Aleš Vaupotič

Osebni podatki v zakonodaji in etiki novomedijske kulture

Personal Data in the Law and Ethics of New Media Culture

Digitalna in spletna novomedijska umetniška dela podobno kot ostale storitve t. i. novih informacijskih tehnologij zbirajo in nato uporabljajo podatke, ki so zelo pogosto povezani z uporabniki. Je to dovoljeno, za koga veljajo pravila, povezana z osebnimi podatki, na kaj je treba paziti? Vprašanja o zakonitosti in etičnosti obdelave podatkov povezujejo novomedijsko umetnost s splošnimi vprašanji informacijske etike in etike hitro razvijajočega se področja, ki ga imenujemo umetna inteligenca.[1]

Splošna uredba o varstvu podatkov (GDPR)

Splošna uredba o varstvu podatkov (General Data Protection Regulation, GDPR)[2] se v Evropski uniji uporablja od 25. maja 2018. Njen namen je varstvo posameznikov pri obdelavi osebnih podatkov. Temelji mdr. na Evropski konvenciji o varstvu človekovih pravic, ki pravi: »Vsakdo ima pravico do spoštovanja njegovega zasebnega in družinskega življenja, doma in dopisovanja« (prim. 8. člen). Gre za problematiko, ki postaja vedno bolj pomembna v čedalje bolj digitalizirani družbi, pa vendar o njej morda ne razmišljamo dovolj.

Kdaj je podatek osebni podatek?

Osebni podatki so povezani s posameznico, ko jo je mogoče prek njih določiti. Primeri so:

> ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika. (1. alineja 4. člena GDPR)

Torej, imena oseb so vedno osebni podatki, prav tako standardne identifikacijske številke, kot je EMŠO, telefonske številke, uporabniška imena na družabnih omrežjih, (elektronski) naslovi, tudi službena e-pošta.[3] Podatki o podjetjih z eno zaposleno so lahko osebni podatki, če omogočajo določitev fizične osebe.[4] Fotografija osebe – oz. katerikoli biometričen podatek – je osebni podatek, ker, oz. če, omogoča identifikacijo.[5] Spletni piškotki, ki jih strežnik shrani v računalnike uporabnikov, da bi jih prepoznal prek več spletnih strani ali ob ponovnem obisku spletišča, so lahko osebni podatki.[6] Kombinacije podatkov, torej podatki v povezavi s sicer dostopnimi podatki, lahko omogočijo identifikacije in tako postanejo osebni podatki. V primeru psevdonimiziranih[7] osebnih podatkov je potrebno upoštevati, kako zahteven, dolgotrajen ali kakorkoli dosegljiv je postopek, da se ugotovi konkretna oseba za psevdonimom – anonimizirani podatki niso osebni podatki. Odločilno je torej vprašanje, ali je mogoče določiti, za katero fizično osebo gre, ob upoštevanju dosegljivih finančnih in tehničnih sredstev v trenutku obdelave ter drugih omejitev.

Veljavnost GDPR, odgovornost in načela

Uredba velja za podatke oseb, ki so v Evropski uniji, ne samo podatke državljanov članic, in ne glede na to ali je sedež upravljavca ali obdelovalca v Evropski uniji (ter seveda za vse organizacije s sedežem v Uniji). Gre npr. za osebne podatke strank ali obiskovalcev spletišč. Luciano Floridi v *Etiki umetne inteligence* (*Ethics of Artificial Intelligence*, 2023) zapiše, da je posebna odlika GDPR njen pristop, ko izkorišča »povezavo« osebne identitete in osebnih informacij, da bi obšla »ločitev« prava in ozemeljskosti. To

1 Besedilo je nastalo v okvirih interdisciplinarnega raziskovalnega projekta *Trajnostna digitalna hramba slovenske novomedijske umetnosti* (J7-3158), ki ga financira Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije. Je kratek orientacijski pregled in se ga ne sme tolmačiti kot pravni nasvet za npr. delovanje društev.

2 Zgoščena predstavitev na https://gdpr.eu. GDPR se uporablja neposredno, Zakon o varstvu osebnih podatkov (ZVOP-2) v Sloveniji dodatno ureja nekatera vsebinska in postopkovna vprašanja, ne sme pa spreminjati odločb temeljne evropske uredbe. (Vse povezave v članku so delovale 24. 12. 2024.)

