PRAVO V INFORMACIJSKI DRUŽBI

GV Založba

GV
Založba

Recenzenta:

prof. dr. Vesna Rijavec,
Pravna fakulteta Univerze v Mariboru

prof. dr. Gorazd Trpin,
Pravna fakulteta Univerze v Ljubljani

CIP – Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

34:659.2:004

PRAVO v informacijski družbi / M. Ahtik ... [et al.] ; urednik M. Damjan. – 1. natis. – Ljubljana : IUS Software, GV Založba, 2014

ISBN 978-961-247-278-8
1. Ahtik, Meta 2. Damjan, Matija
273409280

PRAVO V INFORMACIJSKI DRUŽBI

M. Ahtik, M. Bogataj Jančič, M. Brkan, B. Bugarič,
M. Damjan, A. Galič, A. Grah Whatmough,
P. Grilc, M. Juhart, B. Koritnik, J. Kramberger Škerl,
J. Levovnik, B. Markelj, L. Markelj, Š. Mežnar,
N. Muhič, N. Pogorelčnik, J. Pusser, L. Ude,
K. Zajc, S. Zgaga

Urednik: M. Damjan

IUS SOFTWARE®

GV Založba

Ljubljana 2014

AVTORJI

Bojan Bugarič
univerzitetni diplomirani pravnik, doktor pravnih znanosti, izredni profesor na Pravni fakulteti Univerze v Ljubljani

Matija Damjan
univerzitetni diplomirani pravnik, doktor pravnih znanosti, raziskovalec na Inštitutu za primerjalno pravo pri Pravni fakulteti Univerze v Ljubljani

Špelca Mežnar
univerzitetna diplomirana pravnica, doktorica pravnih znanosti, docentka na Mednarodni fakulteti za družbene in poslovne študije v Celju, odvetnica pri Odvetniški družbi Čeferin, o. p., d. o. o.

Peter Grilc
univerzitetni diplomirani pravnik, doktor pravnih znanosti, redni profesor na Pravni fakulteti Univerze v Ljubljani, dekan Pravne fakultete Univerze v Ljubljani

Maja Brkan
univerzitetna diplomirana pravnica, doktorica pravnih znanosti, docentka na Pravni fakulteti Univerze v Maastrichtu

Maja Bogataj Jančič
univerzitetna diplomirana pravnica, doktorica pravnih znanosti, LLM (Harvard), LLM (Torino), direktorica in raziskovalka na Inštitutu za intelektualno lastnino

Jernej Pusser
univerzitetni diplomirani pravnik, LLM (Dunaj), raziskovalec na Inštitutu za intelektualno lastnino

Miha Juhart
univerzitetni diplomirani pravnik, doktor pravnih znanosti, redni profesor na Pravni fakulteti Univerze v Ljubljani

Jure Levovnik
univerzitetni diplomirani pravnik, magister pravnih znanosti, partner v Odvetniški pisarni Jadek&Pensa, d. n. o. – o. p.

Aleš Galič
univerzitetni diplomirani pravnik, doktor pravnih znanosti, izredni profesor na Pravni fakulteti Univerze v Ljubljani

Jerca Kramberger Škerl
univerzitetna diplomirana pravnica, doktorica pravnih znanosti, docentka na Pravni fakulteti Univerze v Ljubljani

Neža Pogorelčnik
univerzitetna diplomirana pravnica, mlada raziskovalka na Pravni fakulteti Univerze v Ljubljani

Katarina Zajc
univerzitetna diplomirana pravnica, doktorica ekonomskih znanosti (George Mason), LLM (Yale), izredna profesorica na Pravni fakulteti Univerze v Ljubljani

Neža Muhič
univerzitetna diplomirana pravnica, sodniška pripravnica na Višjem sodišču v Ljubljani

Luka Markelj
univerzitetni diplomirani pravnik, odvetniški kandidat pri odvetniku Antonu Preglju v Ljubljani

Meta Ahtik
univerzitetna diplomirana pravnica, doktorica ekonomskih znanosti, docentka na Pravni fakulteti Univerze v Ljubljani, ekonomistka pri Evropski centralni banki

Sabina Zgaga
univerzitetna diplomirana pravnica, doktorica pravnih znanosti, docentka za kazensko pravo na Fakulteti za varnostne vede Univerze v Mariboru

Blaž Markelj
univerzitetni diplomirani organizator-informatik, predavatelj za informacijsko varnost na Fakulteti za varnostne vede Univerze v Mariboru

Lojze Ude
univerzitetni diplomirani pravnik, doktor pravnih znanosti, zaslužni profesor na Pravni fakulteti Univerze v Ljubljani, direktor Inštituta za primerjalno pravo pri Pravni fakulteti v Ljubljani

Andrej Grah Whatmough
univerzitetni diplomirani pravnik, specialist davčnega prava, študent znanstvenega magistrskega študija podjetništva na Ekonomski fakulteti Univerze v Ljubljani, direktor podjetij Londinium, d.o.o., in Grah in partnerji, d. o. o.

Boštjan Koritnik
univerzitetni diplomirani pravnik, študent znanstvenega magistrskega študija gospodarskega prava na Pravni fakulteti Univerze v Mariboru, direktor in odgovorni urednik IUS Software, d.o.o., Ljubljana, strokovni urednik revije Pravnik

KAZALO

Uvod

Položaj prava v informacijski družbi

dr. Bojan Bugarič

Na prelomu dvajsetega in enaindvajsetega stoletja se je uporaba informacijskih tehnologij uveljavila na vseh področjih življenja. Računalniki so omogočili digitalni zapis in hitro obdelavo najrazličnejših podatkov, internet in mobilna telefonija pa njihov takojšnji prenos in izmenjavo na velike razdalje. Skoraj vsaka kompleksnejša naprava že vsebuje mikroprocesor in se lahko povezuje z internetom, vsaj za posodobitev programske opreme. Ta temeljni tehnološki preboj je vplival na fizično proizvodnjo in poslovne storitve, osebno in poslovno komunikacijo, medije, trgovino, glasbeno in filmsko industrijo. Spremenil je vse od načina, kako shranjujemo zasebne fotografije, do tega, kako dostopamo do storitev javne uprave. Govorimo lahko o nastanku informacijske družbe, tj. družbe, v kateri je informacijska tehnologija pomembna za gospodarstvo, kulturo in zasebno življenje ter v kateri so ustvarjanje, posredovanje in upravljanje informacij vse pomembnejša kulturna in gospodarska dejavnost.

Preprostejše komuniciranje na daljavo, takojšnja dostopnost najrazličnejših informacij in interaktivni vmesniki uporabniških storitev so odpravili nekatere tehnološke ovire, ki so stoletja narekovale značilnosti družbenih razmerij, ki jih ureja pravo. Internet je na primer zrelativiziral vsa teritorialna pravila o določitvi pristojnosti ali veljavnega prava ter zabrisal mejo med komunikacijami in mediji. Novim okoliščinam porajajoče se informacijske družbe se mora zato prilagoditi tudi pravna ureditev. Prva faza prilagajanja prava novemu informacijskemu okolju je obsegala predvsem reševanje problemov in paradoksov, ki so se pojavili ob soočenju starih pravnih norm z novimi tehnološkimi okoliščinami. Prevladujoči normativni pristop je zajemal uporabo vsebinske analogije in širitev obstoječih pravnih konceptov na nove tehnologije. Elektronska oblika dokumentov in komunikacij v pravnem prometu je bila tako pod določenimi pogoji izenačena s tradicionalno pisno obliko, elektronski podpis s klasičnim podpisom, elektronska reprodukcija avtorskega dela z njegovo mehansko reprodukcijo, pravila o klasičnih knjižnih registrih so se prilagodila elektronskim registrom, klasična pravila o teritorialni pristojnosti se smiselno uporabljajo tudi pri regulaciji interneta, izdajatelj elektronskega medija je za njegovo vsebino odgovoren enako kot izdajatelj klasičnega medija ipd.

Proces prilagajanja prava novim okoliščinam informacijske družbe pa ni končan. Doslej sprejete pravne rešitve so pogosto izhajale iz (delno) napačnih predpostavk o nadaljnjem tehnološkem in ekonomskem razvoju ter o načinih poslovanja, ki naj bi se na tej podlagi razvili. Urejanje po analogiji s tradicionalnimi rešitvami tako ni več primerno, kadar je zaradi novih tehnologij odpadel *ratio* stare ureditve. Pogosto je bilo na primer prezrto, da je bistvena značilnost novega tehnološkega okolja težnja po prostem in nenadzorovanem pretoku vseh dobrin, ki jih je mogoče zapisati v obliki digitalne informacije. Internet omogoča neposreden stik vsakega z vsakim, brez posrednikov, zato informacijsko družbo zaznamuje proces disintermediacije. Tradicionalni modeli centraliziranega ustvarjanja in distribucije znanja niso več samoumevni, saj jih lahko uspešno nadomeščajo nove skupne oblike ustvarjanja in izmenjave dosežkov. To dokazujejo uspešni projekti odprtokodnega programja in prenosa podatkov s protokoli P2P, na katere pravo očitno ni bilo pripravljeno, a so iz ozkega kroga entuziastov prešli v pomembno poslovno rabo. Pravno varstvo tehnoloških ukrepov za zaščito avtorskih del pa je primer zgrešene zakonodajne rešitve, ki je namesto prilagajanja tehnološkim spremembam (neuspešno) skušala zgolj zaščititi tradicionalne poslovne modele centralizirane distribucije.

Možnosti uporabe informacijskih tehnologij v pravu še niso v celoti izkoriščene. Elektronske komunikacije lahko poenostavijo uporabo številnih uradnih postopkov v javni upravi in pravosodju ter strankam olajšajo izvedbo opravil na daljavo. Internet lahko omogoči širši in preprostejši dostop do elektronskih registrov pravic in pravnih dejstev ter do različnih uradnih in programskih gradiv, ki nastajajo v javnem sektorju, ter tako poveča preglednost delovanja državnih organov. Pri tem pa ne gre zanemariti, da razširjena uporaba informacijskih tehnologij poleg priložnosti prinaša tudi nova tveganja. Internetna dostopnost javnih podatkovnih baz na primer povečuje možnost zlonamernih vdorov vanje in zlorabe zbranih osebnih podatkov. Pretirano zanašanje na uporabo informacijskih tehnologij v uradnih postopkih, na primer tako, da je nekatere vloge mogoče podati samo v elektronski obliki, pa lahko vzpostavlja nesmiselne ovire za tiste, ki teh tehnologij ne obvladujejo ali jim ne zaupajo. Uvajanje elektronskih postopkov v nobenem primeru ne bi smelo biti samo sebi namen, ampak mora prinesti jasne prednosti, hkrati pa je treba vnaprej predvideti in ustrezno urediti potencialne slabosti. Nekatere težave niti niso strogo tehnološke ali pravne narave, ampak gre predvsem za problem zaupanja, ki pa ga tudi ne gre zanemariti. To je zlasti razvidno pri elektronskih ali internetnih volitvah, kjer so tehnične možnosti za zlorabe in prilagajanje rezultata sicer bolj omejene kot pri klasičnih postopkih, vendar jih lahko zaznajo samo računalniški strokovnjaki, medtem ko bi klasične volilne liste načeloma lahko vsak državljan ročno preštel in preveril pravilnost objavljenega volilnega izida. Za demokratično legitimnost elektronskih ali inter-

netnih volitev je zato treba najprej doseči ustrezno stopnjo zaupanja javnosti v tovrstne postopke.

V informacijski družbi pa se pojavljajo tudi povsem nova pravna vprašanja, ki so značilnost novega tehnološkega okolja in so pravno samo delno urejena ali prepuščena samoregulaciji ponudnikov storitev informacijske družbe. Najprej sem spada pravna ureditev interneta in elektronskih komunikacij kot informacijske infrastrukture, pravice do internetnih domen, vprašanja določanja internetnih standardov in izkoriščanja patentov na protokolih in tehnologijah, ki so del teh standardov. Nadalje gre za pravna vprašanja v zvezi z novimi pojavi in storitvami, ki pred nastankom interneta niso obstajali, kot so na primer spletno iskanje, računalništvo v oblaku in ponujanje programov kot storitev, družbena omrežja, spletni forumi, virtualne valute, hekerski napadi zaprtih sistemov in napadi porazdeljene omejitve storitve (DDoS). Pomembno vprašanje so tudi pravice uporabnikov internetnih storitev v razmerju do ponudnikov internetnega dostopa na eni strani in do države na drugi strani. Zaradi naraščajočega vpliva informacijske tehnologije na življenje vsakega posameznika pravna regulacija tega področja vse bolj zadeva tudi vprašanja človekovih pravic in demokratične ureditve celotne družbe.

Da bi učinkovito izkoristili vse priložnosti, ki jih ponuja informacijska doba, je potrebno nenehno preverjanje ustreznosti obstoječe pravne ureditve. Vendar za njeno prilagajanje novim tehnološkim okoliščinam niso vedno potrebne zakonodajne spremembe, saj se ustrezne rešitve pogosto razvijejo že v pravni praksi. Zaradi tega je tem bolj pomembno, da pravna teorija nova vprašanja pravočasno zazna in skuša ponuditi odgovore nanje s širšega sistemskega stališča, ki se vsakdanji pravni praksi včasih izmika. Pravniki smo sicer že zaradi narave poklica nekoliko konservativni in se obravnavanju novih vprašanj, ki jih ne razumemo povsem, raje izognemo. Pogost je predsodek, da gre pri pravnih vprašanjih informacijske družbe predvsem za regulacijo uporabe novih tehnologij, zlasti za pravo elektronskih komunikacij. Vendar, kot je bilo v obrisih prikazano, to nikakor ne izčrpa pravnih problemov informacijske družbe, saj uporaba informacijskih tehnologij načenja vedno nova vprašanja tudi na povsem klasičnih pravnih področjih. Ta monografija prinaša pregled in poglobljeno obravnavo nekaterih izbranih pravnih problemov informacijske družbe, ki so bili doslej v slovenski pravni teoriji pomanjkljivo obravnavani. Jasno pa je, da smo s tem predvsem odstrli pogled na široko polje pravnih izzivov, ki jih še zastavlja sodobna informacijska družba.

I.
Zasebnopravna vprašanja interneta

Odškodninska odgovornost internetnih posrednikov*

dr. Matija Damjan

1. Protipravne vsebine

Internet je svetovno omrežje omrežij, zasnovano za prenos najrazličnejših oblik informacij. Pri njegovem delovanju igrajo ključno tehnično vlogo ponudniki internetnih storitev in drugi internetni posredniki, ki informacije hranijo in prenašajo.[1] Na spletnih mestih dostopne vsebine pa lahko na več načinov kršijo pravne norme, kar vodi k civilnopravni ali celo kazenski odgovornosti. Internetna ravnanja, ki bi lahko dala podlago za odškodninske zahtevke, so na primer:

- objava besedila, slik, glasbe ali videoposnetkov, ki določeno osebo žalijo, obrekujejo ali neupravičeno posegajo v njeno zasebnost;
- omogočanje dostopa do nezakonitih kopij avtorskih del (glasba, filmi) ali varovanih podatkovnih baz (na primer imeniki);
- prodaja ponaredkov blaga priznanih blagovnih znamk;
- zavajajoče oglaševanje;
- objava podatkov, ki pomenijo poslovno skrivnost podjetja;
- razširjanje računalniških virusov in črvov, ki povzročajo škodo v informacijskih sistemih oziroma kradejo občutljive podatke.

Tovrstne vsebine z internetno objavo takoj postanejo javno dostopne in s tem povzročajo premoženjsko ali nepremoženjsko škodo osebam, v katerih izključne pravice oziroma osebnostno sfero se neupravičeno posega. Če niso uporabljene posebne tehnične omejitve, je do vsebin, ki kršijo pravne norme, mogoče dostopati kjerkoli na svetu, kar pomeni, da lahko kjerkoli nastane tudi škoda.[2] Do kakšne odškodnine ali nadomestila je oškodovanec upravičen, je poleg splošnih pravil odškodninskega prava odvisno od specialnih pravil posameznega področja

* Prispevek je bil prvič objavljen v: Pravni letopis 2010, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani.

[1] O tehnični zasnovi sodobnega interneta glej Murray, str. 23–26.

[2] Murray, str. 47–48.

(na primer 168. člen ZASP[3] v nekaterih primerih dopušča civilno kazen v obliki dvakratnega povečanja običajnega honorarja).

Pri posredovanju podatkov na internetu je vedno udeleženih več akterjev v različnih vlogah. Vsaj eden med njimi je navadno ponudnik internetnih storitev, tj. organizacija, ki svojim strankam omogoča dostop do interneta,[4] in zato pomeni arhetip internetnega posrednika. Poleg teh se danes pojavlja vse več drugih oblik internetnih posrednikov, kot so upravljavci internetnih portalov, ponudniki iskalnih storitev, forumov, spletnih klepetalnic in blogov itd. Ti posredniki imajo zaradi svoje vmesne vloge delen nadzor nad vsebino, ki jo pri prenosu podatkov posredujejo uporabniki. Problematična vsebina lahko izvira neposredno od ponudnika internetnih storitev; od stranke, ki je s ponudnikom internetnih storitev v pogodbenem razmerju (na primer naročnik); ali pa od tretje osebe brez pogodbene zveze s ponudnikom internetnih storitev. Ključno vprašanje, na katero se omejuje ta prispevek, je, kdaj in v kolikšni meri naj odgovornost za škodo nosijo internetni posredniki in v kolikšni meri naj odgovornost zanjo ostane pri prvotnih avtorjih oziroma ponudnikih vsebin. S tem je povezano vprašanje, s kakšnim ravnanjem se internetni posrednik lahko odgovornosti izogne. Zgodovinsko gledano je bil to eden prvih pravnih problemov interneta, s katerim so se soočila sodišča,[5] vendar zaradi spreminjajoče se narave internetnih storitev problematika še vedno poraja nova vprašanja.[6]

2. Razlogi (za in) proti odgovornosti ponudnika internetnih storitev

Ponudniki internetnih storitev so se kmalu zavedeli, da se kot »vratarji« internetnih objav izpostavljajo tveganju odgovornosti za objavljeno vsebino, zato so lobirali za zakonodajno zagotovitev imunitete pred odgovornostjo za vsebino. Kot glavni razlog za izključitev odgovornosti so navajali dejstvo, da bi bilo tehnično nemogoče sproti pregledovati zakonitost vseh informacij, ki se pretakajo skozi njihove strežnike, oziroma bi bilo to izvedljivo samo z velikimi stroški in zamudami, ki bi ohromile delovanje interneta. Poleg tega bi internetna podjetja s preverjanjem vsebin uporabnikov grobo posegala v zasebne podatke oziroma

[3] Zakon o avtorski in sorodnih pravicah (ZASP), Uradni list RS, št. 21/1995, 9/2001, 30/2001, 85/2001 – Skl. US: U-I-149/98-36, 43/2004, 58/2004 – Odl. US: U-I-200/02-12, 94/2004 – UPB1, 17/2006, 44/2006 – UPB2, 139/2006, 16/2007 – UPB3, 68/2008.

[4] Pogosto je ponudnik internetnih storitev označen kar s kratico ISP, ki izvira iz angleškega izraza *internet service provider*. Primerjaj Tičar, Makarovič, str. 260.

[5] Glej primer *Cubby v. CompuServe 766 F Supp 135 (SDNY 1991)*, o katerem je newyorško sodišče odločalo leta 1991.

[6] Edwards, str. 47–48.

v poslovne skrivnosti svojih strank, zato takšna cenzura vsebin tudi pravno ne bi bila dopustna.

Neprimerno bi bilo prevaliti odgovornost za sporno vsebino na subjekte, ki delujejo zgolj kot posredniki pri prenosu podatkov, saj bi tako kaznovali sla namesto pošiljatelja. Ponudniki storitev prenosa podatkov ali gostovanja spletnih strani drugih subjektov nimajo znanja o vsebinah, ki jih ti objavljajo in zanje ne morejo odgovarjati. Zato jih ne bi smeli obravnavati kot izdajatelje, temveč le kot prenašalce podatkov, enako kot ponudnike poštnih ali telefonskih storitev. Če bi internetnim posrednikom naložili še odgovornost za vsebino, bi jih izpostavili prevelikemu poslovnemu tveganju, kar bi zmanjšalo vlaganja v informacijsko infrastrukturo in s tem zavrlo razvoj elektronskega trgovanja in informacijske družbe na splošno. Tak rezultat pa ne bi bil v javnem interesu.

Ti argumenti so nekje do leta 2000 prepričali zakonodajalce v Evropi in v ZDA, da je smiselno ponudnike internetnih storitev izvzeti iz splošne odgovornosti za protipravne internetne vsebine. Hkrati pa so državne oblasti želele »očistiti« internet najočitneje protipravnih vsebin, zlasti tistih, ki so se redno znašle v središču političnih razprav, na primer otroška pornografija, spodbujanje nestrpnosti, piratska glasba in filmi itd. Zgolj preganjanje (največkrat anonimnih) individualnih uporabnikov zaradi decentralizirane in čezmejne narave interneta v ta namen ne zadostuje. Kolikor toliko učinkovit nadzor nad internetnimi vsebinami je mogoče zagotoviti samo s sodelovanjem internetnih posrednikov.[7] Zakonodajalec mora torej iskati ravnotežje med učinkovitostjo in pravičnostjo nadzora.[8] Zato je bil v zakonodaji ob prelomu stoletja izoblikovan kompromis, po katerem internetni posredniki načeloma ne odgovarjajo za vsebine tretjih strank, pod pogojem, da so pripravljeni na zahtevo odstraniti ali blokirati dostop do gradiva, za katero je bilo ugotovljeno, da je nezakonito ali da krši pravice, ali pa preprečiti dostop do njega.[9]

3. Ureditev po Direktivi o elektronskem poslovanju in ZEPT

Medtem ko sta bila v ZDA iz zgodovinskih in političnih razlogov vzpostavljena ločena režima odgovornosti ponudnikov internetnih storitev glede kršitev pravic intelektualne lastnine in glede drugih vrst civilne in kazenske odgovornosti,[10]

[7] Primerjaj 22. uvodno izjavo Direktive o elektronskem poslovanju: *»Nadzor nad storitvami informacijske družbe mora potekati pri viru dejavnosti, zato da se zagotovi učinkovita zaščita ciljev javnega interesa.«*

[8] Harper, str. 30–33.

[9] Edwards, str. 59–61.

[10] Prvega ureja *Digital Millenium Copyright Act (DMCA), Title 512*, drugega *Communications Decency Act (CDA), section 230(C).*

je v Evropski uniji Direktiva 2000/31/ES o elektronskem poslovanju[11] vzpostavila enoten režim odgovornosti za vse vrste vsebin na internetu.[12] Pravila te direktive o odgovornosti internetnih posrednikov je v slovenski pravni red najprej prenesla novela Zakona o elektronskem poslovanju in elektronskem podpisu (ZEPEP),[13] ki je v zakon vstavila nove člene 13.a do 13.d. Leta 2006 so bile te določbe prenesene v drugo poglavje Zakona o elektronskem poslovanju na trgu (ZEPT).[14]

3.1. Storitve informacijske družbe

Direktiva v členih 12 do 15 uvaja poenoten režim odgovornosti spletnih posrednikov. Naslov 4. oddelka II. poglavja direktive govori o odgovornosti *posrednih ponudnikov storitev*; v naslovu 8. člena slovenskega ZEPT je v enakem pomenu uporabljen izraz *ponudniki posredovalnih storitev*. V vsakem primeru ta režim ne velja samo za ponudnike internetnih storitev v ožjem smislu (torej podjetja, ki uporabnikom zagotavljajo dostop do interneta), temveč za vse *ponudnike storitev informacijske družbe*.

Izraz *storitve informacijske družbe* je opredeljen v drugem odstavku 1. člena Direktive 98/34/ES,[15] definicijo pa prevzema 11. točka 3. člena ZEPT, ki določa, da je storitev informacijske družbe storitev, ki se po navadi zagotavlja za plačilo, na daljavo, z elektronskimi sredstvi in na posamezno zahtevo prejemnika storitev. Pri tem »na daljavo« pomeni, da se storitev zagotavlja, ne da bi bili strani navzoči sočasno. »Z elektronskimi sredstvi« pomeni, da se storitev na začetku pošlje in v namembnem kraju sprejme z elektronsko opremo za obdelavo, vključno z digitalnim stiskanjem, in za shranjevanje podatkov ter v celoti pošlje, prenese in sprejme po žici, radiu, optičnih ali drugih elektromagnetnih sredstvih. »Na posamezno zahtevo prejemnika storitev« pa pomeni, da se storitev zagotavlja s prenosom podatkov na posamezno zahtevo. Storitve informacijske družbe vključujejo zlasti prodajo blaga ali storitev, dostop do podatkov ali oglaševanje na svetovnem spletu ter dostop do komunikacijskega omrežja, prenos podatkov ali shranjevanje prejemnikovih podatkov v komunikacijskem omrežju.

---

[11] Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu, UL L 178, 17. 7. 2000, str. 1–16.

[12] Edwards, str. 50; Tičar, Makarovič, str. 261; Murray, str. 155–160.

[13] Uradni list RS, št. 57/2000, 30/2001, 25/2004, 73/2004 – ZN-C, 98/2004 – UPB1, 61/2006 – ZEPT.

[14] Uradni list RS, št. 61/2006, 45/2008 – ZArbit, 79/2009.

[15] Direktiva 98/34/ES Evropskega parlamenta in Sveta z dne 22. junija 1998 o določitvi postopka za zbiranje informacij na področju tehničnih standardov in tehničnih predpisov, spremenjena z Direktivo 98/48/ES Evropskega parlamenta in Sveta z dne 20. julija 1998 in Direktivo Sveta 2006/96/ES z dne 20. novembra 2006.

Zakon torej ne ureja samo odgovornosti tradicionalnih ponudnikov internetnih storitev (ISP), temveč precej širšega razpona akterjev, udeleženih pri ponujanju blaga ali storitev na internetu (na primer spletne trgovine), pri ponujanju spletnih informacijskih ali iskalnih orodij (na primer Google), pa tudi čistih telekomunikacijskih podjetij, ki ponujajo le storitev dostopa do interneta prek kabelskih ali brezžičnih omrežij. Iz 18. uvodne izjave Direktive o elektronskem poslovanju je razvidno, da določbe o odgovornosti ponudnikov pridejo v poštev tudi v primeru, ko je storitev za prejemnika brezplačna, vendar je del gospodarske dejavnosti ponudnika. Ker je režim odgovornosti iz direktive zasnovan z namenom, da ponudniku storitev koristi, ne da ga obremeni, je pojem ponudnika storitev informacijske družbe primerno razlagati široko.[16] Pač pa direktiva iz tega pojma izrecno izključuje nekatere dejavnosti, na primer dobavljanje blaga ali opravljanje storitev izven spleta, radijsko in televizijsko oddajanje, revizijske preglede, zdravniške nasvete in preglede itd.[17]

3.2. Splošna pravila odgovornosti

Člen 8 ZEPT določa splošna pravila o odgovornosti ponudnikov posredovalnih storitev. Za podatke, ki jih ponudnik storitev za opravljanje storitve informacijske družbe *zagotovi sam*, sam tudi odgovarja po splošnih pravilih obligacijskega in kazenskega prava. Pri tem gre na primer za vsebino spletnega portala ponudnika internetnih storitev, ki jo ponudnik sam ureja (na primer www.siol.net). Bolj zanimivo pa je vprašanje odgovornosti ponudnika storitev za podatke, ki jih *zagotovi prejemnik njegove storitve*. Zakon za te podatke ponudniku

[16] Edwards, str. 63; Tičar, Makarovič, str. 256–258.

[17] Direktiva o elektronskem poslovanju v 18. uvodni izjavi pojasnjuje: »*Storitve informacijske družbe zajemajo široko področje gospodarskih dejavnosti, ki potekajo po internetu; gre predvsem za internetno prodajo blaga; dejavnosti, na primer lokalno dobavljanje blaga ali opravljanje storitev izven spleta, niso zajete; storitve informacijske družbe se ne omejujejo le na sklepanje pogodb v stalnem internetnem poslovanju, temveč se, če gre za gospodarsko dejavnost, razširjajo na storitve, ki jih ne plačajo prejemniki, na primer v zvezi s stalnim dostopom do internetnih podatkov ali komercialnimi sporočili, ali na storitve, ki zagotavljajo mehanizme za iskanje, dostop do in pridobivanje podatkov; storitve informacijske družbe vključujejo tudi prenos podatkov po komunikacijskem omrežju, dostop do komunikacijskega omrežja ali shranjevanje podatkov, ki jih zagotovi prejemnik storitve; televizijsko oddajanje, ki ga ureja Direktiva 89/552/EGS, in radijsko oddajanje se ne štejejo za storitve informacijske družbe, ker se ne zagotavljajo na zahtevo posameznika; nasprotno sodijo k njim storitve, ki se prenašajo samo med dvema točkama, na primer video na zahtevo ali nudenje komercialnih sporočil po elektronski pošti; uporaba elektronske pošte ali podobnih sporočil fizičnih oseb, ki delujejo zunaj svojih trgovskih, poslovnih in poklicnih dejavnosti, vključno z uporabo za sklepanje pogodb med temi osebami, se ne šteje za storitev informacijske družbe; pogodbeno razmerje med delojemalcem in njegovim delodajalcem ni storitev informacijske družbe; dejavnosti, ki se zaradi svoje narave ne morejo opravljati na daljavo in z uporabo elektronskih sredstev, na primer obvezni revizijski pregled računovodstva družb ali zdravniški nasvet z obveznim zdravniškim pregledom pacienta, niso storitve informacijske družbe.*«

ne podeljuje blanketne imunitete, temveč ločeno obravnava tri temeljne dejavnosti ponudnikov storitev informacijske družbe, ki se nanašajo na vsebine tretjih oseb:

- izključni prenos podatkov,
- shranjevanje v predpomnilniku,
- gostiteljstvo.

Kot temeljno načelo velja, da ponudnik storitev pri teh dejavnostih ni dolžan nadzirati ali hraniti podatkov, ki jih pošilja ali hrani, ali dejavno raziskovati okoliščin, nakazujočih na protipravnost podatkov, ki jih zagotavlja prejemnik storitve (15. člen direktive in tretji odstavek 8. člena ZEPT). Načelo izključitve splošne obveznosti nadzora vsebine je izjemno pomembno, saj učinkuje kot oblastna omejitev ter pravica in hkrati dolžnost ponudnika storitev. Ponudnik torej niti ni dolžan nadzirati vsebine niti je sam ne sme nadzirati (zaradi varstva zasebnosti uporabnikov). Splošno načelo pa ne izključuje nadzorne obveznosti v posebnih primerih na podlagi odredb pristojnih organov v skladu s področno zakonodajo. Zakon lahko določi, da mora ponudnik storitev na zahtevo pristojnega organa razkriti podatke, na podlagi katerih je mogoče identificirati prejemnika njegove storitve. Na podlagi ZEPT pa lahko sodišče ali upravni organ ponudniku storitve naloži ustavitev ali preprečitev kršitve ali mu naloži, da odstrani ali onemogoči dostop do podatkov.[18]

3.3. Izključni prenos

Kadar ponudnik storitev zagotavlja samo prenos podatkov v komunikacijskem omrežju ali zgolj zagotavlja dostop do komunikacijskega omrežja prejemniku storitve, ponudnik storitev v skladu z 9. členom ZEPT ni odgovoren za poslane podatke, če:

- ne sproži prenosa podatkov,
- ne izbere naslovnika in
- podatkov, ki jih prenaša, ne izbere ali spremeni.

Prenos in zagotovitev dostopa vključujeta samodejno, vmesno in prehodno shranjevanje poslanih podatkov, če je namenjeno samo izvajanju prenosa v komunikacijskem omrežju zaradi izboljšanja učinkovitosti prenosa in če se podatki ne shranijo za daljši čas, kolikor je za njihov prenos upravičeno potrebno. V takšnem položaju je torej ponudnik internetnih storitev skoraj v celoti odvezan odgovornosti za vsebino, ki jo zagotovijo tretji, saj je njegova storitev povsem tehnične narave, samodejna in pasivna, torej ponudnik storitve informacijske družbe niti ne pozna niti ne more nadzorovati podatkov, ki se prenašajo ali shranjujejo.[19]

[18] Tičar, Makarovič, str. 263–264.

[19] 42. uvodna izjava Direktive o elektronskem poslovanju.

3.4. Shranjevanje v predpomnilniku

Predpomnjenje (angl. *caching*) je povsod prisoten tehnični postopek na internetu, pri katerem se podatki, za katere je verjetno, da bodo ponovno uporabljeni, samodejno, vmesno in prehodno shranjujejo zaradi učinkovitejšega posredovanja podatka drugim prejemnikom storitve na njihovo zahtevo in s tem pospešitve spleta za vse uporabnike. Položaj je nekoliko drugačen kot pri čistem prenosu, saj je ponudnikov nadzor nad prejemnikovim podatkom, ki ga začasno hrani, bistveno večji, kot če ga zgolj prenaša. Zaradi pomena predpomnjenja za delovanje interneta je bistveno, da se ta postopek pravno ne otežuje. Zanj zato 10. člen ZEPT določa enaka pravila kot za izključni prenos, a z nekaj dodatki, ki so namenjeni preprečevanju manipulacij z začasno shranjenimi podatki tretjih.[20] Ponudnik storitev ni odgovoren za vsebino predpomnjenih podatkov, pod pogoji, da:

- podatkov ne spremeni,
- ravna v skladu s pogoji za dostop do podatkov,
- podatke sproti dopolnjuje in posodablja v skladu s splošno priznanimi in uporabljenimi industrijskimi standardi,
- ne posega v zakonito uporabo tehnologij za pridobivanje informacij o rabi podatkov v skladu s splošno priznanimi in uporabljenimi industrijskimi standardi in
- brez odlašanja odstrani ali onemogoči dostop do podatka, ki ga hrani, takoj ko je obveščen, da je bil vir podatka odstranjen iz omrežja ali da je bil dostop do njega onemogočen ali da je sodišče ali upravni organ odredil njegovo odstranitev ali omejitev.

Pod temi pogoji predpomnjenje ostaja vsebinsko nevtralen tehnični postopek, pri katerem ponudnik storitve ne vpliva na vsebino, čeprav jo vmesno in prehodno shranjuje na svojih strežnikih.

3.5. Gostiteljstvo

Medtem ko je omejitev odgovornosti ponudnikov storitev pri dejavnostih izključnega prenosa in predpomnjenja podatkov razmeroma nesporna in se v zvezi s temi dejavnostmi tudi v praksi spori praviloma ne pojavljajo, pa je mnogo bolj kontroverzno vprašanje odgovornosti ponudnika storitev spletnega gostiteljstva (angl. *hosting*). Gre za trajnejše shranjevanje podatkov, ki jih zagotovi prejemnik storitve, in praviloma tudi omogočanje dostopa do teh podatkov tretjim osebam. Gostiteljstvo navadno temelji na pogodbi med ponudnikom in prejemnikom storitve, s katero prejemnik najame diskovni prostor v gostiteljevem

[20] Tičar, Makarovič, str. 267–268.

strežniku. Sem spada na primer gostovanje spletnih strani, spletnih forumov in blogov na strežnikih komercialnih ponudnikov. Shranjene podatke lahko upravljata tako prejemnik storitve (gost) kot ponudnik storitve (gostitelj), pri čemer pa se gostitelj praviloma omejuje na administracijo strežniške infrastrukture in ne posega v vsebino. Vseeno je vsaj potencialni vpliv ponudnika storitve na prejemnikove podatke večji kot pri prenosu ali predpomnjenju, zato mora biti tudi njegova odgovornost določena strožje. Po 14. členu Direktive o elektronskem poslovanju ponudniki storitev ne morejo biti kazensko odgovorni ob odsotnosti dejanskega védenja o ilegalni dejavnosti ali vsebini; imuni pred civilno odgovornostjo pa so, če poleg tega tudi ne poznajo dejstev in okoliščin, iz katerih je ilegalnost očitna.[21]

Člen 11 ZEPT v skladu z direktivo določa, da ponudnik storitev ni odgovoren za podatke, shranjene na zahtevo prejemnika storitve, ki ne deluje v okviru njegovih pooblastil ali pod njegovim nadzorom, pod pogojem, da ponudnik storitev:

- ne ve za protipravno dejavnost ali podatek in mu v zvezi z odškodninsko odgovornostjo niso znana dejstva ali okoliščine, iz katerih izhaja protipravnost, ali
- nemudoma, ko mu je protipravnost znana, ukrepa tako, da podatke odstrani ali onemogoči dostop do njih.

Zakon torej ureja t. i. sistem *notice and take down* (sistem prijave in odstranitve), po katerem ponudnik storitev ni dolžan sam iskati protipravnih vsebin, temveč mora ukrepati, če mu je protipravnost znana ali ko ga imetnik pravic oziroma oškodovanec obvesti o kršitvi.

Seveda lahko ponudniku storitve naloži ustavitev ali preprečitev kršitve tudi sodišče. Zakon posebej določa, da lahko sodišče odredi odstranitev nezakonitih vsebin ali onemogočanje dostopa do njih zaradi odkrivanja in preprečevanja kaznivih dejanj, varstva zasebnosti, varovanja tajnih podatkov in poslovne tajnosti. Takšen predlog lahko sodišču v javnem interesu posredujejo tudi za nadzor pristojni upravni organi, skladno s področno zakonodajo.

Nekoliko manj pa je jasno, kdaj vse se lahko šteje, da je ponudniku storitev protipravnost znana, ne da bi ga o njej posebej obvestila imetnik pravic ali sodišče, in torej nastopi njegova dolžnost ukrepanja. Direktiva ne našteva okoliščin, v katerih se šteje, da bi ponudniki storitev morali vedeti za protipravno dejavnost ali podatek. To ustvarja negotovost glede dolžnega ravnanja ponudnika storitev.[22] Člen 15 direktive določa, da države članice ponudnikom storitev ne smejo predpisati splošne obveznosti za nadzor podatkov pri njihovem prenosu

[21] Edwards, str. 65; Tičar, Makarovič, str. 269–270.

[22] Mazziotti, str. 168.

ali shranjevanju, pa tudi ne za dejavno raziskovanje okoliščin, na podlagi katerih se domneva, da gre za nezakonito dejavnost. Ta določba se v glavnem razlaga v smislu, da se od ponudnikov storitev informacijske družbe ne sme zahtevati, da proaktivno iščejo in filtrirajo kakršnokoli potencialno nelegalno vsebino. Pač pa 48. uvodna izjava direktive določa, da države članice od ponudnikov storitev, ki hranijo podatke od prejemnikov storitev, lahko zahtevajo, da ravnajo s skrbnostjo, ki jo je od njih razumljivo pričakovati in je določena v nacionalnem pravu, tako da odkrijejo in preprečijo nekatere oblike nezakonitih dejavnosti.

4. Odprta vprašanja

4.1. Takojšnje ukrepanje

Člen 11 ZEPT po zgledu direktive določa, da ponudnik storitev ohrani imuniteto, če *nemudoma*, ko mu je protipravnost znana, ukrepa tako, da podatke odstrani ali onemogoči dostop do njih. Niti zakon niti direktiva ne opredeljujeta pomena besede »nemudoma«, zato ni jasno, ali mora ponudnik storitev dostop do spornih podatkov onemogočiti takoj, ko prejme takšno zahtevo domnevnega oškodovanca (na primer v 24 urah po tem), ali pa ima na voljo še primeren čas, da sam preveri dejstva in o vprašanju pridobi ustrezna pravna mnenja.

Za učinkovito varstvo, na primer pred protipravnimi posegi v osebnostne pravice, je bistveno čim hitrejše ukrepanje in onemogočenje dostopa do spornih vsebin. Vendar je zahteva po takojšnji (v fiksnem roku) odstranitvi vsakršnih spornih vsebin, v zvezi s katerimi je ponudnik storitev prejel zahtevo domnevnega oškodovanca, lahko pretirana, saj omogoča zlorabo tovrstnih zahtev. Prekratek rok lahko pomeni tudi praktično težavo za ponudnike storitev, saj lahko traja nekaj časa, da zadeva pride do pristojnega uslužbenca in da se sporna vsebina locira (na primer če se pojavlja na več mestih na kompleksnem spletišču).

Zahteve, da ponudnik storitev ukrepa nemudoma, če se hoče izogniti odgovornosti za sporno vsebino, zato ni primerno razlagati v smislu kratkega fiksnega roka za odstranitev teh vsebin. Primerneje bi bilo zahtevati, da ponudnik storitev, ko dobi zahtevo za odstranitev, ravna z dolžno skrbnostjo in stori vse, kar je razumno potrebno za čimprejšnjo preprečitev nadaljnjega razširjanja sporne vsebine. Koliko časa je razumno potrebno za takšno ukrepanje, pa je treba presoditi glede na okoliščine vsakega posameznega primera.[23]

[23] Edwards, str. 66–67.

4.2. (Ne)utemeljenost zahteve za odstranitev

Zakon ne definira oblike, v kateri mora biti ponudnik storitev informacijske družbe obveščen o protipravnosti podatkov, da je dolžan ukrepati. Zadošča elektronska pošta, telefonski klic, SMS-sporočilo? Je zahteva lahko anonimna ali se mora pošiljatelj identificirati kot imetnik pravic in specificirati pravice, ki naj bi jih sporna vsebina kršila?

Če bi morali ponudniki storitev enako ukrepati ob vsaki zahtevi za odstranitev vsebin, bi to hitro pripeljalo do tega, da bi zaradi finančnega tveganja potencialne odškodninske odgovornosti preprosto odstranili vsako vsebino, glede katere se kdorkoli pritoži, brez preverjanja utemeljenosti te pritožbe. Takšna ureditev omogoča preprosto zlorabo zahteve za odstranitev v politične ali poslovne namene (na primer s strani konkurenčnih podjetij) in ponudnike storitev potiska v zasebno cenzuro, ki je še posebno problematična, ker poteka brez sodelovanja sodišča. Po nekaterih podatkih je v praksi vsaj tretjina zahtev za odstranitev vsebin, ki jih prejmejo ponudniki storitev, neutemeljenih.[24] Več raziskav pa je pokazalo, da ponudniki storitev po prejemu zahteve največkrat blokirajo sporno vsebino brez preverjanja točnosti navedb, celo kadar gre za očitno neutemeljeno zahtevo (na primer, ker gre za avtorsko delo, ki se mu je že zdavnaj izteklo pravno varstvo).[25]

Odstranitev legalno objavljenih vsebin pa je problematična tudi zato, ker ponudnik storitev informacijske družbe s tem lahko krši pogodbo s prejemnikom storitev, tj. ponudnikom vsebin, do katerih je ponudnik storitev onemogočil dostop (če takšna odgovornost ni posebej izključena v pogodbi med tema subjektoma). Ameriški DMCA tak položaj posebej ureja, in sicer ponudniku internetnih storitev daje imuniteto pred odškodninskimi zahtevki prejemnikov storitev, če je pri blokiranju oziroma odstranitvi vsebin ravnal v dobri veri.

Direktiva o elektronskem poslovanju v 46. uvodni izjavi poudarja, da se morata odstranitev ali onemogočenje dostopa izvesti ob upoštevanju načela svobodnega izražanja mnenja in v ta namen določenih postopkov na nacionalni ravni. Direktiva ne posega v možnost držav članic, da predpišejo posebne zahteve, ki jih je treba nemudoma izpolniti pred odstranitvijo ali blokado podatkov. V nacionalni zakonodaji bi bilo torej mogoče predpisati pogoje in postopke, ki

[24] Urban, Quilter, str. 2.

[25] Take primere preučuje *Chilling Effects Clearinghouse*, skupni projekt organizacije Electronic Frontier Foundation in pravnih klinik univerz Harvard, Stanford, Berkeley, University of San Francisco, University of Maine, George Washington School of Law in Santa Clara University, ki je namenjen varstvu zakonitih spletnih dejavnosti pred neutemeljenimi pravnimi grožnjami. http://www.chillingeffects.org.
Glej tudi Nas, *The Multatuli Project ISP Notice & take down*.

jih morata v primeru zahteve za odstranitev oziroma blokado določenih vsebin izpolniti stranka, ki vlaga zahtevo, in ponudnik storitev informacijske družbe.

Pri tem bi se bilo mogoče zgledovati po ameriškem DMCA, ki v par. 512 vsebuje vrsto varovalk pred arbitrarnim odstranjevanjem oziroma blokiranjem spornega gradiva:

- Zahteva za odstranitev vsebine s spletnih strani mora biti ponudniku internetnih storitev posredovana v strogo predpisani obliki. Oseba, ki zahteva odstranitev, se mora ustrezno identificirati kot imetnik kršenih pravic (z uporabo digitalnega podpisa, če zahtevo vlaga po elektronski pošti) in mora specificirati podatke o vsebini, ki naj bi kršila njene pravice. Če je zahteva vložena neutemeljeno, lahko vlagatelj odškodninsko odgovarja.
- Prejeto zahtevo za odstranitev mora ponudnik storitev posredovati ponudniku vsebin, ki je to gradivo objavil, ta pa ima možnost, da se o zahtevi za odstranitev izjavi. Če ponudnik vsebin odstranitvi nasprotuje, mora ponudnik storitev sporno gradivo vrniti na splet.
- Če vlagatelj zahteve za odstranitev pri tej zahtevi vztraja, morata domnevni oškodovanec in domnevni kršitelj svoj spor urediti na sodišču. Med trajanjem postopka pa lahko ponudnik internetnih storitev obdrži gradivo na svoji strani, ne da bi bil za to odškodninsko odgovoren, tudi če na koncu sodišče odloči, da je šlo za kršitev pravic.

V odsotnosti izrecne zakonske ureditve bi bilo mogoče (ob upoštevanju uvodnih izjav direktive) tovrstne varovalke delno uveljaviti tudi skozi samoregulacijo ponudnikov in sodno prakso, ki bi na primer štela, da ponudnik internetnih storitev ni odškodninsko odgovoren, če je odklonil blokado oziroma odstranitev vsebin, dokler vlagatelj zahteve z določeno verjetnostjo ne izkaže, da te vsebine res protipravno posegajo v njegov pravni položaj.[26]

4.3. Oblika odgovornosti

Člen 8 ZEPT določa, da ponudnik storitev odgovarja za podatke, ki jih zagotovi prejemnik njegove storitve, po določbah tega zakona. Pri tem pa ne določa, za kakšno obliko odgovornosti gre, če ponudnik storitev ne ravna v skladu z določbami 9. do 11. člena zakona, temveč v teh členih samo našteva pogoje, ob izpolnitvi katerih je njegova odgovornost izključena. Je torej odgovornost krivdna ali objektivna? Ali je ponudnikovo neupoštevanje zakonskih določb samostojen temelj obveznosti ali pa ponudnik storitev odgovarja za protipravno ravnanje prejemnika storitev, ki je zagotovil sporne vsebine?

[26] Primerjaj Tičar, Makarovič, str. 271.

Odgovornost za drugega zakon predpisuje v primerih, ko neposredni povzročitelj škode dejavnost opravlja za nekoga drugega (na primer za delodajalca) in je njegovo ravnanje mogoče pripisati tej drugi osebi. Ker prejemnik storitev praviloma ne nastopa v imenu ponudnika storitev informacijske družbe in ga ne zastopa v pravnem prometu, ni videti razloga, da bi ponudnik storitev odgovarjal za ravnanje svojih strank kot za lastno ravnanje. Odločilno za odškodninsko odgovornost ponudnika storitev torej ni ravnanje osebe, ki je neposredno zagotovila (tj. na internetu objavila) sporne vsebine, temveč njegovo lastno ravnanje v skladu z določbami 9. do 11. člena ZEPT po tem, ko je izvedel za protipravnost določenih vsebin. Če ustrezno ne ukrepa, potem je javna dostopnost teh vsebin na njegovih strežnikih posledica njegove opustitve, in iz te lahko izvira njegova odgovornost.

Storitev informacijske družbe na splošno ni mogoče šteti za dejavnost, iz katere izvira povečana škodna nevarnost za okolico v smislu drugega odstavka 131. člena Obligacijskega zakonika (OZ),[27] v skladu s tretjim odstavkom istega člena pa se za škodo odgovarja ne glede na krivdo samo v primerih, ki jih določa zakon. Čeprav ZEPT pri določbah o odgovornosti ponudnikov posredovalnih storitev ne omenja krivde, tega ni mogoče šteti za določitev objektivne odgovornosti. Ponudnik storitev torej odgovarja krivdno ob upoštevanju splošnih pravil o odškodnini za posamezno vrsto kršitve (osebnostne pravice, avtorske pravice …) in posebnih pravil ZEPT o pogojih za izključitev odgovornosti.

4.4. Splet 2.0

Ko se je pripravljala ureditev iz Direktive o elektronskem poslovanju, se je razloček med ponudnikom spletnih storitev gostovanja in ponudnikom vsebine zdel precej jasen. Nadaljnji razvoj interneta pa je dal vse večji poudarek interaktivnim zmogljivostim in uporabi omrežja kot platforme, na kateri lahko uporabniki programske aplikacije v celoti zaganjajo preko brskalnika (Web 2.0). Uporabniki tako niso več le goli potrošniki informacij, ki jih zagotavlja ponudnik vsebin, temveč lahko tudi sami upravljajo svoje vsebine na spletni strani, te vsebine uporabnikov pa so pogosto nelegalne, ker kršijo avtorske pravice ali znamke, ali so objektivno žaljive do konkretnih oseb. Spletne storitve, pri katerih uporabniki prispevajo svojo vsebino (*user-generated content*), so doživele izjemno rast in uspeh. Primeri takšnih spletišč so e-Bay, Facebook, Myspace, YouTube, GoogleDocs, Flickr. Lastnik platforme spodbuja uporabnike k spletnemu objavljanju in deljenju vsebin, ki so jih sami ustvarili. Te vsebine generirajo velik

[27] Uradno prečiščeno besedilo OZ – UPB1, Uradni list RS, št. 97/2007.

promet, ki omogoča doseganje znatnih prihodkov od oglaševanja. Uporabnikom pa se praviloma ne zaračunava članarina.[28]

V takšnem položaju ni več mogoče preprosto reči, da so prejemniki storitev (na primer člani socialnega omrežja Facebook) izključni ponudniki vsebine, ponudnik storitev informacijske družbe, ki upravlja spletno mesto, pa še vedno samo nevtralni posrednik informacij, za vsebino katerih ne more odgovarjati. Upravljavec spletnega mesta namreč v takšnem primeru vsaj posredno pridobiva koristi od gostovanja nezakonitih vsebin, ki jih objavljajo člani, vsebine ponudnika in prejemnikov storitev pa se prepletajo. Zato se zastavlja vprašanje, ali ni ponudnik storitev vsaj solidarno odgovoren za protipravno vsebino. To bi bilo mogoče utemeljevati zlasti, kadar ponudnikov poslovni model očitno temelji na gostiteljstvu velikih količin vsebin tretjih oseb, za katere je splošno znano, da so v velikem delu nelegalne. Za to védenje ni potrebno posebno obvestilo imetnika pravic, temveč bi lahko do odgovornosti ponudnika prišlo že na podlagi njegovega lastnega poznavanja dejstev in okoliščin, iz katerih izhaja protipravnost v smislu prve alineje prvega odstavka 11. člena ZEPT.[29] Seveda pa je vprašanje, kako naj ponudnik storitev v takšnem položaju ukrepa, da se izogne odgovornosti. Če ni mogoče učinkovito filtriranje spornih vsebin, je namreč edina alternativa prenehanje opravljanja storitve.

V zadevi *Louis Vuitton Moët Hennesey (LVMH) proti eBay* je francosko sodišče odločilo, da družba eBay odgovarja, ker uporabnikom ni preprečila prodaje ponarejenega blaga na svojem spletišču za spletne dražbe. V podobnem primeru v ZDA je eBay zmagal in Tiffany izgubil. Vprašanje je v prvi vrsti ekonomsko, in ne pravno: kdo naj nosi stroške nadzora nad prodajo ponarejenega blaga ali drugih dobrin, ki kršijo izključne pravice – imetniki izključnih pravic ali ponudniki internetnih storitev, ki imajo od prometa vsaj posredno tudi sami korist?[30] S tega vidika je zanimiv primer *Viacom proti Google (YouTube)*, ki je še v teku. Iz pogajanj o morebitni zunajsodni poravnavi je namreč razvidno, da Google razvija sistem, ki bi omogočil avtomatično filtriranje videoposnetkov, ki bi kršili avtorske pravice. Podoben avtomatiziran sistem bi bilo mogoče vzpostaviti tudi v zvezi s prodajo blaga, ki krši pravice imetnikov znamk. Če takšno filtriranje tehnično postane mogoče, se bodo spremenile nekatere dejanske predpostavke, na katerih temelji sedanja ureditev odgovornosti ponudnikov storitev informa-

[28] George, Scerri, str. 3–5; Murray, str. 107–110.

[29] Edwards, str. 67. Vsebino bi bilo mogoče pripisati ponudniku storitev tudi z argumentom, da že njegova platforma sama avtorizira dejanja ponudnikov vsebine. V smislu zakona: prejemnik storitve ukrepa v okviru pooblastil ali pod nadzorom ponudnika.

[30] Edwards, str. 69.

cijske družbe in se bo najverjetneje od njih zahtevalo aktivnejše preprečevanje dostopnosti nelegalnih vsebin.

Nekoliko drugačen je položaj pisanih komentarjev uporabnikov na blogih, spletnih forumih ali na straneh socialnih omrežij. Značilnost internetnega komuniciranja v takih oblikah je, da je glede načina izražanja in predhodnega razmisleka bolj podobno govoru kakor pisani besedi. Zato so žaljive ali obrekljive opazke (pa tudi kršitve drugih pravic) zapisane mimogrede.[31] Tovrstnih protipravnosti ni mogoče avtomatizirano filtrirati (razen preprostega filtriranja vulgarnih besed), saj program ne razume vsebine besedila. Hkrati pa na primer blogerji nimajo enakih možnosti za preverjanje informacij kot klasični mediji, zato jih glede odgovornosti ne bi bilo primerno podvreči istim pravilom, saj bi to preveč posegalo v svobodo izražanja. Pri tem niti ni bistveno, ali odškodninsko odgovarja samo oseba, ki je objavila sporno besedilo, ali pa mu objavo cenzurira ponudnik storitev zaradi bojazni pred morebitno odškodninsko odgovornostjo. Zaradi varstva svobode izražanja bi bilo za tovrstne internetne objave, ki izražajo predvsem mnenja posameznikov, primerno vzpostaviti drugačen standard kot za objave v profesionalnih medijih.[32]

4.5. Odgovornost za hiperpovezave

Medtem ko ameriški DMCA ponudnikom internetnih storitev pod določenimi pogoji podeljuje tudi imuniteto pred odgovornostjo za vzpostavljene hiperpovezave, evropski pravni režim tega vprašanja ne ureja. Vzpostavljanje povezav na druga spletna mesta ne konstituira gostiteljstva in z njim povezane odgovornosti v smislu Direktive o elektronskem poslovanju oziroma ZEPT. Drugi odstavek 21. člena direktive sicer Evropski komisiji nalaga obveznost, da pri poročanju o izvajanju direktive posebej razčleni potrebo po predlogih v zvezi z odgovornostjo ponudnikov hiperpovezav in iskalnikov, vendar za zdaj sprememb direktive v tej smeri ni mogoče pričakovati.

