ISSN 1855-5861
e-ISSN 3024-0956

Izvirni znanstveni članek
UDK 366.1:342.721:004

Temni vzorci kot pravni problem: kako učinkovita je evropska zakonodaja pri omejevanju digitalne manipulacije?*

MANJA SKOČIR
magistrica prava, magistrica filozofije in primerjalne književnosti, mlada raziskovalka na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani, asistentka na Katedri za kazensko pravo Pravne fakultete Univerze v Ljubljani in doktorska študentka Pravne fakultete Univerze v Ljubljani

Povzetek

Avtorica obravnava pojav temnih vzorcev (angl. *dark patterns*) kot manifestacijo vedenjsko-ekonomskih spoznanj v digitalnem oblikovanju in kot pravni problem, ki ogroža avtonomijo uporabnikov. V prvem delu pojasni psihološke mehanizme, s katerimi temni vzorci vplivajo na uporabniške odločitve – z izrabo kognitivnih pristranskosti, avtomatiziranih odzivov in kontekstualnega uokvirjanja odločanja. Na podlagi analize literature predstavi razvoj koncepta od Brignullove tipologije zavajajočih praks do sodobnih taksonomij, ki temne vzorce razumejo kot večnivojske mehanizme vplivanja, pogosto vgrajene v arhitekturo digitalnih sistemov. V drugem delu se avtorica osredotoča na pravne odzive Evropske unije in ugotavlja, da se je regulacija začela z reinterpretacijo že obstoječih mehanizmov varstva zasebnosti in potrošnikov, danes pa jo dopolnjujejo akti, ki temne vzorce urejajo neposredno. Analiza pokaže, da pravo varstva osebnih podatkov nudi le delno zaščito – omejeno na primere, kjer gre za manipulativno pridobivanje soglasij –, potrošniško pravo pa ponuja širši okvir, vendar trči ob koncept »povprečnega potrošnika«, ki ne odraža realnih vedenjskih pristranskosti. Novi

* *Prispevek je nastal v okviru raziskovalnega projekta SENTRIX: Arhitektura kaznovanja: Izgradnja matrice odločanja, ki ga financira Evropski raziskovalni svet, in v okviru programske skupine Inštituta za kriminologijo – Družbeno nadzorstvo, kazenskopravni sistem, nasilje in preprečevanje viktimizacij v kontekstu visoko tehnološke družbe (P5-0221), ki jo financira ARIS.*

akti, kot sta Akt o digitalnih storitvah in Akt o umetni inteligenci, so pomemben premik k varstvu avtonomije v digitalnem odločanju. Avtorica tako prispeva k vzpostavitvi normativne razprave o temnih vzorcih v slovenskem prostoru in zagovarja potrebo po pravnem okviru, ki presega informacijsko in potrošniško paradigmo ter priznava človeško kognitivno ranljivost kot izhodišče digitalne regulacije.

Ključne besede: temni vzorci, digitalna manipulacija, arhitektura izbire, pravo varstva zasebnosti, pravo varstva potrošnikov.

Dark Patterns as a Legal Problem: How Effective Is European Legislation at Limiting Digital Manipulation?

Abstract

The article examines dark patterns as a manifestation of insights from behavioural economics in digital design, and as a legal issue that threatens user autonomy. The first part explains how dark patterns influence user decisions by exploiting cognitive biases, automated responses and the contextual framing of decision-making. Drawing on an analysis of existing literature, it traces the evolution of the concept from Brignull's classification of deceptive practices to modern taxonomies that recognise dark patterns as multi-level influence mechanisms, frequently embedded within the architecture of digital systems. The second part focuses on the European Union's legal responses, finding that regulation initially involved reinterpreting existing privacy and consumer protection mechanisms, but has since evolved to encompass the direct regulation of dark patterns. The analysis reveals that personal data protection law provides only limited protection, extending only to cases of manipulative consent, while consumer law provides a broader framework, albeit with the drawback of relying on the concept of the "average consumer", which does not accurately reflect real behavioural biases. New legislation, such as the Digital Services Act and the Artificial Intelligence Act, represents a significant shift towards safeguarding autonomy in digital decision-making processes. Thus, the article contributes to establishing a normative debate on dark patterns in the Slovenian context, advocating the need for a legal framework that recognises human cognitive vulnerability as the starting point for digital regulation, rather than relying on the information and consumer paradigms.

Keywords: dark patterns, digital manipulation, choice architecture, data protection law, consumer protection law.

1. Uvod

Vedenjska ekonomija je v zadnjih desetletjih temeljito spodkopala idealiziran model racionalnega posameznika, saj je empirično potrdila tisto, kar je desetletja prej naznanil že Fre-

ud – človek »ni gospodar niti v lastni hiši« – in kar intuitivno občutimo vsi, ki smo se kdaj prenajedli, kupili kaj nepotrebnega ali predolgo odlašali z opravili. Vedenjski ekonomisti so pokazali, da človeško odločanje pogosto ne sledi aksiomom racionalnosti in optimizacije, kakršne predpostavlja klasična ekonomska teorija,[1] saj so naše preference nestabilne, informacije nepopolne, čas pa omejen. Zato so odstopanja od idealizirane racionalnosti pričakovana, predvidljiva in (večinoma) neizogibna.[2]

V vlogi odločevalcev se – kot razkriva vedenjska ekonomija – ljudje pogosto zanašamo na (običajno sicer uporabne in zaželene) kognitivne bližnjice (tako imenovane hevristike),[3] podvrženi smo vplivu čustev, strasti[4] in konteksta.[5] Poleg tega je na naše odločanje mogoče učinkovito vplivati tako z uokvirjanjem[6] in s spreminjanjem odločevalskega okolja[7] kot tudi z uporabo tako imenovanih univerzalnih orožij prepričevanja.[8] Ta spoznanja so močno omajala podobo človeka kot racionalnega in samonadzorujočega akterja, saj so pokazala, da so naše odločitve pogosto predvidljivo neoptimalne in sistematično pristranske. Vendar vedenjska ekonomija ni le pripomogla k boljšemu razumevanju človeškega vedenja, ampak je odprla vrata novim strategijam vplivanja in manipulacije. Razumevanje človeške iracionalnosti ni le pot k boljšim odločitvam, temveč tudi potencialno nevarno in izjemno učinkovito orodje izkoriščanja.

Sodobne digitalne tehnologije so verjetno najizrazitejša manifestacija takšnega izkoriščanja. Zasnovane so na način, ki znanstvena spoznanja o človeškem vedenju pretvarja v tehnične in oblikovalske mehanizme vplivanja. Ideja, da je z nevsiljivimi, svobodo ohranjajočimi intervencijami ljudi mogoče voditi k boljšim odločitvam,[9] je v digitalni sferi prerasla v sistematično, avtomatizirano in personalizirano usmerjanje vedenja uporabnikov – ti v vlogi odločevalcev znotraj digitalnega okolja, pogosto soglašajo s politiko zasebnosti, ki ni v njihovem interesu, opravijo transakcijo za storitve, ki jih ne želijo, se prijavijo na prejemanje reklamnih sporočil, ki jih ne želijo. Za poimenovanje praks, ki s strateškim izkoriščanjem vedenjskih pristranskosti in subtilnim oblikovanjem uporabniških vmesnikov usmerjajo uporabnike v dejanja, ki jih sicer ne bi storili, in izbire, ki niso v njihovem interesu, se je v referenčni literaturi uveljavil

---

1 Strle in Markič, str. 21–24.

2 Kahneman, str. 151–273.

3 Prav tam.

4 Več na primer Damasio.

5 Ariely, str. 32–33.

6 Tversky in Kahneman, 1974, str. 1124 in nasl.

7 Thaler in Sunstein, 2022, str. 119–219; Tversky in Kahneman, 1981, str. 453–458.

8 Cialdini, str. 16–35.

9 Gre za tako imenovane dregljaje (angl. *nudge*), koncept, ki sta ga razvila Richard H. Thaler (2008) in Cass R. Sunstein (2022). Avtorja sta ga opredelila kot nevsiljivo obliko vplivanja na vedenje posameznikov z oblikovanjem »arhitekture izbire«, ki ljudi spodbuja k boljšim odločitvam, ne da bi pri tem omejevala njihove možnosti izbire.

izraz temni vzorci (angl. *dark patterns*).[10] Ti so resna grožnja avtonomiji in zasebnosti uporabnikov digitalnih okolij, zato zaslužijo podrobno analizo in oceno ustreznosti veljavne pravne regulacije.

