«. Tak način izražanja je pogosto uporabljen tudi v politikah zasebnosti in zamegljuje razumevanje uporabnikov, zato naj bi bil portal zgolj del področja odnosov z javnostmi (Crain, 2016, str. 6).

Preigra tudi potencialno situacijo, v kateri bi portal moral razkriti vse te informacije, pri čemer obstaja veliko vprašanje težav, s katerimi bi se srečali posamezniki pri procesiranju tako obsežnih informacij, in ugotavlja, da tudi to ne bi pomagalo k večji odgovornosti trgovcev s podatki, saj je struktura industrije taka, da preprečuje transparentnost – mnogi trgovci npr. podatke kupujejo od drugih trgovcev, kar pomeni, da bi se sledi izvora podatkov hitro zakrile, poleg tega so načini analize teh podatkov poslovna skrivnost trgovca. Poslovne skrivnosti običajno varuje tudi zakonodaja, predvsem pa obstaja močan diskurz v obrambo poslovnih skrivnosti. Težava je torej tudi v tem, da trgovci s podatki sami nimajo nujno pregleda nad vsemi operacijami in destinacijami podatkov. Preglednost sama po sebi tako ne

prinaša rešitve, saj je poslovni model trgovcev s podatki inherentno nepregleden. Tako se v zadnjem času tudi v ZDA več govori o omejevanju namenov nadaljnje uporabe zbranih osebnih podatkov, da lahko posameznik pričakuje razumen obseg morebitne nadaljnje uporabe njegovih podatkov v drugih kontekstih, kot v tistem, za katerega so bili zbrani, in da se upošteva t. i. kontekstualna integriteta (Nissenbaum, 2010) in se o posamezniku za določen namen zbirajo in uporabljajo enaki podatki, če npr. posluje z banko online, pri okencu ali na bankomatu. Prav tu pa leži srž problematike trgovcev s podatki, saj ti vedno obdelujejo osebne podatke za drugačne namene od prvotnih in v situacijah, ki posamezniku niso vnaprej znane, in je to bistveno za njihovo delovanje (Crain, 2016, str. 7–8).

Druga omejitev, ki jo vidi Crain v poudarjanju preglednosti pa je, da je namen tega pravzaprav odganjanje iniciativ po strožji zakonski regulaciji in politični cilj nadaljevanje komercialnega nadzora s čim manj omejitvami. Na področju trženja in vse bolj ekstenzivnega zbiranja podatkov za ta namen na internetu so se iniciative po strožji regulaciji začele pojavljati že v 90-ih letih prejšnjega stoletja, vendar je industrija kmalu ustanovila različna cehovska združenja, ki so s poudarjanjem pomembnosti samoregulacije in obveščenosti posameznikov učinkovito odganjala poskuse omejevanja te hitro rastoče industrije. Ko je industrija pričela kombinirati podatke, zbrane na spletu in izven, in so se pojavili močnejši pritiski k omejevanju teh praks, je industrija pričel ponujati možnost zavrnitve take obdelave osebnih podatkov in so nastala mnoga *opt-out* orodja, ki pa so zelo omejeno učinkovita in v resnici nimajo posebnega vpliva na varovanje pravic posameznikov. Kljub temu pa je ideja *opt-out* možnosti, izbire potrošnikov in preglednosti postala dovolj močna, da je preglasila možnosti strožjih ureditev in se industrija trgovanja s podatki lahko razvija naprej (Crain, 2016, str. 8–9).

Priloga F: Vedenjsko oglaševanje na digitalni TV

Ameriški regulator FTC je leta 2017 sklenil poravnavo s ponudnikom Vizio, ki je brez ustreznega obvestila in privolitve sledil, kaj gledajo njegovi uporabniki in te podatke obdeloval za namen ciljnega oglaševanja. Leta 20014 je Vizio uvedel pametne televizije, ki so avtomatično sledile, kaj uporabniki gledajo in podatke prenašale nazaj ponudniku. Starejše modele svojih televizij je preko oddaljenih nastavitev posodobil, vse to brez vednosti in strinjanja uporabnikov. Pametne televizije so beležile podatke na ravni sekunde in zajele, kaj je uporabnik gledal preko kabelske povezave ali internetne povezave, preko pretočnih storitev, DVD predvajalnikov. Podatke o gledalskih navadah milijonov uporabnikov je nato Vizio prodal oglaševalcem in drugim subjektom. Preprodajalcem podatkov je posredoval njihove IP naslove, da so lahko preko kombiniranja s svojimi bazami identificirali posamezne uporabnike. Pogodbenim partnerjem je sicer prepovedal identifikacijo uporabnikov po imenu, lahko pa so uporabili druge kategorije kot je spol, starost, izobrazba, itd. Vizio je dovolil, da se uporabnikom sledi in jim dostavlja oglase na različnih napravah (Fair, 2017). Epilog zgodbe je poravnava Vizio s FTC, v katerem se je kršitelj strinjal s plačilom 2,2 milijona dolarjev, ker je spremljal gledalske podatke 11 milijonov gledalcev brez njihove vednosti ali privolitve. FTC je od njega zahteval tudi, da jasno obvesti uporabnike in pridobi njihove izrecne privolitve za svoje praske obdelave in posredovanja podatkov ter izbriše vse podatke pridobljene pred 1. marcem 2016. Implementirati mora celostni program varovanja osebnih podatkov in redne ocene tega programa (Fair, 2017).

Podoben primer, vendar z manj ekstenzivno obdelavo osebnih podatkov, je obravnaval nizozemski nadzorni organ za varstvo osebnih podatkov in sicer ponudnika digitalne televizije Ziggo, enega največjih ponudnikov na Nizozemskem, ki je zbiral in obdeloval osebne podatke naročnikov, ne da bi jih ustrezno obvestil o tem in pridobil njihovo soglasje. Podatke je uporabil za izdelavo statistik gledanosti, poleg tega pa je nadzoroval uporabo svoje storitve videa na zahtevo, da je lahko naročnikom ponujal ciljno prilagojene vsebine ter podatke obdeloval za namen neposrednega trženja. Nadzorni organ je poudaril, da podatki o gledalskih navadah razkrivajo navade in interese naročnikov in so lahko tudi občutljive narave (npr. razkrivajo spolno usmerjenost). Po izvedenem nadzoru je Ziggo spremenil svoje prakse in pričel ustrezno obveščati uporabnike o obdelavi osebnih podatkov ter pridobivati njihove privolitve, implementiral je anonimizacijske ukrepe, s katerimi podatki o gledanosti

ne morejo biti več povezani s posameznim uporabnikom (Fouad, 2015). Tudi slovenski nadzorni organ, Informacijski pooblaščenec, je skupaj z regulatorjem elektronskih komunikacij[88] izdal Stališče o obdelavi osebnih podatkov s strani operaterjev digitalne televizije, ki poudarja pomen privolitve uporabnika pri uporabi podatkov za namen personaliziranih vsebin in oglasov ter ustrezne obveščenosti, pa tudi anonimizacijskih ukrepov (IP, 2017).

[88] Agencija za komunikacijska omrežja RS

Priloga G: Cambridge Analytica, Facebook in Brexit referendum

V Združenem kraljestvu je nadzorni organ za varstvo osebnih podatkov (ICO) preiskavo uporae podatkovne analitike v okviru referenduma o izstopu Združenega Kraljestva iz EU usmeril na mnoge subjekte, ki so bili povezani z dejavnostmi Cambridge Analytice ter političnimi kampanjami, in sicer na družbena omrežja, preprodajalce podatkov, ponudnike analitike, akademske institucije, politične stranke in kampanje, pri čemer so bili nekateri teh subjektov iz tretjih držav (ICO, 2018a, 7).