Vzpostavljanje hiperpovezav je na internetu vse večjega pomena. Kot hiperpovezave so na primer prikazani rezultati iskanja s katerimkoli od internetnih iskalnikov (na primer Google, Yahoo, Bing, Baidu, Najdi.si), ki jih proizvede ustrezen iskalni algoritem in nad vsebino katerih ponudnik storitve iskanja praviloma nima nadzora. Njegova vloga je torej tehnična in vsebinsko nevtralna, zato v skladu z načeli evropskega režima odgovornosti internetnih posrednikov

[31] Murray, str. 165.

[32] Edwards, str. 57. Drugače (da je bloge pravno treba obravnavati kot medije) meni Zidar Klemenčičeva, str. 14. O razžalitvi prek družbenega omrežja Facebook glej Murray, str. 162–164.

za vsebino prikazanih hiperpovezav ponudnik iskanja ne bi smel odgovarjati.[33] Vprašanje pa je, koliko je drugačen položaj, kadar ponudnik spletnega iskanja iz komercialnih razlogov prireja vrstni red prikazanih rezultatov (zaradi trženja boljšega vrstnega reda).[34] Kljub vplivu na rezultat iskanja pa ponudnik storitve tudi v takšnem položaju nima nadzora nad vsebino spletnih mest, na katera vodijo prikazane povezave.

Prav tako so v obdobju po uveljavitvi Direktive o elektronskem poslovanju postali pomemben internetni vmesnik t. i. agregatorji, tj. spletne strani, ki samodejno združujejo vsebino z različnih drugih spletnih mest, tako da lahko uporabnik na primer prebere samo naslov in nekaj vrstic z izbrane strani (na primer Yahoo! News) ali primerja cene (na primer Ceneje.si). Agregatorji torej zgolj vzpostavljajo povezave na različne vsebine tretjih oseb, nad katerimi pa nimajo tehničnega ali vsebinskega nadzora.[35]

Tudi na področju odgovornosti za hiperpovezave pa so najkontroverznejši problem omrežja za izmenjavo datotek *peer-to-peer* (P2P). Spletne strani, ki so trenutno najbolj na udaru zaradi domnevnih kršitev pravic intelektualne lastnine, na primer razvpiti Pirate Bay, namreč same ne gostijo avtorskopravno varovanega gradiva, ampak pri modernih decentraliziranih protokolih samo povezave na datoteke *torrent*, s katerimi programje P2P samo poišče druge uporabnike, ki hkrati pretakajo isto gradivo. Pirate Bay (in mnogo drugih podobnih strani) torej vzpostavlja kvečjemu posredne povezave na gradivo, ki krši izključne pravice avtorjev, oziroma omogoča vzpostavljanje takšnih povezav z uporabo ustreznega programa. Pri tem ponudnik storitev (upravljavec spletnega mesta) nima nadzora nad legalnostjo oziroma ilegalnostjo vsebin. Odškodninske odgovornosti ni mogoče utemeljevati zgolj s spodbujanjem uporabe protokola P2P, saj gre pri tem za vsebinsko nevtralno tehnologijo prenosa podatkov, ki omogoča povsem zakonite prenose velikih datotek in se v ta namen pogosto tudi uporablja (na primer za razširjanje novih različic operacijskega sistema Linux). Njena prednost je, da optimizira uporabo pasovne širine in zato pospešuje hitrost interneta.

Res pa je splošno znano, da je precejšen delež vsebin, ki se prenašajo prek protokolov P2P, nezakonitih, saj so očitno na voljo zunaj klasičnih distribucijskih kanalov, ki jih uporabljajo veliki imetniki pravic na glasbi in filmih. Spletne stra-

[33] V zakonodaji oziroma sodni praksi evropskih držav glede odgovornosti ponudnikov iskalnikov ni enotnega pristopa. Uporabljena so že bila pravila za čisti prenos, za predpomnjenje in tudi za gostiteljstvo. Tičar, Makarovič, str. 276.

[34] Takšno ravnanje je lahko v določenih okoliščinah sporno z vidika konkurenčnega prava, vendar to ni predmet tega prispevka. Glej Tičar, Makarovič, str. 277.

[35] Edwards, str. 77–78. Posebno vprašanje je, kdaj tovrstno združevanje delov vsebin z drugih spletnih strani preide v kršitev avtorskih pravic na objavljenih vsebinah. Glej Murray, str. 228–233.

ni, specializirane za objavljanje povezav do *torrentov,* s to dejavnostjo ustvarjajo promet in dosegajo dohodke od oglaševanja, zato je mogoče trditi, da je omogočanje dostopa do ilegalnih vsebin del njihovega poslovnega modela in da bi se iz okoliščin morali zavedati protipravnosti. Vendar je po drugi strani *torrente* prav tako mogoče iskati s splošnimi iskalniki, kot je na primer Google, ki povezav na potencialno nelegalne vsebine prav tako ne filtrirajo, prihodek pa ustvarjajo s prikazovanjem oglasov ob prikazanih povezavah in si zato prizadevajo za čim večji promet. Težko je skratka postaviti mejo med »dobrimi« in »slabimi« hiperpovezavami. Protokol P2P je še bolj zameglil mejo med »nedolžnimi« internetnimi posredniki na eni in ponudniki vsebin na drugi strani.[36]

V odsotnosti posebne zakonske ureditve je odgovornost za hiperpovezave odvisna predvsem od konkretnih okoliščin posameznega primera, zato so bila tudi v primerjalni sodni praksi glede tega vprašanja zavzeta diametralno nasprotna stališča. Najverjetneje povsem enotnega pravila, ki bi veljalo v vseh okoliščinah, tudi ni mogoče oblikovati.[37]

5. Možne smeri razvoja

Očitno je, da veljavni evropski režim odgovornosti ponudnikov storitev informacijske družbe ne odgovarja na vsa vprašanja odgovornosti različnih internetnih posrednikov in ne ureja zadovoljivo vseh položajev. To je razumljivo, saj se internet še razmeroma hitro razvija in spreminja, zato zakonodaja ni mogla vnaprej predvideti vseh bodočih načinov uporabe in ponujanja storitev na internetu. Številne danes skorajda povsod prisotne spletne storitve so se pojavile šele po sprejemu Direktive o elektronskem poslovanju iz leta 2000. Tako na primer Wikipedia obstaja od leta 2001, YouTube od leta 2005, Facebook od leta 2006. Razvoju interneta s poudarjeno interaktivnostjo in konvergenco različnih storitev se bo morala prilagajati tudi pravna ureditev, bodisi s spremembami zakonodaje bodisi v sodni praksi.

Doslej so bili opazni precejšnji pritiski s strani industrije vsebin (zlasti glasbenih in filmskih založniških hiš ter programerskih podjetij), ki je med velikimi imetniki pravic intelektualne lastnine, da se temeljna rešitev z *ex post* nadzora, kar je sistem *notice and take down* in ki terja aktivnost imetnikov pravic, premakne na sistem *ex ante* nadzora, ki bi ga morali zagotavljati internetni posredniki z vzpostavitvijo sistemov filtriranja vsebin, do katerih omogočajo dostop, sicer

[36] Edwards, str. 79. Glej tudi Klun, str. 21. V primeru *Buma/Stemra v. Kazaa* (C02/186HR) je nizozemsko vrhovno sodišče odločilo, da Kazaa ne odgovarja za nelegalne vsebine uporabnikov in da prenesenih podatkov ni dolžan nadzorovati oziroma filtrirati. Glej Murray, str. 247–248.

[37] Tičar, Makarovič, str. 281.

bi bili sami odškodninsko odgovorni za kršitve. Poleg filtriranja se kot možna vloga ponudnikov storitev omenja še razkrivanje identitete kršiteljev, opozarjanje kršiteljev o možnih posledicah ter odklop ali upočasnjevanje njihovih internetnih povezav. Kot rečeno, 15. člen Direktive o elektronskem poslovanju načeloma preprečuje vzpostavitev splošne obveznosti ponudnikov storitev, da nadzirajo vsebine prejemnikov storitev. Sodišče ali upravni organ pa verjetno lahko v posameznem primeru naloži ponudniku internetnih storitev, da aktivno preprečuje kršitve pravic tudi s filtriranjem vsebin, če je to tehnično izvedljivo.[38]

Zamisli, da bi ponudniki internetnih storitev morali nadzirati vsebino, se pojavljajo tudi v zvezi z otroško pornografijo, širjenjem terorizma in ekstremnega islamizma, spletnimi igrami na srečo itd. Pri takšnih zahtevah je dodatno vprašanje, kako naj ponudnik storitev, ki sam ne gosti teh vsebin, ampak uporabnikom samo omogoča dostop do njih, blokado sploh izvede. Mogoča je blokada internetne domene, blokada IP-naslova ali nadzor s tehnologijo DPI (*deep packet inspection)*, ki preverja samo vsebino posredovanih podatkov. Učinkovito filtriranje omogoča samo zadnja metoda, ki pa lahko pomeni radikalen vdor v zasebnost uporabnikov in je njena zakonitost lahko sporna.[39]

Pravno bo treba doreči poseben položaj hibridnih oblik med gostiteljstvom in ponujanjem vsebin, morda z upoštevanjem finančnih koristi, ki jih posrednik pridobiva z objavljanjem hiperpovezav in gradiva tretjih oseb. Smiselno bi bilo natančneje določiti, kdaj lahko imetniki pravic in državni organi od ponudnikov internetnih storitev zahtevajo preventivno filtriranje ali blokiranje določenih vsebin. Potrebna so tudi posebna pravila o odgovornosti spletnih iskalnikov, ki so bistveni za delovanje interneta. Vse to bi bilo najprimerneje urediti v enotnem evropskem pravnem režimu, vzpostavljenem po sistemu popolne harmonizacije, kar je pri čezmejnem pojavu, kot je internet, najbolj smiselno. Do tedaj pa bodo morala evropsko informacijsko politiko oblikovati sodišča z upoštevanjem temeljnih vrednot, kot so svoboda govora, zasebnost in pravna varnost.

[38] Primerjaj Edwards, str. 82. Glej belgijski primer SABAM v SA Tiscali, v katerem je bila zahteva po filtriranju utemeljena tudi s pravili Direktive 2001/29/ES o avtorski pravici v informacijski družbi.

[39] Edwards, str. 81–83; Mazziotti, str. 170. Kot opozarja Harper, sta obseg in podrobnost podatkov, ki jih posredujejo ponudniki internetnih storitev, dramatično večja od tistih, ki se prenašajo prek telefonske komunikacije, poleg tega je gradivo v digitalni obliki razmeroma lahko prestreči, shraniti in brati. Zato je potreba po varstvu zasebnosti pri internetni komunikaciji še večja kot pri telefonskih komunikacijah, pri katerih pa ni dvoma o tem, da telefonski operaterji ne smejo poljubno prisluškovati in snemati klicev uporabnikov. Harper, str. 31.

Literatura

Edwards, L.: The Fall and Rise of Intermediary Liability Online, v: L. Edwards, C. Waelde (ur.), *Law and the Internet.* Oxford: Hart Publishing, 2009.

George, C., Scerri, J.: Web 2.0 and User-Generated Content: legal challenges in the new frontier, *Journal of Information, Law and Technology,* št. 2/2007, dostopno na: http://go.warwick.ac.uk/jilt/2007_2/george_scerri.

Harper, J.. Against ISP Liability. Do ISPs have a duty to protect the world? *Regulation,* Spring 2005, str. 30–33.

Klun, G.: Peer to peer (P2P), *Pravna praksa,* št. 40/2007, str. 21.

Mazziotti, G.: *EU Digital Copyright Law and the End-User.* Berlin, Heidelberg: Springer, 2008.

Murray, A.: *Information Technology Law: The law and society.* Oxford: Oxford University Press, 2010.

Nas, S.: *The Multatuli Project ISP Notice & take down***,** Bits of Freedom, SANE, 1 October 2004, Revised article, 27 October 2004, dostopno na: http://www.bof.nl/docs/researchpaperSANE.pdf.

Tičar, K., Makarovič, B.: Udeleženci internetne komunikacije, v: *Pravni vodnik po internetu* (ur. B. Makarovič, J. Toplišek), Ljubljana: GV Založba, 2007.

Urban, J. M., Quilter, L.: *Efficient Process or »Chilling Effects«? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act: Summary Report*. Dostopno na: http://mylaw.usc.edu/documents/512Rep-ExecSum_out.pdf.

Zidar Klemenčič, N.: Odstranitev bloga na podlagi odredbe sodišča, *Pravna praksa,* št. 48/2006, str. 14.

Civilna odgovornost za anonimne komentarje na internetu

dr. Špelca Mežnar

1. Uvod

Anonimno komentiranje na internetu je v zadnjih letih postalo tako razširjeno in žal tudi problematično, da potrebuje jasno in strožjo pravno regulacijo.[1] Kakor vsako drugo izražanje mnenj in pogledov je tudi komentiranje na internetu kot izraz svobode izražanja omejeno s temeljnimi pravicami drugih – do zasebnosti, dobrega imena in časti, lastne podobe, družinskega življenja … Na žalost se v Sloveniji (ki sicer v tem pogledu ni izjema niti v svetu niti v Evropi) prepogosto ali celo praviloma dogaja, da se komentiranje na portalih, blogih, forumih, družabnih omrežjih zlorablja za izražanje frustracij, sovraštva, predsodkov, žalitev in pavšalnih obdolžitev ali širjenje laži.[2]

Ključno vprašanje v zvezi s civilno odgovornostjo za komentarje je preprosto: ali za izključitev protipravnega ravnanja zadošča, da upravljavci spletnih strani komentarje pregledujejo in po potrebi odstranjujejo naknadno, ko so že objavljeni, ali bi moral veljati strožji standard skrbnosti, ki od njih zahteva, da vsak komentar preverijo, še preden odobrijo njegovo objavo.

Izhodiščna teza je, da je odgovornost za komentarje na internetu pravno in vsebinsko primerljiva z odgovornostjo tiskanih medijev za pisma bralcev.[3] Ni

---

[1] Razlogov za razširjenost spletnega komentiranja je gotovo več, na primer izredno povečanje dostopnosti interneta in računalnikov, zlasti pa dejstvo, da je komentiranje v primerjavi s tradicionalnimi pismi bralcev mnogo preprostejše in hitrejše. Glej tudi Lemut Strle, str. 13–15.

[2] Glej Klipšteter, Petkovič, http://www.dnevnik.si/objektiv/v-objektivu/smrad-na-internetu1.

[3] Ta teza ni neproblematična. Tako je na primer hamburško sodišče analogijo med komentarji na internetu in pismi bralcev izrecno zavrnilo ter jo raje potegnilo med komentarji na internetu in televiziji ali radiu, ki jih pri oddajanju v živo dajejo tretje osebe. Višje sodišče v Hamburgu, sodba 7 U 50/06 z dne 22. 8. 2006. Nemško zvezno vrhovno sodišče (Bundesgerichtshof – BGH) pa je v zadevi VI ZR 101/06 z dne 27. 3. 2007 zavrnilo analogijo s TV-oddajami v živo; odgovornost upravljavca foruma za žaljive komentarje je primerjalo z možnostjo TV-hiš, da naknadno nadzorujejo predvajanje posnetkov oddaj z žaljivo vsebino – podobno lahko tudi upravljavec spletnega foruma po objavi spornega komentarja v celoti vpliva na to, da ga odstrani. BGH je tudi odločilo, da je zoper upravljavca foruma dopusten opustitveni zahtevek na prepoved bodočih kršitev, in to ne glede na to, ali je bila tožniku identiteta žaljivega komentatorja znana. To je pomenilo dokončno potrditev stališča, da se privilegij ekskulpacije za internetne posrednike nanaša zgolj na kazensko in

vprašljivo, da so za protipravne vsebine primarno odgovorni avtorji komentarjev (spletni uporabniki) po splošnih pravilih civilnega prava; a v trenutnih razmerah, ko je zaradi (pre)visoke ravni varstva zasebnosti skoraj nemogoče priti do identifikacijskih podatkov anonimnih piscev komentarjev na internetu (brez tega pa ne moremo vložiti civilne tožbe), je z vidika varstva oškodovanca toliko bolj pomembna morebitna odgovornost drugih oseb, ki spletne komentarje omogočajo, spodbujajo, urejajo ali imajo korist od njihove hiperprodukcije, tj. spletnih urednikov, izdajateljev portalov in lastnikov spletnih strani. Njihovi odgovornosti bo zato namenjena večina tega prispevka, v katerem želim ugotoviti, katere osebe so poleg avtorja komentarja v slovenskem civilnem pravu lahko še solidarno odgovorne za kršitev pravic, povzročeno s protipravnim komentiranjem, in kako (poleg odškodninskega je v praksi še pomembnejši prepovedni zahtevek na podlagi 134. člena OZ). Poleg slovenske je treba upoštevati tudi zakonodajo in prakso Sodišča EU ter Evropskega sodišča za človekove pravice v Strasbourgu, ki je leta 2013 izdalo zanimivo sodbo glede odgovornosti urednikov novičarskih portalov za komentarje anonimnih uporabnikov. Ob koncu predlagam možne pravne rešitve odgovornosti za spletno komentiranje *de lege ferenda* ter opozarjam na nujnost ureditve posebnega postopka, v katerem bo lahko upravičena oseba zahtevala razkritje identitete anonimnega uporabnika spleta.

Zavedam se, da se marsikdo s stališči, izraženimi v tem članku, ne bo strinjal, saj se zavzemam za strožjo odgovornost spletnih urednikov in izdajateljev, kakršna trenutno velja v sodni praksi nemškega zveznega vrhovnega sodišča.[4] Enako kot pri nas se tudi po svetu upravljavci forumov in spletnih portalov lastni odgovornosti za vsebine uporabnikov (*user generated content*) skušajo izogniti bodisi s klavzulami o omejitvi in izključitvi odgovornosti (*disclaimer*) bodisi s sklicevanjem na imuniteto internetnih posrednikov. To dejansko pomeni, da upravljavci spletnih portalov in forumov odgovarjajo šele pod pogojem, da so s sporno vsebino seznanjeni (kar se na primer zgodi, ko jih nanjo opozori oškodovanec), pri čemer jih ne veže splošna dolžnost pregledovati vsebino tretjih, preden dopustijo njeno objavo na lastnih spletnih straneh.

odškodninsko odgovornost, ne izključuje pa opustitvenih zahtevkov. Ti so tako tudi zoper internetne posrednike dopustni, če so izpolnjeni pogoji, ki jih je navedlo sodišče.

[4] Glej prejšnjo opombo. Sodna praksa nemških sodišč je sicer zelo neenotna, za najstrožji glede vprašanja odgovornosti upravljavcev spletnih strani veljata hamburško deželno in višje sodišče. Glej na primer LG Hamburg, sodba 324 O 794/07 z dne 4. 12. 2007.

2. Splošno o civilni odgovornosti za objave na internetu

Protipravna vsebina na internetu se lahko pojavlja v najrazličnejših oblikah, na primer kot žaljiv zapis na blogu,[5] sovražni govor v forumu,[6] žaljiv in obrekljiv članek na novičarskem portalu, neresnična ocena storitve ali produkta na potrošniškem portalu, objava tuje fotografije, sovražen in žaljiv komentar … V tem prispevku se omejujem izključno na (anonimne) komentarje, ki so neke vrste derivat, saj nastanejo kot odziv na primarno objavljeno vsebino – članek na spletni strani, zapis na blogu, razpravo na forumu. Ker so komentarji praviloma odziv »zunanjih, tretjih oseb«, torej tistih, ki niso neposredno vpletene v sestavo primarnih vsebin, se mi zdi odgovornost za komentiranje na internetu smiselno primerjati z odgovornostjo urednikov oziroma izdajateljev časopisov za objavo pisem bralcev.

2.1. Odgovornost za objavo novinarskih prispevkov

Za objave žaljivih vsebin v klasičnih medijih veljajo splošna pravila obligacijskega prava, po katerih ima oškodovanec na voljo različne zahtevke, med katerimi je v praksi zahtevek za prepoved (bodočih) kršitev po 134. členu OZ vsaj tako pomemben kot odškodninski. Strinjam se, da je z vidika oškodovanca pri kršitvah v množičnih medijih ta zahtevek v našem sistemu za varstvo osebnostnih pravic verjetno koristnejši in primernejši od klasičnega odškodninskega, saj je nepremoženjsko škodo nemogoče reparirati – pravi reparaciji (vrnitvi v stanje, kakršno je bilo pred kršitvijo) je še najbližja prepoved nadaljnjih kršitev na podlagi začasne odredbe (ki jo je seveda treba upravičiti s tožbo).[7] Temu pritrjuje sodna praksa, saj je v primerih kršitev osebnostnih pravic na internetu prepovedni zahtevek enako pogost kot odškodninski, oškodovanci pa posežejo tudi po zahtevku za objavo preklica in objavo sodbe.[8] Pri tem velja opozoriti, da uspešno uveljavljanje prepovednega zahtevka po 134. členu OZ ni odvisno od krivde, kar pomeni, da tudi ekskulpacije iz razloga zadostne skrbnosti (ali nevednosti) ni.

---

[5] Zidar Klemenčič, str. 14–15.

[6] Primerjaj Samaluk, http://blog.eun.org/insafe/2006/02/slovenija_pomen_regulacije_sov.html: »O sovražnem govoru govorimo takrat, ko gre za izražanje mnenj in idej, ki so po svoji naravi ksenofobični, diskriminatorni, rasistični in naperjeni predvsem zoper razne manjšine (etnične, verske, kulturne) in zajema tako govorno, pisno kot nebesedno (parade, insignije, simboli ipd.) komunikacijo.« S sovražnim govorom na internetu se je v zadnjem času ukvarjalo kar precej (nepravnih) diplomskih in magistrskih del, na primer Andrej Motl, Sovražni govor v slovenskih medijih na spletu, FDV, Ljubljana 2009, in tam našteta nadaljnja literatura.

[7] Zidar Klemenčič, Prepovedni zahtevek, str. 7.

[8] Glej na primer VSL II Cp 4539/2010 z dne 15. 12. 2010 in VSM I Cp 1033/2013 z dne 19. 11. 2013.

Glede pasivne legitimacije – kroga oseb, ki jih je dopustno tožiti zaradi medijskih kršitev – pa v sodni praksi obstaja prava zmeda. Nesporno je le, da je za objavo spornega članka gotovo odgovoren izdajatelj medija (časopisa), torej medijska hiša (na primer družba Delo, d. d.). Vendar pa je Vrhovno sodišče v vsaj dveh meni znanih primerih[9] pasivno legitimacijo razširilo še na novinarja in odgovornega urednika, čeprav bi zanju moralo veljati pravilo 147. člena OZ, po katerem sta lahko neposredno tožena samo v primeru naklepne povzročitve škode. Takšno stališče je zavzelo z uporabo dveh argumentov, ki ju žal v nobeni izmed obeh citiranih sodb ni podrobneje utemeljilo: da je neposredna odgovornost novinarjev in urednikov določena z Zakonom o medijih ter da pisanje in objavljanje člankov že samo po sebi pomeni naklepno ravnanje.[10]

Po mojem mnenju Zakon o medijih (ZMed) nikakor ni specialnejši zakon v primerjavi z OZ, ki določa temeljno pravilo o odgovornosti delodajalca za škodo, ki jo povzročijo njegovi delavci.[11] Ne 6. ne 18. člen ZMed ne dajeta pravne podlage za derogacijo 147. člena OZ (temeljnega in izjemno pomembnega pravila *respondeat superior*, po katerem delavec za navadno malomarnost sploh ne odgovarja, za hudo malomarnost odgovarja samo regresno, za naklep pa solidarno z delodajalcem) in vzpostavitev neposredne odškodninske odgovornosti zaposlenega novinarja ali urednika. Prepričana sem, da bi tudi v primeru medijskih tožb moralo veljati enako kot v vseh drugih poklicih: neposredni zahtevek zoper zaposlene osebe oškodovanec lahko vloži le, če zatrjuje in dokaže njihovo naklepno ravnanje, kar pa seveda ni pisanje in urednikovanje *per se*; naklepna povzročitev škode pomeni, da mora biti tožencu (novinarju ali uredniku) dokazan namen oškodovati tožnika, ne pa zgolj namen napisati članek.[12] Naj omenim še, da ima Višje sodišče v Ljubljani glede istega vprašanja popolnoma nasprotno

[9] Sodbi II Ips 658/2004 z dne 7. 12. 2006 in II Ips 326/2009 z dne 6. 12. 2012.

[10] Iz obrazložitve sodbe II Ips 658/2004: »Drugi toženec v reviziji sicer navaja, da mu ni mogoče očitati, da je škodo povzročil namenoma. Vendar si spričo dejanskih ugotovitev v pravnomočni sodbi *po naravi stvari ni mogoče predstavljati, da bi s to trditvijo utegnil resno meriti na možnost sklepanja, da sta bila za tožnika škodljiva članka napisana in objavljena morda iz malomarnosti (?)*, česa takega pa ni med postopkom tudi nikoli zatrjeval. … z materialnopravnega vidika pa je treba drugega toženca s tem v zvezi napotiti le še na z določbo 7. člena v času povzročitve škode veljavnega Zakona o javnih glasilih (Uradni list RS, št. 18/94) izrecno predvideno tudi osebno odgovornost novinarja za posledice njegovega dela.« Enako določbo vsebuje tudi veljavni Zakon o medijih v 6. členu (op. Š. M.).

[11] Pojem delavca se sicer v sodni praksi razlaga široko in nedvomno zajema vse osebe, ki opravljajo delo v korist »delodajalca«, čeprav niso v delovnem razmerju, kot je opredeljeno v delovnem pravu (na primer podjemne in avtorske pogodbe). Glej na primer sklep VS RS II Ips 295/99 z dne 27. 1. 2000.

[12] Če bi argumentacija Vrhovnega sodišča obveljala, lahko ugotovimo, da večina delavcev škodo povzroča naklepno – kirurg ne operira iz malomarnosti, temveč z jasnim namenom (naklepom) izvesti operacijo.

stališče, s katerim se v celoti strinjam,[13] medtem ko Višje sodišče v Mariboru vsaj glede odgovornih urednikov meni, da »njihova odgovornost ni primerljiva s katerimkoli delavcem …, saj je od njih pričakovati večjo skrbnost pri nadzoru informacij kot pa od kateregakoli drugega delavca (na primer novinarja)«. Enako kot Vrhovno sodišče zato zaključuje, da bi bila uporaba 147. člena OZ v primeru odgovorne urednice v nasprotju z njeno vlogo in nalogami, ki jih opravlja, saj bi jo razbremenila vsakršne odškodninske odgovornosti. Podlago za njeno neposredno odgovornost je zato videlo v 18. členu ZMed.[14]

2.2. Odgovornost za objavo pisem bralcev v časopisu

V primeru pisem bralcev je sicer navedena sodna praksa manj pomembna, saj avtor pisma navadno ni »delavec« po OZ in zanj ne more veljati privilegij po 147. členu OZ. Avtor pisma (bralec) zato nesporno samostojno in neposredno odškodninsko odgovarja, če pismo vsebuje protipravno vsebino. Povsem logično se zdi, da je poleg njega za objavo odgovoren tudi urednik, ki je svoje delo očitno opravil malomarno, saj je dopustil objavo, s tem pa prispeval k nastanku

[13] Glej na primer sodba VSL I Cp 4698/2010 z dne 28. 9. 2011: »Ne glede na navedeno pa pritožbeno sodišče še dodaja, da … to ne bi zadostovalo za zaključek o odškodninski odgovornosti drugega toženca kot odgovornega urednika. Sodišče prve stopnje je sicer štelo, da predstavlja podlago odškodninske odgovornosti drugega toženca 18. člen ZMed, po katerem odgovorni urednik odgovarja med drugim za uresničevanje programske zasnove in za vsako objavljeno informacijo, s čimer pa se pritožbeno sodišče ne strinja. Z navedenim členom ZMed je sicer vzpostavljena določena odgovornost odgovornega urednika, vendar (zgolj) odgovornost v smislu ZMed, ki določa dolžnosti odgovornega urednika in hkrati tudi sankcije v primeru, da slednji ne ravna tako, kot mu zakon nalaga (na primer odgovorni urednik mora objaviti popravek, če so izpolnjeni zakonski pogoji; če pa odgovorni urednik ne objavi popravka v roku in na način, določen z zakonom, ima tisti, ki zahteva objavo popravka, pravico vložiti tožbo zoper odgovornega urednika za objavo popravka pri sodišču – 26. in 33. člen ZMed), pri čemer med temi sankcijami ni navedena odškodninska sankcija oziroma ZMed nikjer ne določa, da mora odgovorni urednik, če pride z objavljeno informacijo do kršitve osebnostne pravice, prizadeti osebi povrniti škodo. Da 18. člen ZMed ne predstavlja podlage za odškodninsko odgovornost odgovornega urednika, pa po oceni pritožbenega sodišča izhaja tudi iz same dikcije tega člena. V njem namreč niso uporabljeni izrazi, ki bi nakazovali na odškodninsko odgovornost – ni navedeno, da gre za odgovornost za škodo oziroma za odškodninsko odgovornost odgovornega urednika, še manj za kakšno obliko odgovornosti naj bi šlo (ali za krivdno ali za objektivno). Odškodninsko odgovornost odgovornega urednika je zato treba presojati po določbah OZ o odškodninski odgovornosti, in sicer (zlasti) po določbi 147. člena OZ, ki ureja odgovornost delodajalca za ravnanje delavca (odgovorni urednik je delavec v smislu tega člena). Skladno z drugim odstavkom te zakonske določbe ima oškodovanec pravico zahtevati povrnitev škode tudi neposredno od delavca, vendar zgolj v primeru, če je ta škodo povzročil namenoma. Ker tožeča stranka v postopku pred sodiščem prve stopnje, kljub temu, da je tožena stranka ves čas opozarjala na določbe 147. člena OZ, ni zatrjevala, da je drugi toženec v konkretnem primeru ravnal z naklepom, tožeča stranka s tožbenim zahtevkom zoper drugega toženca tudi iz tega razloga ne bi mogla uspeti.«

[14] VSM I Cp 1033/2013 z dne 19. 11. 2013. S citirano razlago neposredne odgovornosti odgovorne urednice se seveda ne strinjam.

škode. Vendar mora tudi v tem primeru veljati, da neposrednega zahtevka zoper zaposlenega urednika oškodovanec ne more vložiti. Na podlagi 147. člena zanj odgovarja njegov delodajalec, kar je v praksi najpogosteje izdajatelj časopisa. Oškodovanec ima tako možnost solidarno tožiti pisca in izdajatelja.[15]

2.3. Odgovornost za objavo (anonimnih) komentarjev na internetu

Če imamo opravka z žaljivim komentarjem na internetu, pod katerim je avtor podpisan z resničnim imenom in priimkom, lahko oškodovanec brez težav sproži civilni postopek. Sodišče v takšnem primeru uporabi enaka merila kot v siceršnjih postopkih zaradi kršitve osebnostnih pravic in sklicevanja na svobodo izražanja – test sorazmernosti in tehtanje, kateri izmed pravic bo v konkretnih okoliščinah dalo prednost. Seveda ni nujno, da bo to vselej tožnikov interes.[16] Žal so podpisani komentarji na spletu bolj izjema in ne pravilo.

Civilnopravno je nekoliko bolj zapletena situacija klasičnega sovražnega govora, ko avtor komentarja ne napada konkretne osebe, temveč skupino oseb, ki jih družijo določene lastnosti (narodnost, spolna usmerjenost, politične preference). V tem primeru mora oškodovanec dodatno upravičiti svojo aktivno legitimacijo, to pa bo storil, če bo dokazal, da nedvomno spada v skupino, ki je bila tarča spornega komentarja, in da ga je objava tudi osebno prizadela.

Podobno kot v tiskanih medijih objavo pisma bralca omogoči urednik, je za komentiranje na internetu poleg pisca komentarja nujno potrebna še oseba, ki omogoči, da se komentar shrani in objavi. Vprašanje, koga lahko oškodovanec poleg avtorja spletnega komentarja toži, pa je v primeru interneta mnogo bolj pomembno kot v primeru pisem bralcev, saj so spletni komentatorji praviloma anonimni, to pa oškodovancu pravno in dejansko izniči možnosti, da bi zahtevek naperil neposredno zoper spletnega uporabnika. Če hočemo v trenutnih razme-

[15] Pisma bralcev so v časopisih vedno podpisana, tako da identifikacija avtorja ni problematična. Če bi urednik dopustil objavo anonimnega žaljivega pisma bralca, pa so lahko podane okoliščine, v katerih bi bil utemeljen tudi neposredni zahtevek zoper urednika, saj bi upravičeno lahko veljala domneva, da je avtor anonimnega pisma urednik – s tem pa je odgovoren enako kot resnični avtor. Glej na primer I Cp 1231/98: »V tej zvezi je treba še poudariti, da je prvo sodišče tudi pravilno utemeljilo odškodninsko odgovornost sedmotoženca in tudi njegovo pasivno legitimacijo. Iz članka, objavljenega v Dnevniku, ni razvidno, kdo je avtor. Kadar avtor članka ni naveden, odgovarja zanj odgovorni urednik. Pri tem ni pomembno, da je znotraj časopisne hiše sicer znano, kdo je pisec članka, pomembno je, da le-ta ni bil javno objavljen.« Nikakor pa se ne strinjam s stališčem, izraženim v isti sodbi, da je odgovornost novinarjev objektivna, torej neodvisna od njihove krivde: »Po oceni pritožbene stopnje novinarji za škodo pri svojem delu samostojno odgovarjajo, ne glede na to, ali jo povzročijo namenoma ali iz malomarnosti.«

[16] Več o težavah pri tehtanju obeh pravic glej Zidar Klemenčič, str. 14–15; Grčar, str. 6–8; Tekavc, str. XVIII–XX, Velkaverh, str. 27; Teršek, str. 111–134.

rah oškodovancu sploh zagotoviti kakršnokoli pravno varstvo, je zato nujno, da identificiramo druge odgovorne osebe.

Razmerja in vloge različnih posrednikov na internetu niso tako jasni kot v klasičnih medijih – opravka imamo z uredniki in lastniki spletnih strani[17] (na primer blogov), uredniki oziroma moderatorji forumov, izdajatelji in uredniki spletnih medijev (novičarskih spletnih portalov), pa tudi z osebami, ki zgolj tehnično omogočajo objavo komentarjev (na primer lastnik strežnika). Konkretna vloga te tretje osebe, posrednika, je lahko zelo različna in sega od tega, da ponuja zgolj prostor (na primer oddaja prostor na strežniku, kjer je bil objavljen komentar) in nima nikakršnega nadzora nad objavljeno vsebino, prek tega, da komentiranje avtomatično omogoča, a ga ne nadzoruje, do situacije, ko komentarje ureja na enak način kot v klasičnih medijih – vsakega posebej torej preveri in se skladno z uredniško presojo in politiko odloči, ali in s kakšno vsebino bo objavljen. Včasih lahko ista oseba nastopa v več omenjenih vlogah. Medtem ko je nekatere spletne portale (na primer novičarske) brez dvoma mogoče uvrstiti med medije, je pri drugih primerjava z mediji manj ustrezna, ker mnogokrat ne gre za uredniško oblikovane programske vsebine, temveč njihovo vsebino spontano oblikuje množica uporabnikov.[18] Vendar pa mislim, da je o tem, ali konkretna vsebina na spletni strani ustreza definiciji »medija«, treba odločati v vsakem primeru posebej in da na primer ne moremo enostavno zaključiti, da blogi nikoli niso mediji.[19]

---

[17] Urednik bloga je oseba, ki skrbi za objave in ureja komentiranje. Lahko je sam tudi avtor prispevkov, ni pa nujno. Lastnik spletne strani je oseba, ki je registrirala spletno domeno.

[18] Člen 2 ZMed: (1) Mediji po tem zakonu so časopisi in revije, radijski in televizijski programi, elektronske publikacije, teletekst ter druge oblike dnevnega ali periodičnega objavljanja uredniško oblikovanih programskih vsebin s prenosom zapisa, glasu, zvoka ali slike, na način, ki je dostopen javnosti. (2) Programske vsebine po tem zakonu so informacije vseh vrst (vesti, mnenja, obvestila, sporočila ter druge informacije) in avtorska dela, ki se razširjajo prek medijev z namenom obveščanja, zadovoljevanja kulturnih, izobraževalnih in drugih potreb javnosti ter množičnega komuniciranja. (3) Mediji niso bilteni, katalogi ali drugi nosilci objavljanja informacij, ki so namenjeni izključno oglaševanju, poslovnemu komuniciranju, izobraževalnemu procesu ali notranjemu delu gospodarskih družb, zavodov in ustanov, društev, političnih strank, cerkvenih in drugih organizacij, šolska glasila, Uradni list Republike Slovenije, uradna glasila lokalnih skupnosti in druge uradne objave, plakati, letaki, prospekti in transparenti, ter video strani brez žive slike (neplačana obvestila), razen če je s tem zakonom določeno drugače.

[19] Kot je pravilno ugotovilo Višje sodišče v Ljubljani, pa to niti ni bistveno. Sklep VSL II Cp 4539/2010 z dne 15. 12. 2010: »Sodišče prve stopnje ni naredilo potrebnega materialnopravnega preizkusa, ali so posamezne trditve o dejstvih in posamezna mnenja (vrednostne sodbe), ki izhajajo iz spornih zapisov, objektivno žaljiva, temveč je (zgolj) navedlo, da moč spletnih klepetalnic nima moči medijev ter da se pričakuje od povprečnega spletnega obiskovalca, da bo v odnosu do vrednostnih sodb podanih v spletnih klepetalnicah ravnal z določeno rezervo, torej z vednostjo, da kritika anonimne osebe, ki nima ustreznih strokovnih znanj, glede ustreznih kvalifikacij zdravnika in kakovosti njegovega dela ne vzdrži strokovne presoje. Ni res, da z vrednostnimi sodbami, izrečenimi v spletni klepetalnici, ni mogoče prizadeti ugleda in časti posameznika.«

Po mojem mnenju bi morala biti odgovornost urednikov in izdajateljev spletnih strani za objavo komentarjev spletnih uporabnikov odvisna od tega, kako so vpleteni v objavo spornega komentarja, in tega, ali so prispevki uporabnikov bistveni del ponujenih vsebin. Popolnoma se lahko ekskulpirajo le tisti ponudniki internetnih storitev, ki zagotavljajo zgolj tehnične storitve (prenos podatkov, prostor na strežniku) za objave, in to pod pogojem, da s protipravno vsebino niso seznanjeni. Vsi drugi, ki so v komentiranje aktivno vpleteni (že s tem, da z uredniško politiko spodbujajo komentiranje) in imajo od komentiranja ekonomsko korist (na primer s prihodki od oglaševanja), pa bi lahko bili zlasti v primeru žaljivih anonimnih komentarjev tudi sami civilno odgovorni.

V nadaljevanju bom predstavila estonski primer, ki je končal na Evropskem sodišču za človekove pravice, nato pa bom opisala ureditev odgovornosti za anonimne komentarje v slovenskem pravu.

2.3.1. Odgovornost novičarskih portalov za komentiranje anonimnih uporabnikov – primer Delfi

Oktobra 2013 je Evropsko sodišče za človekove pravice izdalo sodbo v zadevi *Delfi*,[20] v kateri je sodišče odločalo, ali izdajatelj novičarskega portala odškodninsko odgovarja za žaljive komentarje, ki jih pod članki objavljajo posamezni, večinoma anonimni in neregistrirani uporabniki. Ob tem se postavita dve zanimivi vprašanji: prvič, ali bi (lahko) tudi slovenska sodišča presodila, da za objavljanje žaljivih komentarjev na novičarskem portalu odškodninsko odgovarja izdajatelj novičarskega portala, čeprav uredništvo skladno s predpisi zagotavlja postopek odstranitve spornih komentarjev; in drugič, ali bi takšna odločitev pomenila kršitev medijske svodobe izražanja v smislu EKČP. Odgovor na drugo vprašanje je nikalen.

Primer je poleg tega odprl še vprašanja:

- ali izdajatelji (in uredniki) novičarskih portalov veljajo za klasične »ponudnike internetnih storitev«[21] in torej uživajo imuniteto pred civilnim in kazenskim pregonom (skladno z Direktivo 2000/31/ES o elektronskem poslovanju) ali pa je njihova vloga aktivnejša in primerljiva s klasičnim delom urednika medija,
- ali in kako na odgovornost portala vpliva dejstvo, da komentarjev ne pregledujejo sproti, vendar pa jih umaknejo takoj, ko so obveščeni o protipravni vsebini (*notice and take-down procedure*),

[20] Sodba št. 64569/09 z dne 10. 10. 2013, dosegljiva na http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{%22appno%22:[%2264569/09%22],%22itemid%22:[%22001-126635%22]}. Glej Cerar, str. 22.

[21] Več o odgovornosti internetnih posrednikov glej Damjan, str. 139–155.

- ali in kako na odgovornost portala vpliva dejstvo, da je komentarjev preveč za sprotno pregledovanje, in kako dejstvo, da je število komentarjev povezano s prihodki od oglaševanja,
- ali in kako na njihovo odgovornost vpliva dejstvo, da je večina komentatorjev anonimnih in torej za oškodovance zaradi strogih ustavnih zahtev tudi *de iure* (in ne le *de facto*) nedosegljivih,
- ali je za odgovornost portala pomembno, o čem in kako govori članek, ki je spodbudil sporne komentarje,
- ali smejo/morajo izdajatelji portalov uporabljati programe za avtomatično pregledovanje in izločanje spornih komentarjev, je registracija komentatorjev zadosten ukrep ali pa je potrebna redakcija vseh komentarjev, preden so objavljeni,
- kako naj se portali izognejo pretnji civilne odgovornosti.

Pri tem je verjetno najpomembnejše prvo vprašanje. Če se namreč izdajatelji in uredniki spletnih novičarskih portalov (podobno velja tudi za forume in bloge) kvalificirajo zgolj za pasivne internetne posrednike, ki na objavljene vsebine nimajo in ne smejo imeti vpliva, je njihovo odgovornost za nezakonite vsebine glede na jasne določbe Direktive 2000/31/ES o elektronskem poslovanju težko uveljaviti. Če pa zavzamemo stališče, da so odgovorni na podoben način kot izdajatelji in uredniki klasičnih medijev, saj njihova vloga ni pasivna, ampak zaradi različnih, zlasti komercialnih interesov aktivno spodbujajo komentiranje, je enaka tudi njihova odgovornost.[22]

2.3.2. Kratek povzetek dejanskega stanja in argumentacije sodišča

Na spletnem portalu Delfi (www.delfi.ee) je bil januarja 2006 objavljen članek o estonski ladijski družbi, ki se je odločila uvesti nove tranzitne povezave, s tem pa bi povzročila uničenje nekaterih »ledenih cest«, ki so pozimi za uporabnike cenejša možnost prometne povezave med kopnim in otoki (javne ceste, ki nastanejo pozimi na zamrznjenem morju). Članek je izzval 185 komentarjev, med njimi je bilo približno 20 grobo žaljivih do fizičnih oseb – članov organov upravljanja ladijske družbe. Uporabniki so lahko komentarje objavljali na koncu članka s preprostim vnosom svojega imena (seveda tudi psevdonima, kar se največkrat dogaja) in elektronskega naslova ter se jim ni bilo treba registrirati. Uredništvo komentarjev ni pregledovalo ali kako drugače vplivalo na njihovo objavo. V uporabi sta bila sicer sistem avtomatičnega izločanja komentarjev, ki so vsebovali nekatere vulgarne besede, in sistem, po katerem so takoj umaknili

[22] Glej na primer članek novinarja Dela, Lenarta J. Kučića, Svoboda komentiranja, http://www.delo.si/mnenja/blog/svoboda-komentiranja.html, 10. 11. 2013.

komentar, za katerega je prizadeta oseba to zahtevala (t. i. *notice and take-down system*). V konkretnem primeru je prizadeta fizična oseba zahtevala odstranitev spornih člankov, čemur je uredništvo tudi takoj ugodilo, vendar so bili do tedaj komentarji na spletu dosegljivi šest tednov. Na podlagi omenjenega je oškodovanec vložil tožbo za povrnitev nepremoženjske škode zaradi kršitve osebnostnih pravic, čemur so estonska sodišča ugodila. Novičarski portal je objavil tudi splošne pogoje, podobne tem, ki jih poznamo z domačih spletnih strani: da ne odgovarja za vsebino objavljenih komentarjev, da jih ne pregleduje in da komentarji ne smejo biti žaljivi, sicer komentatorji zanje odgovarjajo.[23]

Estonsko vrhovno sodišče je potrdilo pravilnost stališč nižjih sodišč, da izdajatelj novičarskega portala ni zgolj internetni posrednik v smislu Direktive 2000/31/ES o elektronskem poslovanju, saj je bistvo njegovega dela v odločilnem vplivu in nadzoru nad vsebino objavljenih informacij. Uredništvo objavljenih komentarjev ne preverja, vendar omogoča in spodbuja njihovo objavo, saj ima od njih neposredno ekonomsko korist. Poleg tega uporabniki (vključno z oškodovano osebo) izgubijo vsak nadzor nad komentarji, ko so enkrat objavljeni, edino možnost njihovega spreminjanja ali brisanja ima izdajatelj. Dejstvo, da izdajatelj te možnosti ni sistematično uporabljal tako, da bi sproti pregledoval vse komentarje in tiste s protipravno vsebino izločal, ne pomeni, da je bil pasiven posrednik brez nadzora nad vsebino. Sodišče je tudi poudarilo, da je vloga izdajatelja portala v primeru objave komentarjev vsebinsko podobna urejanju klasičnih medijev in da ima prizadeta oseba pravico, da izbere, koga bo tožila – bodisi neposrednega povzročitelja (avtorja spornega komentarja) bodisi urednika spletnega portala. Ker je torej izdajatelj opustil svojo zakonsko dolžnost skrbnega ravnanja in nepovzročanja škode tretjim osebam, je odškodninsko odgovoren.

V prepričljivo obrazloženi sodbi je ESČP najprej podalo pregled estonskega prava in drugih relevantnih mednarodnih aktov. Estonska zakonodaja je tako glede ureditve odškodninske odgovornosti za kršitve osebnostnih pravic v primeru medijev kot glede implementacije direktive Direktive 2000/31/ES o elektronskem poslovanju povsem primerljiva s slovensko.[24] Vendar je tudi ESČP zavzelo stališče, da je dopustno izdajatelja novičarskega portala pravno enačiti z izdajateljem klasičnih medijev in ne internetnim posrednikom, ki nad objavljeno vsebino praviloma nima nadzora, ter zato njegovo odgovornost podrediti splošnim pravilom obligacijskega prava.[25] Izrecno je zavrnilo pritožnikov argument, da naj bi bila uporaba splošnih pravil o odgovornosti medijev za objavljene vsebine

[23] Večina slovenskih portalov, ki omogočajo komentarje, vsebuje podobne splošne pogoje.

[24] Primerjaj 8. do 11. člen Zakona o elektronskem poslovanju na trgu, Uradni list RS, št. 61/2006.

[25] Ta več o možnostih in omejitvah ekskulpacije internetnih posrednikov na podlagi Direktive 2000/31/ES o elektronskem poslovanju glej sodno prakso Sodišča EU v zadevah C-236/08 do

na internetu nepredvidljiva, saj je štelo, da gre zgolj za uporabo obstoječih pravil pri novih tehnologijah. Zanimivo je, da je pri tem sodišče opozorilo, da so splošne pravne določbe za prilagoditev prava novim razmeram (na primer internetnim tehnologijam) pogosto primernejše kot pa podrobni pravni predpisi.

2.4. Odgovornost za anonimne komentarje v Sloveniji

Menim, da načeloma ne more biti sporno, da so spletni novičarski portali (pri nas na primer www.siol.net, www.delo.si, www.dnevnik.si, www.rtvslo.si, www.pozareport.si) po svoji vsebini mediji v smislu 2. člena Zakona o medijih (ZMed).[26] Gre namreč za »elektronske publikacije dnevnega ali periodičnega objavljanja uredniško oblikovanih programskih vsebin s prenosom zapisa, glasu, zvoka ali slike, na način, ki je dostopen javnosti« po opredelitvi v prvem odstavku 2. člena ZMed. Pri tem je bistveno, da so objavljeni prispevki na spletnih novičarskih portalih uredniško oblikovani na enak način kot v klasičnih medijih, le da so v klasičnih medijih tudi komentarji bralcev pod uredniškim nadzorom, spletni komentarji pa ne (oziroma je uredniška politika vsaj bistveno šibkejša). Tudi sodna praksa pritrjuje gledanju, po katerem so novičarski spletni portali mediji.[27]

Seveda pa to ne daje avtomatično odgovora na vprašanje, ali so spletni portali tudi internetni posredniki v smislu Direktive 2000/31/ES o elektronskem poslovanju in Zakona o elektronskem poslovanju na trgu (ZEPT), v katerem je v tem delu implementirana.[28] Ponudniki storitev informacijske družbe[29] ne odgovarjajo za izključni prenos in t. i. predpomnjenje (*caching*), saj pri teh dejavnostih ne nadzorujejo posredovanih vsebin (nimajo niti obveznosti niti pravice nadzora). Če ponudnik podatke tudi shranjuje oziroma omogoča dostop tretjim osebam (gostiteljstvo, *hosting*), pa je njegova vloga aktivnejša, zato se lahko ekskulpira samo v primeru nevednosti oziroma v primeru, da skladno z zakonom upošteva sistem prijave in odstranitve spornih vsebin (*notice-and-take-down procedure*). Klasični primer zadnje skupine ponudnikov so podjetja, ki prodajajo oziroma dajejo v zakup prostor na strežnikih. Za te tri kategorije internetnih posrednikov zakon torej omogoča ekskulpacijo civilne odgovornosti s preprostim sistemom obveščanja o spornih vsebinah in ustreznim odzivom ponudnika (umikom sporne vsebine). Breme nadzora je prevaljeno na oškodovanca, ki je dolžan pregledovati

C-238/08, *Google France in Google* [2010] ECR I-2417, z dne 23. 3. 2010, C-324/09, *L'Oréal in drugi,* z dne 12. 7. 2011 in C-70/10, *Scarlet Extended,* z dne 24. 11. 2011.

[26] Uradni list RS, št. 35/2001.

[27] Glej sklep VSL V Kp 201/2010 z dne 7. 4. 2010 in sodbo VSL II Cp 1587/2004 z dne 15. 9. 2004.

[28] Primerjaj 8. do 11. člen Zakona o elektronskem poslovanju na trgu, Uradni list RS, št. 61/2006.

[29] Izrazi »internetni posredniki«, »ponudniki internetnih storitev« in »ponudniki storitev informacijske družbe« so v tem prispevku sinonimi.

spletne vsebine in internetnega ponudnika pozvati k odstranitvi, medtem ko slednji izrecno nima dolžnosti vsesplošnega nadzora objavljenih vsebin. Pri tem je ključno, da je smisel predstavljene ureditve razbremenitev tistih internetnih posrednikov, ki se ne ukvarjajo z vsebino objavljenih informacij, temveč zagotavljajo zgolj nevtralne tehnične storitve, ki omogočajo delovanje informacijske družbe.[30]

2.4.1. Odgovornost urednikov, moderatorjev in izdajateljev spletnih strani

Menim, da za novičarske in druge spletne portale, pa tudi za bloge in forume, če gre za objave komentarjev ob uredniško nadzorovanih vsebinah, po namenski interpretaciji ne more veljati privilegij iz 14. člena direktive ne glede na to, ali se kvalificirajo za ponudnike internetnih storitev po direktivi ali ne. Izrecno o tem ni odločilo niti ESČP (nima namreč pristojnosti razlagati zakonodajo EU) niti Sodišče EU, saj estonsko vrhovno sodišče tovrstnega predhodnega vprašanja ni zastavilo. Vendar pa lahko iz opredelitve namena privilegija v 14. členu direktive sklepamo, da je bil cilj ekskulpirati zgolj tiste internetne posrednike, katerih gospodarska dejavnost ni ukvarjanje z vsebino informacij, temveč bodisi njihov prenos in omogočanje dostopa bodisi njihovo tehnično shranjevanje.[31] Zlasti je pomenljivo pojasnilo št. 48, po katerem »direktiva ne posega v možnost, da države članice od ponudnikov storitev, ki hranijo podatke od prejemnikov storitev, zahtevajo, da postopajo s skrbnostjo, ki jo je od njih razumljivo pričakovati in je določena v nacionalnem pravu, tako da odkrijejo in preprečijo nekatere oblike nezakonitih dejavnosti«. Enako izhaja iz prakse Sodišča EU. V zadevi *L'Oréal* je sodišče jasno povedalo, da zgolj na podlagi dejstva, da gre za ponudnika storitev informacijske družbe, še ne moremo sklepati, da je upravičen do privilegija iz 14. člena direktive, saj je to odvisno od njegove vloge v razmerju do strank. Če je njegova vloga dejavna (na primer optimizacija predstavitve ponudb za prodajo ali njihova promocija) in ne zgolj tehnično nevtralna, se na izjemo ne bo mogel sklicevati.[32]

---

[30] Tako izrecno Sodišče EU v zadevah C-236/08 do C-238/08, *Google France in Google* [2010] ECR I-2417, z dne 23. 3. 2010, C-324/09, *L'Oréal in drugi,* z dne 12. 7. 2011, in C-70/10, *Scarlet Extended,* z dne 24. 11. 2011.

[31] Glej na primer uvodna pojasnila št. 42 do 48 Direktive o elektronskem poslovanju.

