VARSTVO OSEBNIH PODATKOV KOT DIGITALNEGA PORTFELJA V LUČI SODOBNIH METOD OGLAŠEVANJA

ZORAN DIMOVIĆ[1, 2]

[1] Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
zoran.dimovic@student.um.si
[2] Hella Saturnus Slovenija d.o.o., Ljubljana, Slovenija

Zadnje čase smo priča izjemno hitri rasti informatike, umetne inteligence (in velikih podatkov), kar je povzročilo oblikovanje novih tehnik profiliranja uporabnikov, s tem pa tudi ciljnega oglaševanja, ki je prilagojeno navadam in okusu uporabnika. Ne glede na učinkovitost ciljnega oglaševanja pa je treba upoštevati tudi varstvo teh podatkov. Ko uporabnik nevede poda soglasje k zbiranju podatkov, svoje osebne podatke preda v neznano. Ti podatki se nato neznano analizirajo, obdelujejo ter uporabnika segmentirajo v namenske skupine uporabnikov, kar olajša doseg ciljnih in vedenjskih oglaševalskih akcij. Uporabnik se lahko »zaščiti« le s soglasjem k takšni obdelavi podatkov. Splošni režimi, ki jih predvideva prihajajoča Uredba o e-zasebnosti, niso zadostni, zato bi morali uvesti striktne mehanizme zavrnitve zbiranja podatkov. Za namene trženja mora biti uporabnik v središču oglaševanja, vendar pravila o varstvu podatkov morda niso najboljše sredstva za njegovo pravno varstvo.

DOI
https://doi.org/10.18690/um.pf.6.2023.9

ISBN
978-961-286-788-1

Ključne besede:
ciljno oglaševanje,
digitalni portfelj,
intelektualna lastnina,
varstvo osebnih podatkov,
umetna inteligenca

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/10.18690/um.pf.6.2023.9

ISBN
978-961-286-788-1

PROTECTION OF PERSONAL DATA AS OF DIGITAL PORTFOLIO IN LIGHT OF MODERN ADVERTISING METHODS

ZORAN DIMOVIĆ[1, 2]

[1] University of Maribor, Faculty of Law, Maribor, Slovenia
zoran.dimovic@student.um.si
[2] Hella Saturnus Slovenija d.o.o., Ljubljana, Slovenia

Keywords:
artificial intelligence, digital portfolio, intellectual property, personal data protection, targeted and behavioral marketing

We are witnessing an exceptional growth in the field of informatics and artificial intelligence, which has led to the development of new techniques of user profiling and targeted advertising that is tailored to users' habits and preferences. Despite the effectiveness of targeted advertising, data protection must also be taken into consideration. When users unknowingly give their consent to data collection, their personal information is handed over to unknown entities. These data are then analyzed, processed, and used to segment users into different user groups, facilitating targeted and behavioral advertising campaigns. Users can only "protect" themselves through consent for personal data processing. General regimes envisioned by upcoming e-privacy regulations may not be successful, so strict mechanisms for refusing data collection should be implemented. The user should be at the center of advertising for marketing purposes, but data protection rules may not be the most effective means of ensuring their legal protection.

University of Maribor Press

1 Uvod

Živimo v času, ki ga zaznamujejo bliskovite spremembe na vseh področjih življenja, predvsem pa na področju digitalizacije. Prav tako se vzporedno širi vpliv komercializacije interneta in področja informacijsko komunikacijskih tehnologij (IKT).[1] Sam tehnološki razvoj, dostopnost interneta in povezanost na spletu sta povečala dobiček in vrednost deljenih informacij. S tem so predvsem mišljeni podatki osebne narave, osebni, vedenjski in tehnični podatki. Na podlagi zbranih podatkov se je oblikovalo vedenjsko in tudi ciljno oglaševanje, saj sta ti dve obliki s sledenjem uporabnikom, zbiranjem njihovih informacij, dnevnih navad, dojemanja vrednot in psihologije razmišljanja, omogočili razvoj različnih oglaševalskih akcij, ki so usmerjene na točno določene uporabnike ali na skupino uporabnikov. To so jim omogočili zbrani osebni podatki, kakor tudi ostali podatki, ki se zbirajo tako vede in nevede, v času ko krmarimo po svetovnem spletu, prižgemo luč v stanovanju, všečkamo prijateljevo stran na Facebooku ali pa rezerviramo počitnice.

Ker so se tradicionalna pravna načela zelo težko prilagodila hitremu razvoju IKT, so razprave o legitimnosti takšnega načina oglaševanja in na podlagi tako zbranih podatkov in vedenjskega algoritma v sklopu zbiranja osebnih podatkov sporne. Pri tem je treba omeniti, da je togost pravnega okvirja v diametralnem nasprotju s tekočim in nenehno se spreminjajočim IKT sektorjem. Preko vseh omenjenih platform (Facebook, Instagram, Twitter …) do podatkovnih skladišč poteka nenehna izmenjava vseh zbranih podatkov, ki so danes digitalno zlato. Profiliranje in oblikovanje navad iz digitalnega portfelja osebnih podatkov uporabnika je postal ključni del poslovnega modela novodobnega oglaševanja in številih storitev režima Web 3.0.[2] Zakonitost takšnega delovanja nima jasnega pravnega okvirja, čeprav problem ostaja že od režima Web 2.0.[3] Ne glede na učinkovitost ciljnega oglaševanja pa je potrebno upoštevati varstvo teh zbranih podatkov. Edino, s čimer se uporabnik lahko zaščiti, je predhodno ponudnikovo obvestilo o zasebnosti, kjer so informacije, razlogi in namen zbiranja podatkov podrobneje pojasnjeni, prav tako so tudi

[1] Tehnologija se nanaša na izdelke in prakse, ki se uporabljajo za shranjevanje, zapisovanje in različne načine ter vrste obdelave informacij. Predvsem se nanaša na e-okolje in podatke v elektronski obliki.
[2] Web 3.0 nadgrajuje obstoječ režim predhodne tehnologije 2.0, odpravlja pa težave s spletno zasebnostjo, enakomerno porazdelitvijo računalniške moči med vse uporabnike in omogoča svobodo govora. Dejansko pa ne opredeljuje le spletne strani in spletne povezave, temveč tudi odnose med podatki.
[3] Web 2.0 lahko opredelimo kot računalniško in poslovno revolucijo v računalniški industriji, ki jo povzroči premik iz statičnega okolja na internet kot platformo (sistem spletnih dnevnikov, socialna omrežja …).

pojasnjeni razlogi in namen zbiranja podatkov, način prenosa podatkov in način zaščite zbranih podatkov. Ponudniki spletnih in drugih komunikacijskih storitev morajo zagotoviti, da imajo soglasje tistega, od katerega osebne podatke pridobivajo, in da je to soglasje v skladu z zakonskimi zahtevami. In čeprav skoraj vsi predpisi obravnavajo ta fenomen z vidika samega varstva podatkov, je za učinkovito pravno varstvo potreben holističen pristop, pri čemer je treba upoštevati tudi intelektualno lastnino, varstvo potrošnikov in konkurenčno pravo. Pomembno je omeniti, da zakon ponudnikom, predvsem tistim, ki so odgovorni za obdelavo osebnih podatkov, nalaga posebne obveznosti, ki jih je treba upoštevati ves čas. V skladu s tem so potrošniki na katerikoli digitalni platformi obveščeni, da bodo njihovi podatki uporabljeni, obdelovani ter uporabljeni za vnaprej določno znane dejavnosti. S tem si uporabnik sicer na neki način zagotovi zaščito lastnih podatkov, saj mu je s tem omogočena pravica do dostopa, pravica do popravka podatkov, preklica soglasja oziroma tiste pravne varnosti, ki mu jo veljavna zakonodaja vsaj nekoliko omogoča. Če na podlagi oblikovanega profila uporabnika (sestavljen iz vrednot in navad) letemu ponudimo ciljni oglas, ki ga enači kot smiselnega in njemu primernega, pridemo do podobnih zaključkov, do katerih je prišlo v primeru članka *»hungry judges«*.[4] Če iščemo po Google brskalniku, je ta citiran v več kot 1000 člankih (ogledan več kot 250.000-krat do leta 2022), drugi članek, ki razbija »mit« o rezultatih sinteze članka, pa je citiran le v 44 primerih (ogledan samo 1.812 krat do leta 2022). V primeru citiranja originalnega članka ne govorimo več o povprečnem uporabniku, temveč akademsko izobraženih ljudeh, ki so povzeli prvoten članek v svojih delih. Vidimo, da je neposrečeni učinek vedenjskega in ciljnega oglaševanja bodisi po »*hungry judges*« bodisi *»echo chamber«* [5] ali *»filter bubble«* [6] učinkom, v celoti dosežen, če oglaševalci posedujejo tvoje osebne podatke in na podlagi teh oblikujejo oglaševalske akcije.

[4] Študija, ki so jo pripravili *Danzinger* in drugi aprila 2011, govori o rezultatih statistike odločitev izraelske komisije za pogojne izpuste iz leta 2011. Študija je prišla do zaključka, da je bila odobritev pogojnih izpustov 65 % na začetku seje komisije, pred odmorom za obrok pa je le ta padla na vrednost 0 %. Paradoks tega učinka je ugotovitev, da so bili sodniki po obroku bolj popustljivi, pred odmorom pa bistveno strožji oziroma nepopustljivi, kar gre z roko v roku v odvisnosti od zapletenosti primera in časa reševanja primera v povezavi s časom za počitek.

[5] Algoritemska personifikacija in personalizacija oglaševane vsebine ter prilagoditev le-te glede na obstoječe poglede uporabnika (iz zbranih osebnih podatkov).

[6] Izraz je usmerjen v točno določen učinek na podlagi algoritma, ki izkrivlja in omejuje informacije, ki jih uporabnik vidi na internetu. Cilj tega učinka personalizacije je uporabniku predstaviti čim bolj relevantne informacije, vendar pa lahko povzroči popačen pogled na realnost, saj daje prednost informacijam, katere je uporabnik označil za relevantne (zgodovina iskanja, interakcije s spletnimi stranmi, brskalniki, ključne iskalne besede …).