3 V obliki ime.priimek@podjetje.si, ne pa tudi neosebna oblika info@podjetje.si.

4 https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en

5 https://www.ip-rs.si/mnenja-gdpr/6048a64130f43

6 Prim. 225. člen Zakona o elektronskih komunikacijah (ZEKom-2) in https://gdpr.eu/cookies. Še bolj zapleteno je vprašanje IP naslova, številke, ki identificira uporabničin računalnik, ko npr. dostopa do spletne strani na strežniku s spletiščem. Za ponudnika dostopa do interneta, ki npr. izstavlja mesečne račune, je IP naslov uporabnice zaradi dodatnih podatkov očitno osebni podatek, vprašanje pa je bolj odprto, ko gre za ustvarjalce spletnih strani, ki imajo dostop samo do IP številke, ki je sestavni del delovanja spletnih HTTP strežnikov, prim. Lundevall-Unger in Tranvik.

7 Psevdonimizirane podatke »je mogoče z uporabo dodatnih informacij pripisati posamezniku« (Uvodna izjava št. 26 in 5. alineja 4. člena GDPR).

naredi, s tem da utemelji varstvo osebnih podatkov v prvem (na koga so »pritrjeni«, kar je zdaj odločilno) in ne v drugem (kje se obdelujejo, kar ni več pomembno). (8)

S takim pristopom se upošteva globalno dosegljivost storitev in komunikacij prek interneta, kar predstavlja načelno težavo za pravo, ki je povezano z nacionalnimi zakonodajami.

V primeru, da ima upravljavec osebnih podatkov sedež zunaj Evropske unije, je odločilna povezanost obdelave z nudenjem blaga ali storitev posameznikom v Uniji, »ne glede na to, ali so povezane s plačilom.« Sama dostopnost spletišča iz teritorija Unije še ni dovolj, vendar pa

> se lahko z dejavniki, kot so uporaba jezika ali valute, ki se na splošno uporablja v eni ali več državah članicah, z možnostjo naročanja blaga in storitev v tem drugem jeziku, ali navedba strank ali uporabnikov, ki so v Uniji, jasno pokaže, da želi upravljavec nuditi blago ali storitve posameznikom, na katere se nanašajo osebni podatki, v Uniji. (Uvodna izjava št. 23 GDPR)

Prav tako se Uredba uporablja za organizacije zunaj Unije, »kadar je obdelava povezana s spremljanjem vedenja takih posameznikov, na katere se nanašajo osebni podatki, kolikor njihovo vedenje poteka v Uniji« (Uvodna izjava št. 24, prim. tudi 2. odst. 3. člena GDPR).

Strežniki, partnerji in pravne osebe v tujini potemtakem ne omogočajo, da bi se obšlo evropska pravila glede osebnih podatkov. Gre za pomembno vprašanje, ki se bo z rabo različnih oblik generativne umetne inteligence še zaostrovalo.[8] Luciano Floridi opozarja na dvojnost dilem raziskovalne etike in potrošniške etike.

> Npr. podjetje bi lahko izvozilo svoje raziskave in potem zasnovalo, razvilo in naučilo algoritme (npr. za prepoznavanje obrazov) na lokalnih osebnih podatkih v državi zunaj EU, z drugačnim, šibkejšim, neizvajanim etičnim in pravnim okvirjem za varstvo osebnih podatkov. V skladu z GDPR bi bilo to neetično in nelegalno v EU. Vendar pa bi se algoritmi, ko bi bili naučeni, nato lahko uvozili v EU in uporabili brez sankcij, ali da bi to sploh bilo dojeto kot sporno. [Potrošnja neetično pridobljenih dobrin je v primerjavi z raziskovalno etiko še] bolj nejasna, manj očitno problematična in jo je zato bolj težko nadzorovati in omejiti. (*Etika umetne inteligence* 73)[9]

Upravljavec je fizična ali pravna oseba (npr. zastopnica podjetja ali društva, samostojna podjetnica ali ustvarjalka), ki določa namene in sredstva obdelave. »**Upravljavec je odgovoren za skladnost** [obdelave osebnih podatkov …] **in je to skladnost tudi zmožen dokazati** (’odgovornost’)« (2. odst. 5. člena GDPR). Obdelovalec dejansko obdeluje podatke, lahko je to upravljavec ali pa drug izvajalec v imenu upravljavca.[10] **Obdelava podatkov vključuje pravzaprav, karkoli se dela z njimi**, avtomatično ali ne: »zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje« (2. alineja 4. člena GDPR). GDPR ne velja za »fizične osebe med potekom popolnoma osebne ali domače dejavnosti,« kar pomeni, da **tudi fizična oseba lahko postane upravljavka osebnih podatkov**, če posreduje tuje osebne podatke, in je lahko za napake pri tem početju tudi kaznovana.[11]

Namen GDPR, kot je razvidno iz celotnega naslova uredbe, je poleg varstva tudi prosti pretok osebnih podatkov. Kaj je torej dovoljeno in pod kakšnimi pogoji? Npr. v primeru fizičnih oseb, umetnic, samozaposlenih ali društev. Slediti je treba sedmim načelom (5. člen GDPR):