Cambridge Analytica je uporabila podatke uporabnikov Facebooka za to, da je na njih izvedla psihografsko tehniko ocenjevanja osebnosti po metodi OCEAN[89], katere rezultati naj bi omogočili vplivanje na vedenje volivcev. To tehniko so razvijali raziskovalci na univerzi Cambridge[90], ki so, seveda le za raziskovalne namene, analizirali podatke uporabnikov spletih družbenih omrežij, tudi s pomočjo aplikacij, kakršna je bila uporabljena tudi v tem primeru (Rosenberg in Frenkel, 2018). Psihografske tehnike so bile v trženju uporabljene že v zgodovini, za namen ocenjevanja specifičnih osebnosti, stališč in vrednot ter interesov potrošnikov. Potrošniki so reševali vprašalnike oziroma na drugačen način sami prispevali podatke raziskovalcu. Danes je psihografske analize mogoče opraviti na digitalnih podatkih, velikem podatkovju, ki je dostopno na spletu. Ena od metod, uporabljena tudi v primeru Cambridge Analytica, je, da posamezniki rešijo spletni vprašalnik, potem pa se ti podatki uparijo z drugimi podatki, na voljo raziskovalcu – bodisi iz spletnih družbenih omrežij, zgodovine brskanja, itd. Podatki uporabnikov Facebooka so bili v primeru Cambridge Analytica pridobljeni preko Facebook aplikacije thisisyourdigitallife, v kateri so ti za majhno plačilo rešili osebnostni vprašalnik, pri tem pa je aplikacija (skladno s takratnimi pravili in pooblastili omrežja Facebook) pridobila določene podatke s profila uporabnika, ki je rešil kviz in s profilov njegovih prijateljev. Pooblastilo, da lahko aplikacije privzeto dostopajo tudi do podatkov prijateljev uporabnikov aplikacije je Facebook že ukinil. Facebook je množično zbiranje podatkov uporabnikov zaznal že leta 2015 in sčasoma odvzel aplikaciji, ki je bila za to uporabljena, dostop do podatkov, pa vendar o tem pridobivanju podatkov ni obvestil uporabnikov. Niti ni preverjal, za kakšne namene se zbirajo ti podatki (Demos, 2018, 20–22, ICO 2018a).

[89] več v ICO 2018a, 18.
[90] Cambridge University Psychometric Centre

Priloga H: Priporočila ICO glede politik obdelave osebnih podatkov v političnih kampanjah

Priporočila ICO glede politik obdelave osebnih podatkov v političnih kampanjah: (1) Politične stranke bi morale sodelovati z ICO, volilno komisijo in vlado, da bi ustvarile in implementirale rešitve za večjo preglednost rabe podatkov v političnih kampanjah. (2) Vsi ti deležniki bi morali pred naslednjimi volitvami izvesti kampanjo ozaveščanja o varstvu osebnih podatkov, da se dvigne zaupanje volivcev v prakse obdelave osebnih podatkov. (3) Politične stranke morajo skrbno presoditi, ali ponudniki storitev, ki jih najamejo za obdelavo osebnih podatkov volivcev spoštujejo zakonodajo – predvsem, ali so pridobili soglasja posameznikov za obdelavo osebnih podatkov in ali so bili posamezniki ustrezno obveščeni o obdelavi osebnih podatkov.(4) Zakonodajalec bi moral določiti, da se sprejeme poseben kodeks o uporabi osebnih podatkov za politične namene in pri tem sodelovati z ICO. (10) Zakonodajalec bi moral oceniti potrebo po regulaciji vsebine političnega oglaševanja – tudi v smislu zahtev, da se politično oglaševanje lahko arhivira in izvede nadzor, če je to potrebno. (5) Po referendumskih kampanjah bi morale biti opravljene revizije s strani zaupanja vrednih tretjih strank, da so bili podatki izbrisani oziroma so bile za nadaljnjo rabo pridobljene privolitve posameznikov. (6) Opravljena bi morala biti etična diskusija glede vpliva, ki ga imajo nove tehnologije in sofisticirana analitika podatkov v političnih kampanjah. (7)Vse platforme, ki ponujajo oglaševalske storitve političnim strankam in kampanjam bi morale klientom pojasniti in svetovati glede preglednosti in odgovornosti v primeru rabe podatkov za politične namene. (9) Prav tako bi morale izboljšati svoja orodja za preglednost pri političnem oglaševanju in se pri tem posvetovati z ICO in volilno komisijo.(8) ICO bo to temo preiskoval tudi v prihodnje in pri tem sodeloval z drugimi EU nadzornimi organi ter EDPB (ICO, 2018b, str. 4–6).

Priloga I: Priporočila Evropskega nadzornika za varstvo podatkov

Evropski nadzornik za varstvo podatkov meni, da je ključna dopolnitev veljavne zakonodaje s sprejemom ePR in dosledno izvajanje zakonodaje o varstvu osebnih podatkov ter sodelovanje nadzornih organov pri skupni diagnozi glede stanja na področju političnega mikro-ciljanja in manipulacije in načinih za omejitev negativnih posledic. Nujno je sodelovanje organov s področja varstva osebnih podatkov, varuhov konkurence, volilnih komisij, varuhov

potrošniških pravic, pa tudi regulatorjev na področju elektronskih komunikacij, ki bedijo nad pravili za javne RTV servise in avdio-vizualna dela. EDPS priporoča spodbujanje nastanka samo-regulacijskih kodeksov specifično za področje političnega mikro-ciljanja in manipulacije ter poudarja pomembnost opolnomočenja posameznikov, preko dvigovanja preglednosti in obveščanja ter preko spodbujanja implementacije tehnologij, ki bi uporabnikom omogočala lažjo prepoznavo spornih praks ciljanja. Posameznikom morajo biti na voljo pravne možnosti, da svoje pravice uveljavljajo pred pristojnimi organi, kar je zaradi inherentne prikritosti aktivnosti mikro-ciljanja lahko kompleksno. Koristne bi bile možnosti skupnih tožb prizadetih posameznikov (EDPS, 2018, str. 18-22).

Priloga J: Vprašalnik za intervjuje

Prvi sklop je zadeval vlogo vedenjskega oglaševanja v industriji in družbi in njegove prednosti. Ključne so bile razlike prednostmi in slabostmi za manjše akterje na trgu in večje.

- Kako razvoj vedenjskega oglaševanja v elektronskem komuniciranju vpliva na industrijo, uporabnike in širšo družbo (v smislu prihodkov, konkurence, razvoja inovativnih produktov in storitev, rešitev)?
- Kakšen je vpliv vedenjskega oglaševanja na različne akterje v elektronskem komuniciranju: izdajatelje, oglaševalske mreže in oglaševalske vmesnike, iskalnike, ponudnike dostopa do interneta in povezane organizacije, mala in srednje velika podjetja, velike multi-nacionalne korporacije?
- Katere so prednosti za manjše/večje izdajatelje in za velike ponudnike sistemov vedenjskega oglaševanja (družbena omrežja, iskalniki, spletne trgovine)?
- Kakšna je vloga novih akterjev: preprodajalcev podatkov, ponudnikov programatičnega oglaševanja, sledenja na javnih krajih (WiFi slednje)?
- V kolikšni meri vedenjsko oglaševanje prinaša prednosti uporabnikom storitev in spleta? Kakšen je pomen personalizacije vsebine in profiliranja v smislu uporabniške izkušnje s prilagojenimi vsebinami?

Drugi sklop vprašanj se je nanašal predvsem na vpliv vedenjskega oglaševanja na pravice uporabnikov do zasebnosti in varstva osebnih podatkov, pa tudi do enake obravnave in ne-diskriminacije ter druge potrošniške pravice:

- Kako vedenjsko oglaševanje vpliva na zasebnost in varstvo osebnih pravic posameznikov, tudi z vidika obdelave občutljivih osebnih podatkov, informiranosti o praksah vedenjskega oglaševanja, privolitve, hrambe njihovih podatkov in zavarovanja njihovih podatkov?
- Kakšen je vpliv vedenjskega oglaševanja in prevladujočih praks profiliranja ter uporabe algoritmov za odločanje na njihovo pravico do enake obravnave, posebej kadar diskriminacija vključuje različno obravnavo glede na občutljive kategorije podatkov (kot je rasna pripadnost, seksualna usmerjenost, politično prepričanje)?
- Kakšen je pomen t. i. mehurčkov, v katere so zaprti posamezniki (angl. filtre bubbles)
- Kakšna je vloga psevdonimnih podatkov in anonimizacije v varovanju zasebnosti posameznikov pri vedenjskem oglaševanju?

— V kolikšni meri imajo posamezniki znanje in vedenje o vedenjskem oglaševanju in načinih zaščite pred profiliranjem in sledenjem? V kolikšni meri lahko uveljavljajo svoje pravice?
— Kako učinkoviti so mehanizmi, ki so uporabnikom trenutno na voljo za varovanje zasebnosti?

