PRAVNI IZZIVI UPRAVLJAVCEV DIGITALNIH PLATFORM V OKVIRU PARADOKSA ZASEBNOSTI

ZORAN DIMOVIĆ
Hella Saturnus Slovenija d.o.o., Ljubljana, Slovenija
zoran.dimovic@student.um.si

Digitalna industrija že dlje časa spodbuja rast digitalnih platform, ki pridobivajo vedno večji tržni delež, kar kaže na nadaljevanje tega trenda tudi v prihodnje. Infrastruktura delovanja se je premaknila v mobilno in digitalno okolje, kjer so posamezniki vse bolj izpostavljeni delitvi osebnih podatkov. Akt o digitalnih trgih opredeljuje ključne obveznosti za upravljavce platform, zlasti glede dostopa do osebnih podatkov. Platforme morajo omogočiti brezplačen dostop poslovnim uporabnikom do teh podatkov. V tem članku se raziskuje paradoks zasebnosti, pri čemer se osredotoča na ravnotežje med digitalnim udobjem in zaščito pravice do zasebnosti. Avtor obravnava izzive, s katerimi se soočajo upravljavci digitalnih platform, in kako ti vplivajo na ravnotežje med tehnološkimi inovacijami in varovanjem osebnih podatkov.

DOI
https://doi.org/10.18690/um.pf.5.2024.9

ISBN
978-961-286-931-1

Ključne besede:
varstvo osebnih podatkov, digitalne platforme, zasebnost, konkurenčnost, enotni trg, digitalni trg, paradoks zasebnosti

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/10.18690/um.pf.5.2024.9

ISBN
978-961-286-931-1

Legal Challenges of Digital Platform Operators in the Context of the Privacy Paradox

Zoran Dimović
Hella Saturnus Slovenija d.o.o., Ljubljana, Slovenia
zoran.dimovic@student.um.si

Keywords:
personal data,
digital platforms,
privacy,
market competition,
single market,
digital market,
privacy paradox

The digital industry has long driven the growth of platforms that dominate market share, a trend expected to continue. The shift to mobile and digital environments exposes individuals to sharing personal data. The Digital Markets Act outlines key responsibilities for platform operators, particularly regarding access to personal data, requiring platforms to provide business users with free access. This article explores the privacy paradox, focusing on the balance between digital convenience and the right to privacy, and examines the challenges faced by platform operators in balancing innovation with data protection.

University of Maribor Press

1 Uvod

Nenehna rast velikih digitalnih podjetij, koncentracija digitalnega trga in neharmonizirana ureditev digitalnega okolja je sprožila vrsto polemik, predvsem na področju zasebnosti, delovnopravne zakonodaje, varstva potrošnikov v digitalnem okolju, upravljanja podatkov ter varstva osebnih podatkov, predvsem zaradi izjemno močne koncentracije in monopola digitalnih igralcev, za katere do sprejema Akta o digitalnih trgih ne bi bila uporabljiva preprosta načela konkurence. Prav zaradi slednjega je Evropska komisija bila prisiljena predlagati nova pravila, namenjena učinkovitejšemu obravnavanju konkurenčno omejevalnih ravnanj v skladu z določili 101. in 102. člena Pogodbe o delovanju Evropske Unije[1] (PDEU), ki se je odrazil s sprejemom uredbe, ki regulira delovanje digitalnega trga ter njegovih digitalnih igralcev. Tako je 2. maja 2023 pričela veljati 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[2] (Akt o digitalnih trgih), ki ga je Evropska komisija sprejela 1. novembra 2022. Akt o digitalnih trgih vsebinsko spada v širšo strategijo enotnega digitalnega trga, ki je s seboj prinesla številne predloge uredb urejanja digitalnega trga.[3]

Akt o digitalnih trgih v pravno terminologijo digitalnega okolja umešča nov izraz, »vratar« oziroma digitalni posrednik. Sam izraz je le navidezno izviren, saj se ta izraz v enakovrednem kontekstu uporablja bistveno dlje časa. Za samo navidezno izvirnostjo besede ter njenega vsebinskega konteksta pa se zdi, da tudi s sprejemom Akta o digitalnih trgih ostajajo digitalni igralci, torej podjetja, ki so v zadnjih letih imela monopol na digitalnem trgu, enaka. V samem Aktu o digitalnih trgih je zaslediti

[1] UL C 326, 26. 10. 2012, strani 1–271.
[2] UL L 265/1, 12. 10. 2022, strani 1–66.
[3] Sporočilo komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in odboru regij »Strategija za enotni digitalni trg za Evropo«, COM(2015) 192 final, 6. 5. 2015; glede najnovejših uredb glej spletno stran Evropske komisije, na primer »Evropa, pripravljena na digitalno dobo«, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_sl; med najnovejše akte pa sodijo Uredba (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. oktobra 2022 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (UL L 277, 27. 10. 2022, strani 1–102; Akt o digitalnih storitvah); Uredba (EU) 2023/1781 Evropskega parlamenta in Sveta z dne 13. septembra 2023 o vzpostavitvi okvira ukrepov za okrepitev evropskega polprevodniškega ekosistema in spremembi Uredbe (EU) 2021/694 (UL L 229, 8. 9. 2023, strani 1–53; Akt o čipih); Predlog Uredbe Evropskega parlamenta in Sveta o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo okvira za evropsko digitalno identiteto (Akt o digitalni identiteti), SEC(2021) 228 final; Uredba (EU) 2023/2854 Evropskega parlamenta in Sveta z dne 13. decembra 2023 o harmoniziranih pravilih za pravičen dostop do podatkov in njihovo uporabo ter spremembi Uredbe (EU) 2017/2394 in Direktive (EU) 2020/1828 (UL L 2023/2854, 22. 12. 2023; Akt o podatkih); predlog Uredbe Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci) in spremembi nekaterih zakonodajnih aktov Unije (21. 4. 2021, COM(2021) 206 final); ter ostali.

številne izraze, s katerimi so jasno opredeljeni sedanji in prihodnji monopolni igralci, kar omogoča večplastno naravo tržnega vpliva. Ti izrazi so oblikovani z namenom, da zajamejo vsa podjetja, ki so že do sedaj dominirala na digitalnem trgu, ter omogočijo, da njihov vpliv ostane oportunitetno zajet in nadzorovan. In čeprav nekaterim od teh izrazov manjka strogost definicije, ki se pričakuje od pravne terminologije, ima tudi sam Akt o digitalnih trgih mestoma dvoumne utemeljitve in nepregledne rešitve ter dejansko ponuja komaj kaj več od obstoječih predpisov, ki jih imajo predpisi o varstvu osebnih podatkov, nadzora nad podatki in informacijami ter predpisi o konkurenčnosti in poštenosti digitalnega sektorja. Vsled svojem namenu spodbujanja poštenosti in konkurenčnosti na digitalnih trgih pa s seboj prinaša tudi posledice na račun inovativnega podjetniškega okolja in pravne varnosti potrošnikov. Akt o digitalnih trgih nalaga vratarjem *ex ante* regulativne obveznosti, ki se razlikujejo od dosedanjih *ex post* protimonopolnih odgovornosti. S tem akt prepoveduje inovativne poslovne prakse, ki so bile prej sprejete, saj bi takšne inovacije zdaj lahko izvajali le potencialni vratarji, kar omejuje možnosti ostalih podjetij na digitalnem trgu. Takšna inherentna subjektivnost s premikom k *ex ante* regulaciji vzpostavlja *status quo* napram podjetniški inovativnosti. Akt o digitalnih trgih vsebinsko daje prednost statični konkurenci in omejuje dinamičnost konkurenčnega okolja, z drugimi besedami daje prednost previdnosti pred inovacijami.

Razen že prej navedenih, ima Akt o digitalnih trgih v svoji zasnovi več primarnih pomanjkljivosti. Prvič, vsebinsko ne prispeva politiki Digitalne strategije EU,[4] katere cilj ni fragmentirano in neharmonizirano pravo EU, temveč digitalna inovativnost, učinkovitost in produktivnost. Kot tak bo Akt o digitalnih trgih deloval v diametralnem nasprotju s cilji Digitalne strategije EU, predvsem zaradi uvajanja omejevalnih ukrepov in regulativnih obveznosti, ki že same po sebi škodujejo inovacijam. Sama zasnova Akta o digitalnih trgih državam članicam EU daje moč izvršilne veje oblasti posamezne države članice, kar omogoča razdrobljenost sekundarnih pravnih virov EU ter je *a priori* v nasprotju z načelom primarnosti prava EU.[5] In drugič, Akt o digitalnih trgih vsebuje *per se* prepovedi, ki niso z ničemer

[4] Glej »Evropa, pripravljena na digitalno dobo« [dostopno na https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_sl] (obiskano 30. 1. 2024).

[5] Čeprav ni navedeno v PEU in PDEU, načelo primarnosti (tudi »prevlada« ali »nadrejenost«) prava EU temelji na tem, da v primeru navzkrižij med vidikom prava EU in vidikom prava države članice EU (nacionalnega prava) prevlada pravo EU. V nasprotnem primeru bi države članice EU lahko preprosto dosegle, da bi njihovi nacionalni predpisi prevladali nad primarno ali sekundarno zakonodajo EU, izvajanje politik EU pa bi postalo neizvedljivo.

utemeljeni v okviru splošnega načela sorazmernosti EU.[6] Kot tretje vsebuje tudi številne obveznosti in obenem diametralno nasprotne prepovedi, ki bi lahko bili v nasprotju z drugimi uredbami in direktivami EU ter primarnimi pravnimi viri EU, kar bo neizogibno privedlo do pravne negotovosti in posledično sodnih sporov. Samo vedenje o možnosti teh pa po naravi stvari zmanjšuje inovativni potencial podjetij. Poslovni subjekti bodo tako razvojna sredstva, ki so jih do sedaj imeli za razvoj in inovacije, raje umeščali v zasledovanje skladnosti delovanja s sprejetimi predpisi namesto v inovativne digitalne izboljšave.

Bolj natančno vsebinsko gledano, v Aktu o digitalnih trgih vratarji predstavljajo vmesni člen oziroma stično točko med večimi digitalnimi podjetji oziroma znotraj širše skupine digitalnih igralcev, ki zagotavljajo storitve jedrnih platform. Podobno kot pri izrazu »vratar« tudi izrazu »jedrna platforma« manjka jasna definicija, ki je skozi celoten akt ne zasledimo, le drugi odstavek 2. člena Akta o digitalnih trgih navaja, da jedrna platformna storitev pomeni kar koli od naslednjega: (a) spletne posredniške storitve; (b) spletne iskalnike; (c) spletne storitve družbenega mreženja; (d) storitve platform za izmenjavo videov, (e) medosebne komunikacijske storitve, neodvisno od številke; (f) operacijske sisteme; (g) spletne brskalnike; (h) virtualne pomočnike; (i) storitve računalništva v oblaku; (j) storitve spletnega oglaševanja, vključno z oglaševalskimi omrežji, oglaševalskimi izmenjavami in vsemi drugimi oglaševalskimi posredniškimi storitvami, ki jih zagotavlja podjetje, ki zagotavlja katero koli jedrno platformno storitev iz točk (a) do (i). Že na pravi pogled manjkajo storitve digitalne identite, storitve digitalnih denarnic, umetnointeligenčna interakcijska okolja in podobno, ki so tudi med storitvami, ki prežemajo digitalni trg. In navkljub heterogenosti teh postavk (vse pripadajo digitalnemu okolju), imajo osnovne storitve jedrnih platform nekatere značilnosti, ki bi lahko pomembno vplivale na razvoj digitalnih trgov. Med te štejemo tako ekonomijo obsega, kakor tudi omogočanje dostopa do enormnih količin podatkov ter obdelavo osebnih podatkov, pri čemer je bil namen Evropske komisije, da vratarji predstavljajo stičišče med poslovnimi uporabniki in končnimi uporabniki, izven tega konteksta pa v resnici predstavljajo vstopno točko varovanega dostopa, s tem pa tudi nadzora nad pretokom digitalnih informacij ter njihove »zakonite« obdelave (v tem kontekstu osebnih podatkov, zasebnih slik, videov in podobno). Tako so z Aktom o digitalnih

[6] Poleg tega, da lahko posamezen poseg v določene pravice temelji le na legitimnem, stvarno upravičenem cilju, je treba po ustaljeni presoji vselej oceniti še, ali je ta v skladu z načeli pravne države, in sicer s tistim izmed teh načel, ki prepoveduje prekomerne posege EU ali države tudi v primerih, ko se z njimi zasleduje legitimen cilj (t. i. splošno načelo sorazmernosti).

trgih dejansko regulirane samo vstopne točke digitalnih velikanov, ne pa tudi osnovne oziroma izvorne platforme, ki poganjajo regulirane vratarje. V tem kontekstu digitalni vratarji v ekosistemu interneta zbirajo enormne količine podatkov, sam dostop do takšnih količin podatkov pa je pomemben parameter konkurenčnosti na digitalnem trgu in odpira številna pravna vprašanja glede konkurenčnosti in varovanja zasebnosti, pri čemer je ta članek osredotočen na varstvo zasebnosti in varstvo osebnih podatkov v kontekstu Akta o digitalnih trgih, ostala pravna vprašanja pa so izpostavljena le toliko, kolikor je potrebno, da bi bilo razumljivo tudi ozadje varstva temeljnih človekovih pravic in svoboščin.