Članek analizira pojav temnih vzorcev kot manifestacijo vedenjsko-ekonomskih spoznanj v digitalnem oblikovanju ter pojasni psihološke mehanizme, s katerimi vplivajo na vedenje uporabnikov. Sistematično predstavi obstoječe in nove regulativne odzive Evropske unije na ravni prava varstva zasebnosti, potrošniškega prava ter horizontalnih digitalnih uredb, kakršna sta Akt o digitalnih storitvah in Akt o umetni inteligenci. Namen članka je (1.) predstaviti in kritično ovrednotiti pravno regulacijo vedenjskih mehanizmov in praks digitalne manipulacije ter (2.) v slovenski raziskovalni prostor vnesti izrazje in razpravo o temnih vzorcih, ki doslej še nista bila sistematično obdelana.

2. Temni vzorci – poskus opredelitve

Izraz temni vzorci (angl. *dark patterns*)[11] je leta 2010 skoval britanski oblikovalec uporabniške izkušnje Harry Brignull, da bi z njim poimenoval in pod skupni pojem konsolidiral – številnim uporabnikom poznane, vendar do tedaj neimenovane – spletne prakse, katerih najmanjši skupni imenovalec je zavajanje posameznikov k dejanjem ali izbiram, ki jih sicer ne bi opravili.[12] Istega leta je vzpostavil spletno platformo darkpatterns.org, namenjeno sistematičnemu dokumentiranju in razkrivanju takšnih praks in tudi podjetij, ki jih uporabljajo.[13]

Vzpostavitev digitalnega arhiva spornih uporabniških vmesnikov je sprožila opazno rast zanimanja raziskovalcev za pojav temnih vzorcev. Raziskovanje tega pojava se je najprej razvilo v okviru študij interakcije človek–računalnik (angl. *human-computer interaction*), ki so analizirale njihovo zasnovo in vpliv na uporabniško vedenje.[14] Z razvojem digitalnih okolij pa so postali relevanten predmet proučevanja tudi v psihologiji, vedenjski ekonomiji, pravu in računalništvu, kar je spodbudilo interdisciplinarni raziskovalni okvir za razumevanje njihovih

---

[10] Colin in dr., str. 1–22. Dodati je treba, da se v literaturi občasno pojavljajo opozorila, da izraz »temni vzorci« lahko nehote krepi negativne asociacije ali stereotipe, zato nekateri avtorji (glej na primer spletišče Deceptive Design) zagovarjajo njegovo opustitev in raje uporabljajo »zavajajoče oblikovanje« ali sorodne nevtralnejše označbe. Vendar pa je v evropskem prostoru izraz »temni vzorci« v zadnjih letih dobil jasno pozitivnopravno oporo tudi v zakonodajnih aktih (najprej v Aktu o digitalnih storitvah – Uredba (EU) 2022/2065), zato ga v nadaljevanju besedila uporabljam tudi sama.

[11] Za poimenovanje istega pojava se uporabljajo tudi nekateri drugi izrazi, na primer zavajajoči vzorci (angl. *deceptive patterns*), zavajajoč dizajn (angl. *deceptive design*) in psihološki vzorci (angl. *psychological patterns*).

[12] Leiser, 2022, str. 240.

[13] Brignull, 2020.

[14] Mathur in dr., str. 1–18; Gray in dr., 2018.

mehanizmov in posledic.[15] Vzporedno z akademskimi raziskavami so interne študije o učinkovitosti zavajajočih spletnih praks pospešeno izvajala tehnološka in e-trgovinska podjetja, vendar njihovi rezultati večinoma niso bili objavljeni, saj so varovani kot poslovne skrivnosti, hkrati pa bi njihova razkritja lahko spodbudila javno neodobravanje ali sprožila regulativne ukrepe.[16]

V zadnjih letih so temni vzorci pritegnili tudi pozornost regulatorjev. Na pojav so se odzvali številni nadzorni in zakonodajni organi – od Zvezne komisije za trgovino (angl. *Federal Trade Commission*)[17] in britanskega Urada za konkurenco in trg (angl. *Competition and Markets Authority*) do Evropske komisije in Evropskega odbora za varstvo podatkov – ki so v svojih smernicah začeli obravnavati zavajajoče oblikovalske prakse kot obliko manipulacije.[18]

2.1. Opredelitev, pojavne oblike in taksonomije

Z rastjo zanimanja za temne vzorce se je v akademski literaturi hitro povečalo tudi število njihovih opredelitev.[19] Ker se koncept uporablja v različnih disciplinah, ne preseneča, da ni enotne definicije.[20] V tem besedilu izraz temni vzorci uporabljam za označevanje premišljeno oblikovanih elementov uporabniškega vmesnika in interakcijskih praks, ki s prisilo, napeljevanjem ali zavajanjem uporabnikov omogočajo pridobivanje treh temeljnih dobrin sodobne digitalne družbe: denarja, podatkov in pozornosti. Kot bo podrobneje pojasnjeno v naslednjem razdelku, temni vzorci delujejo tako, da izkoriščajo kognitivne pristranosti in psihološke ranljivosti uporabnikov ter jih s tem vodijo k odločitvam, ki niso v njihovem interesu.[21]

2.1.1. Zgodnje raziskave

Prvo obdobje znanstvene obravnave temnih vzorcev (okvirno med letoma 2010 in 2018) so zaznamovali poskusi njihovega poimenovanja in kategorizacije, ki so pozneje prerasli v obsežnejše empirične raziskave o njihovi razširjenosti in učinkih.

Še preden je Brignull s svojo platformo pripomogel k uveljavitvi izraza temni vzorci, so nekateri avtorji zavajajoče in manipulativne uporabniške vmesnike raziskovali pod drugimi imeni.

---

15 Glej na primer Luguri in Strahilevitz, str. 44–109; Bösch in dr., str. 237–254; Fritsch, str. 93–100; Leiser in Yang, str. 484–528.

16 Luguri in Strahilevitz, str. 46.

17 Federal Trade Commission, Bringing Dark Patterns to Light, 2022.

18 Evropska komisija, Behavioural study on unfair commercial practices in the digital environment, 2023.

19 Colin in dr., str. 1–22.

20 Luguri in Strahilevitz, str. 44.

21 Leiser in Caruana, str. 237–245; Luguri in Strahilevitz, str. 43–105.

Conti in Sobiesk sta denimo pod krovnim izrazom škodljive vmesniške tehnike oziroma škodljiv vmesniški dizajn (angl. *malicious interface techniques/design*) identificirala enajst skupin takšnih praks, ki sta jih razvrstila glede na učinke, ki jih povzročajo pri uporabnikih (na primer prisila, zmeda, izraba napak, prisilno delo in šok).[22]

Pod kategorijo »prisila« sta uvrstila prakse, ki od uporabnika zahtevajo, da vpiše vse svoje osebne podatke, preden lahko nadaljuje uporabo strani; »zmeda« zajema uporabo zavajajočih vprašanj in nepotrebnih informacij; »motenje« vključujejo odvračanje pozornosti z izkoriščanjem nezavednega zaznavanja; »izraba napak« se nanaša na primere, ko napačen URL vodi do oglasnega okna namesto do zahtevane vsebine; »prisilno delo« se denimo manifestira v obveznem ogledovanju oglasov ali oteženem preklicevanju naročnin; »manipulativno usmerjanje« uporabnika zavajajoče napeljuje k ciljem oblikovalca vmesnika; »zastiranje« pomeni prikrivanje pomembnih informacij ali vmesniških elementov; »omejevanje funkcionalnosti« zmanjšuje uporabnikove možnosti; »šok« uporabnika pretrese s svojo vsebino; »triki« pa vključujejo zavajanje z lažnimi vsebinami ali vmesniškimi elementi.[23]

Te kategorije že nakazujejo temeljne mehanizme vplivanja, ki jih je poznejša literatura prepoznala kot značilne za temne vzorce, zato lahko Contijev in Sobieskov prispevek razumemo kot pomemben konceptualni predhodnik poznejših taksonomij zavajajočih uporabniških vmesnikov.

Kmalu zatem je Harry Brignull s svojo spletno platformo darkpatterns.org prispeval k širši prepoznavnosti pojava in k uveljavitvi izraza temni vzorci. Identificiral je dvanajst osnovnih tipov temnih vzorcev,[24] ki kljub nadaljnjemu razvoju raziskav ostajajo izhodišče večine sodobnih sistematizacij.[25] Tukaj jo navajam v celoti – tudi zato, da predlagam slovenske ustreznice za posamezne izraze.