Zgoraj navedeno odpira številna pravna vprašanja, pri čemer je ta prispevek osredotočen v pravno zaščito digitalnega portfelja osebnih podatkov. V povezavi z zgoraj navedenimi sistemi oglaševanja je prikazan fenomen »*echo chamber*«, pri čemer se zastavlja tudi vprašanje, ali je takšno oglaševanje, ki deluje na podlagi zbiranja podatkov, mogoče regulirati preko nepoštenih poslovnih praks. Med drugim to sproža vprašanja glede varstva konkurence zaradi »zlorabe« instrumenta proste izmenjave idej na trgu. Samo varstvo konkurence se sicer lahko uporablja za zaščito raznolikosti vsebin na trgu, vendar je ta pravna zaščita pred veliko večjim izzivom, kot je bila v času razvoja digitalizacije. Če že algoritmi poskušanju zadovoljiti želje ciljne skupine uporabnikov, ni nujno, da so ponujene vsebine v nasprotju z ideali potrošnikove suverenosti, avtonomije in lastne izbire, na katerih temelji konkurenčno pravo. Vendar pa je mogoče v teoriji prava to regulirati preko sistema nepoštenih poslovnih praks.

Oglaševalska podjetja v večini ne izvajajo režima soglasja k zbiranju podatkov kot edino pravno varstvo uporabnikov, ker so tem podjetjem ti podatki dani na razpolago na podlagi pogodbenega razmerja med oglaševalskim podjetjem in podjetjem za obdelavo podatkov, katerega vsebina je uporabnikom nedosegljiva. Splošni režimi soglasja k obdelavi podatkov ter obvestilo o tem, kot ga predvidevajo 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 (Splošna uredba o varstvu podatkov – GDPR),[7] Uredba (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. oktobra 2022 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (Akt o digitalnih storitvah)[8] in Uredba (EU) 2022/1925 Evropskega parlamenta in Sveta z dne 14. septembra 2022 o tekmovalnih in pravičnih trgih v digitalnem sektorju in spremembi direktiv (EU) 2019/1937 in (EU) 2020/1828 (Akt o digitalnih trgih),[9] Direktiva (EU) 2019/770 Evropskega parlamenta in Sveta z dne 20. maja 2019 o nekaterih vidikih pogodb o dobavi digitalne vsebine in digitalnih storitev (Direktiva o digitalni vsebini)[10] in prihajajoči Predlog Uredbe Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstva osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi

[7] UL L 119, 4. 5. 2016, strani 1–88.
[8] UL L 277, 27. 10. 2022, strani 1–102.
[9] UL L 265, 12. 10. 2022, strani 1–66.
[10] UL L 136, 22. 5. 2019, strani 1–27.

Direktive 2002/58/ES[11] (Predlog uredbe o e-zasebnosti) opisanega problema niso uspeli rešiti, zato bi morali uvesti zelo striktne mehanizme glede soglasja k zbiranju podatkov, pod pogojem, da se pravica do preklica soglasja dejansko uveljavlja. V prispevku je s tem namenom tudi opisano relevantno pravno tolmačenje uporabnikovega soglasja do zgoraj navedenih pravnih aktov, s čimer je se tudi poudarja pravna zaščita uporabnikov iz prav teh aktov. Uporabnik mora vsekakor z namenom trženja biti v središču dogajanja, vendar pa pravila o varstvu podatkov mogoče niso najboljše sredstvo za njegovo pravno varstvo.

2 Oglaševanje v odnosu do osebnih podatkov

2.1 Splošno o oglaševanju

V uvodu je treba opredeliti pojem oglaševanje. Več različnih avtorjev je soglasnih, da je oglaševanje najprej družbeni proces z izrazno obliko na vseh segmentih družbenega življenja. V bistvu gre za čisto tržno komunikacijsko dejavnost z namenom povečanja prodaje in ustvarjanje dobička, kar je tudi glavno vodilo oglaševanja – obveščanje o produktih, zamislih in storitvah, s tem pa ustvarjanje konkurenčnega okolja. Če izhajamo iz te osnove, se oglaševanje deli na psihološki, komunikacijski in ekonomski proces, ki se dalje deli še na ustvarjalni in inovativni proces, nato sledi izvedbeni proces.[12]

V Republiki Sloveniji je pravna ureditev urejena na strokovnem področju in na ravni države, samo oglaševanje je urejeno v več različnih zakonih, urejen pa je prav tako nadzor nad oglaševanjem. Oglaševanje ni v celoti regulirano, saj zakoni ne veljajo za vse položaje in za vse čase, upravni in pravdni postopki pa so dolgotrajni in negotovi. Nadzor nad temi opravlja nadzorni organ, prav tako pa je izvedba sama nadzorovana preko prostovoljnega nadzora. Samoregulativa oglaševanja je podana v okviru etičnih kodeksov, ki jih sprejmejo organizacije, ki opravljajo dejavnost oglaševanja in so praviloma združena v Slovensko oglaševalsko zbornico.[13]

[11] COM/2017/010 final – 2017/03(COD), 10. 1. 2017.
[12] Jančič in Žabkar, 2013, stran 20.
[13] Repas et al., 2005, stran 186.

2.2 Klasifikacija osebnih podatkov in način pridobivanja

Osebne podatke je mogoče glede na njihov izvor razvrstiti med prostovoljno dane, opazovane, izpeljane in algoritemsko ugotovljene. Prostovoljno posredovani podatki izvirajo iz neposrednih dejanj posameznikov (spletni računi, podatki o kreditni kartici, objave na Facebook računu, Twiterju in ostalih spletnih in družabnih aplikacijah). Čeprav so v tem primeru uporabniki seznanjeni z informacijo o zbiranju podatkov, po veliki verjetnosti niso seznanjeni z njihovo obdelavo in nadaljnjim prenosom. Te podatke je mogoče ločiti na sprožene (npr. registracija na spletnem mestu), transakcijske (npr. nakup izdelka s kreditno kartico) in objavljene (npr. objava na družbenih omrežjih). Opazovane osebne podatke zbirajo podjetja, ki se ukvarjajo z zbiranjem podatkov. Te podatke ločimo na angažirane (npr. spletni piškotki, kartice zvestobe, podatki iz lokacijskih senzorjev na mobilnih napravah), nepredvidene (senzorske tehnologije) in pasivne (slike iz posnetkov kamer). Medtem ko so v primeru angažiranih podatkov uporabniki v določeni meri seznanjeni, da se o njih zbirajo določeni podatki, je temu popolnoma drugače v primeru nepredvidenih ali pasivnih podatkov. Uporabniki v teh primerih sploh ne vedo, da so opazovani in da se na podlagi slikovnega, glasovnega ali drugega gradiva o njih zbirajo informacije. Izpeljani podatki so nadalje izpeljani iz osebnih podatkov na podlagi deterministčnih izračunov in kot takšni postanejo novi delci osebnih podatkov, ki so neposredno povezani z uporabnikom. Izpeljane podatke lahko ločimo na računske (npr. aritmetični izračun povprečni čas obiska spletne strani) in notacijske (npr. segmentiranje uporabnikov v skupine glede na skupne lastnosti, kot so starost, spol). Algoritemsko izpeljani podatki pa izvirajo iz različnih analitičnih in deterministčnih procesov, ki temeljijo na določeni verjetnosti, predvsem v smislu statističnih metod (npr. posojilne ocene) in analitičnih procesov (npr. verjetnost glasovanja za določeno politično stranko). V takšnih primerih uporabniki niso vključeni v proces in se ne zavedajo končnih rezultatov, ki so iz algoritemsko izpeljanih podatkov ugotovljeni.

2.2 Opredelitev ciljnega in vedenjskega oglaševanja

Na tem mestu je v povezavi z načini oglaševanja na podlagi zbranih osebnih podatkov potrebno opredeliti tudi ciljno in vedenjsko oglaševanje predvsem v smislu varstva osebnih podatkov, ki je povezano z učinki *»echo chamber«, »hungry judges«* in »*filter bubble*«.[14]

[14] Glej 3. poglavje.

Ciljno oglaševanje je oblika oglaševanja, ki vključuje tudi spletno oglaševanje in je usmerjeno k ciljni skupini uporabnikov z določenimi skupnimi lastnostmi, predvsem izdelka ali oglaševane osebe (npr. politični kandidati). Skupne lastnosti so lahko demografske (spol, starost, rasa, ekonomski status, starost, stopnja izobrazbe) ali psihografske (potrošniške navade, vrednote, osebnost, življenjski slog in zanimanja), lahko pa so tudi skupek posameznih lastnosti iz obeh skupin. Poudarek na zadnjem lahko vsebuje tudi vedenjske spremenljivke, kot so podatki iz zgodovine brskalnikov, zgodovine nakupov ali ostale spletne dejavnosti, katerih informacije so predvsem pridobljene preko t. i. piškotkov. Algoritmi so namreč pripravljeni že do te faze, da znajo izločiti nepotrebne podatke in obdržati tiste, s katerimi bodo dosegli ciljno avdienco.

Oglaševanje omogoča oglaševalski industriji, da doseže uporabnike z izdelki, storitvami in blagovnimi znamkami, ter s tem ustvarja dohodek, potreben za financiranje storitev, obenem pa s tem omogoča oglaševalskim platformam in podjetjem promocijo, marketinško pozicijo ter tudi ustvarjanje dobička. V sistem oglaševanja je vključenih ogromno ponudnikov oglaševalske tehnologije (*adtech*),[15] založnikov in oglaševalcev. Zasnova je razmeroma preprosta: oglaševalci želijo prikazati oglase skupini potrošnikov, ki bodo po veliki verjetnosti kupili oglaševan izdelek, potrošniki pa želijo videti oglase, ki so zanje tako ali drugače pomembni. V ozadju takšnega odnosa stoji informacijski sistem in zapleten sistem obdelave podatkov, ki vključuje pridobljene podatke profiliranja, sledenja, skupne rabe osebnih podatkov in podatke, zbrane od tretjih oseb. Zanašanje na tako zbrane osebne podatke pomeni, da ima varstvo osebnih podatkov bistveno, če ne že primarnih vlog pri gradnji zaupanja med industrijo in potrošniki. Pravna zaščita omejuje zlorabo pridobljenih osebnih podatkov in ščiti posameznikovo zasebnost pred javnostjo.[16] Razpoložljive tehnološke rešitve in način njihove uporabe lahko namreč v spletnem oglaševanju močno posežejo v potrošnikovo zasebnost, predvsem s tega vidika, da se podatki lahko pridobijo celo v realnem času in na podlagi tako zbranih podatkov (socialna omrežja, spletne platforme, telekomunikacijske storitve, elektro industrija, …) oblikujejo dnevne, psihološke, socialne in privzete navade (in tudi vrednote) potrošnika – dejansko imajo različni akterji na trgu vpogled v zasebnost potrošnika, ki je bila prej dostopna le njemu.