Prispevek je vsebinsko razdeljen na tri bistvena poglavja. Uvodu sledi poglavje, ki opredeljuje razvoj vratarjev ter ostali pojmi za razumevanje ozadja nastanka pojmov s historičnega in sintaktičnega vidika, oboje v kontekstu varstva temeljnih človekovih pravic. Temu poglavju sledi poglavje o izzivih informacijske zasebnosti na digitalnih trgih, pri čemer je opredeljen tudi njen regulativni okvir. Najbolj pomembno je zadnje poglavje, katerega namen je izpostaviti nekatera pravna vprašanja nedoslednosti trenutne ureditve Akta o digitalnih trgih ter pravne izzive digitalnih vratarjev v okviru paradoksa zasebnosti kot konceptualnega modela, ki poskuša zajeti kompromis med digitalnim udobjem in informacijsko zasebnostjo posameznikov. Temu poglavju sledi zaključek, v katerem so substancirano prikazani posamezni zaključki raziskovalnih vprašanj ter izpostavljena druga vprašanja, ki bi jih bilo potrebno raziskati v okviru nadaljevanja vsebinskega raziskovanja izpostavljenega okvirja tega prispevka.

2 Digitalne platforme v kontekstu varstva pravice do zasebnosti

2.1 Trgovanje z osebnimi podatki v digitalnem okolju

Zbiranje in uporaba osebnih podatkov sta ključna dejavnika komercialnega uspeha številnih digitalnih platform. Uporabniki se nevede odpovedujejo svoji zasebnosti, ko uporabljajo brezplačne storitve, kot sta Facebook ali Google. Ti namreč s pomočjo piškotkov sledijo uporabnikom pri njihovem brskanju po spletu. Prav to zbiranje podatkov omogoča, da uporabnikom nudijo »brezplačen« dostop do svojih digitalnih platform. Osebni podatki in podatki na splošno so danes valuta, ki zagotavljajo t. i. »brezplačni« dostop do številnih spletnih storitev, izdelkov in tudi

naprednega digitalnega okolja. Na spletu[7] je mogoče najti podatke, da imajo osebni podatki uporabnikov določljivo vrednost. V okviru vrednotenja tehnoloških podjetij in njihovih uporabnikov je ocenjeno, da lahko osebni podatki enega uporabnika dosegajo vrednost do 720 $ na leto. Glede na navedeno je zbiranje in uporaba osebnih podatkov poslovni model digitalnih platform ter v povezavi z vedenjskim oglaševanjem personalizacija in uporabniku v celoti prilagojena storitev. S tem olajšanim delovanjem na spletu uporabniki dejansko sami sebi nastavijo ogledalo in preidejo v polje paradoksa zasebnosti, kot konceptualnega modela, ki poskuša zajeti kompromis med udobjem in temeljnimi pravicami, med katerimi je tudi pravica do zasebnosti. Medtem ko različne študije kažejo,[8] da ljudje želijo skrbno varovati svoje osebne podatke in svojo zasebnost, je enostavnost, s katero lahko stranke zaobidejo pogoje storitve ali pravilnike o zasebnosti v spletnih aplikacijah in na ostalih digitalnih platformah, del uganke varovanja zasebnosti v digitalni dobi, ki se predvsem tiče filozofije naravi človeka kot individuuma v družbenem okolju, v katerega je ta vpet.

2.2 Digitalne platforme in spletni iskalniki v okviru Akta o digitalnih trgih

Uvodoma je potrebno opredeliti pojem digitalne platforme. Digitalna platforma je bistveni gradnik razvoja digitalizacije in ima kot takšna bistveno vlogo v evropski digitalni družbi in njenem gospodarstvu. Po svoji vsebini digitalne platforme prevzemajo najrazličnejše oblike, od spletnih tržnic, multimedijskih vsebin, trgovin z aplikacijami, družbenimi mediji, spletnimi iskalniki in podobno. Digitalne platforme imajo skupen osnovni gradnik, tj. je uporaba informacijsko komunikacijskih tehnologij, ki v digitalnem svetu omogočajo lažjo interakcijo med poslovnimi subjekti in uporabniki ter z in med uporabniki. Digitalne platforme nenehno zbirajo in akumulirajo podatke o izvedenih interakcijah na različnih digitalnih okoljih, s tem pa prestavljajo repozitorij enormnih količin osebnih podatkov uporabnikov ter po drugi strani njegovo digitalno sito.

Za trg digitalnih platform so značilne različne oblike ekonomije obsega, dodane vrednosti digitalnega portfelja osebnih podatkov, kar posledično povečuje težnjo h koncentraciji digitalnega tržišča, s tem pa tudi dostop do tega digitalnega portfelja. V takšnem okolju, kjer velja načelo, da zmagovalec prevzame vse, se osnovna načela

[7] Glej Mitchell, 2023, https://medium.com/mydex/beware-what-you-wish-for-e59dd1975f79 (obiskano 30. 1. 2024).
[8] Antón in Young, 2010, stran 24.

konkurenčnega prava soočajo z nizom izzivov, ki jih razvoj velikih igralcev na digitalnem trgu s seboj prinaša. To velja tudi za sam Akt o digitalnih trgih. Prvič, takšna regulacija ne bo mogla učinkovito preprečiti izkrivljanja konkurence ter posledično ohraniti osnovnih oblik dinamik rivalstva, ki ga spodbuja vstop potencialnih konkurentov na koncentriran digitalni trg, saj bi ti lahko ogrozili uveljavljene tržne položaje. Kot drugič, sama konkurenčnost ima svoje korenine v strukturnih značilnostih posamezne industrije, za kar veljajo osnovna pravila konkurence, vendar v primeru digitalnega okolja ta zahteva širši nabor pravnih sredstev od tistih, ki so do sedaj na razpolago. Kot tretje, z neharmoniziranimi in neusklajenimi pravili digitalnega trga, se povzroča pravna negotovost in posledično kršitev temeljnih človekovih pravic, med katerimi sta tudi pravica do zasebnosti in pravica do varstva osebnih podatkov.[9]

Spletni iskalniki opravljajo tri ključne funkcije. Prva je zbiranje informacij, ki so dostopne na spletu, z uporabo programov, ki omogočajo prehode s spletne strani na spletno stran (imenovano »*crawling*«). To pomeni, da iskalnik z algoritmi pregleduje vsebino različnih spletnih mest in zbira informacije, ki so javno dostopne. Druga funkcija je zbiranje podatkov in metapodatkov ter ustvarjanje indeksirane baze teh podatkov. Ta indeksirana baza omogoča hitrejše iskanje določenih spletnih mest, ko uporabnik vnese iskalni izraz. Tretja in zadnja funkcija je uporaba te indeksirane baze, da uporabniku omogoči prikaz relevantnih rezultatov iskanja glede na vneseni iskalni pogoj.

Brez spletnih iskalnikov bi bilo iskanje po spletu veliko bolj zamudno in zahtevno, saj bi morali uporabniki ročno preiskovati posamezna spletna mesta. Spletni iskalniki pa s svojo funkcionalnostjo omogočajo enostaven dostop do informacij. Zbirajo različne vrste podatkov, vključno z osebnimi podatki uporabnikov, ki jih lahko nato uporabijo za prilagajanje rezultatov iskanja. Iskalniki v resnici niso ustvarjalci digitalnih vsebin, saj razvrščajo in prikazujejo vsebine drugih spletnih mest. V tem kontekstu delujejo kot »meta medij«, ki omogoča dostop do izbranih informacij na podlagi svojih algoritmov. Ker ti algoritmi delujejo na subjektiven način, je mogoče, da nekatere pomembne informacije izpustijo ali uporabniku ne prikažejo.[10]

[9] Siagian 2023, strani 514–516.
[10] Asunción, 2017, strani 36–47.

Čeprav spletni iskalniki kot taki omogočajo večji dostop do informacij, dejansko posegajo v pravico posameznika do zasebnosti. S tem ko zbirajo podatke o uporabnikih, kot so njihovi iskalni izrazi, obiskanost spletnih mest in druge interakcije na spletu, ustvarjajo profil uporabnika, ki se lahko uporablja za oglaševanje ali druge komercialne namene. Prav zaradi tega se pojavlja vprašanje kršitve pravice do varstva osebnih podatkov.

Glede na zakonodajo EU spletni iskalniki ne spadajo neposredno pod določbe Akta o digitalnih trgih. Spletni iskalniki niso v celoti opredeljeni kot telekomunikacijske storitve in zato ne spadajo v kvantitativna merila, ki jih določa zakonodaja. Na primer, tretji odstavek 1. člena Akta o digitalnih trgih določa, da se ta ne uporablja za trge, ki so povezani z elektronskimi komunikacijskimi omrežji, kot so opredeljeni v Direktivi (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacij[11] (Evropski zakonik o elektronskih komunikacijah). To pomeni, da spletni iskalniki, kljub svoji pomembni vlogi v digitalnem ekosistemu, ostajajo v pravnem vakuumu, saj ne sodijo neposredno pod ta pravila. Tretji odstavek 1. člena Akta o digitalnih trgih namreč določa, da se ta ne uporablja za trge, povezane z elektronskimi komunikacijskimi omrežji. Ti so opredeljeni v 1. točki 2. člena Evropskega zakonika o elektronskih komunikacijah). Obenem se ne uporablja za elektronske komunikacijske storitve, kakor so opredeljene v 4. točki 2. člena Evropskega zakonika o elektronskih komunikacijah, razen tistih, ki so povezane z medosebnimi komunikacijskimi storitvami, neodvisnimi od številke. Za te velja, da gre za prenosne sisteme, ne glede na to, ali temeljijo na stalni infrastrukturi ali centralizirani upravni zmogljivosti, in, kjer je primerno, komutacijsko ali usmerjalno opremo ter druge vire, vključno z omrežnimi elementi, ki niso aktivni, ki omogočajo prenos signalov po žicah, z radijskimi valovi, z optičnimi ali drugimi elektromagnetnimi sredstvi, vključno s satelitskimi omrežji, fiksnimi (vodovno in paketno komutiranimi, vključno z internetom) in mobilnimi omrežji, električnimi kabelskimi sistemi, če se uporabljajo za prenos signalov, omrežji, ki se uporabljajo za radijsko in televizijsko radiodifuzijo, ter z omrežji kabelske televizije, ne glede na vrsto prenesenih informacij.