[32] Primer C-324/09, *L'Oréal in drugi* [2011]: »Sodišče je glede tega že pojasnilo, da je za to, da bi ponudnik internetne storitve lahko spadal na področje uporabe člena 14 Direktive 2000/31, bistveno, da je v skladu z namenom, ki ga je imel zakonodajalec v okviru oddelka 4 poglavja II te direktive, 'posredni ponudnik storitev' (glej prej navedeno sodbo *Google France in Google,* točka 112) … To pa ne velja, če ima ponudnik storitve, namesto da bi zgolj nevtralno opravljal storitev s povsem tehnično in samodejno obdelavo podatkov, ki jih sporočijo njegove stranke, dejavno vlogo, zaradi katere bi lahko te podatke poznal ali nadzoroval (navedena sodba *Google France in Google,* točki 114 in 120).«

Glede na opisano zakonodajo in prakso Sodišča EU[33] bi lahko v primeru objave žaljivega anonimnega komentarja tudi v Sloveniji odškodninsko odgovarjal izdajatelj spletnega novičarskega portala na podlagi ZMed in splošnih pravil obligacijskega prava (krivdna odgovornost), pri tem pa se ne bi mogel uspešno sklicevati na privilegije, ki veljajo za nevtralne ponudnike internetnih storitev.[34] Njegova odgovornost obstaja torej tudi, če je urednik sporni komentar odstranil takoj, ko je bil o njem obveščen oziroma je prejel takšno zahtevo. Komentarji na novičarskih portalih niso ne vsebinsko ne tehnično ločeni od objavljenih člankov (lastnih vsebin), zaradi česar smiselno sestavljajo vsebinsko sklenjeno celoto; prav je torej, da odgovornost za zakonitost celotne vsebine (tako lastnih prispevkov kot pod njimi objavljenih komentarjev) nosi ista oseba – izdajatelj novičarskega portala (oziroma urednik, ki pa je navadno »delavec« po 147. členu OZ, zaradi česar ne more biti neposredno tožen). V tem primeru namreč omogočanje komentiranja ni nevtralna tehnična dejavnost, temveč vsebinska dopolnitev avtorskih prispevkov. Če obstajajo podlage za krivdno odgovornost upravljavcev spletnih strani, pa je seveda toliko bolj dopusten tudi prepovedni zahtevek (prepoved objave bodočih kršitev) na podlagi 134. člena OZ.

Podobno po mojem mnenju velja tudi za komentiranje na blogih in v forumih ter na drugih uporabniških portalih. Za upravljavca bloga praviloma velja oseba, ki je blog (domeno) registrirala; če ta ni identična uredniku, ki skrbi za objave na blogu, je lahko za anonimne komentarje odgovoren tudi urednik.[35] Tudi forumi imajo moderatorje, ki bi morali skrbeti za nadzor nad komentarji kot bistvenim delom spletnih skupnosti. Če moderator dopušča anonimno komentiranje brez vsakega nadzora in gre za javnosti dostopen forum, menim, da morata biti odgovorna tako moderator kot upravljavec foruma.[36] V teh primerih se svoji odgovornosti ne morejo izogniti niti v primeru, ko so na poziv oškodovanca sporni komentar odstranili (če je bil seveda pred tem dostopen dovolj časa, da je lahko povzročil škodo), in seveda tudi ne s klavzulami o izključitvi odgovornosti (*disclaimer*), ki so navadno vključene v splošne pogoje. Menim torej, da so

[33] Glej tudi judikaturo Sodišča EU v zadevah C- 236/08 do C-238/08, *Google France in Google* [2010], ter zadeva C-70/10, *Scarlet Extended* [2011].

[34] Pri tem ne izključujem možnosti, da velja novičarski spletni portal za ponudnika internetnih storitev po definiciji, ki jo vsebuje Direktiva o elektronskem poslovanju.

[35] Za izdajatelja in urednico bloga bi lahko tako šteli družbo TSmedia, d. o. o., lastnico portala Blog.siol.net, ki objavlja bloge številnih uporabnikov, pri tem pa tudi moderira vsebino spletnega portala. Spletni portal blog.siol.net je pred leti imel tudi posebnega urednika (fizično osebo), zdaj pa očitno tega dela ne opravlja nihče.

[36] Če je med izdajateljem spletnega portala (bloga, foruma) in urednikom ali moderatorjem podrejeno razmerje po 147. členu OZ (urednik ali moderator dela v korist in po navodilih izdajatelja, gre za različni osebi), pa je treba upoštevati, da zoper malomarnega »zaposlenega« urednika ali moderatorja ni mogoče vložiti neposrednega zahtevka, kar pomeni, da ima oškodovanec možnost tožiti izdajatelja.

upravljavci spletnih strani vsaj v primeru, da omogočajo anonimno komentiranje, dolžni vsak anonimni komentar pregledati, in če je očitno protipraven, onemogočiti njegovo objavo na svoji spletni strani.[37]

Vem, da je moje stališče precej radikalno. Vendar pa upoštevam specifično slovensko okolje, kjer se je anonimno komentiranje sprevrglo v čisto nasprotje uresničenja svobode izražanja – namesto da bi spodbujalo kakovostno in spoštljivo izmenjavo mnenj (debato), ga vsaj anonimni komentatorji uporabljajo za ventil, ki jim omogoča izraziti bes, jezo in žal tudi zlobo. Težko si zato predstavljam, da bi v takšnem okolju vsaj brez resnih dvomov zdržalo stališče, da imajo anonimni spletni komentatorji in osebe, ki imajo od tega ekonomsko korist, prednost pred oškodovanci. Če uredniki komentarje lahko pregledajo (in jih morajo pregledati!) po tem, ko so bili nanje opozorjeni, ni posebnega razloga, da jim te obveznosti vsaj za anonimne komentarje ne bi naložili na splošno in kot pogoj, da komentar sploh objavijo.[38]

Slovenska sodna praksa je v zanimivem primeru »med vrsticami« izrekla, da bi se ponudnik gostiteljskih storitev za bloge (Blog.siol.net, ki je bil odškodninsko tožen) lahko ekskulpiral, če bi se pravočasno odzval na poziv oškodovanke,[39] vendar se v podrobno razčlenitev njegove odgovornosti nato ni spuščalo.[40] Glede na predstavljena stališča bi sodišče po mojem mnenju tudi v tem primeru moralo ugotavljati, ali ponudnik internetnih storitev gostiteljstva poleg tehnične[41] opravlja še katero drugo funkcijo, na primer uredniško ali izdajateljsko. Ravno omenjeni portal namreč res objavlja bloge registriranih uporabnikov, ne lastnih vsebin, vendar pa hkrati nekatere bloge tudi izpostavlja, jih razvršča po branosti in številu komentarjev in jih torej vsaj delno ureja. Glede na stališče Sodišča EU v zadevi *L'Oréal* bi bilo treba za uporabo privilegija, ki velja za nevtralne ponudnike storitev, nujno ugotoviti, da je bila vloga gostitelja pri konkretnem

[37] Podobno stališče je zavzelo hamburško deželno sodišče v zadevi 324 O 794/07 z dne 4. 12. 2007, ko je presojalo, ali je avtor in lastnik bloga dolžan pred objavo pregledovati očitno protipravne komentarje, ki so jih na njegovem blogu puščali uporabniki. Sodišče je poudarilo, da je treba vsebino skrbnosti sicer določati v vsakem primeru posebej, da pa standard skrbnega ravnanja upravljavca bloga v situacijah, ko obstaja velika verjetnost žaljivih komentarjev, pomeni obveznost vnaprejšnjega pregledovanja vseh komentarjev. Sodišči v Hamburgu (deželno in višje) sta sicer znani po strogih stališčih do svobode izražanja in sta izjema v siceršnji nemški sodni praksi.

[38] Podobno argumentacijo je zavzelo VSM v sodbi I Cp 1033/2013 z dne 19. 11. 2013.

[39] Glej sodbo VSP I Cp 3037/2011 z dne 9. 5. 2012. Šlo je za objavo spornega besedila na enem najbolj branih blogov spletnega ponudnika Blog.siol.net. Ponudnik – gostitelj ne objavlja nobenih lastnih vsebin, temveč le bloge registriranih uporabnikov.

[40] Za to ni bilo niti potrebe, saj ni bilo dvoma, da se ponudnik na poziv oškodovanca k odstranitvi spornih vsebin ni odzval, s čimer ni izpolnil temeljnje predpostavke za ekskulpacijo.

[41] Če opravlja izključno funkcijo t. i. ponudnika gostovanja (*host-provider*), je njegova odgovornost lahko izključena pod pogoji iz direktive. Tako tudi sodba BGH VI ZR 93/10 z dne 25. 10. 2011.

prispevku (blogu) zgolj posredniška (ponujanje prostora na strežniku). Če pa je vsebino predstavljal kot posebej vredno branja in s tem posredno pridobival tudi premoženjsko korist (šlo za enega najbolj branih blogov na tem spletnem portalu), se na omenjeni prilvilegij ne bi mogel sklicevati niti v primeru, da bi prispevek na pobudo prizadete osebe umaknil.

Še bolj zanimivo je dejansko stanje v primeru VSL II Cp 4539/2010 z dne 15. 12. 2010. Sodišče je moralo presojati o predlogu za izdajo začasne odredbe, s katero se toženi stranki (upravljavcu foruma) nalaga, da takoj odstrani s spletne strani v predlogu za začasno odredbo navedene zapise, ter se ji prepoveduje ponovna objava zapisov s takšno vsebino.[42] Prvostopenjsko sodišče je predlog zavrnilo, pritožbeno pa je takšno odločitev razveljavilo. Izrecno je zavrnilo argumentacijo sodišča prve stopnje, da komentiranje v spletnih forumih (klepetalnicah) ne more poseči v čast in dobro ime, z razlago, da »moč spletnih klepetalnic nima moči medijev ter da se pričakuje od povprečnega spletnega obiskovalca, da bo v odnosu do vrednostnih sodb, podanih v spletnih klepetalnicah, ravnal z določeno rezervo«. Višje sodišče je opozorilo, da iz dejstva, da informacije na spletnih forumih niso nujno zanesljive, še ni mogoče sklepati, da ne morejo nikoli vplivati na zdravnikovo dobro ime. Judikat je pomemben zlasti zato, ker pasivna legitimacija izdajatelja spletne strani očitno ni bila problematična (ne za toženca ne za sodišče), kar pomeni, da so tudi pri nas dopustni zahtevki zoper izdajatelja spletne strani na podlagi 134. člena, vključno z začasnimi odredbami.

V povsem novi zadevi VSM I Cp 1033/2013 z dne 19. 11. 2013 pa je višje sodišče poleg pisca spornega prispevka (kolumne, objavljene na spletni strani) obsodilo še izdajatelja in celo odgovorno urednico, in to na objavo preklica in sodbe ter plačilo odškodnine. Pri tem je zanimiva utemeljitev sodišča, da za izdajatelja imuniteta po 11. členu ZEPT ne velja, saj se izdajatelj, ki ima zaposleno odgovorno urednico, ne more sklicevati na svojo »nevednost« pri objavi kolumne, ki jo je urednica odobrila. Vprašanje je, ali bi enak argument zdržal tudi ob presoji odgovornosti za komentarje, treba pa je priznati, da je odločitev sodišča v navedeni zadevi pogumna in dobro obrazložena (razen točke 11 sodbe, v kateri je sodišče po mojem mnenju napačno vzpostavilo neposredno odgovornost odgovorne urednice).

[42] Tožnik (zdravnik) je trdil, da je tožena stranka izdajateljica spletne strani, na kateri je v rubriki spletne klepetalnice objavljena tema z naslovom Dr. A. – operacija krčnih žil. V tej temi naj bi bile zapisane neresnice, laži, ki so povezane s tožnikom. Neresnice in izkrivljeno prikazana dejstva merijo na diskreditiranje tožnika kot zdravnika in grobo posegajo v njegove osebnostne pravice, zlasti v njegovo čast in dobro ime. Toženi stranki očita, da dopušča nedovoljene objave naključnih piscev in tako omogoča, da ti posegajo v tožnikove osebnostne pravice. Zahteval je odstranitev spornih zapisov iz foruma in prepoved ponovne objave zapisov s takšno vsebino.

2.4.2. Problem anonimnih komentatorjev

Tudi ESČP je opozorilo, da nesporni obstoj odškodninske odgovornosti neposrednega povzročitelja škode – komentatorja – sam po sebi ni zadosten razlog za razbremenitev spletnega portala, saj se upravičeno postavlja vprašanje učinkovitosti odgovornosti anonimnih komentatorjev.

Enako kot v Estoniji tudi v Sloveniji uporabnik, ki je objavil sporni komentar, nedvomno odgovarja za povzročeno škodo. Vendar pa ESČP opozarja na dejansko nemoč in pravno nezmožnost oškodovancev pri uveljavljanju tovrstnih odškodninskih zahtevkov, ki jo povzroča izjemno visoka raven varstva zasebnosti uporabnikov spleta, v katero spada tudi pravica do varstva osebnih podatkov, vključno z IP-številko (ki omogoča identifikacijo uporabnika konkretnega računalniškega priključka).

V Sloveniji je zaradi ustavnega varstva pravice do zasebnosti in komunikacijske tajnosti[43] ter odsotnosti zakonske ureditve, ki bi urejala problem kolizije pravic komentatorja in razžaljene osebe, podatke o tožencu – neposrednem povzročitelju škode – skoraj nemogoče dobiti, saj je za to potrebna posebna sodna odredba, do katere je očitno mogoče priti le v okviru kazenskega postopka.[44] Četrti odstavek 8. člena Zakona o elektronskem poslovanju na trgu določa, da »morajo ponudniki storitev vsem pristojnim organom na njihovo zahtevo najkasneje v roku treh dni od njenega prejema sporočiti podatke, na podlagi katerih je mogoče identificirati prejemnike njihove storitve (ime in priimek, naslov, firma, elektronski naslov). Navedene podatke morajo ponudniki storitev sporočiti zaradi odkrivanja in preprečevanja kaznivih dejanj na podlagi odredbe sodišča, brez odredbe sodišča pa, če tako določa področni zakon.«

V teoriji nisem našla stališč o tem, za kakšno odredbo naj bi šlo, a glede na vezanost odredbe na namen »odkrivanja in preprečevanja kaznivih dejanj« domnevam, da je do nje mogoče priti le v kazenskem postopku. To je seveda za oškodovance, ki bi želeli svoje pravice zaščititi v civilnem postopku (bodisi s prepovednimi bodisi odškodninskimi zahtevki), popolnoma nekoristno. Prvič zato, ker ureditev od oškodovanca zahteva nesorazmeren vložek energije, časa in denarja, drugič pa zato, ker vsi civilni delikti, ki so lahko storjeni s komentiranjem, niso nujno kazniva dejanja. V tem drugem primeru torej oškodovanec sploh nima pravne možnosti, da od sodišča zahteva razkritje identitete anonimnega komentatorja. Trenutno je v Sloveniji anonimni komentator tako varovan, da

[43] Glej odločbo US št. Up-106/05 z dne 2. 10. 2008.

[44] Tako tudi mnenje Informacijskega pooblaščenca št. 0712-1/2012/1999 z dne 13. 6. 2012, dostopno na https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=2210&cHash=a5817d2b73b2ff932a79ed01dd8efb3a (20. 11. 2013).

lahko brez tveganja objavlja, karkoli želi, saj oškodovanec nima pravne podlage za pridobitev podatkov, ki bi mu sploh omogočili vložitev civilne tožbe. Menim, da sedanja ureditev ni skladna z Ustavo, saj v koliziji oškodovančevih temeljnih pravic in komentatorjeve pravice do izražanja daje absolutno prednost slednji, hkrati pa skoraj gotovo tudi krši 8. člen EKČP. ESČP je namreč v primeru *K. U. proti Finski* ugotovilo, da je Finska, ki podobno kot Slovenija oškodovancu (dvanajstletnemu dečku, čigar podatke je nekdo objavil na spletni strani za zmenke) ni zagotovila pravnih možnosti za identifikacijo povzročitelja škode, kršila EKČP.[45]

Glede na povedano niti ne presenečajo podatki informacijske pooblaščenke, da je policija podatke o spletnih uporabnikih leta 2012 večinoma dobila na nezakonit način, brez sodne odredbe. Vendar se ponudniki internetnih storitev vse bolj zavedajo svojih obveznosti in takšne zahtevke zavračajo.[46]

V prihodnje bo nujno urediti poseben postopek, v katerem bodo lahko prizadete osebe zahtevale razkritje identite anonimnih komentatorjev (in drugih oseb, ki protipravno ravnajo na internetu).[47] Druga praktična rešitev je lahko v tem, da ponudniki storitev od uporabnikov začnejo dosledno zahtevati registracijo, ob kateri morajo navesti kontaktne podatke, vključno z imenom, priimkom in naslovom. Takšno prakso bi na primer spodbudila preprosta zakonska določba, da za avtorja anonimnega komentarja na spletu velja upravljavec spletne strani.

2.5. Kriteriji za vzpostavitev odgovornosti posrednikov

Že ESČP je v sodbi *Delfi* opozorilo na vrsto drugih dejavnikov, ki so pomembni za odločitev o obstoju odgovornosti lastnikov spletnih strani:

- ali spletni portal z objavljanjem in omogočanjem komentarjev pridobiva ekonomsko korist (višji prihodki od oglaševanja), kriterij je zlasti pomemben pri komercialnih in zasebnih forumih;[48]
- ali je urednik na podlagi profesionalnih izkušenj lahko predvidel, da bo članek dvigoval veliko prahu, in bi zato moral izkazati več skrbnosti pri nadzoru nad komentarji;

[45] Primer *K. U. proti Finski,* sodba št. 2872/02 z dne 2. 12. 2008. Glej tudi Lemut Strle, prav tam.

[46] Glej https://www.dnevnik.si/magazin/znanost-in-tehnologija/policija-naj-bi-nezakonito-pridobivala-podatke-o-bralcih-spletnih-portalov.

[47] Da je to realen in vse večji problem tudi drugod, potrjuje nedavna pogumna odločitev spletnega novičarskega portala na Hrvaškem (jutarnji.hr), ki je javno objavil najbolj primitivne, sovražne in žaljive komentarje, vključno z imeni in fotografijami posameznih komentatorjev, http://www.jutarnji.hr/mracna-strana-hrvatske--ovo-su-pritajeni-ekstremisti-medu-nama/1140564/.

[48] Višje sodišče v Hamburgu, sodba 7 U 50/06 z dne 22. 8. 2006.

- ali izdajatelj uporablja tehnične pripomočke, na primer računalniške programe za avtomatiziran pregled in izločanje spornih vsebin po ključnih besedah ali besednih zvezah …

Pomembna kriterija se mi zdita tudi število objavljenih komentarjev in podatek o njihovi branosti. Bolj ko je število komentarjev obvladljivo (da jih torej urednik lahko posamično prebere in odloči, ali so primerni za objavo), manj je razlogov za neredigirano objavo. Višja ko je branost komentarjev, bolj je pomembno, da se nad njimi izvaja nadzor. In končno: za anonimne komentarje mora veljati strožja odgovornost kot za tiste, pri katerih je uporabnikova identiteta znana.

Na splošno menim, da bi v vseh primerih, ko je objavljanje komentarjev pomemben (ali celo bistven, na primer v forumih) vsebinski prispevek spletnih strani, moralo veljati, da za anonimne komentarje poleg piscev odgovarjajo osebe, ki so sicer odgovorne za objavo vsebin – lastniki spletnih strani in uredniki ali moderatorji, kadar te osebe niso identične. Če so uredniki ali moderatorji v razmerju do lastnika spletne strani v podobnem položaju kot novinarji in uredniki do medijske hiše, ob upoštevanju 147. člena OZ neposredni zahtevek zoper njih ni mogoč (izjema je naklepna povzročitev škode, kar pa je redkost). Ni razloga, da bi bilo anonimno komentiranje na internetu pravno mileje obravnavano kot na primer pisma bralcev. To še posebej velja, če identitete anonimnega komentatorja sploh ni dopustno razkriti. Ravno k temu (anonimnosti komentatorjev) namreč bistveno prispeva uredniška in siceršnja vsebinska politika lastnikov spletnih strani, zato naj tudi nosijo tveganje za odgovornost za škodo.

Drži, da bi takšna razmeroma stroga odgovornost bistveno vplivala na poslovne modele na spletu in bi lahko celo povzročila ukinitev mnogih portalov in forumov, ki temeljijo na (anonimnem) komentiranju.[49] Ekonomska neupravičenost (spletna podjetja bi se odgovornosti lahko razbremenila le, če bi pred objavo pregledovala celotno vsebino, ki jo prispevajo uporabniki) in dejanska nemožnost predhodnega pregledovanja množice komentarjev sta najpogostejša argumenta proti strožji odgovornosti spletnih ponudnikov. A vendar je prepričljiv tudi protiargument: kdor želi imeti korist od vsebin uporabnikov, naj zanje tudi odgovarja.

[49] Vse bolj razširjeni so portali, na katerih potrošniki ocenjujejo različne izdelke, storitve in v zadnjem času tudi osebe – na primer zdravnike, učitelje … Berlinsko sodišče je odločilo, da se morajo javni kritiki izpostaviti tudi visokošolski učitelji. Na spletnem portalu MeinProf.de so lahko (tudi anonimni) uporabniki ocenjevali svoje profesorje, pri čemer je bil tožnik označen za psihopata. Na prvi stopnji je s prepovednim zahtevkom uspel (čeprav je upravljavec spletne strani komentar na zahtevo tožnika nemudoma izbrisal), na drugi pa je sodišče zahtevek zavrnilo z obrazložitvijo, da ne obstaja splošna dolžnost vnaprejšnega pregledovanja komentarjev, zaradi česar tudi ni dopusten pavšalen prepovedni zahtevek, naperjen zoper vse kritične komentarje; http://www.lawblog.de/index.php/archives/2007/06/04/lg-berlin-keine-globale-haftung-fur-kommentare/.

3. Sklep

Možnih rešitev problema anonimnega komentiranja je več. Za začetek bi država morala omogočiti posebno tožbo, s katero bi prizadeti posameznik lahko zahteval razkritje identitete anonimnega uporabnika. S tem bi se takoj povečala pravna varnost in oškodovančeve možnosti za civilnopravno varstvo. Mislim, da bi tudi upravljavce spletnih strani (tiste, ki so odgovorni za vsebino in niso zgolj tehnični posredniki internetnih storitev) morali zavezati k večji skrbnosti pri »izkoriščanju« anonimnih uporabniških komentarjev. To lahko sicer stori sodna praksa, a se bojim, da bi se rezultati pokazali šele po daljšem času. Zato bi bilo verjetno bolj učinkovito, če bi preprosto določili, da za anonimne komentarje objektivno odgovarja upravljavec spletne strani (se šteje za njihovega avtorja). To bi v praksi povzročilo, da bi uredniki vsaj anonimne komentarje morali pregledovati redno in še pred objavo. Prepričana sem, da bi priljubljenost žaljivega anonimnega komentiranja ob takšnih ukrepih hitro skopnela.

Literatura

Cerar, Matej: Odgovornost novičarskega portala za komentarje bralcev, *Pravna praksa,* št. 44/2013, str. 22.

Damjan, Matija: Odškodninska odgovornost internetnih posrednikov, *Pravni letopis,* Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani, 2010, str. 139–155.

Grčar, Cene: Koliko je vredna svoboda izražanja, *Pravna praksa,* št. 37/ 2009, str. 6–8.

Klipšteter, Tomaž, Petkovič, Blaž: Smrad na internetu, 1. 6. 2013, Objektiv, *Dnevnik.* Dostopno na http://www.dnevnik.si/objektiv/v-objektivu/smrad-na-internetu1.

Lemut Strle, Rosana: Osebnostne pravice proti internetni anonimnosti, *Pravna praksa,* št. 38/2009, str. 13–15.

Motl, Andrej: *Sovražni govor v slovenskih medijih na spletu,* FDV, Ljubljana 2009.

Samaluk, Barbara: Slovenija: Pomen regulacije sovražnega govora na internetu, dostopno na http://blog.eun.org/insafe/2006/02/slovenija_pomen_regulacije_sov.html.

Tekavc, Janez: Odškodninska odgovornost novinarjev in medijev, *Pravna praksa,* št. 19/2001, str. XVIII–XX.

Teršek, Andraž: Svoboda medijev in varstvo zasebnosti: kritika dveh precedensov, predlog razvrstitve »javnih oseb« in predlog ustavnopravnih standardov, v: *Izbrane teme civilnega prava:* zbornik Inštituta za primerjalno pravo pri Pravni fakulteti v Ljubljani, Ljubljana: Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani, 2006, str. 111–134.

Velkaverh, Aleš: Kolizija med pravico do zasebnosti in svobodo (rumenega) tiska, *Pravna praksa,* št. 42-43/2013, str. 27.

Zidar Klemenčič, Nina: Odstranitev bloga na podlagi sodbe sodišča, *Pravna praksa,* št. 48/2006, str. 14–15.

Zidar Klemenčič, Nina: Prepovedni zahtevek po 134. členu OZ – učinkovito varstvo osebnostnih pravic pred neupravičenimi posegi medijev?, *Pravna praksa,* št. 41-42/2006, str. 7–9.

Nekateri pravni vidiki spletnega oglaševanja (posebej zavajajočega)

dr. Peter Grilc

1. Uvod

Če razdelimo problematiko oglaševanja na groba obdobja, ki ne sledijo uveljavljenim zgodovinskim ali pravnim zgodovinskim metodologijam, že iz zgodnjega obdobja, 3000 let pred našim štetjem, poznamo kričače, ki so jih najemali babilonski trgovci, iz antičnega Rima pa obvestila na mestnih zidovih. V srednjem veku so oglaševali storitve in blago zlasti ustno, a so se trgovci že promovirali tudi z zapisi na karticah. Iz leta 1625 poznamo prve publikacije z oglasi in tedenske novice trgovcev. Začetek pravega, sistemskega oglaševanja sega v dobo industrializacije, ko se je razbohotilo oglaševanje v časopisih in je nastalo razmerje med oglaševalcem kot naročnikom in medijem. S pojavom elektronskih medijev, zlasti televizije, je oglaševanje prestopilo v nove medije, v sredini sedemdesetih let je domala vsaka televizijska postaja imela splošne oglasne bloke ali vrinjene bloke med rednim programom. V tem obdobju je nastala tudi potreba po nadzoru nad nedopustnimi praksami.

Svetovni splet je prinesel vrsto novih oglaševalskih praks, interaktivnost, razširil je možnosti za sodelovanje adresata oglasov. Omenimo le oglaševanje na spletnih straneh, ki omogoča ponudniku oglaševanje korporacijske identitete, ponuja informacije o izdelkih, omogoča primerjavo med posameznim izdelkom tega ponudnika in drugimi izdelki istega ponudnika ali drugih ponudnikov. Omogoča iskanje, stike s potrošniki, predpogodbeno in popogodbeno podporo kupcem, direktno prodajo, beleženje obiskanosti in s tem merjenje raznovrstnih marketinških in drugih parametrov ipd.[1] Druge možnosti so uporaba spletnih pasic na straneh iskalnikov ali drugje, oglaševanje prek brskalnikov (zlasti povezave na druge spletne strani), s pomočjo orodij ali strategij, ki posameznega ponudnika dvigujejo na lestvici zadetkov proti vrhu strani. Možnosti so tudi vrinjeni oglasi, utripajoči, le nekajsekundni oglasi, spletni iskalniki, ki so poleg spletnih strani ponudnikov ali spletnih strani tistih, ki združujejo ponudbe, močno ogla-

[1] Lesperance, Legal aspects of advertising on the internet, http://www.docstoc.com/docs/83387257/Legal-Issues-in-Internet-Advertising, str. 2.

ševalsko orodje na spletu, oglaševanje v novičkarskih skupinah, sponzoriranje spletnih strani, oglaševanje na zasebnih blogih, oglaševanje prek nenaročene elektronske pošte in elektronskih oglaševalskih tabel[2] ter spletne nagradne igre kot oglaševalsko orodje za pridobivanje kupcev.

Svetovni splet ni trčil le ob problematiko oglaševanja, temveč tudi ob vrsto drugih pravnih področij, s katerimi pa se ta prispevek ne ukvarja, na primer mednarodno zasebno pravo (čezmejno oglaševanje in problem relevantnega prava ter sodne pristojnosti), avtorsko pravo, pravo omejevanja konkurence, pogodbeno pravo, pravo varstva potrošnikov,[3] pravo osebnostnih pravic, kazensko pravo, upravno pravo, pravne ureditve različnih reguliranih trgov (od finančnih instrumentov, bančništva, zavarovalništva do dobave in distribucije energentov in posameznih reguliranih izdelkov, na primer kemičnih, farmacevtskih, živil).[4]

2. Primernost splošne ureditve za oglaševanje na spletu

Zaradi razvoja in stalnega širjenja oglaševalskih tehnik prek svetovnega spleta je neizogibno vprašanje, ali je obstoječi zakonodajni instrumentarij, osredinjam se zlasti na pravo zatiranja nelojalne konkurence in pravo varstva potrošnikov, zadosten za odziv na mnogotere pojavne tehnike na svetovnem spletu.

Pri nedavnem empiričnem raziskovanju sem se sicer osredinil na normativno ureditev oglaševanja v slovenski zakonodaji na splošno. Z iskanjem v specializiranih pravnih bazah (Ius Info) in s pomočjo spletnih iskalnikov je bilo mogoče ugotoviti, da termine s koreni besed ogla* (*oglas, oglaševanje, oglaševati)* in reklam* (*reklama, reklamirati*)[5] med pomembnejšimi predpisi pokaže 24 zadetkov,[6] 35 pa je takih, ki so s problematiko vsaj oddaljeno povezani ali pa je pojem uporabljen v določenem kontekstu.[7]

---

[2] Sredstvo, na katerem po skupinah združujejo in usmerjajo ponujene izdelke podjetja, ki se ukvarjajo z direktno prodajo.

[3] Primerjaj Madon, Nelojalno oglaševanje pri spletnem trgovanju, Pravna fakulteta, Ljubljana, 2010.

[4] Primerjaj Radej, Oglaševanje zdravil, medicinskih pripomočkov in »zdravih živil«, Pravna fakulteta, Ljubljana 2001; Jurišić; Pravno varstvo v oglaševanju »zdravih« živil, Pravna fakulteta, Ljubljana, 2007; Slovenec, Varstvo potrošnika pri kupovanju živil v EU, Pravna fakulteta, Ljubljana, 2013.

[5] Starejša in z vidika teorije oglaševanja manj primerna terminologija, ki izhaja iz francoskega termina reclamér (kričati), kar ni bistvo sodobnega oglaševanja. Njegovo bistvo je sporočanje, komunikacija, obveščanje ipd.

[6] ZVK, ZVPot, ZVPNPP, ZMed, ZPOmK, ZOUTI, ZZMP, ZKozP (kozmetika), ZZdr (zdravila), ZKem (kemikalije), ZJG (javna glasila), ZOdv (odvetništvo), ZSpo (šport), ZPSto (poštne storitve), ZZVR (zdravstveno varstvo rastlin), ZIL, ZASP, ZZUZIS (zdravstvena ustreznost živil in izdelkov ter snovi, ki prihajajo v stik z živili), ZPotK, ZPSPD (predhodne sestavine za prepovedane droge), ZVolK, ZJN, ZJC, ZKmet, Zakon o ratifikaciji Evropske konvencije o čezmejni televiziji.

[7] ZRTVS, KZ, CZ, ZTVP, ZISDU, ZPSPID, OZ, ZZavar, ZVCP, ZIS, ZDDPO, ZIZ, ZPD, ZDDV, ZLet, ZGSH, ZMZPP, ZON, ZOSRL, ZMR, ZZP, ZZODPM, ZAGA, ZPDZC, ZPPŽP, ZUT, ZKL,

Zakonodaja je torej obsežna in raznolika. Z generalno klavzulo v Zakonu o varstvu konkurence (ZVK) je na prvi pogled tudi dovolj abstraktna in z vsakokratno opredelitvijo dobrih poslovnih običajev, ki se spreminjajo v času in prostoru, ob inteligentni uporabi lahko v praksi zajame najmodernejše oglaševalske tehnike, torej tudi vedno nove, uveljavljene prek svetovnega spleta. S pravnim varstvom v ZVK[8] in Obligacijskem zakoniku (OZ) prek ZVK[9] lahko pokriva skoraj vsa področja. Podobne rezultate omogočata primerjalnopravna ureditev in praksa.[10] Tudi pravo varstva potrošnikov vsebuje nekaj specialnih določb, ki se nanašajo na splet. Tako so storitve informacijske družbe tiste gospodarske dejavnosti, ki se izvajajo prek svetovnega spleta oziroma interneta in vključujejo prodajo storitev in blaga na podlagi sklepanja pogodb prek svetovnega spleta oziroma interneta ter brezplačne storitve, kot so posredovanje podatkov in oglasna sporočila, če ni drugače urejeno.[11] Podjetje lahko v pisnih sporočilih, ki niso namenjena individualno določenemu potrošniku, uporablja tudi skrajšano firmo, če je s skrajšano firmo vpisano v register, in kraj, kjer posluje, ali naslov spletnih strani, če je iz njih nedvoumno razvidna identifikacija podjetja,[12] pri prodaji na daljavo pa je treba med sredstva za komuniciranje na daljavo šteti svetovni splet oziroma

ZRPSJ, ZPCP, vrsta zakonov o ratifikacijah konvencij (na primer o vzajemnih posebnih ugodnostih za določena vina, aromatizirane alkoholne pijače, o poenotenju nekaterih pravil za letalski prevoz, o izogibanju dvojnega obdavčenja, o gospodarskem sodelovanju, o mednarodnem cestnem prometu, o letalskem prometu, o začasnem uvozu).

[8] Po prvem odstavku 26. člena lahko prizadeti udeleženec v prometu blaga ali storitev na trgu s tožbo v pravdnem postopku zahteva prepoved nadaljnjih dejanj nelojalne konkurence, uničenje predmetov, s katerimi je bilo storjeno dejanje nelojalne konkurence, in vzpostavitev prejšnjega stanja, če je to mogoče. Če je bilo dejanje nelojalne konkurence storjeno s sredstvi javnega obveščanja ali na podoben način ali je dejanje prizadelo veliko udeležencev, lahko prizadeti udeleženec po drugem odstavku zahteva tudi objavo sodbe v sredstvih javnega obveščanja.

[9] Po 27. členu ZVK sme tisti, ki mu je bila z dejanji, ki so po tem zakonu nedopustna, storjena škoda, zahtevati odškodnino po pravilih obligacijskega prava (po 131. členu OZ, po katerem je tisti, ki povzroči drugemu škodo, to dolžan povrniti, če ne dokaže, da je škoda nastala brez njegove krivde).

[10] Primerjaj člen 1382 Code civil (F), člen 2598 CC, Pariško konvencijo o varstvu industrijske lastnine, ki sicer uvršča nelojalno konkurenco med kategorije industrijske lastnine, in doktrino »*passing-off*« v anglosaškem pravu: *Passing off is available where there is a prospect of confusion of identity through (i) the unauthorised use of similar marks or (ii) get up, and such use damages, or (iii) is likely to damage the goodwill and reputation of a business. Unregistered marks and passing off can apply to virtually any name, mark, logo or get-up which distinguishes a company, business, product or service.* Case of Reckitt & Colman Ltd v Borden Inc [1990] 1 RPC1 341 1 (the Jif Lemon case) – pogoji Lorda Oliverja za uspešno tožbo na passing off: *a successful plaintiff must establish, as follows (i) he must establish a goodwill or reputation attached to the goods or services ...; (ii) he must demonstrate a misrepresentation by the defendant to the public (whether or not intentional) leading or likely to lead the public to believe that the goods or services offered by him are goods or services of the plaintiff ... (iii) he must demonstrate that he suffers [loss or damage as a consequence of the erroneous belief that the goods or services of the defendant are the goods or services of the plaintiff].*

[11] Glej deseti odstavek 1. člena ZVPot.

[12] Primerjaj tretji in četrti odstavek 2. člena ZVPot.

internet.[13] Zakonodajno urejene in v sodni praksi, zlasti v tuji, ki jo je mogoče navajati kot referenco zaradi primerjalnopravno podobne ureditve in pristopa, so dovolj dobro obravnavane tudi posamezne pojavne oblike oglaševanja. Predvsem prek prava zatiranja nelojalne konkurence in zaradi odprtosti generalne klavzule v 13. členu ZVK (z aktualizacijo standarda dober poslovni običaj) jih je mogoče uporabiti tudi za oglasne pristope na svetovnem spletu.

Pri tem imam poleg najbolj klasičnih oblik oglaševanja[14] v mislih zlasti:

- neresnično oglaševanje,
- oglaševanje z zlorabo potrošnikov,
- očrnjevanje,
- superlativno oglaševanje,
- prikrito oglaševanje in oglaševanje iz zasede *(ambush),*
- primerjalno oglaševanje (brez natančnejše analize opozarjam le na določbo 12.c člena Zakona o varstvu potrošnikov – ZVPot),
- nedostojno oglaševanje – po 12.a členu ZVPot je nedostojno oglaševanje blaga in storitev oglaševanje, ki vsebuje sestavine, ki so žaljive ali bi lahko bile žaljive za potrošnike, bralce, poslušalce in gledalce, ali sestavine, ki nasprotujejo morali,
- trditve »*so what*«, kot trditve, ki so navedbe dejstev, a hkrati trdijo, da konkurentovi izdelki ne ponujajo tega ali ne dosegajo potrošnikovih normalnih pričakovanj (Primer: »*Pijača vsebuje pomarančni sok, ki ima dodan kalcij.*« Vprašanje: Ali res potrebujemo več kalcija, kot ga zagotovi tak sok? Ali ga konkurenca nima?),

[13] Primerjaj tretji odstavek 43. člena ZVPot.

[14] Metodološko po 13. členu ZVK: neresnično oglaševanje, zavajajoče oglaševanje (reklamiranje, oglašanje ali ponujanje blaga ali storitev z navajanjem neresničnih podatkov ali podatkov in izrazov, ki ustvarjajo ali utegnejo ustvariti zmedo na trgu ali z zlorabo nepoučenosti ali lahkovernosti potrošnikov); neresnično oglaševanje (reklamiranje, oglašanje ali ponujanje blaga ali storitev z navajanjem podatkov ali uporabo izrazov, s katerimi se izkorišča ugled drugega podjetja, njegovih proizvodov ali storitev oziroma ocenjuje ali podcenjuje kvaliteto proizvodov drugega podjetja); oglaševanje z omalovaževanjem in diskriminacijsko oglaševanje (reklamiranje, oglašanje ali ponujanje blaga ali storitev ali omalovaževanje drugega podjetja s sklicevanjem na narodnostno, rasno, politično ali versko pripadnost); prodaja blaga z označbami ali podatki, ki ustvarjajo ali utegnejo ustvariti zmedo glede izvora, načina proizvodnje, količine, kakovosti ali drugih lastnosti blaga; oglaševanje navidezne razprodaje ali navideznega znižanja cen in podobna dejanja, ki zavajajo potrošnike glede cen; neupravičena uporaba imena, firme, znamke ali kakšne druge oznake drugega podjetja, ne glede na to, ali je drugo podjetje dalo soglasje, če se s tem ustvari ali utegne ustvariti zmeda na trgu; premijski posli (pridobivanje kupcev blaga ali uporaba storitev z dajanjem ali obljubljanjem nagrad ali kakšne druge premoženjske koristi ali ugodnosti, ki po vrednosti občutneje presega vrednost blaga ali storitve, s katero naj kupec pridobi možnost nagrade).

- majave trditve – trditev je majava, če je nejasna in je ni mogoče preveriti (Primer: »*Najboljše, kar lahko dobite.*«),
- trditve s pričevanjem (*testimonials*); uporaba znanih oseb ali prizorov, ki naj služijo kot vzor potrošniku (Primer: »*Tudi ti imaš lahko tako telo kot jaz.*« Sledi podpis znane osebe, vzornika ipd.),
- uporaba vprašljive statistike ali nepreverjene trditve (Primer na spletni strani: »*Višje ravni* vitamina B6 in B12 za podporo vašemu zdravju.*« Na dnu strani je navedba: »**Te trditve niso preverjene pri pristojnih zdravstvenih organih. Izdelek ni namenjen za diagnosticiranje, zdravljenje ali preprečevanje bolezni.*«),
- igranje na pamet, pretkanost potrošnika (na primer oglas, ki potrošnika napelje na prepričanje, da je on boljši, ker bo izbral ta izdelek: »*Izbirčne mame izberejo izdelek X.*« Ali: »*Najboljše gume na svetu imajo velik napis XYZ.*«),
- agresivne poslovne prakse:[15] za internetno oglaševanje relevantna ureditev, a v manj primerih (agresivne poslovne prakse, ki v vseh okoliščinah veljajo za nepoštene),[16]
- šokantno oglaševanje (ne z normo, pač pa prek sodne prakse, ki pa v odločbah, zlasti na višjih instancah v primerjalnem pravu, sooča pravo zatiranja nelojalne konkurence, pravo osebnostnih pravic, svobodno gospodarsko pobudo, svobodo govora in ožje podjetniške komunikacije),[17]
- suženjsko posnemanje,[18]
- diskriminacija med spoloma,[19]

---

[15] Agresivna praksa po Zakonu o varstvu potrošnikov pred nepoštenimi poslovnimi praksami – ZVPNPP (8. in 9. člen).

[16] Med primeri agresivne prakse po 10. členu je več takih, ki so relevantni tudi za poslovanje prek spleta; primerjaj tiste, ki so navedeni v *3., 5., 6., 7. in 8. alineji.*

[17] Obširna literatura (na primer http://scholar.google.si/scholar?hl=sl&q=schockierende+werbung &btnG=), zato le nekaj omemb: Grilc, Šokantna reklama – med etiko, moralo in komercialnostjo, Zbornik znanstvenih razprav, 1996, letnik 56, str. 97–120; Wünnenberg, Schockierende Werbung – Verstoß gegen § 1 UWG? Europäische Hochschulschriften, European University Studies, Publications Universitaires Européennes, Volume 1858, 1996; Classen, Die wettbewerbs- und verfassungsrechtliche Beurteilung produktunabhängiger Wirtschaftswerbung, Darstellung am Beispiel der Benetton-Rechtsprechung des BGH und BVerfG, Beck, 2006.

[18] Primerjaj oglase dveh različnih proizvajalcev fotografskih stativov, družb Manfrotto in Canon, z vrsto slikovnih objav na spletu; glej tudi original na naslovu http://www.youtube.com/watch?v=2Bb8P7dfjVw in zatrjevano suženjsko posnemanje ali parodijo na http://www.youtube.com/watch?v=9bnRi3BnR4E.

[19] Primerjaj http://www.adweek.com/video/sexist-ads-mercedes-133388; ali oglas za kuhinjske mešalnike s sliko ženske in moškega in napisom: »*The chef does everything but cook – that's wifes are for.*«; ali http://imgur.com/r/pics/rmb6X; ali oglas za avto s sliko prestrašene voznice in napisom: »*The Mini Automatic. For simple driving.*«; ali serija oglasov za proizvajalca ur premijskega razreda z napisi: (i) »*Fast so kompliziert wie eine Frau. Aber pünktlich.*« (ii) »*Fast so schön wie eine Frau. Is aber leichter zu tragen.*« (iii) »*Fast so schön wie eine Frau. Redet aber nicht.*« (iv) »*Fast so schön wie eine Frau. Liegt aber auch nach Jahren noch gut in der Hand.*«

- zavajajoče oglaševanje, ki je po normativni definiciji zavajajoče glede obstoja ali narave izdelka; glede glavnih značilnosti izdelka, na primer njegove razpoložljivosti, prednosti, tveganj, izvedbe, sestave, dodatkov, poprodajnih storitev za potrošnike in obravnavanja pritožb, postopka in datuma izdelave ali dobave, dostave, primernosti za namen, uporabe, količine, specifikacije, geografskega ali tržnega porekla ali rezultatov, ki se lahko pričakujejo od njegove uporabe, ali rezultatov in stvarnih značilnosti preizkusov ali pregledov izdelka; glede obsega obveznosti podjetja, motivov za uporabo določenih poslovnih praks in narave prodaje, kakršne koli izjave ali znaka v povezavi s posrednim ali neposrednim sponzorstvom ali odobritvijo podjetja ali izdelka; glede cene ali načina izračunavanja cene ali določene cenovne prednosti; glede potrebe po storitvi, nadomestnem delu, zamenjavi ali popravilu; glede narave, lastnosti in pravic podjetja ali njegovega zastopnika, na primer njegove identitete in premoženja, kvalifikacij, statusa, odobritve, članstva ali povezav ter imetništva pravic intelektualne lastnine ali nagrad in priznanj, ki jih je prejel; glede pravic, ki jih ima potrošnik v skladu z zakonom, ki ureja varstvo potrošnikov, vključno s pravico do zamenjave blaga, vračila kupnine, garancije, stvarnih napak in nepravilno opravljenih storitev ali drugih tveganj, s katerimi se lahko sreča. Poslovna praksa se šteje za zavajajočo tudi, če v konkretnem primeru ob upoštevanju vseh njenih značilnosti in okoliščin povzroči ali bi utegnila povzročiti, da povprečen potrošnik sprejme odločitev o poslu, ki je sicer ne bi sprejel, in vključuje: (i) kakršenkoli način trženja izdelka, vključno s primerjalnim oglaševanjem, ki ustvarja zmedo zaradi zamenjave s kakršnimkoli drugim izdelkom, znamko, trgovskim imenom ali drugim znakom razlikovanja konkurenta; (ii) kršitev kodeksa, za katerega se je podjetje zavezalo, da ga bo spoštovalo, če pri zavezi ne gre zgolj za namero, temveč za trdno zavezo, ki jo je mogoče preveriti, in podjetje v okviru določene poslovne prakse navaja, da ga zavezuje kodeks.[20] Zavajajoče oglaševanje je lahko eksplicitno,[21] v praksi je potrjeno, da je nedopustno zavajanje glede stroškov ali plačila,[22] glede učinkov,[23] v zvezi z rabati,[24] da je lahko

[20] Primerjaj 5. člen ZVPNPP.

[21] Na primer: (i) Slika ženske z napisom *»Pleasure to Burn.«* Gre za implikacijo, da je cigareta ključna za navezovanje intimnih razmerij z žensko. (ii) Neposredni nagovor mladih žensk s strani samostojne in samozavestne osebe z eksplicitnim sporočilom, da kajenje vodi v neodvisnost.

[22] Na primer oglas z besedilom: *»No More Late Fees.«* (Po osmih dneh se potrošniku zaračuna polna cena na kreditni kartici; če vrne film v 30 dneh, se mu odračuna polna cena filma, še vedno pa se mu zaračunajo stroški skladiščenja; po 30 dneh ni nikakršnega nadomestila.)

[23] Sporočilo: »... *takojšnje olajšanje ob glavobolu ...*«, niso pa objavljene študije, po katerih bi sestavine to omogočile. Rezultat oglasa: pet milijonov prodanih zavojčkov v 11 mesecih.

[24] Oglašuje se rabat, a v drobnem tisku je navedba, da velja le omejen čas ali da ni vračila denarja pod določenimi pogoji.

zavajajoča promocijska ali vstopna ponudba[25] ali predstavitev,[26] zavajanje z nedokončanimi nagovori,[27] zavajanje s trditvami o edinstvenosti,[28] zavajanje z navajanjem dejstev,[29] implicitno ali z opustitvijo resnice.[30] Navajam določbo 7. člena ZVPNPP, saj izčrpno navaja primere zavajajočih praks, ki v vseh okoliščinah veljajo za nepoštene. S tem želim le ilustrirati, kako široko in eksplicitno je zastavljena zakonodaja, ki na prvi pogled pokriva vse pojavne oblike zavajajočega oglaševanja. Za tako prakso gre vedno, če podjetje: trdi, da je podpisnik kodeksa ravnanja, čeprav ni; prikazuje znak zaupanja, kakovosti ali podobno, ne da bi za to pridobilo ustrezno dovoljenje; trdi, da je kodeks ravnanja odobrila javna ali druga organizacija, čeprav to ni res; trdi, da izpolnjuje pogoje za pridobitev ustreznega dovoljenja ali da je za podjetje (vključno z njegovimi poslovnimi praksami) ali za izdelek izdal ustrezno dovoljenje javni organ ali druga organizacija, čeprav to ni res; vabi k nakupu izdelkov po določeni ceni, ne da bi razkrilo, da obstajajo utemeljeni razlogi, zaradi katerih ne bo moglo zagotoviti dobave določenih izdelkov ali njim enakovrednih izdelkov po navedeni ceni, za ustrezno obdobje in v ustreznih količinah glede na izdelek, obseg oglaševanja izdelka in ponujeno ceno, ali ne bo moglo zagotoviti, da bi izdelke pod pogoji iz prejšnje alineje zagotovilo drugo podjetje (»*bait*« oglaševanje); vabi k nakupu izdelkov po določeni ceni, pa potrošnikom ne pokaže izdelka, ki se oglašuje, ali noče sprejeti naročil zanj ali ga dostaviti v razumnem času ali pokaže vzorec z napako z namenom pospeševati prodajo drugega izdelka (tehnika »*bait-and-switch*«); lažno zatrjuje, da bo izdelek na voljo zelo omejen čas ali da bo na voljo samo pod posebnimi pogoji zelo omejen čas, da bi tako potrošnika napeljalo k takojšnji

[25] Na primer navedba v besedilu, da komitent ne bo imel letnih stroškov, da bo nekaj transakcij brezplačnih in da bo prejel dobropis za znesek, ki presega določeno vsoto; dejansko transakcije niso bile brezplačne.

[26] Oglaševalec oglašuje, naj potrošnik kupi zdravilo, ker je odobreno (na primer s strani pristojnega urada za zdravila), dejstvo pa je, da v državi ni dopustno prodajati zdravil brez dovoljenja; trditev je sicer resnična, a zavajajoča, ker povzroča napačno predstavo, da druga zdravila niso dobila dovoljenja.

[27] Nagovor oziroma trditev pušča manevrski prostor za samospraševanje potrošnika, na primer slogan: *Bodite prvi, ki boste vedeli.* Sodišče se vpraša: *Vedeli kaj*?

[28] Oglašuje se edinstvenost proizvoda, a to ne pomeni nujno, da je proizvod boljši od drugih.

[29] Oglas: *Pivo X, naravno pivo, iz žitnih zrn in vode.* Vsako pivo je zvarjeno iz teh sestavin, zato trditev ne pove nič in ne prikaže prednosti pred drugimi izdelki.

[30] Po abstraktni definiciji zavajajoče oglaševanje pomeni vsako oglaševanje, ki na kakršenkoli način, vključno s predstavitvijo blaga in storitev, zavaja ali utegne zavajati potrošnika, ki mu je oglaševanje namenjeno ali ga lahko doseže in ki bi zaradi svoje zavajajoče narave verjetno vplivalo na ekonomsko obnašanje potrošnika ali ki iz enakih razlogov škodi ali bi verjetno škodilo konkurentom. Tako zavajajoče oglaševanje je zlasti oglaševanje, ki izkorišča ali bi lahko izkoriščalo potrošnikovo neizkušenost in neznanje v dobičkonosne namene, ki vsebuje nejasnosti, čezmerno pretiravanje ali druge podobne sestavine, ki potrošnika zavajajo ali bi ga lahko zavajale (12.b člen ZVPOt).

odločitvi in ga prikrajšalo za možnost ali čas, za izbiro na podlagi informacij; se obveže, da bo potrošnikom, s katerimi se je pred sklenitvijo posla sporazumevalo v jeziku, ki ni uradni jezik države članice, v kateri ima podjetje sedež, zagotavljalo poprodajno storitev, potem pa to storitev ponuja izključno v drugem jeziku, ne da bi bili potrošniki na to jasno opozorjeni, preden so se zavezali k sklenitvi posla; izjavi ali sicer ustvari vtis, da se izdelek lahko zakonito prodaja, čeprav to ni res; pravice, ki jih imajo potrošniki po zakonu, predstavlja kot posebnost ponudbe; uporabi programske vsebine medijev za promocijo izdelka in samo plača tako promocijo, ne da bi bilo to jasno označeno v vsebini, slikah ali zvokih, ki jih potrošnik z lahkoto prepozna (ta določba ne posega v določbe zakona, ki ureja področje medijev); navaja vsebinsko netočno trditev glede narave in obsega tveganja za osebno varnost potrošnika ali njegove družine, če potrošnik ne kupi izdelka; izdelek, ki je podoben izdelku drugega proizvajalca, predstavlja tako, da namerno zavaja potrošnika v prepričanje, da je izdelek proizvedel ta proizvajalec, čeprav to ni res; ustanovi, vodi ali spodbuja piramidni sistem pospeševanja prodaje, pri katerem si potrošnik obeta plačilo ali nagrado predvsem zato, ker je v sistem uvedel nove potrošnike, ne pa toliko zaradi prodaje ali uporabe izdelkov; trdi, da bo v kratkem prenehalo z dejavnostjo ali preselilo poslovne prostore, čeprav tega ne namerava storiti; trdi, da lahko izdelki pripomorejo k zmagi v igrah na srečo; lažno zatrjuje, da lahko izdelek pozdravi bolezni, motnje v delovanju organov ali telesne hibe; daje bistveno netočne informacije o tržnih pogojih ali o možnostih, da se izdelek najde, da bi tako napeljalo potrošnika k nakupu izdelka pod pogoji, ki so manj ugodni kot običajni tržni pogoji; v okviru poslovne prakse trdi, da se razpisuje nagradno tekmovanje ali da je mogoče prejeti promocijsko nagrado, ne da bi se napovedane nagrade ali ustrezna nadomestila tudi dejansko razdelile; izdelke označi kot »gratis«, »zastonj«, »brezplačno« ali podobno, če mora potrošnik plačati kakršenkoli strošek, razen neizogibnih stroškov, nastalih, ker se je odzval na poslovno prakso, kot so stroški prevzema ali dostave izdelka; v marketinško gradivo vključi račun ali podoben dokument za plačilo, ki daje potrošniku vtis, da je že naročil izdelek, ki se oglašuje, čeprav tega ni storil; lažno zatrjuje ali daje vtis, da ne deluje za namene, ki so povezani z njegovo trgovsko, poslovno, obrtno dejavnostjo ali svobodno poklicno dejavnostjo, ali se lažno predstavlja za potrošnika; ustvarja lažen vtis, da so poprodajne storitve za izdelek na voljo v državi članici, ki ni tista, v kateri se izdelek prodaja.[31]

[31] Nekaj primerov iz prakse: (i) zavajanje proizvajalcev cementa glede uporabe lesa v gradnji: http://www.treehugger.com/green-architecture/canadian-concrete-companies-running-deceptive-ad-campaign-against-wood-construction-2.html; (ii) odškodnina zaradi zavajajočega oglaševanja – *FTC proti Reebok International Ltd.* (US Distr. Court for the Northern District of Ohio, FTC No. 102 3070);

Na področju subliminalnega oglaševanja pravna stališča niso povsem izčiščena oziroma so redka. Zakonodaja in praksa pa varujeta posamezne skupine ljudi (starejši, bolniki, otroci) in druga živa bitja (na primer varstvo živali, ki so bile prikazane v vrsti oglasov, za katere je očitno, da so neetični oziroma v nasprotju z dobrimi poslovnimi običaji),[32] ter sta pozorni na oglase z elementi nasilja in prepovedane oblike oglaševanja posameznih izdelkov. Pri posameznih izdelkih (tobak, alkohol[33]) pokrivata tudi posredne oblike oglaševanja[34] in morebitne obvode v praksi,[35] ki pa jih je mogoče obravnavati tudi na podlagi generalne klavzule ali doktrine *passing-off*.