1. »Zakonitost, pravičnost in preglednost.« Potrebno je npr. objaviti **obvestilo o obdelavi osebnih podatkov, ki je primerno in razumljivo za ciljno skupino uporabnikov,** in si prizadevati za uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki.[12]
2. »Omejitev namena,« posameznici je treba **predstaviti** jasno določene in zakonite **namene**, ki nato določajo meje dovoljenega zbiranja in obdelovanja osebnih podatkov.
3. Obdeluje se »**najmanjši obseg** podatkov« v skladu z namenom.
4. »Točnost,« podatki se morajo **posodabljati**, netočne podatke je treba brez odlašanja **brisati**.
5. »Omejitev shranjevanja,« podatki se hranijo le toliko časa, kolikor je nujno v skladu z namenom obdelave.[13]
6. »Celovitost in zaupnost;« to načelo pomeni, da je nujno zagotoviti varnost, npr. s šifriranjem.
7. »Odgovornost« (predvsem upravljavca, glej zgoraj.)

8 Za pomen izraza umetna inteligenca, ki se ne nanaša na t.i. splošno umetno inteligenco, potencialne zares pametne stroje, ampak na računalniške postopke, ki se danes dejansko uporabljajo, prim. *Opredelitev umetne inteligence: glavne zmogljivosti in znanstvene discipline* Strokovne skupine na visoki ravni za umetno inteligenco pri Evropski komisiji.

9 Prim. Floridi, *Ethics of Artificial Intelligence* pogl. 5.5 *Ethics Dumping*, 5.2 *Ethics Shopping* in 5.3 *Ethics Bluewashing*.

10 Npr.: »Arnes nudi storitve [obdelave osebnih podatkov] članicam omrežja ARNES, preko njih pa njihovim končnim uporabnikom (zaposlenim, šolajočim ipd.). Poleg tega lahko Arnes v dogovoru z ustreznimi resornimi ministrstvi nudi storitve tudi nekaterim posebnim kategorijam posameznikov (samostojni raziskovalci in kulturni delavci, invalidi). / Članice omrežja Arnes […] same upravljajo e-identitete svojih uporabnikov in pri tem obdelujejo njihove osebne podatke. Z izdajanjem teh identitet (AAI-računov) članica omogoča svojim uporabnikom uporabo Arnesovih storitev.« https://www.arnes.si/zavod-arnes/katalog-informacij/varovanje-zasebnosti-uporabnikov-storitev-omrezja-arnes/.

11 Npr. avstrijski nadzorni organ je kaznoval fizično osebo na podlagi GDPR, https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2021-0.518.795.

12 Npr. https://www.ip-rs.si/o-pooblaščencu/informacije-javnega-značaja/informacije-o-obdelavi-osebnih-podatkov.

13 »[O]sebni podatki se lahko shranjujejo za daljše obdobje, če bodo obdelani zgolj za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene v skladu s členom 89(1), pri čemer je treba izvajati ustrezne tehnične in organizacijske ukrepe iz te uredbe, da se zaščitijo pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki.« V 89. členu sta omenjeni psevdonimizacija in obdelava podatkov, ki prepreči indentifikacije posameznikov.

Poleg preglednosti glede namenov zbiranja, tj. samih zbranih in obdelanih podatkov, ter omejitve pri obsegu obdelave, zagotavljanja točnosti, je pomembna tudi skrb za varnost osebnih podatkov. Uredba sledi načelu »vgrajenega in privzetega varstva podatkov« (Uvodna izjava št. 78, GDPR), ki zagotavlja po eni strani tehnične postopke za varnost, kot je dvodejavniška avtentikacija dostopov do osebnih podatkov. **Če pride do vdora ali kraje ipd. (nešifriranih oz. uporabnih) podatkov,** tudi strojne opreme, **je treba takoj oz. najkasneje v 72 urah obvestiti posameznike** (in nadzorni organ, pri nas Informacijskega pooblaščenca Republike Slovenije). Organizacijski vidik zagotavljanja varnosti pomeni mdr. določitev odgovornih oseb v organizaciji in omejitev dostopa do osebnih podatkov.