Prav tako se za spletne iskalnike pogosto uporabljajo izjeme, ki izhajajo iz Direktive 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na

[11] UL L 321, 6. 12. 2003, strani 276–*280*.

notranjem trgu[12] (Direktiva o elektronskem poslovanju). Ta direktiva določa, da se spletni iskalniki štejejo kot storitve informacijske družbe, vendar pa imajo določene izjeme pri prenosu podatkov, kot sta »izključni prenos podatkov« in »shranjevanje v predpomnilniku«. To pomeni, da iskalniki niso odgovorni za vsebino, ki jo prenašajo ali shranjujejo v predpomnilniku, če se podatki med prenosom ne spreminjajo. Pri tem velja opomniti, da za iskalnike izjeme iz 12., 13. in 14. člena Akta o digitalnih trgih ne veljajo. Nadalje to pomeni, da ne glede na določila Uredbe (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[13] (Splošna uredba o varstvu podatkov oziroma GDPR) zanje uporaba postopka obveščanja o koncentracijah ter preprečevanje izogibanja ne velja.

Ker spletni iskalniki niso povsem urejeni z obstoječo zakonodajo, obstaja tveganje, da tehnološka podjetja izkoristijo pravni vakuum v svojo korist. Glede na vrednost osebnih podatkov in potencialne dobičke se lahko podjetja odločijo za obid zakonodaje, saj so kazni pogosto nižje od dobička, ki ga pridobijo s takšnimi praksami. To pomeni, da je zaščita temeljnih pravic, kot je pravica do zasebnosti, pogosto prepuščena arbitrarni presoji teh podjetij. Takšna praksa poudarja potrebo po jasnejših in strožjih pravilih, ki bi omogočila učinkovitejšo zaščito uporabnikov v digitalnem okolju.

Na koncu bo verjetno Sodišče Evropske unije moralo odločati o tem, kako naj se uporabljajo določila zakonodaje glede spletnih iskalnikov in njihove vloge v digitalnem trgu. Do takrat pa spletni iskalniki ostajajo v pravnem vakuumu, ki omogoča neurejeno obdelavo podatkov uporabnikov.

2.3 Razvoj pojma digitalnega posrednika oziroma vratarja

Za namene tega članka bom, ne glede na nejasno opredelitev vratarja v kontekstu Akta o digitalnih trgih, vratarje v nadaljevanju dodatno v najširšem in vsebinsko opredeljenem smislu opredelil tudi kot akterje, ki dejansko akumulirajo in agregirajo ogromno količino informacij in podatkov, jih filtrirajo ter distribuirajo znotraj posameznega poslovnega subjekta, kamor ti vratarji spadajo.

[12] UL L 178, 17. 7. 2000, strani 1–16.
[13] UL L 119, 4. 5. 2016, strani 1–88.

Izraz vratar je prvič mogoče zaslediti leta 1947 pri psihologu *Lewinu*,[14] ki je v sklopu svojega dela raziskoval razlike med prehranjevalnimi navadami družin. Opazil je, da so v opazovanih skupinah družin bile dejansko ženske tiste, ki so odločale o vsem, kar zadeva prehranjevalne navade družine in so na takšen način dobile naziv »vratarke«. Opredelitev tega pojma *Lewin* opisuje kot tunel, ki ga mora podatek prečkati, da prispe na cilj, pri čemer pred tunelom stoji množica ostalih podatkov, ki jih vratarji selektivno razvrščajo glede na njihovo pomembnost.[15] Z razvojem digitalnih medijev je pojmovanje tega pojma, razen njegove dejanske uporabe na različnih področjih, ostalo skorajda enako, pri čemer ostaja tudi dejanska vloga vratarja enaka – nadzor nad pretokom informacij znotraj posameznega digitalnega okolja oziroma organizacije digitalnega akterja. Kot taki vratarji dejansko predstavljajo katalizator podatkov. Več avtorjev navaja,[16] da so digitalni posredniki oziroma vratarji obstajali tudi v vseh zgodovinskih obdobjih javnega komuniciranja (na primer časopisne stojnice, kabelska televizija in podobno), pri čemer je določanje njihove dejanske pravne vloge povzročalo nemalo težav. Same časopisne hiše, enako velja tudi za ponudnike kabelske in satelitske televizije, pravno niso bile odgovorne kot neposredni oblikovalci medijskih vsebin, saj niso imele možnosti na kakršenkoli način vplivati na vsebino samega časopisa ali vsebino televizijskega programa. Temu obdobju množičnega komuniciranja in oglaševanja je tudi moč pripisati prve teorije vratarjev kot človeške informacijske filtre, ki so delovali kot časopisni, radijski ali televizijski uredniki in posredniki novic. Vsebinsko gledano bi tako vratarje lahko razdelili na dve osnovni skupini, pri čemer bi prvo skupino opredelili kot vratarje, ki imajo direkten dostop do informacij, drugo skupino pa kot vratarje, ki imajo dostop do pomembnih informacijskih storitev, potrebnih, da uporabniki sploh lahko dostopajo do želene iskane vsebine na spletu.[17] Prva skupina vratarjev je po svoji vsebini podobna klasičnim digitalnim urednikom, ki odločajo o vsebinah posamezne objave, medtem ko so pa vratarji druge skupine dejansko vratarji ponudnikov internetnih storitev (enako kot včasih ponudniki kabelske televizije). Če govorimo o pretoku osebnih podatkov, je pomembno opredeliti vlogo posameznih vratarjev, ki je *per se* odvisna od vloge posameznega vratarja, ki jo ta izvaja, kot na primer platforma družbenih omrežij, platforma spletnih iskalnikov ali platforma prodaje aplikacij. Zadnji dve platformi dejansko redno sprejemata »uredniške« odločitve in sicer tako, da bodisi onemogočata določeno vsebino ali pa jo zbrišeta in odstranita,

[14] Lewin, 1943, stran 38.
[15] Barzilai-Nahon, 2008, stran 7.
[16] Koltay, 2020, stran 623.
[17] Helberger, 2015, stran 53.

da ni več vidna (na primer zaradi zaščite poslovnih interesov), s čimer spadajo takšni vratarji v prvo aktivno skupino predvsem zato, ker imajo neposreden vpliv na pretok informacij. Vratarji, ki imajo nadzor nad platformami družbenih omrežij, pri čemer imajo možnost tudi vpliva na razvrščanje vsebine, spreminjanje fokusa med različnimi deli vsebine z namenom oglaševanja, izpostavljenosti posamezne vsebine ali z ustvarjanjem personalizirane ponudbe za uporabnika, spadajo v drugo skupino. V prvem primeru gre za aktivno, v drugem primeru pa za pasivno vlogo vratarja, ki jo ima ta v komunikacijskemu procesu. Namen Evropske komisije je bil z Aktom o digitalnih trgih regulirati obe vrsti vratarjev, tako aktivne, kakor tudi pasivne, ter vsebinsko prispevati k pravilnemu funkcioniranju celotnega notranjega digitalnega trga, zaradi česar je sam akt dobil naziv »Pan-evropske« zakonodaje.[18] Žal je takšen poskus, zaradi že prej omenjenih razlogov in ob upoštevanju jasno opredeljene pravne terminologije, obsojen na neuspeh.

Splet je in bo vedno omogočal neposreden in brezpogojen dostop osebam, ki želijo preko njega uveljaviti pravico do izražanja in pravico do izbire, sami vratarji pa bodo ostali nepogrešljiv del tega komunikacijskega procesa. V tem kontekstu bodo vratarji predstavljali enako kot nekoč – digitalnega urednika, ki omogoči ali prepreči posamezno objavo na spletu ali dostop do te, vse v skladu z vnaprej določenimi algoritmi. Ta proces poteka pri različnih ponudnikih, vključno s ponudniki internetnih storitev, družbenih omrežjih, iskalnikih, tržnicah z aplikacijami, spletnih trgovinah, novičarskih portalih ter ponudnikih spletnih vsebin. Administratorji – bodisi posamezniki ali algoritmi – pri tem odločajo o objavah in vsebini, ki jih posamezniki delijo v zvezi s konkretnimi članki ali spletnimi objavami. Kot takšni do sedaj niso bili predmet regulacije, zaradi česar so sami lahko določili lastna pravila delovanja v vlogi digitalnih vratarjev, s čimer pa so zasledovali bistven cilj – proinovativnost podjetij z namenom ustvarjanja dobička. Z Aktom o digitalnih trgih bodo do določene mere omejeni, vendar bodo še vedno imeli dostop do celotnega repozitorija zbranih podatkov, ki so jih do sedaj zbrali in za katere ta uredba ne velja, ter dodatnimi osebnimi podatki, za katere ni jasno, kateri del uredbe bo za njih uporaben.[19]

[18] Portuese, 2022, stran 6.
[19] Decarolis, 2023, stran 9.

2.4 Vratarji v kontekstu Akta o digitalnih trgih

Kot izhaja iz prvega odstavka 1. člena Akta o digitalnih trgih, je njegov namen prispevati k pravilnemu delovanju notranjega trga z določitvijo harmoniziranih pravil, ki za vsa podjetja zagotavljajo tekmovalne in pravične trge v digitalnem sektorju po vsej EU, na katerih delujejo vratarji, vse v korist poslovnim in končnim uporabnikom. Na prvi pogled izstopa sestavek »… za vsa podjetja…«, če je jasno, da akt v svoji osnovi daje prednost subjektivno določenim merilom za imenovanje bodočih vratarjev, ki v okviru svojega delovanja omogočajo jedrne platformne storitve, pri čemer ta merila niso podana kvalitativno ter abstraktno, temveč kvantitativno, s čimer so vnaprej določeni posamezni vratarji na notranjem digitalnem trgu EU, ter so v celoti podani izključno skozi ekonomski vidik. Kot prvo, za vratarja v kontekstu Akta o digitalnih trgih velja, da se podjetje lahko obravnava kot vratar, kadar ponuja jedrno storitev, pri čemer velja, da mora ta jedrna storitev imeti pomemben vpliv na notranji trg. Druga predpostavka je določena z velikostjo letnega prometa in tržno kapitalizacijo podjetja. Pomemben vpliv na notranji trg je uresničen, če je imel domnevni vratar v zadnjih treh poslovnih letih vsaj 7,5 milijarde evrov letnega prometa oziroma če njegova tržna kapitalizacija presega 75 milijard evrov. Pri tem velja tudi dodatna omejitev, da mora takšen domnevni vratar ponujati svojo jedrno platformno storitev vsaj v treh državah članicah EU. V skladu z določilom 1.b odstavka 3. člena Akta o digitalnih trgih mora ponudnik jedrne platformne storitve, da bi se sploh lahko štel za vratarja, dodatno tudi služiti kot pomembna vstopna točka, preko katere poslovnih uporabniki dosežejo končne uporabnike. Takšna zahteva je v skladu z 2.b točko 3. člena Akta o digitalnih trgih izpolnjena, če ima potencialni vratar v zadnjem poslovnem letu vsaj 45 milijonov mesečno aktivnih končnih uporabnikov, ki imajo sedeže ali se nahajajo v EU, in vsaj 10.000 letno aktivnih poslovnih uporabnikov s sedežem v EU, opredeljenih in izračunanih v skladu z metodologijo in kazalniki.[20] Pri tem velja, da gre v primeru končnih uporabnikov za tiste uporabnike, ki jih ni mogoče uvrstiti med poslovne subjekte, ne glede na to, ali gre za fizične ali pravne osebe. Takšna kvantitativna merila lahko subjektivno razvrščajo podjetja z enakovredno dejavnostjo in tržno pozicijo, oboje samo glede na merila, ki jih določa Akt o digitalnih trgih.