- Prikriti oglasi (angl. *disguised ads*): oglasi, ki so oblikovani tako, da posnemajo običajno vsebino spletnega mesta (na primer novičarske članke ali gumbe za prenos), kar uporabnike zmede in jih spodbudi h kliku na oglasno vsebino, ne da bi se tega zavedali.
- Prisilno nadaljevanje (angl. *forced continuity*): uporabnik se po izteku brezplačnega preskusnega obdobja samodejno znajde v plačljivi naročnini, ne da bi bil o tem jasno obveščen ali imel možnost preprosto preklicati storitev.
- Zloraba stikov (angl. *friend spam*): vmesnik uporabnika spodbuja ali zavede, da platformi omogoči dostop do svojih stikov, nato pa sistem samodejno pošilja vabila ali promocijska sporočila v njegovem imenu.

---

22 Conti in Sobiesk, str. 272–273.

23 Prav tam.

24 Glej na primer Conti in Sobiesk, 2010; Gray in dr., 2018; Mathur in dr., 2019.

25 Luguri in Strahilevitz, str. 44 in nasl.; Gray in dr., 2018, str. 1–14.

- Vaba in zamenjava (angl. *bait and switch*): uporabniku se predstavi obljuba o določeni funkciji, izdelku ali ugodnosti, vendar se po kliku ali izvedbi dejanja ponudi nekaj drugega, običajno manj ugodnega in/ ali plačljivega.
- Skriti stroški (angl. *hidden costs*): dodatni stroški, kot so stroški dostave, davki ali provizije, se razkrijejo šele v zadnjem koraku nakupa, potem ko je uporabnik že vložil čas in trud v izpolnjevanje naročila.
- Preusmeritev pozornosti (angl. *misdirection*): oblikovne tehnike, ki z vizualnimi poudarki ali oblikovanjem gumbov preusmerijo uporabnikovo pozornost z dejanskih možnosti, pogosto tako, da uporabnik nevede izbere možnost, ki je v korist podjetja.
- Onemogočanje primerjave cen (angl. *price comparison prevention*): zasnova strani uporabniku otežuje ali onemogoča neposredno primerjavo cen izdelkov ali storitev z drugimi ponudniki, s čimer se zmanjša preglednost in konkurenčnost trga.
- Prisilno deljenje osebnih podatkov (angl. *privacy zuckering*): gre za temni vzorec, poimenovan po ustanovitelju Facebooka, ki označuje oblikovne strategije, namenjene spodbujanju čezmernega razkrivanja osebnih podatkov. Tipični primeri vključujejo privzete nastavitve, ki favorizirajo deljenje, neintuitivne postopke za prilagoditev zasebnostnih nastavitev in zavajajoče vizualne elemente. Namen teh praks je povečati obseg podatkov, dostopnih platformi, zlasti za oglaševalske in druge komercialne namene.
- Nepričakovne težave pri odjavi (angl. *roach motel*): gre za temni vzorec, pri katerem se uporabnik izjemno preprosto vključi v nek sistem (z enim klikom za brezplačni preizkus; enostaven vstop v igro), nato pa sistem namerno oteži izstop - skrije gumb za odjavo, zahteva stik z uporabniško podporo ali vpelje dolgotrajen postopek odjave prek več (bolj ali manj zapletenih) korakov. Poimenovanje izhaja iz pasti za ščurke – »notri zlahka, ven nikoli« – in ponazarja namerno oblikovano asimetrijo med vstopom in izstopom iz storitve.
- Skrito dodajanje v košarico (angl. *sneak into basket*): izdelek ali storitev se samodejno doda v uporabnikovo nakupovalno košarico brez njegove izrecne privolitve – pogosto gre za dodatne, plačljive postavke ali razširitve osnovne storitve.
- Zavajajoča vprašanja (angl. *misleading questions*): vprašanja ali obrazci, ki so namerno zapleteni ali formulirani z dvojnimi negacijami, tako da uporabniki nehote izberejo možnost, ki je v korist ponudnika (na primer »Ali res ne želite prejeti naših obvestil?«).
- Sramotenje ob zavrnitvi (angl. *confirmshaming*): tehnika, ki pri uporabniku vzbuja občutek krivde ali sramu, ker je zavrnil ponudbo, naročilo ali prijavo. Pogosti so čustveno nabiti gumbi, kot na primer »*Ne, raje ostanem neobveščen*« ali »*Ne, ni mi mar za svoje zdravje*«.[26]

[26] Za več primerov glej na primer <https://paylode.com/articles/confirmshaming>.

2.1.2. Poznejše klasifikacije

Raziskave, ki so sledile Brignullovemu pionirskemu delu, so poskušale temne vzorce konceptualno poglobiti in jih sistematično klasificirati. Gray in soavtorji (2018) so jih glede na strategije in motivacije oblikovalcev razvrstili v pet kategorij:

- priganjanje (angl. *nagging*), ki se kaže kot vztrajno prigovarjanje uporabniku, naj stori nekaj, kar koristi oblikovalcu;
- oviranje (angl. *obstruction*), s katerim vmesnik uporabniku otežuje določeno dejanje (na primer odjavo od storitve ali primerjavo cen);
- prikrivanje (angl. *sneaking*), kjer gre za poskuse skrivanja ali zakrivanja informacij, ki bi lahko vplivale na uporabnikovo odločitev;
- motenje vmesnika (angl. *interface interference*), ki privilegira določene izbire v korist ponudnika; in
- prisilno dejanje (angl. *forced action*), ki od uporabnika zahteva izvedbo nekega koraka, da bi lahko dostopal do želene vsebine.[27]

Naslednji pomemben prispevek k razvoju koncepta predstavljata Leiser in Yang (2022), ki sta oblikovala štiristopenjsko taksonomijo temnih vzorcev glede na to, ali ti izrabljajo informacijsko asimetrijo ali omejujejo svobodo odločanja uporabnikov.

Med temne vzorce, ki izrabljajo informacijsko asimetrijo, spadajo uporabniški vmesniki, ki uporabnike zavajajo z nezanesljivimi informacijami (prikazovanje lažnih ocen in mnenj, lažno navajanje omejene razpoložljivosti) in zavajajočim dizajnom (zavajajoča vprašanja – »Ali se res ne želite ne odjaviti od prejemanja naših obvestil?«), ki vodi v instinktivno, neinformirano izbiro (na primer vizualno izpostavljeno strinjanje z obdelavo osebnih podatkov). Med temne vzorce, ki izrabljajo informacijsko asimetrijo, spadajo tudi temni vzorci, ki prikrivajo informacije – denimo onemogočajo primerjanje cen ali razkrivajo skrite stroške tik pred zaključkom nakupa.

Skupina temnih vzorcev, ki omejujejo svobodo odločanja uporabnikov, zajema prakse, ki to svobodo zmanjšujejo bodisi z vsiljevanjem določenih izbir bodisi z omejevanjem razpoložljivih možnosti. Pri temnih vzorcih, ki vsiljujejo določene izbire, gre za prakse, pri katerih vmesnik uporabnika potiska v določena dejanja, denimo samodejno dodajanje izdelkov v košarico (angl. *sneak into basket*), prisilna prodaja, ponavljajoča se pojavna okna (angl. *repeated pop-ups*), sramotenje zaradi nesoglašanja (*angl. confirmshaming*), zloraba zasebnosti (angl. *privacy Zuckering*), skrite prijave, prikrito oglaševanje ter tako imenovana vaba in zamenjava (angl. *bait and switch*), pri kateri mikavna ponudba uporabnika zvabi k določenemu nakupu, naknadno pa se mu predstavi drugačna ali manj ugodna možnost. V drugi skupini so vzorci,

---

[27] Gray in dr.Nepr 2018, str. 1–14.

ki uporabnika omejujejo na nevsiljiv, toda nezaželen način – z oteževanjem ali onemogočanjem določenih dejanj. Sem spadajo prisilna ravnanja, kot je pogojevanje dostopa do vsebine s plačilom, in tako imenovane nepričakovane težave pri odjavi (angl. *roach motel*), kjer je vstop v storitev preprost, njen preklic pa zapleten, dolgotrajen ali celo nemogoč.[28]

V enem od najaktualnejših prispevkov na tem področju sta Leiser in Santos razširila obstoječe razumevanje temnih vzorcev s konceptom »spektra vidnosti«, s katerim sta analizo zavajajočih praks z ravni uporabniškega vmesnika razširila na sistemsko arhitekturo digitalnih orodij. S tem sta opozorila, da se manipulativne prakse ne odvijajo le na površini interakcije, temveč so pogosto vgrajene globoko v algoritmične procese in arhitekturne oziroma oblikovalske odločitve, ki so uporabniku nevidne. Takšno razlikovanje med bolj in manj vidnimi plastmi manipulacije ima pomembne posledice tudi za oceno ustreznosti pravne regulacije, saj izziva tradicionalno razumevanje transparentnosti in odgovornosti oblikovalcev sistemov.[29]

Različne taksonomije temnih vzorcev – od Brignullove deskriptivne tipologije do Leiserjeve sistemske analize – razkrivajo razvoj od površinskih oblik zavajanja do kompleksnih arhitekturnih mehanizmov vplivanja. Skupna značilnost vseh je zavestno izkoriščanje kognitivnih pristranosti uporabnikov in delovanje proti njihovim interesom. Prav ta značilnost utemeljuje potrebo po njihovem normativnem vrednotenju in pravni regulaciji, ki bo tema naslednjih razdelkov.