[15] Mednarodna serija digitalnih oglaševalskih in tehnoloških konferenc in razstav interaktivnega marketinga.
[16] Bainbridge, 1996, stran 14.

Ciljno strukturirano oglaševanje je tržni trend razširilo v ustvarjanje priložnosti oglaševalcem, da dosežejo tisti tip potrošnikov, ki jim je po naravi navad vsebina takšnega oglasa namenjena. S tem lahko oglaševalska podjetja ponudijo prilagojene oglase. To počnejo preko infrastrukture informacijsko komunikacijskih storitev. Oglaševalska podjetja in statično-analitska podjetja zbirajo, združujejo, obdelujejo, posredujejo oziroma trgujejo z ogromno količino osebnih podatkov potrošnikov, kar je med temi povzročilo pomisleke glede zasebnosti in vdora v ustavno zagotovljene pravice. Predvsem se lahko v sklopu tega pojavi težava pri pretoku takšnih informacij med oglaševalsko platformo in oglaševalskimi/analitičnimi omrežji, postopki profiliranja potrošnikov, viri in merili oglaševanja, analizo meritev ciljnega oglaševanja na osnovi vedenjskega oglaševanja ter postopkom oglaševanja k uporabniku v času njegove uporabe bodisi aplikacije socialnega omrežja bodisi spletnega brskalnika.[17]

Po drugi strani pa je vedenjsko oglaševanje osredotočeno na dejanja in dejavnost uporabnikov, zato ga je lažje izvesti v spletnem okolju. Zgodovino brskanja in tam vnesene preference po spletnih mestih je mogoče zbrati preko podatkovnega rudarjenja, ki omogoča ustvarjanje vedenjskih vzorcev uporabnikov. Tisti oglaševalci, ki uporabljajo to metodo, verjamejo, da bodo na takšen način pridobili občinstvo, katerim je oglas bodisi po vrednotah bodisi po vzorcu obnašanja bližji, zato jim bo posredovan oglas bližji. Na primer, če bi potrošnik cel čas iskal potovanje in oddih, bi algoritem v kasnejši fazi to prepoznal in pričel istemu uporabniku pričel prikazovati povezane oglase potovanj na nepovezanih spletnih mestih (kot je npr. Facebook, Instagram). Prednost takšnega načina oglaševanja je prilagoditev oglaševanja interesom ciljnih uporabnikov, ne pa tudi skupini ljudi, katerih interesi in vrednote so lahko različni.[18]

2.3 Pravna ureditev v EU

Varstvo osebnih podatkov je specifična evropska inovacija, ki je bila zunaj EU sprejeta različno. K ureditvi so predvsem prispevale Smernice OECD o varstvu zasebnosti in čezmejni izmenjavi osebnih podatkov iz leta 1980,[19] Konvencija o

[17] Štirn, 2003, stran 29.
[18] Leka, 2016, stran 42.
[19] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

zaščiti posameznikov v razmerju do samodejne obdelave podatkov iz leta 1981[20] in Smernice UN glede ureditve računalniških zbirk osebnih podatkov iz leta 1990.[21] Takšna ureditev izhaja iz zgodovinskega konteksta nastanka mednarodnega sodelovanja EU.[22] V tem kontekstu sta bila odločilna dva dejavnika, prvič bliskovit tehnološki razvoj in mednarodni izzivi, ki jih ta prinaša, drugič pa potreba po medsebojni izmenjavi in prenosu osebnih podatkov znotraj EU ter reševanje potrošniških sporov v različnih pravnih ureditvah držav članic. In čeprav je tehnološki razvoj dodatno napredoval, je ostala zgradba varstva osebnih podatkov preprosta.[23]

Kot vidimo, je varstvo osebnih podatkov kompleksno vprašanje, ki se tradicionalno povezuje z zasnovo varstva zasebnosti v okviru obdelave osebnih podatkov. Vendar pa sta, vsaj v skladu z zakonodajo EU, varstvo zasebnosti in varstvo osebnih podatkov različni, a dopolnjujoči se temeljni pravici.[24] Takšno stališče je omogočilo, da je varstvo osebnih podatkov prevladalo nad drugačnimi interesi in tej pravici dalo pravno zaščito, s katero ni mogoče ekonomsko trgovati.[25] Varstvo osebnih podatkov je pridobilo ključno vlogo s sprejetjem Lizbonske pogodbe.[26] Določba 39. člena Pogodbe o Evropski uniji (PEU)[27] in 16. člen Pogodbe o delovanju Evropske unije (PDEU)[28] vsebujeta posebne določbe v zvezi z varstvo osebnih podatkov, pri čemer 16. člen opredeljuje varstvo osebnih podatkov v splošnem pomenu ter razlaga temeljna načela, zakonodajalcem pa nalaga obveznost, da vzpostavijo jasen in določen pravni okvir za varstvo osebnih podatkov. Poleg tega je Lizbonska pogodba vzpostavila zavezujoč pravni status Listine Evropske unije o temeljnih pravicah[29] in zagotovila posebne določbe v zvezi s pravnim pomenom Evropske konvencije o človekovih pravicah[30] (EKČP), ki v 8. členu opredeljuje varstvo osebnih podatkov in varstvo zasebnosti.

[20] Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, ETS no. 108, 1981.
[21] Tene, 2010, strani 1–8.
[22] Kelleher, 2006, stran 14.
[23] Hert, 2012, strani 130–142.
[24] Borghi, 2013, strani 109–153.
[25] Prav tam, 2013, stran 142.
[26] UL C 306, 17. 12. 2007, strani 1–271.
[27] UL C 326, 26. 10. 2012, strani 1–*412*.
[28] UL C 326, 26. 10. 2012, strani 1–271.
[29] UL C 83, 30. 3. 2010, strani 1–408.
[30] Uradni list RS, št. 3-20/1994 (RS 11/1994).

V veljavi sta dva pravna predpisa, ki imata ključno vlogo pri varstvu osebnih podatkov. Prva je GDPR, druga pa še vedno veljavna Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij[31] (Direktiva 2002/58). Direktiva 2002/58 se uporablja kot *lex specialis* napram *lex generalis* GDPR. Uporabnost obeh temelji na treh pomembnih pravnih kategorijah: na tistih, ki se nanašajo na prenašanje informacij ter obdelavo podatkov; tistih, ki se nanašajo na privolitev in soglasje uporabnika; in tistih, ki se nanašajo na vse ostale obveznosti, ki so kot takšne določene v GDPR.

2.4 Ureditev v Republiki Sloveniji

Za učinkovito varstvo osebnih podatkov in zasebnosti so potrebni prilagodljivi in učinkoviti ukrepi, uporaba ustreznih tehnoloških rešitev ter izobraževanje posameznikov, ki morajo sami odločati o uporabi njihovih osebnih podatkov. Potrebno je zagotoviti ustrezno razmerje med interesi ponudnikov in drugih uporabnikov informacij, ki zbirajo osebne podatke, ter pravico pridobivanja informacij z namenom omogočiti polno izkoriščenost možnosti, ki jih omogoča moderni način zbiranja in obdelovanja podatkov. Pravica do zasebnosti je ustavna pravica, določena v 35. členu Ustave Republike Slovenije[32] (URS), varstvo osebnih podatkov pa ureja 38. člen URS, ki opredeljuje uporabo podatkov v skladu z namenom njihovega zbiranja, pravico, da se posameznik seznani z osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi. Ker ustava ne omenja elektronskih podatkov, je podrobno urejanje tega področja prepuščeno zakonu.

Področje varstva osebnih podatkov primarno ureja Zakon o varstvu osebnih podatkov[33] (ZVOP-2), ki v slovensko zakonodajo prenaša določila GDPR.

V povezavi z elementi oglaševanja, kakor tudi glede ureditve varstva osebnih podatkov, je najbolj pomemben Zakon o varstvu potrošnikov[34] (ZVPot-1). Za razliko od ZVPot,[35] ki je veljal od leta 2004, je ZVPot-1 vnesel določbe o digitalni

[31] UL L 201, 12. 7. 2002, strani 37–47.
[32] Uradni list RS, št. 92/21.
[33] Uradni list RS, št. 163/22.
[34] Uradni list RS, št. 130/22.
[35] Uradni list RS, št. 98/2004.

vsebini, načinu informiranja potrošnikov ter določbe glede izpolnitve obveznosti. Oglaševanje je v ZVPot-1 urejeno v 36. do 45. členu, določbe o nepoštenih, zavajajočih in agresivnih poslovnih praksah so določene v 46. do 54. členu. Treba je izpostaviti, da primere digitalnih vsebin v povezavi z varstvom osebnih podatkov obravnava 1. člen, ki določa: »kadar se določbe tega zakona uporabljajo za digitalno vsebino, ki se ne dobavi na materialnem nosilcu podatkov, ali za digitalno storitev, se uporabljajo tudi v primeru, kadar se podjetje zaveže, da bo dobavilo digitalno vsebino, ki se ne dobavi na materialnem nosilcu podatkov, ali opravilo digitalno storitev za potrošnika, pri čemer se potrošnik zaveže, da bo podjetju posredoval osebne podatke, razen kadar podjetje obdeluje osebne podatke, ki jih zagotovi potrošnik, izključno za namen dobave digitalne vsebine ali izvedbe digitalne storitve ali za to, da podjetje zagotovi skladnost s pravnimi zahtevami, ki veljajo zanj, ter teh osebnih podatkov ne obdeluje za noben drug namen.« Določba tretjega odstavka 3. člena ZVPot-1 navaja, da se osebni podatki potrošnika zbirajo, obdelujejo in varujejo v skladu s predpisi, ki urejajo varstvo osebnih podatkov, pri čemer pri razlagi izraza osebni podatki iz 12. točke 4. člena ZVPot-1 ta napotuje na razlago iz določil GDPR.

Oglaševanje je v okviru Zakona o medijih[36] (ZMed) opredeljeno v 46. do 51. členu, prav tako pa tudi v 93. do 99. členu, pri čemer so pomembne tudi določbe 129., 130. in 138. člena. Določba 47. člena Zmed, ki se nanaša na varstvo osebnih podatkov, navaja, da se z oglaševanjem ne sme prizadeti spoštovanje človekovega dostojanstva in škoditi interesom uporabnikov. V odnosu do tega gre za osnovno vodilo, ki izhaja tudi že iz določil ustavno zagotovljenih pravic iz 34., 35. in 38. člena URS o osebnem dostojanstvu in varnosti, o varstvu zasebnosti in osebnostnih pravic ter varstvu osebnih podatkov. Drugih napotil na varstvo osebnih podatkov v predmetnem zakonu ni zaslediti.