[20] Metodologija in kazalniki opredeljujejo jedrne platformne storitve, pri čemer se za aktivne končne uporabnike štejejo tisti, ki so vsaj enkrat mesečno uporabili določeno storitev (prijava, iskanje itd.). Aktivni poslovni uporabniki pa so edinstveni poslovni subjekti, ki so imeli vsaj en izdelek registriran na spletni posredniški storitvi skozi celo leto ali so izvedli transakcijo ali interakcijo s končnim uporabnikom.

Po svoji vsebini in določitvi kvantitativnih meril Akt o digitalnih trgih sploh ne upošteva temeljna načela in pojmov konkurenčnega prava (na primer prevladujoči položaj na trgu). Na takšen način nekatera podjetja, ki imajo sedaj prevladujoči položaj na trgu, sploh ne bodo mogla biti vratarji, saj za njih glede na kvantitativna merila Akta o digitalnih trgih določbe ne bodo veljale, s čimer je Akt o digitalnih trgih dejansko paradoks konkurenčnemu pravu. Konkretno gledano, 5. točka uvodnih pojasnil Akta o digitalnih trgih navaja, da tržni procesi pogosto ne morejo zagotoviti poštenih gospodarskih rezultatov v zvezi z jedrnimi platformnimi storitvami, in čeprav se za ravnanje vratarjev uporabljata 101. in 102. člen PDEU, je področje uporabe teh določb omejeno na nekatere primere tržne moči, na primer prevladujoč položaj na specifičnih trgih in protikonkurenčno ravnanje, uveljavljata pa se naknadno, pri čemer so potrebne obsežne preiskave pogosto zelo zapletenih dejstev za vsak primer posebej. Nadalje ta navaja, da obstoječe pravo EU ne obravnava ali ne obravnava učinkovito izzivov, ki jih za učinkovito delovanje notranjega trga predstavlja ravnanje vratarjev, ki nimajo nujno prevladujočega položaja v smislu konkurenčnega prava. S takšno uveljavitvijo so do sedaj uveljavljena načela konkurenčnega prava v celoti obrnjena na glavo.[21]

Glede na določbe iz prvega odstavka 1. člena je namen Akta o digitalnih trgih v veliki meri izvotljen. Akt o digitalnih trgih namreč dejansko omogoča *ex ante* urejanje konkurence, kar pomeni alternativno izvajanje predpisov Akta o digitalnih trgih v primerjavi z obstoječim konkurenčnim pravom posamezne države članice (torej namesto *ex post* urejanja). S tem ni odpravljena primarnost konkurenčnega prava države članice, ki ureja delovanje podjetij v digitalnem okolju, povečuje pa možnosti za neenotno izvajanje Akta o digitalnih trgih na območju EU. Primeroma je na tem mestu izpostaviti, da v skladu z določili šestega odstavka 1. člena Akta o digitalnih trgih ta ne posega v uporabo 101. in 102. člena PDEU, pri čemer tudi ne posega v uporabo nacionalnih pravil o konkurenci, ki prepovedujejo protikonkurenčne sporazume, sklepe podjetniških združenj, usklajena ravnanja in zlorabe prevladujočega položaja; nacionalnih pravil o konkurenci, ki prepovedujejo druge oblike enostranskega ravnanja, kolikor se uporabljajo za podjetja, ki niso vratarji, ali pomenijo nalaganje dodatnih obveznosti vratarjem; Uredbe Sveta (ES) št. 139/2004

[21] V glasbeni industriji bo glede na pravila Akta o digitalnih trg pretočne vsebine reguliral vratar Apple Music s 15-odstotnim tržnim deležem, medtem, ko bo Spotify z 31-odstotnim tržnim deležem izvzet. Podobno velja primeroma tudi za družbena omrežja, medijsko vsebino digitalnega trga bo reguliral Facebook, medtem ko Twitter ne dosega kvantitativnih meril Akta o digitalnih trgih.

z dne 20. januarja 2004 o nadzoru koncentracij podjetij[22] (Uredba EU o združitvah) in nacionalnih pravil o nadzoru združitev.

3 Informacijska zasebnost na digitalnih trgih

3.1 Splošno o zasebnosti

Na splošno je znano, da je pravica do zasebnosti v različnih časovnih obdobjih in različnih državah različno opredeljena, generalno pa bi *latu sensu* lahko rekli, da je že po teleološki razlagi osebnostna pravica posameznika, da se ga pusti pri miru, tako pred samovoljnim delovanjem države in njenih organov, kakor tudi pred posegom drugih posameznikov v njegovo osebno okolje. V demokratični družbi se je močno uveljavilo prepričanje, da posameznik kljub voljnemu razkrivanju svoje osebnosti v odnosu do drugih ohranja željo po zasebnosti v določenih vidikih vsakdanjega življenja. To pa ne zato, ker bi želel skriti te informacije pred drugimi, temveč preprosto zato, ker ne pričakuje, da bi družba izražala interes za vpogled vanje in s tem izoblikovala smiselno celoto dogajanja posameznikovega vsakdana. Danes se je s takim stališčem moč poistovetiti, saj zasebnosti nad informacijami, ki jih voljno javno delimo, niso nujno varne pred namensko obdelavo. Dejansko posamezna informacija konkretno ne pove veliko o posamezniku, agregirani podatki oziroma zbrana količina podatkov, predvsem kadar gre za dolgoročno agregirane, pa o posamezniku povedo veliko več in dejansko dajejo vpogled v celotno njegovo življenje, odvisno sicer od tega, ali jih zbira posamezni pravni subjekt ali več njih.

Sama pravica do zasebnosti spada na področje osebnostnih pravic, je univerzalna in absolutna ter ustavno varovana pravica. Deluje *erga omnes*, naproti vsem, tako proti državi, kakor tudi proti ostalim pravnim subjektom, ter je sestavni del človekove osebnosti in integritete, predvsem pa je nepremoženjska. Vendar ima kot taka svoje omejitve, in je zatorej relativna. Konkretno je to pravico mogoče omejiti le v primerih, ko gre za vprašanja nacionalne ali javne varnosti, blaginje prebivalstva ali javne morale. Pri tem je pomembno, da je pravica omejena le v skladu z enakimi pravicami drugih, na podlagi načela sorazmernosti. To pomeni, da je treba oceniti, ali je poseg v določene pravice in svoboščine upravičen ter ali je poseg primeren glede na zastavljeni cilj ali uporabljeno sredstvo.

[22] UL L 24, 29. 1. 2004, strani 1–22.

K temu pravnemu pojmu sta pomembno prispevala avtorja, ki sta v svoji študiji[23] pojem zasebnosti definirala kot pravico posameznika, da se ga pusti pri miru. Ne glede na to, da moderni pravni sistemi varujejo temeljno pravico do zasebnosti in glede na to, da je zasebnost dejansko odvisna od družbenega okolja in obdobja, v katerem živimo, med pravniki ne obstaja konsenz in jasna definicija, kaj je zasebnost, kaj točno se s to pravico varuje in kaj dejansko predstavlja zasebnost kot pravni pojem. Sama pravica do zasebnosti je vsebinsko abstraktna, pri čemer jo na splošno lahko delimo na več kategorij: (a) informacijska zasebnost, ki zajema tako zbiranje in upravljanje z osebnimi podatki, kakor tudi varstvo osebnih podatkov; (b) telesna zasebnost, ki pokriva področje, povezano z genetskimi ali drugimi preiskavami; (c) komunikacijsko zasebnost, ki zagotavlja zasebnost pošte, telefonskih pogovorov, prometnih podatkov ter drugih oblik sporazumevanja; (d) zasebnost v prostoru, ki omejuje poseg v zasebnost na delovnem mestu ali doma. Ker gre za izjemno kompleksen pojem, je zasebnost težko omejiti na samostojno bistvo, ki bi zasebnost *per se* jasno definiral. Pri zasebnosti gre za pluralnost različnih dejavnosti, ki nimajo skupne točke, vendar so si po naravi stvari podobni.[24] V tem kontekstu je mogoče reči, da je takšno pluralistično teorijo zasebnosti mogoče povezati tudi z mozaično teorijo zasebnosti,[25] ki samo zasebnost opredeljuje kot niz informacij, ki kot takšne niso pomembne, vendar so na agregatni ravni in v kombinaciji z drugimi informacijami neprecenljive, saj povedo skorajda vse o posamezniku. Ker so tako zbrani podatki dejansko agregirane informacije, ki o posamezniku povedo veliko več kot le posamezna informacija ali podatek, bi posledično morali uživati veliko večjo stopnjo pravne zaščite, vendar pa je v današnjem času bliskovitega napredka tehnološkega in informacijskega razvoja pravico do zasebnosti težko ustrezno varovati, saj nad njo največkrat prevladajo drugi »javni« interesi.[26] Tudi že novodobna izpeljava znamenitega Ciceronega načela »*Salus populi suprema lex esto*«[27] izkazuje moč države, da v določenih primerih odstopi od zaščite človekovih pravic ter jih prvenstveno derogira zaradi na primer zagotavljanja lastnega obstoja ali varnosti družbene skupnosti.[28]

[23] Warren, 1890, stran 197. [dostopno na https://faculty.uml.edu/sgallagher/Brandeisprivacy.htm] (obiskano 30. 1. 2024).
[24] Solove, 2020, stran 24.
[25] Iz obrazložitve sodbe *United States v. Marchetti*, 466 F.2d 1309, 1318 (4th Cir. 1972) povzeto izhaja, da različni podatki sami po sebi nimajo vsebinske vrednosti, agregirani skupaj v neko celoto pa pridobijo na svoji pomembnosti. Mozaična teorija poudarja relevantnost enega podatka v soodvisnosti od drugih zbranih podatkov.
[26] Glej na primer tretji odstavek 15. člena v povezavi z 2. členom Ustave RS.
[27] Blaginja ljudstva naj bo višji zakon.
[28] Konkretno na primer pandemija Covid-19.

Solove je v svoji pluralistični teoriji zasebnosti izpostavil šest kategorij zasebnosti, med katere sodijo pravice biti puščen na miru, samoomejevanje, tajnost, nadzor nad osebnimi podatki, identiteta in intimnost. Vendar so tudi te kategorije preveč ozke, saj so tradicionalne metode konceptualiziranja pojmov v času napredka informacijske tehnologije preveč osredotočajo na nujnost in zadostnost pojma in so zatorej preveč abstraktne za jasno definicijo pravne zaščite te pravice, ki je odvisna od časa in družbenega okolja, v katerem živimo. Na tem mestu je v povezavi z razvitimi teorijami zasebnosti pomembno izpostaviti še teorijo o kontekstualni integriteti toka osebnih podatkov, ki izhaja iz predpostavke, da so naši osebni podatki vedno povezani z določenim družbenim kontekstom.[29]

Vendar, tako kot za ostale ustavno varovane pravice, tudi za pravico do zasebnosti obstajajo izjeme,[30] pri čemer je bistvo vseh izjem, da tisto, kar posameznik voljno in vestno izpostavi javnosti, ne more uživati pravnega varstva in statusa zasebnosti. Tudi kopičenje posameznih podatkov po mozaični teoriji zasebnosti povzroči dejansko vzpostavitev vzorca posameznika in s tem posredno vdor v njegovo zasebno sfero. Pri tem je potrebno omeniti, da četudi je podana voljna sestavina razkriti določeno informacijo posameznika, slednje ne pomeni, da ja konkludentno podana tudi zavestna volja ali soglasje k zbiranju ostalih podatkov tega posameznika. Prostovoljnost v konkretnem primeru dejansko pomeni tako zavestno, kakor voljno komponento izpostaviti določen del ali določen sklop podatkov javnosti. Namreč, vsakič ko posameznik javnosti predoči svoj del zasebnosti, pokaže tudi del svoje osebnosti, tako fizične kakor psihične posameznikove integritete, ki je pri pravici do varstva zasebnosti pomembna. Z zbiranjem vseh ostalih nepovezanih podatkov bi lahko dejansko sestavili profil posameznika, vendar pa velja, da se preostalim podatkom z enkratno izpostavitvijo posameznik ni odpovedal, za njih še vedno velja, da posameznik upravičeno pričakuje njihovo zasebnost. Tudi informacija, ki je javno dostopna in znana javnosti, in jo državne organizacije sistematično hranijo, spada pod varstvo iz 8. člena Evropske konvencije o varstvu človekovih pravic[31] (EKČP). Ta namreč varuje tudi posameznikovo interakcijo z družbo in izgradnjo njegove osebne integritete v stiku s socialnim okoljem brez vmešavanja tretjega v njegove odnose z drugimi.[32]

---

[29] Nissenbaum, 2004, stran 133.
[30] Na primer doktrina tretje stranke, doktrina prosto vidnih dokazov ter doktrina razkritja javnosti.
[31] Evropsko sodišče za človekove pravice, Rim, 4. 11. 1950.
[32] Glej 32. točko sodbe ESČP *Botta v. Italy*, št. 21439/93 z dne 24. 2. 1998. Podobno tudi *Niemietz v. Germany*, št. 13710/88, A251-B, z dne 16. 12. 1992.