3. Mehanizmi delovanja: temni vzorci in temna psihologija

Socialni psiholog Robert Cialdini svojo odmevno monografijo Vplivanje: Psihologija prepričevanja (1984) uvaja s primerom puranje matere, ki se ob pivkajočih mladičkih začne nagonsko vesti materinsko, molčeče piščančke pa prezre. Enako ljubezniva kot do oglašajočih se mladičev, je puranja mati tudi do vseh preostalih predmetov, ki spuščajo njim podoben zvok – ta je namreč tisti, ki v njej aktivira specifičen (materinsko-ljubeč) vzorec vedenja, pri tem pa je povsem nepomembno, ali zvok prihaja iz kljuna mladička ali iz vezja, vgrajenega v plišasto igračko.[30]

Vedenjska ekonomija je pokazala, da podobna samodejna vedenjska zaporedja in intuitivni odzivi obstajajo tudi pri ljudeh – le da ti običajno niso telesni, ampak kognitivni in psihološki. Naše vedenje in odločanje pogosto temeljita na hitrih in avtomatskih procesih,[31] ki nam omo-

---

[28] Leiser in Yang, str. 484–528.

[29] Leiser in Santos, str. 1–22.

[30] Cialdini, str. 20 in nasl.

[31] Teoretski okvir za razlago odločanja, sklepanja, presojanja, učenja in mišljenja, ki ga je prevzela vedenjska ekonomija, je tako imenovana teorija dvojnega procesiranja oziroma teorija dveh sistemov, ki (bolj ali manj

gočajo, da se v omejenem času in ob nepopolnih informacijah odzovemo učinkovito, čeprav ne vedno optimalno. Pri tem se zanašamo na kognitivne bližnjice (hevristike), preprosta miselna pravila, ki zmanjšujejo kognitivne napore, vendar nas hkrati izpostavljajo sistematičnim napakam oziroma kognitivnim pristranskostim.[32]

Vedenjska ekonomija teh pristranosti ni le sistematično preučila, ampak je ponudila tudi nekatere pristope za njihovo obvladovanje – kognitivne pristranosti so sicer vir neracionalnih (neoptimalnih) odločitev, vendar jih je ob ustrezni zasnovi odločevalskega okolja mogoče usmeriti v korist posameznika. Richard H. Thaler in Cass R. Sunstein sta znamenito ugotovitev Amosa Tverskega in Daniela Kahnemana, da preference ljudi niso stabilne, saj na to, katero alternativno možnost bomo izbrali, pomembno vpliva okvir, v katerem so predstavljene,[33] nadgradila z razvojem tehnike vedenjskega vplivanja, imenovane dregljaji (angl. *nudges*). Ti so bili predstavljeni kot nevsiljiv, svobodo ohranjajoč način spodbujanja boljših odločitev in so sprožili val zanimanja za vedenjskoekonomske pristope kot alternativo klasični regulaciji.[34]

Z množično digitalizacijo so se spoznanja vedenjske ekonomije začela uporabljati tudi pri zasnovi spletnih in aplikacijskih vmesnikov, ki so postali nova infrastruktura vsakdanjega odločanja. Ugotovitve o delovanju kognitivnih pristranosti so se izkazale za izjemno učinkovite – tako pri izboljševanju uporabniške izkušnje (na primer z usmerjanjem k izbiri varnejših gesel) kot tudi pri podaljševanju časa in pozornosti, ki ju uporabniki namenjajo digitalnim okoljem, ter pri subtilnem oblikovanju njihovih potrošniških in političnih izbir.

Dejstvo, da isti mehanizmi, s katerimi je mogoče spodbujati posameznikovo blaginjo, omogočajo tudi sistematično izkoriščanje njegovih kognitivnih ranljivosti za doseganje ciljev, ki niso v njegovem interesu, je eden najmočnejših ugovorov zoper dregljaje kot obliko regulacije vedenja.[35] In temni vzorci utelešajo prav to drugo obliko vedenjskega vplivanja. Oblikovalci digitalnih okolij se dobro zavedajo, da so uporabniki zaradi nestabilnih preferenc, omejene pozornosti in nagnjenosti k intuitivnemu odločanju dovzetni za različne pristranosti in hevri-

---

prepričljivo) opisuje nekakšno dvojno naravo človekove duševnosti (Evans in Frankish, 2009; Kahneman, 2016, str. 31–151). V skladu s to teorijo je mogoče razlikovati med dvema tipoma procesiranja, med »samodejnim, intuitivnim sistemom 1« in »nadzorovanim, prizadevnim ter razmišljujočim sistemom 2«. Zgoraj je bil opisan sistem 1, katerega jedro je asociacijski spomin, in ki deluje samodejno, intuitivno, hitro in brez nadzora ter tako ustvarja vtise, občutke, nagnjenja ter intuitivne, vendar običajno uporabne in zadostne odgovore na izzive vsakdanjega življenja. Nasprotno je sistem 2 bistveno počasnejši, vendar analitičen način razmišljanja, ki zahteva naš napor in zavedanje. Sistem 2 je, drugače kot sistem 1, ki je nenehno v pogonu, v »stanju pripravljenosti« ter se aktivira.

32 Cialdini, str. 23; Kahneman, str. 21 in nasl.

33 Tversky in Kahneman, 1981, str. 455–458.

34 Za pregled različnih intervencij vedenjskih enot po svetu glej OECD, 2017, za razvoj v Evropi pa poročilo Evropske komisije, 2016.

35 Schmidt in Engelen, 2020; Hausman in Welch, 2010; Grüne-Yanoff, 2012; Rebonato, 2012.

stike, ki jih je mogoče sprožiti in okrepiti s premišljenim oblikovanjem konteksta odločanja.[36] Pristranskost uokvirjanja (angl. *framing effect*), denimo, omogoča vplivanje na odločitve z načinom predstavitve informacij. Zato so izbire, ki koristijo korporacijam (na primer »strinjam se z obdelavo podatkov«), praviloma vizualno poudarjene, možnosti, ki varujejo interese (na primer zasebnost) uporabnika, pa so manj opazne. Evropski odbor za varstvo podatkov je v odločbi 2/2023[37] kot primer takšne prakse označil TikTokovo pojavno okno, ki je mladoletne uporabnike sistematično usmerjalo k javnim nastavitvam uporabniškega računa.

Pogost mehanizem je tudi ustvarjanje občutka pomanjkanja, ki izkorišča mehanizem, imenovan odpor do izgube (angl. *loss aversion*): z lažnimi odštevalniki časa, prikazovanjem omejenih zalog ali števila drugih kupcev se pri uporabniku sproži občutek nujnosti in strahu pred izgubo priložnosti. Drugi razširjeni mehanizem, ki ga izkoriščajo temni vzorci, so privzete izbire (angl. *defaults*), ki izrabljajo pristranskost *statusa quo* in pravilo najmanjšega napora, saj uporabniki praviloma ohranijo vnaprej določene nastavitve – tudi kadar te niso v njegovem interesu (na primer zato, ker vodijo v invazivno obdelavo osebnih podatkov). Značilen primer takega temnega vzorca je tako imenovani *privacy zuckering*, ki uporabnika zavajajoče spodbudi, da razkrije precej več osebnih podatkov, kot bi jih ob jasni in pošteni predstavitvi dejansko želel deliti. Oblikovalci digitalnih okolij svoje interese optimizirajo tudi z izrabljanjem hevristike sidranja (angl. *anchoring bias*), po kateri ljudje vrednotijo izbire glede na prvo predstavljeno možnost. V digitalnem okolju to pomeni, da se uporabniku kot začetna – in zato merodajna – prikaže možnost, ki najmanj varuje njegovo zasebnost ali finančni interes.

Vse naštete prakse povezuje izraba avtomatskih, intuitivnih, nezavednih odzivov in zmanjšanje verjetnosti zavestnega premisleka: s tem, ko digitalno okolje vztrajno spodbuja intuitivno odločanje, spodnaša sposobnost uporabnika za reflektirano presojo ter povečuje njegovo vedenjsko predvidljivost.