Ureditev oglaševanja v povezavi z osebnimi podatki sledi tudi iz Zakona o avdiovizualnih medijskih storitvah[37] (ZAvMS). Pri tem je v ospredju zaščita otrok, katerih osebni podatki so zaščiteni po določilih devetega odstavka 14. člena. Osebni podatki otrok, ki jih ustvarijo ponudniki avdiovizualnih medijskih storitev, se lahko obdelujejo le za namene preverjanja starosti uporabnikov.

[36] Uradni list RS, št. 82/21.
[37] Uradni list RS, št. 204/21.

Sicer je v slovenski pravni ureditvi oglaševanje urejeno tudi v Zakonu o omejevanju uporabe tobačnih in povezanih izdelkov[38] (ZOUTPI), ki v 10. odstavku 22. člena določa, da se osebni podatki obdelujejo v skladu s predpisi, ki urejano varstvo osebnih podatkov, pri čemer je mišljena določba 38. člena URS ter določila GDPR. Oglaševanje je urejeno tudi v Zakonu o zdravstveni ustreznosti živil in izdelkov ter snovi, ki prihajajo v stik z živili[39] (ZZUZIS), vendar skozi prizmo oglaševanja ne izpostavlja osebnih podatkov ter tudi ne opredeljuje načina zbiranja in varstva osebnih podatkov. Prav tako je oglaševanje opredeljeno v 23. členu Zakona o javni rabi slovenščine[40] (ZJRS) in v 57. do 61. členu Zakona o medicinskih pripomočkih[41] (ZMedPri).

Oglaševanje je tako v Republiki Sloveniji dokaj dobro umeščeno v različne zakone, ki opredeljujejo različne vrste in oblike oglaševanja ter v skladu s tem postavljajo omejitve in prepovedi. V delu, ki se nanaša na varstvo osebnih podatkov, pa vsi zakoni, če ni izrecno navedeno, napotujejo na veljavno zakonodajo s področja varstva osebnih podatkov, ustavna določila glede varstva osebnih podatkov ter določila GDPR.

2.5 Načini zbiranja podatkov z namenom oglaševanja

Ciljni oglaševalski trg je usmerjen v ustvarjanje trdne povezave med oglasi in uporabniki. S tem so vzpostavljeni različni procesi, ki upravljajo veliko podatkov in zahtevajo veliko količino podatkov, da se lahko razporedijo do vseh tržnih akterjev. Dodana vrednost je usmerjena prav v pridobivanja različnih podatkov, navedenih v točki 2.1 tega članka, preko spremljanja uporabnikove spletne dejavnosti, ki se predvsem zanaša na zmogljive algoritme inteligentne računalniške tehnologije. Podatki se zbirajo pri različnih akterjih na trgu.

Najprej je treba omeniti same upravljavce podatkov in posredniške agente (podjetja oziroma računalniški strežniki), ki sodelujejo s podjetji za upravljanje s podatki. Ti podatke zbirajo, združujejo, analizirajo z namenom ujemanja oglasov z ustvarjenim profilom ciljne potrošniške skupine. S tem namenom iz digitalnega portfelja

[38] Uradni list RS, št. 29/17.
[39] Uradni list RS, št. 42/02.
[40] Uradni list RS, št. 8/10.
[41] Uradni list RS, št. 98/09.

podatkov ustvarjajo uporabniške profile, ki vključujejo tako demografske podatke, kakor tudi preference, želje in potrebe. Gredo celo tako daleč, da lahko na podlagi zbranih podatkov opredelijo vrednote posameznika, s čimer že čezmerno posegajo v zasebnost potrošnikov. V splošnem poznamo tri širše oblike podjetij za upravljanje podatkov, med katere sodijo podatkovni posredniki, platformna podjetja za upravljanje s podatki ter podjetja za analizo zbranih podatkov in ustvarjanje tržnih raziskav. Vsa navedena podjetja zbirajo in obdelujejo osebne podatke uporabnikov, v določenih primerih se njihove dejavnosti prekrivajo, čeprav ima vsako od navedenih podjetij točno določen namen v sistemu oglaševanja.

Drugi tip so t. i. podatkovni posredniki. Ti podatke, ki jih pridobijo ali iz komercialnih ali vladnih virov, zbirajo, združujejo in analizirajo. Zbrani podatki se uporabljajo za namen profiliranja potrošnikov, same podatke pa lahko prodajajo drugim podjetjem ali kako drugače trgujejo z njimi. Največji podatkovni posredniki so iz Združenih držav Amerike, primat na področju EU ima francosko podjetje Dawex,[42] ki ponuja varno platformo, imenovano Gaia-X za izmenjavo osebnih podatkov med različnimi podjetji. Podjetja, ki so vključena v to platformo, lahko uporabljajo baze osebnih podatkov, prav tako pa lahko dodajajo druge osebne podatke o posameznikih ter ostale osebne informacije, s čimer soustvarjajo obogateni digitalni portfelj osebnih podatkov na vseh platformah.

V povezavi z zgornjima dvema tipoma so tudi podjetja za analizo podatkov in izvedbo tržnih raziskav. Rezultate delijo proti plačilu z zainteresiranimi tržnimi deležniki. Tem pomagajo analizirati, razvrščati in segmentirati posameznike. Oglaševalcem omogočajo, da oglaševalska akcija doseže prav določen tip ljudi s skupnimi interesi, preko sporočil na določenih internetnih kanalih ali napravah (npr. Facebook, pasice na spletnih mestih ...). Vsa podjetja, ki izvajajo analizo osebnih podatkov, na tržišču ponujajo storitve profiliranja potrošnikov (po namerah in vrednotah), napovedno analitiko in personalizacijo uporabnikov, segmentacijo strank, digitalni marketing, e-trgovino, pri čemer so vse te storitve osnovane na pametni tehnologiji nevronskih mrež in strojnega učenja.

[42] https://www.dawex.com/en/ (obiskano: 3. 1. 2023).

Analitika zbranih podatkov omogoča zavajanje uporabnikov, kot je to razvidno na učinkih *»echo chamber«, »hungry judges«* in »*filter bubble*«. V konkretnem primeru govorimo o t. i. metodi »*Dark patterns*« vzorcev obdelave podatkov.[43] Na podlagi ocen navad potrošnikov in njihovih vrednot namreč oglaševalska podjetja namerno spodbujajo in zavajajo uporabnike, da počnejo in nakupujejo stvari, ki jih morda ne želijo početi. To počnejo bodisi z grafičnimi podobami (besedilo, barva vizualnih elementov) bodisi interaktivnim posredovanjem (npr. navedba, da bo izdelek ali storitev kmalu razprodana) ali preko različnih psiholoških elementov kot npr.:

- Občutka krivde, ki onemogoča uporabnikov pravilno izbiro izmed danih možnosti (npr. ko se uporabnik poskuša odjaviti od e-novic, je preusmerjen na stran s sporočilom »Prosimo, ne odidite!«). Takšne metode so največkrat implementirane v oglasne pasice.
- »*Zuckering*« je sestavljen iz namerne prevare uporabnikov, da javno delijo več informacij o sebi, kot bi to želeli. V konkretnem primeru gre predvsem za uporabo Facebook Messengerja, ki je v bistvu zasnovana za zbiranje osebnih informacij kot npr. modra puščica potrditve v sami aplikaciji in manjkajoča puščica za preklic sporočila.
- Prikriti oglasi, ki so predstavljeni kot druga vrsta vsebine, da bi uporabnike spodbudili h kliku. Npr. oglas vsebuje poziv k dejanju, kot je obisk spletne strani ali prijava na e-novice, vendar je tak poziv diskreten in ne bo prevladoval nad zgodbo - prikriti oglas poskuša ustvariti povezavo med pozitivnim občutkom in produktom, ne da bi ga očitno oglaševal.

V vseh zgornjih primerih gre za sporne oglaševalske prakse, ki ne omogočajo učinkovitega pravnega varstva. »*Zuckering*« je v nasprotju z več določili GDPR, in sicer enajstim odstavkom 4. člena (glede soglasja), 12. členom (glede transparentnosti), uvodno točko 32 (soglasje mora biti specifično ter jasno). Prav tako se 5., 6. in 7. člen GDPR nanašajo na zakonitost obdelave podatkov ter legitimni razlog zbiranja podatkov, s čimer je vsaj iz predpisov onemogočena namerna prevara porabnikov. Enako velja tudi za sporno prakso, sestavljeno bodisi iz občutka krivde ali iz naslova prikritih oglasov, pri čemer je razen že prej navedenih določil GDPR treba omeniti Direktivo 2002/58. Prav tako je Sodišče EU glede uporabe takšnih

[43] https://www.deceptive.design/ (obiskano: 3. 1. 2023).

praks že odločalo v zadevi *Bundesverband der Verbraucherzentralen*,[44] pri čemer je v 55. točki navedlo, da je glede na sporno prakso in način zbiranja podatkov nemogoče priti do zaključka, na kakšen način je uporabnik podal svoje soglasje. Spletna stran ponudnika je namreč ponujala le možnost ogleda vsebine brez soglasja k obdelavi podatkov ob preusmeritvi. Ob omejitvi ogleda te vsebine in pojavu ikone za nadaljevanje ogleda je uporabnik preusmerjen na ciljni oglas, čeprav tega sploh ni želel.