Organizacija mora imenovati pooblaščeno osebo za varstvo podatkov, če je javna ustanova ali če s svojo dejavnostjo redno in obsežno spremlja posameznike (zavarovalnice in npr. spletne trgovine, ki izdelujejo profile kupcev) ali če obdeluje občutljive podatke, t. i. posebne vrste podatkov (npr. politično mnenje, etnično poreklo).[14] **Obveznosti dokumentiranja dejavnosti obdelav osebnih podatkov** se razlikujejo glede na velikost organizacije: če je zaposlenih več kot 250, je treba evidentirati vse dejavnosti obdelav, sicer pa le **dejavnosti, ki niso občasne** ali **ki predstavljajo tveganje za pravice in svoboščine** posameznikov, na katere se nanašajo podatki, ali ki vključujejo posebne vrste osebnih podatkov oz. podatke v zvezi s kazenskimi obsodbami in prekrški.[15] Evidenca dejavnosti obdelave vsebuje vsaj naslednje informacije:

1. kontaktne podatke upravljavca (in obdelovalca, če to ni upravljavec);
2. namene in vrsto obdelave;
3. opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst osebnih podatkov;
4. kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, ali informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo;
5. predvidene roke za izbris podatkov;
6. splošni opis tehničnih in organizacijskih varnostnih ukrepov.[16]

Kdaj je obdelava osebnih podatkov dovoljena?

Obdelava osebnih podatkov je zakonita, upoštevajoč enega od šestih pogojev (6. člen GDPR):

a. privolitev,
b. če je potrebno za pripravo in izvajanje pogodbe,
c. zakonska obveznost, ki velja za upravljavca,
d. reševanje življenj,
e. »opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu,« (npr. privatno komunalno podjetje);
f. zakoniti interes.

Večina razlogov je razumljivih. Zadnji, zakoniti interes, je s pravnega vidika zahteven – je sicer fleksibilen, vendar nad takimi interesi upravljavca prevladajo interesi ali temeljne pravice in svoboščine posameznice, še posebej če gre za osebne podatke otrok. Opraviti je treba pravno presojo zakonitega interesa in to dokumentacijo hraniti. Izbira te podlage pomeni sprejetje dodatne odgovornosti za varovanje interesov in pravic posameznikov. Ko se določi podlaga za obdelavo osebnih podatkov, je treba odločitev dokumentirati in v skladu z načelom preglednosti obvestiti posameznico o delu z njenimi osebnimi podatki.[17]

Privolitev posameznice, da se njeni osebni podatki obdelujejo, vključuje ločeno jasno prošnjo za vsak namen posebej, privolitev je treba dokumentirati, omogočiti je treba preklic privolitve (podlage za obdelavo npr. ni mogoče naknadno spremeniti), pred 13. letom starosti se zahteva tudi dovoljenje staršev (v Sloveniji pred 15. letom, prim. 8. člen Zakona o varstvu osebnih podatkov, ZVOP-2).

Vprašanje privolitve je vsebinsko povezano z zaupanjem na področju digitalne obdelave podatkov in npr. umetne inteligence, kjer je poleg različnih kršitev in nezakonitih ter neetičnih ravnanj poseben problem razložljivost delovanja uporabljenih algoritmov in njihovih rezultatov (prim. *Etične smernice za zaupanja vredno umetno inteligenco* Strokovne skupine na visoki ravni za umetno inteligenco). V zvezi s privolitvijo je mogoče omeniti problematični pojav širitve prvotnega pomena (*function creep*), ki pomeni obliko zavajanja (Koops; Floridi, *Etika umetne inteligence* pogl. 5.3 Ethics Bluewashing), ali pa pritiske in pogojevanja, ki onemogočijo prostovoljnost izbire, ali uporabo po nepotrebnem zapletenega oz. za skupino naslovnikov prezahtevnega jezika. Molk ali vnaprej izpolnjeni obrazci ter taktika utrujanja (*click fatigue*, Hornuf in Mangold) niso oblike veljavne privolitve. Obstajata veljavna in **izrecna privolitev, ki je potrebna** za obdelavo že omenjenih t. i. posebnih vrst, torej občutljivih podatkov, ob prenosu podatkov v tretje države ali mednarodne organizacije, pri čemer niso sprejeti ustrezni zaščitni ukrepi (49. člen GDPR), in **ko odločanje o posameznici temelji izključno na avtomatizirani obdelavi,**

14 »Prepovedani sta obdelava osebnih podatkov, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.« Razen pod posebnimi pogoji (prim. 9. člen GDPR). O pooblaščeni osebi govori 37. člen GDPR.

15 Besedilo *Working party 29 position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR* obravnava izjeme od zahtev po dokumentiranju dejavnosti obdelav, https://ec.europa.eu/newsroom/article29/items/624045.

16 V določenih primerih so obvezne t. i. ocene učinkov v zvezi z varstvom osebnih podatkov, v primeru če obstaja velika verjetnost tveganja za pravice in svoboščine (oblikovanje profilov oseb, obsežno sistematično spremljanje javnega območja ipd.), prim. *Ocene učinkov na varstvo podatkov: Smernice Informacijskega pooblaščenca* (2019), https://www.ip-rs.si/prirocniki_smernice/Smernice_o_ocenah_ucinka.pdf. Prim. tudi https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/ključna-področja-uredbe/evidenca-dejavnosti-obdelave.