Vse to skrbi še toliko bolj, ker empirične študije kažejo, da so temni vzorci postali sistemski del digitalnega okolja: kar 97 odstotkov najbolj priljubljenih spletnih mest in aplikacij uporablja vsaj enega.[38] Njihova učinkovitost je visoka – občutno povečajo stopnjo »konverzije«, torej deleža uporabnikov, ki izvedejo določeno dejanje. Tako se lahko na primer s pomočjo temnih vzorcev delež uporabnikov, ki se prijavijo v storitev, poveča za dva- do štirikrat, delež privolitev v obdelavo podatkov pa za več kot 20 odstotnih točk.[39] Te prakse vse pogosteje in vse

---

[36] Deceived by Design, str. 6–7.

[37] Zavezujoča odločitev Evropskega odbora za varstvo podatkov je v celoti dostopna na povezavi: <https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en>.

[38] Evropska komisija, Behavioural Study on Unfair Commercial Practices in the Digital Environment, str. 29–61.

[39] Mathur in dr., str. 1–16.

bolj prefinjeno uporabljajo spletni trgovci, platforme družbenih omrežij, ponudniki videoiger in mobilne aplikacije, da bi spodbudili razkrivanje osebnih podatkov, povečali angažiranost uporabnikov ali spodbujali kompulzivno vedenje.[40]

4. Pravna regulacija

Empirično potrjeni učinki temnih vzorcev – njihova zmožnost vplivati na vedenje uporabnikov in jih usmerjati k odločitvam, ki jih sicer ne bi sprejeli – so se z razvojem umetne inteligence, avtomatiziranih sistemov odločanja in personaliziranega oglaševanja še okrepili. Tehnološki napredek je omogočil, da so prakse izkoriščanja vedenjskih pristranskosti postale subtilnejše, težje zaznavne in učinkovitejše.

Zato ne preseneča, da so se na njihove nevarnosti začeli resneje odzivati tudi regulatorji. Leta 2020 je Evropska komisija temne vzorce prepoznala kot poslovne prakse, ki ogrožajo pravico potrošnikov do svobodnega odločanja, izkoriščajo njihove kognitivne pristranskosti in izkrivljajo odločevalne procese.[41] Od tedaj dalje je Evropska unija pomembno okrepila prizadevanja za njihovo regulacijo.[42] Začetna prizadevanja so se osredotočila na identifikacijo obstoječih pravnih mehanizmov, s katerimi bi bilo mogoče omejiti ali sankcionirati tovrstne prakse. Izkazalo se je, da so temni vzorci v nasprotju z načeli varstva osebnih podatkov ter s pravili o poštenih poslovnih praksah, kakršne določa potrošniška zakonodaja.[43] Regulacija temnih vzorcev v EU se je tako začela z reinterpretacijo že veljavnih pravnih režimov, pozneje pa se je nadgradila z akti, ki vključujejo izrecne prepovedi manipulativnega oblikovanja digitalnih vmesnikov.

4.1. Pravo varstva zasebnosti

Splošna uredba o varstvu podatkov (v nadaljevanju: Splošna uredba)[44] temnih vzorcev ne regulira neposredno, prav tako neposredno ne prepoveduje (obdelave podatkov z namenom) manipulativnega izkoriščanja posameznikovih psiholoških ranljivosti. Kljub temu pa lahko številne oblike temnih vzorcev štejemo za nezdružljive z več temeljnimi načeli varstva osebnih

---

[40] Di Geronimo in dr., str. 4–14.

[41] Brenncke, str. 42–43.

[42] Podobno je tudi ameriška Zvezna komisija za trgovino prepoznala nevarnosti temnih vzorcev in okrepila prizadevanja za njihovo regulacijo. Glej: Federal Trade Commission, Staff Report, Bringing Dark Patterns to Light, 2022. Tudi Organizacija za gospodarsko sodelovanje in razvoj (OECD) je ugotovila, da utegnejo temni vzorci povzročiti bistveno škodo potrošnikom. Glej: OECD, Dark Commercial Patterns, Digital Economy, 2022.

[43] Brenncke, str. 44 in nasl.; Leiser, 2022, str. 240 in nasl.

[44] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. april 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, Uradni list EU L 119, 4. maj 2016.

podatkov, saj vodijo do obdelave osebnih podatkov, ki ni poštena, pregledna ali sorazmerna. To zlasti velja za tiste temne vzorce, katerih namen je z izkoriščanjem psiholoških mehanizmov uporabnikov doseči, da ti podajo soglasje za obdelavo osebnih podatkov.

Splošna uredba zahteva, da so osebni podatki obdelani zakonito, pošteno in pregledno, za določen, izrecen in zakonit namen ter v obsegu, ki je omejen na tisto, kar je nujno potrebno za dosego tega namena.[45] Poleg tega vključuje režim varstva podatkov po Splošni uredbi tudi načeli vgrajenega in privzetega varstva podatkov (angl. *privacy by design* in *privacy by default*), ki upravljavcem nalagata, da zagotovijo varstvo zasebnosti že na ravni zasnove informacijskih sistemov in privzetih nastavitev.[46]

4.1.1. Načelo preglednosti

Načelo preglednosti je eno temeljnih orodij za zagotavljanje nadzora posameznika nad lastnimi podatki. Temni vzorci, ki s prikrito zasnovo vmesnika uporabnika spodbudijo k podaji soglasja za obdelavo podatkov ali k razkritju podatkov, to načelo neposredno ogrožajo, saj si prizadevajo obvoziti posameznikovo racionalno dejavnost in na prikrit način pridobiti soglasje za obdelavo osebnih podatkov. Taki temni vzorci so manipulativni, saj uporabnika napeljujejo k soglašanju z obdelavo na način, da se uporabnik sploh ne zaveda, da se je strinjal s posegom v zasebnost, torej niti ne opravi vrednostnega premisleka o tem, kaj počne.

Kljub temu pa ima načelo preglednosti – kot opozarjata Leiser in Yang[47] – pomembne omejitve. Tudi »transparentno« oblikovani temni vzorci lahko ohranjajo neravnotežje moči med uporabnikom in ponudnikom storitve in s tem spodkopavajo avtonomijo posameznika. V takšnih okoliščinah zgolj preglednost torej ni zadostna varovalka.

4.1.2. Načelo poštenosti

Načelo poštenosti iz točke a prvega odstavka 5. člena je osrednjega pomena za presojo skladnosti temnih vzorcev s Splošno uredbo in je hkrati glavno načelo pravnega režima varstva osebnih podatkov. Poštenost zahteva, da obdelava podatkov poteka na način, ki za posameznika ni škodljiv, diskriminatoren, nepričakovan ali zavajajoč.[48] Temni vzorci so grožnja temu načelu, saj si do osebnih podatkov (oziroma soglasja za njihovo obdelavo) prizadevajo priti na način, ki je zavajajoč oziroma nepričakovan.

---

[45] Prvi odstavek 5. člena Splošne uredbe.

[46] Člen 25 Splošne uredbe.

[47] Leiser in Yang, str. 484–528.

[48] Evropski odbor za varstvo podatkov, Smernice št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov Različica 2.0, 2020, str. 6–12.

V skladu s takšnim razumevanjem vloge in pomena načela poštenosti je Evropski odbor za varstvo podatkov v svoji zavezujoči odločitvi (2/2023),[49] katere pravno presojo je pozneje v končno odločitev vključil Irski organ za varstvo podatkov, ugotovil, da je podjetje TikTok Technologies kršilo načelo poštenosti iz Splošne uredbe. Sporni sta bili dve oblikovalski praksi. Prva taka praksa so bila manipulativna pojavna obvestila, ki so negativno vplivala na varstvo zasebnosti otrok, starih med 13 in 17 let. Pojavno okno za registracijo je otroke spodbujalo k izbiri javnega računa, tako da je vizualno izpostavljen desni gumb z oznako »preskoči« povzročil kaskadni učinek na otrokovo zasebnost na platformi. V primeru druge sporne prakse je šlo za pojavno okno za objavo videoposnetkov, ki je otroke spodbujalo, naj med alternativnima možnostma, med katerima je desna, »objavi zdaj«, bila zapisana v krepkem, temnejšem besedilu, leva »prekliči« pa v neizstopajočem svetlem, izberejo desno.

Toda opozoriti je treba, da je »poštenost« vsebinsko zelo odprto načelo, saj vključuje razpršeno presojo pričakovanj uporabnikov, ravnotežja interesov in vpliva konteksta. Kljub tej odprtosti se prav načelo poštenosti kaže kot najprimernejši pravni temelj za oceno skladnosti temnih vzorcev s Splošno uredbo, saj omogoča presojo tako namenov kot tudi učinkov (zavajajočih) uporabniških vmesnikov.