3 *Ipso facto* učinki oglaševanja na podlagi »pobranih« osebnih podatkov

Kot je že zgoraj opisano, je ciljno oglaševanja tržna praksa za prikazovanje oglasov in ostalih oblik tržnih akcij komercialne vsebine, ki uporablja osebne in ostale podatke uporabnikov, pridobljenih na več različnih načinov. Vključuje kontekstualno oglaševanje, ki temelji na spletni vsebini in vnosu ključnih iskalnih besed, segmentirano oglaševanje, ki temelji na lastnostih uporabnikov, in vedenjsko oglaševanje, ki temelji na vedenjskih podatkih. Oglasi so prikazani na več načinov, odvisno od spletne strani, ključnih besed, družbenih medijev, mobilnih naprav, namenskih programov in chatbotov (pogovorna okna). Pri zadnjih se uporabniki sploh ne zavedajo, da o njih obstajajo podatki, za katere ne vedo. Za sledenje uporabnikov se uporabljajo različne metode, kot so piškotki, lokacijski podatki naprave ipd. »*Dark patterns*« spodbujajo uporabnike, da posredujejo podatke proti svoji volji, predvsem na podlagi spremljanja vedenjskih lastnosti uporabnikov, kar lahko vodi do nadzora zasebnih in javnih akterjev, vdora v zasebnost, diskriminacije ali celo krajo identitete. Zbrani podatki se uporabljajo za različne analize in profiliranje uporabnikov na podlagi tehnologij kognitivnega računalništva, pa tudi analitike nevronskih mrež. Tako analizirani podatki se lahko razvrstijo v različne segmente in nato uporabnike segmentirajo v skupine s podobnimi interesi, stališči ali vedenji. Tako oblikovane strukture ljudi dosežejo ciljni oglasi z namenom, da imajo vpliv na uporabnike. Skratka, osebni podatki so v oglaševalskem sistemu »digitalni portfelj«, kateri se obdelujejo in izmenjujejo na različne načine, da bi zagotovili potrebne informacije tržnikom in drugim osebam oglaševalske industrije.

[44] Zadeva C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV proti Planet49 GmbH, ECLI:EU:C:2019:801 (*Bundesverband der Verbraucherzentralen*).

Posamezniki se dejansko ne zavedajo, kako se njihovi podatki obdelujejo in kakšen vpliv ima takšna obdelava podatkov na njihovo življenje.

Po mnenju Evropske komisije (EK)[45] ciljno oglaševanje vsebuje:

- kontekstualno oglaševanje, ki meri na uporabnike na podlagi spletne vsebine, katero obiskujejo uporabniki, ali iskane ključne besede;
- segmentirano oglaševanje, ki temelji na posameznih lastnostih uporabnika;
- vedenjsko oglaševanje, ki temelji na opazovanju vedenja uporabnikov (na podlagi računalniških algoritmov pri obdelavi osebnih podatkov preučuje vedenjske navade uporabnika glede na ponavljajoče se obiske spletnih mest, iskanih ključnih besed);
- vedenjsko segmentiranje, ki združuje uporabnike glede na njihove spletne navade (nakup blagovni znamk, politične razprave ipd.) in njihove nakupovalne navade (določeni proizvajalci, prejšnje ocene izdelkov).

Informacije, navedene zgoraj in uporabljene z namenom profiliranja, so lahko tudi pogojne, kar pomeni, da se lahko na njihovi podlagi napove nagnjenost k odzivu na določeno nakupovalno vedenje ali odziv na določeno vrsto sporočila s spremembo uporabniškega razpoloženja. Takšne napovedi ocenjujejo vedenje uporabnika glede na verjetnost, da bo sodelovanje z njim prineslo koristi oglaševalcem.

Vse to se odraža v različnih učinkih, ki jih zbiranje osebnih podatkov prinaša. Raziskava o pravnih odločitvah izraelske komisije za pogojne izpuste,[46] v kateri so primeri za odločanje zaporedno predstavljeni na sejah, je pokazala, da je verjetnost pozitivne rešitve komisije na začetku odločanja padla s 65 % na 0 %. Enako velja tudi pri odločanju pred odmorom za kavo, pri čemer se verjetnost pozitivne rešitve nazaj povzpne na 65 % po odmoru, malici ali počitku. Avtorji raziskave trdijo, da te ugotovitve izkazujejo očitno duševno izčrpanost sodnikov. Pri izvedbi analiz so ugotovili, da je takšen učinek mogoče razložiti s statistično metodo, ki daje prednost ugodnim odločitvam v času trajanja dobrega počutja sodnikov, ko so primeri bolj kompleksni in dlje časa trajajoči. Sodnik namreč ni zmožen voditi takšnega primera

[45] Glej https://ec.europa.eu/info/publications/consumer-market-study-onlinemarket-segmentation-through-personalised-pricing-offers-european-un=). 2018. (obiskano: 12. 1. 2022).
[46] Danziger et al., 2011, strani 6889–6892.

v času pred počitkom za kavo ali malico. Z vidika oglaševanja in zbranih osebnih podatkov uporabnikov je na podlagi oblikovanja vrednot in vedenja uporabnikov letem mogoče ponuditi prav ta kontekst. Če je namreč v uporabniku zasidrana ideja, da so sodne odločitve ne le nepravične, temveč tudi ne temeljijo na pravni utemeljitvi, se mu bo, ko bo iskal podobno vsebino, prikazal prav rezultat, ki bo ga usmeril prav na takšno raziskavo, ki je citirana v več kot 1000 člankih (ogledan več kot 250.000-krat do leta 2022). Drugi članek, ki razbija »mit« o rezultatih sinteze članka, pa je citiran le v 44 primerih (ogledan samo 1.812-krat do leta 2022). Za normalnega uporabnika je namreč zaželeno, da so rezultati sodnih primerov odvisni zgolj od zakonov in relevantnih dejstev in da drugi dejavniki na sodnike nimajo vpliva. Vendar imajo zbrani osebni podatki o različnih vrednotah uporabnikov in segmentiranje uporabnikov tudi drugačne rezultate na podlagi samih zbranih osebnih podatkov. Te podatke uporabnik lahko poda tudi s predhodnim soglasjem k zbiranju podatkov še preden mu spletna stran dejansko omogoči ogled spletne strani. Paradoks »*hungry judges*«, ki ga predstavlja prav ta študija, je pogosta referenčna točka za poudarjanje človeške pristranskosti pri sodnem odločanju, kar predstavlja vrednostno vsebino, ki je posebej izrazito pri algoritmih umetne inteligence v pravu v povezavi z vedenjskim oglaševanjem. Vendar je veljavnost tega paradoksa problematična prav iz dveh razlogov, prvič do napačne razlage težave, drugič do prikaza neučinkovitega in pristranskega pravosodnega sistema, ki je uporabnikom bližje.[47]

Študija[48] je pokazala, da lažne novice potujejo hitreje kot prave, vendar pa na širjenje informacij vpliva veliko dejavnikov. Poleg tega so uporabniki naklonjeni k dajanju prednosti informacijam, ki so bližje lastnim prepričanjem ter tako ustvarjajo skupino enakomiselnih oseb. Temu pojavu pravimo »*echo chamber*« učinek, saj se na podlagi predhodno zbranih osebnih podatkov in vsiljevanju spletnih informacij ali dezinformacij oblikuje skupina, ki ima bodisi enako politično prepričanje, politično nagnjenost ali druge skupne vrednote. Iz tega izhaja tudi uspešnost »*hungry judges*« učinka, vse pa je podano preko zbiranja osebnih podatkov in ciljnega ter vedenjskega oglaševanja določene spletne vsebine. Podobno velja za »*filter bubble*« učinek. V tem konkretnem primeru algoritem na podlagi baze zbranih osebnih podatkov, lokacijskih podatkov, preteklega spletnega vedenja in zgodovine iskanja selektivno

[47] Omer, 2010, strani 1–8.
[48] Vosoughi, 2018, strani 1146–1151.

ugiba, katere informacije bi uporabnik želel videti in mu te ponudi ter ga tako usmerja v dejanja, ki so lastna oglaševanju in ustvarjanju dobička.

4 »Učinkovito« varstvo podatkov v digitalnem svetu – soglasje uporabnika

4.1 Soglasje uporabnika

Kot izhaja iz zgoraj navedenega, je edino pravno varstvo uporabnikov mogoče doseči le z njihovim soglasjem.

Oglaševanje je ključno gonilo digitalnega gospodarstva. Spodbuja številne tehnološke inovacije, prodrlo je v spletno okolje in prispevalo k oblikovanju dostopa do različnih informacij ter iteracij med ljudmi. Spletno oglaševanje temelji na podatkih o posameznikih, vključno z njihovimi demografskimi podatki, preferencami, sledenju spletnih aktivnosti in ostalem. Zmožnost pošiljanja vse bolj učinkovitih ciljnih oglasov ljudem zagotavlja nadzor, kar pa vodi v še bolj poglobljeno zbiranje podatkov. Čedalje bolj so na razpolago tudi tehnike zaznavanja čustev, čustvenih stanj in predvidevanje reakcij. Učinki tega modela niso omejeni samo na komercialno področje, temveč tudi v sistem nadzora in sistem zbiranja podatkov. Edina pravna podlaga za izvedbo ciljnega oglaševanja je privolitev oziroma soglasje uporabnika. Vendar je to soglasje, s katerim se nato zbirajo osebni podatki, zlorabljeno enako kot pravna podlaga za uvedbo slednjega. Podjetja namreč lahko v večini primerov napeljejo večino uporabnikov, da privolijo v kakršno koli obdelavo z namenom oglaševanja. Nastanek takšnega modela je posledica konvergence dveh ideologij, ki imata pomembno vlogo v internetni kulturi – po eni strani libertansko egalitarne ideologije, po kateri morajo informacije prosto krožiti po spletnem okolju, spletne storitve pa morajo biti prosto dostopne vsakomur, po drugi strani pa podjetniške ideologije, usmerjene v uspešno poslovanje in ustvarjanje dobička.[49] Ne glede na uspešnost druge ideologije, ki je pripeljala do nekaterih najbolj uspešnih in inovativnih podjetij (Facebook, Google), je uspešnost z vidika prve ideologije vprašljiva, saj ta model prispeva k nadzoru uporabnikov. Od piškotkov, ki so predvsem omogočili zbiranje podatkov, se zdaj pojavljajo personalizirani oglasi, nove tehnike pa so razvite s prav tem namenom.[50]

[49] Lanier, 2018, stran 42.
[50] Sartor, 2020, stran 6.

V skladu z zakonodajo o varstvu osebnih podatkov in varstvu potrošnikov obstaja v EU ogromen nabor pravnih instrumentov, ki so namenjeni pravni zaščiti posameznikov pred ciljnim in vedenjskim oglaševanjem. Vendar pa ti instrumenti doslej niso bistveno vplivali na iznajdljivost podjetij ali na spletni angažma uporabnikov. Glavni razlog za takšno stanje je povezan z načinom, s katerim je soglasje uporabnika pridobljeno, in način na kakšen je takšno soglasje dano. Za obdelavo osebnih podatkov je pravna podlaga podana v 8. členu Listine Evropske unije o temeljnih pravicah[51] (LEUTP), ki v prvem odstavku določa, da vsakdo ima pravico do varstva osebnih podatkov, ki se nanj nanašajo, v drugem odstavku pa, da se osebni podatki morajo obdelovati pošteno, za določene namene in na podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom. To bi moralo zagotavljati, da se osebni podatki obdelujejo le v primeru, ko to prispeva k interesom uporabnikov, ki prostovoljno privolijo v obdelavo svojih podatkov v skladu z določbo 1.a točke 6. člena GDPR ali kadar je obdelava potrebna za izvajanje pogodbe iz 1.b točke 6. člena GDPR.