Tretji sklop vprašanj se je nanašal na regulatorni okvir za vedenjsko oglaševanje: trenutni in predlagane rešitve za prihodnost, ki bi lahko bolje dosegale ravnovesje med vpletenimi interesi industrije in varovanja pravic posameznikov:

— Kakšen je trenutni pravni okvir za varovanje zasebnosti in varstvo osebnih podatkov v EU in ZDA? Kakšne so razlike med obema sistemoma?
— Kako se zakonodaja razvija: sprejem nove uredbe v EU in propadli poskusi federalne zakonodaje v ZDA?
— Kakšna je vloga zakonodaje, samoregulacije in standardizacije, ko-regulacije in regulacije s kodo?
— Kakšna je vloga privolitve v sistemih varovanja zasebnosti v EU in ZDA?
— Kakšne so izkušnje z regulacijo piškotkov in profiliranja v EU?Je skladnost s pravili na trgu večja?
— Kakšen vpliv ima na regulacijo vedenjskega oglaševanja konkurenčnost EU in ZDA? Kako na regulacijo vplivajo odnosi med regulatorji in drugimi prizadetimi deležniki v EU in ZDA?
— Kakšna naj bo regulacija vedenjskega oglaševanja v prihodnosti, da bi bolje pretehtala interese različnih deležnikov: vloga zakonodaje, samo regulacije, standardizacije, certificiranja, z vidika vprašanj privolitve, izobraževanja uporabnikov, novih poslovnih modelov v industriji (programatično oglaševanje), standarda »ne sledi«, ad blockerjev (PETs)? Kako naj bodo različna orodje povezana?
— V kolikšni meri je za uspešno regulacijo s katerim koli orodjem pomemben učinkovit nadzor in sankcioniranje?
— Kakšna je vloga nadzornih organov in s kakšnimi izzivi se soočajo zaradi tehnološko zahtevnega okolja in praks vedenjskega oglaševanja?

Priloga K: Direktiva 2002/58/ES in določbe o piškotkih

Direktiva 2002/58/ES ureja vprašanja zasebnosti pri uporabi elektronskih komunikacij in med drugim nalaga ponudnikom javno dostopnih elektronskih storitev, da morajo zagotavljati zaupnost komunikacij, opredeljuje, za kakšne namene smejo ti uporabljati prometne in lokacijske podatke uporabnikov elektronskih komunikacij, na kašne način se izdajajo imeniki, pod kakšnimi pogoji se elektronska pošta, SMS in MMS sporočila ter druge storitve elektronskih komunikacij smejo uporabljati za namen pošiljanja oglasnih sporočil, in druge teme, med njimi tudi uporabo piškotkov.

Ob razmahu uporabe piškotkov in podobnih tehnologij je bila Direktiva 2002/58/ES leta 2009 spremenjena z Direktivo 2009/136/ES in omejitve za uporabo teh tehnologij strožje zastavljene. Razlog za spremembo je bila vse večja zaskrbljenost glede posegov v zasebnost uporabnikov s pomočjo piškotkov in drugih tehnologij (npr. spletni svetilniki, odtis naprave ali brskalnika) na spletnih straneh. Te omogočajo sledenje uporabnikom in nosijo unikatno identifikacijsko oznako, na podlagi katere je uporabnika mogoče prepoznati med brskanjem po različnih spletnih straneh. Zakonodaja se je začela izvajati leta 2013.

Ključna za področje vedenjskega oglaševanja je določba o piškotkih in podobnih tehnologijah, ki omogočajo dostop do uporabnikove naprave in podatkov (Direktiva 2002/58/ES, 2009, 3. odstavek 5. člena):

> Države članice zagotovijo, da je shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika, dovoljeno samo pod pogojem, da je zadevni naročnik ali uporabnik v to privolil po tem, ko je bil jasno in izčrpno obveščen v skladu z Direktivo 95/46/ES, med drugim o namenih obdelave. To ne prepreči nobenega tehničnega shranjevanja ali dostopa izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja, ali, če je nujno potrebno, da ponudnik zagotovi storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahtevata.

Za razumevanje določil o piškotkih so pomembne tudi sledeče uvodne izjave:

> Terminalna oprema uporabnikov omrežij elektronskih komunikacij in vsak podatek, shranjen na taki opremi, sta del zasebnega področja uporabnikov, ki zahteva varstvo v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin. Tako imenovana vohunska programska oprema, program za prikriti nadzor računalnika, omrežni hrošči, skriti identifikatorji in druge podobne naprave lahko vdrejo v uporabnikov terminal brez njegove vednosti, da bi pridobili dostop do podatkov, shranili skrite podatke ali izsledili uporabnikove dejavnosti, in lahko resno motijo zasebnost teh uporabnikov. Uporaba takih naprav mora biti dovoljena samo za zakonite namene, z vednostjo prizadetih uporabnikov (Direktiva 2002/58/ES, 2009, 24. uvodna izjava).

> Vendar so lahko take naprave, na primer tako imenovani "piškotki", zakonito in uporabno orodje, na primer za ocenjevanje učinkovitosti zasnove spletne strani in oglaševanja ter za preverjanje identitete uporabnikov, vključenih v sprotne ("on-line") transakcije. Kadar so takšne naprave, na primer piškotki, namenjene za zakonito uporabo, kot je olajšati ponudbo storitev informacijske družbe, je treba njihovo uporabo dovoliti, pod pogojem da uporabniki prejmejo jasne in natančne podatke v skladu direktivo 95/46/ES o namenih piškotkov ali podobnih naprav, tako da je zagotovljeno, da so uporabniki seznanjeni s podatki, nameščenimi na terminalsko opremo, ki jo uporabljajo. Uporabnikom mora biti dana možnost, da zavrnejo shranitev piškotka ali podobne naprave na njihovo terminalsko opremo. To je zlasti pomembno takrat, kadar imajo uporabniki, ki niso izvirni uporabniki, dostop do te terminalske opreme in s tem do vseh podatkov, ki vsebujejo občutljive zasebne podatke, shranjene na taki opremi. Podatki za uporabo raznih naprav, ki naj bi se namestile na uporabnikovo terminalsko opremo, kot tudi pravica do zavrnitve teh naprav, se lahko ponudijo samo enkrat med isto zvezo in se nanašajo tudi na vsako morebitno nadaljnjo uporabo na podlagi teh naprav pri poznejših zvezah. Načini dajanja podatkov, zagotavljanja pravice do zavrnitve ali zahteve za privolitev morajo biti čim bolj uporabniško prijazni. Dostop do posebne vsebine na spletišču je še vedno lahko pogojen z dobro zavestnim sprejetjem piškotka ali podobne naprave, če se ta uporablja za zakonite namene (Direktiva 2002/58/ES, 2009, 25. uvodna izjava).
>
> Tretje strani si morebiti želijo shranjevati informacije o uporabnikovi opremi ali pridobiti dostop do že shranjenih podatkov iz najrazličnejših razlogov, ki zajemajo vse od legitimnih namenov (na primer določene vrste piškotkov) do tistih, ki obsegajo neupravičen vdor v zasebnost (na primer vohunska programska oprema ali virusi). Zato je izjemno pomembno, da so uporabniki jasno in izčrpno obveščeni pri vseh dejavnostih, ko bi lahko prišlo do takšnega shranjevanja ali dostopanja. Načini obveščanja in zagotavljanja pravice do zavrnitve bi morali biti čim bolj uporabniško prijazni. Izjeme glede obveznosti obveščanja in zagotavljanja pravice do zavrnitve bi morale biti omejena na primere, ko je tehnično shranjevanje ali dostop nujno potreben za legitimni namen omogočanja uporabe posebne storitve, ki jo je izrecno zahteval naročnik ali uporabnik. Uporabnikovo privolitev, da se strinja z obdelavo, je mogoče izraziti z uporabo ustreznih nastavitev v brskalniku ali drugih aplikacijah, in sicer v primeru, da je to tehnično izvedljivo in učinkovito ter v skladu z ustreznimi določbami Direktive 95/46/ES. Uveljavljanje teh zahtev bi moralo postati učinkovitejše, in sicer s podelitvijo večjih pooblastili ustreznim nacionalnim organom (Direktiva 2002/58/ES, 2009, 66. uvodna izjava).

3. odstavek 5. člena Direktive 2002/58/ES dopušča shranjevanje podatkov ali pridobitev dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika le po tem, ko je bil ta ustrezno obveščen in v to privolil. Določba je tehnološko nevtralna, zato se ne uporablja samo za piškotke, ampak tudi za vsako drugo tehnologijo, ki se uporablja za shranjevanje podatkov v terminalski opremi posameznika in dostopanje do njih (tudi vohunska in zlonamerna programska oprema itd.). Vnaprejšnja privolitev v prejemanje piškotkov in podobnih tehnologij ni potrebna, če ti izpolnjujejo eno od naslednjih meril:

— Merilo A: piškotek oz. druga podobna tehnologija se uporablja „izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja“;

— Merilo B: piškotek oz. druga podobna tehnologija je „nujno potreben, da ponudnik zagotovi storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahtevata“ (WP29, 2012, str. 1).