4.1.3. Načeli vgrajenega in privzetega varstva podatkov

Temni vzorci so sporni tudi iz vidika načel vgrajene in privzete zasebnosti (angl. *privacy by design* in *privacy by default*), v skladu s katerima mora biti tehnologija zasnovana tako, da so osebni podatki uporabnikov varovani samodejno v vsakem informacijskem sistemu, kar pomeni, da posamezniku ni potrebno nič storiti, da bi zaščitil svojo zasebnost, saj je zaščita zasebnosti vgrajena v sistem ter hkrati njegova privzeta izbira. Načelo vgrajene zasebnosti od upravljavcev zahteva, da so sistemi, ki obdelujejo podatke, zasnovani tako, da vključujejo temeljna načela varstva podatkov, načelo privzete zasebnosti pa, da so privzete nastavitve digitalnih naprav vedno v korist maksimalne zaščite zasebnosti.[50] V literaturi je široka razprava o tem, kakšne obveznosti ima upravljavec podatkov v zvezi z načelom vgrajene zasebnosti[51] – vendar je neizpodbitno, da temni vzorci na splošno kršijo *ethos* tega načela (tako kot tudi *ethos* celotnega režima varstva zasebnosti).[52]

---

[49] Zavezujoča odločitev Evropskega odbora za varstvo podatkov je v celoti dostopna na povezavi: <https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en>.

[50] Leiser in Yang, str. 484–528.

[51] Koops in Leenes, str. 159 in nasl.

[52] Nekdanji nadzornik EU za varstvo podatkov Giovanni Buttarelli je temne vzorce označil za ključno gonilo procesa preobrazbe posameznikov iz uporabnikov in prejemnikov storitev v služabnike podatkovne industrije.

Zdi se, da razširitev načela vgrajene zasebnosti na preprečevanje vključevanja temnih vzorcev v zasnovo sistema ne pomeni ustvarjalnega preseganja zakonodajnega namena niti ne zahteva obsežne vnovične razlage pravnega reda o varstvu podatkov. V uvodni izjavi Splošne uredbe 78 je navedeno, da »bi moral upravljavec sprejeti notranje politike in izvajati ukrepe, ki izpolnjujejo zlasti načeli vgrajenega varstva podatkov in privzetega varstva podatkov«.

4.1.4. Omejitve

Ključna omejitev prava varstva osebnih podatkov kot regulacijskega okvira pri obravnavi temnih vzorcev je, da zajema le ožji segment tovrstnih praks – nanaša se samo na tiste temne vzorce, ki ciljajo na posege v zasebnost, specifično v pridobivanje pravne podlage za obdelavo osebnih podatkov – kar pa je samo ena od vrst temnih vzorcev.

Nasprotno pa številne druge oblike manipulativnega oblikovanja – denimo prisiljevanje k nakupu, naročnini ali nadaljevanju storitve – ne vključujejo obdelave osebnih podatkov in zato presegajo področje uporabe Splošne uredbe. Pravo varstva osebnih podatkov torej samo po sebi ne zagotavlja celovitega odgovora na problem temnih vzorcev, temveč mora delovati v sinergiji z drugimi regulativnimi režimi, ki obravnavajo informacijsko, potrošniško in tehnološko asimetrijo sodobnih digitalnih okolij.

4.2. Pravo varstva potrošnikov

Večina akademskih analiz o regulaciji temnih vzorcev je sprva opozarjala na to, da gre za prakse, ki pomenijo kršitve varstva osebnih podatkov, in da je zato Splošna uredba o varstvu podatkov najprimernejša pravna podlaga za njihovo regulacijo.[53] Vendar pa, kot je pokazala raziskava Mathura in sodelavcev, temni vzorci ne ogrožajo zgolj zasebnosti in varstva osebnih podatkov uporabnikov, ampak se zelo pogosto uporabljajo kot poslovne strategije, namenjene vplivanju na potrošnike, da opravijo določeno transakcijo. Leiser in Caruana sta pokazala, ne le, da meja med varstvom osebnih podatkov in varstvom potrošnikov ni zelo ostra, saj ima posameznik pogosto sočasno vlogo nosilca osebnih podatkov in potrošnika, hkrati pa oba režima sledita istemu cilju, tj. varovanju avtonomije posameznika, ampak tudi, da spadajo številne oblike manipulativnega oblikovanja uporabniških vmesnikov v materialno področje evropske potrošniške zakonodaje, zlasti v okvir Direktive o nepoštenih poslovnih praksah,[54]

---

[53] Bösch in dr., 237–254; Fritsch in dr., str. 93–104.

[54] Direktiva Evropskega parlamenta in Sveta 2005/29/ES z dne 11. maja 2005 o nepoštenih poslovnih praksah podjetij v razmerju do potrošnikov na notranjem trgu ter o spremembi Direktive Sveta 84/450/EGS, direktiv Evropskega parlamenta in Sveta 97/7/ES, 98/27/ES in 2002/65/ES ter Uredbe (ES) št. 2006/2004 Evropskega parlamenta in Svet, Uradni list EU L 149, 11. junij 2005.

pa tudi Direktive o pravicah potrošnikov[55] in Direktive o nepoštenih pogodbenih pogojih.[56] Te določajo splošno prepoved nepoštenih, zavajajočih ali agresivnih praks in so dovolj pomensko odprte, da zajamejo tudi sodobne digitalne oblike vplivanja. Potrošniško pravo ima poleg tega tudi večji potencial za regulacijo temnih vzorcev, saj v primerjavi s Splošno uredbo vsebuje konkreten standard poštenosti[57] in poleg tega mogoča boljše mehanizme uveljavljanja pravic kot pravo varstva osebnih podatkov.

Krovni akt Evropske unije na področju varstva potrošnikov – Direktiva o nepoštenih poslovnih praksah – temnih vzorcev sicer ne ureja izrecno in tudi ne vsebuje prepovedi praks, ki izkoriščajo kognitivne pristranskosti potrošnikov. Vendar pa je Evropska komisija v svojih razlagalnih smernicah in poročilih pojasnila, da je mogoče na podlagi pomensko odprtih in na načela opirajočih se določb prepovedati temne vzorce v okviru prepovedi zavajajočih[58] in agresivnih[59] poslovnih praks.[60]

Zavajajoče poslovne prakse vključujejo ravnanja, ki potrošnika preslepijo, mu prikrivajo (popačijo) bistvene informacije (denimo o ceni, obsegu storitve, pogojih naročnine) ali izkrivljajo način predstavitve in s tem uporabnika potiskajo k neželenim odločitvam. Mednje je mogoče uvrstiti temne vzorce, ki otežujejo primerjavo cen, prikrivajo dodatne stroške ali ustvarjajo lažen vtis o (bodisi časovni bodisi količinski) omejenosti neke ponudbe. Agresivne poslovne prakse pa se nanašajo na primere, kjer trgovec uporablja prisilo, nadlegovanje ali neupravičen vpliv in s tem pomembno omejuje potrošnikovo svobodno odločanje. V to kategorijo je mogoče uvrstiti temne vzorce, ki uporabniku otežujejo odpoved naročnine, izhod iz digitalnega okolja ali izbris računa.

Večina raziskovalcev podpira razlagalno širitev področja uporabe direktive na temne vzorce,[61] kakor je v razlagalnih smernicah predlaga Evropska komisija, saj omogoča prilagodljivo uporabo že veljavnega potrošniškega prava za odzivanje na nove (digitalne) prakse. Vendar nekateri avtorji opozarjajo na konceptualno napetost med izhodišči direktive in naravo temnih

---

55 Amandma Direktive o pravicah potrošnikov v novem 16. e členu prevzema ureditev iz 25. člena Akta o digitalnih storitvah (glej naslednji podrazdelek).

56 Direktiva Sveta 93/13/EGS z dne 5. aprila 1993 o nedovoljenih pogojih v potrošniških pogodbah, Uradni list EU L 95, 21. april 1993.

57 Direktiva o nepoštenih pogodbenih pogojih, denimo, določa, da je pogodbeni pogoj nepošten, če je v nasprotju z načelom dobre vere in povzroči znatno neravnovesje med pravicami in obveznostnim pogodbenih strank v škodo potrošnika.

58 Direktiva o nepoštenih poslovnih praksah, 6. in 7. člen.

59 Direktiva o nepoštenih poslovnih praksah, 8. člen.

60 Glej: Evropska komisija, »Commission Notice: Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market«, 2021 (razdelka 4.2.7 in 4.2.9).