3. Samoregulacija

V tem delu se le dotikam pojma in pomena samoregulative oziroma avtonomnih virov v gospodarskem pravu, posebej v pravu nelojalne konkurence in pri oglaševanju. Samoregulacija pomembno dopolnjuje državno ali nadnacionalno normativno urejanje. Samoregulacija je način normodaje, s katerim poklicna ali interesna skupina ali organizacija zasebnega prava uredi in s tem tudi promovira svoje cilje tako, da sprejme in uporablja avtonomna zavezujoča pravila za poslovanje ali delovanje članov ali uporabnikov, ki vstopajo v sistem, prek članskega razmerja, z uporabo etičnih kodeksov, standardov ali navodil, disciplinskih postopkov, z organizacijo izobraževalnih programov in programov usposabljanja. Na področju oglaševanja velja posebej opozoriti na etične kodekse posameznih nacionalnih in mednarodnih združenj, ki se lahko uporabljajo samostojno, lahko pa s svojim etičnim nabojem omogočijo napolnjevanje abstraktnih standardov, v primeru oglaševanja, tudi na spletu, dobrih poslovnih običajev po 13. členu

---

Civil Action Number 1:11-cv-02046-DCN; poravnava na http://www.ftc.gov/os/caselist/1023070/index.shtm; oglas v zvezi z zadevo na http://www.ftc.gov/opa/2011/09/video/fitness.shtm; (iii) grafično popravljanje slikovnega materiala (http://www.youtube.com/watch?v=j6WF5v4Jhxs, http://www.youtube.com/watch?v=PRNvhGND7Kc). Pravno neproblematičen pa je, ne glede na to, da skoraj do konca ne razkrije, kateri izdelek oglašuje, oglas, ki močno pretirava glede moči sesalnika za prah, a je povprečni potrošnik sposoben zaznati, da gre za pretiravanje http://www.youtube.com/watch?v=zLLoiiFZFDo.

[32] Na primer oglasa za Fordov avtomobil Ka na spletnem naslovu http://www.youtube.com/watch?v=5dzi_8Rscfs; http://www.youtube.com/watch?v=xxSex9VxlwI; oglas za Umbro http://www.youtube.com/watch?v=hjc8f7LEB2s.

[33] Oglaševanje alkoholnih pijač ureja ZZUZIS (15. in 15.a člen).

[34] Primerjaj zlasti 10. člen Zakona o omejevanju uporabe tobačnih izdelkov – ZOUTI.

[35] Primer takega obvoda bi bila uporaba motivov, ki asociirajo na ime izdelka, ki ga sicer ni dovoljeno oglaševati, vendar v drugem kontekstu, če bi bila prikrita identiteta izdelka, ki ga ni dopustno oglaševati; primerjaj oglase za cigarete Silk cut, ki jih prikaže slikovno iskanje Google.

ZVK.[36] Po določbah Slovenskega oglaševalskega kodeksa je predmet presoje tudi oglaševanje v elektronskih medijih, vključno z oglaševanjem na internetu na za to zakupljenem spletnem oglasnem prostoru (na primer reklamne pasice, tekstovni oglasi, ….) in drugimi oblikami oglaševanja na nezakupljenem prostoru (tudi viralna oglaševalska sporočila prek e-pošte in drugih kanalov, video- in druge oglaševalske vsebine na portalih, ki so namenjeni druženju), ter vse druge vsebine, ki niso objavljene na spletnem mestu oglaševalca in za katere je mogoče trditi, da jih je objavil oglaševalec.[37] Kodeks vsebuje tudi specialna pravila.[38]

V oglaševanju je samoregulativa sistem, s katerim si oglaševalska industrija sama postavlja meje ustvarjalnega, a hkrati korektnega in družbeno odgovornega oglaševanja. V različnih državah je uveljavljena v različnih oblikah, vendar pa je bistveno načelo samoregulative vedno enako: oglaševanje naj bo zakonito, dostojno, resnično in nezavajajoče. Pripravljeno naj bo z občutkom odgovornosti do družbe in potrošnika ter z dolžnim spoštovanjem do pravil konkurenčnosti. Samoregulativa v spletni skupnosti je možnost uporabnikov, da preprečujejo objavo neprimernih vsebin na spletnem mestu ter izločajo uporabnike, ki objavljajo sporno vsebino oziroma ne upoštevajo vseh pravil skupnosti in s tem splošnih pogojev. Kolektivna zavest in odgovornost vseh uporabnikov in tudi posameznih uporabnikov torej omogoča izločitev posameznih prispevkov iz javno dostopnih knjižnic, izločitev zapisa ali pa blokado uporabnika in s tem uporabniškega računa tistemu, ki ne upošteva splošnih pogojev in objavlja sporno vsebino.[39]

Za samoregulacijo v oglaševanju, tudi spletnem, veljajo splošne ugotovitve o njenih prednostih in slabostih. Med prednostmi se omenja zlasti izraba pobude zasebnega sektorja, ki ima podlago v zaupanju (potrošnikov), ugledu in velikem tržnem deležu, kar ji daje kredibilnost. Prednost je tudi informacijska asimetrija, ko reguliranec vedno ve več od klasičnega zakonodajalca, prožnost, prilagojenost posebnim okoliščinam ali primerom, hitra uvedba tehnologije, ki je na voljo, zmanjševanje stroškov in visoka stopnja identifikacije (reguliranec je regulator). Med slabostmi je sindrom lisice v kokošnjaku, ki je povezan s poudarjenim in potenciranim ter potencialno zlorabljenim lastnim interesom osebe, ki postavlja

[36] Primerjaj Slovenski oglaševalski kodeks – SOZ; http://www.soz.si/uploads/slovenski_oglasevalski_kodeks.pdf.

[37] Niso pa predmet presoje po tem kodeksu: (i) mali oglasi, vključno z internetnimi; vendar pa je male oglase dopustno presojati, če sporočilo presega značaj malega oglasa in (ii) vsebine spletnih mest, razen tistih, ki so predmet presoje po tem kodeksu.

[38] Na primer 23.5., po katerem oglaševanje izdelkov za lepoto in zdravje ne sme vsebovati ponudbe za diagnosticiranje, svetovanje, predpisovanje po pošti (po pošti tu pomeni po telefonu, pošti, internetu, e-pošti ali faksu).

[39] Primerjaj Grilc, Samoregulacija gospodarskih razmerij in Obligacijski zakonik. *Pravni letopis* ..., 2012, str. 59–66.

samoregulacijska pravila, podnormiranost ali nadnormiranost. Kot slabost se omenja, da država s prepuščanjem področja samoregulaciji ali avtonomiji opušča zakonodajno pobudo in ustvarja vrzel v poznavanju problematike, kar lahko sistemsko vodi tudi prevrednotenje znanj v sistemu države. Med slabostmi so tudi: nevarnost, da sistem ne bo učinkovit, ker je dajanje pobud skrčeno na omejeno skupino pobudnikov, politična tveganja in izguba občutka za nadzor, prezrta kompleksnost sistema, samoregulacija kot protikonkurenčno orodje (kot orodje za zmanjševanje konkurenčnosti in/ali kot orodje za omejevanje konkurence) ter nevarnost izgube transparentnosti v postopku »uzakonjanja« samoregulativnih pravil. Zato ustvarjanje pravil avtonomnega gospodarskega prava ne sme biti stihijsko, temveč kontrolirano, lahko je dopolnilo pravnim zahtevam, zlasti s kodeksi za natančnejše urejanje sektorja, delovanje samoregulatorja (sektorja) in države pa mora biti načrtovano in usklajeno. Država je samoregulatorju ali ustvarjalcu avtonomnih pravil lahko partner, lahko je pobudnik, pospeševalec, zagotavlja lahko soglasje ali je vir sankcij ali zavrnitev, nujno pa mora izvajati monitoring ter mora biti sposobna zaznati in ovrednotiti (vse) dejavnosti samoregulatorja. Glede na navedeno je kontrolirana samoregulacija pristop, ki povečuje sposobnost sektorja. Samoregulacija je dopolnitev, ne pa nadomestek zakonske ureditve, in je lahko del strategije države, vendar to ni nujno lažji pristop, saj država kot normodajalec ne sme izginiti; biti mora selektivna, izvedena, učinkovita in strateška.[40]

4. Dinamika zadnjega obdobja

Pravo zatiranja nelojalne konkurence je osrednje orodje za reguliranje nelojalnega oglaševanja. Če ga opazujemo skozi optiko primerjalnega prava in unifikacijskih ter harmonizacijskih prizadevanj, je poudarjeno nacionalno (razlike med civilnopravnimi sistemi in sistemi *common law;* tri paradigme znotraj civilnopravnih sistemov – nemška, italijanska, francoska; različni nomotehnični pristopi: taksativno naštevanje, nelojalna konkurenca kot civilni delikt, urejanje prek generalne klavzule, urejanje prek doktrine *passing off*).

Tako ni evropskega (na ravni prava EU) konsenza o tem, (i) kaj je nelojalna konkurenca, (ii) kako se razume poštenost, etičnost, (iii) ali sprejeti splošno odškodninsko ali posebno konkurenčno načelo (iv) koga naj pravo zatiranja nelojalne konkurence varuje (le konkurente, le potrošnike, konkurente in potrošnike ter splošno javnost). Drugače je seveda, če oglaševanje presojamo skozi optiko prava varstva potrošnikov, ki je že precej harmonizirano.

[40] Prav tam.

Posledica le delne urejenosti je, da je harmonizacija prava zatiranja nelojalne konkurence (s tem oglaševanja, tudi prek spleta) le delna. Malo verjeten je tudi projekt enotne ureditve prava nelojalne konkurence. Na ravni mednarodnega (javnega) prava je nelojalna konkurenca skoraj v celoti izključena iz TRIPS, zanjo pa je uporaben člen 10 bis Pariške konvencije. Različne so tudi zgodovinske korenine in s tem posredno tudi položaj prava zatiranja nelojalne konkurence v nacionalnih sistemih.

Če analiziramo možnosti širše od okvira zatiranja nelojalne konkurence, je mogoče ugotoviti, da se je v zadnjem obdobju dopolnjevala medijska zakonodaja, ki je sledila cilju zagotavljanja večje konsistentnosti predpisov, tudi glede prikritega oglaševanja, sponzorstva in privilegiranih subjektov varstva. Na področju telekomunikacij in novih medijev je pričakovati razcvet zakonodaje, na področju prava varstva potrošnikov pa po oblikovanju in izčiščenju predpisov zmerno dopolnjevanje. Prav pri pravu varstva potrošnikov je še precej manevrskega prostora na področju oglaševanja, tudi spletnega. O tem pričajo uspešni projekti (direktive) o prepovedi zavajajočega in dopustitvi primerjalnega oglaševanja v sredini devetdesetih let prejšnjega stoletja. Na tem področju je vendarle pričakovati zmerno dopolnjevanje predpisov, zlasti glede regulacije potrošniških pogodb, nenaročene pošte ipd.

Smernice za ureditev v posameznih sektorjih (na primer hrana, farmacija, tobak, alkohol, zavarovalništvo, bančništvo) bodo določene z že precej podrobno sektorsko zakonodajo, ki se bo po pričakovanjih zmerno dopolnjevala.

Na področju oglaševanja se je natančno oblikovala sodna praksa, ne le v ožjih okvirih oglaševanja, pač pa tudi na področjih, ki lahko vplivajo nanj (na primer produktna odgovornost – tobak, farmacija), vendar zenit še ni dosežen.

Pričakovati je tudi zmeren napredek pri poenotenju gospodarskih pogodb in vedno večjo vlogo korporacijskih standardov, ki prehitevajo zakonodajalske (mejna koristnost). Pričakovati je krepitev varstva družbeno nemočnih in artikulacijsko in interesno manj sposobnih skupin, o senzibilizaciji družbe v zvezi s tem, kaj je dober poslovni običaj, pa se ne moremo izreči. Krepilo se bo tudi avtonomno urejanje, kar utegne biti posebej pomembno prav za splet in oglaševanje.

5. Sklepne ugotovitve

Oglaševanja na spletu ni treba niti ni mogoče obravnavati drugače kot oglaševanje v drugih medijih. Zakonodajni modeli in metodologije v primerjalnem pravu (taksativno naštevanje, generalna klavzula, civilni delikt, *passing-off*) so samostojno ali v kombinaciji (prepoved prek posebne konkurenčne ali sektorske zakonodaje in odškodninsko varstvo, mogoče je še dodano sklicevanje na pravice

intelektualne lastnine, kar postopek, zlasti dokazovanje, dodatno olajša) dovolj prožni za uspešno uveljavljanje varstva pred zavajajočim ali drugim nelojalnim oglaševanjem. Vrsto nelojalnih praks spletne možnosti potencirajo; izluščimo lahko vse, ki so povezane s konceptom *passing-off* (predstavljanje izdelka kot izdelka nekoga drugega, ponarejanje, pripenjanje na dobro ime uveljavljenega ponudnika ali znamke). Čeprav je koncept anglosaški, je mogoče enakovredno varstvo v kontinentalnih sistemih.[41] Posebna zakonodaja, ki se deloma ali v celoti posveča spletnim problemom, je že nastala, v prihodnosti pa je pričakovati njeno dopolnjevanje in ureditev področij, ki doslej niso bila urejena, zlasti v pravu varstva potrošnikov. Pomembno je tudi avtonomno urejanje področja.

[41] Primerjaj sodbo v zadevi *Zlatorog (Laško)/Kozorog* – III Ips 121/98, z dne 15. 10. 1998: »*Toženka je z uporabo besed Kozorog pivo v silhueti s kozorogom v ovalu s stiliziranimi gorami posnemala registrirane znamke tožeče stranke, s čimer je kršila te znamke v smislu določil drugega in tretjega odstavka 94. člena Zakona o industrijski lastnini (Uradni list RS, št. 13/92, 27/93, 34/97 in 75/97), po katerih »posnemanje obstoja, če povprečen kupec blaga ... lahko opazi razliko le, če je posebno pozoren ...«. Obravnavana kršitev predstavlja tipično posnemanje, ki zavaja kupce, da kupujejo proizvode tožeče stranke. Toženka uporablja tudi posnemajočo oznako Kozorog pivo na etiketi, ki je enako zelene barve in pravokotne oblike z značilnim robom, kot je etiketa tožeče stranke. Gre tedaj za izrazito vizualno podobnost.*«

Varstvo osebnih podatkov v spletnem okolju

dr. Maja Brkan

Personal data in today's world
is the currency of the digital market.
Viviane Reding[1]

1. Uvod

Varstvo osebnih podatkov je eno od področij, ki so v zadnjem času, predvsem z neustavljivim povečevanjem uporabe interneta in socialnih omrežij, pritegnila pozornost ne le pravnikov, temveč tudi širše javnosti. Afere v zvezi s prisluškovanjem mobilnemu telefonu nemške kanclerke Angele Merkel in kontroverzna razkritja Edwarda Snowdna dodatno opozarjajo na pomen tega področja v današnji informacijski družbi. Strah, na katerega nakazujejo slogan »Google ve vse« ali različne njegove izpeljanke,[2] med uporabniki spleta narašča, pojavile pa so se tudi skupine aktivistov, ki skušajo na alternativne načine – ker pravo trenutno na tem področju še ne daje ustreznega varstva – zavarovati svoje osebne podatke in s tem zasebnost in osebno integriteto.[3] Navedbe, da je mogoče na podlagi rezultata iskanj na spletnih iskalnikih napovedati epidemije gripe, gibanje finančnih trgov ali na splošno (bližnjo) prihodnost posameznika ali družbe, so v določenih pogledih morebiti koristne, a za uporabnike interneta dokaj strašljive. Poleg tega je mogoče z zbiranjem osebnih podatkov ustvariti profile posameznih potrošnikov, ki se lahko uporabijo za selektivno in ciljno internetno oglaševanje.[4] Pri tem ni potrebno, da se uporabnik identificira z imenom in priimkom, njegov profil

[1] Viviane Reding v govoru leta 2012; govor je dostopen na spletnem portalu YouTube, http://youtu.be/9binnTteKeA.

[2] Na primer »Obstajam, ker me je mogoče najti na Googlu.« Glej na primer http://www.knowledgeoftoday.org/2012/02/privacy-is-dead-google-knows-all-about.html.

[3] Primer je spletni iskalnik DuckDuckGo (https://duckduckgo.com/), ki naj ne bi shranjeval osebnih podatkov uporabnikov.

[4] Možina, str. 36, poudarja, da imajo tovrstni profili za spletne ponudnike veliko tržno vrednost. Pomen zbiranja osebnih podatkov potencialnih kupcev je poudarjen tudi v sporočilu Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij z naslovom Varovanje zasebnosti v povezanem svetu, Evropski okvir varstva podatkov za 21. stoletje (COM/2012/09 final), str. 2.

se ustvari na podlagi internetnega protokola (IP) uporabnikovega računalnika in/ali na podlagi t. i. piškotkov (*cookies*), tj. majhnih datotek, ki se shranjujejo na uporabnikovem računalniku, ko ta deska po spletu.[5] Strežniki avtomatično shranjujejo te informacije, na podlagi katerih se potem ustvari uporabnikov profil. V zvezi z zbiranjem osebnih podatkov na spletu je zato sporno predvsem vprašanje sorazmernosti:[6] ali je shranjevanje vseh osebnih podatkov upravičeno, če uporabnik v to ni privolil in če je lahko upravičena narava takega zbiranja le minimalna? Vprašanje je torej, ali je na spletu sploh še mogoče učinkovito varovati osebne podatke ali ohraniti zasebnost oziroma kolikšno ceno plačujemo za to, da smo v nenehnem stiku z informacijami in vseskozi elektronsko povezani.

2. Pravna podlaga za varstvo osebnih podatkov in varstvo zasebnosti v EU

2.1. Varstvo osebnih podatkov in varstvo zasebnosti kot temeljni pravici

Uvodoma je treba poudariti, da sta varstvo osebnih podatkov in varstvo zasebnosti različni pravici, ki pa sta med seboj tesno povezani. Varstvo zasebnosti je pravica, ki je po nastanku starejša; vključena je bila namreč že v Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin (EKČP),[7] podpisano leta 1950. Ta v 8. členu določa, da ima vsakdo »pravico do spoštovanja svojega zasebnega […] življenja, svojega doma in dopisovanja« in da se javna oblast »ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom«. Nasprotno pa se je pomen varstva osebnih podatkov povečal šele v osemdesetih letih prejšnjega stoletja, ko je bila v okviru Sveta Evrope sprejeta Konvencija št. 108 o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov.[8] Ta konvencija vsebuje temeljna načela za varstvo osebnih podatkov (na primer, da morajo biti pridobljeni in obdelani v skladu z zakonom in shranjeni samo

[5] Več o piškotkih glej na primer v Luzak, str. 221 in nasl. (opredelitev na str. 222); Možina, navedeno delo.

[6] Načelo sorazmernosti v okviru varstva osebnih podatkov je poudarjeno v več predpisih EU, najprej v Direktivi Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23. 11. 1995, str. 31), ki v točki c prvega odstavka 6. člena določa, da morajo biti osebni podatki »primerni, ustrezni in ne pretirani glede na namene, za katere se zbirajo in/ali naprej obdelujejo«. Glej tudi 28. uvodno izjavo te direktive. Tudi Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31. 7. 2002, str. 37) v 11. uvodni izjavi poudarja pomen tega načela. V teoriji glej na primer Hijmans in Scirocco, str. 1487.

[7] Uradni list RS, MP, št. 33/1994.

[8] Uradni list RS, MP, št. 11/1994.

za določene in zakonite namene v skladu z načelom sorazmernosti[9]) ter pravila glede prenosa podatkov čez meje[10] in medsebojnega sodelovanja med pogodbenicami.[11]

Varstvo zasebnosti in osebnih podatkov sta pripoznani kot temeljni pravici tudi na ravni EU. Listina EU o temeljnih pravicah (v nadaljevanju Listina)[12] ju varuje v 7. in 8. členu; 7. člen, naslovljen Spoštovanje zasebnega in družinskega življenja, med drugim določa, da ima vsakdo pravico do spoštovanja svojega zasebnega življenja in komunikacij, 8. člen pa v prvem odstavku določa, da ima vsakdo pravico do varstva svojih osebnih podatkov. Poleg tega 8. člen v drugem odstavku določa, da se morajo osebni podatki »obdelovati pošteno, za določene namene in na podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom«, in da ima vsakdo »pravico dostopa do podatkov, zbranih o njem, in pravico zahtevati, da se ti podatki popravijo«. Postulat varstva osebnih podatkov vsebuje tudi prvi odstavek 16. člena Pogodbe o delovanju Evropske unije (PDEU).[13] V zvezi s tem členom je pomembno poudariti, da je relevanten tudi za policijsko in pravosodno sodelovanje v kazenskih zadevah,[14] saj je bila ob uveljavitvi Lizbonske pogodbe odpravljena t. i. stebrna struktura[15] EU. Kljub temu pa je na področju skupne zunanje in varnostne politike varstvo tovrstnih podatkov še vedno podvrženo drugačni pravni podlagi,[16] saj so na področju te politike ohranjene nekatere specifičnosti.[17] Podobno velja za Ustavo RS, ki varstvo osebnih podatkov zagotavlja v 38. členu, v katerem je uporaba teh podatkov v nasprotju z namenom njihovega zbiranja prepovedana.[18] Varstvo zasebnosti pa je zagotovljeno v 35. členu Ustave RS.

---

[9] Glej 5. člen Konvencije št. 108 o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov.

[10] Glej 12. člen navedene konvencije.

[11] Glej 13. člen navedene konvencije in nasl.

[12] UL C 83, 30. 3. 2010, str. 389.

[13] UL C 326, 26. 10. 2012, str. 47.

[14] To je izrecno poudarjeno v navedenem sporočilu Komisije (COM/2012/09 final), str. 3.

[15] T. i. stebrna struktura vključuje tri stebre Evropske unije; prvi steber je pravo Skupnosti, drugi steber skupna zunanja in varnostna politika, tretji pa policijsko in pravosodno sodelovanje v kazenskih zadevah. Glej Trstenjak, Brkan, str. 78 in 83.

[16] Glej 39. člen Pogodbe EU.

[17] O problematiki varstva osebnih podatkov na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah in področju skupne zunanje in varnostne politike glej v teoriji Hijmans in Scirocco, str. 1485.

[18] Ta člen določa tudi, da »[z]biranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon« in da ima vsakdo »pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi«.

Del teorije pravico do varstva osebnih podatkov sicer obravnava kot del pravice do zasebnosti in jo poimenuje informacijska zasebnost,[19] saj je vrednotna podlaga varstva osebnih podatkov enaka kot podlaga za varstvo zasebnosti na drugih področjih.[20] Sicer pa teorija podarja, da med pravico do zasebnosti in pravico do varstva osebnih podatkov obstajajo pomembne razlike; ne le, da sta v pravu EU nomotehnično urejeni posebej in da je pravica do varstva osebnih podatkov po nastanku novejša od pravice do zasebnosti,[21] temveč so med njima tudi vsebinske razlike.[22] Kot je pojasnilo že Sodišče prve stopnje ES (zdaj Splošno sodišče EU) v zadevi *Bavarian Lager proti Komisiji,*[23] vsi osebni podatki še niso nujno varovani s pravico do zasebnosti, saj niso vsi tudi tajni.[24] Razkritje osebnih podatkov tako samo po sebi še ne pomeni, da gre tudi za kršitev zasebnosti, saj »vsi osebni podatki niso taki, da bi lahko ogrožali zasebnost posameznika«.[25] Osebni podatki torej niso samo podatki, ki vsebujejo zasebne informacije o neki osebi, temveč, kot izhaja iz opredelitve v Direktivi 95/46/ES o varstvu osebnih podatkov[26] (točka a 2. člena), vključujejo »katerokoli informacijo, ki se nanaša na določeno ali določljivo fizično osebo«. Pojem osebnega podatka je torej bolj objektivne narave, medtem ko je varovanje zasebnosti bolj subjektiven pojem.[27] Poudariti pa je treba tudi, da je Sodišče EU s področja uporabe varstva osebnih podatkov izključilo pravne osebe, na primer v združenih zadevah C-92/09 in C-93/09, *Volker, Schecke in Eifert*.[28] Poleg tega se zastavlja vprašanje, ali bi z vidika področja uporabe *ratione personae* ti dve pravici bilo treba razlagati tako, da lahko nalagata obveznosti tudi posameznikom, ne le javnim organom, oziroma ali so fizične osebe ti dve temeljni pravici dolžne spoštovati. Sodišče EU do zdaj še ni dovolilo horizontalnega učinka temeljnih pravic,[29] ni pa izključeno, da tega ne bo storilo v prihodnosti.

---

[19] Glej na primer Cerar, str. 1409.

[20] Prav tam, str. 1412.

[21] Tzanou, str. 25–26.

[22] Tzanou, str. 26.

[23] Sodba z dne 8. novembra 2007 v zadevi *Bavarian Lager proti Komisiji* (T-194/04, ZOdl., str. II-04523).

[24] Prav tam, točka 118.

[25] Prav tam, točka 119.

[26] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23. 11. 1995, str. 31).

[27] Tzanou, str. 28.

[28] V teoriji tako Kokott in Sobotta, str. 89.

[29] Glej sodbo v zadevi C-176/12, *Association de médiation sociale*, v kateri je Sodišče EU odločilo, da se na enega od členov Listine EU o temeljnih pravicah (v konkretni zadevi na 27. člen) ni mogoče sklicevati v sporu med posamezniki.

2.2. Sekundarni pravni viri varstva osebnih podatkov na ravni EU

Sredi devetdesetih let je bil na ravni EU sprejet prvi predpis glede varstva osebnih podatkov – Direktiva 95/46/ES o varstvu osebnih podatkov.[30] Temeljni postulat, iz katerega izhaja ta direktiva, je posameznikova privolitev v obdelavo osebnih podatkov – osebni podatki se lahko obdelujejo samo, če je oseba, katere osebni podatki se zbirajo in obdelujejo, nedvoumno dala privolitev,[31] oziroma v drugih primerih, ko je tovrstna obdelava podatkov potrebna iz določenih objektivnih razlogov, kot na primer, ker je to predpisano z zakonom, za izvajanje ukrepov v javnem interesu, zaradi drugih zakonitih interesov ali za varstvo življenjskih interesov posameznikov ali pa za izvajanje pogodbe, ki jo je podpisala ta oseba.[32] Privolitev je tudi temelj za zbiranje bolj občutljive vrste osebnih podatkov, na primer tistih, ki se nanašajo na rasno, etnično ali versko pripadnost, ali tistih, ki razkrivajo informacije o posameznikovem zdravju ali spolnem življenju.[33] Splošno načelo je, da obdelava osebnih podatkov iz teh kategorij ni dovoljena, od te prepovedi pa je mogoče odstopiti samo s posameznikovo privolitvijo, a še to samo, če je zakonodaja države članice ne izključuje.[34] Posameznik je torej v središču pravil, s katerimi se zagotavlja uspešno in učinkovito varstvo osebnih podatkov, vendar pa teorija utemeljeno poudarja, da je poznavanje tega področja pomembno tudi (ali celo predvsem) za organe, tako za javni kot zasebni sektor, ki jih pravila o obdelavi osebnih podatkov zavezujejo.[35]

Direktiva 95/46/ES o varstvu osebnih podatkov, v slovenski pravni red prenesena z Zakonom o varstvu osebnih podatkov,[36] sicer vsebuje dokaj natančna pravila glede obdelave osebnih podatkov, kljub temu pa v njej ni ustreznih oziroma dovolj specifičnih pravil, ki bi lahko odgovorila na sodobne probleme v zvezi z internetom, elektronsko komunikacijo in elektronskim okoljem na splošno. Ta vprašanja na ravni EU trenutno – vendar le deloma – ureja oziroma obravnava Direktiva

[30] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23. 11. 1995, str. 31).

[31] Glej točko a 7. člena Direktive 95/46/ES.

[32] Natančneje glede teh razlogov 7. člen Direktive 95/46/ES.

[33] Glej točko a drugega odstavka 8. člena Direktive 95/46/ES.

[34] Prav tam.

[35] Trstenjak, str. 1415.

[36] Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/2004; za uradno prečiščeno besedilo glej ZVOP-1-UPB1, Uradni list RS, št. 94/2007. Glede statusa prenosa te direktive v drugih državah članicah glej spletno stran http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm#h2-23.

2002/58/ES o zasebnosti in elektronskih komunikacijah,[37] ki je bila sprejeta prav z namenom, da dopolni določila Direktive 95/46/ES o pravici do zasebnosti glede obdelave osebnih podatkov na področju elektronskih komunikacij.[38] Ta direktiva države članice zavezuje, da v svojih nacionalnih predpisih zagotovijo zaupnost sporočil v javnem komunikacijskem omrežju in tistih, ki se pošiljajo prek elektronskih komunikacijskih storitev.[39] Izjema od tega zagotavljanja zasebnosti je – podobno kot pri Direktivi 95/46/ES o varstvu osebnih podatkov – situacija, v kateri je posameznik privolil v to, da določena sporočila niso obravnavana zaupno, oziroma ko tako nezaupno obravnavanje predvideva zakon.[40] Primeri take zakonske podlage, ki dovoljuje omejevanje pravice do varstva osebnih podatkov, so na primer varovanje državne varnosti, preprečevanje, preiskovanje in pregon kaznivih dejanj ali nedovoljena uporaba elektronskih komunikacijskih sistemov.[41] Vendar pa je razmerje med Direktivo 95/46/ES in Direktivo 2002/58/ES dokaj specifično, saj slednja ne obravnava vprašanj varstva osebnih podatkov in je specializiran predpis na področju elektronskih komunikacij.[42]

Poleg tega je treba omeniti tudi Uredbo 45/2001 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah [EU],[43] s katero se zagotavlja varstvo osebnih podatkov v institucijah EU.[44] Ta uredba vsebuje pravila glede obdelave osebnih podatkov v institucijah EU,[45] glede prenosa teh podatkov med institucijami EU[46] ali drugimi organi, ki niso institucije EU,[47] in seveda opredeljuje pravice osebe, na katero se nanašajo osebni podatki (na primer pravica do dostopa, popravka ali izbrisa).[48] Podobno kot Direktiva 95/46/ES tudi navedena uredba izrecno prepoveduje obdelavo občutljivih kategorij podatkov, kot so podatki o etničnem ali rasnem poreklu, veroizpovedi ali zdravstvenem stanju osebe, razen

[37] Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31. 7. 2002, str. 37).

[38] Glej 1. člen Direktive 2002/58/ES.

[39] Glej prvi odstavek 5. člena Direktive 2002/58/ES.

[40] Prav tam.

[41] Glej prvi odstavek 15. člena Direktive 2002/58/ES.

[42] Glej 11. uvodno izjavo Direktive 2002/58/ES, ki določa, da se Direktiva 95/46/ES uporablja le za tista vprašanja glede elektronskih komunikacij, ki niso izrecno zajeta z Direktivo 2002/58/ES.

[43] Uredba (ES) 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12. 1. 2001, str. 1).

[44] Glej 1. člen Uredbe 45/2001.

[45] Glej predvsem 5. člen Uredbe 45/2001.

[46] Glej 7. člen Uredbe 45/2001.

[47] Glej 8. in 9. člen Uredbe 45/2001.

[48] Glej 13. do 19. člen Uredbe 45/2001.

v določenih omejenih primerih.[49] Uredba vsebuje posebna pravila glede varstva osebnih podatkov v telekomunikacijskih omrežjih,[50] vendar v njej ni izrecnih pravil, ki bi urejala vprašanja varstva osebnih podatkov na spletu ali v elektronskem okolju.

V zadnjem času so zelo aktualna vprašanja varstva osebnih podatkov za namene preprečevanja terorizma oziroma širše, na področju kazenskega prava.[51] Vihar odzivov je tako sprožila t. i. Direktiva 2006/24/ES o hrambi podatkov,[52] sprejeta za ureditev shranjevanja osebnih podatkov, ki jih je mogoče pridobiti v zvezi z elektronskimi komunikacijskimi storitvami in komunikacijskimi omrežji z namenom »preprečevanja, preiskovanja, odkrivanja in pregona hudih kaznivih dejanj«.[53] Na podlagi te direktive imajo države članice obveznost hrambe številnih podatkov, in sicer so to podatki o klicih v fiksnem in mobilnem telefonskem omrežju, podatki o dostopu do interneta, internetne elektronske pošte in internetne telefonije, pri čemer se ne shranjuje vsebina te komunikacije, temveč na primer telefonske številke oseb, ki komunicirajo, datum in čas začetka in konca komunikacije, datum in čas prijave ter odjave dostopa na internet ali do elektronske pošte, in podobni podatki.[54] Direktiva določa, da se ti podatki shranjujejo od šest mesecev do maksimalno dve leti.[55] Problem te direktive je predvsem v tem, da zahteva shranjevanje navedenih podatkov za vse osebe, neodvisno od tega, ali so osumljene kaznivih dejanj, zato se zastavlja vprašanje sorazmernosti njenih norm. Ta direktiva je sprožila burne odzive v literaturi,[56] implementacijski ukrepi držav članic, sprejeti za prenos te direktive, pa so (bili) predmet presoje ustavnih sodišč številnih držav članic,[57] tudi Ustavnega sodišča RS,[58] sama direktiva pa je trenutno tudi v postopku presoje veljavnosti na Sodišču EU.[59]

---

[49] Glej 10. člen Uredbe 45/2001.

[50] Glej 34. do 40. člen Uredbe 45/2001.

[51] Glej na primer v zvezi s tem Bard, str. 13 in nasl.

[52] Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, 13. 4. 2006, str. 54).

[53] Glej prvi odstavek 1. člena Direktive 2006/24/ES.

[54] Za natančnejša pravila glej 5. člen Direktive 2006/24/ES.

[55] Glej 6. člen Direktive 2006/24/ES.

[56] Glej na primer le Konstadinides, str. 722–736.

[57] Glej na primer odločbo nemškega ustavnega sodišča z dne 2. marca 2010 (NJW 2010, str. 833); odločbo romunskega ustavnega sodišča št. 1258 z dne 8. oktobra 2009, češkega ustavnega sodišča z dne 31. marca 2011. V teoriji glej na primer Kosta, str. 339–363. Posebej o odločbi nemškega ustavnega sodišča glej Kaiser, str. 503–517.

[58] Glej zadevo U-I-65/13-16.

[59] Zadevi C-293/12, *Digital Rights Ireland*, in C-594/12, *Seitlinger in drugi*.

V EU so za varstvo osebnih podatkov pomembni tudi nekateri drugi predpisi, na primer Direktiva 2009/136/ES[60] ali na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah Okvirni sklep 2008/977/PNZ.[61] Zaradi hitrega razvoja elektronskih komunikacijskih sistemov in širjenja socialnih omrežij je Evropska komisija predlagala sprejetje nove zakonodaje, ki naj bi odgovorila na te sodobne izzive. To zakonodajo, ki je trenutno v postopku sprejemanja, obravnavamo v nadaljevanju.

Zdaj veljavna zakonodaja EU je precej razdrobljena, zaradi česar je poslovanje prek spleta oteženo, hkrati pa tudi manj transparentno. V javnosti je namreč dokaj razširjeno mnenje, da spletna dejavnost prinaša precejšnje nevarnosti za varstvo posameznikov.[62] Zato so udeleženci na trgu zakonodajo precej kritizirali in kot argumente za spremembo navajali pravno varnost in jasnejša pravila o mednarodnem prenosu osebnih podatkov, torej o prenosu podatkov ven iz EU.[63]

2.3. Prihodnost: nova zakonodaja na ravni EU

Evropska komisija se je na navedene kritike odzvala. Na ravni EU sta trenutno v zakonodajnem postopku dva predpisa, ki bosta v prihodnosti pomembno vplivala na varstvo osebnih podatkov: **Predlog Uredbe o varstvu podatkov**[64] in **Predlog Direktive o varstvu osebnih podatkov za namene pregona kaznivih dejanj**.[65] Predpisa ohranjata temeljna pravila glede varstva osebnih podatkov, hkrati pa vsebujeta nova in podrobnejša pravila, ki so prilagojena hitremu razvoju novih tehnologij, zlasti interneta. V pojasnilih k uredbi je jasno navedeno, da

[60] Direktiva 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov (UL L 337, 18. 12. 2009, str. 11).

[61] Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (UL L 350, 30. 12. 2008, str. 60).

[62] Glej sedmo uvodno izjavo Predloga Uredbe Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (COM/2012/011 konč).

[63] Obrazložitveni memorandum k Predlogu Uredbe Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (COM/2012/011 konč), str. 4.

[64] Predlog Uredbe Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (COM/2012/011 konč).

[65] Predlog Direktive Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov (COM/2012/010 konč).

nova ureditev ne bo posegla v temeljna načela varstva osebnih podatkov.[66] Prav tako iz sedme uvodne izjave k tej uredbi jasno izhaja, da »cilji in načela Direktive 95/46/ES še vedno veljajo«. Poleg tega pa je, kot je bilo že omenjeno, bila potrebna prilagoditev novim tehnologijam, zlasti hitremu razvoju interneta.[67]

Za prilagoditev temu razvoju navedena predpisa prinašata nekaj novosti. Kot opozarja teorija, je ena pomembnejših novosti, ki jih bo uvedla Uredba o varstvu podatkov, širša opredelitev pojma osebnih podatkov v prvem odstavku 4. člena.[68] V praksi je bilo do zdaj sporno, ali t. i. spletni identifikatorji spadajo med osebne podatke ali ne, predlog uredbe pa vsebuje jasno določbo, ki take spletne identifikatorje vključuje pod pojem osebnega podatka.[69] Spletni identifikatorji so na primer naslovi internetnega protokola ali identifikatorji piškotkov.[70] Ti spletni identifikatorji sicer sami po sebi ne omogočajo identifikacije osebe z imenom in priimkom, temveč lahko k taki identifikaciji pripomorejo v povezavi z drugimi osebnimi podatki, na primer, če oseba, ki ji pripada določen IP-naslov, opravi spletni nakup, v okviru katerega spletnemu prodajalcu da na voljo svoje ime in naslov. Kot izhaja iz uvoda k predlogu navedene uredbe, se lahko ti spletni identifikatorji »skupaj z edinstvenimi identifikatorji in drugimi informacijami, ki jih prejmejo strežniki, uporabijo za oblikovanje profilov posameznikov in njihovo identifikacijo«.[71] Vendar pa je mogoče tudi, da tovrstni spletni identifikatorji, identifikacijske številke, podatki o lokaciji ali drugi podobni podatki niso vedno opredeljeni kot osebni podatki v smislu navedene uredbe.[72]

Uredba je prilagojena spletnemu okolju tudi glede privolitve. Navaja namreč, da mora biti privolitev vedno dana izrecno;[73] implicitna privolitev torej ni veljavna privolitev. Treba je poudariti, da se taka privolitev ne da samo z jasno izjavo ali s podpisom, temveč tudi s tem, da spletni uporabnik na spletni strani označi v ta namen opredeljeno okence ali s kakšnim drugim nedvoumnim ravnanjem pokaže, da daje privolitev.[74]

V novi zakonodaji je posebej poudarjen tudi pomen načela preglednosti, ki zahteva, da morajo biti vse informacije glede varstva osebnih podatkov posameznika »lahko dostopne in razumljive ter izražene v jasnem in preprostem

[66] Obrazložitveni memorandum k Predlogu Uredbe o varstvu podatkov, str. 4.
[67] Prav tam.
[68] V slovenski teoriji glej Burnik, str. 10.
[69] Prav tam.
[70] Glej 24. uvodno izjavo Predloga Uredbe o varstvu podatkov.
[71] Prav tam.
[72] Prav tam.
[73] Glej 25. uvodno izjavo Predloga Uredbe o varstvu podatkov.
[74] Prav tam.

jeziku«, zlasti v primeru spletnega oglaševanja.[75] V takem primeru posameznik namreč težko ugotovi, ali se osebni podatki sploh zbirajo in s kakšnim namenom se zbirajo.[76]

Pomembna novost, ki jo uvaja ta uredba, je tudi pravna ureditev pravice biti pozabljen in pravice do izbrisa, ki jo vsebuje 17. člen predloga. Zdaj veljavna Direktiva 95/46/ES take pravice ne ureja in prav to je eno od vprašanj, ki je sporno v zadevi C-131/12, *Google Spain in Google*.[77] Če bo predlog uredbe sprejet, bo imel posameznik, na katerega se nanašajo osebni podatki, pravico »pri upravljavcu doseči izbris osebnih podatkov v zvezi z njim in opustitev nadaljnjega razširjanja takih podatkov«.[78] Ta pravica je pomembna zlasti v primeru, kadar so se osebni podatki objavili na spletu, ko je bila oseba še otrok, kot odrasla oseba pa je svojo privolitev za obdelavo osebnih podatkov preklicala, ali kadar podatki ne izpolnjujejo več svojega namena.[79] Na podlagi te nove zakonodaje naj bi se ta pravica razlagala dokaj široko, da se omogoči njeno dejansko uresničevanje. Uredba namreč predvideva možnost, da upravljavec spletne strani, na kateri so bili objavljeni osebni podatki neke osebe, obvesti tretje osebe – obdelovalce teh podatkov, da oseba zahteva izbris osebnih podatkov in vseh povezav ali kopij podatkov.[80] Poleg tega je lahko upravljavec tudi odgovoren, če je odobril, da tretja oseba objavi osebne podatke.[81]

Predlog te zakonodaje pa doslej še ni bil sprejet. Komisarka Redingova je zato v govoru na Svetu EU decembra 2013 to institucijo pozvala k ukrepanju.[82] Sprejetje nove zakonodaje je za zdaj odloženo za čas po volitvah v Evropski parlament.[83]

3. Sodna praksa Sodišča EU s področja varstva osebnih podatkov

Sodišče EU (pa tudi Evropsko sodišče za človekove pravice in sodišča v državah članicah EU) vse pogosteje obravnava vprašanja temeljnih pravic v zvezi

[75] Glej 46. uvodno izjavo Predloga Uredbe o varstvu podatkov.

[76] Prav tam.

[77] Za analizo zadeve glej v nadaljevanju prispevka.

[78] Glej prvi odstavek 17. člena Predloga Uredbe o varstvu podatkov.

[79] Prav tam.

[80] Glej 54. uvodno izjavo Predloga Uredbe o varstvu podatkov.

[81] Prav tam.

[82] Govor komisarke Redingove na Svetu EU za pravosodje dne 6. decembra 2013, dostopen na http://europa.eu/rapid/press-release_SPEECH-13-1027_en.htm.

[83] Glej EU Observer: »EU data bill delayed until after May elections«, http://euobserver.com/justice/122853.

z informacijskimi tehnologijami, zlasti vprašanja varstva podatkov in varstva zasebnosti, zaščite intelektualne lastnine in svobode izražanja. V zvezi s tem so relevantne številne zadeve, na primer sodbe pred Sodiščem EU v zadevah C-92/09 in C-93/09, *Volker, Schecke in Eifert*, C-293/12, *Digital Rights Ireland,* ali C-594/12, *Seitlinger*. Med zadevami pred ESČP je treba omeniti na primer *Wegrzynowski in Smolczewski proti Poljski*,[84] v kateri je šlo za izbris informacij o dveh odvetnikih s spletne strani in v kateri je ESČP ugotovilo, da Poljska ni kršila pravice do zasebnosti iz 8. člena EKČP. Tovrstne zadeve pa so pogoste tudi pred sodišči držav članic, na primer spori v zvezi s kršitvijo avtorskih pravic s spletno stranjo Pirate Bay na Švedskem[85] in Nizozemskem.[86] Ta prispevek se omejuje na analizo določenih zadev pred Sodiščem EU v zvezi s problematiko varstva osebnih podatkov.

3.1. Zgodnejša sodna praksa

Zgodnejša sodna praksa pred Sodiščem EU obsega na primer zadeve C-101/01, *Lindqvist*, C-524/06, *Huber*, C-553/07, *Rijkeboer,* ter C-73/07, *Satakunnan Markkinapörssi in Satamedia*. Poudariti je treba, da se vse te zadeve iz zgodnejše sodne prakse nanašajo na razlago (in ne na veljavnost) Direktive 95/46/ES in v javnosti ali pri nacionalnih ustavnih ali vrhovnih sodiščih niso sprožile tako burnih odzivov kot novejše zadeve. Pomembno je poudariti tudi, da se samo prva od teh zadev (*Lindqvist*) nanaša na objavo osebnih podatkov na internetu, druge pa na bolj »klasične« načine obdelave in objave osebnih podatkov.

V zadevi **C-101/01, *Lindqvist*,** je Sodišče EU obravnavalo združljivost švedske zakonodaje, ki je določala strožje varstvo osebnih podatkov, z Direktivo 95/46/ES.[87] Vprašanja so se zastavila v kazenskem postopku zoper gospo Bodil Lindqvist. Ta je na spletni strani objavila osebne podatke o nekaterih prostovoljcih, ki so prostovoljno delali v eni od župnij švedske protestantske cerkve. Spletna stran je vsebovala podatke o Bodil Lindqvist in njenih kolegih, med temi podatki pa so bili poleg imen in priimkov navedeni še družinski stan, telefonska številka, prostočasne dejavnosti, pri eni od kolegic pa je bilo navedeno, da si je poškodovala nogo in da je to razlog za njeno odsotnost z dela. Za objavo teh

[84] Sodba ESČP z dne 16. 7. 2013 v zadevi *Wegrzynowski in Smolczewski proti Poljski* (no. 33846/07).

[85] Glej sodbo prvostopenjskega sodišča v Stockholmu z dne 17. 4. 2009 (št. B 13301-06), sodbo pritožbenega sodišča v Stockholmu z dne 26. 11. 2010 (št. B 4041-09) in sodbo Vrhovnega sodišča z dne 1. 2. 2012 (št. B 5880-10). Glej v teoriji na primer Larsson, str. 1 in nasl.

[86] Glej na primer sodbo pritožbenega sodišča v Haagu z dne 28. 1. 2014 (zadeva 200.105.418/01), v kateri je to sodišče odločilo, da preprečevanje dostopa do spletne strani Pirate Bay ni učinkovito sredstvo za preprečevanje kršitev avtorskih pravic.

[87] Za komentar zadeve glej na primer Coudray, str. 1361 in nasl.; Siemen, str. 306 in nasl.

informacij ni pridobila privolitve oseb, poleg tega pa objave ni pisno prijavila pristojnim organom.[88]

Sodišče EU je v sodbi ugotovilo, da gre v obravnavani zadevi za »obdelav[o] osebnih podatkov v celoti ali delno z avtomatskimi sredstvi«, kot je predvideno v prvem odstavku 3. člena Direktive 95/46/ES, in da ta obdelava ne spada v nobeno od izjem od uporabe te direktive, predvidenih v drugem odstavku 3. člena.[89] Drugi odstavek 3. člena te direktive namreč izključuje njeno uporabo na določenih področjih (na primer javna varnost, obramba, državna varnost) in tudi v primeru, da gre za obdelavo osebnih podatkov, ki jo opravlja fizična oseba »med potekom popolnoma osebne ali domače dejavnosti«. Poleg tega je Sodišče EU v tej zadevi odločalo o vprašanju, ali Direktiva 95/46/ES državam članicam dopušča, da določijo strožje varstvo osebnih podatkov (vertikalna dimenzija) ali širše področje uporabe (horizontalna dimenzija) kot ta direktiva.[90] Sodišče EU je odločilo, da višja raven varstva ni mogoča – poudarilo je, da morajo biti ukrepi držav članic »v skladu z določbami Direktive 95/46/ES in njenim ciljem«. Ta direktiva torej ne vsebuje minimalne harmonizacije, ampak celovito harmonizacijo.[91] Drugače pa je odločilo glede razširitve področja uporabe te direktive – države članice lahko nacionalno zakonodajo, ki v nacionalni pravni red prenaša to direktivo, razširi na področja, ki s to direktivo niso urejena.[92] Zadeva *Lindqvist* je torej pomembna predvsem zato, ker je v njej jasno navedeno, kakšne so meje Direktive 95/46/ES in katero vrsto harmonizacije prinaša. Ob minimalni harmonizaciji bi lahko države članice namreč sprejele strožje predpise za varstvo osebnih podatkov, kar pa v konkretnem primeru ni mogoče (vertikalna dimenzija). Države članice pa so proste glede širše uporabe nacionalne zakonodaje, ki prenaša to direktivo (horizontalna dimenzija).

V zadevi **C-524/06, *Huber*,** je bil sporen obstoj centralnega registra, ki je obstajal samo za tujce, ne pa tudi za nemške državljane. Huber je bil avstrijski državljan, ki je bil vpisan v navedeni register tujcev – register je vseboval na primer te osebne podatke: priimek, ime, datum in kraj rojstva, državljanstvo, zakonski stan, spol, podatke o preteklih vstopih na nemško ozemlje in izstopih s tega ozemlja, status rezidenta, podatke o potnem listu in druge podatke.[93] Huber je zahteval izbris navedenih osebnih podatkov iz registra; tak register naj bi bil namreč v nasprotju z načelom prepovedi diskriminacije na podlagi državljanstva,

[88] Natančneje za dejansko stanje glej sodbo C-101/01, *Lindqvist*, točke 2 in 12–17.

[89] Glej sodbo C-101/01, *Lindqvist*, točki 27 in 48.

[90] Prav tam, točka 91.

[91] Prav tam, točka 96.

[92] Prav tam, točka 99.

[93] Natančneje glej sodbo C-524/06, *Huber*, točka 31.

s pravico ustanavljanja in z Direktivo 95/46/ES.[94] Nemško predložitveno sodišče je v postopku predhodnega odločanja Sodišče EU prosilo za odgovor na vprašanje, ali je takšna obdelava osebnih podatkov v navedenem registru v nasprotju s pravom EU.[95] Sodišče EU je odločilo, da tak register za tujce ni dopusten, saj krši načelo prepovedi diskriminacije na podlagi državljanstva.[96] Poleg tega je Sodišče EU odločalo tudi o vprašanju, ali je v obravnavani zadevi izpolnjen kriterij »nujnosti« iz Direktive 95/46/ES. Ta direktiva namreč v točki e 7. člena določa, da je osebne podatke mogoče obdelovati, če je taka obdelava »nujna za izvajanje naloge, ki se opravlja v javnem interesu ali pri izvrševanju javne oblasti«. V obravnavani zadevi je Sodišče EU odločilo, da je »nujnost« obdelave osebnih podatkov podana le, če register vsebuje samo podatke, ki so nujni, da lahko pristojni organi izvajajo upoštevne predpise, in če »njegova centraliziranost omogoča učinkovitejše izvajanje teh predpisov z vidika pravice do prebivanja državljanov Unije, ki niso državljani te države članice«, nikakor pa obdelava podatkov ni nujna, če se opravlja za statistične namene.[97]

Zadeva **C-553/07, *Rijkeboer*,** je pomembna za razlago direktive v zvezi s časovno omejitvijo shranjevanja osebnih podatkov. Vprašanje za predhodno odločanje se je zastavilo v sporu med Rijkeboerjem in rotterdamskim občinskim svetom[98] in se je nanašalo na to, ali direktiva dopušča ureditev, v skladu s katero je mogoče omejiti pravico neke osebe do dostopa do informacij glede prejemnikov osebnih podatkov o tej osebi in glede vsebine teh podatkov na eno leto.[99] V konkretni zadevi so se osebni podatki, ki jih je zahteval Rijkeboer, po obdobju enega leta avtomatično izbrisali, zato informacij o vsebini teh podatkov ni mogel pridobiti.[100] Natančneje, zadeva se je nanašala na razlago odstavka a 12. člena Direktive 95/46/ES, ki posamezniku omogoča, da od upravljavca pridobi podatke o tem, ali in kateri podatki o njem se zbirajo. Sodišče EU je v zadevi odločilo, da mora biti rok za shranjevanje osebnih podatkov tak, da zagotavlja ravnovesje med interesi osebe, katere osebni podatki se shranjujejo, in bremenom, ki ga za upravljavca pomeni obveznost shranjevanja teh informacij.[101] V konkretnem primeru ureditev, v skladu s katero je shranjevanje podatkov omejeno na obdobje enega leta, s čimer je omejen tudi dostop do teh podatkov, ne zagotavlja takega

94 Glej sodbo C-524/06, *Huber*, točka 33.

95 Prav tam, točka 41.

96 Prav tam, točka 81.

97 Prav tam, točke 66–68.

98 Natančneje za dejansko stanje glej sodbo C-553/07, *Rijkeboer*, točke 23–28.

99 Prav tam, točka 31.

100 Prav tam, točka 25.

101 Prav tam, točka 70.

pravičnega ravnovesja; tako ravnovesje bi lahko bilo podano samo, če bi bilo shranjevanje teh podatkov za upravljavca osebnih podatkov pretirano breme.[102] Iz te sodbe torej izhaja, da so države članice dokaj omejene pri določanju obdobja, za katero se morajo podatki shranjevati, saj morajo pri tem varovati pravico oseb, na katere se ti podatki nanašajo, do dostopa do teh informacij.

Med starejšimi zadevami je treba omeniti tudi zadevo **C-73/07, *Satakunnan Markkinapörssi in Satamedia*,** v kateri je Sodišče EU zaradi njenega pomena odločalo v velikem senatu. Dve finski družbi sta pri finskih davčnih organih zbirali podatke o dohodku iz kapitala in obdavčenju premoženja oseb, katerih dohodek presega določene prage, in jih za plačilo posredovali s kratkimi sporočili sms.[103] V konkretni zadevi je finski pooblaščenec za varstvo osebnih podatkov od finske komisije za varstvo osebnih podatkov zahteval uvedbo prepovedi tovrstne obdelave osebnih podatkov. Ker je slednja to zahtevo zavrnila, je pooblaščenec sprožil sodni spor in v pritožbenem postopku je finsko sodišče na Sodišče EU naslovilo vprašanja o skladnosti take ureditve z Direktivo 95/46/ES.[104] V obravnavani zadevi ni bilo sporno, da je šlo za obdelavo osebnih podatkov v smislu te direktive[105] in da taka obdelava osebnih podatkov glede imenskih zbirk, ki vsebujejo le podatke, že objavljene v medijih, spada na področje uporabe te direktive.[106] Natančneje, dejavnost, ki je bila v obravnavani zadevi sporna, je obsegala štiri operacije, in sicer (1) zbiranje podatkov o dohodku in premoženju fizičnih oseb na podlagi javnih dokumentov davčne uprave, (2) objavo teh podatkov po abecednem redu in po vrsti dohodkov, (3) prenos teh podatkov na CD-romu in (4) posredovanje teh podatkov na zahtevo po telefonu s sms.[107] V zadevi se je zastavilo tudi vprašanje, ali se obdelava podatkov, ki so javni, lahko šteje za obdelavo podatkov, ki se izvaja »zgolj v novinarske namene«, v smislu 9. člena te direktive. Sodišče EU je odločilo, da lahko res gre za obdelavo v novinarske namene, če je edini cilj navedenih dejavnosti razkritje informacij, mnenj ali idej javnosti, vendar pa je v konkretnem primeru za presojo, ali v konkretni zadevi gre za tako razkritje informacij, pristojno predložitveno sodišče.[108]

---

[102] Prav tam, točka 70.

[103] Natančneje o dejanskem stanju glej sodbo C-73/07, *Satakunnan Markkinapörssi in Satamedia*, točke 25–33.