3.2 Pravna ureditev zasebnosti in varstva osebnih podatkov 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,[33] Konvencija o zaščiti posameznikov v razmerju do samodejne obdelave podatkov iz leta 1981[34] in Smernice UN glede ureditve računalniških zbirk osebnih podatkov iz leta 1990.[35] Takšna ureditev izhaja iz zgodovinskega konteksta nastanka mednarodnega sodelovanja EU.[36] V tem kontekstu sta bila odločilna dva dejavnika: bliskovit tehnološki razvoj in mednarodni izzivi, ki jih ta prinaša, in 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.[37]

Osebne podatke kot take je mogoče glede na njihov izvor razvrstiti med prostovoljno dane, opazovane, izpeljane in algoritemsko ugotovljene, pri čemer 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 preko vratarja. Te podatke je mogoče ločiti na sprožene (na primer registracija na spletnem mestu), transakcijske (na primer nakup izdelka s kreditno kartico) in objavljene (na primer objava na družbenih omrežjih). Opazovane osebne podatke zbirajo podjetja, ki se ukvarjajo z zbiranjem podatkov. Te podatke ločimo na angažirane (na primer 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

[33] Glej https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (obiskano 30. 1. 2024).
[34] Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, ETS no. 108, 1981.
[35] Tene, 2010, strani 1–8.
[36] Kelleher, 2006, stran 14.
[37] De Hert, 2012, strani 130–142.

podlagi deterministčnih izračunov in kot taki postanejo novi delci osebnih podatkov, ki so neposredno povezani z uporabnikom. Izpeljane podatke lahko ločimo na računske (na primer aritmetični izračun povprečni čas obiska spletne strani) in notacijske (na primer 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 statistčnih metod (na primer posojilne ocene) in analitičnih procesov (na primer 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. Za te podatke tudi ne veljajo določila Akta o digitalnih trgih

Samo varstvo osebnih podatkov je 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.[38] Takšno stališče je omogočilo, da je varstvo osebnih podatkov prevladalo nad drugačnimi interesi in tej pravici dalo pravno varstvo, s katero ni mogoče ekonomsko trgovati.[39] Varstvo osebnih podatkov je pridobilo ključno vlogo s sprejetjem Lizbonske pogodbe.[40] Določba 39. člena Pogodbe o Evropski uniji[41] (PEU) in 16. člen PDEU vsebujeta posebne določbe v zvezi z varstvo osebnih podatkov, pri čemer 16. člen PDEU 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[42] (LEUTP) in zagotovila posebne določbe v zvezi s pravnim pomenom EKČP, ki v 8. členu opredeljuje varstvo osebnih podatkov in varstvo zasebnosti.

V veljavi sta še dva pravna predpisa, ki imata ključno vlogo pri varstvu osebnih podatkov. Prvi je GDPR, drugi 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[43] (Direktiva 2002/58).

[38] Borghi, 2013, strani 109–153.
[39] Prav tam, 2013, stran 142.
[40] UL C 306, 17. 12. 2007, strani 1–271.
[41] UL C 326, 26. 10. 2012, strani 1–412.
[42] UL C 83, 30. 3. 2010, strani 1–408.
[43] UL L 201, 12. 7. 2002, strani 37–*47*.

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 take določene v GDPR. Glede na navedeno, so nekatere določbe Akta o digitalnih trgih v celoti neuporabljive.

4 Pravni vidiki in izzivi vratarjev v kontekstu akta o digitalnih trgih

4.1 Parcialnost akta o digitalnih trgih

Kot je bilo že navedeno, 2. maja 2023 pričel veljati Akt o digitalnih trgih, ki ga je Evropska komisija sprejela 1. novembra 2022. Vmesno šestmesečno obdobje je veljalo za obdobje implementacije. Namen Akta je odprava nepoštenih poslovnih praks monopolnih podjetij, ki zagotavljajo jedrne platformne storitve, obenem pa je njegov vsebinski namen zagotovitev enakih konkurenčnih pogojev za vsa podjetja, ki primarno delujejo na digitalnem trgu. Pravna podlaga Akta o digitalnih trgih izhaja iz prvega odstavka 114. člena PDEU glede približevanja določb zakonov in drugih predpisov v državah članicah, katerih predmet je vzpostavitev in delovanje skupnega notranjega trga. Ta pozitivnopravna obveznost ukrepov izhaja iz 26. člena PDEU, ki EU nalaga obveznost sprejemov različnih harmoniziranih aktov za vzpostavitev, delovanje in zagotavljanje delovanja notranjega trga. Pri tem velja, da notranji trg zajema območje brez notranjih meja, na katerem je na podlagi PEU in PDEU zagotovljen prost pretok blaga, oseb, storitev in kapitala.

Vsebinski cilj Akta o digitalnih trgih je zagotoviti konkurenčne pogoje in prispevati k pravilnem delovanju notranjega trga z določitvijo harmoniziranih pravil, ki vsem podjetjem zagotavljajo enako – tekmovalne in pravične trge po vsej EU, torej za vse digitalne storitve, kjer so prisotni vratarji, v korist poslovnim in končnim uporabnikom. Konkretno gre torej za del zakonodaje, ki ureja poslovno delovanje vratarjev oziroma ponudnikov storitev osrednjih digitalnih platform, ki jih gospodarske družbe potrebujejo za posredni dostop do svojih strank oziroma uporabnikov. In čeprav bi Akt o digitalnih trgih lahko označili kot skladnega s konkurenčno politiko, bi ga glede na njegovo primarno naravo opisali kot sektorski specifični pravni predpis z asimetrično uporabnostjo, ki postavlja obveznosti različnim podjetjem različno, predvsem glede njihovega tržnega položaja, tržne

pozicije oziroma ostalih relevantnih dejavnikov.[44] Slednja asimetrična regulacija že sedaj velikih tehnoloških velikanov bi lahko izvotlila pomen primarnega vodila PDEU iz uvodne točke 5, ki govori o sprejemu PDEU v spoznanju, da je za odstranjevanje sedanjih ovir nujno usklajeno delovanje, ki bo zagotovilo stalen napredek, uravnoteženo trgovino in pošteno konkurenco. Enako velja tudi za 32.b člen PDEU, ki Evropski komisiji nalaga izvajanje nalog pri razvoju pogojev konkurence na enotnem trgu znotraj EU v smislu izboljšanja konkurenčne sposobnosti podjetij. Vsled navedenega velja tudi določilo 101. člena PDEU (ob smiselni uporabi 102. člena PDEU ter ne glede na njegov 106. člen) v poglavju o konkurenci, ki jasno izpostavlja, da so nezdružljivi z notranjim trgom vsi tisti sporazumi in ravnanja, katerih cilj oziroma učinek je preprečevanje, omejevanje ali izkrivljanje konkurence na notranjem trgu, med drugim zaradi uvajanja neenakih pogojev za primerljive posle z drugimi trgovinskimi partnerji, ki jih postavljajo v podrejen konkurenčen položaj.

Akt o digitalnih trgih je po svoji naravi uredba EU, zaradi česar zanj velja uporaba načela primarnosti, vendar se zaradi nekaterih njegovih določil pojavljajo pravne negotovosti ter nedoslednosti v povezavi s primarnim pravom EU. Iz petega odstavka 1. člena Akta o digitalnih trgih izhaja, da države članice, predvsem v smislu ohranitve enotnega digitalnega trga, ne smejo vratarjem nalagati nadaljnjih obveznosti na podlagi zakonov, uredb ali upravnih ukrepov, katerih namen je zagotoviti tekmovalne in pravične trge. Pri tem velja, da državam članicam nič ne preprečuje, da bi v zvezi z zadevami, ki ne spadajo na področje uporabe tega akta podjetjem, vključno s podjetji, ki zagotavljajo jedrne platformne storitve, naložile obveznosti, pod pogojem, da so te obveznosti združljive s pravom EU in ne izhajajo iz tega, da imajo zadevna podjetja status vratarja v smislu Akta o digitalnih trgih.[45] Po drugi strani pa je v šestem odstavku istega člena navedeno, da ta ne posega v uporabo 101. in 102. člena PDEU, kakor tudi ne v uporabo nacionalnih pravil o konkurenci, ki prepovedujejo protikonkurenčne sporazume, usklajena ravnanja in zlorabe prevladujočega položaja. Na tem mestu je izpostaviti, da so nekatere države članice EU sprejele nacionalne pravne akte, ki naslavljajo podobna ravnanja enakovrednih podjetij, kot jih naslavlja Akt o digitalnih trgih.

[44] Montero, 2020, strani 186–187.
[45] Glej peti odstavek 1. člena Akta o digitalnih trgih.

Nekateri menijo, da gre za postavitev novih pravil uporabe interneta, katerih cilj je povečati varnost za uporabnike, zagotoviti pošteno poslovno okolje za podjetja in izboljšati pravno predvidljivost. To naj bi dosegli z določanjem večje odgovornosti za posredniške platforme..[46] Cilj Akta o digitalnih trgih je sicer bil nasloviti strukturne težave, ki so se pojavljali na digitalnih trgih in jih ni bilo mogoče ustrezno obravnavati z obstoječimi pravili varstva konkurence. Ključne težave bodo, ne glede na posodobljena pravila na digitalnih trgih, vključevale še vedno nepoštene prakse v odnosu do manjših poslovnih uporabnikov, pomanjkanje konkurence ter visoko monopolno koncentracijo na trgih, kjer delujejo velike digitalne platforme, skupaj z razdrobljenostjo regulativnega okvira znotraj EU. Harmonizirana pravila regulacije digitalnih trgov na ravni EU naj bi z vsebinskimi določili omogočala inovativnost, rast ter konkurenčnost, ni pa v nobenem primeru jasno, kako bo s svojo implementacijo Akt o digitalnih trgih pripomogel k rasti manjših platform, da bi s tem omogočil njegovo osnovno vodilo konkurenčnosti. Akt se uporablja le za velika podjetja, ki so opredeljena kot »vratarji« v skladu z objektivnimi merili. To pa so tehnološki giganti oziroma podjetja, ki imajo zaradi svoje velikosti in vpliva posebno pomembno vlogo na notranjem trgu že sedaj. Ta podjetja že sedaj nadzorujejo vsaj eno ključno platformno storitev, kot so iskalniki, družbena omrežja, nekatere storitve sporočil, operacijski sistemi, spletne tržnice itd., ter imajo trajno in obsežno bazo uporabnikov v več državah EU. Sprejem Akta o digitalnih trgih *per se* ustvarja domnevo, da so izpostavljene strukturne težave, zaradi česar je ta predpis primarno bil sprejet, škodljive, in bodo takšnim škodljivim posledicam manjši upravljavci digitalnih platform še vedno direktno izpostavljeni, saj za njih (vsaj v tej fazi) ne veljajo pravila Akta o digitalnih trgih.