61 Leiser in Caruana, str. 237–251; Brenncke, str. 44 in nasl.

vzorcev. Trdijo, da se Direktiva o nepoštenih poslovnih praksah opira na standard »povprečnega potrošnika«, ki je preudaren, informiran in racionalen subjekt.[62] Tak potrošnik po definiciji ni dovzeten za kognitivne pristranskosti, na katerih temeljijo temni vzorci. Zato naj direktiva, ki temelji na predpostavki racionalnosti, ne bi bila ustrezno orodje za regulacijo praks, ki prav to predpostavko izpodbijajo.[63]

Razhajanja glede razlage pojma »povprečnega potrošnika« so eden ključnih razlogov, zaradi katerih je Direktiva o nepoštenih poslovnih praksah omejeno učinkovita pri zajezitvi temnih vzorcev. Ta sicer – drugače od Splošne uredbe – zagotavlja *ex ante* zaščito uporabnikov digitalnih storitev, torej že pred sklenitvijo pogodbe, varstvo zasebnosti pa praviloma nastopi šele ob obdelavi osebnih podatkov.[64] Vendar dokler se standard povprečnega potrošnika ne bo reinterpretiral v luči spoznanj vedenjskih znanosti (in opustil predpostavko o povsem racionalnem posamezniku), bo obseg zaščite pred praksami, ki izkoriščajo kognitivne pristranskosti, ostal omejen. Prizadevanja za učinkovito regulacijo temnih vzorcev na področju zaščite potrošnikov se poleg tega spopadajo z izzivom, da številni zavajajoči uporabniški vmesniki pogosto delujejo v sivi coni med zakonitimi tehnikami prepričevanja in očitno nezakonitimi metodami vplivanja na vedenje potrošnikov, kakršni sta prisila in zavajanje.[65]

4.3. Regulacija platform

Omejena učinkovitost Direktive o nepoštenih poslovnih praksah kot tudi režima varstva zasebnosti – ki se, kot je bilo ugotovljeno, nanaša samo na temne vzorce, katerih namen je pridobivanje osebnih podatkov, in ne zagotavlja *ex ante* zaščite – je eden ključnih razlogov, da se je Evropska unija odločila za neposredno regulacijo temnih vzorcev v okviru novonastajajoče pravne panoge, ki zadeva regulacijo spletnih platform (angl. *platform governance*). Prvi zakonodajni akt, ki v evropskem pravnem redu neposredno definira temne vzorce, je Akt o digitalnih storitvah.[66] V uvodni izjavi 67 temne vzorce opredeli kot »prakse spletnih vmesnikov, ki namerno ali dejansko bistveno izkrivljajo ali zmanjšujejo zmožnost prejemnikov storitve, da sprejemajo samostojne in ozaveščene izbire ali odločitve«.[67]

Akt o digitalnih storitvah v 25. členu od ponudnikov spletnih platform zahteva, da ti »ne zasnujejo, organizirajo ali upravljajo svojih spletnih vmesnikov na način, ki zavaja ali mani-

---

[62] Poncibò in Incardona, str. 30–31.

[63] Prav tam, str. 21–38.

[64] Brenncke, str. 44; Leiser in Caruana, str. 240 in nasl.

[65] Brenncke, str. 42.

[66] Uredba (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. oktobra 2022 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES.

[67] Uvodna izjava 67.

pulira prejemnike njihove storitve ali kako drugače bistveno izkrivlja ali zmanjšuje zmožnost prejemnikov njihovih storitev, da sprejemajo svobodne in informirane odločitve«. V skladu z uvodno izjavo 39 določba ščiti vse prejemnike storitev – tako potrošnike kot tudi poslovne uporabnike.

Drugače kot Direktiva o nepoštenih poslovnih praksah Akt o digitalnih storitvah izrecno priznava obstoj vedenjskih pristranskosti in širi varstvo tudi na »neracionalne« uporabnike, saj izhaja iz empiričnega spoznanja, da način predstavitve informacij ter struktura uporabniškega vmesnika pomembno vplivata na posameznikovo vedenje.[68] Uvodna izjava 67 tako utemeljuje definicijo temnih vzorcev na premisi, da lahko izbirna arhitektura neposredno vpliva na kognitivne procese uporabnika in s tem spodkopava njegovo avtonomijo.

Ureditev iz Akta o digitalnih storitvah je mogoče razumeti kot manifestacijo premika poudarka z varstva ustrezne informiranosti potrošnika na varstvo procesov odločanja. Vlogo osrednje dobrine, ki jo mora regulacija digitalnih platform varovati, prevzema avtonomija. Vendar pa kljub temu ostajajo odprta vprašanja glede razmejitve med dopustnim vplivanjem (na primer tržno prepričevanje) in nedopustno manipulacijo, kar kaže na potrebo po nadaljnjem konceptualnem razvoju tega področja.

4.4. Akt o umetni inteligenci

Zadnji člen v tej regulativni verigi je Uredba o določitvi harmoniziranih pravil o umetni inteligenci (v nadaljevanju: Akt o umetni inteligenci).[69] Uredba razvršča sisteme umetne inteligence glede na stopnjo tveganja, ki ga pomenijo za temeljne pravice in varnost posameznikov, pri čemer posebej obravnava sisteme, katerih uporaba pomeni nesprejemljivo tveganje. Mednje uvršča tudi tiste, ki uporabljajo

> »subliminalne tehnike, ki presegajo zavest osebe, ali namerno manipulativne ali zavajajoče tehnike, s ciljem ali učinkom bistvenega izkrivljanja vedenja osebe ali skupine oseb, tako da se znatno zmanjša njihova sposobnost, da sprejmejo informirano odločitev, zaradi česar sprejmejo odločitev, ki je sicer ne bi sprejeli, na način, ki tej osebi, drugi osebi ali skupini oseb povzroči znatno škodo ali za katerega obstaja razumna verjetnost, da bo povzročil znatno škodo«.[70]

---

[68] Brenncke, str. 48.

[69] Uredba (EU) 2024/1689 Evropskega parlamenta in sveta z dne 13. 6. 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828, Uradni list EU L, 2024/1689, 12. julij 2024.

[70] Prvi odstavek 5. člena Akta o umetni inteligenci.

Čeprav je namen določbe jasen – preprečiti izkoriščanje kognitivnih in čustvenih ranljivosti uporabnikov –, pa uporaba izrazov, kot so »subliminalne tehnike«, »onkraj zavesti« in »bistveno izkrivljanje vedenja«, odpira številne razlagalne možnosti in s tem tudi potencialne težave. Poleg tega je učinek določbe vezan na nastanek znatne (telesne ali psihične) škode, kar izključuje številne oblike bolj subtilnih, kumulativnih škod, ki jih (lahko) povzročajo temni vzorci – denimo erozijo pozornosti, postopno zmanjševanje zavedanja nad lastnimi izbirami ali utrjevanje vedenjskih odvisnosti.[71] Takšno pogojevanje lahko močno zmanjša preventivni doseg uredbe.[72]

Kljub tem omejitvam pa je Akt o umetni inteligenci pomemben premik v pravnem priznavanju manipulacije kot specifičnega tveganja, povezanega z avtomatiziranimi sistemi. Uredba tako simbolno povezuje digitalno regulacijo z vprašanjem, ki je skupno vsem obravnavanim režimom – tj. z vprašanjem avtonomije posameznika. S tem dopolnjuje prizadevanja drugih aktov, ki prav tako izhajajo iz predpostavke, da digitalna arhitektura odločanja ni zgolj tehnično, temveč tudi normativno in etično vprašanje.

5. Sklep

Vedenjska ekonomija se je začela razvijati kot projekt boljšega razumevanja, če že ne izboljševanja človekovega odločanja. Vendar so se njena spoznanja v digitalni sferi pretežno preobrazila (tudi) v orodje vplivanja in nadzora. Najizrazitejša manifestacija te preobrazbe so temni vzorci, ki so benevolentno tehniko »dreganja« nadgradili v industrijo subtilnega in pretkanega, toda dobičkonosnega usmerjanja vedenja, ki ogroža avtonomijo, svobodo izbire in zaupanje v digitalna okolja, hkrati pa ustvarja različne oblike škode – od posegov v zasebnost in ogrožanja ekonomskega interesa uporabnikov do odvisnosti in kognitivne apatije.

Temni vzorci, ki se najočitneje manifestirajo na ravni uporabniške izkušnje – v zasnovi gumbov, vmesnikov ali zaporedij odločitev – so le vrh kompleksne infrastrukture manipulacije, v kateri se prepletajo vedenjske znanosti in podatkovna analitika. Sodobni digitalni ekosistemi tako delujejo kot večnivojske, prekrivajoče se – intersekcijske manipulativne pojavnosti, kjer oblikovalske odločitve praviloma niso nevtralne, temveč instrumentalizirane v korist ekonomskih in političnih ciljev. Sodobne digitalne prakse tako postavljajo na preizkušnjo temeljno pravico do samoodločanja. Ključen izziv sodobnega prava je razviti učinkovite mehanizme njenega varstva v digitalnem prostoru.