[104] Za vprašanja za predhodno odločanje glej prav tam, točka 34.

[105] Prav tam, točka 37.

[106] Prav tam, točka 49.

[107] Prav tam, točka 37.

[108] Prav tam, točka 62.

3.2. Hramba osebnih podatkov

Kot je bilo že omenjeno, je bila v zadnjem času med navedenimi eden najbolj spornih predpisov Direktiva 2006/24/ES o hrambi podatkov.[109] Poglavitni namen te direktive je hramba osebnih podatkov za namen preprečevanja, preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, kakor jih opredeljuje nacionalna zakonodaja vsake od držav članic (1. člen). Preden je bila direktiva sprejeta, je bila sporna predvsem njena pravna podlaga, saj ni bilo jasno, ali bi morala biti sprejeta v okviru tedanjega prvega ali tretjega stebra.[110] Ta problematika je bila tudi predmet obravnave pred Sodiščem EU v zadevi **C-301/06, *Irska proti Parlamentu in Svetu***, v kateri je to odločilo, da ima direktiva pravo pravno podlago (95. člen ES, zdaj 114. člen TFEU).[111] Sodišče EU je poudarilo, da »so določbe te direktive predvsem omejene na dejavnosti ponudnikov storitev in da ne urejajo dostopa policijskih ali sodnih organov držav članic do podatkov niti njihove uporabe«,[112] zato so postopki, urejeni v tej direktivi, po mnenju Sodišča EU »neodvisni od izvajanja vsakega morebitnega policijskega in sodnega ukrepa sodelovanja na kazenskem področju«.[113] Problematika pravne podlage navedene direktive torej po tej sodbi Sodišča EU ni bila več sporna.

Drugače je glede skladnosti same direktive s temeljnimi pravicami oziroma glede sorazmernosti njenih ukrepov. V trenutni sodni praksi se zastavlja vprašanje, ali ta zakonodajni instrument EU krši temeljne pravice državljanov EU. Ustavnost te direktive oziroma njeno združljivost s temeljnimi pravicami so namreč presojala številna vrhovna ali ustavna sodišča in sicer vrhovno upravno sodišče Bolgarije, ciprsko in romunsko vrhovno sodišče; češko, nemško, poljsko in slovaško ustavno sodišče,[114] o podobnih vprašanjih pa trenutno odloča tudi Ustavno sodišče RS.[115] Ta direktiva je izpodbijana tudi v dveh zadevah pred Sodiščem EU, **C-293/12, *Digital Rights Ireland*,** in **C-594/12, *Seitlinger in drugi***, v katerih Sodišče EU še ni odločilo. Sodišče EU mora v navedenih zadevah, ki sta mu jih predložila irsko sodišče (*High Court of Ireland*) in avstrijsko ustavno sodišče (*Verfassungsgerichtshof*), odločiti o veljavnosti Direktive 2006/24/ES o hrambi podatkov. Zadevi odpirata več vprašanj, najpomembnejša pa so skladnost

[109] Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, 13. 4. 2006, str. 54).

[110] Kosta, str. 340.

[111] Sodba C-301/06, *Irska proti Parlamentu in Svetu*, točka 93.

[112] Prav tam, točka 80.

[113] Prav tam, točka 83.

[114] Kosta, str. 340–341.

[115] Sklep z dne 26. 9. 2013 v zadevi U-I-65/13-16.

določb te direktive z načelom sorazmernosti v smislu četrtega odstavka 5. člena PEU, omejevanje temeljnih pravic v smislu prvega odstavka 52. člena Listine EU o temeljnih pravicah in skladnost navedene direktive z načelom sorazmernosti, prav tako v smislu člena prvega odstavka 52. člena Listine.[116]

V navedenih zadevah so bili 12. decembra 2013 predstavljeni sklepni predlogi generalnega pravobranilca Cruza Villalóna, ki Sodišču EU predlaga, naj ugotovi, da Direktiva 2006/24/ES o hrambi podatkov ni v skladu s prvim odstavkom 52. člena Listine EU o temeljnih pravicah.[117] Ta člen namreč ureja obseg temeljnih pravic in načel ter njihovo razlago in v prvem odstavku določa, da mora biti kakršnokoli omejevanje uresničevanja pravic iz te listine predpisano z zakonom in v skladu z načelom sorazmernosti. Omejitve so na podlagi tega člena v skladu z načelom sorazmernosti, »če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih«. Generalni pravobranilec v svojih sklepnih predlogih najprej pojasni razlikovanje med sorazmernostjo v smislu tega člena in splošnim načelom sorazmernosti, ki izhaja iz četrtega odstavka 5. člena PEU, v skladu s katerim ukrepi Unije ne smejo presegati tistega, kar je potrebno za doseganje ciljev Pogodb. Po mnenju generalnega pravobranilca ima sorazmernost v okviru Listine »posebno moč«, saj je pogoj za kakršnokoli omejevanje temeljnih pravic. Analiza v sklepnih predlogih ima dva temelja: neskladnost te direktive kot celote s prvim odstavkom 52. člena Listine in neskladnost njenega 6. člena[118] s tem istim členom Listine.

Generalni pravobranilec ugotavlja, da določbe te direktive ne izpolnjujejo pogoja, da morajo biti omejitve določene z zakonom, kakor zahteva prvi odstavek 52. člena Listine. Po njegovem mnenju bi moral zakonodajalec Unije določiti temeljna načela za opredelitev minimalnih zaščitnih ukrepov glede dostopa do zadevnih osebnih podatkov.[119] Ker ti zaščitni ukrepi niso bili določeni, naj bi direktiva kot celota kršila prvi odstavek 52. člena Listine.[120]

Hkrati pa v analizi skladnosti z načelom sorazmernosti generalni pravobranilec ugotavlja predvsem, da je problematično obdobje, za katero se podatki shranjujejo; v skladu s 6. členom te direktive se podatki namreč hranijo najmanj šest mesecev in največ dve leti, kar lahko določijo države članice. Čeprav se tak

[116] Glej sklepne predloge generalnega pravobranilca Cruza Villalóna v zadevah C-293/12, *Digital Rights Ireland*, in C-594/12, *Seitlinger in drugi*, točka 2.

[117] Prav tam, točka 159.

[118] Ta člen določa obdobja hrambe podatkov: »Države članice zagotovijo, da se kategorije podatkov [iz te direktive] hranijo za obdobje najmanj šestih mesecev in največ dveh let od datuma komunikacije.«

[119] Prav tam, točka 125.

[120] Prav tam, točka 131.

ukrep lahko šteje za legitimen in ustrezen,[121] pa se zastavlja vprašanje, ali je tudi nujen. Po mnenju generalnega pravobranilca ni nujen, saj naj obdobje hrambe podatkov, ki ga določijo države članice, ne bi smelo biti daljše od enega leta; potencialni dveletni rok shranjevanja je torej po mnenju generalnega pravobranilca nesorazmeren.[122] Pri tem gre za nesorazmerno omejitev temeljne pravice do zasebnosti, ki je urejena v 7. členu Listine, zato navedeni 6. člen Direktive 2006/24/ES krši tako 7. člen Listine kakor tudi prvi odstavek 52. člena, saj državam članicam omogoča, da podatke shranjujejo za obdobje do dveh let.[123]

Pred Ustavnim sodiščem RS je trenutno še neodločena zadeva U-I-65/13-16, v kateri je to sodišče prekinilo postopek do odločitve v zadevah C-293/12, *Digital Rights Ireland*, in C-594/12, *Seitlinger in drugi*. Poudariti je treba, da je bilo to ustrezno, ni pa edina procesna možnost, ki jo je to sodišče imelo na voljo, saj bi lahko Sodišču EU tudi predložilo vprašanje za predhodno odločanje. Prekinitev postopka je bila v tem primeru bolj smiselna rešitev, saj bi Sodišče EU, ki sta mu bili obe navedeni zadevi predloženi že leta 2012,[124] z odločitvijo v morebitni slovenski zadevi v vsakem primeru počakalo do odločitve v že predloženih zadevah. Ustavno sodišče je v navedenem sklepu U-I-65/13-16 pravilno presodilo, da o zadevi ne more odločiti, dokler Sodišče EU ne odloči o veljavnosti Direktive 2006/24/ES o hrambi podatkov, saj je Sodišče EU izključno pristojno za odločanje o veljavnosti predpisov EU.[125] Prekinitev postopka pred Ustavnim sodiščem se zdi torej ustrezna rešitev, odločilo pa bo lahko šele po sodbi Sodišča EU.

3.3. Uporaba Direktive 95/46/ES za spletne iskalnike

V devetdesetih letih, torej ob sprejetju Direktive 95/46/ES, se je internet šele začel razvijati, zato ta direktiva ne vsebuje posebnih določb v zvezi z internetom ali spletnimi iskalniki. Do sprejetja nove zakonodaje so torej pravni položaj spletnih iskalnikov in njihove dolžnosti v zvezi z varstvom osebnih podatkov negotovi, hkrati pa je lahko v praksi njihova dejavnost za varstvo osebnih podatkov dokaj problematična. Spletni iskalniki lahko namreč shranjujejo veliko število različnih informacij: ne le iskalni niz, temveč tudi IP-naslov, različne vrste piškotkov (obi-

[121] Prav tam, točka 143.

[122] Prav tam, točka 149.

[123] Prav tam, točka 152.

[124] Predlog za sprejetje predhodne odločbe v zadevi *Digital Rights Ireland* je bil Sodišču EU predložen 11. junija 2012, v zadevi *Seitlinger* pa 19. decembra 2012.

[125] Sklep US RS U-I-65/13-16, točka 10.

čajne piškotke in t. i. *flash*-piškotke, ki jih je težje izbrisati), URL spletne strani, s katere je bilo iskanje izvedeno, jezik in druge podatke.[126]

Neustreznost veljavne zakonodaje o varstvu osebnih podatkov v zvezi z internetom se je dobro pokazala v še neodločeni zadevi **C-131/12, *Google Spain in Google***, v kateri bo Sodišče EU moralo obravnavati vprašanja dolžnosti in odgovornosti spletnega iskalnika v zvezi z varstvom osebnih podatkov. Vprašanja za predhodno odločanje so se zastavila v sporu med spletnim gigantom Google ter špansko Agencijo za varstvo osebnih podatkov (*Agencia Española de Protección de Datos*) in posameznikom, na katerega so se nanašali osebni podatki. Španski državljan je pri nacionalni agenciji od dveh akterjev – nacionalnega časnika in spletnega iskalnika Google – zahteval, naj s spleta odstranita informacije o postopku izvršbe oziroma nepremičninski dražbi zaradi neplačila socialnih prispevkov, ki je bil proti njemu izveden konec devetdesetih let. Agencija je njegovo zahtevo do časnika zavrnila, ker je za (spletno) objavo obstajala pravna podlaga, družbi Google pa je odredila, naj osebne podatke navedene osebe umakne s svojega indeksa in onemogoči dostop do njih. Družba Google se je proti tej odločitvi pritožila in v okviru tega postopka je nacionalno sodišče na Sodišče EU naslovilo več vprašanj za predhodno odločanje.[127] Bistveno vsebino teh vprašanj za predhodno odločanje je mogoče razvrstiti v tri skupine.[128] Prva skupina vprašanj zadeva ozemeljsko področje uporabe (*ratione loci*) Direktive 95/46/ES, v drugi kategoriji so vprašanja v zvezi s področjem uporabe *ratione materiae* te direktive in pravnim položajem spletnih iskalnikov v sistemu te direktive, v tretjo skupino pa spadajo vprašanja v zvezi s t. i. pravico biti pozabljen (*right to be forgotten*).[129] Sodišče EU v zadevi še ni odločilo, 25. junija 2013 pa so bili predstavljeni sklepni predlogi generalnega pravobranilca Jääskinena.

V zvezi s prvo skupino vprašanj generalni pravobranilec meni, da se navedena direktiva uporablja *ratione loci*, kadar se osebni podatki obdelujejo v okviru dejavnosti ustanovitve poslovne enote upravljavca.[130] V skladu s prvim odstavkom 4. člena Direktive 95/46/ES se namreč ta direktiva oziroma, natančneje, nacionalni predpisi, ki to direktivo prenašajo v nacionalni pravni red, uporabljajo v treh primerih: če se podatki obdelujejo »v okviru dejavnosti ustanovitve upravljavca na ozemlju države članice« (točka a), če upravljavec ni ustanovljen v eni od držav

[126] Glej Mnenje 1/2008 o vprašanjih varstva podatkov v zvezi z iskalniki, sprejeto 4. aprila 2008, Delovna skupina za varstvo podatkov iz člena 29, 00737/SL WP 148, str. 27.

[127] Natančneje glede dejanskega stanja glej sklepne predloge generalnega pravobranilca Jääskinena, predstavljene 25. junija 2013, v zadevi *Google Spain in Google* (C-131/12, še neobjavljeno v ZOdl., točke 18–22).

[128] Prav tam, točka 6.

[129] Prav tam, točka 6.

[130] Prav tam, točka 68.

članic, ampak na ozemlju, na katerem se nacionalna zakonodaja uporablja na podlagi mednarodnega javnega prava (točka b), in če upravljavec ni ustanovljen v eni od držav članic, vendar za obdelavo osebnih podatkov uporablja opremo, ki je na ozemlju države članice (točka c). Čeprav ima Google, s sedežem v Kaliforniji, podružnice v več državah članicah EU, pa generalni pravobranilec meni, da to ne more avtomatično pomeniti, da se direktiva uporablja na tej podlagi, saj ni jasno, ali te podružnice dejansko obdelujejo osebne podatke v smislu navedene direktive.[131] Zato predlaga, naj se v zvezi z uporabnostjo direktive upošteva glavni vir dohodkov navedenega spletnega iskalnika, to je oglaševanje na podlagi ključnih besed,[132] in naj se šteje, da se »osebni podatki obdelujejo v okviru dejavnosti 'ustanovitve [poslovne enote]' upravljavca v smislu člena točke a prvega odstavka 4. člena Direktive«, če je – z namenom trženja in prodaje oglasnega prostora na iskalniku – v državi članici ustanovljena podružnica, katere dejavnost je usmerjena k prebivalcem navedene države članice.[133]

Ta pravobranilčeva ugotovitev je zanimiva z dveh vidikov. Po eni strani je uporaba direktive za spletne iskalnike zelo odvisna od poslovnega modela, na katerem ti temeljijo. Vendar pa v konkretni zadevi ni šlo za dejavnost spletnega oglaševanja, temveč za dejavnost preprostega iskanja na spletu, zato nisem prepričana, da je to pravi kriterij. Menim, da bi bilo ustrezneje direktivo uporabiti za spletne iskalnike že na podlagi dejstva, da imajo v neki državi članici podružnico.

Po drugi strani se rešitev generalnega pravobranilca močno približuje tisti, ki jo je Sodišče EU podalo glede 15. člena Uredbe Bruselj I[134] v zadevi C-585/08, *Pammer in Hotel Alpenhof,* in zadevah, ki so ji sledile, na primer C-190/11, *Mühlleitner*, in C-218/12, *Emrek*. Generalni pravobranilec namreč v razlago točke a prvega odstavka 4. člena Direktive 95/46/ES doda element »usmerjanja«. Tudi ta kriterij se mi zdi v okviru Direktive 95/46/ES problematičen. Ne le, da elementa »usmerjanja« v navedenem členu direktive ni, temveč se s tem elementom na neki način izniči kriterij »ustanovitve« upravljavca v državi članici; ni namreč jasno, v katerih situacijah bi lahko upravljavec bil ustanovljen v neki državi članici in hkrati v to državo članico ne usmerjal svoje dejavnosti. Dodati ta kriterij je smiselno samo, če se direktiva uporablja za spletni iskalnik, ki je ustanovljen v eni državi članici, a svojo dejavnost usmerja v drugo državo članico. V vsakem primeru pa se zdi smiselno, da je ta kriterij subsidiaren in ne primaren, kot očitno meni generalni pravobranilec.

---

131 Prav tam, točka 63.

132 Prav tam, točka 64.

133 Prav tam, točka 68.

134 Uredba Sveta (ES) št. 44/2001 z dne 22. decembra 2000 o pristojnosti in priznavanju ter izvrševanju sodnih odločb v civilnih in gospodarskih zadevah (UL L 12, 16. 1. 2001, str. 1).

Zanimivo je tudi stališče generalnega pravobranilca do druge skupine vprašanj glede pravnega položaja spletnega iskalnika z vidika določb Direktive 95/46/ES. Medtem ko meni, da spletni iskalnik sicer »obdeluje« osebne podatke na spletnih straneh,[135] pa hkrati meni tudi, da ta spletni iskalnik ni »upravljavec« v skladu s točko d 2. člena Direktive. »Obdelovanje« osebnih podatkov v tej zadevi je bilo očitno in ga ni bilo težko dokazati. Generalni pravobranilec v sklepnih predlogih jasno obrazloži, kako deluje spletni iskalnik: med iskanjem po spletnih straneh Google ustvari kopijo teh spletnih strani, ki se potem analizirajo s t. i. funkcijo indeksiranja, pri čemer se pripravijo ključne besede in iskalni nizi, ki se potem shranijo v indeks iskalnika. Ključne besede skupaj z URL-naslovi sestavljajo indeks iskalnika, ki pravzaprav omogoča iskanje po spletnih straneh.[136] Tovrstna operacija se po mnenju generalnega pravobranilca – menim, da utemeljeno – šteje za »obdelovanje« v smislu Direktive 95/46/ES.

Zanimivo pa je, da je generalni pravobranilec prišel do drugačnega odgovora na vprašanje, ali je Google »upravljavec« osebnih podatkov, predvsem zato, ker so vse stranke – razen družbe Google in grške vlade – menile, da je Google mogoče označiti za »upravljavca«. Sicer je res, da z jezikovno razlago težko pridemo do rezultata, v skladu s katerim bi Google lahko bil označen za upravljavca, ki je v točki d 2. člena Direktive 95/46/ES opredeljen kot »fizičn[a] ali pravn[a] oseb[a] […], ki sam[a] ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov«. Google morda res nima pristojnosti določati namenov in sredstev obdelave *osebnih* podatkov, kakor poudarja generalni pravobranilec, saj res obdeluje »datoteke, ki nenačrtno, neselektivno in po naključju vsebujejo osebne in druge podatke«.[137] Vendar pa je taka razlaga točke d 2. člena Direktive 95/46/ES dokaj restriktivna.

Poleg tega je po mojem mnenju analogija med iskalnikom Google in katerokoli osebo, »ki je lastnik pametnega telefona, ali tabličnega računalnika, ali prenosnega računalnika«,[138] dokaj problematična. Generalni pravobranilec namreč meni, da bi razlaga navedenega člena, v skladu s katero bi se Google štel za »upravljavca«, vodila do tega, da bi bil »upravljavec« tudi vsakdo, ki uporablja pametni telefon ali računalnik. Vendar pa je treba pri tem po mojem mnenju upoštevati, za kakšne namene različni uporabniki uporabljajo navedene podatke. Google lahko na primer pridobljene podatke uporablja za profiliranje in oglaševanje – torej komercialno –, medtem ko drugi navedeni uporabniki pridobljene podatke uporabljalo le za svojo osebno rabo. Poleg tega Google *med drugim* tudi

[135] Glej sklepne predloge generalnega pravobranilca Jääskinena, predstavljene 25. junija 2013, v zadevi *Google Spain in Google* (C-131/12, še neobjavljeno v ZOdl., točka 75).

[136] Prav tam, točka 73.

[137] Prav tam, točka 81.

[138] Prav tam, točka 81.

pridobiva osebne podatke (čeprav ne le teh), drugi uporabniki pa jih načeloma ne pridobivajo.

Glede tretje skupine vprašanj, o pravici posameznika »biti pozabljen«, pa generalni pravobranilec meni, da pravo Unije – niti določbe Listine niti določbe Direktive 95/46/ES – ne vsebuje pravice »biti pozabljen«. Sicer priznava, da navedena direktiva vsebuje pravico do popravka, izbrisa, blokiranja in ugovora (točka b 12. člena Direktive 95/46/ES), vendar se ta pravica nanaša na informacije, ki so nepopolne ali netočne,[139] zato ne more biti pravna podlaga za pravico »biti pozabljen«. Prav tako po njegovem mnenju tovrstne pravice ni mogoče izpeljati iz določb Listine (varstva zasebnosti iz 7. člena Listine), saj bi bilo to v nasprotju s svobodo izražanja in obveščanja.[140]

4. Sklep

Iz navedenega izhaja, da je sprememba obstoječe zakonodaje na področju varstva osebnih podatkov nujna. Predvsem jo je treba prilagoditi informacijskim tehnologijam, s katerimi sta shranjevanje in obdelava osebnih podatkov veliko lažja in hitrejša kot s »klasičnimi« sredstvi obdelave. Z vidika varstva osebnih podatkov pa ne zbuja skrbi le današnje stanje, temveč tudi (oziroma predvsem) prihodnji razvoj. Tako na primer Google razvija storitev Glass,[141] ki bo omogočala uporabo posebnih očal, v katera bo vgrajena tehnologija z značilnostmi pametnih telefonov in s katerimi bo mogoče na govorni ukaz na primer deskati po spletu, fotografirati in posneti videoposnetke ter jih pošiljati drugim osebam, pošiljati e-pošto ali kratka sporočila sms in podobno.[142] Z vidika varstva zasebnosti in osebnih podatkov je taka tehnologija lahko problematična, saj uporabnikom na primer omogoča, da osebo fotografirajo brez njene vednosti (in s tem tudi brez njene privolitve).[143] Poleg tega omogoča prepoznavanje obraza (*face recognition*); Google je sicer napovedal, da te storitve ne bo ponudil,[144] a kljub temu so mogoče zlorabe. Še nekaj časa je torej treba počakati na sprejetje nove zakonodaje, ki bo, upajmo, s seboj prinesla tudi ustrezno raven varstva osebnih podatkov.

[139] Prav tam, točka 104.

[140] Prav tam, točka 133.

[141] Glej http://www.google.com/glass/start/.

[142] Glej na primer http://www.sociallyawareblog.com/2013/09/09/peering-into-the-future-google-glass-and-the-law/.

[143] Prav tam.

[144] Prav tam.

Literatura

Bard, Petra: Boj proti terorizmu: evropski standardi varstva osebnih podatkov in vzpostavitev družbe nadzora. *Pravna praksa*, 2009, št. 11, str. 13–14.

Burnik, Jelena: Prenovljen okvir za varstvo osebnih podatkov v EU. *Pravna praksa*, 2012, št. 19, str. 10–12.

Cerar, Miro: Vrednotna izhodišča varstva informacijske zasebnosti. *Podjetje in delo,* 2009, št. 6-7, str. 1403–1413.

Coudray, Ludovic: Case C-101/01, Bodil Lindqvist. *Common Market Law Review*, 2004, št. 5, str. 1361–1376.

Hijmans, Hielke, Scirocco, Alfonso: Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to help?. *Common Market Law Review*, 2009, št. 5, str. 1485–1525.

Kaiser, Anna-Bettina: German Federal Constitutional Court: German Data Retention Provisions Unconstitutional in Their Present Form; Decision of 2 March 2010, NJW 2010, str. 833. *European Constitutional Law Review*, 2010, št. 6, str. 503–517.

Kokott, Juliane, Sobotta, Christoph: The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, V: Hijmans, H., Kranenborg, H. (ur.), *Data protection anno 2014: How To Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004–2014)*. Intersentia, 2014, str. 83–95.

Konstadinides, Theodore: Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, *European Law Review*, 2011, št. 5, str. 722–736.

Kosta, Eleni: The Way to Luxembourg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection, *SCRIPTed*, 2013, št. 3, str. 339–363.

Larsson, Stefan: Metaphors, law and digital phenomena: the Swedish pirate bay court case, *International Journal of Law and Information Technology,* 2013, str. 1–26.

Luzak, Joasia: Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive regarding Cookies. *European Review of Private Law*, 2013, št. 1, str. 221–245.

Možina, Damjan: Varstvo osebnih podatkov na internetu – cookie: piškotek ali Veliki brat. *Pravna praksa*, 2000, št. 36-37, str. I–VII.

Siemen, Birte: Grundrechtsschutz durch Richtlinien/Die Fälle Österreichischer Rundfunk u.a. und Lindqvist, *Europarecht,* 2004, str. 306–321.

Trstenjak, Verica, Brkan, Maja: *Pravo EU. Ustavno, procesno in gospodarsko pravo EU*, GV Založba, Ljubljana 2012.

Trstenjak, Verica: Sodna praksa Sodišča ES na področju varstva osebnih podatkov. *Podjetje in delo*, 2009, št. 6-7, str. 1414–1422.

Tzanou, Maria: *The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement*, doktorska disertacija, European University Institute, Department of Law, 2012.

II.
Intelektualna lastnina v informacijski družbi

Digitalizacija in osirotela dela

dr. Maja Bogataj Jančič, Jernej Pusser

Predlog Direktive o osirotelih delih je kljub večletnemu prizadevanju Evropske komisije za ureditev te problematike izgubljena priložnost.[1]

1. Uvod

Digitalizacija kulturnega gradiva olajšuje dostop do svetovnega znanja, zbranega v pisnem, zvočnem, filmskem in drugem gradivu, ki je na voljo v knjižnicah, muzejih, galerijah, arhivih in drugih ustanovah za varstvo kulturne dediščine. Digitalizacija ni samo pomembno sredstvo za zagotavljanje boljše dostopnosti kulturnega gradiva in njegove uporabe, ampak je lahko v nekaterih primerih edini način za ohranitev kulturnega gradiva za prihodnje generacije in je tudi zato izjemnega pomena.

Povsod po svetu potekajo veliki projekti javne ali zasebne digitalizacije kulturne dediščine. Tudi Evropa si s spodbujanjem digitalizacije kulturnega gradiva prizadeva ponuditi svojim državljanom širok dostop do raznovrstne in večjezične kulturne dediščine, hkrati pa ohraniti vodilni mednarodni položaj na kulturnem področju in področju kreativnih vsebin.[2] Eden velikih problemov pri digitalizaciji kulturne dediščine je, da velik del gradiva, ki ga hranijo knjižnice, arhivi in muzeji, ni javno dostopen v tem smislu, da ni ali ni več varovan s pravicami intelektualne lastnine, zlasti z avtorskimi pravicami.[3] Pred objavo del v digitalizirani obliki je zato treba razčistiti avtorske pravice, to je od imetnikov pravic na delih, ki se digitalizirajo, pridobiti ustrezne pravice. Postopek pridobivanja teh pravic je lahko oviran ali celo onemogočen, če katerega od imetnikov pravic tudi po skrbni preiskavi ni mogoče identificirati ali najti.[4] V takšnem primeru govorimo o osirotelem delu.

---

[1] M. Ress.

[2] Priporočilo Komisije o digitalizaciji in spletni dostopnosti kulturnega gradiva ter njegovi digitalni hrambi.

[3] Prav tam.

[4] L. Virag.

2. Direktiva o osirotelih delih

V avtorskem pravu ni enotne definicije osirotelega dela, vendar pa so bistveni elementi v vseh definicijah enaki: osirotelo delo je avtorskopravno varovano delo, v zvezi s katerim ni mogoče izslediti imetnika pravic.[5] S primerjalnopravnega vidika je mogoče govoriti o različnih nacionalnih sistemih obravnavanja osirotelih del, o tem pa je podrobneje pisala že Eneja Drobež v članku,[6] objavljenem v reviji Pravnik. Tu se bomo osredinili le na evropski vidik problematike osirotelih del.

Problematika osirotelih del je bila kot ena pomembnejših ovir pri izvajanju obsežnih procesov digitalizacije in spletne dostopnosti kulturnega gradiva v Evropi prepoznana že leta 2006, ko je Evropska komisija izdala priporočilo,[7] v katerem je države članice spodbujala k vzpostavitvi mehanizmov za omogočanje uporabe osirotelih del in vzpostavitvi javno dostopnih seznamov znanih osirotelih del. V tem času je Evropska komisija ustanovila tudi posebno skupino strokovnjakov na visoki ravni (High Level Expert Group, HLEG),[8] da bi Komisiji svetovala glede organizacijskih, pravnih in tehničnih vprašanj ter prispevala k skupnemu pogledu v zvezi evropskimi digitalnimi knjižnicami. Na prvem srečanju je bila pod vodstvom profesorja Marca Ricolfija imenovana podskupina za avtorsko pravo, ki je po dveh vmesnih poročilih junija 2008 predstavila končno poročilo, v katerem je problematiko osirotelih del prepoznala kot eno ključnih področij v zvezi z digitalizacijo gradiva in delovanjem digitalnih knjižnic. Poročilu skupine strokovnjakov je leta 2011 sledilo poročilo posvetovalnega odbora na visoki ravni (t. i. odbora modrecev) o digitalizaciji evropske kulturne dediščine. Poročilo z naslovom The New Renaissance[9] je bilo pripravljeno na predlog evropske komisarke za digitalno agendo Neelie Kroes in evropske komisarke za izobraževanje in kulturo Androulle Vassiliou ter predstavljeno 10. januarja 2011. Odbor v poročilu države članice EU poziva, naj okrepijo prizadevanja za prenos zbirk, ki jih hranijo v knjižnicah, arhivih in muzejih, na splet, poudarja pa tudi nujnost rešitve problematike osirotelih del. Odbor tako navaja, da je za reševanje tega vprašanja treba kar se da hitro uzakoniti evropski pravni instrument. Končni rezultat teh prizadevanj je 27. oktobra 2012 sprejeta Direktiva o osirotelih delih[10] (v nadalje-

[5] Prav tam. str. 10.

[6] E. Drobež. str. 706–720.

[7] Priporočilo Komisije z dne 24. 8. 2006 o digitalizaciji in spletni dostopnosti kulturnega gradiva in digitalnem arhiviranju (2006/585/ES).

[8] Sklep Komisije z dne 27. 2. 2006 o ustanovitvi skupine strokovnjakov na visoki ravni za digitalne knjižnice.

[9] Comité des Sages, The New Renaissance, Reflection Group on bringing Europe's cultural heritage online.

[10] UL L 299, z dne 27. 10. 2012.

vanju Direktiva), ki po mnenju Evropske komisije prinaša učinkovito in trajno rešitev za uporabo osirotelih del v procesih digitalizacije kulturnega gradiva.

Direktiva naj bi bila eden pomembnejših končanih projektov Evropske komisije v sklopu Digitalne agende za Evropo. Splošni cilj digitalne agende je poskrbeti, da bo enotni digitalni trg prispeval k zagotavljanju trajnih gospodarskih in družbenih koristi za Evropsko unijo.[11] Sodobna digitalna tehnologija, ki je motor razvoja evropskega digitalnega trga, med drugim ponuja izjemne možnosti za digitalizacijo, razširjanje in vnovično uporabo evropske kulturne dediščine, s čimer se zagotavljajo nove možnosti gospodarskega in družbenega razvoja, kar vodi k družbenemu napredku in povečanju družbene blaginje. Pri izkoriščanju teh možnosti imajo ključno vlogo kulturne institucije, kot so to knjižnice, arhivi in muzeji, ki pod svojo streho hranijo ogromno kulturnega in znanstvenega gradiva. Vzpostavitev digitalnih zbirk podatkov je kljub razvoju tehnike zahteven podjem, ki ga poleg visokih stroškov omejujejo tudi določbe avtorskopravne zakonodaje. Postavlja se vprašanje, ali je Evropska komisija izkoristila priložnost in z Direktivo res izboljšala pravni okvir za učinkovitejšo digitalizacijo osirotelih del, njihovo razširjanje in vnovično uporabo ali pa je Direktiva rezultat slabih kompromisov in prinaša več težav kot učinkovitih rešitev.

Kot pojasnjuje 1. člen Direktive, se ta nanaša na določene vrste uporabe osirotelih del s strani javno dostopnih knjižnic, izobraževalnih ustanov in muzejev ter tudi arhivov, ustanov filmske in avdio dediščine in javnih RTV-organizacij, s sedežem v državah članicah. V nadaljevanju so primeroma našteta dela, za katera se Direktiva uporablja, pri čemer je pomemben zlasti 2. člen, ki določa pogoje, kdaj je neko delo mogoče šteti za osirotelo. Po 2. členu Direktive so osirotela dela tista, pri katerih nihče izmed imetnikov pravic na delu ali fonogramu, kljub opravljenemu in zabeleženemu skrbnemu iskanju, ni opredeljen ali najden. Definicija »skrbnega iskanja« je zapisana v 3. členu Direktive, ki določa, da za namene odločitve, ali spada delo ali fonogram med osirotela dela, organizacije iz 1. člena Direktive zagotovijo, da se za vsako delo ali druge zaščitene vsebine izvede skrbno iskanje v dobri veri, s pregledom ustreznih virov za kategorijo zadevnih del in drugih zaščitenih vsebin. Skrbno iskanje je treba opraviti pred uporabo dela ali fonograma. V prilogi Direktive je seznam virov in podatkovnih baz, ki jih mora uporabnik upoštevati, v domeni držav članic pa je, da določijo vire, ki so ustrezni za posamezno kategorijo del ali fonogramov.[12] Direktiva v 4. členu določa, kakšni so pogoji za medsebojno priznavanje statusa osirotelega dela. Delo ali fonogram, ki se v eni državi članici šteje za osirotelo delo, se v skladu z 2. členom šteje za osirotelo delo v vseh državah članicah. V 5. členu Direktiva pojasnjuje, da morajo

[11] Več o Digitalni agendi za Evropo na http://ec.europa.eu/digital-agenda/.

[12] Glej tudi E. Drobež, str. 703.

države članice zagotoviti, da imajo imetniki pravic do dela ali fonograma, ki se šteje za osirotelo delo, kadarkoli možnost, da status osirotelega dela odpravijo, kar zadeva njihove pravice. Države članice morajo zato po prvem odstavku 6. člena urediti izjemo glede pravice reproduciranja ali pravice dajanja na voljo javnosti tako, da navedenim neprofitnim organizacijam omogočijo, da osirotela dela reproducirajo v digitalni obliki in jih dajejo na voljo javnosti, vendar pa ima nacionalni zakonodajalec pri določitvi izjeme v korist uporabnikov osirotelih del obveznost, da zagotovi, da ima pozneje najdeni imetnik pravic na osirotelem delu možnost prepovedati nadaljnjo uporabo tega dela ter da pozneje najdeni imetnik pravic prejme tudi pošteno nadomestilo za dotedanjo uporabo dela.[13] Države članice morajo sprejeti ustrezne zakone in druge predpise, potrebne za uskladitev določb Direktive z nacionalnim pravnim redom, najpozneje do 29. oktobra 2014.

3. Avtorskopravne ovire pri digitalizaciji

Večina del, ki se digitalizirajo, je varovana z avtorsko oziroma avtorski sorodno pravico, kar pomeni, da imajo avtorji teh del izključne materialne in moralne pravice do njihove uporabe v telesni ali netelesni obliki. Za objavo del v okviru projektov digitalizacije je treba od avtorjev ali imetnikov pravic pridobiti ustrezne materialne avtorske pravice: pravica reproduciranja je praviloma omejena že na podlagi zakona, odločilna za ponujanje del prek spleta pa je pravica dajanja na voljo javnosti, ki jo je treba razčistiti.[14]

Že ob nastanku Europeane,[15] enega največjih projektov digitalizacije v Evropski uniji, ki naj bi ponujal velike priložnosti za ustvarjalce, raziskovalce, študente in vse druge, ki bi se po vsem širnem svetu radi poučili o bogati evropski zgodovini in kulturi, shranjeni v virih, ki so z digitalizacijo postali globalno dostopni, se je postavljalo vprašanje, zakaj znanje, zakladi in viri, ki so nastali v prejšnjem stoletju, niso dostopni. Odgovor se skriva v avtorskem pravu oziroma v posledicah, ki se kažejo v težavah in velikanskih transakcijskih stroških, povezanih z razčiščevanjem avtorskih pravic.[16]

Dodatne težave in stroški nastanejo, kadar imetnikov pravic niti s skrbno preiskavo ni mogoče ugotoviti ali najti. V tem primeru govorimo o osirotelih delih, ki, kot pojasnjuje Paul Keller v prispevku Communiae,[17] postanejo »žrtev«

[13] Prav tam.

[14] Glej 32.a člen Zakona o avtorski in sorodnih pravicah (ZASP), Uradni list RS, št. 21/1995, s spremembami.

[15] Glej http://www.europeana.eu (20. 3. 2014).

[16] M. Bogataj Jančič. str. 1235.

[17] Glej P. Keller.

rigidnih avtorskopravnih pravil, ki ne gredo v korak z družbenimi in tehnološkimi spremembami. Osirotelih del ni mogoče zakonito uporabljati, saj zanje ni mogoče pridobiti ustreznih pravic. Dela, katerih avtorjev oziroma imetnikov pravic ni mogoče najti, tako ostajajo skrita globoko v arhivih kulturnih institucij. To zmanjšuje družbeno blaginjo, saj od neobjave del nimajo koristi niti avtorji oziroma imetniki pravic na teh delih, ki bi z objavo lahko spet pridobili nadzor nad pravicami, niti kulturne institucije, ki so vlagale v zbiranje in ohranjanje osirotelih del, niti končni uporabniki, ki posredno prek javnih dajatev financirajo dejavnosti kulturnih institucij in bi si zato želeli dostop do čim večjega števila del.[18] Ocenjuje se, da je v Evropski uniji okoli 3 milijone osirotelih del.[19]

4. Pomanjkljivosti Direktive

In harmonia progressio,[20] toda sprejeta Direktiva ima številne pomanjkljivosti, zaradi katerih je njen prispevek k reševanju problema osirotelih del dvomljiv.

Kot izhaja iz preambule Direktive, je njen temeljni namen omogočiti uporabo avtorsko varovanega dela brez dovoljenja pogrešanega imetnika pravic pod posebnimi pogoji.[21] Že v uvodnih določbah pa se pokaže prva in ena večjih pomanjkljivosti Direktive, in sicer njena ozkost.[22] Direktiva namreč dovoljuje uporabo osirotelih del samo javno dostopnim knjižnicam, izobraževalnim ustanovam, muzejem, arhivom in ustanovam filmske ali avdio dediščine in javnim RTV-organizacijam.[23] Samo navedene organizacije so na podlagi pogojev, ki jih določa Direktiva, in v skladu s cilji javnega interesa upravičene do uporabe osirotelih del. Ker pa dostop do kulturnega bogastva lahko ponujajo tudi drugi subjekti na trgu, na primer posamezniki ali pa zasebne nepridobitne pobude (npr. Wikipedia), bi se obseg upravičencev do uporabe osirotelih del v skladu z določbami Direktive moral razširiti tudi na te uporabnike osirotelih del. Prispevek nepridobitnih organizacij k ohranjanju in prenašanju kulturne dediščine je seveda zelo pomemben, toda Direktiva bi za dosego svojega cilja morala upoštevati tudi profitne organizacije, zlasti kadar imajo te močan vpliv na delovanje notranjega trga.[24] Dodatna omejitev je določba, da se Direktiva uporablja samo za dela, ki so v zbirkah neprofitnih

[18] Analiza družbenih stroškov osirotelih del je prikazana tudi v študiji Orphan Works, Analysis and Proposal, Center for the Study of the Public Domain. Duke Law School, http://web.law.duke.edu/cspd/pdf/cspdproposal.pdf (20. 3. 2014).

[19] Glej A. Vuopala.

[20] Slovensko: Usklajevanje vodi k napredku.

[21] Glej tretjo uvodno izjavo Direktive 2012/28/EU.

[22] Podobno ugotavlja tudi M. Ress.

[23] Glej prvi odstavek 1. člena Direktive 2012/28/EU.

[24] Glej M. Ress.

organizacij. Tako so, kot opozarja Paul Keller v prispevku Communiae,[25] zaradi ozkega kroga upravičencev, na katere se direktiva nanaša, lahko ogroženi projekti digitalizacije osirotelih del, organizirani v obliki javno-zasebnih partnerstev. Glavna spodbuda za zasebne partnerje, ki vlagajo v digitalizacijo kulturnih vsebin, je pogosto tudi uporaba vsebin v njihovih lastnih storitvah. Če zasebnim partnerjem ne bo dovoljeno uporabljati osirotelih del, bodo pri sklepanju javno-zasebnih partnerstev digitalizacijo osirotelih del najverjetneje izključili.

Problematična je tudi večplastna definicija osirotelih del. Določbe Direktive se uporabljajo samo za dela, objavljena v obliki knjig, revij, časopisov in drugih besedil, vključno z deli, ki jih ta dela vsebujejo, ter tudi za dela, predvajana ali objavljena v obliki avdiovizualnih ali kinematografskih del, vključno s fonogrami.[26] Direktiva se tako na primer ne nanaša na fotografije, ki so pogosto pomemben del zbirk kulturnih ustanov, kar pomeni, da je digitalizacija tovrstnih osirotelih del še vedno nemogoča. Naslednji pogoj, ki mora biti izpolnjen, da lahko govorimo o osirotelih delih, je, da so bila prvič objavljena ali predvajana v eni od držav članic EU. Šteje se, da ta pogoj izpolnjujejo tudi dela, ki so jih organizacije iz prvega odstavka dale na voljo javnosti ob soglasju imetnikov pravic, če se upravičeno domneva, da imetniki pravic ne bi oporekali uporabi iz 6. člena Direktive. Končno je za definicijo osirotelih del pomembno tudi to, da so dela varovana z avtorskimi ali sorodnimi pravicami, saj v nasprotnem primeru ni potrebno razčiščevanje pravic za uporabo teh del.

Za knjižnice, izobraževalne ustanove, muzeje, arhive in javne RTV-organizacije je težavno vprašanje, na kakšen način in s kolikšno stopnjo verjetnosti je treba ugotoviti, da je avtorsko delo resnično osirotelo. Povedano drugače, kakšen je postopek, na podlagi katerega je mogoče skleniti, da imetnika pravic na posameznih delih v zbirkah upravičencev ni mogoče najti. Direktiva zahteva, da uporabniki osirotelih del v dobri veri (*in good faith*) izvedejo posebno skrbno iskanje (*dilligent search*) za vsako posamezno delo, za katero ni mogoče ugotoviti ali najti imetnika pravic.[27] Skrbno iskanje, kot ga predvideva Direktiva, vsebuje najmanj pregled virov, ki so določeni v Prilogi Direktive, ter shranjevanje in objavo rezultatov iskanja v posebej temu namenjenih nacionalnih in evropskih evidencah.[28] Problem, na katerega so opozarjali že upravičenci Direktive v postopku sprejemanja direktive, so visoki stroški izvedbe takšnega skrbnega pregleda. Dodatno negotovost in tveganje za upravičence pomeni tudi pogoj dobre vere, ki ga morajo upoštevati. V tem delu se žal jasno kaže miselnost evropskega

[25] Glej P. Keller.

[26] Glej 2. člen Direktive 2012/28/EU.

[27] Glej prvi odstavek 3. člena Direktive 2012/28/EU.

[28] Glej drugi, četrti in peti odstavek 3. člena Direktive 2012/28/EU.

zakonodajalca pri sprejemanju zakonodaje o osirotelih delih, ki predpostavlja, da so upravičenci Direktive tudi potencialni kršitelji avtorskopravne zakonodaje, zaradi česar Direktiva zavzema obrambni položaj in določa večplasten in strog test ugotavljanja osirotelih del. Tako so znova ogroženi procesi digitalizacije gradiva v zbirkah upravičencev Direktive. Jasno je namreč, da si nepridobitne javne ustanove zaradi omejenih sredstev pogosto ne morejo privoščiti tako obširnega pregleda in razčiščevanja pravic na osirotelih delih.[29]

Negotovost uporabnikov osirotelih del še dodatno povečuje 5. člen Direktive, ki določa, da imajo imetniki pravic na osirotelih delih možnost kadarkoli odpraviti status osirotelega dela. Dodatno peti odstavek 6. člena Direktive daje imetnikom pravic možnost zahtevati tudi plačilo poštenega nadomestila (*fair compensation*) za preteklo uporabo njihovega dela kot osirotelega dela v skladu z določbami Direktive. Takšna ureditev nikakor ne spodbuja upravičencev Direktive k vlaganju sredstev v uporabo oziroma digitalizacijo osirotelih del, saj morajo poleg stroškov skrbnega iskanja računati tudi na potencialne stroške za kompenzacije tistim avtorjem oziroma imetnikom pravic, ki bodo *ex tunc* zahtevali plačilo za izkoriščanje njihovih pravic na osirotelih delih. V nekaterih primerih bodo upravičene organizacije tako imele dvojne stroške pri uporabi osirotelih del – stroške razčiščevanja in stroške kompenzacije za uporabo osirotelih del za nazaj.[30]

Tudi koristi od uporabe osirotelih del ne pretehtajo stroškov razčiščevanja pravic na teh delih. Direktiva upravičenim organizacijam dovoljuje samo dajanje na voljo javnosti in reproduciranje z namenom digitalizacije, razpolaganja, označevanja, katalogiranja, ohranjanja ali obnavljanja osirotelih del v skladu s cilji javnega interesa.[31] Zaprt seznam oblik uporabe osirotelih del je problematičen zlasti z dveh vidikov. Kot pojasnjuje Keller, seznam našteva oblike uporabe del, ki niso zajete z Direktivo o avtorski pravici v informacijski družbi,[32] na primer katalogiranje in označevanje, kar lahko pomeni tudi prikrite težnje po širitvi obsega avtorskopravnega varstva.[33] Opozarja, da tako zaprt seznam dovoljenih oblik uporabe osirotelih del pomeni tudi neustrezno rešitev v povezavi s hitrim tehnološkim razvojem. Glede na izkušnje z drugih področij urejanja avtorske pravice v povezavi z novimi tehnologijami[34] bi pričakovali, da bo Direktiva

[29] Glej tudi podobno kritiko glede višine stroškov razčiščevanja pravic v članku M. Ress.

[30] Glej P. Keller.

[31] Glej 6. člen Direktive 2012/28/EU.

[32] Glej Direktivo 2001/29/ES Evropskega parlamenta in Sveta z dne 22. 5. 2001 o usklajevanju določenih vidikov avtorske in sorodnih pravic v informacijski družbi.

[33] Glej P. Keller.

[34] Glej zlasti razprave v zvezi s spremembami Direktive Sveta 93/83/EGS z dne 27. 9. 1993 o uskladitvi določenih pravil o avtorski in sorodnih pravicah v zvezi s satelitskim radiodifuznim oddajanjem in kabelsko retransmisijo.

predvidela hiter tehnološki razvoj in dovoljevala tudi druge, v tem trenutku še ne razvite oblike digitalnega izkoriščanja osirotelih del. To pomeni, tako tudi Keller,[35] da bi Direktiva morala dovoliti upravičenim uporabnikom uporabo osirotelih del na kakršenkoli način, ki je v skladu z javnim interesom teh organizacij, ne pa da določa zaprt in nepopoln seznam dovoljenih oblik uporabe, ki je lahko ob hitrem razvoju tehnologije in novih oblikah izkoriščanja del že jutri ovira za uporabo osirotelih del.

S tem ko Direktiva zahteva natančno določen namen uporabe osirotelih del, izključuje množično širjenje in uporabo osirotelih del s strani njenih upravičencev in končnih uporabnikov. Z omejevanjem uporabe osirotelih del Direktiva ne omogoča prožnosti, ki je nujno potrebna za uporabnike del v digitalnem okolju.[36]

5. Implementacija v Republiki Sloveniji

Slovenija mora Direktivo o osirotelih delih ne glede na njene pomanjkljivosti implementirati do 29. oktobra 2014, sicer jo lahko doletijo sankcije. Slovenija bo Direktivo implementirala s spremembo Zakona o avtorski in sorodnih pravicah.

Smiselno je, da Slovenija pri implementaciji sledi navodilom, ki bodo javnim institucijam pomagala pri izvajanju obveznosti zaradi spremembe avtorskopravne zakonodaje, kot jo narekuje Direktiva.[37] Navodila, ki jih razlagamo v nadaljevanju, je pripravila organizacija EIFLA.

5.1. Slovenija naj pri implementaciji ne dodaja virov

Za objavljena dela mora biti skrbno iskanje izvedeno v državah članicah, kjer so dela prvič objavljena, ne pa tam, kjer ima institucija svoj sedež. Skrbno iskanje imetnikov pravic je potrebno tudi za dela, ki so vključena v posamezna dela ali fonograme, saj se ta štejejo za ločena od glavnega dela. Vire, ki so ustrezni za izvedbo skrbnega iskanja za posamezno kategorijo avtorskih del, določi vsaka država članica po posvetovanju z imetniki pravic in uporabniki. Kot minimum pri skrbnem iskanju je treba upoštevati vire, ki so navedeni v prilogi k Direktivi. Države članice lahko pri implementaciji Direktive dodajo vire, kar pa ni priporočljivo, saj je že obstoječ seznam zelo obsežen in zahteven. Z dodajanjem virov bi se postopek preverjanja lahko še dodatno zapletel.

[35] Glej P. Keller.

[36] Glej M. Ress.

[37] Glej EIFLA, http://www.eifl.net (20. 3. 2014).

5.2. Primerna določitev poštenega nadomestila v skladu z Direktivo 2001/29/ES[38]

Države članice zagotovijo, da imetniki pravic, ki za svoje delo ali druge varovane vsebine odpravijo status osirotelega dela, prejmejo pošteno nadomestilo za dotedanjo uporabo teh del ali drugih varovanih vsebin. Državam članicam, v katerih ima organizacija, ki uporablja osirotelo delo, sedež, je prepuščeno, da določijo okoliščine, v katerih se sme organizirati plačilo takšnega nadomestila. Pri določanju višine poštenega nadomestila bi bilo treba med drugim ustrezno upoštevati nekomercialno uporabo s strani zadevnih organizacij, doseganje ciljev v zvezi z njihovim poslanstvom in javnim interesom ter morebitno oškodovanje imetnikov pravic. Direktiva 2001/29/ES določa, da v določenih situacijah, ko je škoda imetnika pravic minimalna, plačilo ni potrebno.[39] Nadomestilo za uporabo osirotelih del naj sledi istemu načelu, posebno v primerih, ko so dela že dolgo zunaj komercialne rabe.

5.3. Primeren sistem za dokazovanje upravičenosti zahtevka za nadomestilo

Imetnik pravic, ki uveljavlja svoje pravice na osirotelem delu, mora brez dvoma dokazati obseg svojih pravic na osirotelem delu (imetnik lahko deli pravice tudi z drugimi, neugotovljenimi imetniki pravic). Države članice naj uzakonijo predvidljiv in preprost sistem za dokazovanje upravičenosti zahtevkov, ki bo zagotavljal ustrezno pravno varnost.

5.4. Poseben režim dostopa do neobjavljenih del

Direktiva se nanaša le na objavljena dela. Države članice naj vzpostavijo poseben režim za neobjavljena dela, ki naj bodo na vpogled v kulturnih institucijah z dovoljenjem imetnika pravic.

Direktiva predvideva možnost, da države članice določijo, da se Direktiva nanaša tudi na neobjavljena dela, ki bodo izročena knjižnici ali drugi kulturni instituciji po 29. oktobru 2014, saj je smiselno, da se Direktiva nanaša na čim širši krog avtorskih del.

[38] Glej Direktivo 2001/29/ES Evropskega parlamenta in Sveta z dne 22. 5. 2001 o usklajevanju določenih vidikov avtorske in sorodnih pravic v informacijski družbi.

[39] Glej 35. uvodno izjavo Direktive 2001/29/ES.

6. Sklep

Kljub trudu Evropske komisije, da bi spodbudila digitalizacijo gradiva kulturnih institucij in s tem omogočila množičen dostop do evropske kulturne dediščine, sprejeta Direktiva ne rešuje problemov glede osirotelih del, ampak jih še povečuje. Visoki stroški izvedbe skrbnega pregleda bodo za slovenske javne ustanove najverjetneje nepremagljiva ovira in ne spodbuda za digitalizacijo zbirk podatkov, ki bodo tako ostali zakopani globoko v arhivih in skladiščih. Dodatna težava je pravna negotovost, povezana z uporabo osirotelih del, še zlasti, če nacionalni zakonodajalec ne bo določil jasnih pravil glede nadomestil oziroma določil, da je nadomestilo v posebnih primerih lahko minimalno oziroma enako nič.

Direktiva ni izpolnila pričakovanj, ampak prinaša dodatne administrativne ovire, ki bodo v nekaterih primerih za javne ustanove in nepridobitne projekte nepremagljive. Z določanjem dodatnih in nepotrebnih omejitev je slab primer reševanja avtorskopravnih problemov novega tisočletja. Direktiva, ki so jo javne knjižnice, arhivi in muzeji težko pričakovali, je slab kompromis, ki prinaša več novih težav kot rešitev.

Literatura

Bogataj Jančič, Maja: Avtorskopravne ovire digitalizacije javnih knjižnic (Google v. Europeana). *Podjetje in delo*, št. 6-7/2009, str. 1235–1248.

Comite des sages, The New Renaissance, Reflection Group on bringing Europe's cultural heritage online, dostopno na http://ec.europa.eu/information_society/activities/digital_libraries/comite_des_sages/index_en.htm (24. 3. 2014).

Digitalna agenda za Evropo, http://ec.europa.eu/digital-agenda/ (20. 3. 2014).

Drobež, Eneja: Osirotela dela v primerjalnem in evropskem pravu. *Pravnik*, št. 9-10/2013, str. 706–720.

EIFLA, http://www.eifl.net (20. 3. 2014).

EUROPEANNA, http://www.europeana.eu (20. 3. 2014).

Keller, Paul: *Orphan works' compromise fails to deliver*, objavljeno 25. 6. 2012 in dostopno na http://www.communia-association.org/2012/06/25/orphan-works-compromise-fails-to-deliver/ (19. 2. 2014).

Orphan Works, Analysis and Proposal, Center for the Study of the Public Domain. Duke Law School, http://web.law.duke.edu/cspd/pdf/cspdproposal.pdf (20. 3. 2014).

Ress, Manon: *The European Orphan Works Directive: a missed opportunity?*, dostopno na: http://www.keionline.org/node/1445 (21. 3. 2014).

Virag, Luka: *Problematika osirotelih del pri digitalizaciji vsebin javnih knjižnic*. Diplomsko delo. Pravna fakulteta Univerze v Ljubljani, Ljubljana 2011.

Vuopala, Anna: *Assessment of the Orphan works issue and Cost for Rights Clearance,* EC DG Information Society and Media, May 2010, dostopno na http://ec.europa.eu/information_society/activities/digital_libraries/doc/reports_orphan/anna_report.pdf (19. 2. 2014).

Direktiva 2012/28/EU o nekaterih dovoljenih uporabah osirotelih del, UL L 299, z dne 27. 10. 2012.

Direktiva 2001/29/ES Evropskega parlamenta in Sveta z dne 22. 5. 2001 o usklajevanju določenih vidikov avtorske in sorodnih pravic v informacijski družbi. UL L 167, z dne 22. 6. 2001.

Priporočilo Komisije z dne 24. 8. 2006 o digitalizaciji in spletni dostopnosti kulturnega gradiva in digitalnem arhiviranju (2006/585/ES).