Delovna skupina iz člena 29 obravnava različne primere piškotkov, za katere veljata navedeni izjemi. Ob tem opozarja tudi na čas trajanja piškotka in opozarja, da mora biti ta pri piškotku, ki je izvzet iz zahteve po soglasju, neposredno povezan z namenom, za katerega se uporablja, in mora biti nastavljen tako, da poteče takoj, ko ni več potreben (WP29, 2012, str. 5). Piškotke tretjih strank *(angl. third party cookie)* razume kot tiste piškotke, ki jih določijo upravljavci podatkov, ki ne upravljajo spletne strani, ki si jo uporabnik trenutno ogleduje. Nasprotno, izraz piškotek ponudnika *(angl. first party cookie)* uporablja za piškotek, ki ga določi upravljavec podatkov (ali kateri koli od pooblaščenih obdelovalcev), ki upravlja spletno stran, ki si jo trenutno ogleduje uporabnik, glede na spletni naslov, ki je običajno prikazan v naslovni vrstici brskalnika. Poleg tega poudarja, da piškotki *tretjih strank* običajno niso „nujno potrebni“ za uporabnika, ki si ogleduje spletno stran, saj so ti piškotki običajno povezani s storitvijo, ki se razlikuje od storitve, ki jo je uporabnik „izrecno zahteval“. Veliko verjetneje je torej, da bodo iz zahteve po soglasju izvzeti sejni piškotki ponudnika kot pa trajni piškotki tretjih strank (WP29, 2012, str. 4–5).

Primeri piškotkov, pri katerih ni potrebna privolitev uporabnika:

— Piškotki za pravilen pretok zahtev (angl. *load balancing*). Podatki v piškotku so namenjeni izključno identifikaciji ene od končnih točk komunikacije (enega od strežnikov v skupini), zato mora komunikacija nujno potekati prek omrežja. Za take piškotke po mnenju Delovne skupine iz člena 29 ni potrebno soglasje v skladu z merilom A (WP29, 2012, str. 7–8).
— Piškotki, povezani z vnosi uporabnika: so sejni piškotki, s katerimi si spletno mesto lahko zapomni uporabnikove vnose v spletne obrazce, artikle, ki jih je predal v nakupovalno košarico, ipd. V tem primeru uporabnik jasno izrazi željo po storitvi s tem, da klikne na gumb »dodaj v košarico« ali podobno. Taki piškotki so izvzeti po kriteriju B (WP29, 2012, str. 5; IP, 2013, str. 9).
— Piškotki za avtentikacijo uporabnika: so namenjeni prepoznavi uporabnika potem, ko se je prijavil v določeno storitev (npr. spletna banka, storitve, kjer se uporabnik vpiše s svojim uporabniškim imenom in geslom...). Piškotek je potreben, da uporabnik

pridobi dostop do določene vsebine. V nasprotnem primeru bi se moral vpisati na vsaki pod-strani spletnega mesta. Tak piškotek je izvzet glede na merilo B (WP29 2012, 6; IP 2013, 9).

— Piškotki, ki so potrebni zaradi varnosti in zavarovanja: taki piškotki npr. zaznavajo napačne vpise in tako preprečujejo zlorabe sistemov za vpisovanje in registracijo. Običajno imajo daljši rok trajanja, prav zaradi svojega namena. Podobno kot pri piškotkih za avtentikacijo, gre tu za izjemo po merilu B (WP29, 2012, str. 7).

— Piškotki, ki omogočajo predvajanje multi-medijskih vsebin: ti so potrebni zato, da se predvaja video ali avdio vsebina na spletnem mestu. Namenjeni so shranjevanju tehničnih podatkov, kot so parametri za kakovost slike, hitrost omrežne povezave in medpomnjenje. Ko je vsebina predvajana, naj bi takemu piškotku prenehal rok trajanja, saj ni več potreben za izvedbo storitve. Izvzet je po kriteriju B. Če se piškotek uporablja še za kak drug namen, ne more več veljati izjema (WP29, 2012, str. 7).

— Piškotki za prilagoditev nastavitev uporabnikovim željam (za nastavitve jezika ali npr. način razvrščanja rezultatov/vsebine (število zadetkov na strani, ipd.). Ker uporabnik tako zahtevo nedvomno izrazi z izborom določenega ukaza in brez piškotka tega ni moč izvesti, gre tu za izjemo po merilu B. Če spletno mesto uporablja trajne piškotke, ki ne prenehajo po koncu seje, pa mora biti uporabnik o tem posebej obveščen ob izbiri določene preference (WP29, 2012, str. 8).

— Piškotki vtičnikov družbenih omrežij (angl. *social media plug-ins*): družbena omrežja omogočajo spletnim mestom, da v svojo vsebino integrirajo njihove vtičnike – tako lahko uporabniki delijo vsebine s svojimi prijatelji. Vtičniki temeljijo na piškotkih, tako da lahko družbena omrežja identificirajo svoje člane, ko ti pridejo na spletno mesto z vtičnikom. Glede na pojasnila Delovne skupine iz člena 29 lahko take piškotke razumemo kot izjemo le pri uporabnikih, ki so prijavljeni v družbeno omrežje in hkrati obiščejo tudi druga spletna mesta, ki vsebujejo vtičnike, na podlagi merila B. Piškotek mora prenehati, ko se uporabnik izpiše iz omrežja. Pri uporabnikih, ki niso prijavljeni v družbeno omrežje, ali sploh niso člani, takih piškotkov ni mogoče šteti kot izjemo. Za nalaganje piškotkov s strani vtičnikov je potrebno soglasje teh uporabnikov (WP29 2012, 9; IP 2013, 9).

Kjer ni mogoče govoriti o enem izmed meril, opisnih zgoraj, je za piškotek treba pridobiti soglasje uporabnika. Privolitev je tako potrebna v naslednjih primerih:

1. Piškotki, ki omogočajo boljše funkcionalnosti, boljše delovanje spletnega mesta in boljšo uporabniško izkušnjo, pa niso nujno potrebni, da se izvede neka storitev, ne spadajo med izjeme in mora torej ponudnik pridobiti privolitev uporabnika. Primer je npr. piškotek, s katerim je zaznana lokacija uporabnika, da spletno mesto deluje v njem znanem jeziku, pa uporabnik tega ni posebej zahteval (IP, 2013, str. 10).

2. Piškotki za analiziranje prometa (npr. za štetje obiskovalcev, identifikacijo brskalnikov in ključnih besed, ki vodijo na mesto, za zaznavanje problemov pri navigaciji) so na spletnih mestih zelo pogosti in za dobro delovanje tudi zelo pomembni, vendar pa ne izpolnjujejo nobenega od kriterijev, ki jih izpostavlja Delovna skupine iz člena 29 in jih tako ni mogoče šteti za izjeme, kar pomeni, da mora spletno mesto uporabnika o njih obvestiti in pridobiti njihovo privolitev (WP29, 2012, str. 10). Invazivnost analitičnih piškotkov je različna. Če spletno mesto s svojimi lastnimi piškotki analizira svoje delovanje, analitični piškotki ne pomenijo nesorazmernega posega v zasebnost uporabnikov. Lahko pa spletno mesto uporablja tudi storitev pogodbenega partnerja – izvajalca analitike[91]. Če partner zbranih podatkov ne uporablja za svoje namene, je uporaba piškotkov še vedno relativno ne-invazivna. Če pa zunanji ponudnik zbrane podatke uporablja tudi za svoje lastne namene (npr. izvaja analitiko na različnih spletnih mestih, podatke pa kombinira in uporablja za namen svojega lastnega produkta), to pomeni večji poseg v zasebnost uporabnika, saj ponudnik take analitike lahko sledi določenemu uporabniku preko vseh spletnih strani, ki uporabljajo tak produkt (IP, 2013, str. 10; WP29, 2012, str. 10).

3. Piškotkov vtičnikov družbenih omrežij, s katerimi lahko ponudnik uporabniku sledi preko različnih spletnih strani ni mogoče šteti za „nujno potrebne“ za zagotavljanje možnosti, ki jih izrecno zahteva uporabnik, zato ti sledilni piškotki ne morejo biti izvzeti v smislu merila B. Brez privolitve ponudniki družbenih omrežij ne smejo obdelovati podatkov posameznikov, ki niso člani omrežja. Socialni vtičniki torej ne bi smeli privzeto uporabljati piškotkov tretjih strank na straneh, prikazanih nečlanom (WP29, 2012, str. 9).