Evropska unija se na te prakse odziva vse bolj odločno. Od reinterpretacije obstoječih mehanizmov v okviru varstva zasebnosti in potrošnikov do izrecnih prepovedi v Aktu o digitalnih

---

71 O tovrstni škodi glej na primer Carr.

72 Leiser, 2024, str. 26–20.

storitvah in Aktu o umetni inteligenci se vzpostavlja koherenten, večstopenjski sistem varstva uporabnikov. V središču teh prizadevanj se postopno oblikuje nov normativni ideal – varstvo avtonomije v digitalnem odločanju. Premik od zaščite informacij k zaščiti procesov odločanja je ena ključnih evolucij sodobnega prava digitalnih tehnologij.

Kljub temu pa ostajajo odprta nekatera pomembna vprašanja: pravni odziv še vedno zaostaja za hitrostjo tehnološkega razvoja, kar ustvarja vrzel med normativnimi načeli in realnostjo algoritmičnega oblikovanja. Tako je meja med dopustnim vplivanjem in nedopustno manipulacijo pogosto nejasna, kar zahteva natančnejše konceptualno razlikovanje med prepričevanjem, napeljevanjem in prisilo. In nazadnje, številne oblike manipulacije so danes skrite v globljih, nevidnih plasteh digitalnih sistemov – v podatkovnih arhitekturah, algoritmih in personalizacijskih modelih – zato zahteva učinkovita regulacija premik pozornosti od vidnih (uporabniških vmesnikov) k sistemskim, vgrajenim oblikam manipulacije.[73] Še posebej pomembno je prepoznati, da številne oblike digitalnega vplivanja posegajo v samo jedro duševne integritete posameznika. Razprave o tako imenovani *kognitivni zasebnosti* so se doslej večinoma osredotočale na nevrotehnologije, vendar Stefano Faraoni utemeljeno širi ta okvir tudi na področje prepričevalnih tehnologij.[74] Faraoni opozarja, da manipulativne oblike tako imenovane računske manipulacije (angl. *computational manipulation*) ogrožajo človekovo notranjo avtonomijo in zato upravičujejo razmislek o novi človekovi pravici – pravici do kognitivne zasebnosti.

Čeprav pravo še ne ponuja popolnega odgovora, postaja jasno, da mora prihodnja regulacija digitalnih okolij preseči meje upravnega in civilnega prava ter – v posebej hudih primerih – vključiti tudi kazenskopravno odzivanje. Najinvazivnejše oblike digitalne manipulacije, ki povzročajo hude psihološke, ekonomske ali družbene posledice, bi lahko zahtevale obravnavo tudi skozi prizmo kazenskopravnega varstva človekove avtonomije.[75]

Vse jasneje se namreč kaže, da prihodnja regulacija digitalnih okolij ne more temeljiti le na ekonomskih in tehničnih merilih, temveč mora izhajati iz normativnega priznanja človeka kot avtonomnega, ranljivega in manipulabilnega bitja. Prav v tem prepoznavanju človeške ranljivosti kot temeljnega izhodišča digitalne regulacije se skriva možnost, da se temni vzorci – paradoksalno – osvetlijo: kot priložnost za vnovično utemeljitev etike in prava v dobi avtomatiziranega vplivanja.

---

73 Leiser in Santos, str. 1–22.

74 Faraoni, 2023.

75 Glej na primer Ziermann.

Literatura

ARIELY, Dan. *Predvidljivo nerazumni*. Ljubljana: Mladinska knjiga, 2010.

BÖSCH, Christoph, ERB, Benjamin, KARGL, Frank, KOPP, Henning, in PFATTEICHER, Stefan. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. Proceedings on Privacy Enhancing Technology, 2016, letn. 4, str. 237–254.

CARR, Nicholas. *Plitvine: kako internet spreminja naš način razmišljanja, branja in pomnjenja.* Ljubljana: Cankarjeva založba, 2011.

CIALDINI, B. Robert. *Vplivanje: psihologija prepričevanja*. Ljubljana: Umco, 2015.

DAMASIO, Antonio. *Iskanje Spinoze: veselje, žalost in čuteči možgani*. Ljubljana: Založba Krtina, 2009.

DI GERONIMO, Linda, BRAZ, Larissa, FREGNAN, Enrico, in dr. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. *CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, str. 1–14.

EVROPSKA KOMISIJA, Behavioural study on unfair commercial practices in the digital environment, 2023.

EVROPSKA KOMISIJA, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to--consumer commercial practices in the internal market, 2021.

EVROPSKA KOMISIJA, Behavioural Insights Applied to Policy: European Report 2016. Luxembourg: Publications Office of the European Union, 2016.

EVROPSKI ODBOR ZA VARSTVO PODATKOV, Smernice št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov. Različica 2.0, 2020, <https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_sl.pdf> (15. 10. 2025).

FARAONI, Stefano. Persuasive Technology and Computational Manipulation: Hypernudging Out of Mental Self-Determination. *Frontiers in Artificial Intelligence*, 2023, letn. 6, str. 1–14.

FEDERAL TRADE COMMISSION, Bringing Dark Patterns to Light, 2022.

FRITSCH, Lothar. Privacy dark patterns in identity management. Open Identity Summit, 2017, str. 93–104.

GRAY, Colin, KOU, Yubo, BATTLES, Bryan, in dr. The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, članek št. 534, str. 1–14.

GRAY, Colin, SANTOS, T. Cristiana, BIELOVA, Nataliia, in dr. An Ontology of Dark Patterns: Foundations, Definitions, and a Structure for Transdisciplinary Action. *CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024, članek št. 289, str. 1–22.

KAHNEMAN, Daniel. *Razmišljanje: hitro in počasno*. Ljubljana: UMco, 2017.

KOOPS, Bert-Jaap, LEENES, Ronald E. Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law (March 15, 2014). *International Review of Law, Computers & Technology*, 2014, letn. 28, št. 2, str. 159–171.

LEISER, Mark, CARUANA, Mirelle. Light to Be Found in Europe's Consumer Protection Regime. *Journal of European Consumer and Market Law*, 2021, letn. 10, št. 6, str. 237–251.

LEISER, Mark. Dark Patterns: The Case for Regulatory Pluralism. V: Kosta, E., Leenes, R., Kamara, I. (ur.), *Research Handbook on EU Data Protection Law*. Taylor and Francis, 2022, str. 240–269.

LEISER, Mark, YANG, Wen-Ting. Illuminating Manipulative Design: From 'Dark Patterns' to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive. *Consumer Law Review*, 2022, letn. 34, št. 3, str. 484–528.

LEISER, Mark, SANTOS, Cristiana. Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface. BILETA Special Issue, 2024, letn. 15, št. 1.

LEISER, Mark. Psychological Patterns and Article 5 of the AI Act. *Journal of AI Law and Regulation*, 2024, letn. 1, št. 1, str. 5–23.

LUGURI, Jamie, STRAHILEVITZ, Lior Jacob. Shining a Light on Dark Patterns. *Journal of Legal Analysis, 2021,* letn. 13, št. 1, str. 43–109.

MATHUR, Arunesh, MAYER, Jonathan, KSHIRSAGAR, Mihir. What Makes a Dark Pattern ... Dark? Design Attributes, Normative Considerations, and Measurement Methods. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, str. 1–18.

OECD (2017): Behavioural Insights and Public Policy: Lessons from Around the World, 2017, <https://doi.org/10.1787/9789264270480-en> (15. 10. 2025).

OECD, Dark Commercial Patterns, No. 336, 2022, <https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf> (15. 10. 2025).

PONCIBÒ, Cristina, INCARDONA, Rossella. The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution. Journal of Consumer Policy Issue, 2007, letn. 30, št. 1, str. 21–38.

STRLE, Toma, MARKIČ, Olga. *O odločanju in osebni avtonomiji.* Maribor: Aristej, 2021.

SUNSTEIN, R. Cass, THALER, H. Richard. *Dregljaj: Izboljšanje odločitev o zdravju, blaginji in sreči: Dokončna izdaja*. Ljubljana: Umco, 2022.

TVERSKY, Amos, KAHNEMAN, Daniel. Judgement under uncertainty: Heuristics and Bias. *Science*, 1974, letn. 185, št. 4157, str. 1124–1131.

TVERSKY, Amos, KAHNEMAN, Daniel. The Framing of Decisions and the Psychology of Choice. *Science*, 1981, letn. 211, št. 4481, str. 453–458.

ZIERMANN, Fabian. Dark patterns: Can criminal law remedy the shortcomings of antitrust law? *New Journal of European Criminal Law*, 2024, letn. 15, št. 4, str. 388–411.