Priporočilo Komisije z dne 27. 10. 2011 o digitalizaciji in spletni dostopnosti kulturnega gradiva ter njegovi digitalni hrambi, dostopno na: http://ec.europa.eu/information_society/activities/digital_libraries/doc/recommendation/recom28nov_all_versions/sl.pdf (24. 3. 2014). str. 1–2.

Sklep Komisije z dne 27. 2. 2006 o ustanovitvi skupine strokovnjakov na visoki ravni za digitalne knjižnice, dostopno na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:063:0025:0027:SL:PDF (20. 3. 2014), spletna stran Skupine http://ec.europa.eu/information_society/activities/digital_libraries/experts/hleg/index_en.htm (20. 3. 2014).

Zakon o avtorski in sorodnih pravicah (ZASP), Uradni list RS, št. 21/1995, s spremembami.

Nekateri avtorskopravni problemi vzpostavitve digitalnega repozitorija na Univerzi v Ljubljani

dr. Miha Juhart

1. Uvod

Univerza je prostor, v katerem nenehno poteka ustvarjalni proces kreiranja novega znanja, v tem procesu pa nenehno nastajajo intelektualne stvaritve, ki izpolnjujejo vse elemente avtorskega dela. Pri tem gre tako za različne vrste avtorskih del kot tudi za različne vloge, ki jih imajo ustvarjalci v študijskem procesu. Že zdavnaj so minili časi, ko so v pedagoško-raziskovalnem procesu ustvarjali samo univerzitetni učitelji in sodelavci. Prispevek študentov k ustvarjanju znanja je vse bolj opazen in uživa celovito avtorskopravno zaščito. Poslanstvo univerzitetnega prostora pa ni samo ustvarjanje novega znanja, ampak že po definiciji tudi njegova širitev in s tem ustvarjanje razmer za novo in novo ustvarjanje. Gre torej za cikličen proces, ki je zgodovinsko gledano gibalo tehnološkega in družbenega razvoja, kar najlepše izraža pogosto navedena misel velikega uma Isaaca Newtona: »Če sem videl dlje, sem zaradi tega, ker sem stal na ramenih velikanov.«

Načini in možnosti za razširjanje znanja so se skozi čas spreminjali, in če je prvo veliko prelomnico v tem pomenil tisk, je druga brez dvoma informacijska tehnologija. Objave na spletu omogočajo hiter, preprost in učinkovit dostop do znanstvenih besedil in bistveno spreminjajo razmerja, ki so pred tem temeljila na tiskanih objavah in ustvarila poseben položaj založnikov kot nosilcev te gospodarske dejavnosti. Poseben položaj založnikov tudi v digitalnem okolju ohranjajo zaprti in plačljivi sistemi, povsem drugačen pa je pogled tako imenovanega gibanja za odprti dostop (*open access*), ki zagovarja pravico do popolnega in brezplačnega dostopa do znanstvenih spoznanj prek spleta.[1] Zahteva po odprtem dostopu je toliko bolj utemeljena, ko gre za javne univerze, ki se financirajo predvsem iz javnih sredstev. Prav nobenega razloga ni, da bi si materialne koristi iz znanja, financiranega iz javnih sredstev, prisvajali založniki. V novem pristopu postaja vidna misel, da je znanje javna dobrina, zato naj korist,

[1] Glej slovensko spletno stran: http://www.openaccess.si/razlogi-za-odprti-dostop.

ki jo prinaša, uživajo tisti, ki so v ta proces vložili in ki jim je ne nazadnje to znanje tudi namenjeno.

Namen in definicijo odprtega dostopa lahko povzamemo po enem prvih dokumentov, ki so utemeljevali to usmeritev. Gre za »prosto dosegljivost na javnem internetu, ki vsakemu uporabniku omogoča, da prebere, prenese (*download*), kopira, distribuira, natisne, poišče ali objavi povezavo na celotno besedilo objave, oziroma drugačno uporabo za vsak pravno dopusten namen, brez kakršnihkoli finančnih, pravnih ali tehničnih ovir, razen tistih, ki so povezane z dostopom do interneta. Edina omejitev pri reprodukciji in distribuciji ter edina vloga avtorske pravice na tem področju bi morala biti ta, da se avtorjem zagotovita nadzor nad integriteto njihovega dela in pravica, da so ustrezno priznani kot avtorji in na ustrezen način navedeni (citirani).«[2]

Koncept odprtega dostopa se v akademskem svetu izraža predvsem na dveh področjih. Pojavlja se vse več znanstvenih in strokovnih revij, ki sledijo konceptu odprtega dostopa in objavljajo prispevke učiteljev in raziskovalcev. Univerze in druge raziskovalne inštitucije pa vzpostavljajo digitalne repozitorije, v katerih se zbirajo objave univerzitetnih učiteljev, raziskovalcev in drugih sodelavcev ter zaključna dela študentov. Takšni repozitoriji so odlična referenca kakovostne univerze, saj odkrivajo njen celotni znanstvenoraziskovalni opus. To je še posebej pomembno za javno univerzo, ki s takšno predstavitvijo uresničuje svoje poslanstvo in upravičuje družbeno vlogo. Univerzitetni repozitoriji bodo verjetno bolj ali manj prevzeli funkcijo univerzitetnih knjižnic in v srednjem roku postali templji znanja, kamor bo lahko vstopil vsak. Ti dve področji pa se vsaj delno prekrivata z dvema vsebinskima pristopoma k zagotavljanju koncepta odprtega dostopa: z odprtim dostopom do znanstvenih publikacij in odprtim dostopom do raziskovalnih podatkov. Če so objave v znanstvenih publikacijah rezultat raziskovalne dejavnosti, financirane iz javnih sredstev, naj pravila financiranja določijo ukrepe, s katerimi se bo spodbudilo objavljanje v publikacijah, ki izhajajo ob upoštevanju načel odprtega dostopa. Odprt dostop do raziskovalnih podatkov pa je mogoče zagotavljati s pravili sistemskega financiranja raziskovalne dejavnosti, ki naj takšno obveznost naložijo v proces nadzora in ocenjevanja raziskovalnih dosežkov.

Koncept odprtega odstopa je bil sprejet tudi pri nas, najprej na področju raziskovalne dejavnosti, ki se financira iz proračunskih in evropskih sredstev. S tem je upoštevano tudi priporočilo Evropske komisije o objavljanju in hrambi znanstvenih podatkov.[3] Čeprav ta dokument ni zavezujoč, ni mogoče prezreti,

[2] Open Society Institute (2002). Budapest Open Access Initiative and reaffirmed in 2012 BOAI-10: Budapest Open Access Initiative after 10 years 'Recommendations': http://www.soros.org.

[3] Glej stran http://ec.europa.eu/research/science-society/document_library/pdf_06/recommendation-access-and-preservation-scientific-information_en.pdf.

da je pomembno pospešil uveljavljanje koncepta odprtega dostopa. Priporočilo izhaja iz omenjene delitve in predvsem kaže na nekatere možne ukrepe, ki jih države članice lahko uveljavijo za doseganje ciljev. Morda velja omeniti poziv, da naj univerze v pravilih kariernega napredovanja primerno upoštevajo in nagradijo objave v publikacijah, ki temeljijo na konceptu odprtega dostopa.[4] Zahteva po odprti objavi znanstvenih podatkov pa se uveljavlja tudi v velikem evropskem raziskovalnem programu Obzorja 2020.[5] Evropska komisija v programu Obzorja 2020 posebej opozarja na pomen odprtega dostopa pri objavljanju raziskovalnih člankov v periodičnih publikacijah in objavi raziskovalnih podatkov. Uveljavljanje prednosti pri financiranju iz programa za tiste, ki upoštevajo načela odprtega dostopa, pa je verjetno tudi eden najbolj učinkovitih spodbujevalnih mehanizmov. Zato lahko utemeljeno pričakujemo, da bo koncept odprtega dostopa v prihodnjih letih temeljito posegel v način objavljanja in razširjanja znanstvenoraziskovalnih in strokovnih dosežkov.

Vzpostavitev digitalnega repozitorija je zato nujna tudi v slovenskem prostoru. Nekaterim posamičnim poskusom je sledil skupni projekt slovenskih univerz ODUN, ki so ga finančno podprli Ministrstvo za izobraževanje, znanost, kulturo in šport ter evropski strukturni skladi. Namen projekta je bilo zainteresirani javnosti doma in v tujini omogočiti dostop do intelektualne produkcije slovenskih univerz.[6] Projekt je bil uspešno končan avgusta 2013 in jeseni istega leta so na vseh štirih slovenskih univerzah zaživeli digitalni repozitoriji, ki so povezani v enoten sistem. To pa poleg osnovne funkcije razširjanja znanja omogoča tudi večji nadzor nad vsebino zaključnih del na vseh ravneh študija in s tem olajšuje odkrivanje neustreznih praks pri navajanju tujih avtorskih del. Vsako oddano zaključno delo je mogoče še pred končno oceno na enostaven način primerjati z vsemi objavami v skupnem repozitoriju in ga izločiti, če ne izpolnjuje pogoja samostojnega ustvarjanja oziroma prikazuje tuje delo kot lastno.[7] Ker je tako imenovano plagiatorstvo v zadnjem času vse bolj pogosto, je pomagalo, ki naj bi močno omejilo možnosti nepoštenih ravnanj, zelo dobrodošlo.

[4] Na večini univerz sistem kariernega napredovanja temelji na kvalitativni oceni posameznikovega dela, pri čemer se upoštevata predvsem rangiranje znanstvene publikacije in faktor njenega vpliva. Oba kazalnika kakovosti je mogoče doseči s potekom časa, zato so nove znanstvene publikacije v tem pogledu za objavo manj zanimive, saj ne dosegajo želene ravni.

[5] Glej podrobneje http://ec.europa.eu/research/science-society/document_library/pdf_06/background-paper-open-access-october-2012_en.pdf.

[6] Glej M. Ojstršek, Predstavitev možnosti vključitve raziskovalnih podatkov v nacionalno infrastrukturo odprtega dostopa, http://www.adp.fdv.uni-lj.si/odpp10D3/presentations/Milan_Ojstersek.pdf.

[7] Glej podrobneje M. Juhart, Razlogi in postopek za odvzem naslova v aktih Univerze v Ljubljani, Podjetje in delo, št. 6-7/2013.

2. Način objave v konceptu odprtega dostopa

Bistvena značilnost odprtega dostopa je zagotavljanje znanstvenoraziskovalnih objav na svetovnem spletu brez naročniških ali avtorskopravnih omejitev. Odprtodostopna publikacija (*libre open access*) ustreza tema kriterijema:

- »avtor in nosilec materialne avtorske pravice vsem uporabnikom v svetovnem merilu dajeta prosto, nepreklicno in stalno pravico dostopa do publikacije ter dovoljujeta razmnoževanje, uporabo, razširjanje, prenos in javni prikaz dela, izdelavo in distribucijo izpeljanih del v kateremkoli digitalnem mediju za katerikoli odgovoren namen (dovoljeno uporabo označita npr. z licencami avtorskopravnega modela Creative Commons) in dopuščata, da uporabniki naredijo manjše število izpisov za lastno uporabo,
- celotna publikacija in vsa dodatna gradiva, vključno z dovoljenjem iz prejšnje točke, so takoj po objavi odloženi v vsaj en spletni repozitorij, ki omogoča prost dostop, neomejeno distribucijo, medobratovalnost (interoperabilnost) in trajno hranjenje.«[8]

V praksi se pojavljata dva načina.[9] O »zelenem« odprtem dostopu (*green open access*) ali samoarhiviranju govorimo, če avtor prispevek shrani v digitalnem repozitoriju matične institucije pred objavo v znanstvenem tisku ali hkrati z njo. Pri takšnem pristopu je mogoč kompromis med interesi založnikov plačljivih znanstvenih publikacij in konceptom odprtega dostopa tako, da se dostopnost vpogleda v objavljeno besedilo v repozitoriju za določen čas zadrži (*embargo period*). V tem času, ko objava pomeni novost in je vsaj na nekaterih področjih znanstvenega ustvarjanja tudi interes za seznanitev z njeno vsebino največji, je ohranjen poseben položaj plačljivih medijev in omejen splošni dostop. Šele po poteku tega časa pa objava zaživi v skladu z vsemi načeli odprtega dostopa. V današnjem času je to verjetno nujen kompromis, njegov bistveni problem pa je seveda določanje časa embarga. Pričakovati je mogoče, da se bo ta čas s krepitvijo koncepta odprtega dostopa skrajševal. Drugi način je »zlati« odprti dostop (*gold open access*), pri katerem že prva objava znanstvenega dela izpolnjuje pogoje za odprt dostop. Gre predvsem za objave v znanstvenih publikacijah, ki same delujejo po pravilih odprtega dostopa. Njihovo število se povečuje, zvišuje pa se tudi njihov faktor vpliva.

Večina znanstvenoraziskovalnih objav ima vse lastnosti avtorskega dela, zato je treba tudi v konceptu odprtega dostopa upoštevati vsa pravila avtorskega prava. Na pomen avtorskopravne urejenosti ne nazadnje opozarja že prej navedeno

[8] Spletna stran http://www.openaccess.si/definicije-in-deklaracije.

[9] Povzeto po http://ec.europa.eu/research/science-society/document_library/pdf_06/background-paper-open-access-october-2012_en.pdf.

izhodišče odprtega dostopa. Pri tem gre tako za vprašanje moralnih kot materialnih avtorskih pravic. Ne da bi zmanjševali pomen moralnih avtorskih pravic, se bomo v nadaljevanju omejili na materialnopravne. Drugi odstavek 22. člena ZASP našteva materialne avtorske pravice oziroma upravičenja. Materialne avtorske pravice so sinonim za izključna premoženjska upravičenja avtorja na svojem delu, katerih vsebina je monopol nad izkoriščanjem dela, vsebina posameznih materialnih avtorskih pravic pa je monopol nad določenim postopkom, obliko ali načinom izkoriščanja dela.[10] V 22. členu ZASP so naštete samo nekatere temeljne oblike izkoriščanja avtorskega dela in nikakor ni mogoče govoriti o zaprtem krogu materialnih avtorskih pravic. Objava avtorskega dela v publikaciji, ki upošteva načela prostega dostopa, oziroma v odprtem repozitoriju znanstvenoraziskovalne institucije brez dvoma pomeni izkoriščanje avtorskega dela. Zakon o spremembah in dopolnitvah zakona o avtorski in sorodnih pravicah (ZASP-A)[11] je leta 2001 nabor naštetih materialnih avtorskih pravic razširil s pravico dajanja (avtorskega dela) na voljo javnosti (32.a člen ZASP): »Pravica dajanja na voljo javnosti je izključna pravica, da se po žici ali brezžično delo naredi dostopno javnosti na način, ki omogoča posameznikom dostop do njega s kraja in v času, ki ju sami izberejo, ali da se delo pošlje posamezniku na podlagi ponudbe, ki je namenjena javnosti.« Kot lahko vidimo, vsebina te pravice v celoti zajema oba načina objav v konceptu odprtega dostopa, kar nas vodi v sklep, da mora izdajatelj publikacije ali upravljavec repozitorija od avtorja pridobiti ustrezno materialno avtorsko pravico. Za njeno pridobitev veljajo splošna pravila avtorskega prava, kot veljajo za vsako drugo avtorsko pravico. V nadaljevanju se bomo omejili na problem pridobivanja avtorskih pravic v sistemu Univerze v Ljubljani in objav v njenem repozitoriju (v nadaljevanju RUL).[12]

3. Avtorskopravne podlage delovanja RUL

3.1. Uvod

Ker objava avtorskega dela v repozitoriju pomeni obliko izkoriščanja avtorskega dela, se mora za tako obliko izkoriščanja pridobiti materialna avtorska pravica dajanja na voljo javnosti. RUL ni samostojna pravna oseba, zato mora ustrezno avtorsko pravico pridobiti Univerza v Ljubljani kot upravljavec repozitorija. Tu pa lahko nastanejo različni pravni položaji v zvezi z načinom pridobitve avtorskih

[10] B. Oman, v: Trampuž, Oman, Zupančič, Zakon o avtorski in sorodnih pravicah s komentarjem, Gospodarski vestnik, Ljubljana 1997, stran 90.

[11] Uradni list, št. 9/2001.

[12] Dostop do repozitorija UL poteka prek spletnega naslova http://repozitorij.uni-lj.si/Iskanje.php?lang=slv.

pravic. RUL je primarno namenjen objavam in arhiviranju avtorskih del zaposlenih učiteljev in raziskovalcev. Pri njihovih objavah pridejo v poštev najprej splošna pravila o materialnih avtorskih pravicah iz delovnega razmerja. V sodobni znanosti in raziskovanju pa so vse bolj pogosti multidisciplinarni in multiinstitucionalni projekti, v katerih združujejo svoje intelektualne potenciale znanstveniki iz različnih institucij. Avtorsko delo je lahko rezultat prispevkov več znanstvenikov iz različnih institucij, od katerih vsaka ustvarja svoj repozitorij objav. Ob tem pa se postavi vprašanje pogojev za hkratno objavo v več repozitorijih. Dodatno ga zapletejo različni načini sodelovanja posameznih znanstvenikov pri nastajanju dela. Nekateri so lahko z upravljavcem repozitorija v delovnem razmerju, drugi pa so lahko z njim v zelo šibkih in gibkih povezavah, kot je sodelovanje matične institucije pri skupnem projektu. Poleg tega naj bi univerzitetni repozitorij ne bil zaprt za druge objave univerzitetnih učiteljev in raziskovalcev, ki niso nastale v okviru delovnega razmerja. Končno pa so tu tudi študentska dela, ki so nastala v okviru študijskih programov. Stvaritev samostojnega avtorskega dela je pogost pogoj za dokončanje študija po študijskem programu, kar spet načenja vprašanje o vsebini odnosa med študentom in univerzo.

3.2. Hramba zaključnih del po študijskih programih v RUL

Študijski programi univerzitetnega študija od študentov zahtevajo izdelavo različnih nalog, ki so sestavni del študijskega procesa in pogoj za dokončanje študija. Takšne naloge so rezultat študentovega samostojnega dela, ki pa ga pogosto usmerja bodisi visokošolski učitelj bodisi visokošolski sodelavec. Pri tem ne gre le za zaključna diplomska dela na vseh treh študijskih stopnjah. Sodobni študijski proces spodbuja individualno delo študentov in njihovo vključevanje v pedagoško in znanstvenoraziskovalno delo. Študentje danes bolj kot v preteklosti sodelujejo z individualnimi prispevki v obliki seminarskih nalog, predstavitev, raziskovalnih projektov in prispevkov. Na Univerzi v Ljubljani (v nadaljevanju UL) ne smemo prezreti niti umetnostnih študij, v katerih že zaradi vsebine študija prihaja do avtorskega ustvarjanja oziroma poustvarjanja. Nobenega dvoma ni, da takšni izdelki v veliki večini izpolnjujejo pogoje za priznavanje avtorskega dela. Najpogosteje imajo takšna dela pojavno obliko književnih del, na umetniških akademijah pa nastajajo tudi druge oblike. Številne avtorske stvaritve v študijskem procesu odpirajo tudi vprašanja zaščite avtorskih pravic in uporabe tovrstnih del. Toliko bolj, ker veljavna zakonodaja ne določa posebnih pravil, ki bi veljala za akademsko področje, splošna pravila avtorskega prava pa se včasih pokažejo kot neprimerna, ker ne upoštevajo posebnosti tega področja. Te stvaritve so primarno namenjene študijskemu procesu in so podvržene posebnemu postopku ocenjeva-

nja. Pozitivna ocena zaključnega dela je pogoj za zaključek študija in pridobitev naziva ter izkazuje diplomantovo sposobnost za opravljanje poklica.

Ker zakon ne določa nobenih posebnih avtorskopravnih pravil glede del študentov, ki nastanejo v študijskem procesu, je treba uporabiti splošna pravila avtorskega prava. Morda je treba najprej stopiti korak nazaj v času in opisati način delovanja v obdobju tiskanih del. Večina študijskih programov od študentov zahteva, da ob zaključku študija predložijo natisnjeno zaključno (diplomsko) delo. Univerza oziroma posamezna fakulteta[13] od študenta zahteva, da ji predloži določeno število izvodov, eden od teh izvodov pa je praviloma namenjen fakultetni oziroma univerzitetni knjižnici. Takšen način delovanja je tradicionalen in ni v celoti urejen z avtonomnimi pravnimi pravili. Gre preprosto za zahtevo študijskega programa, da študent izroči primerek svojega zaključnega dela. Primerek se nato hrani v knjižnici in je dostopen javnosti pod pogoji knjižnične izposoje. Od tu naprej velja pravno pravilo iz 36. člena ZASP. Ta določba ureja materialno avtorsko pravico javnega posojanja avtorskega dela. Posojajo se lahko knjige, časopisi, revije, note, gramofonske plošče, videokasete, fotografije, umetniške slike in drugo.[14] Za posojanje avtorskega dela pripada avtorju pravica do ustreznega nadomestila, posebne izjeme pa so določene z drugim odstavkom 36. člena ZASP. Med njimi je za zaključna dela študentov pomembna tista iz 1. točke, ki določa, da pravica do ustreznega nadomestila ne velja za uporabo izvirnikov ali primerkov pisnih del v nacionalni, šolskih in visokošolskih ter specialnih knjižnicah. Takšna ureditev je sicer avtorjem v škodo, vendar upošteva izobraževalno, kulturno in drugo poslanstvo javnih knjižnic.[15]

Čeprav univerzitetni digitalni repozitoriji prevzemajo vlogo univerzitetnih (fakultetnih) knjižnic, enostavna analogna uporaba pravil za tiskane izvode ne pride v poštev. Nedvomno ni mogoče prezreti povsem različnega dostopa javnosti pri teh dveh oblikah hrambe. Če knjižnica hrani oddani primerek zaključnega dela, je dostop do tega dela omejen na možnost individualnega vpogleda in sposojanja. Dostop do zaključnega dela v repozitoriju pa omogoča povsem drugačen način vpogleda in s tem tudi razmnoževanja zaključnega dela. Do dela v repozitoriju lahko dostopa več oseb hkrati oziroma v kratkem časovnem obdobju, in ko ga uporablja ena oseba, to ne izključuje uporabe drugim, kar je značilno za izposojo. Ob upoštevanju teh značilnosti uporabe dela, shranjenega

[13] Upoštevati je treba posebnost ureditve visokega šolstva, da ima v delu, ki se nanaša na izvajanje nacionalnega programa visokega šolstva, kamor spada študijska dejavnost, pravno sposobnost univerza, čeprav študijski proces poteka na fakultetah, ki imajo sicer pravno subjektiviteto, vendar ne na tem področju.

[14] M. Trampuž, v: Trampuž, Oman, Zupančič, Zakon o avtorski in sorodnih pravicah s komentarjem, Gospodarski vestnik, Ljubljana 1997, str. 119.

[15] Prav tam, str. 120.

v digitalnem repozitoriju, sklepam, da bi bila analogna uporaba pravil, ki veljajo za tiskane izvode, v nasprotju s temelji avtorskega prava, ki izhaja iz osnovnega načela, da je v dvomu z avtorja prenesenih manj pravic. Zato se mi zdi pravilna in utemeljena rešitev, ki jo je uvedel statut UL in se nanaša na delovanje RUL. Del študijskega reda UL je določba tretjega odstavka 127. člena statuta UL, da mora študent na UL neodplačno, neizključno, prostorsko in časovno neomejeno prenesti pravici shranitve avtorskega zaključnega (diplomskega) dela v elektronski obliki in reproduciranja ter pravico omogočanja javnega dostopa do avtorskega zaključnega (diplomskega) dela na svetovnem spletu prek RUL. Večinoma se to zahteva s podpisom izjave pred obrambo zaključnega dela, ki vsebuje tudi izjavo o samostojnosti in upoštevanju pravic drugih avtorjev. Takšna praksa pa spet odpira nekatera vprašanja. Splošna pravila avtorskega pogodbenega prava za pogodbe, s katerimi se prenašajo materialna avtorska upravičenja, predpisujejo pisno obliko (80. člen ZASP). Ker je namen pisne oblike predvsem zaščita avtorja, bi lahko šteli, da je pogoj oblike izpolnjen že z enostransko izjavo, čeprav listine ni podpisala pooblaščena oseba univerze. Bolj občutljivo pa je lahko vprašanje, ali univerza sploh lahko zahteva takšno izjavo kot pogoj za dokončanje študija. Ker to vprašanje nima avtorskopravne narave, se z njim tu ne bomo podrobneje ukvarjali. Statut UL načeloma zahteva takojšno objavo celotnega dela v repozitoriju, vendar predvideva možnost, da se v utemeljenih primerih vpogled v objavo omogoči s časovnim zamikom (tako imenovani zeleni dostop). Pravni akt, na katerega se sklicuje statut, še ni sprejet, zato tudi ne moremo podrobneje predstaviti njegove vsebine. Zdi pa se, da je treba študentu omogočiti komercialno izkoriščanje svojega avtorskega dela, če takšna možnost obstaja.

Ob takšnem stanju se mi zdi najbolj primerno, da bi se vprašanje hrambe študentskih del v univerzitetnem repozitoriju uredilo s posebno zakonsko določbo. V poštev pride posebna določba ZASP ali zakona s področja visokega šolstva. Univerza oziroma drug visokošolski zavod bi že na podlagi zakona pridobil pravico omogočanja javnega dostopa do avtorskega zaključnega (diplomskega) dela na svetovnem spletu prek univerzitetnega repozitorija. Prenos te materialne avtorske pravice bi bil neodplačen, neizključen in časovno neomejen. Ustrezno pa bi bilo treba oblikovati tudi pogoje za začasno zadržanje javnega dostopa za določen čas.

3.3. Hramba avtorskih del zaposlenih v RUL

Za različna avtorska dela zaposlenih na univerzi je odločilnega pomena okoliščina, ali je avtorsko delo nastalo v okviru zaposlitve ali ne. Pri opravljanju univerzitetnega poklica učitelji in sodelavci ustvarjajo različna avtorska dela. Ob strani bomo pustili govorna avtorska dela, ki niso neposredno povezana z delovanjem univerzitetnih repozitarjev. Kljub temu pa ne gre prezreti možnosti, da se

tudi govorna dela fiksirajo in se v repozitoriju hranijo njihovi posnetki. V nadaljevanju se bomo omejili le na pisna dela, ki jih univerzitetni učitelji in sodelavci ustvarjajo pri znanstvenoraziskovalnem delu. Znanstvenoraziskovalno delo je ena bistvenih sestavin njihovega dela in domneva se, da je nujna podlaga za uspešno predavateljsko delo. Tedenska delovna obremenitev univerzitetnega učitelja je tako sestavljena iz neposrednega pedagoškega dela (predavanja in druge oblike kontaktnih ur), posrednega pedagoškega dela (individualno delo s študenti) in znanstvenega raziskovanja. Univerzitetno karierno napredovanje v veliki meri upošteva količino in kakovost objavljenih dosežkov znanstvenega raziskovanja. Univerzitetni učitelji morajo izpolnjevati pogoje za izvolitev v določen naziv in v habilitacijskem postopku izkazovati predpisano število točk, ki jih dosežejo z objavami v periodiki in monografskimi deli. Zato lahko sklenemo, da v zaposlitev univerzitetnega učitelja ne spadajo samo govorna avtorska dela, ampak so njen nujni sestavni del objave pisnih znanstvenih in strokovnih del, kot so članki in knjižne monografije.

Če univerzitetni učitelj ali sodelavec ustvari avtorsko delo v okviru svoje zaposlitve, veljajo najprej splošna pravila avtorskega prava. Avtor sam odloča, ali bo svoje avtorsko delo objavil ali ne, kar je sestavni del njegovega osebnega (moralnega) avtorskega položaja. Delodajalec od njega ne more izsiliti objave avtorskega dela, lahko pa v skladu s pravili delovnega prava ukrepa proti tistemu, ki ne izpolnjuje predpisanih pogojev. Po avtorjevi odločitvi, da se avtorsko delo objavi, je izhodišče določba prvega odstavka 101. člena ZASP. Ta za avtorska dela, ki jih ustvari delojemalec pri izpolnjevanju svojih obveznosti ali po navodilih delodajalca, določa, da so materialne avtorske pravice in druge pravice avtorja na tem delu izključno prenesene na delodajalca za deset let od dokončanja dela, če ni s pogodbo določeno drugače. Prednost, ki jo ZASP daje delodajalcu, je v tem, da zakon v prvem odstavku 101. člena določa izključni prenos vseh materialnih avtorskih pravic na delodajalca (tako imenovani *cessio legis*) za obdobje deset let od dokončanja dela, če delojemalec takšno delo ustvari pri izpolnjevanju svojih obveznosti ali po navodilih delodajalca.[16] Če pustimo ob strani možnost drugačnega urejanja s pogodbo, ima univerza kot delodajalec in upravljavec repozitorija jasen pravni položaj. Ker velja domneva, da so na univerzo prenesene vse materialne avtorske pravice, so na delodajalca prenesene tudi vse pravice, ki so povezane s hrambo avtorskega dela v repozitoriju. To pomeni, da univerza sama lahko sprejme odločitev glede načina objave avtorskega dela, ki nastane v delovnem razmerju, v svojem repozitoriju. Na prvi pogled je rešitev preprosta, nekatere dejanske okoliščine pa lahko stvari zelo zapletejo. Gre predvsem za trk med

[16] A. Zupančič, Še enkrat o avtorskem delu iz delovnega razmerja, Pravna praksa, 1998, št. 11, str. 27–28.

interesom objave avtorskega dela v čim bolj kakovostni publikaciji in interesom popolnosti in ažurnosti repozitorija. Interes za objavo dela v najbolj kakovostni publikaciji je pogosto skupen avtorju in instituciji. Kot smo že omenili, je kakovost objave pomembna za karierno napredovanje univerzitetnih učiteljev. Objave v kakovostnih publikacijah pa so pomembne tudi za univerzo kot institucijo, saj so eno najbolj upoštevanih meril pri razvrščanju univerz v mednarodnem prostoru. Kakovost objave se lahko upošteva tudi kot merilo za ocenjevanje uspešnosti znanstvenoraziskovalne dejavnosti v razmerju do sistemskih financerjev in kot merilo na razpisih za pridobivanje sredstev za nadaljnje raziskovanje. Interes vsakega repozitorija objav pa je zagotavljanje objav na način zlatega dostopa. Problem nastane, če izdajatelj znanstvene publikacije kot pogoj za objavo postavi izključen in trajen prenos vseh materialnih avtorskih pravic. Z avtorskopravnega stališča lahko takšni zahtevi izdajatelja ustrežeta samo univerza in avtor skupaj. Na univerzo kot delodajalca so materialne avtorske pravice na podlagi 101. člena ZASP prenesene časovno omejeno. Zato univerza kot imetnik omejenih materialnih avtorskih pravic z njimi ne more razpolagati časovno neomejeno obdobje. Po preteku zakonsko določenih deset let vse materialne avtorske pravice pripadajo avtorju, ki je ustvaril delo v okviru svoje zaposlitve, zato lahko le on razpolaga z materialnimi avtorskimi pravicami, če se učinki razpolaganja raztezajo tudi na to obdobje. Univerza in avtor morata najti soglasje glede takšne zahteve izdajatelja publikacije in se dogovoriti o načinu razpolaganja z materialnimi avtorskimi pravicami. Takšen dogovor je mogoč tudi vnaprej in je lahko del pogodbe o zaposlitvi. Realnost znanstvenega ustvarjanja pa je pogosto drugačna. Na UL učitelji in raziskovalci sami vzpostavljajo stik in urejajo razmerja z izdajatelji publikacij.[17] Zato včasih razpolagajo z materialnimi avtorskimi pravicami, ki jih nimajo, saj so te na podlagi 101. člena ZASP prešle na delodajalca. Za zdaj nam ni znano, da bi zaradi takšnih ravnanj prišlo do sporov, vseeno pa se postavlja zanimivo vprašanje, kakšne so posledice ravnanj avtorja, ki sam v lastnem imenu razpolaga z materialnimi avtorskimi pravicami na avtorskem delu, ustvarjenem v delovnem razmerju. ZASP tega položaja ne ureja s posebno določbo, kar kaže, da je treba uporabiti splošna pravila. Pravni temelj vsakega razpolaganja je uveljavljeno pravno načelo, da nihče ne more učinkovito razpolagati s pravico, za katero nima razpolagalnega upravičenja (*nemo plus iuris transferre potest, quam ipse habet*). Iz takšnega razpolaganja ne nastanejo učinki singularnega pravnega nasledstva in velja, da pravica sploh ni prešla s premoženja imetnika na tretjega. Izjema so le primeri, ko tretji pridobi pravico na podlagi posebne zakonske

[17] Tudi v tujini nekatere univerze ne kažejo interesa za uveljavljanje avtorskih pravic zaposlenih, glej M. Trampuž, v: Trampuž, Oman, Zupančič, Zakon o avtorski in sorodnih pravicah s komentarjem, Gospodarski vestnik, Ljubljana 1997, str. 233.

določbe.[18] Takšna posebna izjema za razpolaganje z materialnimi avtorskimi pravicami ni predvidena, kar po mojem mnenju pomeni, da bi lahko univerza uveljavljala svoje zahtevke tako proti izdajatelju znanstvene publikacije kot proti avtorju, ki je nepooblaščeno razpolagal z materialnimi avtorskimi pravicami. Proti izdajatelju bi lahko nastopila z avtorskopravnimi zahtevki zaradi kršitve materialnih avtorskih pravic, proti avtorju pa predvsem s sankcijami, ki izvirajo iz zaposlitvenega razmerja. Vendar UL vsaj za zdaj teh zahtevkov ne uporablja, saj je veliko vprašanje, ali s takšnim načinom upravljanja svojih pravic ne bi povzročila več škode in si s tem predvsem zmanjšala možnosti na razvrstitvenih lestvicah. Povsem načelno pa lahko sklenemo, da bi lahko univerza kot imetnik materialnih avtorskih pravic na vseh avtorskih delih, ki jih ustvarijo zaposleni v okviru delovnega razmerja, izvedla objavo v repozitoriju, čeprav je bila objava opravljena v katerikoli znanstveni publikaciji ali monografiji, če ni sama prenesla materialnih avtorskih pravic na izdajatelja.

V prihodnosti pa bo delovanje univerzitetnih repozitorijev močno otežila zakonska določba o časovno omejenem prenosu materialnih avtorskih pravic na avtorskih delih iz delovnega razmerja. Nobenega dvoma ni, da ima univerza kot delodajalec na podlagi prenesenih avtorskih pravic v obdobju desetih let moč, da odloča glede načina objave v svojem repozitoriju. Po izteku desetih let pa je nosilec vseh materialnih avtorskih pravic avtor sam in s potekom roka ugasne tudi upravičenje univerze, da izvršuje materialno avtorsko pravico dajanja na voljo javnosti iz 32.a člena ZASP. Univerza ima sicer na voljo zahtevek iz drugega odstavka 101. člena ZASP, s katerim lahko zahteva ponovni prenos materialnih avtorskih pravic proti plačilu primernega nadomestila. Določba ima naravo prisilne licence, primernost nadomestila pa se presoja po 81. členu ZASP.[19] Uveljavljanje takšne prisilne licence si vsaj javna univerza težko privošči, saj za to nima namenskih sredstev. Zato takšna rešitev za univerzo večinoma ne bo izvedljiva. Vprašanje pa je, kakšna materialna avtorska pravica je potrebna za objavo določenega avtorskega dela v repozitoriju. Tu se jasni odgovori še niso izoblikovali. Ali pomeni uresničitev pravice z objavo v repozitoriju trajno pravico do javne objave in kakšne so posledice, potem ko ta pravica preneha? Ali mora univerza kot upravljavec repozitorija po izteku roka pridobiti pravico od avtorja oziroma ali lahko avtor, potem ko se mu vrnejo materialne avtorske pravice, objavo iz repozitorija umakne?

[18] Glej na primer 64. člen SPZ, ki ureja pridobitev lastninske pravice od razpolagalno nesposobne osebe, vendar pri tem ne gre za derivativni, ampak originalni način pridobitve lastninske pravice.

[19] M. Trampuž, v: Trampuž, Oman, Zupančič, Zakon o avtorski in sorodnih pravicah s komentarjem, Gospodarski vestnik, Ljubljana 1997, str. 232.

Univerzitetni repozitorij je ogledalo kakovosti univerze, zato je njegov namen, da se v njem zajame celoten znanstvenoraziskovalni opus učiteljev in sodelavcev. V repozitoriju se lahko objavijo tudi avtorska dela, ki jih ustvarjajo učitelji in sodelavci, čeprav niso nastala v okviru delovnega razmerja. Tu se nismo spustili v eno najbolj spornih vprašanj razmerja med univerzo in njenimi učitelji in sodelavci, to je razmejevanje med avtorskim ustvarjanjem v delovnem razmerju in zunaj njega.[20] Za objavo avtorskih del, ki nastanejo zunaj delovnega razmerja, veljajo splošna pravila avtorskega prava. Avtor in univerza se morata s pogodbo dogovoriti glede prenosa materialnih avtorskih pravic, ki so potrebne za objavo takšnega dela v repozitoriju. Položaj je smiselno enak kot pri študentskih delih. Enako velja v primerih, ko avtorsko delo nastane v soavtorstvu in so nekateri avtorji v delovnem razmerju z univerzo, drugi pa ne. Univerza mora za objavo skupnega dela v repozitoriju pridobiti ustrezne materialne pravice od vseh, kar pomeni, da bo morala sestaviti svoje upravičenje iz pravic, ki so bile nanjo prenesene na podlagi zakona, in pravic, ki jih bo pridobila s pogodbo.

4. Sklep

Ob vzpostavitvi RUL se postavljajo avtorskopravna vprašanja, ki so tesno povezana z nekaterimi posebnostmi delovanja univerzitetnega prostora. Te posebnosti odstopajo od splošnega modela urejanja avtorskopravnih razmerij, zato morda ne bi bilo odveč razmišljati tudi o posebni zakonski ureditvi tega področja in poiskati ravnotežje med interesi avtorjev in javnosti, tako glede dostopa do znanja kot tudi glede zagotavljanja in preverjanja kakovosti v visokem šolstvu. Upoštevati je treba namen repozitorijev, da postopoma prevzamejo naloge univerzitetnih knjižnic. Zato naj bo zakonska ureditev takšna, da ob upoštevanju interesa avtorjev zagotavlja takšen namen.

[20] Glej podrobneje M. Trampuž, v: Trampuž, Oman, Zupančič, Zakon o avtorski in sorodnih pravicah s komentarjem, Gospodarski vestnik, Ljubljana 1997, str. 119.

Pravno varstvo podatkovnih baz – izbrani pravni vidiki

mag. Jure Levovnik

1. Uvod

Pod pojmom podatkovna baza (ali tudi baza podatkov[1]) navadno razumemo bolj ali manj obsežno (elektronsko) zbirko gradiva, urejenega oziroma upravljanega na način, ki omogoča enostaven dostop do posameznih elementov gradiva in njihovo obdelavo.

Podatkovne baze so nastale kot plod zbiranja, razvrščanja in urejanja podatkov, enega osnovnih gradnikov človekovega razvoja in napredka. Temeljna funkcija podatkovnih baz je informacijska: v določenih primerih sploh omogočajo, drugič pa »zgolj« olajšujejo dostop do podatkov ter njihovo obdelavo in uporabo.[2] Podatkovne baze nudijo okvir za shranjevanje velikih količin podatkov, centraliziran nadzor nad podatki, možnost hitre obdelave in preoblikovanja podatkov, vzdrževanje kompleksnih sistemov povezav med podatki in nadzor na dostopom do podatkov. S temi funkcionalnostmi so podatkovne baze postale ključen instrument razvoja informacijskega trga in informacijske družbe (tj. družbe, v kateri so ustvarjanje, distribucija, obdelava in (ponovna) uporaba informacij s pomočjo digitalnih tehnologij ključni za industrijo in gospodarstvo[3]).

Podatkovne baze se pojavljajo v najrazličnejših oblikah in se uporabljajo na praktično vseh področjih človekove dejavnosti (v znanosti, športu, politiki, kulturi, upravi, industriji zabave itd.). Predstavljajo sestavni del našega zasebnega in poklicnega vsakdana in jih lahko srečamo na primer v obliki telefonskega imenika, slovarja, enciklopedije, antologije, spletnega imenika, baze predpisov, strokovnih člankov in sodne prakse, kataloga ponudnikov blaga in storitev z določenega področja, zbirke kuharskih receptov, zbirke športnih rezultatov, registra nepremičnin, registra podjetij, interne baze strank podjetja, baze osebnih podatkov, baze podatkov o ekonomskem obnašanju kupcev itd.

---

[1] Pojma uporabljam kot sopomenki.

[2] Primerjaj Herr (2008), str. 29.

[3] Glej Beunen (2007), str. 44, opomba 240.

Izdelava podatkovne baze pogosto zahteva občutne naložbe (finančne, tehnične, človeške). V digitalni dobi, ko je mogoče hitro in enostavno prekopirati in ponovno uporabiti velike količine podatkov iz že obstoječih baz, so tovrstne naložbe v izdelavo baz postale zelo ranljive. V pravu je zato prišlo do spoznanja, da je treba izdelovalcem podatkovnih baz – z namenom spodbujanja izdelovanja podatkovnih baz – nuditi pravno varstvo, na podlagi katerega bi lahko tretjim osebam prepovedali določene posege v njihove baze in s tem zaščitili svoje naložbe.

Namen tega prispevka je najprej na kratko predstaviti, kako pravo EU (na podlagi pravice *sui generis*) in slovensko nacionalno pravo (na podlagi pravic izdelovalcev podatkovnih baz) varujeta naložbe v izdelavo podatkovnih baz, nato pa nekoliko podrobneje tako s teoretičnega kot tudi s praktičnega vidika osvetliti nekatera izmed temeljnih vprašanj pravnega varstva podatkovnih baz oziroma naložb v njihovo izdelavo. Ta vprašanja se nanašajo na opredelitev podatkovne baze, pogoje za nastanek pravic na podatkovni bazi, imetništvo pravic ter vsebino in kršitev pravic. Predstavitev in analiza omenjenih vprašanj bosta temeljili na veljavni pravni ureditvi, sodni praksi Sodišča EU (SEU), tuji literaturi in na lastnih izkušnjah iz prakse.

2. Varstvo naložb v izdelavo podatkovnih baz

Pravno varstvo podatkovnih baz je na ravni EU urejeno z Direktivo 96/9/ES Evropskega parlamenta in Sveta z dne 11. marca 1996 o pravnem varstvu baz podatkov (Direktiva), ki je ustvarila pogoje za harmonizacijo dvotirnega pravnega varstva podatkovnih baz, in sicer (1) varstva na podlagi avtorske pravice in (2) varstva na podlagi t. i. pravice *sui generis*, ki je namenjena varstvu naložbe (če je ta znatna) izdelovalca podatkovne baze v pridobivanje, preverjanje ali predstavitev vsebine podatkovne baze. Medtem ko se avtorska pravica veže na strukturo baze oziroma na bazo kot táko (pod pogojem, da izbira, uskladitev ali razporeditev vsebine baze predstavlja individualno intelektualno stvaritev), pa se pravica *sui generis* veže na sámo vsebino baze (gradivo oziroma podatke), ki je odraz naložbe v izdelavo baze. Pravica *sui generis* velja na glede na upravičenost do varstva z avtorsko ali drugimi pravicami.[4]

Pravica *sui generis* je, poenostavljeno povedano, izključna pravica izdelovalca podatkovne baze, ki je v izdelavo baze vložil znatno naložbo, da (razen v primeru nekaterih predpisanih izjem) prepreči neupravičeno jemanje izvlečkov in/ali ponovno uporabo celotne vsebine svoje baze ali njenega bistvenega dela. Gre za

[4] Člen 7(4) Direktive. Glej tudi člen 141a(2) Zakona o avtorski in sorodnih pravicah (ZASP).

pravico, ki je prenosljiva; nastane z dnem zaključka izdelave baze ter traja še 15 let po prvem januarju v letu, ki sledi dnevu izdelave baze.

Uvedba povsem nove izključne pravice je posledica spoznanja, da so za izdelavo podatkovnih baz potrebne znatne človeške, tehnične in finančne naložbe, medtem ko sodobna tehnologija omogoča, da se baze lahko kopira ali se dobi dostop do njih le za majhen del stroškov, potrebnih za njihovo neodvisno stvaritev.[5] Neupravičeno jemanje izvlečkov in/ali ponovna uporaba vsebine baze sta dejanji, ki imata lahko resne gospodarske in tehnične posledice.[6] Pravno varstvo naj bi varovalo in s tem spodbujalo naložbe v napredne sisteme za obdelavo informacij, ki so potrebni zaradi skokovitega naraščanja količine informacij v vseh gospodarskih in industrijskih sektorjih.[7]

Posebna oblika pravnega varstva podatkovnih baz se je izkazala za potrebno zato, ker avtorska pravica, ki je tradicionalno predstavljala osrednji temelj varstva podatkovnih baz, izdelovalcu baze ne omogoča, da bi preprečil kopiranje in uporabo same vsebine baze in s tem zaščitil svojo naložbo v pridobitev, predstavitev ali preveritev vsebine baze.[8] Avtorska pravica na primer ne nudi varstva baz, katerih struktura je preprosta (na primer abecedni vrstni red, časovna razporeditev podatkov), četudi je morda izdelovalec v izdelavo baze vložil ogromna sredstva.

Splošno prevladujoče stališče v tuji literaturi je, da je pravica *sui generis* svojevrstna pravica intelektualne lastnine, ki ima podobne značilnosti kot avtorska pravica.[9] Usmerjena je v zagotovitev varstva in plačila naložbe izdelovalca podatkovne baze v pridobivanje, preverjanje ali predstavitev vsebine podatkovne baze,[10] nastane pa le, če je takšna naložba znatna. Njenemu imetniku daje izključno upravičenje, da prepove jemanje izvlečkov oziroma ponovno uporabo celotne ali znatnega dela vsebine baze. Tako kot avtorski pravici je tudi v pravico *sui generis* vraščen nenehen konflikt med interesi izdelovalca baze (imetnika pravice) na eni strani (ki želi ustrezen nadzor nad vsebino svoje baze) in uporabnikov na drugi strani (ki želijo čim bolj prost dostop do vsebine baze).

Slovenski zakonodajalec je Direktivo v delu, ki se nanaša na pravico *sui generis,* implementiral tako, da je v poglavje o sorodnih pravicah uvrstil t. i. pravice

[5] Uvodni izjavi (7) in (38) Direktive.

[6] Uvodna izjava (8) Direktive.

[7] Uvodna izjava (10) Direktive.

[8] Glej tudi uvodno izjavo (38) Direktive.

[9] Tako na primer Hugenholtz (2005). Glej tudi Westkamp (2003a), str. 1. To potrjuje tudi Komisija (glej First Evaluation, str. 8). Več o pravni naravi glej na primer še Leistner (2000), str. 128–143.

[10] Uvodni izjavi (39) in (40) Direktive. Glej tudi odstavek 46 *BHB.*

izdelovalcev podatkovnih baz.[11] Slovenska ureditev v bistvenih elementih sledi ureditvi pravice *sui generis* iz Direktive, zato bom v tem prispevku predstavil in analiziral le ureditev po Direktivi, na ureditev po ZASP pa opozoril le, kadar bom to ocenil za potrebno z vidika primerjave z Direktivo.

3. Pojem podatkovne baze

3.1. Uvod

V Direktivi je podatkovna baza opredeljena kot zbirka neodvisnih del, podatkov ali drugega gradiva, ki je sistematično ali metodično razporejeno in individualno dostopno z elektronskimi in drugimi sredstvi.[12] Praktično enotno stališče je, da je definicija podatkovne baze široka.[13]

Pravnega varstva po Direktivi ne uživajo računalniški programi, ki se uporabljajo pri izdelavi ali delovanju podatkovnih baz, dostopnih z elektronskimi sredstvi.[14] Varstvo pa se lahko razteza tudi na gradiva, nujna za delovanje ali vpogled v določene baze podatkov, na primer tezavre in indeksacijske sisteme.[15]

3.2. Oblika podatkovne baze

Definicija zajema baze v vseh oblikah,[16] ne glede na namen uporabe, vsebino, način shranjevanja podatkov ali način dostopa do podatkov.[17] Varstvo tako ni omejeno le na elektronske (digitalne) baze (bodisi *on-line* bodisi *off-line*[18]), temveč se razteza tudi na baze v kakršnikoli drugi, neelektronski obliki (elektromagnetski, elektro-optični ali analogni).[19]

Ne glede na obliko baze pa je že po naravi stvari bistveno, da je fiksirana na določenem nosilcu[20] (ne more biti na primer v ustni obliki, kar si je v praksi tudi težko predstavljati); fiksacija je predpogoj, da je do posameznih elementov vsebine sploh mogoče dostopati.

---

[11] Glej naslov 6. oddelka petega poglavja ZASP.

[12] Člen 1(2) Direktive.

[13] Beunen (2007), str. 49; Davison (2003), str. 70; Derclaye (2007), str. 4; Hugenholtz (2004); Westkamp (2003a), str. 3; Leistner (2000), str. 41; Stokes (2009), str. 60. Takšen je bil očitno tudi namen normodajalca (glej odstavek 20 *OPAP*).

[14] Člen 1(3) Direktive.

[15] Uvodna izjava (20) Direktive.

[16] Člen 1(1) Direktive.

[17] Gaster (1999), str. 30, odstavek 28.

[18] Gaster (1999), str. 30, odstavek 27.

[19] Uvodni izjavi (13) in (14) Direktive.

[20] Odstavek 29 *OPAP*.

3.3. Vrste gradiva

Vsebino podatkovne baze lahko sestavljajo avtorska dela, podatki ali kakršnokoli drugo gradivo (besedila, zvoki, podobe, številke, dejstva itd.).[21] Zdi se, da je Direktiva želela med podatkovne baze uvrstiti zbirke kakršnihkoli vrst gradiva, brez vnaprejšnjih omejitev.

Med avtorska dela spadajo avtorska dela vseh vrst (na primer literarna, likovna, glasbena), pri čemer oblika avtorskega dela ni pomembna, pa tudi ne vrsta materialnega nosilca, na katerem se avtorsko delo nahaja. Tako bi bilo teoretično mogoče, da bi tudi umetnostna galerija ali knjižnica predstavljali podatkovno bazo (ob izpolnjevanju drugih pogojev iz definicije).

Kaj je mišljeno s pojmom »podatki«[22], je že nekoliko manj jasno. Brez dvoma gre za gradivo, ki ne izpolnjuje pogojev za avtorsko delo. Ni pomembno, kakšne vrste podatkov so.[23] Nekateri avtorji[24] zastopajo stališče, da gre pri podatkih pravzaprav za informacije, ki so človeku razumljive in imajo neki pomen, ne pa za surove podatke, ki človeku niso razumljivi.

Najmanj definiran je pojem »drugo gradivo«. Poleg avtorskih del in podatkov si je težko zamisliti, kaj bi s tem pojmom še lahko bilo zajeto. Teoretično bi lahko zajemal karkoli, kar ni avtorsko delo ali podatek. Uvodne izjave Direktive kot drugo gradivo omenjajo besedila, zvoke, podobe, številke, dejstva, kar kaže na to, da se lahko pojma »podatki« in »drugo gradivo« tudi prekrivata.

Pri vrstah gradiva ni pomembno, ali je gradivo ustvarjeno s strani izdelovalca baze ali s strani tretje osebe.[25] Gradivo je torej lahko obstajalo že prej, lahko pa je ustvarjeno šele za potrebe izdelave podatkovne baze.[26]

3.4. Neodvisnost gradiva

Da lahko govorimo o podatkovni bazi, morajo biti elementi vsebine, ki jo baza vsebuje, med seboj neodvisni. Gre za pomemben pogoj,[27] zaradi katerega marsikatera zbirka ne bo izpolnjevala pogoja za podatkovno bazo.

Neodvisnost pomeni, da morajo biti elementi vsebine med seboj ločljivi, ne da bi bila zaradi ločljivosti spremenjena njihova informativna, literarna, umetniška,

[21] Uvodna izjava (17) Direktive.

[22] Ki se v pravni znanosti pogosto (čeprav nepravilno) uporablja kot sinonim za pojem informacije (glej na primer Bensinger (1999), str. 125).

[23] Odstavek 22 *OPAP*. Tako na primer tudi Pitkänen, Virtanen, Välimäki, str. 4.

[24] Na primer Derclaye (2008), str. 58.

[25] Odstavek 24 *OPAP*.

[26] Derclaye (2008), str. 57.

[27] Leistner (2000), str. 46.

glasbena ali druga vrednost.[28] Da bi bil neodvisen, mora torej element vsebine imeti lastno neodvisno informativno vrednost:[29] njegov pomen ne sme biti odvisen od neke druge informacije.[30] Pojem neodvisnosti se torej v smislu Direktive razume kot konceptualna oziroma logična, in ne kot fizična neodvisnost.[31] Pogoj neodvisnosti se razlaga tudi tako, da dodajanje ali odvzemanje elementov vsebine ne sme pomeniti, da bi baza kot celota izgubila svoj pomen oziroma celovitost.[32]

Če so elementi vsebine medsebojno ločljivi na način, da izločitev enega elementa ne vpliva na vrednost oziroma pomen celotne vsebine, potem je ta pogoj izpolnjen.[33] Direktiva primeroma pojasnjuje, da ravno iz tega razloga posnetek avdiovizualnega, kinematografskega, literarnega ali glasbenega dela ne spada v področje uporabe Direktive[34] in tako ne predstavlja podatkovne baze. Razlog za to je, da posamezni elementi tovrstnih del med seboj niso neodvisni, saj delu ne morejo biti odvzeti ali dodani, ne da bi le-to izgubilo pomen, vrednost oziroma sporočilo (iz knjige na primer ni mogoče odvzeti enega poglavja, ne da bi s tem celotno delo izgubilo del pomena). Kot primer del, ki ne predstavljajo podatkovne baze, se pogosto navajajo tudi multimedijska dela[35] in videoigre.

3.5. Sistematična ali metodična urejenost gradiva

Gradivo v podatkovni bazi mora biti sistematično ali metodično urejeno. SEU je pojasnilo, da je gradivo sistematično ali metodično[36] urejeno tedaj, ko obstaja zbirka na trajnem nosilcu kakršnekoli vrste in vsebuje tehnično sredstvo (kot je elektronski, elektromagnetni ali elektrooptični proces) ali drugo sredstvo (kot je indeks, kazalo, načrt ali poseben način razvrstitve), ki v okviru vsebine zbirke omogoča izločitev vsakega neodvisnega elementa.[37] Po tem se baza podatkov v smislu navedene definicije razlikuje od zbirke gradiv, ki nima nobenega sredstva

[28] Odstavek 29 *OPAP*. Podobno Leistner (2000), str. 47.

[29] Odstavek 32 *OPAP*. Glej tudi Westkamp (2003), str. 36.