4.2 Varstvo informacijske zasebnosti

Kot je bilo že zgoraj navedeno, je zasebnost eno bolj kompleksnih načel in temeljnih človekovih pravic, ki izhaja iz varovanja človekovega dostojanstva in njegove avtonomije, povezane z varovanjem osebnega prostora in pogosto operacionalizirana kot pravica do varstva osebnih podatkov. Kot takšno si pravico do zasebnosti lahko predstavljamo kot mejnik med javnim in zasebnim. V kontekstu Akta o digitalnih trgih je varovanje informacijske zasebnosti, predvsem ker gre za digitalno okolje, eden bolj kompleksnih izzivov, predvsem v kolikor zasebnost

[46] Obvestilo Službe Vlade RS za digitalno preobrazbo z 15. julija 2022. [Dosegljivo na https://www.gov.si/novice/2022-07-15-evropski-parlament-potrdil-nova-pravila-za-digitalne-platforme/] (obiskano 30. 1. 2024).

razlagamo skupaj z načelom konkurenčnosti, načelom svobodne gospodarske pobude ter v okviru digitalne ekonomije. Iz ekonomskega vidika je zasebnost mogoče izpeljati iz posameznikove preference glede informacijske zasebnosti (zasebnost kot okarakterizirana vrednota posameznika) oziroma drugih prednosti, ki jih ima ohranjanje zasebnih informacij v zasebni sferi posameznika (oportunitetna zasebnost). Posamezniki se pogosto odločijo razkriti svoje zasebne informacije v zameno za uporabo »brezplačnih« storitev digitalnih platform. Pri tem je pomembno razumeti, da tako razkritje kot nerazkritje zasebnih podatkov prinašata določene prednosti in stroške. Posamezniki, ki razkrijejo svoje podatke, pridobijo dostop do storitev, vendar hkrati tvegajo izgubo zasebnosti. Na drugi strani pa poslovni subjekti, ki te podatke zbirajo in hranijo, pridobijo dragocene informacije, vendar prevzamejo tudi odgovornost za varstvo teh podatkov.[47] S prostovoljnim razkritjem zasebnih podatkov, na primer preko piškotkov, ki hranijo vedenje in obnašanje posameznika na spletu, tehnoloških velikanom omogoča ogromno informacij tako o preferencah, kakor tudi glede vzorca obnašanja uporabnikov. Slednje je povezano tudi z vedenjskim oglaševanjem. V okviru konkurenčnega prava je potrebno varstvo informacijske zasebnosti obravnavati tudi izven sfere EU. Medtem ko je na primer v ZDA zbiranje, trgovanje in uporaba osebnih podatkov na splošno dovoljeno, je na področju EU dokaj restriktivno, s čimer imajo poslovni subjekti iz EU bistveno nižjo mednarodno konkurenčnost.

V okviru Akta o digitalnih trgih obstajajo posamezne določbe, ki same po sebi predstavljajo tveganje v okviru ohranjanja pravice do zasebnosti ter pravice do varstva osebnih podatkov, pri čemer nespoštovanje teh določb ne spremljajo nobeni izrecni ukrepi ali pa so varovala, ki varujejo pravico do zasebnosti, nezadostna. V tem kontekstu je potrebno Akt o digitalnih trgih razlagati iz vidika 7. in 8. člena LEUTP, ki utemeljujeta pravico do zasebnosti in pravico do varstva osebnih podatkov. V 5. členu Akta o digitalnih trgih so na primer navedene številne obveznosti vratarjev, pri čemer je določeno, kot to izhaja iz določbe 2.b točke 5. člena, da se podatki iz jedrne platformne storitve ne smejo združevati s podatki iz katerihkoli drugih storitev, iz 2.c. točke 5. člena, ki preprečuje navzkrižno uporabljanje podatkov, ter iz 2.d točke 5. člena, ki prepoveduje vpisovanje končnih uporabnikov v druge storitve vratarja z namenom združevanja osebnih podatkov. Tako 2.c točka 5. člena prepoveduje tudi navedeno navzkrižno uporabo podatkov, pri čemer so »podatki« v tem primeru osebni podatki v smislu GDPR. Vendar pa

[47] Acquisti et al., 2016, strani 444–492.

tudi razlaga posameznih določb Akta o digitalnih trgih z vidika LEUTP mogoče ne bo zadostna, temveč bo potrebno posamezne določbe interpretirati tudi z vidika ostalih primarnih pravnih virov EU. Glede na prvi odstavek 52. člena LEUTP velja, da mora biti kakršno koli omejevanje uresničevanja pravic in svoboščin, ki jih priznava LEUTP, predpisano z zakonom in spoštovati bistveno vsebino teh pravic in svoboščin. Ob upoštevanju načela sorazmernosti so omejitve dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava EU, ali če so potrebne zaradi zaščite pravic in svoboščin drugih. Glede na navedeno je določila Akta o digitalnih trgih, ki se nanašajo na temeljne človekove pravice, potrebno v primeru dvoma o ustreznosti sekundarne zakonodaje (kamor ta predpis sodi) razlagati vedno v luči LEUTP.

Za primerjavo lahko vzamemo enostavni primer interoperabilnosti posameznih storitev, na katere se določila Akta o digitalnih trgih nanašajo. Na najosnovnejši ravni, to je v kontekstu digitalnih storitev jedrnih platformnih storitev, se zahteva po interoperabilnosti nanaša na uvedbo možnosti izmenjave informacij med posameznimi računalniškimi sistemi. Najbolj enostavni primer je na primer e-pošta, ki je del interoperabilnega standarda, ki ga večina uporabnikov danes uporablja. Sama e-pošta (oziroma njen SMTP protokol)[48] je bil razvit na izjemno enostaven način in je kot takšen omogočil enako varen zasebnosti kot sporočilo na razglednici. V skladu z zahtevo interoperabilnosti posamezne storitve bo torej ne glede na to, da se uporabnik ne strinja z izmenjavo njegovih osebnih podatkov s storitvami tretjih oseb v skladu z določbami GDPR, na podlagi Akta o digitalnih trgih vratar te podatke posredoval tretjim osebam v popolnoma nezasebni obliki, kot je na primer alternativna oblika SMTP protokola. Da bi zagotovili informacijsko zasebnost, je potrebno izmenjavo osebnih podatkov, kakor tudi občutljivih osebnih podatkov, izvajati le preko dvosmernih vmesnikov in še to v realnem času, v smislu API

[48] S temi protokoli prenašamo elektronsko pošto med različnimi sistemi, povezanimi s TCP/IP. To so samo protokoli, ki so namenjeni za prenose elektronske pošte, medtem ko potrebujemo za sestavo pošte druge programe, ki jim pravimo uporabniški agenti (user agents). SMTP struktura je osnovana na sledečem modelu povezave kot rezultat zahteve uporabnika pošte. SMTP vzpostavi obojestranski prenosni kanal sprejemniku. Sprejemnik je lahko končni ali vmesni. Odgovori SMTP-ja so poslani od sprejemnika pošiljatelja v odgovor na ukaze, ko je prenosni kanal vzpostavljen, pošiljatelj pošlje poštne ukaze, ki označujejo pošiljatelja pošte. Če ima sprejemnik prost kanal, sprejme in odgovori z OK. SMTP pošiljatelj pošlje RCPT ukaz, ki identificira prejemnika pošte. Če prejemnik SMTP-ja lahko sprejme pošto za tega prejemnika, odgovori z OK, če ne, ti odgovori oziroma zavme tega prejemnika (toda ne celotne pošiljke transakcije prenosa). SMTP pošiljatelj in SMTP prejemnik se pogajata. Ko se dogovorita, pošiljatelj SMTP-ja pošlje sporočilo, ki je določen s specialnimi sekvencami. Če je sprejemnik SMTP-ja uspešno prejel sporočilo, zopet odgovori z OK.

protokolov.[49] Vendar anonimizacije Akt o digitalnih trgih ne predpisuje. Tudi sama obveznost razkritja informacij iz Akta o digitalnih trgih je v nasprotju z določili GDPR. Obveznost razkritja podatkov se namreč v okviru Akta o digitalnih trgih nanaša le na podatke, ki so neposredno povezani z uporabo, ki jih izvaja uporabnik sam v zvezi z izdelki ali storitvami, ki jih ponuja poslovni subjekt. Takšna opredelitev omejitve obsega podatkov, ki jih določa Akt o digitalnih trgih, je v nasprotju z 20. členom GDPR, ki ureja prenosljivost osebnih podatkov. Ta določa, da ima posameznik, na katerega se nanašajo osebni podatki, pravico, da prejme osebne podatke v zvezi z njim, ki jih je posedoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral, kadar: (a) obdelava temelji na privolitvi v skladu s točko a) prvega odstavka 6. člena ali točko a) drugega odstavka 9. člena ali na pogodbi v skladu s točko b) prvega odstavka 6. člena se obdelava izvaja z avtomatiziranimi sredstvi. Pri uresničevanju pravice do prenosljivosti podatkov v skladu s prvim odstavkom 20. člena ima posameznik, na katerega se nanašajo osebni podatki, pravico, da se osebni podatki neposredno prenesejo od enega upravljavca k drugemu, kadar je to tehnično izvedljivo. Tako je dejansko vratar prepuščen lastni izbiri. V obeh primerih tvega neskladnost vsaj z enim pravnim predpisom, bodisi z GDPR bodisi s 6. členom Akta o digitalnih trgih, pri čemer v obeh primerih omejuje pravico do varstva osebnih podatkov ter obenem s kakršnim koli ravnanjem pravico do varovanja zasebnosti.

Uvedba Akta o digitalnih trgih pomembno vpliva na različne jedrne platforme, vratarje in storitve aplikacij v okviru digitalnih platform v okviru istega podjetja na digitalni trg. Ker se tehnologija še naprej hitro razvija, velja poudariti, da morajo tehnološki konglomerati slediti zakonodajnim spremembam in se nanje strateško odzivati. To nas opominja, da se med inovacijami in predpisi nenehno ohranja nasprotje, ki bo zagotovo zaznamovalo digitalno prihodnost, pri čemer v ozadje vedno bolj tone pravica do zasebnosti posameznika.

[49] API določa programsko komponento v smislu njenih operacij, izhodnih in vhodnih podatkov in z njimi povezanih tipov podatkov. API na ta način definira funkcionalnost programskih komponent na način, ki je neodvisen od dejanske implementacije. To omogoča različne implementacije komponente, ne da bi bil pri tem ogrožen predpisan vmesnik za uporabo komponente. API poenostavi razvoj programov s tem, da definira sestavne bloke, ki jih program sestavi pri izdelavi aplikacij.