Privolitev oziroma uporabnikovo soglasje je šibek člen takšne ureditve. Podjetja lahko večino uporabnikov v veliki večini primerov pripravijo do tega, da privolijo v kakršno koli obdelavo osebnih podatkov za namene oglaševanja, tako da je zaščitne mehanizme, ki jih določa zakonodaja o varstvu osebnih podatkov, preprosto mogoče zaobiti. To je mogoče doseči s kombinacijo metod, ki na različne načine izkoriščajo neznanje ali nepozornost uporabnikov ter obenem njihovo potrebo po prostem dostopu do storitev in vsebin, ki so ponujene v spletnem okolju. Soglasja uporabnika, na katerega se nanašajo osebni podatki, da privoli ali prekliče obdelavo svojih podatkov, ni mogoče opisati kot blanketno pooblastilo v zvezi z načinom obdelave njihovih podatkov.

4.2 Pravna funkcija in meja soglasja

Soglasje uporabnika obravnava evropska zakonodaja z več pravnimi sredstvi. LEUTP obravnava soglasje kot pravno podlago za obdelavo osebnih podatkov v skladu z odločitvijo uporabnika, na katerega se osebni podatki nanašajo. Sekundarna zakonodaja soglasju določa zahteve in omejitve, namenjene preprečevanju zlorab in izkoriščanju ranljivosti uporabnikov, na katere se osebni podatki nanašajo. Čeprav

[51] UL C 83/389, 30. 3. 2010, strani 1–408.

so te zahteve in omejitve zelo pomembne, doslej niso zadostovale za zagotovitev poštenosti danega soglasja porabnikov ali za preprečevanje množičnega zbiranja osebnih podatkov. GDPR določa, da mora soglasje biti prostovoljno dano in specifično za vsak primer posebej. Prav tako mora uporabnik biti informiran pred nedvoumno navedbo in željo, da poda izjavo ali izvede kakršno koli drugo konkludentno ravnanje. Vendar pa ni vse tako dorečeno. Temeljna nedorečenost v GDPR se namreč nanaša na svobodo privolitve, kadar je takšna privolitev zahtevana v zameno za storitev oziroma kadar je storitev pogojena s privolitvijo k obdelavi osebnih podatkov, zlasti z namenom ciljnega oglaševanja. GDPR v takem primeru neposredno ne izključuje prisilne izbire. Zato je v poslovnih praksah za dostop do spletnih storitev skoraj vedno potrebno soglasje. To pa uporabnike spodbuja k privolitvi in preprečuje uveljavitev pravice do preklica soglasja ali ugovora k obdelavi osebnih podatkov. Tudi Predlog uredbe o e-zasebnosti zahteva soglasje uporabnikov preko piškotkov, vendar tudi ta določba ne omejuje zbiranja in izkoriščanja osebnih podatkov, saj so uporabniki preprosto nevedni glede informacij o zbiranju podatkov in ne morejo oceniti kaj točno zapletene zahteve pomenijo, predvsem ker nimajo potrebnega pravnega znanja in časa ter potrebujejo nemoten dostop do spleta. Soglasje uporabnika obravnava tudi sporna določba v Direktivi o digitalni vsebini, ki navaja, da se zakon uporablja tudi za pogodbe, za katere je nasprotna storitev sestavljena iz osebnih podatkov uporabnikov. Sporno določilo v Direktivi o digitalni vsebini je podano ob predpostavki, da so osebni podatki že postali tržno blago. In čeprav so ti pogoji zaostreni v Aktu o digitalnih storitvah in Aktu o digitalnih trgih, ki predvsem preprečujejo posredovanje zbranih osebnih podatkov na osnovni platformi drugim sekundarnim platformam.

Akt o digitalnih storitvah določa vrsto obveznosti za spletne platforme, predvsem v smeri zahtev glede informacij o ciljnem oglaševanju, za zelo velike spletne platforme pa tudi zahteve glede oglasnega prostora, s tem da zadnjim nalaga tudi dolžnosti priprave ocene tveganja pravne zaščite temeljnih pravic in temeljnih svoboščin svojih uporabnikov. Glavno vodilo je privolitev uporabnika oziroma njegovo soglasje. To ima lahko eno (ali obe) od dveh funkcij: možnost uveljavljanja preklica in podajanja soglasja, ki je zavezujoče za druge, ter soglasje k pogodbenim določilom. Uporabnik lahko privoli v oboje, kar je tudi njegova avtonomna pravica. Vendar dano soglasje ni vedno pravno veljavno, kot to določajo splošna pravna pravila (nesposobnost, napaka volje, goljufija, prisila ali grožnja).

4.3 Soglasje v odnosu do Listine o temeljnih pravicah EU

Soglasje uporabnika, na katerega se nanašajo osebni podatki, je posebej navedeno v drugem odstavku 8. člena EKČP, ki določa, da je treba osebne podatke obdelovati pošteno in na podlagi privolitve uporabnika ali druge zakonske podlage. Potreba, da ima vsaka posamična obdelava osebnih podatkov pravno podlago, izhaja iz priznavanja varstva osebnih podatkov kot temeljne pravice, zajema pa celotno obdelavo podatkov in ne samo varstvo osebnih podatkov. Takšno načelo pomeni, da je obdelava osebnih podatkov prepovedana, če ni izpolnjen kateri koli od danih pogojev:

- obdelava mora temeljiti na svobodni izbiri uporabnika, na katerega se nanašajo osebni podatki, s čimer se odpoveduje prepovedi (gl. točke 1.b do 1.f 6. člena GDPR);
- obdelava temelji na nujnosti namena, ki upravičuje poseg v temeljno pravico uporabnika.

Soglasje uporabnika dano za namene ciljnega oglaševanja je tako eden od najpogosteje zahtevanih z namenom nadaljnje obdelave osebnih podatkov. Takšna obdelava ne vpliva samo na nadaljnje nakupe, temveč tudi na prikaze javnega mnenja, javnih anket in politične razprave. Trenutno veljavni poslovni oglaševalski model zahteva soglasje, kar uporabnika prisili v privolitev, s tem pa tudi k širjenju svojih osebnih podatkov. Po eni strani to lahko povzroči vsesplošen nadzor, po drugi strani pa uporabnike izpostavlja možnostim manipulacij v odločitve, ki jih drugače ne bi sprejeli. Vse te zbrane podatke je mogoče tudi nadalje prodati na podatkovnem trgu, kjer dosegajo astronomske vrednosti.

4.4 Soglasje uporabnika v odnosu do GDPR

Soglasje oziroma privolitev uporabnika je opredeljena v 11. točki 4. člena GDPR, pri čemer je to pojmovano kot vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj. Takšna opredelitev velja tudi za primere ciljnega oglaševanja. Glavno vprašanje pa je, ali in pod kakšnimi pogoji je uporabnik privolil v zbiranje osebnih podatkov v komercialne namene in ali takšno soglasje izpolnjuje vse zakonske

zahteve. S tem namenom je opredelitev soglasja, podana v GDPR, razširjena z nekaterimi uvodnimi točkami.

Zahteva po informiranosti je specifična zahteva, saj zadeva količino in vrsto ustrezno podanih informacij, ki morajo biti na razpolago posamezniku. Kot je navedeno v točki 42 GDPR, mora biti posameznik, na katerega se osebni podatki nanašajo, obveščen o identiteti upravljavca podatkov in namenu obdelave osebnih podatkov. V uvodni točki 32 je tudi določeno, da bi moralo soglasje zajemati vse načine obdelave osebnih podatkov. Načelo obveščenosti in s tem privolitve je povezano z idejo o transparentnosti, saj lahko rečemo, da so uporabniki, na katere se nanašajo osebni podatki, obveščeni le takrat, ko imajo možnost v celoti poznati specifičnost obdelave njihovih osebnih podatkov. Zato mora biti ta informacija izčrpna in natančna ter obenem jasna in razumljiva, kar izhaja tudi iz uvodne točke 58, ki se nanaša na spletno oglaševanje. Načelo transparentnosti oziroma preglednosti zahteva, da so vse informacije, naslovljene širši skupini ali posamezniku, na katerega se nanašajo osebni podatki, jedrnate, lahko dostopne in razumljive, da se uporablja jasen in preprost jezikovni slog ter tam, kjer je to primerno, tudi vizualni prikaz. Vendar takšna transparentnost izgubi pomen, ko se podatki posredujejo v obdelavo tretjim osebam, ne da bi uporabnik poznal identiteto teh oseb in način obdelave njihovih osebnih podatkov. Če uporabnik prebere pravilnik o zasebnosti katere koli aplikacije, lahko zasledi, da te tretje osebe, ki bodo obdelovale njegove osebne podatke, sploh niso poimensko imenovane. In če gremo še dlje, lahko te tretje osebe podatke izmenjujejo s svojimi tretjimi partnerji in tako dalje. Povedano drugače, uporabnik sploh nima pregleda, kako in kam se prenašajo njegovi osebni podatki ter tudi ne kako se uporabljajo. Preprosta transakcija na spletu lahko vključuje na stotine tretjih oseb, ki imajo svojo politiko glede obdelave podatkov in uporabnik do teh ne more dostopati, kakor tudi ne podati soglasja. Čeprav to ni izrecno navedeno v GDPR, lahko trdimo, da bi moralo načelo transparentnosti in informiranosti zajemati tudi informacijo o vseh nadaljnjih obdelavah in posredovanju osebnih podatkov, posebej pa bi moralo vključevati navedbo o tem, kakšna so tveganja, če uporabnik poda soglasje.[52] Takšna ideja je podana v uvodni točki 20 Predloga uredbe o e-zasebnosti, ki se glasi: »Ponudniki storitev morajo sprejeti ustrezne ukrepe za zagotovitev varnosti svojih storitev, če je treba, skupaj s ponudnikom omrežja, in obvestiti naročnike o vseh posebnih tveganjih za kršitve varnosti omrežja. Takšna

[52] Lavrijssen et al, 2022, strani 1–24.

tveganja so zlasti možna pri elektronskih komunikacijskih storitvah v odprtem omrežju, kot sta internet ali analogna mobilna telefonija. Za naročnike in uporabnike takšnih storitev je zlasti pomembno, da jih njihov ponudnik storitve v celoti seznani z obstoječimi varnostnimi tveganji, ki so zunaj obsega ponudnikovih možnih sredstev za ukrepanje. Ponudniki storitev, ki ponujajo javno dostopne elektronske komunikacijske storitve prek interneta, morajo obvestiti uporabnike in naročnike o ukrepih, ki jih lahko sprejmejo za zagotovitev varnosti sporočil, na primer z uporabo posebnih vrst programske opreme ali tehnologij šifriranja. Zahteva po obveščanju naročnikov o posebnih varnostnih tveganjih ne razrešuje ponudnika storitve njegove obveznosti, da na svoje stroške sprejme ustrezne in takojšnje ukrepe za odpravo vsakih novih, nepredvidenih varnostnih tveganj in da zopet vzpostavi običajno raven varnosti storitve. Zagotovitev podatkov o varnostnih tveganjih za naročnika mora biti brezplačna, razen morebitnih nominalnih stroškov, ki jih naročnik lahko utrpi pri sprejemanju ali zbiranju podatkov, na primer z nalaganjem sporočila, poslanega po elektronski pošti. Varnost se ocenjuje z vidika 17. člena GDPR.