[30] Leistner (2000), str. 48 in 49; Westkamp (2003), str. 34; Bensinger in Grützmacher, v: Derclaye (2008), str. 62.

[31] Aplin (2005), str. 46–47. Element gradiva je konceptualno neodvisen, kadar ima enak pomen tako znotraj kot tudi zunaj zbirke.

[32] Primerjaj Derclaye (2008), str. 62.

[33] Primerjaj Bensinger (1999), str. 128.

[34] Uvodna izjava (17) Direktive.

[35] Glede teh nekateri menijo, da lahko predstavljajo tudi podatkovne baze (glej na primer Aplin (2005)).

[36] Bensinger navaja, da ni videti pomembne razlike med pojmoma »sistematično« in »metodično« (Bensinger (1999), str. 132).

[37] Odstavek 30 *OPAP*.

za obdelavo posameznih elementov, ki jo sestavljajo[38] (na primer v primeru zbirk tridimenzionalnih objektov), oziroma ki uporabniku ne omogoča, da bi izločil posamezni element. Način, na katerega je gradivo dostopno, torej ni pomemben.

V teoriji se poudarja, da je bistveno, da je gradivo razvrščeno na logičen, prikladen in urejen način,[39] ni pa potrebno, da bi bila razvrstitev individualna intelektualna stvaritev. Za izpolnitev tega pogoja tudi ni potrebno, da bi bilo gradivo shranjeno na organiziran način[40] oziroma da bi bila urejenost gradiva navzven razvidna. Zadošča, da obstaja neko sredstvo (kakršnekoli oblike), ki omogoča priklic želenega elementa vsebine baze.

3.6. Posamična dostopnost elementov vsebine

Medtem ko je SEU glede sistematične ali metodične urejenosti že dalo določene smernice, pa to ne velja glede pogoja posamične dostopnosti elementov vsebine. Gre za pogoj, ki je tesno povezan tako s pogojem sistematične ali metodične urejenosti[41] kot tudi s pogojem posamične dostopnosti[42] in ki se v teoriji razlaga na različne načine.[43] Bistveno je, da mora obstajati funkcija iskanja po vsebini baze[44] oziroma sredstvo za iskanje med posamičnimi elementi baze, ki omogoča priklic posameznega elementa, ne da bi bilo treba za to preiskati celotno vsebino baze.[45] Ni pa potrebno, da bi bil priklic posameznega elementa omogočen samo človeku; temu pogoju je zadoščeno tudi, če priklic podatkov in njihova uporaba potekata znotraj naprave (na primer računalnika) brez sodelovanja človeka.[46]

3.7. Dodatni pogoji

3.7.1. Informacijski namen

Iz prakse SEU izhaja, da posebnost izraza »baza podatkov« v smislu Direktive temelji na funkcionalnem kriteriju in da je pojem treba razumeti tudi v smislu

[38] Odstavek 31 *OPAP*.

[39] Derclaye (2008), str. 65.

[40] Uvodna izjava (21) Direktive.

[41] Glej na primer Aplin (2005), str. 51. Za nekatere se ta pogoj zdi že zajet v pogoju sistematične ali metodične urejenosti ter kot tak celo odvečen (Derclaye (2008), str. 66–67).

[42] Bensinger (1999), str. 130.

[43] Več o tem Derclaye (2008), str. 65–67.

[44] Koo (2010), str. 314.

[45] Beunen (2007), str. 59. Podobno Hugenholtz, v: Beunen (2007), str. 59; Westkamp (2003), str. 38; Bensinger (1999), str. 130.

[46] Bensinger (1999), str. 131.

funkcije baze kot sistema za shranjevanje in obdelavo informacij.[47] To napeljuje na stališče, da je za opredelitev zbirke kot podatkovne baze bistveno tudi to, da ima zbirka funkcijo sistema za shranjevanje in obdelavo informacij in da ne gre le za zbirko predmetov, ki je na primer namenjena estetskim ali drugačnim užitkom imetnika ali uporabnikov. Tudi nekateri avtorji se zavzemajo za restriktivno razlago pogojev za podatkovno bazo, iz katere bi sledilo, da mora imeti baza informacijski namen.[48] Ta pogoj bi iz definicije podatkovne baze izključil marsikatere zbirke tridimenzionalnih objektov, zlasti takšnih, ki niso avtorska dela.

3.7.2. Količina gradiva

Ker je podatkovna baza oblika zbirke, je vprašanje, ali je količina gradiva, ki ga vsebuje baza, kvalifikatorni element, da lahko govorimo o podatkovni bazi. Definicija v Direktivi ne daje odgovora na to vprašanje. Še zlasti ne, ali obstaja spodnja meja količine gradiva, pod katero ne moremo govoriti o podatkovni bazi, čeprav sicer zbirka izpolnjuje vse izrecno določene elemente definicije podatkovne baze.[49]

Po eni strani Direktiva nikjer izrecno ne zahteva, da bi moralo iti pri podatkovni bazi za večjo količino gradiva,[50] po drugi strani pa bi že pojem zbirka lahko napeljeval na to, da mora baza vsebovati določeno kritično količino gradiva, ki pomeni več kot le majhno število elementov.[51] SEU je potrdilo, da zahteva po določeni količini gradiva ne obstaja,[52] tako da bi lahko teoretično podatkovna baza bila sestavljena zgolj iz dveh elementov.[53] V teoriji glede tega vprašanja ni enotnega stališča.[54] Medtem ko nekateri ne zagovarjajo postavljanja spodnje meje količine gradiva,[55] pa drugi zastopajo stališče, da bi definicija morala vsebovati pogoj, da gre za veliko ali večje število elementov gradiva[56] (čeprav bi se v takem primeru vsakič znova odprlo vprašanje, kje je spodnja meja glede števila elementov gradiva). Zanimivo je stališče, da naj bi morala baza vsebovati

[47] Odstavka 27 in 28 *OPAP* ter uvodni izjavi (10) in (12) Direktive.

[48] Na primer Beunen (2007), str. 66 in 69; Davison (2003), str. 71.

[49] Zadevo še bolj zaplete uvodna izjava (19) Direktive, kjer je zapisano, da zbirka (kompilacija) več posnetkov glasbenih izvedb na CD-ju ne pade v predmet varstva po Direktivi tudi zato, ker ne predstavlja zadostne naložbe, da bi lahko bila predmet varstva s pravico *sui generis*.

[50] Kot je to sprva v postopku sprejemanja Direktive predlagal Evropski parlament.

[51] Primerjaj Derclaye (2008), str. 55–56.

[52] Odstavek 24 *OPAP.*

[53] Derclaye (2008), str. 56. Derclaye opozarja na nevarnost, da bi se v takih primerih lahko varstvo take baze zelo približalo varstvu posameznih podatkov.

[54] Za nasprotna stališča glej na primer Beunen (2007), str. 67–68.

[55] Na primer Leistner (2000), str. 45.

[56] Derclaye (2008), str. 273; Bensinger, v: Beunen (2007), str. 68.

vsaj toliko elementov gradiva, da posamezni element ne bi mogel predstavljati kakovostno ali količinsko znatnega dela,[57] s čimer bi se preprečila monopolizacija sicer nevarovanega gradiva.

3.8. Primeri zbirk, ki so podatkovne baze

Iz tuje literature in tam navedene sodne prakse[58] izhaja, da so se kot podatkovne baze že priznale denimo: zbirka povesti, zbirka pesmi, zbirka filmov, zbirka glasbenih del, zbirka računalniških programov, seznam podatkov v računalniških programih, koledar nogometnih tekem, bibliografije, časopisi, revije, seznami strank, zemljevidi, zbirke hiperpovezav, spletne strani, spletna mesta[59] (razen kadar so posamezne strani medsebojno odvisne), knjižnice, rezultati športnih tekem, zbirka poslovnih in pravnih informacij o podjetjih, seznami TV-programov, telefonski imeniki, seznami prodajanih nepremičnin, seznam elektronskih naslovov, zbirka receptov, seznam mest, zbirka pravnih besedil, seznami finančnih poročil in podatkov in še bi lahko naštevali.

Že na prvi pogled se vidi, da so tuja sodišča pojem podatkovne baze razlagala dokaj široko,[60] v nekaterih primerih verjetno celo preširoko. Iz tuje literature je mogoče razbrati, da so sodišča v večini omenjenih primerov preprosto predvidevala, da so naštete zbirke podatkovne baze, ne da bi posebej preverjala izpolnjevanje vsakega posameznega pogoja iz definicije.[61] To napeljuje na ugotovitev, da sodišča vprašanju, ali je neka zbirka podatkovna baza, običajno ne posvečajo veliko pozornosti, kar lahko pomeni tveganje, da določeni zbirki priznajo varstvo na podlagi pravice *sui generis*, čeprav si takega varstva morda sploh ne bi zaslužila ali ga niti ne bi potrebovala.

4. Pogoji za nastanek pravice *sui generis*

4.1. Uvod

Za nastanek pravice *sui generis* se zahteva, da je pridobitev, preveritev ali predstavitev vsebine baze zahtevala kakovostno ali količinsko znatno naložbo. Naložba mora torej biti znatna (ocenjeno bodisi kakovostno bodisi količinsko)

[57] Beunen (2007), str. 68–69.
[58] Delno povzeto po Derclaye (2008), str. 69–72.
[59] Več o tem tudi Leistner (2000), str. 62–64.
[60] Glej tudi Hugenholtz, Maurer, Onsrud (2001), str. 789.
[61] Derclaye (2008), str. 72.

in mora biti usmerjena v izdelavo podatkovne baze, natančneje v pridobitev, preveritev ali predstavitev vsebine baze.[62]

4.2. Vrste naložb

Čeprav iz besedila Direktive ni mogoče razbrati vsebine pojma »naložba«, pa je iz njenih uvodnih izjav razvidno, da je pojem naložbe treba razlagati široko in da se upoštevajo vse vrste naložb, ki so usmerjene v izdelavo podatkovne baze, kot na primer zagotovitev finančnih sredstev ali pa poraba časa, truda in energije.[63] Naložbe so torej lahko finančne (denarna sredstva), materialne (v smislu pridobitve opreme za izdelavo baze) ali človeške (čas, trud in energija).[64]

4.3. Znatnost naložbe

Iz Direktive ni razvidno, kdaj se neka naložba šteje za znatno, prav tako pa se glede tega vprašanja še ni opredelilo niti SEU. Vprašanje je, ali in kje obstaja spodnja meja, ki jo mora naložba doseči, da jo je mogoče opredeliti kot znatno. Že na prvi pogled je jasno, da gre pri pojmu »znatna« za pomensko zelo odprt standard, ki dopušča različne razlage.[65]

Prvo vprašanje je, kakšno naj bo merilo presoje znatnosti: ali je za presojo znatnosti pravilneje uporabiti objektivno merilo (ne upoštevajoč konkretnega izdelovalca, njegove finančne, tehnične in druge zmožnosti) ali subjektivno merilo (upoštevajoč konkretnega izdelovalca, njegove finančne, tehnične in druge zmožnosti). Če bi uporabili subjektivno merilo, bi enako velika naložba enkrat lahko bila znatna (če bi bil njen izdelovalec manjši subjekt), drugič pa neznatna (če bi bil njen izdelovalec velik subjekt). To z vidika pravne varnosti in predvidljivosti ne bi bilo primerno, prav tako pa bi omogočalo zlorabe in presojo znatnosti naložbe močno otežilo. Zato se zdi primernejše objektivno merilo.[66] Vendar pa to ne pomeni, da pri presoji, ali je naložba znatna, ne bi smeli konkretne naložbe vsaj na načelni ravni primerjati z morebitnimi naložbami v baze s primerljivo vsebino

[62] Pogoje za varstvo s pravico *sui generis* je že razlagalo tudi SEU: glej sodbe v zadevah *OPAP, Veikkaus, Svenska Spel, BHB*. Ker so si obrazložitve v teh štirih sodbah v nekaterih delih identične, se bom v takih primerih skliceval samo na sodbo *OPAP*.

[63] Uvodna izjava (40) Direktive in odstavek 44 *OPAP.*

[64] Uvodna izjava (7) Direktive. Primerjaj Derclaye (2008), str. 73–74. Med človeške naložbe spadajo tudi sposobnosti, znanje, tehnična ustvarjalnost ali psihološke naložbe (primerjaj Gaudrat, v: Derclaye (2008), str. 74).

[65] Tako tudi Derclaye (2008), str. 75.

[66] Tako tudi Derclaye (2008), str. 84.

in velikostjo.[67] Objektivno merilo bo pogosto smiselno dopolniti tudi z določenimi subjektivnimi merili, ki odražajo specifično naravo konkretnega primera.[68]

V tuji literaturi so mnenja o tem, kaj se šteje za znatno naložbo, zelo različna. Zagovorniki nizkega praga menijo, da zadošča že simbolična naložba[69] oziroma naložba, ki izključuje povsem neznatne izdatke (vsakodnevne naložbe).[70] Zanimivo je stališče, da je vsaka naložba, ki si jo je nekdo tretji želel prihraniti s kopiranjem vsebine tuje baze, očitno dovolj znatna, da si naložba zasluži varstvo.[71] Prepričljivo se zdi tudi stališče, da bi Direktiva zgrešila svoj namen spodbujanja razvoja informacijskega trga, če bi varovala le baze, ki so rezultat velikih naložb.[72] Na drugi strani zagovorniki visokega praga menijo, da je pogoj »znatna« moral biti zapisan z namenom. Nekateri izmed njih menijo, da visok prag zmanjšuje nevarnost monopolizacije informacij,[73] medtem ko nizek prag pomeni, da več manjših baz postane predmet izključne pravice *sui generis* in da se s tem javna domena oži.

Na koncu bo posamezno sodišče tisto, ki bo moralo od primera do primera, upoštevajoč vse okoliščine (tudi vrsto podatkovne baze in naravo naložb, uporabljenih za njeno izdelavo), presojati, ali je naložba znatna ali ne. Takšno je tudi večinsko stališče v teoriji.

V tuji sodni praksi so sodišča kot znatne štela zelo različne naložbe, na primer: plačilo 800 EUR mesečno, nekaj ur dela, stalno vnašanje in preverjanje informacij, izdelava seznama 1650 e-naslovov, izdelava zbirke 251 hiperpovezav na spletne strani organizacij za starše itd.[74] Nekateri teoretiki menijo, da velika večina sodišč držav članic EU zagovarja nizek prag in redko zavrne varstvo zaradi prenizke naložbe.[75]

4.4. Količinski in/ali kakovostni vidik

Ali je naložba znatna, se lahko presoja bodisi s količinskega bodisi s kakovostnega vidika. SEU je pojasnilo, da se količinska presoja naložbe nanaša na sredstva, ki se jih da izraziti s številkami (kot na primer denar, čas ali število

[67] Primerjaj Beunen (2007), str. 145, in *Svenska Spel* (mnenje AG), odstavka 38 in 39.

[68] Tako tudi Westkamp (2003), str. 124–126.

[69] Pollaud-Dulian, v: Derclaye (2008), str. 84.

[70] Na primer Gaster (1999), str. 121, odstavek 476. Enako Beurskens (2004), str. 49.

[71] Glej na primer Leistner (2000), str. 168; Beurskens (2004), str. 49.

[72] Derclaye (2008), str. 88.

[73] Westkamp, v: Derclaye (2008), str. 87. Glej tudi Westkamp (2003a), str. 4 in naslednje. Derclaye se s tem stališčem ne strinja (glej Derclaye (2008), str. 87).

[74] Za pregled konkretnih primerov iz tuje sodne prakse glej Derclaye (2008), str. 76–83.

[75] Derclaye (2008), str. 83.

ljudi), ne pa tudi na količino podatkov v bazi ali na količino naložbe. Kakovostna presoja naložbe, ki naj bi bila po mnenju nekaterih v razmerju do količinske dopolnilna,[76] pa se nanaša na trud, ki se ga ne da količinsko opredeliti, kot je intelektualni trud ali poraba energije,[77] ne pa tudi na kakovost elementov gradiva v bazi.[78] Ni potrebno, da bi naložba vključevala ustvarjalnost, individualnost ali izvirnost (v smislu avtorskega prava).[79]

4.5. Predmet (namen) naložbe

Za pridobitev pravice *sui generis* so upoštevne samo tiste naložbe, ki se nanašajo na pridobivanje, preverjanje ali predstavitev vsebine baze. Gre za naložbe, namenjene vzpostavitvi same baze.[80] Naložbe, ki so usmerjene v dejavnosti, ki niso izdelava podatkovne baze, niso upoštevne.

4.5.1. Pridobivanje vsebine

Izdelovalec lahko vsebino baze v celoti ali deloma ustvari sam ali jo pridobi iz enega ali več virov. SEU pojem naložbe v pridobivanje vsebine baze razlaga ozko, in sicer tako, da ta zajema sredstva, namenjena pridobivanju obstoječih elementov in njihovem zbiranju v tej bazi, ne vključuje pa sredstev, zagotovljenih za ustvarjanje sestavnih elementov vsebine baze podatkov.[81] Poenostavljeno povedano, pojem »pridobivanje« vsebine baze ne vključuje »ustvarjanja« vsebine baze. Ta razlaga izhaja iz namena pravice *sui generis*, ki je v spodbujanju vzpostavitve sistemov za shranjevanje in obdelavo obstoječih informacij, ne pa v ustvarjanju gradiv, ki bi lahko bila pozneje zbrana v bazi podatkov.[82]

Podatkovne baze, ki vsebujejo s strani izdelovalca ustvarjene podatke, so zlasti pogoste v primeru subjektov, ki tovrstne baze izdelujejo kot stranski produkt svoje osnovne dejavnosti. SEU pri svojem stališču sicer ne razlikuje med bazami, ki so stranski produkt, in preostalimi bazami.[83] Pojasnilo je, da okoliščina, da naj bi bila vzpostavitev baze podatkov povezana z opravljanjem osnovne dejavnosti, v okviru katere je oseba, ki vzpostavi bazo, hkrati tudi oseba, ki ustvari gradiva, vsebovana v tej bazi, sama po sebi ne izključuje možnosti, da bi ta oseba lahko

[76] Leistner (2000), str. 162. Enako Beunen (2007), str. 107.
[77] Odstavek 44 *OPAP*.
[78] Derclaye (2008), str. 91.
[79] Primerjaj Bensinger (1999), str. 157.
[80] Odstavek 39 *OPAP*.
[81] Odstavek 40 *OPAP*.
[82] Odstavka 39 in 41 *OPAP*, v povezavi z uvodno izjavo (39) Direktive.
[83] Tak pristop kritizira Beunen (glej Beunen (2007), str. 128).

zahtevala zaščito s pravico *sui generis*. Mora pa dokazati, da je pridobitev tega gradiva, njegovo preverjanje ali predstavitev zahtevala kakovostno ali količinsko precejšno naložbo, z neupoštevanjem sredstev, zagotovljenih za ustvarjanje tega gradiva.[84]

V praksi bo v primeru baz, ki vsebujejo s strani izdelovalca ustvarjene podatke, pogosto težko ugotoviti obstoj znatne naložbe, ki bi bila neodvisna od naložbe v ustvarjanje podatkov, saj je težko potegniti črto med dejavnostjo ustvarjanja podatkov in dejavnostjo pridobivanja podatkov.[85] Posledično se lahko zgodi, da bo večina podatkovnih baz, ki so edini vir podatkov, ki jih vsebujejo (t. i. *sole source* baze), ostala brez varstva s pravico *sui generis*,[86] kar načeloma vsaj delno preprečuje nastanek monopolov nad informacijami v tovrstnih bazah, ki bi jih ustvarjalo varstvo na podlagi pravice *sui generis*.[87]

S tem stališčem je SEU implicitno zavrnilo t. i. teorijo *spin off*, ki je nastala v nizozemski sodni praksi in v skladu s katero so sodišča zavračala obstoj pravice *sui generis* v povezavi z bazami, ki so jih njihovi izdelovalci izdelali kot stranski proizvod njihove osnovne dejavnosti (na primer koledarji dogodkov, TV-sporedi in radijski sporedi, letalski ali vlakovni vozni red, telefonski imenik, cene delnic, seznami športnih parov itd.), če so z vsebino baze razpolagali že na podlagi opravljanja svoje osnovne dejavnosti.[88] Je pa po drugi strani SEU tudi povzelo številne argumente, na katere je oprta omenjena teorija.[89]

Med naložbe v pridobivanje podatkov načeloma spadajo tudi plačila licenčnin za pridobitev podatkov ali drugega gradiva.[90] Vprašanje pa je, ali se kot naložba v pridobivanje podatkov šteje tudi plačilo za pridobitev podatkov, kadar gre za pridobitev vsebine iz enega samega vira, ki je tudi edini vir podatkov. Glede tega v literaturi ni enotnega stališča,[91] je pa odgovor na to vprašanje zelo pomemben. Če bi se takšna naložba štela za upoštevno, bi se dalo stališče SEU, po katerem naložba v ustvarjanje podatkov ni upoštevna, dokaj enostavno obiti: družba, ki bi ustvarila podatke, bi ustanovila hčerinsko družbo, hčerinska družba pa bi

[84] Odstavek 45 *OPAP*.

[85] Derclaye (2008), str. 94–95.

[86] Derclaye (2008), str. 96.

[87] Obstajajo tudi protiargumenti, zakaj naj to stališče SEU vendarle ne bi bilo učinkovito za preprečevanje monopolov nad informacijami (glej Beunen (2007), str. 133–134; Hugenholtz (2005).

[88] Več o tem Derclaye (2008), str. 94 in naslednje; Beunen (2007), str. 107 in naslednje; Derclaye (2004); Hugenholtz (2005), str. 203–219; Hugenholtz (2003).

[89] Tako Hugenholtz (2005).

[90] Glej na primer Leistner (2000), str. 150–151; Bensinger (1999), str. 158.

[91] Več o tem Beunen (2007), str. 127; Westkamp (2003), str. 119. Glej tudi Gaster (1999), str. 122, odstavki 478–480.

nato kupila podatke od družbe matere in iz njih ustvarila bazo ter uveljavljala pravico *sui generis*.

Za izdelovalce podatkovnih baz, ki tudi sami ustvarjajo podatke za podatkovne baze, je glede na stališče SEU zelo pomembno, da skrbno vodijo evidence o naložbah v aktivnosti, ki s samim ustvarjanjem podatkov niso povezane, saj se bodo samo te upoštevale v primeru spora o obstoju oziroma kršitvi pravice *sui generis*.[92]

4.5.2. Preverjanje vsebine

Naložba v preverjanje vsebine zajema sredstva, ki so zaradi zagotavljanja zanesljivosti informacije v tej bazi namenjena preverjanju pravilnosti (točnosti) pridobljenih gradiv ob vzpostavitvi te baze in tudi v obdobju njenega delovanja.[93] V tem pojmu so zajete aktivnosti preverjanja, popravljanja in posodabljanja vsebine.[94] Ni pa nujno, da bi baza morala biti zaradi teh aktivnosti kakorkoli spremenjena.[95]

Sredstev, namenjenih preverjanju gradiva v fazi ustvarjanja gradiva, ki je pozneje zbrano v bazi podatkov, pojem »preverjanje vsebine« ne zajema.[96]

4.5.3. Predstavitev vsebine

Naložba v predstavitev vsebine zajema sredstva, ki so namenjena temu, da se bazi doda funkcija obdelave podatkov, tj. tista sredstva, ki so namenjena sistematični ali metodični razvrstitvi gradiva, vsebovanega v bazi, kot tudi za organiziranje njihove individualne dostopnosti.[97]

Kot primer tovrstnih naložb se v literaturi navajajo naložbe v izdelavo uporabniškega vmesnika, tezavra, indeksa, prenosa med različnimi mediji (na primer digitalizacija podatkov iz analogne oblike), prevoda vsebine baze v druge jezike,[98] pa tudi na primer izdelava spletne strani za bazo, nakup strojne in programske opreme, potrebne za izdelavo in predstavitev baze[99] ter dodajanje informacij osnovnim podatkom (na primer povzetkov ali opisov).

---

[92] Podobno Koo (2010), str. 315.
[93] Odstavek 43 *OPAP*.
[94] Hugenholtz, v: Derclaye (2008), str. 97.
[95] Gaudrat, v: Derclaye (2008), str. 97.
[96] Odstavki 40–42 *BHB*.
[97] Odstavek 43 *OPAP*.
[98] Derclaye (2008), str. 98.
[99] Beunen (2007), str. 135–136.

Če je naložba v predstavitev vsebine neločljivo povezana z ustvarjanjem vsebine baze, takšna naložba ni upoštevna pri presoji znatnosti naložbe.

5. Imetnik pravice *sui generis*

Pravica *sui generis* izvorno pripada izdelovalcu baze.[100] To je oseba, ki prevzame pobudo in tveganje investiranja v izdelavo baze, pri čemer se podpogodbeniki ne štejejo za izdelovalce.[101] Imetnik pravice je lahko tako fizična kot tudi pravna oseba.

Kdo se šteje za izdelovalca podatkovne baze, pogosto ni povsem jasno, saj Direktiva glede tega ne ponuja konkretnejših smernic.[102] V literaturi se denimo pojavlja vprašanje, ali je prevzem pobude za investiranje sploh bistven in ali ni ključen zgolj pogoj prevzema tveganja investiranja.[103] Nejasno je tudi, kaj sploh pomeni »tveganje investiranja«: ali zadošča zgolj prevzem finančnega tveganja, ali pa je ključno organizacijsko ali morda še kakšno drugo tveganje.[104]

Kadar gre za velike in kompleksne podatkovne baze, je povsem običajno, da pri njihovi izdelavi sodeluje več oseb, ki vsaka prispeva svoj del naložbe v izdelavo. Vprašanje imetništva pravice *sui generis* je v takih primerih odvisno od tega, kdo je prispeval znatne naložbe, ki so z vidika Direktive pogoj za obstoj pravice *sui generis*.[105] Seveda je v takih primerih mogoče tudi hkratno imetništvo pravice *sui generis* s strani več oseb. V takih primerih je izredno pomembna pogodbena ureditev imetništva pravic.

Kadar gre za derivativnega imetnika pravice *sui generis,* ki je na primer to pravico pridobil na podlagi pogodbe ali univerzalnega pravnega nasledstva,[106] za aktivno legitimacijo za sodno uveljavljanje pravic ne bi smelo biti pomembno, kakšna je bila naložba pridobitelja v pridobitev pravice *sui generis*. Pogoja znatne naložbe, ki je pogoj za nastanek pravice *sui generis*, namreč ne gre širiti tudi na derivativnega pridobitelja pravic. Pridobitelj pravic lahko pravice pridobi tudi brezplačno, pa to na obstoj pravice *sui generis* in na njegovo aktivno legitimacijo nima vpliva. Za nastanek pravice *sui generis* je pomembna zgolj presoja, ali je izdelovalec v izdelavo baze vložil znatno naložbo, brez pomena pa je vprašanje,

[100] Člen 7(1) Direktive.

[101] Uvodna izjava (41) Direktive.

[102] Podrobneje o pojmu izdelovalca glej npr. Beunen (2007), str. 146–158; Leistner (2000), str. 169–171; Bensinger (1999), str. 170–181.

[103] Beunen (2007), str. 148.

[104] Nekateri menijo, da je bistven prevzem organizacijskega tveganja in da zgolj finančno tveganje ne zadošča (Beunen (2007), str. 152).

[105] Beunen (2007), str. 153–154; Bensinger (1999), str. 181.

[106] Člen 7(3) Direktive.

koliko je pravica *sui generis* vredna v pravnem prometu oziroma kakšno ceno (če sploh kakšno) lahko doseže.

6. Vsebina in kršitev pravice *sui generis*

6.1. Uvod

Direktiva vsebino pravice *sui generis* opredeljuje kot pravico preprečiti neupravičeno jemanje izvlečkov in/ali ponovno uporabo celotne vsebine baze podatkov ali njenega bistvenega dela, ocenjenega kakovostno in/ali količinsko. Ta pravica se nanaša na dejanja uporabnika, ki presegajo njegove zakonite pravice in s tem škodujejo naložbam izdelovalca baze.[107]

Iz Direktive izhajata torej dve pravici: pravica preprečiti neupravičeno jemanje izvlečkov in pravica preprečiti neupravičeno ponovno uporabo. Obe sta novost, čeprav sta podobni nekaterim že znanim pravicam (upravičenjem) v okviru avtorske pravice[108] in ju mnogi avtorji z njimi tudi primerjajo ali celo enačijo.[109] Glede na opredelitev obeh pravic in zlasti glede na njuno razlago s strani SEU pa se je izkazalo, da gre vendarle za nekoliko posebni pravici, ki v nekaterih pogledih odstopata od svojih sorodnic v okviru avtorske pravice.

SEU je pojma »jemanje izvlečkov« in »ponovna uporaba« razlagalo široko, tako da se nanašata na vsako neupravičeno dejanje prilastitve in razširjanja v javnosti celotne vsebine baze podatkov ali njenega dela kot rezultata naložb izdelovalca, s čimer se izdelovalcu odvzamejo dohodki, ki bi mu omogočili amortizacijo stroškov naložbe.[110] Predmet varstva s tema pravicama je omejen in obsega jemanje ali uporabo:[111]

1. celotne vsebine podatkovne baze,
2. vsakega kakovostno ali količinsko znatnega dela vsebine podatkovne baze in
3. kakovostno ali količinsko neznatnih delov vsebine podatkovne baze, kadar se ti uporabljajo ponovljeno in sistematično, pa je to v nasprotju z običajno uporabo te podatkovne baze ali v nerazumni meri (*unreasonably*)[112] prizadene zakonite interese njenega izdelovalca.

---

[107] Uvodna izjava (42) Direktive.

[108] Davison (2003), str. 87.

[109] ZASP ne govori o jemanju izvlečkov in/ali ponovni uporabi, temveč izrecno našteva, katere izključne pravice pripadajo izdelovalcu baze (141.c člen ZASP). Pravice po ZASP vsebinsko približno ustrezajo pravicama iz Direktive.

[110] Odstavek 51 *BHB*.

[111] Glej člen 7(1) in 7(5) Direktive ter člen 141.b ZASP.

[112] Slovenski prevod Direktive sicer po mojem mnenju z uporabo pojma »neupravičeno« ni ustrezen. ZASP pravilno sledi izvirniku v angleščini.

6.2. Pravice

6.2.1. Jemanje izvlečkov

Jemanje izvlečkov je v Direktivi opredeljeno kot stalni ali začasni prenos celotne vsebine baze podatkov ali njenega bistvenega dela na drug nosilec na katerikoli način in v katerikoli obliki.[113]

Bistveno je, da gre za prenos vsebine baze na drug nosilec, pri čemer ni pomembno, ali je ta nosilec enake vrste kot nosilec izvirne podatkovne baze ter ali je prenos stalen ali začasen.[114] Razlikovanje med stalnim in začasnim prenosom pa je lahko – odvisno od nacionalnega prava – upoštevno pri presoji teže kršitve oziroma pri višini odškodnine zaradi kršitve.[115]

Jemanje izvlečkov se zgodi v trenutku, ko je celotno vsebino baze ali njen bistven del mogoče najti na drugem nosilcu,[116] ni pa potrebno, da vsebina varovane baze izgine z izvirnega nosilca.[117]

SEU se zavzema za široko razlago pojma »jemanje izvlečkov«, ki je brez formalnih, tehničnih ali fizičnih meril.[118] Zato sta narava (vrsta) in oblika postopka, uporabljenega za jemanje izvlečkov, brezpredmetni.[119] Ni pomembno, ali prenos vsebine temelji na tehničnem postopku kopiranja vsebine varovane baze podatkov (kot je elektronski, elektromagnetni, elektro-optični ali analogni postopek) ali pa na preprostem ročnem postopku (na primer ročnem prepisovanju).[120]

Pojem »jemanje izvlečkov« ni odvisen od cilja, ki mu s prenašanjem vsebine podatkov iz varovane baze sledi kršitelj.[121] Za kršitev gre tudi tedaj, ko prenos vsebine iz varovane baze ni izveden z namenom nadaljnje uporabe prenesene vsebine (na primer za izdelavo nove, konkurenčne podatkovne baze). Če pa že je izveden z namenom nadaljnje uporabe prenesene vsebine, pa tudi ni pomembno, kakšen je ta namen: nepomembno je, ali je cilj izdelava druge baze podatkov (ki je konkurenčna prvotni bazi ali pa tudi ne ali pa je enako ali različno velika) ali

[113] Člen 7(2)(a) Direktive. Sklicevanje na celotno vsebino baze ali njen bistven del v definiciji jemanja izvlečkov in ponovne uporabe sta logična napaka (glej tudi Aplin (2005), str. 138–139).

[114] Za stalni prenos gre, če je gradivo trajno nameščeno na nosilcu, ki ni isti kot nosilec prvotne baze podatkov, medtem ko gre za začasni prenos, če je to gradivo za določeno krajše obdobje shranjeno na drugem nosilcu, na primer v delovnem pomnilniku računalnika (odstavek 44 *Apis*).

[115] Odstavek 43 *Apis*. V slovenskem pravu bi ta okoliščina lahko prišla v poštev pri odmeri civilne kazni.

[116] Odstavek 36 *Directmedia*.

[117] Odstavka 29–30 *Directmedia*.

[118] Odstavek 38 *Directmedia*.

[119] Odstavek 35 *Directmedia*.

[120] Odstavek 37 *Directmedia*.

[121] Odstavek 47 *BHB*.

pa to dejanje spada v dejavnost, ki ni izdelava baze podatkov (bodisi da je ta dejavnost komercialna bodisi da ni).[122]

Pri presoji jemanja izvlečkov ni pomembno, kaj se s prenesenimi podatki zgodi v morebitni kršiteljevi bazi. Ni pomembno, ali se zaradi prenosa vsebine varovane baze razporeditev zadevnih podatkov v kršiteljevi bazi razlikuje od razporeditve, ki je značilna za varovano bazo. Zato v pojem jemanja izvlečkov ne spada zgolj dejanje mehanskega reproduciranja vsebine baze podatkov ali njenega dela, brez preurejanja, s klasičnim postopkom kopiraj/prilepi.[123] Prav tako ni pomembno, ali je prenesena vsebina v kršiteljevi bazi spremenjena ali urejena na drugačen način kot v varovani bazi.

Kršitev pravice *sui generis* ni pogojena z neposrednim dostopom do varovane baze.[124] To pomeni, da varstvo obsega tudi primere posrednega jemanja izvlečkov (enako tudi posredne ponovne uporabe) podatkov, ki sicer izhajajo iz varovane baze, vendar jih je uporabnik pridobil iz nekega drugega vira.[125] To preprečuje obid prepovedi iz člena 7(1) Direktive.[126]

Zanimivo je stališče SEU, da t. i. vpogled v bazo (angl. *consultation*) ne pomeni jemanja izvlečkov in je dopusten brez soglasja imetnika pravic.[127] Vprašanje je vezano na digitalne podatkovne baze, ki jih izdelovalci dajo na voljo javnosti. SEU je pojasnilo, da dejstvo, da je izdelovalec baze omogočil ali dovolil dostop javnosti do vsebine baze (ne glede na to, ali je ta dostop odplačen ali ne), sicer ne vpliva na pravico izdelovalca, da prepreči dejanja jemanja izvlečkov in/ali ponovne uporabe celotne vsebine neke baze ali njenega bistvenega dela, da pa se v takem primeru varstvo ne nanaša na dejanje vpogleda tretjih oseb v bazo.[128] Kaj dejanje vpogleda dejansko pomeni, SEU ni pojasnilo,[129] je pa s tem zmanjšalo tveganje, da bi pravica jemanja izvlečkov delovala kot pravica dostopa do baze.[130]

---

122 Odstavek 48 *BHB.* Prvotni predlog Direktive je bil usmerjen le zoper dejanja kršiteljev, ki imajo komercialni namen.

123 Odstavka 39–40 *Directmedia*.

124 Odstavek 53 BHB.

125 Odstavek 52 BHB.

126 Aplin (2005), str. 140. Prepoved posrednega jemanja izvlečkov (drugače kot posredna ponovna uporaba) po mnenju nekaterih sicer preveč širi doseg pravice *sui generis* (več o tem Beunen (2007), str. 161–162; primerjaj Westkamp (2003a), str. 7).

127 Nekateri »pravico do vpogleda« (*right of consultation*) celo štejejo kot novo pravico, ki naj bi jo ustvarilo SEU (na primer Herr (2008), str. 112, 149).

128 Odstavki 54–56 BHB in odstavki 51–53 *Directmedia.*

129 Iz omenjenih sodb bi bilo mogoče razbrati, da gre za dejanje, pri katerem za prikaz vsebine baze na ekranu ni potreben prenos – stalni ali začasni – celotne vsebine ali njenega znatnega dela na drug nosilec. Več o vsebini pravice do vpogleda glej Herr (2008), str. 149–150; Davison, Hugenholtz (2005), str. 11.

130 Aplin (2005), str. 140.

6.2.2. Ponovna uporaba

Ponovna uporaba je v Direktivi opredeljena kot vsaka oblika dajanja na voljo javnosti celotne vsebine baze podatkov ali njenega bistvenega dela z distribuiranjem primerkov, z dajanjem v najem, s sprotnim prenosom (*on-line*) ali drugimi oblikami prenosa.[131] Gre za ravnanja, ki imajo običajno komercialno naravo.[132] Za ponovno uporabo gre na primer že v trenutku, ko je vsebina baze naložena na (javno) računalniško omrežje, pri čemer ni nujno, da bi vsebina baze dejansko že dosegla uporabnike.[133]

Enako kot pri jemanju izvlečkov tudi pri ponovni uporabi cilj oziroma namen ponovne uporabe ni pomemben.[134] Za kršitev gre ne glede na to, ali je vsebina varovane baze uporabljena v okviru konkurenčne baze kršitelja ali za povsem drug namen.

6.3. Predmet varstva (obseg pravic)

6.3.1. Znaten del, gledano kakovostno in/ali količinsko

6.3.1.1. Uvod

Jemanje izvlečkov in/ali ponovna uporaba sta prepovedana, kadar sta storjena v obsegu, ki zajema celotno bazo ali njen kakovostno ali količinsko znaten del. Ali je del vsebine baze znaten, je mogoče presojati tako s količinskega kot tudi s kakovostnega vidika.

Direktiva ne daje odgovora na vprašanje, kdaj se del baze šteje za znatnega in kako razlagati količinsko in kakovostno merilo. SEU je že pojasnilo, da izraz nebistveni (neznatni) del vsebine baze podatkov zajema vsak del, ki ne ustreza izrazu bistveni del, tako s količinskega kot kakovostnega stališča.[135] Obratno to pomeni, da je znaten vsak del vsebine, ki ni neznaten. S tem pa SEU še ni rešilo vprašanja, kje je meja med neznatnim in znatnim. To je razumljivo, saj absolutne meje ni mogoče postaviti, temveč je treba upoštevati okoliščine konkretnega primera,[136] vključno na primer z vrsto podatkovne baze oziroma njene vsebine. Koliko bolj so znatne naložbe v izdelavo baze, toliko manj znaten mora biti odvzeti del vsebine baze, in obratno.[137] To na primer pomeni, da gre pri bazi, v

[131] Člen 7(2)(b) Direktive.
[132] Gaster (1999), str. 130, odstavek 515.
[133] Beunen (2007), str. 169; Bensinger (1999), str. 194.
[134] Primerjaj Bensinger (1999), str. 189.
[135] Odstavka 73 in 82 *BHB*.
[136] Primerjaj Gaster (1999), str. 127, odstavek 497; Derclaye (2008), str. 109; Herr (2008), str. 143.
[137] Bensinger (1999), str. 205.

izdelavo katere je bila vložena naložba, ki komaj izpolnjuje pogoje znatne naložbe, za kršitev šele tedaj, če je odvzet ali ponovno uporabljen pretežen del vsebine; pri bazi, ki je rezultat velike naložbe, pa znaten del lahko predstavlja že sorazmerno manjši del vsebine.[138]

SEU je potrdilo, da mora obstajati korelacija med znatnim delom vsebine in znatno naložbo, kar je skladno z ekonomsko utemeljitvijo pravice *sui generis*.[139] Z drugimi besedami: o znatnem delu vsebine baze govorimo tedaj, ko z neupravičenim ravnanjem imetniku pravic nastane občutna škoda za amortizacijo njegove naložbe.[140]

Brez dvoma je znaten del vsebine tisti, ki tudi sam izpolnjuje pogoje za varstvo s pravico *sui generis* (na katerega je torej vezana znatna naložba).[141] Običajno pa je težko ugotoviti, kolikšen del naložbe v izdelavo podatkovne baze je vezan na točno določen del vsebine baze, zato je v praksi to merilo ugotavljanja znatnosti manj uporabno.[142] Treba je tudi upoštevati, da deli vsebine, ki sami po sebi ne bi izpolnjevali pogojev za varstvo s pravico *sui generis*, prav tako lahko predstavljajo znaten del vsebine.[143]

Stališča v tuji literaturi o tem, kaj pomeni znaten, so različna, vendar se zdi, da prevladuje stališče, da mora biti v tem primeru prag sorazmerno visok,[144] če naj preprečuje nastanek izključnih pravic na posameznih elementih vsebine in s tem zagotavlja prost pretok informacij.

6.3.1.2. Količinsko znatni del

Izraz bistven (oziroma znaten) del vsebine baze, ocenjen količinsko, se nanaša na količino podatkov, ki so bili izvlečeni ali ponovno uporabljeni iz baze, in ga je treba presojati glede na količino celotne vsebine varovane baze. Količina gradiva v bazi domnevnega kršitelja, v katero je preneseno gradivo iz izvirne baze, pri tej presoji ni relevantna.[145]

Če uporabnik jemlje izvlečke in/ali ponovno uporablja količinsko velik del vsebine podatkovne baze, za izdelavo katere so bila potrebna znatna sredstva, potem je po mnenju SEU sorazmerno znatna tudi naložba, ki ustreza izvlečenemu

[138] Prav tam.
[139] Tako tudi Koo (2010), str. 318.
[140] Leistner (2000), str. 173.
[141] Glej tudi Bensinger (1999), str. 203.
[142] Isti, str. 204.
[143] Prav tam.
[144] Na primer Beunen (2007), str. 186.
[145] Odstavek 60 *Apis*.

in/ali ponovno uporabljenemu delu.[146] Takšno stališče je lahko z vidika prostega pretoka informacij nevarno, saj predpostavlja, da je znatna naložba enakomerno porazdeljena po celotni vsebini baze, in zanemarja možnost, da je pretežni del naložbe vložen le v količinsko manjši del vsebine baze.[147] Posledično se lahko zgodi, ko bi kršitelj odvzel in/ali ponovno uporabil ravno tisti del vsebine baze, ki je sicer količinsko znaten, a ni zahteval znatne naložbe: v takem primeru bi šlo za kršitev, čeprav kršitelj v znatno naložbo izdelovalca baze sploh ne bi bil posegel. To bi bilo v nasprotju z namenom Direktive, ki je v tem, da prepreči zgolj tista ravnanja, ki kakovostno ali količinsko občutno škodujejo naložbi.[148] Uporaba zgolj količinskega merila je torej lahko nevarna.

SEU ni dalo natančnejših usmeritev glede tega, kaj naj bi predstavljalo količinsko znaten del. Čeprav naj bi bil po mnenju nekaterih avtorjev količinsko znaten del vsebine sorazmerno enostavno ugotovljiv,[149] v praksi in teoriji stališča o tem, kaj se šteje za količinsko znaten del, še zdaleč niso enotna. V tuji sodni praksi se je kot količinsko znaten del štelo na primer že 20 odstotkov vsebine baze,[150] medtem ko se v literaturi pojavlja stališče, da naj bi to pomenilo vsaj 50 odstotkov vsebine baze[151] oziroma visok odstotek vnosov.[152]

Ker enotnega in absolutnega merila ni, je treba upoštevati specifičnosti konkretne baze in količino elementov, ki jih vsebuje. Pri tem pa bi se veljalo izogibati situacijam, ko bi zgolj en element lahko predstavljal količinsko znaten del vsebine baze, saj bi to vodilo k monopolizaciji posameznih informacij.[153] Utemeljen se zato zdi argument, da bi zbirka izpolnjevala pogoje za podatkovno bazo šele tedaj, ko bi vsebovala toliko elementov, da posamezni element ne bi mogel predstavljati količinsko (ali kakovostno) znatnega dela vsebine.[154]

6.3.1.3. Kakovostno znatni del

Kakovostni vidik bo v praksi običajno igral vlogo dopolnilnega merila, zlasti kadar preneseni ali ponovno uporabljeni del vsebine ne bo količinsko znaten.

146 Odstavka 70 in 82 *BHB*.
147 Primerjaj Westkamp (2003a), str. 13–14.
148 Uvodna izjava (42) Direktive. Glej tudi Gaster (1999), str. 127, odstavek 496.
149 Davison, Hugenholtz (2005), str. 9.
150 Derclaye (2008), str. 114.
151 Bensinger (1999), str. 207.
152 Westkamp (2003a), str. 13.
153 Glej Bensinger (1999), str. 210, opomba 960.
154 Beunen (2007), str. 188.

Bolj kot je odvzeti ali ponovno uporabljeni del vsebine količinsko znaten, manjšo vlogo igra kakovostni vidik, in obratno.[155]

Izraz bistveni (oziroma znatni) del vsebine baze, ocenjen kakovostno, se nanaša na višino naložbe v pridobivanje, preverjanje ali predstavitev vsebine, ki je bila predmet jemanja izvlečkov in/ali ponovne uporabe, ne glede na to, ali je ta del vsebine količinsko bistveni del vsebine varovane baze. Po mnenju SEU lahko tudi količinsko zanemarljiv del vsebine baze s stališča pridobivanja, preverjanja in predstavitve pomeni veliko človeško, tehnično ali finančno naložbo.[156]

Resnična, notranja vrednost *(intrinsic value*) gradiva, ki je predmet jemanja izvlečkov ali ponovne uporabe, ni merilo za presojo, ali je zadevni del znaten.[157] Tako na primer ni pomembno, ali ima gradivo poseben pomen za izdelovalca baze ali za kršitelja, prav tako ni pomembno, kakšna je ekonomska vrednost elementa.[158] To preprečuje, da bi lahko bil zgolj posamezni element baze, najsibo sam po sebi še tako vreden, označen kot znaten del, če nanj ni vezana znatna naložba. Takšno stališče je pravilno glede na to, da naj pravica *sui generis* ne bi pomenila razširitve varstva na gola dejstva ali podatke,[159] prav tako pa naj ne bi omogočila nastanka nove pravice na samih delih, podatkih ali gradivu.[160] Namen Direktive je varstvo naložb v izdelavo podatkovne baze, ne pa varstvo podatkovne baze zaradi ekonomske ali drugačne vrednosti njene vsebine.[161]

6.3.2. Neznatni deli

Prepoved ponavljajočega se in sistematičnega jemanja izvlečkov ali ponovne uporabe neznatnih delov vsebine baze iz člena 7(5) Direktive naj ne bi predstavljala posebne pravice oziroma naj ne bi širila obsega pravice *sui generis;*[162] namen te prepovedi je zgolj preprečiti izogibanje prepovedi iz člena 7(1) Direktive prek ponavljajočega se in sistematičnega jemanja izvlečkov in/ali ponovne uporabe neznatnih delov vsebine baze, ki bi zaradi svojega kumulativnega učinka resno škodila naložbi izdelovalca baze.[163] Določba posledično preprečuje jemanje

[155] Bensinger (1999), str. 207.

[156] Odstavka 71 in 82 *BHB*. Ravno iz tega razloga nekateri avtorji opozarjajo na problematičnost kakovostnega merila (Davison, Hugenholtz (2005), str. 10). Postavlja se tudi vprašanje, ali lahko znaten del vsebine baze pomeni le en element, za pridobitev katerega pa je izdelovalec porabil znatna sredstva.

[157] Odstavek 72 *BHB.*

[158] Glej tudi Beunen (2007), str. 194.

[159] Glej uvodno izjavo (45) Direktive.

[160] Glej uvodno izjavo (46) Direktive.

[161] Tako tudi Beunen (2007), str. 193.

[162] Tako tudi Westkamp (2003a), str. 9.

[163] Odstavek 86 *BHB.*

izvlečkov, ki ga izvede uporabnik baze, ki bi s svojim ponavljanjem in sistematičnostjo privedlo do rekonstrukcije (brez dovoljenja imetnika pravic) celotne baze ali vsaj njenega znatnega dela.[164] Določba prav tako preprečuje tretji osebi, da bi se izognila prepovedi ponovne uporabe iz člena 7(1) Direktive s tem, da bi javnosti sistematično in ponavljajoče se dajala na voljo neznatne dele vsebine baze.[165]

Kdaj se šteje, da je ravnanje uporabnika v nasprotju z običajno uporabo oziroma kdaj neupravičeno prizadene zakonite interese izdelovalca baze, ni povsem jasno. Vprašanje je, ali med zakonite interese izdelovalca baze spada le interes za povrnitev začetne naložbe v izdelavo baze ali pa tudi interes za kasnejše ustvarjanje prihodkov z uporabo baze,[166] ter ali mora biti izkazana že dejanska škoda ali pa zadošča že možnost nastanka škode.[167]

6.4. Škodovanje naložbi kot impliciten pogoj kršitve

Iz uvodne izjave (42) Direktive izhaja, da se pravica *sui generis* nanaša na dejanja uporabnika, ki presegajo njegove zakonite pravice in s tem škodujejo naložbam; ne nanaša se le na izdelavo parazitskega konkurenčnega izdelka, temveč tudi na vsakega uporabnika, ki s svojimi dejanji kakovostno ali količinsko občutno škoduje naložbi. Iz tega izhaja, da je škodovanje naložbi bistveni pogoj kršitve. Takšno razlago je potrdilo tudi SEU, ki je vzpostavilo vez med znatno naložbo in testom kršitve: če nekdo prenese ali uporabi znaten del vsebine baze, ki ni rezultat znatne naložbe, kršitev ne bo podana.[168]

Direktiva predpostavlja, da je škodovanje znatni naložbi podano takoj, ko gre za neupravičen prenos celotne vsebine ali znatnega dela vsebine baze.[169] To pomeni, da imetnik pravic v takem primeru ni dolžan še posebej dokazovati, da kršitev škoduje njegovi naložbi. Mora pa to dokazovati v primeru, ko gre za sistematično jemanje izvlečkov in/ali ponovno uporabo neznatnih delov vsebine baze: tam je škodovanje naložbi izrecen znak kršitve.[170]

7. Nekateri praktični vidiki uveljavljanja pravnega varstva

V sporu zaradi kršitve pravice *sui generis* je z vidika imetnika pravic ključnega pomena konkretizirano zatrjevanje in dokazovanje znatne naložbe v izde-

[164] Odstavek 87 *BHB.*

[165] Odstavek 88 *BHB.*

[166] Več o tem Beunen (2007), str. 203–207.

[167] Beunen (2007), str. 207.

[168] Derclaye (2008), str. 111.

[169] Tako tudi Beunen (2007), str. 201; Davison (2003), str. 89.

[170] Tako tudi Beunen (2007), str. 201.

lavo podatkovne baze. Zaradi lažjega poznejšega dokazovanja je pomembno, da izdelovalec že v fazi izdelave baze poskrbi za skrbno dokumentiranje naložb. Glede na predstavljeno prakso SEU mora morebitne naložbe v ustvarjanje vsebine baze ločiti od naložb v pridobivanje, preverjanje in predstavitev vsebine baze. Pri dokazovanju finančnih in materialnih naložb ali porabe časa pri izdelavi baze bo običajno zadoščalo, da izdelovalec svojo naložbo dokazuje na osnovi prejetih računov (na primer za pridobitev programske opreme za izdelavo baze, za izdelavo spletne strani). Pri dokazovanju intelektualnega truda ali energije pa bodo v poštev prišla zlasti zaslišanja oseb, udeleženih pri izdelavi baze, ter dokazila o izobrazbi, znanjih in izkušnjah teh oseb.

Kadar je pri izdelavi baze udeleženih več izdelovalcev, je z vidika vsakega izmed njih pomembno, da ločeno dokumentira svoje naložbe. Za potrebe poznejšega uveljavljanja pravnega varstva je tudi pomembno, da so v takih primerih pravna razmerja glede imetništva pravic pogodbeno urejena na način, ki bo v sodnem postopku omogočal nedvoumno dokazovanje imetništva pravic.

Najzahtevnejši del postopka uveljavljanja pravice *sui generis* navadno predstavlja dokazovanje njene kršitve. Da bi imetnik pravice dokazal kršitev, bo moral dokazati, da podatki, ki jih je pridobil oziroma ponovno uporabil toženec, izvirajo (vsaj posredno) prav iz njegove podatkovne baze. Zlasti v primeru elektronskih podatkovnih baz se imetnik pravic pogosto sooči s težavo, kako temu dokaznemu bremenu zadostiti in sodišče z zadostno stopnjo verjetnosti prepričati v obstoj kršitve. Razlog za to težavo je v prvi vrsti ta, da je navadno izjemno težko (ali pa celo nemogoče) dokazati sámo dejanje prenosa podatkov iz varovane baze. Podatki o prometu po elektronskih komunikacijskih omrežjih, s katerimi razpolagajo operaterji in ki bi v določenih primerih lahko kazali, na čigav naslov je bila prenesena vsebina varovane baze, so za imetnika pravic praviloma nedosegljivi, zlasti kadar jih operaterji ne smejo hraniti za potrebe civilnega (pravdnega) postopka.[171]

Imetniku pravic praviloma ostane na voljo le dokazovanje kršitve s pomočjo posrednih dokazov oziroma indicev. Če na primer kršitelj vsebino varovane baze prenese in uporabi za izdelavo svoje baze, lahko na prenos podatkov iz varovane baze kažejo različne okoliščine, na primer enakost ali velika podobnost vsebine obeh baz; obstoj enakih napak v obeh bazah; obstoj več podatkov v obeh bazah, ki niso javno dostopni ali so zelo težko javno dostopni; enak ali zelo podoben izbor podatkov v obeh bazah (zlasti kadar je izbor v varovani bazi zelo omejen in specifičen); enaka ali zelo podobna struktura obeh baz; obstoj podatkov v

[171] Kot je to primer v slovenskem pravu, glej 163. člen Zakona o elektronskih komunikacijah (ZEKom-1).

kršiteljevi bazi, ki imajo v varovani bazi smisel (glede na naravo ali namen baze), v kršiteljevi pa ne; neobstoj istih podatkov v obeh bazah itd.

Dokazovanje kršitve je za tožnika še posebej težavno v primeru, kadar je gradivo, ki ga vsebuje njegova baza, mogoče pridobiti tudi iz javno dostopnih virov. Toženec bo namreč lahko ugovarjal, da je vse podatke pridobil iz javno dostopnih virov, in ne iz varovane baze. Za tožnika bo pomembno, da z dokazom posebnih okoliščin (glej prej navedeno) procesno dokazno breme prevali na toženca, ki bo potem moral dokazovati, da je svoje podatke dejansko pridobil iz javno dostopnih virov. V takem primeru za toženca ne bo zadoščal zgolj splošen ugovor, da je te podatke mogoče pridobiti tudi iz javno dostopnih virov (okoliščina, da je varovana baza javno dostopna, pa tudi ni relevantna). Za vsakogar, ki zbira podatke, je torej skrbno sprotno dokumentiranje virov pridobivanja podatkov lahko izrednega pomena, saj mu bo to omogočilo bodisi uspešno aktivno uveljavljanje svojih pravic bodisi uspešno obrambo zoper zahtevke imetnika pravic.