4.3 Varstvo osebnih podatkov in soglasje uporabnika

Kot izhaja iz zgoraj navedenega, je edino pravno imperativ varstva pravic uporabnikov mogoče doseči le z njihovim soglasjem. 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.[50]

Soglasje uporabnika obravnava zakonodaja EU 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 EU soglasju določa zahteve in omejitve, namenjene preprečevanju zlorab in izkoriščanju ranljivosti uporabnikov, na katere se osebni podatki nanašajo. Čeprav 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 biti soglasje dano prostovoljno 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. Predlog Uredbe o e-zasebnosti prav tako zahteva soglasje uporabnikov za uporabo piškotkov. Vendar ta določba učinkovito ne omejuje zbiranja in izkoriščanja osebnih podatkov, saj so uporabniki pogosto nevedni o

[50] Dimović, 2023, stran 212.

načinih zbiranja podatkov in ne razumejo, kaj zapletene zahteve v resnici pomenijo. To je predvsem posledica pomanjkanja pravnega znanja, časa in potrebe po nemotenem dostopu do spleta, zaradi česar ne morejo celovito oceniti posledic svojega soglasja. 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 z osnovne platforme na druge sekundarne platforme, še vedno obstajajo vrzeli. Podjetja lahko najdejo načine za obdelavo podatkov na osnovni platformi ali za uporabo informacij na načine, ki niso izrecno prepovedani. Poleg tega ostaja vprašanje, kako učinkovito bodo te omejitve izvajane in nadzorovane v praksi, saj je uspešno varstvo zasebnosti odvisno od zavedanja uporabnikov, transparentnosti podjetij in doslednega izvrševanja zakonodaje s strani pristojnih organov.[51]

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 po tem, 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 (glej 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

[51] Dimović, 2023, stran 204.

model zahteva soglasje, kar uporabnika prisili v privolitev, s tem pa tudi k širjenju njegovih 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.

Soglasje oziroma privolitev uporabnika je opredeljena v 11. točki 4. člena GDPR, pri čemer je to pojmovano kot vsaka prostovoljna, izrecna, informirana in nedvoumna izjava 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.[52]

Zahteva po informiranosti je specifična zahteva, saj zadeva količino in vrsto ustrezno podanih informacij, ki morajo biti na razpolago posamezniku. Kot je navedeno v uvodni 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 navedeno, 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

[52] Prav tam, stran 206.

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.[53] Takšna ideja je podana v uvodni točki 20 Predloga Uredbe Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstva osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES,[54] 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 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

[53] Lavrijssen, 2022, strani 1–24.
[54] COM/2017/010 final – 2017/03(COD), 10. 1. 2017.

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 GDPR, 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[55] 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*,[56] 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[57] (Direktiva 95/46) 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.

[55] UL L 95, 21. 4. 1993, strani 29–34.
[56] Prav tam, točki 57 in 58.
[57] UL L 281, 23. 11. 1995, strani 31–50.

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 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.

4.4 Paradoks zasebnosti

Akt o digitalnih trgih v drugem odstavku 5. člena navaja, da vratar ne sme: (a) obdelovati osebnih podatkov končnih uporabnikov tretje strani, ki uporabljajo jedrne platformne storitve vratarja, za namen zagotavljanja storitev spletnega oglaševanja; (b) združevati osebnih podatkov iz zadevnih jedrnih platformnih storitev z osebnimi podatki iz drugih jedrnih platformnih storitev ali katerih koli drugih storitev, ki jih zagotavlja vratar, ali z osebnimi podatki iz storitev tretjih strani; (c) uporabljati osebnih podatkov iz zadevne jedrne platformne storitve navzkrižno pri drugih storitvah, ki jih vratar zagotavlja ločeno, vključno z drugimi jedrnimi platformnimi storitvami, in obratno; (d) vpisovati končnih uporabnikov v druge storitve vratarja, da bi združil osebne podatke. Pri tem je v nadaljevanju drugega odstavka 5. člena podano izključitveno pravilo glede prej navedenih prepovedi in sicer, da te prepovedi ne pridejo v poštev, ko končni uporabnik poda izrecno izbiro

in privolitev iz 11. točke 4. člena[58] ter 7. člena GDPR, pri čemer slednji opredeljuje pogoje za soglasje.

Primarno je na tem mestu izpostaviti povezanost tega člena z uvodno točko 36 Akta o digitalnih trgih, kjer je navedeno, da vratarji lahko neposredno zbirajo osebne podatke za namene zagotavljanja storitev spletnega oglaševanja, in sicer zbirajo osebne podatke končnih uporabnikov, ki uporabljajo spletišča in programske aplikacije tretjih strani. Zbiranje teh osebnih podatkov je pogojeno z uporabo določenih storitev, ki jih vratarji zagotavljajo v okviru svojih jedrnih platformnih storitev in na takšen način dejansko uporabnika prisilijo k soglasju k zbiranju osebnih podatkov, če želi dostopati do storitev, ki jih vratar zagotavlja v okviru svojega namena. Dejansko takšna »prisila« ne predstavlja svobodne izbire uporabnika k zbiranju osebnih podatkov, temveč je uporabniku podana izbira vzemi ali pusti, kar pa dejansko ni prosta izbira. Čeprav naj bi takšna opredelitev predstavljala vprašanje pravne varnosti zasebnosti, je v podobnem primeru nemški organ za varstvo konkurence (Bundeskartellamt) v okviru zakonskih določil nemškega zakona o prepovedi omejevanja konkurence (Gesetz gegen Wettbewerbsbeschränkungen;[59] GWB) v primeru *Facebook ZDA* in *Facebook Nemčija*[60] odločil, da Facebook ne sme več združevati podatke med Facebook-om ter pridruženimi storitvami Facebook-a, kot so Instagram ter WhatsApp, obenem pa tudi ne iz podatkov storitev tretjih oseb, ki jih Facebook zbira preko pridružene storitve FB Business Tools. Iz navedene odločitve je ugotoviti, da naj bi zaradi zlorabe prevladujočega položaja Facebooka po določbi GWB in 102. členu PDEU prišlo do kršitev predpisov o varstvu osebnih podatkov, kot jih naslavlja uvodna točka 47 GDPR. Iz tega sledi, da ima sprejet Akt o digitalnih trgih dokaj velike pomanjkljivosti, ki same odpirajo pojmovanje paradoksa zasebnosti.

Pravilo iz drugega odstavka 5.a člena Akta o digitalnih trgih je namreč vsebinsko toliko nejasno, da bi se ga opredelilo kot *ex ante* pravilo *per se*. Da bi bilo takšno pravilo samoizvršljivo, mora biti namreč jasno, točno in določno, da je zagotovljeno pravno varstvo tako porabnikov kot vratarjev v primeru kršitev.[61] Sicer so same besede osebni podatki, združevanje osebnih podatkov in obdelava osebnih

[58] »Privolitev posameznika, na katerega se nanašajo osebni podatki, pomeni 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.«
[59] Gesetz BGBI, I S. 1750, 3245 in BGBI. 2023 I Nr. 405, 22. 12. 2023.
[60] Bundeskartellamt odločba št. B6-22/16 z dne 6. februar 2019.
[61] Glej 7. člen Akta o digitalnih trgih.

podatkov dokaj jasni pojmi, sploh v povezavi z določili GDPR, vendar pa sam pojem izrecne izbire nima jasne pravne opredelitve. V skladu z 36. točko uvodnih pojasnil Akta o digitalnih trgih morajo vratarji, da ne bi nepravično vplivali na konkurenčnost jedrnih platformnih storitev, uporabnikom omogočiti manj personalizirano, vendar enakovredno alternativo. S tem bi končnim uporabnikom zagotovili možnost svobodne izbire, torej izbiro, ali se želijo vključiti v prakse obdelave podatkov ali ne. Dejansko bi to pomenilo, da bi uporabniki imeli na razpolago dve možnosti, pri čemer sploh ni jasno opredeljen pojem manj personalizirane možnosti in kaj se za vsebino te možnosti dejansko skriva. Ta točka v nadaljevanju navaja »… ne da bi uporabo jedrne platformne storitve ali nekaterih njenih funkcionalnosti pogojevali s privolitvijo končnega uporabnika ...«, kar bi pomenilo, da je za alternativno možnost onemogočena kakršno koli združevanje podatkov jedrnih platform. Na takšen način, ne glede na uvodno točko 37, tudi ni jasno, ali mora biti alternativna možnost enakovredna primarni ter kakšne možnosti sploh ima uporabnik, če se tudi za takšno nejasno možnost ne odloči in je ne izbere. Če pa bi jo izbral, pa bi po sedanji vsebini Akta o digitalnih trgih to lahko tudi pomenilo bistveno okrnjene funkcije storitev ali celo plačilo določenih pristojbin uporabe določenih storitev jedrnih platform, saj prav uvodna točka 37 Akta o digitalnih trgih navaja » … razen če je poslabšanje kakovosti neposredna posledica tega, da vratar ne more obdelati takih osebnih podatkov ali končnih uporabnikov ne more vpisati v storitev…«. Slednje pa je v nasprotju s pravičnostjo, ki naj bi jo akt zasledoval, sam uporabnik pa ne bo izbiral med ponujenimi možnostmi in iskal razlike med obema, temveč bo, v skladu s psihološko naravo posameznika, izbral najlažjo, s čimer pa tudi preidemo v polje paradoksa zasebnosti.

Izpostaviti je, da Akt o digitalnih trgih vratarjem po eni strani nalaga obveznost zagotavljanja pravočasnega in brezplačnega dostopa do enormnih količin podatkov, ki obsega tako agregirane kakor posamične podatke, kot so osebni podatki, pridobljeni s prodajo izdelkov, spletnim brskanjem, različnimi digitalnimi poizvedbami ter podobno, po drugi strani pa je njegov namen vzpostaviti enakovredne konkurenčne pogoje digitalnega okolja, ne da bi bila ogrožena temeljna pravica do zasebnosti uporabnikov. Še toliko bolj je to vprašanje kompleksno pri uporabi orodij umetne inteligence. Njihovi algoritmi so namreč zasnovani na obsežnemu naboru podatkov, ki te algoritme nadgrajujejo. Če umetna inteligenca deluje na omejenem naboru podatkov ter njihova vloga znotraj Akta o digitalnih trgih ni jasno opredeljena, kako se potem zagotavlja načelo preglednosti in pridobljenih soglasij, kako se dejansko prepreči zlorabo osebnih podatkov

(vpogledov), ki jih vodi umetna inteligenca. Sama umetna inteligenca ima lastno transformativno moč pri preoblikovanju interakcije vratarjev z osebnimi podatki, pridobljenimi s katere koli strani. Algoritmi umetne inteligence lahko za svoj namen strojnega učenja in napredne analitike izberejo katere koli podatke iz zbirke podatkov, ki so jim na razpolago. Ena od ključnih dilem je algoritemska pristranskost, kjer lahko sistem umetne inteligence, če je postavljena na pristranskih naborih podatkov, bistveno poslabša obstoječe družbene predsodke. Kako naj umetna inteligenca upošteva načelo poštenosti in pravičnosti?