17 Prim. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

vključno z oblikovanjem profilov. Izrecna privolitev naj bi bila pisna, lahko je elektronska, svetuje se dvostopenjsko preverjanje privolitve (npr. prek potrditvenega SMS). Preklic privolitve mora biti enako enostaven kot sama privolitev, o načinu preklica mora biti posameznica obveščena pred privolitvijo.

GDPR obravnava **uresničevanje pravic posameznice**, na katero se nanašajo osebni podatki, in to obsega seznanitev tako glede samih podatkov in načinov obdelave kot tudi glede pravic posameznice v skladu z načelom preglednosti: dostop do osebnih podatkov posameznice, ki jih obdeluje upravljavec, popravek, izbris (pravica do pozabe), omejevanje obdelave, prenosljivost (npr. posredovanje digitaliziranih podatkov v strojno berljivi datoteki na uporabničino zahtevo), pravica do ugovora (ob avtomatizirani obdelavi in ustvarjanju profilov). Upravljavec mora zagotoviti izvajanje teh pravic najkasneje v roku enega meseca od zahteve in načeloma brezplačno (3. odst. 12. člena GDPR).

Pravo, etika in digitalizacija medijev

Akti Evropske unije o umetni inteligenci, digitalnih storitvah in digitalnih trgih

Evropski parlament je 13. marca 2024 podprl Akt o umetni inteligenci. Gre seveda za področje, ki se zelo hitro razvija in je težko obvladljivo. Pristop temelji na določitvi stopnje tveganja pri končni uporabi umetne inteligence; če je stopnja visoka, bo omejitev več, če je stopnja nizka, bo regulacije manj ali je ne bo. Akt o umetni inteligenci uvaja štiri kategorije glede na stopnjo tveganja:

1. nesprejemljiva stopnja tveganja – takšna raba algoritmov umetne inteligence je prepovedana (rangiranje posameznikov v družbi, govoreče igrače, ki napeljujejo na nevarno obnašanje ipd.).
2. Visoko stopnjo tveganja pomeni npr. raba umetne inteligence v sodbah sodišč (prim. Angwin *et al.*) – tovrstni sistemi bodo registrirani pri Evropski uniji, potreben bo certifikat, ob bistveni spremembi delovanja umetne inteligence se preverjanje in postopek dodelitve certifikata ponovi.
3. Stopnja omejenega tveganja se osredotoča na vprašanje preglednosti delovanja, npr. če se uporabnica na spletu pogovarja s sistemom umetne inteligence, je treba to predhodno izrecno povedati.
4. Akt dovoli uporabo umetne inteligence, kadar predstavlja minimalno tveganje, primer poleg iger so tudi filtri za neželeno spletno pošto.[18]

Pristop se torej podobno kot v zvezi z osebnimi podatki osredotoča na učinke in uvaja pravila, izhajajoč iz ocene vplivov računalniških oz. hibridnih sistemov (to so storitve, kjer v obdelavi sodelujejo tudi ljudje). Kot ni mogoče živeti brez obdelave osebnih podatkov, tako tudi ostalih (digitalnih) podatkov ne bo mogoče kratko malo ubraniti pred – sicer trenutno v splošni javnosti zelo slabo razumljeno – umetno inteligenco. Omenjeni akt se povezuje z Aktom o digitalnih storitvah, ki sledi načelu, kar je nezakonito v realnem svetu, je nezakonito tudi na spletu (lažne novice, reklame namenjene otrokom … dotika se v prvi vrsti družbenih medijev, platform in spletnih tržnic, pri nas npr. Bolhe), uporablja se od 17. februarja 2024.[19]

Akt o digitalnih trgih pa ščiti podjetja pred zlorabo monopolov globalnih platform. Uporablja se

> le za velika globalna podjetja. Ta so v uredbi v skladu z objektivnimi merili opredeljena kot vratarji (ang. gatekeepers). Gre za podjetja, ki nadzorujejo vsaj eno jedrno platformno storitev, kot so iskalnik, družbeno omrežje, storitve za pošiljanje sporočil, operacijski sistem ali spletna tržnica, ter imajo veliko uporabnikov v več državah Unije. Vratarji bodo morali ostalim podjetjem omogočati interoperabilnost s svojimi storitvami, dostop do podatkov […][20]

Trenutni seznam vratarjev vključuje podjetja Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, ki morajo od 7. marca 2024 dalje v celoti ustrezati zahtevam. Evropska unija je že 25. marca sporočila, da je v zvezi z morebitnim kršenjem Akta o digitalnih trgih uvedla preiskavo Mete, Appla in Alphabeta (ki ima v lasti Google).[21]