4. Oglaševalske piškotke lahko naloži obiskano spletno mesto (*first party*) ali pa prihajajo s strani tretjih (oglaševalske mreže, partnerske spletne strani, ponudniki storitev (*third party*). To so piškotki za namen omejevanja števila prikazovanja oglasov (*frequency capping*),

91 Kot npr. Google Analytics, Piwik, itd.

zaznavanje prevar pri klikanju (*click fraud*), raziskave in marketinške analize, izboljšave produkta glede na podatke o uporabi, piškotki za razlikovanje cen glede na profil uporabnika in prilagajanje vsebine glede na profil (IP, 2013, str. 10). Še posebej so ti piškotki invazivni za zasebnost posameznika, kadar jih naloži tretja stranka, ki lahko spremlja aktivnost uporabnika preko različnih spletnih strani, npr. oglaševalska mreža. Za uporabo takih piškotkov je potrebna privolitev uporabnika, saj nobenega od teh namenov ni mogoče šteti za povezanega s storitvijo ali možnostjo storitve informacijske družbe, ki jo izrecno zahteva uporabnik, v skladu z merilom B (WP29, 2012, str. 10).

Priloga L: Več o Splošni uredbi za varstvo osebnih podatkov

Evropska komisija je prvi predlog Uredbe 2016/679 objavila že v začetku leta 2012. Temeljil je na določbah Direktive 95/46/ES, vendar bolj jasno določil nekatere pojme in prakse, pravice posameznikov, obveznosti upravljavcev in pristojnosti nadzornih organov. Cilj prenove pravnega okvira naj bi večja odgovornost upravljavcev in tudi strožje omejitve pri obdelavi osebnih podatkov posameznikov pri spletnih storitvah. Objavi so sledila leta intenzivnih pritiskov industrije, za katero naj bi odslej veljali strožji standardi, in diskusij o vplivu višje ravni varstva osebnih podatkov posameznikov na ekonomske kazalce in konkurenčnost tehnološke industrije v EU, katere gorivo so vse pogosteje uporabniški podatki, njihova analiza in uporaba. Končni, kompromisni tekst uredbe, tako ne glede na višje standarde v nekaterih delih raven varstva osebnih podatkov v drugih delih niža, saj dopušča denimo širjenje namenov obdelave osebnih podatkov (Burnik, 2016a).

Uredba 2016/679 vzpostavlja ureditveni okvir za zagotovitev ravnovesja med visoko ravnjo varstva zasebnosti posameznika in prostim pretokom osebnih podatkov v okviru Evropske unije (EU). Uporablja se v primeru obdelave osebnih podatkov z avtomatskimi sredstvi (na primer informacijsko bazo podatkov strank) in podatkov, ki so vsebovani ali se pojavljajo v zbirki, ki ni avtomatska (tradicionalne papirne zbirke). Njen cilj je zaščititi pravice in svoboščine posameznikov glede obdelave njihovih osebnih podatkov z določitvijo ključnih meril za zakonitost obdelave in načel kakovosti podatkov.

Oseba, katere podatki se obdelujejo, posameznik, na katerega se nanašajo osebni podatki, ima po Uredbi 2016/679 naslednje pravice:

- pravica do pridobitve informacij o obdelavi osebnih podatkov: upravljavec mora posamezniku, na katerega se osebni podatki nanašajo, zagotoviti določen informacije (istovetnost upravljavca, nameni obdelave podatkov, prejemniki podatkov itd.) (12., 13. in 14. člen);
- pravica do dostopa do podatkov: vsakemu posamezniku, na katerega se nanašajo osebni podatki, je zajamčena pravica, da pridobi od upravljavca informacije o obdelavi svojih podatkov (15. člen);
- pravica posameznika do popravka netočnih podatkov (16. člen) in izbrisa (pravica do pozabe) (17. člen), ter pravica do omejitve obdelave osebnih podatkov (18. člen);

— pravica do prenosljivosti podatkov od enega upravljava k drugemu (20. člen),
— pravica posameznika, na katerega se nanašajo osebni podatki, do ugovora v primeru avtomatiziranega sprejemanja odločitev in neposrednega trženja (21. člen).

Pomemben vidik obdelave osebnih podatkov je tudi zagotavljanje njihovega zavarovanja pred uničenjem, izgubo ali nepooblaščenim dostopom in varovanje njihove zaupnosti in poročanja v primeru incidentov (Uredba 2016/679, 32., 33., 34. člen). Uredba naj bi prispevala k boljšemu zavarovanju podatkov, tako da spodbuja uporabo tehnologij, ki varujejo zasebnost podatkov z minimiziranjem shranjevanja osebnih podatkov in udejanja koncepta vgrajenega in privzetega varstva podatkov (Uredba 2016/679, 25. člen) ter uvaja splošno obveznost za upravljavce podatkov, da organe za varstvo podatkov in posameznike nemudoma obvestijo o kršitvah zavarovanja podatkov.

Upravljavci osebnih podatkov bodo morali izpolnjevati tudi nekatere nove zahteve. Kadar bo šlo za obdelavo podatkov, ki bi lahko pomenila veliko tveganje za pravice posameznika, bodo morali pripraviti oceno vplivov na varstvo osebnih podatkov (ang. *data protection impact assessment)* in se prej posvetovati z nadzornim organom (Uredba 2016/679, 33. člen). Novost so tudi visoke sankcije za prekrške – v nekaterih primerih bo lahko upravljavca doletela globa v višini štirih odstotkov letnega prometa (Uredba 2016/679, 79. člen) (Burnik 2016a).

Priloga M: Podrobneje o profiliranju

Profiliranje po Uredbi 2016/679 opredeljujejo trije elementi: (1.) mora biti avtomatizirana obdelava, (2.) mora biti izvedeno na osebni podatkih in (3.) cilj profiliranja mora biti ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom. Ocenjevanje osebnih vidikov implicira, da profiliranje vključuje neko vrsto ocene ali sodbe glede posameznika. To pomeni, da zgolj klasifikacija/segmentiranje posameznikov glede na znane značilnosti, kot so npr. starost, spol in višina, ne vodi nujno v profiliranje. Če je namen le razvrščanje in ni dodatnega koraka izpeljave nekega zaključka ali predikcije o posamezniku, taka segmentacija še ni profiliranje (WP29, 2017a, str.7). Za oblikovanje profilov veljajo pravila, ki urejajo obdelavo osebnih podatkov, na primer glede pravne podlage za obdelavo ali načela varstva podatkov (Uredba 2016/679, uvodno pojasnilo št. 72).

Strožje pogoje določa 22. člen Uredbe 2016/679 za posebne primere, in sicer, da ima posameznik, na katerega se nanašajo osebni podatki, pravico, da zanj ne velja odločitev, ki temelji (1) zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov, (2) ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva. Avtomatizirano sprejemanje posameznih odločitev je lahko končni rezultat profiliranja ali s profiliranjem delno sovpada. Avtomatizirano odločanje tako ne vključuje nujno profiliranja in ga ni moč enačiti z njim. Zgolj avtomatizirano odločanje pomeni, da je odločitev sprejeta izključno na podlagi tehničnih sredstev, brez intervencije človeka, glede na podatke, ki jih priskrbijo sami posamezniki (npr. v vprašalniku), podatke, ki so o posamezniku zbrani (npr. podatke o lokacijah, ki jih zbere aplikacija) ali podatke, ki izhajajo iz že ustvarjenega profila posameznika. (WP29, 2017a, str. 8).

Dodaten pogoj je, da ima zgolj avtomatizirana obdelava, vključno z oblikovanjem profilov pravne učinke v zvezi s posameznikom ali na podoben način nanj znatno vpliva. Primeri pravnih učinkov so npr. odpoved pogodbe, pridobitev ali zavrnitev določene podpore, ki jo opredeljuje zakon – npr. otroški dodatek, zavrnitev vstopa v državo ali državljanstva (WP29, 2017, str. 21). Primeri učinkov, ki na podoben način znantno vplivajo na posameznika, pa so posledica odločitve, ki pomembno zadevajo okoliščine, vedenje ali izbire, na voljo posamezniku, ki imajo dalj trajajoč ali stalen vpliv na posameznika ali vodijo v izključitev ali diskriminacijo, npr.: odločitev o kreditu, o dostopu do zdravstvenih storitev, o možnosti

zaposlitve, o dostopu do izobrazbe, npr. sprejemu na univerzo (WP29, 2017, str. 22). Taka obdelava podatkov in odločanje pomeni za posameznika tudi največje tveganje, zato so pogoji zanjo strožji. Primeri so avtomatska zavrnitev spletne prošnje za posojilo ali prakse zaposlovanja prek spleta brez človekovega posredovanja oziroma „oblikovanje profilov“ na podlagi katerih se ocenjuje in predvideva uspešnost pri delu, ekonomski položaj, zdravje, osebni okus ali interesi, zanesljivost ali vedenje, lokacija ali gibanje (Uredba 2016/679, uvodno pojasnilo št. 71).