Uvodna točka 32 GDPR uvaja idejo o celovitosti informacij in razdrobljenosti, kar je mogoče obravnavati kot posledico informiranosti in specifičnosti z zahtevo, da privolitev zajema vse dejavnosti obdelave, izvedene v isti namen ali namene. Kadar je namreč obdelava večnamenska, je treba podati soglasje za vse namene obdelave. Od uporabnikov se pogosto zahteva splošno soglasje za obdelavo uporabnikovih osebnih podatkov v t. i. komercialne namene ali v namene s prilagojeno vsebino. Zahteva po razdrobljenosti pa je omejena pri znanstvenih raziskavah, kot to izhaja iz uvodne točke 33, ki dovoljuje privolitev le za nekatera znanstvenoraziskovalna področja, seveda ob upoštevanju priznanih etičnih standardov znanstvenega raziskovanja.

Uvodna točka 42 GDPR obravnava prostovoljno privolitev. V zvezi s tem navaja, da ta predpostavlja razpoložljivost ustreznih možnosti privolitve in da zavrnitev privolitve ne sme povzročiti škode. Privolitev se ne šteje kot prostovoljna, če posameznik, na katerega se osebni podatki nanašajo, nima možnosti dejanske ali prostovoljne izbire ali ne more umakniti podanega soglasja brez škode. V povezavi s to točko zakonodajalec glede nedovoljenih pogodbe napotuje na Direktivo Sveta 93/13/EGS z dne 5. aprila 1993 o nedovoljenih pogojih v potrošniških pogodbah[53]

[53] UL L 95, 21. 4. 1993, strani 29–34.

in zahteva, da je izjava o privolitvi s strani upravljavca vnaprej pripravljena, v zvezi z nedvoumnostjo in jasnostjo informacij pa določa, da mora biti vsaka takšna izjava, podana v razumljivi in lahko dostopni obliki, z uporabo jasnega in preprostega jezika in ne sme vsebovati nedovoljenih pogojev. Zahtevo, da je privolitev dana s pritrdilnim dejanjem je Sodišče EU obravnavalo v zadevi *Bundesverband der Verbraucherzentralen*,[54] kjer je navedlo, da privolitev ne zajema opustitve; da mora biti izjava volje iz točke h) 2. člena Direktive 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 (Direktiva 95/46)[55] med drugim »posebna« v smislu, da se mora nanašati prav na obdelavo zadevnih podatkov in je ni mogoče izpeljati iz izjave volje, ki ima drug cilj; in da ne gre za veljavno privolitev iz točke f) 2. člena in tretjega odstavka 5. člena Direktiva o zasebnosti in elektronskih komunikacijah v povezavi s točko h) 2. člena Direktive 95/46, če se shranjevanje podatkov ali dostop do podatkov, shranjenih v terminalski opremi uporabnika spletnega mesta, dovoli s potrditvenim poljem, ki ga je vnaprej označil ponudnik storitve in ki bi ga moral uporabnik, da zavrne svojo privolitev, odznačiti.

GDPR ima tudi poseben poudarek na »oblikovanju profilov« oziroma profiliranju, ki pomeni 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, kot to izhaja iz druge točke 4. člena. Profiliranje je namreč namenjeno razvrščanju oseb po skupinah, ki imajo skupne značilnosti, skupne vzorce vedenja, kar v povezavi z oglaševanjem striktno daje možnost ciljnemu oglaševanju ali vedenjskemu oglaševanju, saj so osebni podatki segmentiranih oseb že na razpolago, so analizirani, obdelani in pripravljeni z razpolagalnim namenom.

Kot je že zgoraj navedeno, je privolitev uporabnika ena od šestih podlag za zakonito obdelavo osebnih podatkov, kot to izhaja iz 6. člena GDPR. Taka obdelava je zakonita, če je izpolnjen vsaj eden od taksativno naštetih pogojev. Kot primarno je naveden pogoj, da je posameznik, na katerega se nanašajo osebni podatki, podal privolitev v obdelavo njegovih osebnih podatkov v enega ali več s tem določenih

[54] Prav tam, točki 57 in 58.
[55] UL L 281, 23. 11. 1995, strani 31–50.

namenov. To izhaja iz drugega odstavka 8. člena LEUTP, v katerem je privolitev izrecno navedena kot pravna podlaga za zakonito obdelavo osebnih podatkov. Soglasje je omenjeno tudi v četrtem odstavku 6. člena GDPR, kjer so podani pogoji, pod katerimi se osebni podatki lahko obdelujejo v druge namene, za katere uporabnik ni podal soglasja. Sprememba namembnosti podanega soglasja je dovoljena le, če je združljiva s prvotnim namenom privolitve.

GDPR ureja tudi obveščenost o možnosti preklica privolitve, kot to izhaja iz točke c) drugega odstavka 13. člena. Če namreč obdelava temelji na točki a) prvega odstavka 6. člena ali točki a) drugega odstavka 9. člena, ima uporabnik pravico, da lahko privolitev kadar koli prekliče, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na tej pravni podlagi izvajala do njenega preklica. Uporabniki se načeloma ne zavedajo te možnosti, saj ne berejo pravilnikov o zasebnosti.

4.5 Soglasje v odnosu do Predloga uredbe o e-zasebnosti

Soglasje kot možnost, predvsem zaradi obdelave osebnih podatkov v namene oglaševanja, je v Predlogu uredbe o e-zasebnosti navedena na več mestih.

Soglasje je omenjeno v prvem odstavku 5. člena, kjer je kot takšno navedeno za zbiranje podatkov na podlagi poslušanja, prisluškovanja, shranjevanja ali na drugih načinih prestrezanja ali nadziranja komunikacije (sporočila) in z njimi povezanih prometnih podatkov. V drugem odstavku tega člena je določeno, da prvi odstavek ne vpliva na zakonsko dovoljeno zapisovanje in snemanje, vendar le v primeru, da se to izvaja v okviru zakonite poslovne prakse z namenom, da se zagotovi dokaz o tržni transakciji ali kateri koli drugi komunikaciji. Takšna določba je ključnega pomena, saj obravnava predvsem piškotke in druge načine identifikacije in sledenja uporabnikov s spodbujanjem njihovih spletnih dejavnosti. Praksa, ki temelji na teh določbah, je paradigmatičen primer mehanizma privolitev. Njena implementacija, čeprav je predvsem namenjena zaščiti uporabnikov in njihovi obveščenosti pri odločanju o soglasju, je povzročila, da so prav ti uporabniki preobremenjeni z ogromnim številom zahtev za soglasje in dejansko soglasje podajo pasivno, ne zavedajoč se vsebine zahteve. V povezavi s piškotki je na tem mestu potrebno omeniti uvodno točko 25, ki navaja, da so vendar lahko take naprave, npr. t. i. »piškotki«, zakonito in uporabno orodje za ocenjevanje učinkovitosti zasnove spletne strani in oglaševanja ter za preverjanje identitete uporabnikov, vključenih v

sprotne (»on-line«) transakcije. Kadar so takšne naprave, npr. 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 z Direktivo 95/46 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.[56]

Soglasje je podano tudi na več drugih mestih v Predlogu uredbe o e-zasebnosti, in sicer: v tretjem odstavku 6. člena kot pogoj za neposredno tržno komuniciranje ponudnikov javno dostopnih elektronsko komunikacijskih storitev; v prvem odstavku 9. člena kot pogoj za zbiranje neanonimnih lokacijskih podatkov; v tretjem odstavku 12. člena kot pogoj za uporabo podatkov v naročniškem imeniku brez iskanje kontaktov (čeprav imajo možnost uporabniki umakniti svoje podatke iz takšnih imenikov); v 13. členu kot pogoj za sprejem nenaročenih avtomatiziranih klicev in komunikacijskih sistemov (uporabniki imajo možnost zavrniti kakršnekoli nenaročene klice neposrednega trženja).

Namen predvidene Uredbe o e-zasebnosti, s katero bi se nadomestila Direktiva 2002/58, je dopolniti določila GDPR v zvezi z elektronsko komunikacijo in obdelavo podatkov, s čimer bi se nadgradilo pojem in zahteve privolitve, ki so opredeljeni v GDPR.

[56] Zadeva C-673/17, Planet49 GmbH proti Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV, ECLI:EU:C:2019:801 (*Bundesverband der Verbraucherzentralen*), točka 7.