Mehka etika kot podpora za prakso znotraj meja zakonitega ravnanja

Poseben problem – poleg nesorazmerja moči – predstavlja na področju digitalne komunikacije preglednost delovanja algoritmov, ki so s strojno obdelavo podatkov na še pred kratkim nesluten način olajšali prenosljivost in zbiranje podatkov. (Gre tudi za tehničen problem, ki pa v tem besedilu ne bo obravnavan.) Zakonodaja v tem kontekstu pravzaprav pričakovano zamuja, kar pa seveda ni opravičilo. Nove oblike obdelave podatkov praviloma vključujejo možnost obdelave osebnih podatkov – npr. z merjenjem fizičnega videza in obnašanja posameznikov je osebo kaj hitro mogoče določiti. Kako se v takem okolju obnašati, kdaj smo v mejah zakona, kdaj delujemo etično? Luciano Floridi ob obravnavi izzivov in priložnosti umetne inteligence pregleda in komentira rešitev, ki jo predstavlja GDPR, ki deluje

18 https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

19 Prim. https://www.consilium.europa.eu/sl/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act in https://www.gov.si/novice/2024-02-19-zakljucena-prva-obravnava-predloga-zakona-o-izvajanju-uredbe-eu-o-enotnem-trgu-digitalnih-storitev.

20 Prim. https://www.gov.si/novice/2022-11-04-v-veljavo-stopil-akt-o-digitalnih-trgih.

21 Prim. https://www.bbc.com/news/technology-68655093 in podrobneje https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689.

v mešani resničnosti digitalnega in analognega, s spletom povezanega in nepovezanega.

Floridi si pri razumevanju primera uredbe s področja varstva podatkov pomaga z ločevanjem med mehko in trdo etiko (*Etika umetne inteligence* 6. pogl.). Delitev je privzeta iz prava, ki razlikuje trdo in mehko pravo, slednjega predstavljajo resolucije in priporočila, ki niso zavezujoča (Shaffer in Pollack). Trda etika obstaja pred zakonodajo in jo nato tudi sooblikuje, Floridi jo poveže z načelom Rose Parks, ki se je v svoji akciji državljanske nepokorščine odločila za neupoštevanje neetičnega zakona, ki je takrat zahteval, da Afriške Američanke ali Američani odstopijo sedež na avtobusu belcem, celo v delu namenjenem nebelim potnikom. V primeru trde etike ne pomeni, da, če bi s pravnega vidika oseba nekaj morala narediti, to sme narediti tudi z vidika etike. Upor kot aktivna trda etika vodi – vsaj v nekaterih primerih – v spremembo zakonodaje. Nasprotno t. i. mehka etika nastopi po spoštovanju zakonov, tukaj velja načelo: če je nekaj predpisano z zakonom, je to tudi etično dovoljeno.

V skladu s Kantom etične zahteve privzemajo, da je takšno delovanje tudi izvedljivo, ni etično zahtevati nemogočega. Skozi čas se obseg izvedljivega zaradi tehničnih inovacij širi. Mehka etika je torej omejena s tem, kar je moralno dobro (v Evropski uniji so to najmanj vsaj človekove pravice) in kar je zakonito, onkraj tega je protizakonito, kjer lahko nastopi trda etika. Mehka etika je neuporabna v nemoralnih družbah, Floridi omeni neupoštevanje človekovih pravic na Kitajskem, dodaja pa, da so tudi v Evropski uniji potrebni posegi trde etike, npr. v primeru irskega referenduma o splavu iz leta 2018, ki je prinesel ustavni amandma.

> Znotraj EU se lahko upravičeno uporablja mehka etika za pomoč agentom (vključno s posamezniki, skupinami, podjetji, vladami, organizacijami), da z moralnega vidika bolj in bolje izkoristijo priložnosti, ki jih ponujajo digitalne inovacije. Kajti tudi za EU velja, zakonodaja je potrebna, vendar nezadostna. (84)

Primer mehke etike je samoregulacija. Seveda je mogoče delovati nezakonito in neetično, prav tako strah pred tehnologijo pogosto vodi v potiskanje glave v pesek z negativnimi posledicami … kar pa je na tem mestu pomembneje, je to, da je tudi prostor za zakonito delovanje pravzaprav širok, nabor možnih izbir je velik in razumevanje posledic, npr. posledic računalniške obdelave podatkov, ni enoznačno in preprosto. Že sama določitev, kaj je osebni podatek, je prepuščena odločitvi upravljavca, ki sledi prej očrtanim načelom iz GDPR in drugim etičnim premislekom. Priložnost, ki jo omenja Floridi, ni primer zaslepljene vere v tehnološke inovacije, ampak, kot zapiše, upošteva, da trenutno glavni izziv ni več inovacija, izumljanje novega, temveč upravljanje z digitalnimi in ostalimi informacijskimi viri, gre za enega od treh normativnih pristopov, ki dopolnjuje etiko in pravo. Dobro upravljanje namreč samo po sebi ni nujno vezano na dvojnosti moralnega in nemoralnega ali zakonitega in nezakonitega (79).