Priloga N: Psevdonimni podatki

Uporabo psevdonimizacije Uredba 2016/679 obravnava kot način zagotavljanja vgrajene zasebnosti in jo priporoča (3b. odstavek 4. člena). V primeru vedenjskega oglaševanja upravljavci osebnih podatkov pogosto hranijo le identifikatorje piškotkov, naprav, ipd. na podlagi katerih ločijo med sabo različne posameznike, ne hranijo pa njihovih imen ali priimkov, naslova e-pošte in drugih podatkov. Identifikatorje bi tako lahko razumeli tudi kot psevdonimne podatke (Burnik, 2016a). Od predstavitve prvega predloga uredbe je bilo mogoče spremljati pritiske s strani spletne industrije, da bi psevdonimne podatke izvzeli iz obsega osebnih podatkov in torej zanje strogo varstvo ne bi veljalo, saj naj bi obdelava identifikatorjev, na podlagi katerih posameznika ni mogoče takoj prepoznati, pomenila le majhen poseg v njihovo zasebnost. Izvajalci vedenjskega oglaševanja tako ne bi obdelovali osebnih podatkov, zanje ne bi veljala obveza obveščanja posameznikov in pridobivanja njihove privolitve itd. (Zuiderveen Borgesius, 2014). Končno besedilo ni sledilo tem argumentom, pač pa je prepoznalo, da je sledenje posameznikom na podlagi identifikatorjev vse bolj prevladujoča dejavnost, ki ima lahko resen vpliv na zasebnost posameznika. Stalno spremljanje spletnih aktivnosti nekoga lahko pomeni ustvarjanje obsežnega profila o njem ter izrabo teh podatkov za vplivanje nanj (s prilagajanjem oglasov, ponudbe, tudi cene). Psevdonimizacija tako nastopa kot orodje za boljše zavarovanje osebnih podatkov, ne pa kot olajševalna okoliščina, pri kateri upravljavcem ne bi bilo treba spoštovati pravil o obveščanju posameznikov in upoštevanju določb glede pravnih podlag.

Priloga O: Obveščanje posameznika po Uredbi 2016/679

Tabela O: Obveščanje posameznika po Uredbi 2016/679

	13. člen – podatki so zbrani neposredno od posameznika	14. člen – podatki niso zbrani neposredno od posameznika
Identiteta in kontaktni podatki upravljavca in njegovega predstavnika, kadar ta obstaja	Člen 13(1)(a)	Člen 14(1)(a)
Kontaktni podatki pooblaščene osebe za varstvo podatkov, kadar ta obstaja	Člen 13(1)(b)	Člen 14(1)(b)
Namen in pravna podlaga za obdelave	Člen 13(1)(c)	Člen 14(1)(c)
Zakoniti interesi, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba, kadar pravno podlago za obdelavo predstavljajo zakoniti interesi	Člen 13(1)(d)	Člen 14(2)(b)
Vrsta zadevnih osebnih podatkov	Se ne zahteva	Člen 14(1)(d)
Uporabniki (ali kategorije uporabnikov) osebnih podatkov	Člen 13(1)(e)	Člen 14(1)(e)
Informacije o dejstvu, da se podatki prenašajo v tretje države, podrobnosti o prenosih in podrobnosti o ustreznih zaščitnih ukrepih (vključno z obstojem ali neobstojem sklepa Komisije o ustreznosti), sredstvih za pridobitev njihove kopije ali informacije o tem, kje so na voljo	Člen 13(1)(f)	Člen 14(1)(f)
Dodatne informacije, ki so potrebne za zagotovitev poštene in pregledne obdelave		
Obdobje hrambe (ali, če to ni mogoče, merila, ki se uporabijo za določitev tega obdobja)	Člen 13(2)(a)	Člen 14(2)(a)
Pravice posameznika, na katerega se osebni podatki nanašajo, do: • dostopa; • popravka; • izbrisa; • omejitve obdelave; • ugovora obdelavi in • prenosljivosti	Člen 13(2)(b)	Člen 14(2)(c)
Kadar obdelava temelji na privolitvi (ali izrecni privolitvi), pravica, da se privolitev kadar koli prekliče	Člen 13(2)(c)	Člen 14(2)(e)
Pravica do vložitve pritožbe pri nadzornem organu	Člen 13(2)(d)	Člen 14(2)(e)
Ali je zagotovitev podatkov zakonsko določena ali pogodbena obveznost ali potrebna za sklenitev pogodbe ter ali velja obveznost zagotoviti podatke in morebitne posledice, če se podatki ne zagotovijo	Člen 13(2)(e)	Se ne zahteva
Vir osebnih podatkov in po potrebi, ali izvirajo iz javno dostopnega vira	Se ne zahteva	Člen 14(2)(f)
Obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov, po potrebi pa tudi smiselne informacije o razlogih zanj ter pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki	Člen 13(2)(f)	Člen 14(2)(g)

Vir: povzeto po WP29 (2017, stran 38–46)

Priloga P: Pristojnost nadzornih organov v EU

Pristojnost nadzornih organov v EU določata Direktiva 2002/58/ES in Uredba 2016/679. Direktiva 2002/58/ES se glede na 1. odstavek 3. člena uporablja za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v EU, kar pomeni, da zavezuje ponudnike dostopa do elektronskih komunikacij – operaterje oziroma telekome. Pri tem je treba opozoriti, da bo obseg storitev, ki sodijo pod okrilje te zakonodaje, po sprejemu ePR mnogo širši (tudi npr. ponudniki kot je WhatsApp ali Skype), in bodo tudi pravila o pristojnosti določena širše – najverjetneje z ozirom na to, ali so take storitve ponujene na trgu EU .

Uredba 2016/679 določa široko pristojnost evropskih nadzornih organov, ne le za upravljavce, ki so ustanovljeni v EU in imajo stabilno ureditev na teritoriju EU, ampak tudi za tiste, ki so ustanovljeni izven EU, če državljanom EU ponujajo storitve ali izdelke, oziroma spremljajo njihovo vedenje. Daljša roka evropske zakonodaje je posledica želje po učinkovitejšem nadzoru nad (predvsem) spletnimi velikani, ustanovljenimi zunaj EU, ki dobičkonosno poslujejo na evropskem trgu, tudi s pomočjo vedenjskega oglaševanja in sledenja posameznikom za druge namene. Za presojo, ali mora določen subjekt izven EU upoštevati uredbo, je relevantno, ali ponuja storitve oziroma izdelke v lokalni valuti in jeziku, ali je mogoče naročiti njegove izdelke oz. storitve iz lokacije v EU, ali nagovarja uporabnike iz EU in ali ustvarja profile uporabnikov iz EU ter analizira njihove preference in vedenje (Burnik, 2016a). Slednje se nanaša prav na ponudnike vedenjskega oglaševanja in oglaševalske mreže ter ponudnike naprednih možnosti analiz spletnega vedenja posameznikov, ki v veliki meri prihajajo iz ZDA.

Priloga R: Sektorska zakonodaja v ZDA

Uporabo osebnih podatkov za namen izdelave kreditne ocene potrošnika urejata *Fair Credit Reporting Act (FCRA)* in *Fair and Accurate Credit Transactions Act of 2003 (FACTA)*. Njun namen je varovanje zaupnosti informacij glede kreditne sposobnosti in stanja potrošnikov. Zakon zato omejuje dopustne namene, za katere smejo biti taka poročila o potrošnikih posredovana in nadzorni organi morajo preveriti, da vsak, ki zahteva taka poročila, izpolnjuje zahtevo glede dopustnega namena. Informacije o preverbah ozadja posameznika običajno temeljijo na informacijah, ki spadajo med javne evidence, npr. kazenska, evidenca civilno pravnih zadev, bankrotov, profesionalnih licenc, vozniških dovoljenj, itd. Zakon omejuje vključevanje nekaterih informacij v poročila o potrošnikih. Zaposlovalci, ki preverjajo kandidate in zaposlene, so prav tako omejeni z delovno-pravno zakonodajo in ne smejo obdelovati informacij o starosti, rasni pripadnosti, verovanju, invalidnostih ali politični pripadnosti, saj bi to lahko vodilo v nezakonito diskriminacijo.