4.6 Soglasje v odnosu do Direktive o digitalni vsebini

Privolitev v obdelavo osebnih podatkov implicitno navaja Direktiva o digitalni vsebini v prvem odstavku 3. člena, v skladu s katerim se ta uporablja za vse pogodbe, pri katerih trgovec potrošniku dobavi digitalno vsebino ali digitalno storitev ali se k temu zaveže, potrošnik pa plača kupnino ali se k temu zaveže. Direktiva se ne uporablja le, kadar potrošnik plača kupnino, ampak tudi, kadar protistoritev vključuje posredovanje osebnih podatkov, ki niso potrebni za zagotovitev storitve. Ta direktiva se ne uporablja za digitalno vsebino ali digitalne storitve, ki so vključene v blago v smislu 3. točke 2. člena ali so z njim medsebojno povezane in ki se zagotavljajo z blagom v skladu s prodajno pogodbo za to blago, ne glede na to, ali tako digitalno vsebino ali digitalno storitev dobavlja prodajalec ali tretja oseba. V primeru dvoma, ali je dobava vključene ali medsebojno povezane digitalne vsebine ali digitalne storitve del prodajne pogodbe, se šteje, da je digitalna vsebina ali digitalna storitev zajeta s prodajno pogodbo. Očitno je, da ta določba predpostavlja, da se lahko osebni podatki prevzemajo z namenom oglaševanja ali drugih komercialnih poslov kot protistoritev vsebini. Med prvim odstavkom 3. člena GDPR in sedmim odstavkom 4. člena GDPR obstaja diskrepanca, saj slednji zagotavlja domnevo prostovoljnosti privolitve v takšne transakcije. Na tem mestu je treba opozoriti, da zagotovitev osebnih podatkov ne bi smela šteti za protistoritev ponujene storitve, niti se ne bi smelo šteti kot plačilo, pod katerim koli drugim opisom. Privolitev tudi ne bi smela biti združena s sprejemom pogojev, temveč bi morala biti ločena od privolitve, ki je potrebna zaradi sklenitve pogodbe. V tretjem odstavku 8. člena je navedeno, da ta direktiva ne vpliva na zakonodajo o varstvu podatkov, isti člen pa nadalje določa, da v primeru nasprotja med določbami te direktive in pravom EU o varstvu osebnih podatkov prevlada slednje.

Soglasje v trenutno veljavni Direktivi 2002/58 ni bilo ustrezno opredeljeno, predvsem zato, ker je bilo sprejeto v času počasnega razvoja spletnega okolja. Prav ta pomanjkljivost je razlog za reformo. V uvodnih točkah Predloga uredbe o e-zasebnost je navedeno, da veljavna Direktiva 2002/58 ni bila učinkovita v zvezi z zasebnostjo nameščene terminalske opreme ter da soglasje uporabnikov pri uporabi terminalskih naprav (ki shranjujejo oziroma zbirajo osebne podatke iz uporabnikovih naprav) ni ščitilo uporabnika, hkrati pa je ustvarila nepotrebno breme tako za podjetja kakor za potrošnike.

Določba 6. člena GDPR določa pogoje, pod katerimi lahko dano soglasje zagotavlja pravno podlago za obdelavo komunikacijskih podatkov in metapodatkov (identifikatorji posameznikov, ki komunicirajo s podatki o njihovi lokaciji). V skladu s točko c) 2. odstavka je s soglasjem uporabnikov dovoljena obdelava metapodatkov le za namene, ki jih ni mogoče doseči samo z uporabo anonimnih podatkov.

5 Zaključek

Ciljno in vedenjsko oglaševanje je postalo vseprisotno na internetu, kar je sprožilo nastanek novih internetnih sistemov, katerih vmesni sistemi imajo dostop do osebnih in zasebnih podatkov milijarde uporabnikov. Resno tveganje za zagotavljanje zasebnosti uporabnikov je v pomanjkanju preglednosti spletnega oglaševanja, predvsem v smislu naprednih in vsiljivih sistemov sledenja, pretoka informacij med različnimi oglaševalskimi platformami ter oglaševalskimi podjetji in podjetij za analizo podatkov, sistemov profiliranja na podlagi osebnih podatkov in način dostave ciljnih oglasov. V različni literaturi je bilo ponujenih več rešitev za povečanje varstva zasebnosti v tako zapletenem oglaševalskem sistemu. Prva ideja je, da varstvo zasebnosti in varstvo osebnih podatkov kot temeljni pravici uporabnika vključuje tudi njegovo svobodo, da razpolaga s svojimi osebnimi podatki kot »digitalnim portfeljem« oziroma premoženjem, s katerim lahko trguje. Takšna opredelitev bi pomenila, da bi morali imeti posamezniki, na katere se nanašajo osebni podatki, individualno moč za izključno licenciranje svojih osebnih podatkov v zameno za protistoritev ali drugo vrsto ekonomsko vrednega nadomestila. Takšno »nadomestilo« bi vključevalo soglasje, da rezultati obdelave osebnih podatkov vplivajo na uporabnika samega v smislu prejemanja ciljnega oglaševanja ali celo vedenjskega oglaševanja. Druga ideja je, da bi morali uporabniki, na katere se nanašajo osebni podatki, uživati svobodo bivanja v digitalnem svetu, ne da bi bili izpostavljeni možnostim izkoriščanja, diskriminacije in manipulacije, ki jih omogoča obdelava njihovih osebnih podatkov, prav tako tudi, da ne bi bili s posredovanjem osebnih podatkov podvrženi vsesplošnemu nadzoru. Položaj posameznikov proti položaju upravljavcev podatkov je diametralno nasproten, saj pravica do privolitve skoraj vedno povzroči, da posamezniki, na katere se nanašajo osebni podatki, kot predpogoj ali kot protistoritev prostovoljno dajo na razpolago svoje podatke. Na ta način z namenom oglaševanja lahko oddani posebni podatki povzročijo bodisi »*hungry judges*« bodisi »*echo chamber*« bodisi »*filter bubble*« učinke in cilj oglaševanja je dosežen – doseže namreč le tisto publiko, ki jo želi doseči.

Za pravno varstvo ima uporabnik trenutno na razpolago le soglasje, ki je opredeljeno v različnih pravnih aktih, vendar je to soglasje v veliki večini le pravna opredelitev, ki ne doseže namena povprečnega uporabnika. Ta namreč da v zameno lahkotnosti bivanja v digitalnem okolju soglasje za obdelavo svojih podatkov. Prav takšna obdelava pa povzroči segmentiranje tega uporabnika v določeno skupino ciljno ali vedenjsko segmentiranih skupin, do katere bo akcijski oglas v zelo kratkem prišel ali se bo uporabnik z njim seznanil. Ker mu bo blizu bodisi po enem od demografskih podatkov bodisi po vrednotah, bo sredstvo opravičevalo cilj, uporabnik pa bo na podlagi lastnih osebnih podatkov postal tudi kupec ali prejemnik akcijske vsebine oglasa. Uporabnik je z namenom oglaševanja sicer v središču dogajanja, pri čemer obstoječa pravila o varstvu podatkov niso najboljše sredstvo za njegovo pravno varstvo.

Literatura

Bainbridge, D. (1996) EC Data Protection Directive (Current EC legal developments) (Vancouver: Lexis Law Publishing).

Borghi, M. (2013) Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK. International Journal of Law and Information Technology, strani 109–153.

Danziger, S., Leval, J., Avnaim-Pesso, L. (2011) Extraneous factors in judicial decisions. *Proc Natl Acad Sci USA* 108, strani 6889–6892.

De Hert, P. (2012) The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer law & Security Review, 28(2), strani 130–142.

Jančič, Z., Žabkar, V. (2013) Oglaševanje (Ljubljana: Založba FDV).

Kelleher, D. (2006) Privacy and Data Protection Law in Ireland (Galway: Tottel Publishing).

Lanier, J. (2018) Ten arguments for deleting your social media accounts right now (New York: Henry Holt & Co).

Lavrijssen, S., Apraez B.E., ten Caten, T. (2022) The legal complexities of processing and protecting personal data in electricity sector, Energies, 15(3), strani 1–24.

Primožič Leka, B. (2016) Oglaševanje: orodje za spreminjanje navad uporabnika, magistrsko delo (Ljubljana: Fakulteta za družbene vede).

Omer, T. (2010) Privacy: The new generations, International Data Privacy Law Advance, 1(1), strani 1–8.

Repas, M., Vrenčur, R., Zajc, B. (2005) Pravni priročnik za trženje (Ljubljana: GV Založba).

Sartor, G. (2020) New Aspects and Challenges in Consumer Protection, Study PE 648.790, European Parliamentary Research Service, Policy Department for Economic, Scientific and Quality of Life Policies (Luxemburg: European Parliament).

Štirn, T. (2003) Nove oblike oglaševanja ob prelomu tisočletja, diplomsko delo (Ljubljana: Fakulteta za družbene vede).

Vosoughi, S. (2018) The spread of true and false news online, Science, 359(6380), strani 1146–1151.

SUMMARY

Nowadays, we are witnesses of the extremely rapid growth of informatics, cloud computing, artificial intelligence (e.g., machine learning, neural networks, and language prediction) and big data ("big data" in the sense of predictive analytics), which has led to the creation of new techniques for tracking and profiling users, and thus also targeted advertising that is adapted to the habits and tastes of the user to whom it refers. Regardless of the effectiveness of targeted advertising, it is also necessary to consider the protection of data collected in this way. And although almost all regulations deal with this phenomenon from the point of view of data protection itself, effective legal protection requires a holistic approach, considering intellectual property, consumer protection and competition law itself.

However, a fundamental human right is the protection of personal data, which nowadays has become digital gold and, as such, the user's digital portfolio. Based on the collection of the user's personal data, when the latter unknowingly confirms any notification about the collection of data, he hands over his personal data for an unknown purpose of processing and to an unknown data manager who disposes with them freely. On this basis, the collected data is analysed, processed and the user is segmented into different groups of users, either according to their values or according to other demographic data, which significantly facilitates the achievement of targeted and behavioural advertising campaigns, and here the ads deliberately reach these groups to whom these ads are intended. Google is used as an example, as the largest player in the world of targeted advertising. From this point of view, behavioural advertising is shown in connection with the "*echo chamber*" and "*filter bubble*" effects and whether such advertising can be prevented or regulated through the regime of unfair business practices. Furthermore, as part of the same browser, the original article "*Hungry judges*", published in 2011, is shown in comparison with articles on the same topic but with different study results. This is to show how advertising algorithms and collected user personal data are already prepared at this stage to be able to evaluate how the user thinks, what are his values and, above all, to offer him the search results that are closest to him.

The user can only "protect" himself with the consent he gives when visiting websites. However, it must be recognised that advertising companies are not implementing the data collection consent regime required by regulators, and general regimes such as notice and consent envisaged by the upcoming e-Privacy regulation cannot succeed in a ready manner, so companies should be introduced with very strict opt-out mechanisms provided that the right to cancel is exercised. At the same time, the information that the user receives before giving consent must be clear, short, and given in an interactive and unified system, so that the lay user can understand it. For marketing purposes, the user should be at the centre of advertising, but data protection rules may not be the best means of ensuring his legal protection.