Floridi mehko etiko razume kot etično ogrodje, ki pomaga pri razumevanju etičnih dilem, ki se pojavljajo. Za razumevanje njene vloge je treba upoštevati pet komponent, ki se povezujejo po dveh načelih, načelu generiranja in načelu interpretiranja (pogl. 6.5). Trda etika je podlaga za nastanek zakonodaje, predvsem devetindevetdesetih členov GDPR, pa tudi za sto triinsedemdesetih Uvodnih izjav. Zakon nato generira etične, pravne in družbene implikacije in priložnosti, tako tisto, kar neposredno sledi členom, kot tudi vprašanja, ki se deloma ali v celoti razkrijejo ob tej uredbi (upoštevati je treba, da priložnosti niso nujno pozitivne z vidika družbene dobrodejnosti). Povezave od mehke etike do Uvodnih izjav in naprej do členov potekajo prek odnosov interpretiranja: Uvodne izjave pojasnjujejo razloge in določbe zakonov in same po sebi niso zavezujoče, hkrati pa so neposredno orodje za pojasnjevanje členov. Mehka etika prispeva k interpretiranju Uvodnih izjav in s tem samih členov. Kot že rečeno, skladna mora biti s trdo etiko, ki generira zakonodajo. Prispeva tudi k naboru načinov, kako se je mogoče konstruktivno spopasti z izzivi etičnih in družbenih implikacij zakonodaje na področju digitalne kulture.

Na tem mestu ni mogoče podrobneje razviti konkretnih etičnih načel, ki omogočajo orientacijo na področju današnje poplave podatkov in izzivov njihovih obdelav. Omenimo, da Floridi ob primerjavi bioetike z etiko umetne inteligence dodaja štirim bioetičnim principom – dobrodejnost, preprečevanje škode, spoštovanje človekove avtonomije, pravičnost – še dodatnega petega, razložljivost, ki pomeni nov, še ne razrešen izziv, saj so izhodni podatki algoritmov včasih nerazložljivi, to pa se pojavlja kot problem tudi v zvezi s pomembnimi družbenimi dilemami, npr. avtomatičnega določanja (64).[22] Aktivno upoštevanje in razvijanje digitalne etike ponuja dve prednosti. Ponuja podporo za strateško odločanje o priložnostih – previdnost mora biti uravnotežena z dolžnostjo, da se ne izognemo temu, kar bi bilo treba narediti (tj. uporabiti zbrane podatkovne zbirke in, v premeru umetne inteligence, zaloge t. i. »pametne aktivnosti« nečloveških in hibridnih agentov). Po drugi strani je mehka etika rešitev za upravljanje s tveganji – etični premislek na začetku načrtovanja projektov pomeni prednosti kasneje, oz. preprečevanje napačnih potez. S tega vidika sta seveda smiselna – še posebej v tem trenutku, ko se sistemi obdelave podatkov in njihove uporabe v algoritmih pametnih umetnih agentov oblikujejo za bližnjo in bolj oddaljeno prihodnost – principa iz Uvodne izjave št. 78 GDPR o privzetem in vgrajenem varstvu podatkov.

22 Prim. tudi že omenjene *Etične smernice za zaupanja vredno umetno inteligenco* Strokovne skupine na visoki ravni za umetno inteligenco pri Evropski komisiji.

Varovanje osebnih podatkov mora biti izhodišče pri zasnovi in ne naknadni dodatek k novim informacijskim sistemom.

Zakaj je treba varovati osebne podatke? Etika informacijskih organizmov

Na videz neobičajno vprašanje je vendarle razumljivo in legitimno, saj načrtovanje mehanizmov za varovanje osebnih podatkov ob tako rekoč vseh obdelavah podatkov predstavlja veliko obremenitev za delo na številnih področjih. Zakaj je težava, če nekdo shrani podatke o meni? Saj nič ne izgubim? Ali če nekaj vendarle izgubim, kakšen je pravzaprav negativni učinek name?

Gre za kompleksno problematiko, ki se ji Luciano Floridi izčrpno posveti, na tem mestu pa je mogoče le nakazati smer razmišljanja.[23] Predpostavimo torej, da osebni podatki niso oblika lastnine – zdi se nam, da spričo digitalne reproduktibilnosti podatkov pravzaprav ne izgubim nič otipljivega, nasprotno kot npr. pri kraji avtomobila. Floridi predlaga, da je ljudi mogoče razumeti kot skupke informacij, kot informacijske organizme. S tega vidika je prilaščanje podatkov iz celote, ki je posameznična osebnost, odvzem dela te danosti in poseg v integriteto posameznice. Vendar, kaj konkretno oseba izgubi, ko so shranjeni in obdelani kot kopija? Težava je, da je oseba hkrati navzoča npr. v javnem prostoru, obenem pa prek nadzornih kamer tudi v prostoru, ki ga opazuje in nadzoruje nekdo drug. V tem drugem prostoru je oseba brez možnosti delovanja, saj nadzorovalka sama ne vstopa v opazovani oddaljeni prostor – nadzorovana oseba je, na metaforičen način, ugrabljena. Floridi pravi:

> zasebnost postane obramba osebne identitete in edinstvenosti. Nekonsistentnost med zasebnimi in javnimi prostori se [če je oseba razumljena kot informacijska celota] ne pojavlja več: opazovana želi ohraniti svojo celovitost kot informacijska entiteta, tudi ko je na povsem javnem mestu. Navsezadnje je ugrabitev kaznivo dejanje ne glede na to, kje je storjeno, v javnosti ali ne. Kar nekdo kupi, obleče ali počne v javnosti, spada v sfero, ki ni nikogaršnja posebna last, vendar spremljanje in beleženje tega odvzame tej javni sferi del informacij, ki sestavljajo opazovano [osebo …], in jo naredi del prostora, ki pripada in ga nadzoruje le opazovalka, do katerega opazovana sama nima drugega dostopa, in to na način, ki je za opazovano lahko popolnoma neviden (opazovana se pogosto ne zaveda, da je del njenih informacij ugrabljen). (Floridi, *Etika informacije* 50)

Drugačen primer, pasivna in neprostovoljna navzočnost v tujem informacijskem prostoru in hkrati izpostavljenost toku informacij pa je pravzaprav varianta indoktrinacije ali pranja možganov – naša informacijska celovitost se spreminja zaradi vsiljenega preobilja informacij.

Če povzamemo, prisotnost na daljavo, teleprezenca, je potemtakem lahko zmožnost delovanja v oddaljenem prostoru, ki ga hkrati opazujemo prek telekomunikacij, npr. ko kirurg vodi robotsko roko na daljavo. Gre za ontično teleprezenco, agent, npr. človek, lahko deluje oddaljeno in svoje početje tudi opazuje tako lokalno kot v oddaljenem prostoru. To je t. i. »prisotnost [na daljavo] naprej«. Zgoraj omenjena »vzvratna prisotnost« je prisotnost entitete na oddaljenem nadzornem ekranu, tam ne more delovati, ne more opazovati same sebe v tem oddaljenem prostoru, ker nima dostopa, je le pasivna nosilka lastnosti, s tem pa je kršena njena osebna integriteta. ■

Viri in literatura

Angwin, Julia, Jeff Larson, Surya Mattu in Lauren Kirchner. »Machine Bias.« *ProPublica* 23. 5. 2016. Splet. 8. 7. 2024 <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

Complete Guide to GDPR Complinace. Splet. 8. 7. 2024 <https://gdpr.eu>.

Evropska konvencija o varstvu človekovih pravic

Floridi, Luciano. *Ethics of Artificial Intelligence*. Oxford: OUP, 2023.

--- *Ethics of Information*. Oxford: OUP, 2013.

General Data Protection Regulation oz. Splošna uredba EU o varstvu podatkov (GDPR)

Hornuf, Lars in Sonja Mangold. »Digital Dark Nudges.« *Diginomics Research Perspectives*. Lars Hornuf (ed.). Springer, 2022. 89–104.

Informacijski pooblaščenec. Splet. 8. 7. 2024 <https://www.ip-rs.si>.

Koops, Bert-Jaap: »The concept of function creep.« *Law, Innovation and Technology* 13.1 (2021): 29–56.

Lundevall-Unger, Patrick in Tommy Tranvik. (2011). »IP addresses - Just a number?« *I. J. Law and Information Technology* 19.1 (2011): 53–73.

Shaffer, Gregory C. in Mark A. Pollack. »Hard Vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance.« *Minnesota Law Review* 49 (2010): 706–799.

Strokovna skupina na visoki ravni za umetno inteligenco pri Evropski komisiji, AI HLEG. *Etične smernice za zaupanja vredno umetno inteligenco*. Evropska komisija, 2019. 8. 7. 2024 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60438>.

Strokovna skupina na visoki ravni za umetno inteligenco pri Evropski komisiji, AI HLEG. *Opredelitev umetne inteligence: Glavne zmogljivosti in znanstvene discipline*. Evropska komisija, 2019. 8. 7. 2024 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60667>.

Zakon o elektronskih komunikacijah (ZEKom-2)

Zakon o varstvu osebnih podatkov (ZVOP-2)

23 Prim. predvsem pogl. 3.4.5 *Informacijska zasebnost: od vdora do ugrabitve* v *Etiki informacije* (*Ethics of Information*, 2013).