Obdelavo osebnih podatkov otrok na spletu ureja *Children's Online Privacy Protection Act (COPPA)*, ki nalaga podrobne obveze organizacijam, ki zbirajo osebne podatke otrok, mlajših od 13 let na spletu. Namen zakona je višja raven nadzora staršev in skrbnikov nad obdelavo osebnih podatkov otrok na spletu, nad njihovo uporabo, hrambo in razkrivanje. Obdelavo zdravstvenih podatkov ureja *Health Insurance Portability and Accountability Act (HIPPA)*, ki opredeljuje dopustno uporabo in razkrivanje varovanih podatkov o zdravstvenem stanju, nalaga organizacijam, da uporabnike seznanijo z obvestilom o varovanju zasebnosti in drugih pravicah, določa pogoje, pod katerimi je mogoče uporabljati storitve ponudnikov storitev in podrobno določa zavarovanje elektronskih zdravstvenih podatkov. Obdelavo podatkov, ki jih obdelujejo izposojevalnice videov ureja *Video Privacy Protection Act (VPPA)*, obdelavo osebnih podatkov voznikov pa *Driver's Privacy Protection Act of 1994 (DPPA)*, izvajanje neposrednega trženja po e-pošti ureja *CAN-SPAM Act* (ki med drugim določa, da mora imeti prejemnik možnost opt-outa), izvajanje telefonskega neposrednega trženja pa *The Telephone Consumer Protection Act* (ki določa tudi nacionalni *Do-not-call* register, v katerega se lahko posameznik prijavi, če ne želi klicev) (Sotto in Simpson 2014, 209).

Priloga S: IAB okvir za vedenjsko oglaševanje

Ključen v smislu materialnih zahtev je IAB okvir za vedenjsko oglaševanje, ki zajema naslednja načela:

1. *Obvestilo*: tretje strani morajo imeti na svoji spletni strani celovito obvestilo o obdelavi podatkov v okviru vedenjskega oglaševanja (identiteto in svoje kontaktne podatke, naravo podatkov, ki se obdelujejo, namene, za katere se podatki obdelujejo in morebitne prejemnike, enostaven mehanizem za izražanje uporabnikove izbire glede vedenjskega oglaševanja, informacijo, da je stran skladna s temi načeli in povezavo na spletno stran, kjer lahko uporabnik izrazi izbiro). Dodatno morajo zagotoviti tudi obvestilo o obdelavi podatkov preko ikone, ki se nanaša ob oglasu.
2. *Uporabnikova izbira glede vedenjskega oglaševanja*: tretje stranke bi morale zagotavljati mehanizem za izražanje izbire glede vedenjskega oglaševanja. Ta mora biti dostopen iz obvestila. Če podjetja uporabljajo posebne tehnologije, s katerimi zajemajo podatke iz vseh ali večine spletnih naslovov, ki jih obišče neka naprava, preko različnih domen in te podatke uporabijo za vedenjsko oglaševanje, potrebujejo izrecno privolitev posameznika.
3. *Zavarovanje podatkov* – podjetja morajo vzdrževati primerne fizične, elektronske in administrativne ukrepe za zavarovanje podatkov ter določiti ustrezen rok hrambe podatkov.
4. *Občutljiva področja*: podjetja se strinjajo, da ne ustvarjajo segmentov za vedenjsko oglaševanje, ki so namenjena ciljanju na otroke (12 let in mlajši). Za segmente, ki se nanašajo na občutljive osebne podatke, je potrebno izrecno soglasje.
5. *Izobraževanje*: izvajalci vedenjskega oglaševanja morajo izobraževati posameznike in podjetja, podajati jasne, dostopne informacije o tem kako so podatki pridobljeni, kako so uporabljeni in kako lahko uporabniki izrazijo svojo izbiro.
6. *Skladnost in programi izvajanja*: samoregulacijski okvir vsebuje zahteve za pristopnike, ki samo certificirajo svojo skladnost z načeli. Ta je preverjena s strani neodvisne revizije. Okvir za reševanje pritožb vključuje oglaševalska samoregulacijska telesa v državah članicah ter objavo primerov neskladni ravnanj
7. *Pregled*: vsake tri leta poteka pregled tega okvira in se implementirajo potencialne spremembe (EASA, 2016, str. 19–22).

Priloga T: Tehnologija za konceptom standarda ne sledi in politike glede njegovega upoštevanja

Ko uporabnik na spletu obišče spletno stran, računalnik pošlje ali prejme informacijo preko svetovnega spleta, se zahteva začne z informacijo, ki se imenuje zaglavje (angl. *header*). Zaglavje vključuje podatke o brskalniku na napravi, jeziku in drugih tehničnih podrobnostih. Zaglavje bi pri standardu ne sledi vključevalo še strojno berljiv podatek o tem, da uporabnik ne želi sledenja (DNT:1). Uporabnik bi svojo voljo, da mu tretje spletne strani ne sledijo, izrazil tako, da bi vklopil določeno nastavitev v brskalniku, npr. vklopil »zasebno brskanje« ali podobno nastavitev. Ker izražanje volje uporabnika ne temelji na piškotku, lahko ta izbriše piškotke, pa to ne bo vplivalo na delovanje ne sledi mehanizma. Prav tako se uporabniku ni treba vpisati na posebno listo ali podobno orodje, da bi tako izrazil svojo željo po ne-sledenju. Tako ne nastaja centralizirana lista in ne pride do obdelave osebnih podatkov uporabnikov (Electronic Frontier Foundation, 2016).

Koncept standarda ne sledi temelji na relativno preprosti tehnologiji, obsega pa tudi okvir politik, ki določajo, kaj naj bi signal pomenil prejemniku signala in kako naj bi se ta nanj odzval ter opredeljuje odziv s strani nadzornih teles. Okvir politik glede ne sledi signala naj bi dosegal primerno ravnotežje med varovanjem potrošnikov in varovanjem pravic inovatorjev. Ker je mehanizem »ne sledi« nastal zaradi problematike sledenja uporabnikom s strani uporabniku »nevidnih« tretjih strank, nekateri zagovarjajo, da bi moral biti »ne sledi« omejen na omejevanje sledenja tretjim strankam, ne pa tudi npr. spletni strani, ki jo uporabnik dejansko obišče. Poleg tega zagovorniki zasebnosti menijo, da bi moral imeti nadzorni organ (FTC) premišljene pristojnosti, da vpliva na to, kako prejemniki interpretirajo signal ne sledi (Electronic Frontier Foundation, 2016).

Vprašanja politik glede upoštevanja ne sledi so raznolika. Prvo vprašanje, kakšno sledenje naj bi ne sledi mehanizem sploh omejeval, je povzročilo velike dileme in zastoj dela W3C na standardu. Nekatere vrste sledenja imajo namreč pozitivne posledice za uporabnika, npr. večjo varnost pri opravljanju transakcij ali izogibanje prevaram, če so podatki, ki se pri tem hranijo omejeni in jih ponudniki ne hranijo dlje, kot je to potrebno. Prav tako ni problematično sledenje uporabnikom, ki s tem soglašajo. Slednje s strani splete strani, ki jo je uporabnik dejansko obiskal, naj prav tako ne bi bilo problematično (npr. za namen analitike,

ki jo izvaja ta stran kot prva stranka) (Eckersley, 2011). V procesu grajenja ne sledi standarda so sodelujoči predlagali različne definicije sprejemljivega sledenja, med drugim tudi, da bi moralo biti tudi sledenje za namen oglaševanja dopustna raba kljub temu, da uporabnik sporoča ne sledi signal. Bitke za pomen »ne sledi« signala so se torej odvijale pri vprašanjih, koliko podatkov smejo podjetja zbirati kljub prejemu ne sledi signala in kakšne naj bi bile podrobnosti sprejemljivih uporab teh podatkov (Soghoian, 2011).

Za doseganje, da bodo ponudniki spletnih strani spoštovali ne sledi signal, je bilo predlaganih več pristopov, od ustvarjanja črnih seznamov, kamor bi bili uvrščeni ponudniki, ki signala ne upoštevajo, do ustvarjanja zakonodajnih »varnih pristanov« za tiste ponudnike, ki bi signal ne sledi upoštevali. Predlagane so bile tudi pristojnosti za FTC glede določanja standardov za opt-out (Eckersley, 2011).

Ena od tem je bila tudi, ali naj bo nastavitev »ne sledi« v brskalniku privzeto vklopljena ali ne. Argument zagovornikov zasebnosti je bil, da mora imeti uporabnik svobodo, da se aktivno odloči za sledenje – tako je eden največjih brskalnikov[92] »ne sledi« signal privzeto vklopil, a kasneje to nastavitev spremenil, saj je ponudnik storitev na drugi strani niso upoštevali, češ da se uporabnik ni svobodno odločil, ali želi sledenje ali ne, pač pa je to odločitev namesto njega sprejel brskalnik (Davies, 2015b).