V zgornjem primeru velja, da je paradoks zasebnosti konceptualni model, ki poskuša zajeti kompromis med udobjem in zasebnostjo. Medtem ko študije kažejo, da ljudje želijo skrbno varovati svoje osebne podatke, je enostavnost, s katero lahko stranke zaobidejo posamična pravila zasebnosti (TOS) ali pravilnike o zasebnosti v spletnih aplikacijah, del večne uganke psihologije človekovega varovanja zasebnosti v digitalni dobi.[62] Mestoma je opaziti, da inovativnost spodkopava temelje zasebnosti. Možnost biti neizsledljiv ali neopazovan v digitalni dobi pa je le pravni izraz, s katerim bi se fiktivno varovala zasebna sfera. Že sam vstop v fizično trgovino spremlja množica kamer, katerih sekundarna vloga, razen varovanja lastnine, je tudi spremljanje nakupovalnih navad in vzorcev potrošnikov. Številne nove aplikacije so zasnovane tako, da zagotavljajo storitve v zameno za osebne podatke. Vozila in naprave imajo GPS sledilnike, funkcijske ure spremljajo ravni telesne pripravljenosti, dejavnosti in lokacijo posameznega uporabnika. IoT naprave, med katerimi so tudi gospodinjski aparati, sledijo in spremljajo navade posameznikov in družin v samem domu. Vsi ti bodo preko jedrnih platform imeli možnost postati vratarji. Če pa ne bodo postali vratarji, bo za njih Akt o digitalnih trgih v celoti neuporabljiv. Medtem ko so posamezniki na mobilnih napravah in nenehno komunicirajo med seboj, jim spletne storitve, že tiste jedrne, ki so gradniki operacijskih sistemov, ves čas sledijo. Svetovna pandemija Covid-19 je še bolj povečala premik komuniciranja in nakupovanja v digitalno okolje. Ob tem se razvijajo različne aplikacije, ki dejansko posegajo v zasebnost posameznika in razkrivajo njegove osebne podatke. Ena od teh je na primer v Sloveniji sistem virtualnega zdravstvenega kartona. Posamezniki lahko prenesejo svoj bolniški karton, ki vsebuje izjemno občutljive podatke, na svoj telefon ali računalnik, zaradi povezanosti na splet pa tvegajo razkritje takšnih podatkov oziroma po drugi strani nehote omogočajo vdor v lastno zasebnost. Velja, da paradoks zasebnosti, ki je bil pred več kot 20 leti identificiran kot »nedoslednost

[62] Antón in Young, 2010, stran 27.

med izraženim odnosom do zasebnosti in vedenjem ljudi«, dejansko ni paradoks, ampak je iluzija.[63] V konceptu posameznikovega upravljanja lastne zasebnosti *Solove* vidi nesmiselnost in meni, da je upravljanje lastne zasebnosti obsežen, kompleksen in nikoli končan projekt, ki se ne spreminja in ga je nemogoče narediti celovito, zaradi česar je potrebno svojo zasebnost upravljati naključno in selektivno. Posamezniki se namreč v digitalnem okolju ne morejo naučiti pravil tveganja lastne zasebnosti, da bi lahko sprejemali premišljene odločitve glede narave varovanja te krhke pravice. Internet ljudem olajša izmenjavo informacij brez fizičnih elementov nastopa posameznih posledic. Če bi na primer ljudi lahko postavili v nabito polno dvorano, najverjetneje ne bi povedali enako, kot to povedo na spletu. Ko posamezniki objavljajo na spletu, ne vidijo na stotine obrazov, ki strmijo vanje.[64]

5 Zaključek

Resno tveganje za zagotavljanje zasebnosti uporabnikov je v pomanjkanju preglednosti storitev jedrnih platform, vratarjev ter preferenc oglaševanja v kontekstu samega Akta o digitalnih trgih, 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 pretoka in dostave ciljnih oglasov. V različni literaturi je bilo ponujenih več rešitev za povečanje varstva zasebnosti v tako zapletenem sistemu. Prva ideja je, da varstvo zasebnosti in varstvo osebnih podatkov kot temeljni pravici uporabnika vključujeta 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

[63] Solove, 2020, strani 1–51.
[64] Prav tam.

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.

Za pravno varstvo ima uporabnik trenutno na razpolago le soglasje, ki je opredeljeno v različnih pravnih predpisih, vendar je to soglasje v veliki večini le pravna opredelitev, ki ne doseže namena povprečnega uporabnika, predvsem pa ne v kontekstu Akta o digitalnih trgih. Uporabnik namreč v zameno lahkotnosti bivanja v digitalnem okolju poda 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. Uporabnik in ščitenje njegovih temeljnih pravic v okviru Akta o digitalnih trgih je sicer v središču dogajanja, pri čemer obstoječa pravila o varstvu podatkov niso najboljše sredstvo za njegovo pravno varstvo. Problem je, ker si je Evropska komisija zamislila Akt o digitalnih trgih kot dokument, ki bi že uvodoma poskušal določili celovit in vseobsegajoč okvir obravnavanja vratarjev digitalnih platform, pri čemer pa ni pomislila na to, da bi nomotehnično takšen predlog podala v okviru regulativne konvergence, kjer je mogoče splošna načela in pravila varovanja zasebnosti postopoma prilagoditi heterogenim značilnostim storitev posamezne digitalne platforme na podlagi bolj natančnega sektorskega pristopa. Ugotoviti je, da Akt o digitalnih trgih ne zasleduje cilja, zaradi katerega je bil sprejet, predvsem zato, ker se osredotoča na poslovne subjekte oziroma digitalne igralce, ne upošteva pa vidika uporabnika in njegovih motivacij uporabe digitalnih platform. Digitalne platforme namreč nadzorujejo enormno količino podatkov in ti podatki dajejo celoten vpogled v posameznikovo življenje. Edini konkretni način rešitve takšnega izziva bi bila celostna ločitev osebnih podatkov z jedrne platforme ter onemogočanje naknadnega dostopa vratarja do že uporabljenih osebnih podatkov. In navkljub *prima facie* pomembnim pomanjkljivostim glede skladnosti z LEUTP, je prav v povezavi z le-to posamezne določbe glede varovanja zasebnosti treba razlagati tako, da Akt o digitalnih trgih ne bo le črka na papirju.

Literatura

Acquisti, A. (2010) The Economics of Personal Data and Privacy, 30 Years after the OECD Privacy Guidelines, OECD Conference Centre Paris.

Acquisti, A. (2016) The Economics of Privacy, Journal of Economic Literature, 54(2), strani 449–492.
Antón, A. I., Earp, J. B., & Young, J. D. (2010) How internet users' privacy concerns have evolved since 2002, IEEE Security & Privacy, 8(1), strani 21–27.
Asunción, E. (2017) The business of personal data: Google, Facebook, and privacy issues in the EU and the USA, International Data Privacy Law, 7(1), strani 36–47.
Barzilai-Nahon, K. (2008) Toward a theory of network gate keeping: A framework for exploring infor-mation control, Journal of the American Information Science and Technology, 59(9), strani 1–20.
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.
Decarolis, F. (2023) Regulating online search in the EU: From the android case to the digital markets act and digital services act,
International Journal of Industrial Organization, 90(1), strani 1-17.
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.
Dimović, Z. (2023), Varstvo osebnih podatkov kot digitalnega portfelja v luči sodobnih metod oglaševanja, Univerzitetna založba Univerze v Mariboru, v Repas, M. (ur.) 2023. Dileme sodobnega oglaševanja: Izbrane teme, strani 192–223.
Helberger, N. (2015) Regulating the information intermediaries as gatekeepers of information diversity, Info, 17(6), strani 50–71.
Kelleher, D. (2006) Privacy and Data Protection Law in Ireland. (Galway: Tottel Publishing).
Kolta, A. (2020) Privacy and online gatekeepers, Mississippi Law Journal, 89(4), strani 619–646.
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.
Lewin, K. (1943) Forces behind food habits and methods of change. v The problem of Changing Food Habits, Report of the Committee on Food Habits, Washington, DC: National Academy of Sciences, strani 35–65.
Mitchell, A. (2023) Beware What you Wish for!, https://medium.com/mydex/beware-what-you-wish-for-e59dd1975f79 (obiskano 30. 1. 2024
Montero, J. J. (2019) Asymmetric Regulation for Competition in European Railways, Competition and Regulation in Network Industries, 20(2), strani 186–187.
Nissenbaum, H. (2004) Privacy as contextual integrity, Washington Law Review, Symposium: Tehnology, values, and the justice system, 79(1), strani 119–157.
Portuese, A. (2022) The Digital Markets Act: A Triumph of Regulation over innovation, Information Technology & Innovation Foundation, strani 1–16.
Siagian, R., Siahaan, L. & Hamzah, M., I. (2023) Human Rights in the Digital Era: Online Privacy, Freedom of Speech, and Personal Data Protection. Journal of Digital Learning and Distance Education, 2(1), strani 513–523.
Solove, D. J. (2020) The myth of the privacy paradox, GWU Legal Studies Research Paper Nr. 2020-10, strani 1–51.
Tene O. (2010) Privacy: The new generations, International Data Privacy Law Advance, 1(1), strani 1–8.
Warren, S., Brandeis, L. (1890) The right to privacy, Harward law review. IV(5), strani 193–220.

Summary

The speed of the digital industry has brought out the rise of fast-growing digital platforms, especially those with significant market shares, and this development is expected to continue. The infrastructure of operation has moved to a mobile and digital environment, where an individual is exposed to as much personal data as they share with others, either knowingly or unknowingly, and as a consequence, also allows access to their privacy. EU represents a large target market for globally operating digital platforms, although most of the largest ones come from the US and Asia, where existing competition

law under Article 102 TFEU is considered to attribute to these platforms the nature of essential infrastructure, which are subject to fair enforcement provisions, data sharing obligations and rights of platforms usage. Due to the identified unfair business practices of large online platforms and the resulting impact on competitiveness, the Digital Markets Act (DMA) details in its introductory provisions the obligations and prohibitions imposed on operators of digital platforms. Among these new obligations, perhaps the most dangerous is access to "data sharing", whereby it follows from the tenth indent of Article 6 of the DMA that the gatekeeper must, at the request of business users, provide effective, real-time access to and use of aggregated and non-aggregated data, including personal data, free of charge. Those can be provided or created in the context of product sales, web browsing, inquiries, and the provision of business user services. Such a dynamic digital landscape, however, creates an inherent paradox of privacy, where the competitiveness of the single market ends with the violation of fundamental human rights. As part of this article, the multi-faceted role of gatekeepers is addressed, which includes both sides, tech giants and EU regulators, facing the complexities of data management under the DMA and GDPR, focusing both on key principles such as operational transparency, user consent and liability for illegal operation. In doing so, the legal challenges posed by DMA in relation to the GPDR and mutual coordination of the right to privacy are outlined, regarding the needs of innovation and competitiveness. Within this framework, the question of the impact of artificial intelligence on the transformation of the relationship between gatekeepers and personal data is additionally addressed, with a significant part focusing on the ethical and legal issues related to innovations based on such shared data and the consequences arising from privacy rights of individuals. Namely, the results of exploring the privacy paradox are outlined based on the exchange for the ease of living in a digital environment, in which the user gives their consent to the processing of their data. This kind of processing results in the segmentation of this user into a specific group of targeted or behaviorally segmented groups, to which the promotional advertisement will reach in a very short time, or the user will become familiar with it. The user and the protection of their fundamental rights within the framework of the DMA are otherwise at the center of what is happening, and the existing data protection rules are not the best means for their legal protection. The problem is that the EC envisioned the DMA as a document which, from the outset, would try to define a comprehensive and all-encompassing framework for dealing with gatekeepers of digital platforms but did not think of making such nomotechnical proposal in the context of regulatory convergence, where it is possible to gradually adapt the general principles and rules of privacy protection to the heterogeneous characteristics of individual digital platform services based on a more precise sectoral approach. Considering the form in which it currently exists, the DMA does not pursue the goal with which it was adopted, mainly because it focused on business entities or digital players but did not consider the perspective of the user and their motivations for using digital platforms.

O avtorju

Zoran Dimović je doktorski kandidat na PF Univerze v Mariboru. Diplomiral je na FERI Maribor in magistriral na Mednarodni podiplomski šoli Jožef Stefan. Je avtor številnih znanstvenih in strokovnih prispevkov s področja digitalnega okolja ter varstva osebnih podatkov in zasebnosti, ki so bili objavljeni v domačih in tujih revijah. Prav tako je stalni zapriseženi sodni izvedenec.

Zoran Dimović is a PhD candidate at the Faculty of Law, University of Maribor. He holds a bachelor's degree from FERI Maribor and earned a master's degree from the Jožef Stefan International Postgraduate School. He has authored numerous scientific and professional papers on digital environments, data protection, and privacy, published in both domestic and international journals. Additionally, he is a permanently sworn court expert.