Postavljalo se tudi vprašanje različnih politik uveljavljanja »ne sledi standarda« v ZDA in v EU. Zakonodaja v ZDA podjetjem ne zapoveduje, da morajo pred slednjem uporabnikom na spletu pridobiti njihovo soglasje, dovolj je zagotavljanje možnosti naknadne odjave (opt-out), tudi v primeru signala »ne sledi«, kjer bi bila lahko privzeta nastavitev v brskalniku nastavljena na dopuščanje sledenja, uporabnik pa bi to nastavitev lahko spremenil v »ne sledi«. Zakonodaja v EU pa izrecno določa obveznost pridobivanja soglasja za sledenje uporabnikom na podlagi piškotkov in drugih tehnologij, poleg tega pa zakonodaja s področja varstva osebnih podatkov omejuje upravljavce pri oblikovanju profilov in uporabi osebnih podatkov pridobljenih s slednjem. Ne(uporabnost) standarda za doseganje skladnosti z zakonodajo v EU bi bila velika pomanjkljivost (MacDonald in Zuiderveen Borgesius, 2015).

92 Microsoft Internet Explorer

Priloga U: Odziv Delovne skupine iz člena 29 na standard ne sledi

Odziv na oblikovanje standarda ne sledi je podala tudi Delovna skupina iz člena 29. Poudarila je predvsem, da bi standard ne sledi v državah članicah EU lahko zagotavljal skladnost z zakonodajo le, če bi omogočal pridobivanje veljavne privolitve v sledenje, ki mora biti glede na zakonodajo v EU svobodna, posebna, informirana in temeljiti na uporabnikovi aktivni dejavnosti:

- Če bi bil v brskalniku privzeto nastavljen signal ne sledi in bi ga uporabnik nato sam spremenil v »sledi« - pravila pridobivanja veljavne privolitve v EU izključujejo možnost *opt-out* kot veljavne privolitve.
- Nastavitve slednja bi morale imeti rok trajanja – glede na zakonodajo EU ni mogoče veljavno privoliti v neomejeno sledenje.
- Delovna skupina iz člena 29 je opozorila še na nekatere terminološke neskladnosti, zaradi katerih bi lahko bila ovirana uporaba standarda ne sledi v EU – npr. definicija de-identifikacije, pri kateri imajo ponudniki na spletu manjše odgovornosti. EU pravila postavljajo višje standarde, saj upravljavci nimajo obvez glede na zakonodajo le, če so podatki anonimizirani in se jih ne da povezati s posameznikom in ne le zamenjani z identifikatorjem (WP29, 2014d).
- Opozorila je tudi na spornost signala P (potencialno soglasje) in D (ne-upoštevanje ne sledi), z vidika veljavnega soglasja, ki mora biti po EU pravu dano za točno določen namen (WP29, 2015a).

Standard ne sledi torej v kontekstu prava EU naleti na prenekatere izzive:

- Ker se terminologija razlikuje, skladnost delovanja s standardom ne bi pomenila nujno tudi skladnosti z EU pravom, kar pomeni, da bi morali upravljavci v EU zagotoviti dodatne mehanizme, da bi z uporabo ne sledi nastavitve lahko posameznik podal veljavno soglasje v sledenje. V tem smislu je zgoraj omenjen odziv s P signalom zelo problematičen, saj sme po EU pravu posamezniku slediti le tisti, ki zagotovo (in ne le potencialno) ima njegovo privolitev (WP29, 2015a).
- Standard ne sledi omejuje pri sledenju le tretje strani, medtem ko obiskani spletni strani slednje dovoli, oziroma se lahko ta sama odloči, če bo upoštevala strožji režim – po EU pravu pa je pri sledenju omejena tudi dejansko obiskana spletna stran, ki mora prav tako pridobiti soglasje posameznika. Implementacija ne sledi v EU bi tako morala

omejevati tudi slednje dejansko obiskane spletne strani (Zuiderveen Borgesius in McDonald, 2015, str. 22; Kamara in Kosta, 2016, str. 12).

— v EU ne-nastavljenega ne sledi signala upravljavci ne bi smeli interpretirati kot dovoljenja za sledenje, saj je to dopustno le na podlagi soglasja, torej v primeru ustrezne nastavitve (Zuiderveen Borgesius in McDonald, 2015, str. 18).
— Ker gre za orodje samoregulacije, je vprašljivo tudi, na kakšen način bi bilo mogoče uporabo in upoštevanje standarda »ne sledi« nadzorovati in do katere mere bi nadzorni organi v EU lahko izvajali nadzor v primeru ponudnikov izven EU (Kamara in Kosta, 2016, str. 12).

Glede na vse zapisano je jasno, da bi za skladnost z višjimi standardi EU zakonodaje moral nastati neke vrste ne sledi plus standard. Pozitivni vidik ne sledi standarda je, da ga je zaradi tehnične izpeljave v brskalniku mogoče prilagoditi za različne kontekste. Zuiderveen Borgesius in McDonald (2015) npr. zagovarjata, da bi lahko na podlagi obstoječih specifikacij W3C nastal Evropski ne sledi standard, ki ni nujno da pride s strani W3C skupine. Avtorja tudi ocenjujeta nekaj orodij za omejevanje sledenja in zatrjujeta, da so določena zelo blizu zagotavljanja skladnosti s strožjimi evropskimi pravili in da bi lahko zagotavljala veljavno privolitev, kar pomeni, da:

— podjetja ne bi smela slediti uporabnikom, ki niso nastavili preferenc – ne-aktivnost ne more biti privolitev;
— če nekdo oddaja signal ne sledi mu ni dopustno slediti in zbirati podatke, razen v primeru izjem po EU zakonodaji;
— privolitev se mora zgoditi preden so nastavljeni piškotki z identifikatorjem, ne le preden se podatki nadalje obdelujejo;
— uporabniki morajo imeti možnost, da privolitev naknadno umaknejo in npr. spremenijo nastavitve v brskalniku.

Glede na ta štiri merila naj bi nadgrajena oblika standarda ne sledi, ki ga je razvila nevladna organizacija Electronic Frontier Foundation in je združena z dodatki *Privacy Badger* ali *Disconnect*, ki avtomatično blokirajo sledenje, ki ni skladno z ne sledi signalom uporabnika, po vsej verjetnosti zagotavljala skladnost s pravom EU (Zuiderveen Borgesius in McDonald, 2015, str. 19–31).

Avtorja verjameta, da standard ne sledi načeloma zagotavlja vse potrebne komponente, da lahko nastanejo implementacije, skladne s pravom EU in pozivata k temu, da nastane en usklajen evropski »ne sledi« standard. Na primeru določene novičarke spletne strani tudi pojasnita, na kakšen način bil lahko ta obravnavala zahteve ne sledi, da bi bila skladna z EU zakonodajo. Lahko bi razlikovala uporabnike iz EU, pri katerih ne bi smela izvajati sledenja, če ne bi imeti vklopljene možnosti »sledi« (DNT: 0) ter uporabnike izven EU, ki bi jim lahko sledila, razen, če bi imeli vklopljeno možnost »ne sledi« (DNT:1). Uporabnikom, ki jim ne bi smela slediti, bi lahko ponudila možnost, da soglašajo s sledenjem, lahko bi jim ponudila možnost, da plačajo, če ne želijo sledenja ali pa bi jim zavrnila ogled spletne strani, če se ne bi strinjali s sledenjem (zadnja možnost je sicer sporna glede na EU zakonodajo). Avtorja pojasnjujeta, da bi v primeru prepovedanega sledenja spletna stran omejila nalaganje piškotkov ter morala razmisliti tudi o omejitvi drugih možnostih sledenja in zbiranja podatkov, npr. omejitvi dnevniških zapisov IP naslovov in drugih unikatnih identifikatorjev (Zuiderveen Borgesius in McDonald, 2015, str. 35–36).

Tudi iz mnenja Delovne skupine iz člena 29 izhaja za(upanje) v obete standarda »ne sledi«, oziroma tehničnega mehanizma take vrste na ravni nastavitev v brskalniku. Delovna skupina opominja na pomembnost vnaprejšnjega soglasja pred slednjem na spletu ter ponavlja, da pristop »vzemi ali na pusti«, ki je pogosto uporabljen kot način pridobivanje privolitve, za nalaganje piškotkov ni prava pot, saj je taka privolitev redko svobodna. Prav tako ni mogoče veljavno privoliti v slednje s strani neidentificiranih tretjih strani za neznane namene in podati skupno privolitev za različne namene. Delovna skupina priporoča, da se fokus od zahtev, da soglasje za tretje strani pridobijo dejansko obiskane strani, premakne k ponudnikom iskalnikov in operacijskih sistemov, ki naj ponudijo ustrezne tehnične možnosti, kot npr. signal ne sledi, da lahko uporabnik na tej,višji ravni, izrazi svojo izbiro glede sledenja. Delovna skupina poziva tudi industrijo – upravljavce spletnih strani, da signal ne sledi upoštevajo in spoštujejo (WP29, 2016, str. 17).