Dokazovanja kršitve pravice *sui generis* se je v svoji praksi dotaknilo tudi SEU. V zvezi s tem je pojasnilo, da je okoliščino, da se določeni stvarni in tehnični podatki iz vsebine varovane baze (na primer hiperpovezave, uredniške opombe) ali podatki iz virov, ki niso dostopni javnosti (na primer neobjavljene sodne odločbe), pojavljajo tudi v bazi drugega izdelovalca (toženca), mogoče razlagati kot indic, da je prišlo do jemanja izvlečkov iz varovane baze. SEU pa opozarja, da samo po sebi to ni zadosten dokaz za obstoj jemanja izvlečkov in da je treba presoditi, ali je takšno naključje mogoče razložiti tudi z drugimi dejavniki (na primer s tem, da sta stranki uporabljali iste vire),[172] ne pa s prenosom vsebine med zadevnima bazama. Dejstvo, da se gradivo, ki ga je izdelovalec varovane baze podatkov pridobil iz virov, ki niso dostopni javnosti (na primer neobjavljene sodne odločbe), pojavlja tudi v bazi drugega izdelovalca, samo po sebi prav tako ni zadosten dokaz za obstoj jemanja izvlečkov, lahko pa je njegov pokazatelj.

Izdelovalec baze si lahko poznejše dokazovanje jemanja izvlečkov iz njegove baze olajša že v fazi izdelave baze. V vsebino svoje baze lahko vgradi določene posebnosti ali celo namerne napake, za katere ve samo sam. Če se nato na primer v bazi nekoga tretjega pojavijo enake posebnosti ali napake, je to močan indic, da je ta tretja oseba podatke pridobila iz varovane baze.

Ker je mogoče s podatki v elektronski obliki hitro manipulirati, je z vidika imetnika pravic pomembno, da dokaze o kršitvi čim hitreje in čim učinkoviteje fiksira oziroma zavaruje. Dokaze o tem, s katerimi podatki razpolaga domnevni kršitelj in kako jih morebiti ponovno uporablja, lahko imetnik pravic pridobi na različne načine, odvisno od tega, kje in kako domnevni kršitelj te podatke hrani

[172] Odstavka 51 in 52 *Apis*.

ter kako jih morebiti ponovno uporablja. Kadar imetnik pravic sam nima dostopa do vsebin, ki jih hrani oziroma uporablja domnevni kršitelj, oziroma kadar teh vsebin ne more sam fiksirati, bo lahko pomembno vlogo igral sodni postopek zavarovanja dokazov s pomočjo sodnega izvedenca.

8. Namesto sklepa

Poleg predstavljenih vidikov pravnega varstva naložb v izdelavo podatkovnih baz velja omeniti še nekatera druga vprašanja. Že samo v okviru varstva na podlagi pravice *sui generis* so med drugim zanimiva vprašanja, ki so vezana na trenutek nastanka in trajanje pravice *sui generis*, pravice zakonitih uporabnikov ter vsebinske omejitve oziroma izjeme od pravice *sui generis*.

Ko govorimo o varstvu naložb v izdelavo podatkovnih baz, ne smemo spregledati tudi drugih možnih temeljev pravnega varstva (na primer pravo nelojalne konkurence, pogodbeno pravo, avtorsko pravico, pravno varstvo tehničnih ukrepov za zaščito podatkovnih baz) in njihovo razmerje s pravico *sui generis*.

Zanimiva pravna vprašanja izvirajo tudi iz razmerja med pravico *sui generis* in konkurenčnim pravom, zlasti v primeru podatkovnih baz, ki so edini vir podatkov, ki jih vsebujejo (angl. *sole source databases*). Potencialna nevarnost, da bi pravica *sui generis* v določenih primerih lahko povzročila zlorabo prevladujočega položaja, je identificirana že v sami Direktivi.[173] Zaradi nevarnosti, da bi bila pravica *sui generis* v primeru t. i. neoriginalnih podatkovnih baz (tj. baz, ki vsebujejo sicer nezaščiteno gradivo[174]) sredstvo za ustvarjanje monopolov nad podatki in s tem krčenje javne domene, so se v teoriji pojavile tudi številne polemike o tem, ali je uzakonitev izključne pravice sploh upravičena.[175] Zanimivo je, da je v zgodnejši fazi sprejemanja Direktive varstvo temeljilo na nelojalni konkurenci, a je bila ta ideja v teku sprejemanja Direktive zaradi neusklajenosti prava nelojalne konkurence znotraj EU opuščena.[176]

[173] Uvodna izjava (47) Direktive in člen 16(3) Direktive.

[174] Na primer rezultate športnih tekmovanj, vremenske podatke ali kontaktne podatke podjetij.

[175] Hugenholtz, Maurer, Onsrud (2001), str. 790, so predlagali celo razveljavitev Direktive. Na teoretični ravni naj sicer pravica *sui generis* ne bi pomenila razširitve varstva avtorske pravice na gola dejstva ali podatke, prav tako pa naj ne bi omogočila nastanka nove pravice na samih delih, podatkih ali gradivu. Glej uvodni izjavi (45) in (46) Direktive.

[176] Glej tudi uvodno izjavo (6) Direktive. Podrobneje o zgodovini sprejemanja Direktive glej Beunen (2007), str. 3–14; Herr (2008), str. 85–116, Westkamp (2003), str. 23–31; Chalton (2008), str. 8–39.

Literatura in viri

Knjige in članki

Aplin, Tanya: *Copyright Law in the Digital Society: the Challenges of Multimedia*. Hart Publishing, Oxford – Portland Oregon 2005.

Bensinger, Viola: *Sui generis Schutz für Databanken: Die EG-Datenbank Richtlinie vor dem Hintergrund des nordischen Rechts*. Verlag C. H. Beck, München 1999.

Beunen, Annemarie Christiane: *Protection for databases: The European Database Directive and its effects in the Netherlands, France and the United Kingdom*. Wolf Legal Publishers 2007.

Beurskens, Michael: *Schranken des Rechtlichen Schutzes von Datenbanken*. Heinrich-Heine-University Düsseldorf/Germany, Faculty of Law, 2004, magistrsko delo, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=646664 (9. 11. 2013).

Chalton, Simon: *The Legal Protection of Databases*. Viva Books Private Limited, 2008.

Davison, Mark J.: *The Legal Protection of Databases*. Cambridge University Press, 2003.

Davison, Mark J., Hugenholtz, Bernt: Football fixtures, horseraces and spin offs: the ECJ domesticates the database right. *E.I.P.R.* 2005-3, http://www.ivir.nl/publications/hugenholtz/EIPR_2005_3_databaseright.pdf (28. 10. 2013).

Derclaye, Estelle: *The Legal Protection of Databases: A Comparative Analysis*. Edward Elgar Publishing Limited, 2008.

Derclaye, Estelle: Database sui generis right: the need to take the public's right to information and freedom of expression into account. *New Directions in Copyright Law,* Volume 5. ed. F. Macmillan. Cheltenham: Edward Elgar, 2007, str. 3–23, http://works.bepress.com/estelle_derclaye/20 (28. 10. 2013).

Derclaye, Estelle: What is the Database Sui Generis Right?, *Know IP: Stockholm Network Monthly Bulletin on IPRS*, Issue 9, November 2005, http://works.bepress.com/cgi/viewcontent.cgi?article=1003&context=estelle_derclaye (28. 10. 2013).

Derclaye, Estelle: Databases Sui Generis Right: Should We Adopt the Spin Off Theory. *E.I.P.R.* 2004, 26(9), http://works.bepress.com/cgi/viewcontent.cgi?article=1007&context=estelle_derclaye (28. 10. 2013).

Gaster, Jens-Lienhard: *Der Rechtsschutz von Datenbanken: Kommentar zur Richtlinie 96/9/EG mit Erläuterungen zur Umsetzung in das deutsche und österreichische Recht*. Carl Heymanns Verlag KG, 1999.

Herr, Robin Elizabeth: *Is the Sui Generis Right a Failed Experiment?: A Legal and Theoretical Exploration of How to Regulate Unoriginal Database Contents and Possible Suggestions for Reform*. DJOF Publishing, Kopenhagen 2008.

Hugenholtz, Bernt: Abuse of Database Right: Sole-source information banks under the EU Database Directive, v: Lévêque F. in Shelanski H. (ur.): *Antitrust, patents and copyright: EU and US perspectives*. Cheltenham: Edward Elgar 2005, str. 203–219; http://www.ivir.nl/publications/hugenholtz/abuseofdatabaseright.html (28. 10. 2013).

Hugenholtz, Bernt: Program schedules, event data and telephone subscriber listings under the Database Directive: The spin-off doctrine in the Netherlands and elsewhere in Europe. *11th Annual Conference on International Intellectual Property Law and Policy*. Fordham School of Law, 2003, http://www.ivir.nl/publications/hugenholtz/spinofffordham.html (5. 11. 2013).

Hugenholtz, Bernt, Maurer, Stephen M., Onsrud, Harlan J.: Europe's Database Experiment. *Science*, vol. 294 (26 October 2001), http://www.ivir.nl/publications/hugenholtz/maurer.pdf (28. 10. 2013).

Koo, Anna: Database Right Decoded. *E.I.P.R.,* 2010, 32(7), str. 313–310, http://ssrn.com/abstract=1470676 (28. 10. 2013).

Leistner, Matthias: *Der Rechtsschutz von Datenbanken im deutschen und europäischen Recht: Eine Untersuchung zur Richtlinie 96/9/EG und zu ihrer Umsetzung in das deutsche Urheberrechtsgesetz*. Verlag C. H. Beck, München 2000.

Pitkänen, Olli, Virtanen, Perttu, Välimäki, Mikko: Legal Protection of Mobile P2P Databases. *Helsinki Institute for Information Technology*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.3009&rep=rep1&type=pdf (4. 11. 2013).

Stokes, Simon: *Digital Copyright: Law and Practice*. Hart Publishing, Oxford – Portland Oregon 2009.

Westkamp, Guido: *Der Schutz von Datenbanken und Informationssammlungen in britischen und deutschen Recht*. Verlag C. H. Beck, München 2003.

Westkamp, Guido: EU Database protection for information uses under an intellectual property scheme: has the time arrived for a flexible assessment of the European Database Directive?, *11 th Fordham Intellectual Property and Policy Conference*, Fordham School of Law, 2003, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1115432 (28. 10. 2013) (citirano kot: Westkamp (2003a)).

Sodbe Sodišča EU

Fixtures Marketing Ltd proti Organismos Prognostikon Agonon Podosfairou (OPAP) (C-444/02) z dne 9. 11. 2004 (citirano kot: OPAP).

Fixtures Marketing Ltd proti Oy Veikkaus AB (C-46/02) z dne 9. 11. 2004 (citirano kot: Veikkaus).

Fixtures Marketing Ltd proti Svenska Spel AB (C-338/02) z dne 9. 11. 2004 (citirano kot: Svenska Spel).

The British Horseracing Board Ltd proti William Hill Organisation Ltd (C-203/02) z dne 9. 11. 2004 (citirano kot: BHB).

Directmedia Publishing GmbH proti Albert-Ludwigs-Universität Freiburg (C-304/07) z dne 9. 10. 2008 (citirano kot: Directmedia).

Apis-Hristovich EOOD proti Lakorda AD (C-545/07) z dne 5. 3. 2009 (citirano kot: Apis).

Drugo gradivo

DG Internal Market and Services Working Paper: First Evaluation of Directive 96/9/EC on the Legal Protection of Databases, Bruselj, 12. 12. 2005 (citirano kot: First Evaluation).

Explanatory Memorandum to the First Proposal for a Database Directive, COM(92)24 Final, OJEC 1992 C 156/4, 13. 5. 1992 (citirano kot: Explanatory Memorandum).

Sklepni predlogi Generalne pravobranilke Christine Stix-Hackl z dne 8. 6. 2004 (k zadevi C-338/02 – Svenska Spel) (citirano kot: Svenska Spel (mnenje AG)).

Tridimenzionalno tiskanje in pravice intelektualne lastnine

dr. Matija Damjan

1. Oris problema

Tridimenzionalno (3D) tiskanje mediji v zadnjih letih pogosto opisujejo kot proizvodno tehnologijo, ki bo sprožila novo industrijsko revolucijo in potrošnikom omogočila izdelovanje različnih uporabnih predmetov kar doma.[1] Ameriški predsednik Obama je v letnem nagovoru kongresu februarja 2013 menil, da lahko 3D-tiskanje revolucionarno spremeni način, kako proizvajamo skorajda vse.[2] Širitev nove tehnologije pa bo odprla tudi nekatera pravna vprašanja. Ta prispevek preučuje, kako je možnost reproduciranja obstoječih umetniških ali uporabnih predmetov s 3D-tiskanjem združljiva s pravicami intelektualne lastnine, s katerimi so lahko tovrstni izdelki varovani.

1.1. Tehnologija 3D-tiskanja

Izraz 3D-tiskanje se laično uporablja kot skupna oznaka za različne aditivne proizvodne metode, pri katerih se tridimenzionalni fizični predmeti proizvajajo z nalaganjem tankih vodoravnih plasti materiala ene na drugo. Zaporedni sloji materiala po obliki ustrezajo navideznim vodoravnim prerezom virtualnega modela (načrta) izdelka in se med seboj trdno povežejo. 3D-tiskalnik tako z dodajanjem (tiskanjem) materiala v mnogih drobnih korakih v višino gradi stabilen izdelek in tako pretvarja digitalni model v fizični predmet.[3]

Tehnologij aditivne proizvodnje je več in se med seboj razlikujejo po načinu nanašanja in spajanja plasti ter uporabljenem materialu. Izraz 3D-tiskanje v ožjem

[1] Glej na primer 3D Printing: Second Industrial Revolution is Under Way. *New Scientist*, http://www.newscientist.com/special/3D-printing; Special Report: Manufacturing and Innovation: A Third Industrial Revolution. *The Economist*, 19. 4. 2012; Samuel Gibbs, Metal 3D printing and six key shifts in the 'second industrial revolution'. *The Guardian*, 9. 12. 2013; Jim Chalmers, 3D printing: not yet a new industrial revolution, but its impact will be huge. *The Guardian,* 10. 12. 2013.

[2] »… 3D printing … has the potential to revolutionize the way we make almost everything.« Remarks by the President in the State of the Union Address, February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address.

[3] Weinberg, str. 2, Austin, Grewal, Caddy, str. 22, Wikipedia, *3D Printing*.

pomenu označuje tehnologijo kapljično-prašnega nalaganja, ki je bila prvotno razvita na Massachusetts Institute of Technology. Pri tej metodi se tiskalna glava, podobna tisti pri pisarniškem brizgalnem tiskalniku, pomika po pladnju s prašnim materialom in nanj selektivno brizga tekoče vezivo, ki poveže prah v trdno snov. Po vsaki dodani plasti se pladenj 3D-tiskalnika spusti za debelino sloja, nanese se nov sloj prahu v obliki vodoravnega prereza predmeta in postopek se ponavlja, dokler ni tridimenzionalni izdelek »natisnjen«. Ta metoda se označuje tudi kot ciljno kapljično-prašno nalaganje. Druge metode aditivne proizvodnje so na primer še:

- stereolitografija (tudi selektivno strjevanje), pri kateri se z računalniško krmiljenim laserskim žarkom po plasteh strjuje tekoča, za UV-žarke občutljiva epoksidna ali akrilna smola;
- selektivno lasersko sintranje in selektivno lasersko varjenje, ki temeljita na laserskem taljenju poliamidnega ali kovinskega prahu po plasteh;
- ciljno neprekinjeno nalaganje (*fused deposition modeling*), pri katerem šoba na izdelek po plasteh brizga staljen material, ki se hitro strdi;
- nalaganje krojenih plasti (*laminated object modelling*), pri čemer se obrisi posameznih plasti z laserjem ali rezalnim zapisovalnikom krivulj izrežejo iz papirnate, plastične ali keramične folije in nato zlepijo s segreto epoksidno smolo;
- fotopolimerizacija (PolyJet), pri kateri tiskalna glava nabrizga sloj tekočega fotopolimera, ta pa se strdi pod vplivom UV-svetlobe, ki jo dovajata žarnici, nameščeni na obeh straneh glave.[4]

Kot rečeno, se je izraz 3D-tiskanje v zadnjem času uveljavil kot generična oznaka za vse metode aditivne proizvodnje, najbrž predvsem zato, ker je za laičnega bralca najlaže predstavljiv zaradi analogije z dvodimenzionalnim tiskanjem na pisarniških tiskalnikih. Kot skupno oznako za vse tovrstne proizvodne metode ga zato uporabljam tudi v tem prispevku, saj za tu obravnavana pravna vprašanja tehnične razlike med posameznimi aditivnimi postopki niso pomembne in je mogoče 3D-tiskanje v tem okviru obravnavati kot enoten pojav.

Prednost 3D-tiskanja kot proizvodne metode je, da lahko ena tiskalna naprava proizvede neskončno različnih oblik, ne da bi jo bilo treba v ta namen kakorkoli prilagoditi. V tem se razlikuje od klasičnih proizvodnih tehnik, ki temeljijo bodisi na odstranjevanju materiala s posebnimi orodji (rezanje, vrtanje) bodisi na vlivanju materiala v vnaprej izdelane kalupe. Ker so pri aditivni proizvodnji deli natisnjeni plast za plastjo, ima tiskalnik vedno neoviran dostop do zgornje plasti izdelka, na katero lahko dodaja material. Zato odpade zapleteno izračunavanje

[4] Weinberg, str. 2, http://www.rapiman.net/technology.php?pid=1, Wikipedia, *3D Printing*.

poti računalniško vodenih rezalnih strojev, ki je potrebno pri substrakcijski proizvodni metodi. Delovanje računalniškega programa, ki nadzira tiskalno napravo na podlagi virtualnega modela načrtovane oblike, pa je zelo preprosto. Čeprav je 3D-tiskanje običajno nekoliko manj natančno od rezanja, je sposobno proizvesti bolj zapletene oblike kot katerakoli druga primarna proizvodna tehnologija. 3D-tiskalniki lahko neposredno izdelujejo celo predmete z gibljivimi notranjimi deli. Ni torej treba izdelati vsakega sestavnega dela posebej in jih nato sestaviti, temveč lahko tiskalnik izdela že sestavljeno napravo.[5]

Za 3D-tiskanje je najprej potreben digitalni načrt, ki opisuje površinsko geometrijo tridimenzionalnega predmeta, ki bo natisnjen. Gre za virtualni tridimenzionalni model načrtovanega predmeta. Ti modeli so ustvarjeni s programi za računalniško podprto oblikovanje (*computer-aided design* – CAD), zato navadno govorimo o modelu CAD ali datoteki CAD. Programe CAD uporabljajo oblikovalci, inženirji in arhitekti za predstavitev videza načrtovanih izdelkov oziroma objektov pred izdelavo fizičnih prototipov, saj je model CAD mogoče preprosto spreminjati in tako hitro preizkusiti videz različnih verzij načrta. Model CAD je mogoče ustvariti tudi iz že obstoječega fizičnega predmeta, in sicer tako, da se tridimenzionalno skenira s posebnim 3D-skenerjem. Tako kot pisarniški skenerji s papirja optično odčitajo besedilo ali sliko, lahko 3D-skenerji odčitajo obliko fizičnega predmeta in jo zapišejo v digitalno datoteko. Datoteka CAD ni program, ki bi vodil delovanje 3D-tiskalnika, ampak le triangularna predstavitev tridimenzionalnega predmeta, ki jo ustrezen program šele uporabi kot načrt za tiskanje, in sicer tako, da ga virtualno razreže na vodoravne sloje (prereze predmeta), tiskalniku pa nato narekuje tiskanje zaporednih plasti materiala v obliki teh slojev, enega na drugega, dokler ne ustvari celotnega predmeta.[6]

Tehnološke zmogljivosti 3D-tiskalnikov hitro napredujejo in omogočajo čedalje natančnejše tiskanje z vse več različnimi materiali (plastične mase, kovine, karbonska vlakna, glina, gips, sladkor …).[7] V industriji se je 3D-tiskanje začelo uveljavljati v začetku 80. let prejšnjega stoletja, in sicer najprej pri modeliranju v fazi razvoja novih izdelkov. Tedaj tehnologija aditivne izdelave še ni bila primerna za serijsko proizvodnjo izdelkov, omogočala pa je hitrejše in cenejše izdelovanje prototipov kot s klasičnimi proizvodnimi metodami, zato se kot sinonim za 3D-tiskanje še vedno uporablja tudi izraz hitra izdelava prototipov (*rapid prototyping*).[8] Danes se 3D-tiskanje industrijsko uporablja tudi za izdelavo končnih izdelkov, zlasti za izdelavo posamičnih predmetov, ki morajo biti individualno

[5] Weinberg, str. 2, Bradshaw, Bowyer, Haufe, str. 8.

[6] Weinberg, str. 2–3, Rideout, str. 168, Austin, Grewal, Caddy, str. 22.

[7] Kuehn, str. 27.

[8] Bradshaw, Bowyer, Haufe, str. 8.

prilagojeni (na primer različni prostetični izdelki in medicinski implantati), ali za izdelavo kompleksnih oblik, ki s klasičnimi proizvodnimi tehnologijami niso izvedljive (na primer ležaji za vrata pri letalih Airbus A380). Najbrž pa 3D-tiskanje nikoli ne bo nadomestilo klasičnih proizvodnih tehnologij pri velikoserijski proizvodnji izdelkov, kjer lahko pride do izraza ekonomija obsega.

Dokler se 3D-tiskanje uporablja samo v industriji, še ne moremo govoriti o revolucionarnih spremembah v organizaciji proizvodnje dobrin. Stvari pa postanejo bolj zanimive, tudi s pravnega vidika, ko postane neposredno dostopno končnim uporabnikom. 3D-tiskanje je v potrošniško sfero začelo vstopati v zadnjih nekaj letih, ko so 3D-tiskalniki za domačo rabo postali cenejši in zmogljivejši.[9] Projekt RepRap (*replicating rapid-prototyper*) ponuja 3D-tiskalnik, katerega značilnost je, da se lahko samoreplicira: večino njegovih sestavnih delov je namreč mogoče natisniti na domačem 3D-tiskalniku. Načrti tiskalnika so javnosti na voljo brezplačno pod pogoji proste licence GNU GPL, gre torej za »odprto« strojno opremo (*open hardware*). Stroške domače izdelave takšnega 3D-tiskalnika ocenjujejo na okrog 400 evrov.[10] Po podobnih načelih deluje projekt Fab@Home.[11] Bolj komercialen proizvod je 3D-tiskalnik MakerBot Replicator 2, ki ga ni mogoče izdelati doma, njegov cilj pa je domače 3D-tiskanje čim bolj poenostaviti in ga približati tudi uporabnikom, ki tehnološko niso posebej vešči.[12] Dostopnost in izmenjavo načrtov CAD za 3D-tiskanje MakerBot omogoča na spletni strani Thingiverse.[13] Isto podjetje pa izdeluje tudi domači 3D-skener MakerBot Digitizer, s katerim lahko uporabniki izdelajo model CAD tako, da skenirajo obstoječ fizični predmet. Kombinacija skenerja in tiskalnika torej omogoča kopiranje tridimenzionalnih predmetov (pri čemer je kakovost kopije odvisna od kompleksnosti kopiranega predmeta in zmogljivosti 3D-tiskalnika).

Seveda domače 3D-tiskanje še ni običajna dejavnost v povprečnem gospodinjstvu. Sedanji imetniki 3D-tiskalnikov spominjajo na uporabnike osebnih računalnikov v zgodnjih devetdesetih letih prejšnjega stoletja: gre za razmeroma majhno skupino tehnološko usposobljenih entuziastov, ki jih je pritegnil potencial nove tehnologije, a nakazujejo smer njene širše uveljavitve.[14] Storitev

[9] Weinberg, str. 1. Razlog za to je tudi iztek veljavnosti patentov, s katerimi so bili zaščiteni nekateri postopki 3D-tiskanja.

[10] Spletna stran projekta: http://reprap.org.

[11] Spletna stran projekta: http://www.fabathome.org.

[12] Spletna stran proizvajalca: http://www.makerbot.com.

[13] http://www.thingiverse.com.

[14] Weinberg, str. 1. O sedanjih možnostih potrošniške rabe 3D-tiskanja, celo za tiskanje hrane, glej na primer Jacobs, nav. delo.

3D-tiskanja pa postaja dostopna tudi prek interneta. Spletne strani Shapeways,[15] Sculpteo[16] in i.materialise[17] ponujajo potrošnikom 3D-tiskanje po naročilu: uporabnik lahko izbere za tiskanje katerega od modelov CAD, ki so objavljeni na spletni strani ponudnika, ali pa naloži za tiskanje svoj načrt CAD. To pomeni, da potrošniki niti ne potrebujejo lastnega 3D-tiskalnika, da bi zasnovali in natisnili 3D-predmet.[18]

1.2. Možnost konflikta s pravicami intelektualne lastnine

Mnogi so prepričani, da bo vsakomur dostopna tehnologija 3D-tiskanja povzročila novo industrijsko revolucijo, po kateri bodo potrošniki na internetu le še poiskali digitalne načrte fizičnih izdelkov in jih nato natisnili sami, namesto da bi izdelke kupili v trgovini.[19] Tak razvoj bi korenito posegel v gospodarske interese klasičnih proizvajalcev, saj bi bistveno zmanjšal potrebo po tradicionalnih proizvodnih postopkih, povezanih s fiksnimi stroški prevoza in distribucije blaga.[20] Mogoče je pričakovati, da bodo klasični proizvajalci svoje izdelke skušali čim bolj varovati pred domačim 3D-tiskanjem z uveljavljanjem različnih pravic industrijske lastnine – podobno, kot so ravnale glasbena, filmska in programska industrija, ko je širitev osebnih računalnikov in interneta omogočila preprosto razmnoževanje in razširjanje digitalnih dobrin.[21]

Izdelava novih predmetov s 3D-tiskanjem po lastnih originalnih načrtih največkrat ne bo problematična, prav tako ne kopiranje pravno nevarovanih predmetov.[22] Vendar vsak objekt, izdelan z domačim 3D-tiskalnikom, ne bo rezultat individualnega ustvarjanja, ampak bo pogosto zgolj kopija obstoječega komercialnega proizvoda, za katero bo uporabnik model CAD bodisi izdelal sam s 3D-skeniranjem bodisi si že izdelan model prenesel z interneta.[23] Reproduciranje komercialnih izdelkov bo za potrošnike zanimivo zlasti pri tistem blagu, pri katerem je vrednost samega materiala bistveno manjša od cene izdelka, ta pa izvira zlasti iz posebne oblike, ugleda avtorja oziroma proizvajalca ali iz posebej učinkovite tehnične rešitve.[24]

---

15 http://www.shapeways.com.

16 http://www.sculpteo.com.

17 http://i.materialise.com.

18 Rideout, str. 164. Austin, Grewal, Caddy, str. 22.

19 Rideout, str. 162, Barnatt, str. 192–217.

20 Austin, Grewal, Caddy, str. 22.

21 Brean, str. 781.

22 Lahko seveda krši druge predpise, na primer če gre za proizvodnjo delov orožja.

23 Weinberg, str. 6.

24 Weinberg, str. 4, Bradshaw, Bowyer, Haufe, str. 6.

V nadaljevanju je najprej prikazano, katere pravice intelektualne lastnine sploh pridejo v poštev za pravno varstvo tridimenzionalnih predmetov, nato pa analizirano, v katerih primerih 3D-tiskanje predmetov krši tovrstne izključne pravice oziroma v katerih primerih se lahko uporabniki uspešno sklicujejo na katero od zakonskih izjem. Posebej je obravnavano vprašanje, kdaj lahko kršitev pravic povzročita že sama izdelava in internetno razširjanje digitalnih modelov CAD.

2. Pravno varstvo tridimenzionalnih predmetov

2.1. Varstvo z avtorsko pravico

V skladu s 5. členom Zakona o avtorski in sorodnih pravicah (ZASP)[25] je tridimenzionalni predmet lahko varovan z avtorsko pravico, če gre za individualno intelektualno stvaritev s področja književnosti, znanosti ali umetnosti, ki je na kakršenkoli način izražena. Med kategorijami avtorskih del, ki jih zakon primeroma našteva, so tridimenzionalne oblike nekatera likovna dela (zlasti kipi in reliefi), dela uporabne umetnosti in industrijskega oblikovanja, plastične predstavitve znanstvene, izobraževalne ali tehnične narave (na primer modeli strojev in drugih tehničnih naprav, modeli mest, tridimenzionalni učni pripomočki) [26] ter izvedena arhitekturna dela. Pri fizičnih predmetih je pogoj izraženosti vedno izpolnjen, zato je za obstoj avtorskopravnega varstva odločilno vprašanje, ali delo dosega ustrezno ustvarjalno raven. To merilo je težko jasno opredeliti. Pravna teorija navaja, da mora biti avtorsko ustvarjanje osebni intelektualni proces (ne more biti na primer le rezultat naključja ali delovanja naprave), v delu pa mora biti izražena določena količina individualnosti.[27]

Izmed pravic intelektualne lastnine avtorska pravica najbrž varuje največ tridimenzionalnih predmetov, saj avtorskopravno varstvo nastane že na podlagi zakona s samim trenutkom stvaritve avtorskega dela, medtem ko se pravice industrijske lastnine pridobijo šele z registracijo (razen razmeroma kratkotrajnega neregistriranega modela Skupnosti). Novost dela ni pogoj za pridobitev avtorske pravice, njeno trajanje pa je najdaljše, praviloma še 70 let po avtorjevi smrti. Vendar večina komercialno zanimivih tridimenzionalnih izdelkov vendarle ne uživa avtorskopravnega varstva. Z avtorsko pravico so namreč varovani predvsem predmeti, ki imajo (tudi) umetniško ali okrasno funkcijo, v kateri

[25] Uradni list RS, št. 21/1995, 9/2001, 30/2001, 85/2001 Skl. US: U-I-149/98-36, 43/2004, 58/2004 Odl. US: U-I-200/02-12, 94/2004 – UPB1, 17/2006, 44/2006 – UPB2, 114/2006 – ZUE, 139/2006, 16/2007 – UPB3, 68/2008, 85/2010 Skl. US: U-I-191/09-7, Up-916/09-16, 47/2013 Odl. US: U-I-240/10-15.

[26] Trampuž, Oman, Zupančič, str. 43, Schack, str. 95–96.

[27] Primerjaj Trampuž, Oman, Zupančič, str. 32.

se odraža avtorjeva individualna ustvarjalnost, ne pa tudi čisti funkcionalni predmeti. Nekateri tuji pravni redi, na primer ameriški, funkcionalne predmete (*useful article*) izrecno izključujejo iz avtorskopravnega varstva, ker jih je mogoče varovati že s patentom.[28] Avtorskopravno varstvo priznavajo samo dekorativnim ali ustvarjalnim elementom funkcionalnih predmetov, ki niso neločljivo povezani s funkcijo predmeta, na primer grafični vzorec na tehničnem predmetu, ki bi ga bilo mogoče od predmeta ločiti in uporabiti samostojno (t. i. test ločljivosti).[29] Slovenski pravni red funkcionalnih predmetov sicer posebej ne izloča iz avtorskopravnega varstva, vendar je že iz splošne opredelitve avtorskega dela jasno, da kadar obliko določenega predmeta narekuje predvsem njegova funkcija, delo praviloma ne dosega zadostne ustvarjalne ravni, da bi mu lahko priznali avtorskopravno varstvo. Kot avtorska dela so tako lahko varovani samo tisti funkcionalni predmeti, katerih oblika je ustvarjalni presežek, neodvisen od funkcije predmeta, tako da bi isto funkcijo lahko opravljal tudi predmet bistveno drugačne oblike.[30] Z avtorsko pravico v nobenem primeru ni varovana funkcija, ampak samo konkretna oblika predmeta. Mogoče pa je seveda, da je dvodimenzionalno avtorsko delo, na primer okrasna grafika, na tridimenzionalnem izdelku, ki sam ni avtorsko delo. V takšnem primeru avtorska pravica varuje samo dvodimenzionalno likovno delo, ne preprečuje pa reproduciranja tridimenzionalnega predmeta brez takšnega okrasa.

2.2. Varstvo s patentom

S patentom so lahko varovani postopki in predmeti. Za obravnavano problematiko so relevantni samo patenti na predmetih,[31] pri čemer pa vsak tridimenzionalni izdelek še ni patentabilen, saj patenti ščitijo samo (funkcionalne) izume. Zakon o industrijski lastnini (ZIL-1)[32] v 10. členu določa, da se patent lahko podeli za izum s slehernega področja tehnike, ki je nov, na inventivni ravni in

[28] Glej opredelitev slikovnih, grafičnih in kiparskih del v 17 U.S.C. §101.

[29] Weinberg, str. 6–7, Rideout, str. 168–169. Na podobnih izhodiščih temelji odločitev britanskega vrhovnega sodišča v zadevi *Lucasfilm proti Ainsworth* iz leta 2011, ko ni priznalo avtorskopravnega varstva značilnim čeladam vojakov iz serije filmov Vojne zvezd (*stormtroopers*), češ da gre predvsem za funkcionalni predmet. Austin, Grewal, Caddy, str. 23, Smith, str. 25.

[30] Trampuž ugotavlja, da je pri delih uporabne umetnosti in industrijskega oblikovanja ustvarjalni manevrski prostor zaradi njihovega funkcionalnega poslanstva zožen, pogosto pa je tudi povzemanje rešitev. Trampuž, Oman, Zupančič, str. 42.

[31] Tudi tehnologija 3D-tiskanja je zaščitena z vrsto patentov, za postopke in za predmete, vendar nas tu zanimajo samo patenti, ki varujejo tridimenzionalne predmete, kakršne je mogoče reproducirati s 3D-tiskanjem.

[32] Uradni list RS, št. 45/2001, 96/2002, 7/2003 – UPB1, 37/2004, 102/2004 – UPB2, 20/2006, 51/2006 – UPB3, 100/2013.

industrijsko uporabljiv. Izum je nov, če ni obsežen s stanjem tehnike, ki je bilo dostopno javnosti pred vložitvijo patentne prijave. Šteje se, da je izum na inventivni ravni, če za strokovnjaka predmet izuma očitno ne izhaja iz takega stanja tehnike, in da je uporabljiv, če se predmet izuma lahko proizvede ali uporabi v katerikoli gospodarski dejavnosti, vključno s kmetijstvom.

Patentna zaščita torej pride v poštev za novoizumljene tehnične izdelke, ki so funkcionalni in kakorkoli gospodarsko uporabni. Preprosti predmeti, kot na primer jedilni pribor, s patentom navadno ne morejo biti varovani, ker ne gre za novo tehnično rešitev.[33] Obseg patentne zaščite je omejen še v dveh pogledih. Po eni strani je redko varovan celoten izdelek, ampak samo tisti del izdelka, ki implementira patentirani izum. Po drugi strani je običajno varovan samo patentirani izum kot celota (in to le v okviru patentnih zahtevkov), ne pa tudi vsi njegovi posamezni sestavni deli, če ti niso posebej patentirani.[34] Trajanje patenta je bistveno krajše kot pri avtorski pravici, in sicer traja dvajset let od datuma vložitve patentne prijave. Patenti zato varujejo bistveno manj predmetov kot avtorska pravica in za krajši čas. Je pa patentno varstvo močnejše od avtorske pravice, ker ne predvideva izjeme za neodvisen razvoj izdelka – vse kopije patentiranega izuma kršijo patent, ne glede na to, ali je kršitelj za patent vedel ali ne.

2.3. Varstvo z modelom

Medtem kot patent ščiti funkcionalnost, je model pravica industrijske lastnine, ki je posebej namenjena varstvu videza industrijskih ali obrtnih izdelkov. Če gre pri izdelku za individualno intelektualno stvaritev s področja uporabne umetnosti oziroma industrijskega oblikovanja, pa je lahko poleg modela varovan tudi z avtorsko pravico. Naša zakonodaja namreč sprejema sistem kumulativnega varstva: če so izpolnjeni pogoji po avtorskem in industrijskem statutu, se predmet varuje kumulativno po ZASP in ZIL-1.[35] Ni pa takšno dvojno varstvo nujno, saj se lahko z modelom zaščiti tudi izdelek, ki ni avtorsko delo.

V skladu s 33. členom ZIL-1 se model registrira za videz izdelka, ki je nov in ima individualno naravo. Videz izdelka pomeni izgled celotnega izdelka ali njegovega dela, ki izhaja iz značilnosti zlasti linij, obrisov, barv, oblike, teksture oziroma materialov izdelka samega ali ornamentov na njem. Model lahko varuje tudi posamezne dele kompleksnega izdelka, embalažo, opremo, grafične simbole in tipografske znake. Videz izdelka je nov, če pred datumom vložitve prijave javnosti ni bil dostopen (v bistvenem) enak videz izdelka. Šteje se, da ima videz

[33] Smith, str. 26.

[34] Weinberg, str. 8.

[35] Trampuž, Oman, Zupančič, str. 42,

individualno naravo, če se celotni vtis, ki ga naredi na seznanjenega uporabnika, razlikuje od celotnega vtisa, ki ga naredi kak drug videz izdelka.[36] Skoraj identična opredelitev obsega varstva velja tudi za model Skupnosti, ki z enotnim učinkom velja v vseh državah članicah EU.[37]

Model je najbolj uporabna pravica za zaščito dvo- ali tridimenzionalnega videza komercialnih izdelkov, zato se povečuje njegova uporaba na različnih gospodarskih področjih, kjer je oblika izdelka ključnega pomena za njegovo prodajo. Proizvajalci avtomobilov z modelom vse pogosteje varujejo posamezne zunanje sestavne dele vozil (dele karoserije, žaromete in zrcala), da bi tretjim strankam preprečili vstop na trg nadomestnih delov.[38] Varstvo je strožje kot pri avtorski pravici, saj ne varuje le pred neposrednim kopiranjem obstoječega izdelka, ampak tudi pred zavajajočim posnemanjem in ustvarjanjem enakega videza izdelka pri potrošnikih.

Vendar pa je tudi doseg uporabe modela omejen. Sestavne dele kompleksnega izdelka je mogoče z modelom zaščititi samo, če ostanejo vidni ob normalni uporabi kompleksnega izdelka pri končnem uporabniku (brez opravil vzdrževanja, servisiranja ali popravljanja) in če vidne značilnosti sestavnega dela tudi same izpolnjujejo pogoja glede novosti in individualne narave. Model torej ne more varovati notranjosti izdelka, ampak samo njegovo zunanjo obliko. Druga pomembna omejitev je, da se z modelom ne morejo zaščititi tiste značilnosti videza, ki so določene izključno z njegovo tehnično funkcijo, torej da je določena oblika izdelka ali dela izdelka edina (nenadomestljiva z drugačno obliko) in le takšna zagotavlja zahtevano funkcionalnost izdelka.[39] Enaka izjema velja za značilnosti videza izdelka, ki morajo biti reproducirane v natančni obliki in dimenzijah, zato da bi bilo mogoče izdelek, na katerega se videz nanaša, mehansko povezati z drugim izdelkom ali ga vanj, okrog njega ali ob njega namestiti, tako da lahko vsak izdelek opravlja svojo funkcijo (t. i. izjema *must-fit*).[40] Zaradi teh omejitev mnogi izdelki, ki so zanimivi za domače 3D-tiskanje, ne morejo biti zaščiteni z modelom.[41]

[36] Merili individualnosti po ZASP in po ZIL-1 se razlikujeta. Medtem ko se pri avtorskem delu individualnost intelektualne stvaritve nanaša predvsem na njeno povezavo z osebo avtorja, pa se pri modelu presoja individualnost videza izdelka, in to predvsem z vidika tretje osebe – uporabnika.

[37] Glej 3. do 6. člen Uredbe Sveta (ES) št. 6/2002 z dne 12. decembra 2001 o modelih Skupnosti.

[38] Weinberg, str. 10.

[39] Sodba Višjega sodišča v Ljubljani I Cpg 493/2008 z dne 12. 3. 2009.

[40] Člen 36 ZIL-1, enako 8. člen Uredbe 6/2002.

[41] Bradshaw, Bowyer, Haufe, str. 15–16.

Varstvo z modelom traja eno ali več petletnih obdobij od datuma vložitve prijave, skupaj pa največ petindvajset let. Varstvo z neregistriranim modelom Skupnosti pa traja tri leta, odkar je bil prvič dostopen javnosti v Evropski uniji.

2.4. Varstvo z znamko

Kot znamka se sme registrirati kakršenkoli znak ali kakršnakoli kombinacija znakov, ki omogočajo razlikovanje blaga ali storitev enega podjetja od blaga ali storitev drugega podjetja in jih je mogoče grafično prikazati. Člen 42 ZIL-1 kot primere možnih znamk poleg besed, črk, številk in figurativnih elementov izrecno omenja tudi tridimenzionalne podobe, vključno z obliko blaga ali njegove embalaže. Obliko blaga ali embalaže kot možen razlikovalni znak omenjata tudi 2. člen Direktive 2008/95/ES o harmonizaciji znamk[42] in 4. člen Uredbe 207/2009 o blagovni znamki Skupnosti.[43] Z znamko je torej mogoče zaščititi tudi tridimenzionalno obliko blaga, na primer značilno obliko steklenice Coca-Cole. Z vidika proizvajalcev je znamka privlačna za zaščito oblike izdelkov predvsem zato, ker zanjo ne velja absolutna omejitev trajanja: podeli se za deset let od datuma vložitve prijave, jo je pa mogoče poljubno mnogokrat obnoviti za nadaljnjih deset let.

Drugače kot pri modelu primarni predmet varstva s tridimenzionalno znamko ni sam videz izdelka, ampak njegova razlikovalna funkcija v gospodarskem prometu. Običajne oblike večine izdelkov ne dosegajo takšnega razlikovalnega učinka, zato je sodna praksa pri priznavanju tridimenzionalnih znamk precej restriktivna. Sodišče EU je na primer zavzelo stališče, da ima tridimenzionalna znamka, ki ima videz proizvoda samega, razlikovalni učinek le v primeru, ko se znatno razlikuje od standarda ali navad v sektorju in zato izpolnjuje svojo bistveno nalogo označbe izvora.[44] Temu stališču sledi tudi slovensko Vrhovno sodišče, ki je zavrnilo registracijo znamke za tridimenzionalni znak v podobi zelene steklenice oziroma plastenke za pijače, češ da povprečen potrošnik golo obliko embalaže pijače zaznava kot kazalnik izvora le takrat, ko se ta oblika takoj zazna kot takšna označba, ker je bistveno drugačna od navad v sektorju, in ne gre zgolj za različico ene izmed običajnih oblik.[45] Podobno kot velja za model, pa se z znamko ne more zaščititi oblika izdelka, ki izhaja iz same narave blaga

[42] Direktiva 2008/95/ES Evropskega parlamenta in Sveta z dne 22. oktobra 2008 o približevanju zakonodaje držav članic v zvezi z blagovnimi znamkami.

[43] Uredba Sveta (ES) št. 207/2009 z dne 26. februarja 2009 o blagovni znamki Skupnosti.

[44] Sodba Sodišča EU v zadevi C-238/06 P Develey proti Uradu za usklajevanje na notranjem trgu (znamke in modeli) (UUNT), točki 80–81. Glej tudi sodbo istega sodišča v zadevi C-98/11 P, *Lindt & Sprüngli proti UUNT,* točka 42. Podrobneje Dolžan, str. 24, in Skubic, str. 27.

[45] Sodba Vrhovnega sodišča X Ips 1143/2004 z dne 11. 12. 2007.

ali je nujna za dosego tehničnega učinka ali daje blagu bistveno vrednost.[46] Iz tega razloga na primer ni bila priznana tridimenzionalna znamka za značilno obliko kock Lego.[47] Znamka bo torej razmeroma redko prišla v poštev kot oblika pravnega varstva oblike tridimenzionalnih predmetov.

2.5. Ugotovitve glede pravnega varstva

Nobena od pravic intelektualne lastnine ni takšna, da bi lahko varovala vse tridimenzionalne predmete, zato o enotnem sistemu pravnega varstva takšnih predmetov ni mogoče govoriti. Položaj je torej drugačen kot pri digitalnih dobrinah, na primer elektronskih knjigah, glasbi, filmih ali računalniških programih, ki so vsi primarno varovani z avtorsko pravico, dodatno pa lahko še z drugimi pravicami (sorodne pravice, patent, model, znamka). Za vsak predmet je torej treba posebej ugotavljati, ali je sploh pravno varovan in s katerimi pravicami. Največ predmetov, zlasti umetniške in okrasne narave, varuje avtorska pravica, ki se pridobi brez registracije, nima pogoja novosti in ima dolgo trajanje. Za varovanje videza industrijskih in obrtnih izdelkov je najprimernejši model, izjemoma tudi znamka. Funkcionalnost tehničnih izdelkov pa lahko pred kopiranjem ščiti patent. V nadaljevanju je treba za vsako od teh pravic posebej preučiti, kdaj reproduciranje varovanih predmetov z uporabo 3D-tiskanja pomeni kršitev izključne pravice prvotnega proizvajalca.

3. Kršitev pravic s 3D-tiskanjem in distribucijo predmetov

3.1. Avtorska pravica

Ena od materialnih pravic avtorja je pravica reproduciranja avtorskega dela, to je izključna pravica, da se delo fiksira na materialnem nosilcu ali drugem primerku, in sicer neposredno ali posredno, začasno ali trajno, delno ali v celoti ter s kakršnimkoli sredstvom ali v katerikoli obliki (23. člen ZASP). Reproduciranje je namenoma opredeljeno zelo široko, tako da zajema najrazličnejše možne postopke reproduciranja v telesni obliki, ne glede na njihovo obliko in način. Ni pomembno, ali je kopija izdelana na podlagi izvirnika ali primerka dela, če je izdelana v enakem, povečanem ali zmanjšanem merilu.[48] Med primeri reproduciranja zakon izrecno navaja tudi tridimenzionalno razmnoževanje, zato ne more biti dvoma, da nedovoljeno reproduciranje avtorskega dela z uporabo 3D-tiskanja krši

[46] Točka f prvega odstavka 43. člena ZIL-1, točka e prvega odstavka 3. člena Direktive 2008/95/ES, točka e prvega odstavka 7. člena Uredbe 207/2009.

[47] Sodba Sodišča EU z dne 14. septembra 2010 v zadevi C-48/09 P *Lego Juris A/S proti UUNT.*

[48] Trampuž, Oman, Zupančič, str. 93, Schack, str. 199

avtorjeva materialna upravičenja. Za kršitev avtorske pravice je potrebno dejansko kopiranje izvirnika, na primer z uporabo 3D-skenerja in tiskanjem skeniranega izdelka, saj neodvisna stvaritev enakega dela ne krši avtorske pravice. Vendar pa ni nujno, da je kopiranje identično – zadošča posnemanje bistvenih potez dela, pri čemer gre navadno poleg reprodukcije še za predelavo dela.[49] Zato gre za poseg v avtorsko pravico tudi, če model CAD, ki je podlaga za 3D-tiskanje, ni bil ustvarjen s 3D-skeniranjem obstoječega avtorskega dela, ampak je bil v celoti izdelan na računalniku na podlagi ogledovanja in ročnih meritev obstoječega dela, tako da se je ustvarila njegova bolj ali manj zvesta kopija. Če se s 3D-tiskanjem ustvarjene reprodukcije avtorskega dela brez soglasja imetnika avtorske pravice dajo v promet s prodajo ali drugačno obliko prenosa lastninske pravice ali se s tem namenom ponudijo javnosti, gre pri tem še za kršitev materialne pravice distribuiranja iz 24. člena ZASP. Imetnik 3D-tiskalnika, ki bi z njim serijsko izdeloval in dajal v promet reprodukcije avtorsko varovanih predmetov, bi torej nedvomno kršil avtorsko pravico na teh predmetih.

Nekoliko drugačen je položaj pri osebi, ki s 3D-tiskanjem reproducira avtorsko delo samo za lastne potrebe in tako izdelanih primerkov dela ne daje v promet. V takšnem primeru gre namreč za prosto privatno oziroma lastno reproduciranje, ki ga dopušča 50. člen ZASP. Četrti odstavek 50. člena sicer določa nekatere izjeme od prostega reproduciranja, vendar se nobena ne nanaša na tridimenzionalne predmete, kakršne bi bilo mogoče reproducirati z domačim 3D-tiskalnikom,[50] zato je tovrstno privatno reproduciranje dovoljeno, če so zanj izpolnjeni vsi pogoji. Fizična oseba lahko delo prosto reproducira v največ treh primerkih, če to stori za privatno uporabo, če primerki niso izročeni ali priobčeni v javnosti in če pri tem nima namena dosegati neposredne ali posredne gospodarske koristi. Izraz javnost v skladu z 2. členom ZASP pomeni večje število oseb zunaj običajnega kroga družine ali kroga osebnih znancev. Fizična oseba torej lahko v okviru privatne rabe izdela največ tri primerke dela in jih bodisi uporablja sama bodisi podari sorodnikom ali znancem.[51] Pri tem ni pomembno, kdo tehnično opravi 3D-tiskanje: to lahko opravi fizična oseba sama na svojem 3D-tiskalniku ali pa naroči 3D-tiskanje pri komercialnem ponudniku, kot je na primer že omenjeni Shapeways.[52] Položaj je podoben, kot če v fotokopirnici za študijske potrebe naročimo kopiranje nekaj strani iz knjige, pri čemer pa ponud-

[49] Primerjaj Smith, str. 25.

[50] Izključeno je privatno reproduciranje v obliki izvedbe arhitekturnega objekta. Ta tridimenzionalni predmet bo v prihodnosti najbrž celo mogoče izdelati z uporabo posebnih industrijskih 3D-tiskalnikov, vendar pri tem ne bo šlo za ravno običajen primer domače rabe 3D-tiskanja.

[51] Primerjaj Trampuž, Oman, Zupančič, str. 20.

[52] Primerjaj glede privatnega reproduciranja v fotokopirnici Trampuž, Oman, Zupančič, str. 154.

niku 3D-tiskanja niti ni treba predložiti originalnega dela, ampak zadošča že njegov digitalni model CAD.

Za pravne osebe je prosto lastno reproduciranje bolj omejeno. Zakon ga dopušča samo javnim arhivom, javnim knjižnicam, muzejem ter izobraževalnim in znanstvenim ustanovam, ne pa na primer tudi gospodarskim družbam. Navedene osebe lahko za lastne potrebe prosto reproducirajo delo v največ treh primerkih, če za to uporabijo lastni primerek in če pri tem nimajo namena dosegati neposredne ali posredne gospodarske koristi. Omejitev na reproduciranje iz lastnega primerka pomeni, da ni mogoče lastno reproduciranje tridimenzionalnega avtorskega dela na podlagi načrta CAD, ki je bil pridobljen z interneta, če pravna oseba sama še ne razpolaga s primerkom takšnega dela.

Izjema za dovoljeno privatno reproduciranje fizičnim osebam zagotavlja, da bo 3D-tiskanje avtorskih del za domače potrebe skoraj vedno zakonito. Zakonodajalec v času sprejemanja ZASP tovrstnega razmnoževanja najbrž ni imel v mislih, saj so bile tedanje domače reprodukcijske tehnologije omejene predvsem na fotokopiranje ter na presnemavanje glasbenih in video posnetkov, tridimenzionalna dela pa so se lahko reproducirala predvsem z ročnim delom oziroma obrtnimi tehnikami in torej v zelo omejenem obsegu. Z razvojem 3D-tiskanja in 3D-skeniranja se bo tudi privatno reproduciranje tridimenzionalnih del bistveno razširilo in tako precej bolj poseglo v interese avtorjev, zlasti ker je tudi količinsko omejitev na izdelavo največ treh primerkov dela v zasebnem krogu tako rekoč nemogoče nadzorovati.[53] Izključitev tridimenzionalnega razmnoževanja iz prostega reproduciranja zaradi nemožnosti učinkovitega nadzora ne bi imela smisla, je pa mogoče pričakovati razmišljanje o širitvi plačevanja nadomestila za privatno reproduciranje iz 37. člena ZASP tudi na naprave za 3D-skeniranje in tiskanje, tako da bi se s pavšalnimi plačili delno pokril poseg v gospodarski interes avtorjev tridimenzionalnih del. Zakonsko podlago za to bi lahko iskali v določbi 37. člena ZASP, ki s fotokopiranjem izenačuje druge podobne tehnike reproduciranja, pod kar bi bilo najbrž mogoče subsumirati tudi 3D-tiskanje (odvisno sicer od tega, kako široko razlagamo pojem podobnosti). Vendar menim, da zgolj obstoj tehnične možnosti privatnega reproduciranja tridimenzionalnih avtorskih del še ne bi smel biti zadosten razlog za takojšnjo širitev plačevanja nadomestila na nove naprave (ki bi jih s tem podražili in tako upočasnili uveljavitev nove tehnologije). Najprej bi bilo treba z empirično študijo ugotoviti, ali tovrstno reproduciranje res bistveno posega v gospodarske interese avtorjev tridimenzionalnih del, na primer tako, da v daljšem obdobju zmanjšuje njihovo prodajo in da zato padajo tudi prihodki avtorjev, na primer industrijskih oblikovalcev.

[53] Primerjaj Trampuž, Oman, Zupančič, str. 153.

3.2. Patent

Če je predmet patenta proizvod, zagotavlja patent imetniku izključno pravico preprečiti tretjim osebam, da brez njegove privolitve izdelujejo, uporabljajo, ponujajo v prodajo, prodajajo ali v te namene uvažajo zadevni proizvod. Obseg patentnega varstva je določen z vsebino patentnih zahtevkov, za razlago patentnih zahtevkov pa se uporabljajo tudi opis in skice (18. člen ZIL-1). Za kršitev patenta torej zadošča že izdelovanje patentiranega izuma s 3D-tiskanjem, ne glede na njegovo nadaljnjo uporabo, prodajo, ponujanje v prodajo itd.[54] Do kršitve patenta pride tudi v primeru, da ni bil kopiran obstoječi patentirani izdelek, ampak je avtor načrta CAD neodvisno razvil enako tehnično rešitev in jo uporabil v svojem načrtu, ne da bi se zavedal obstoja patenta. Drugače kot avtorsko pravo patentni sistem ne pozna izjeme za neodvisni razvoj.[55]

Vendar ima patentna zaščita nekaj pomembnih vsebinskih omejitev. Za kršitev patenta gre samo, če je s 3D-tiskanjem izdelan celoten zaščiteni izum. Nov izum pa je pogosto sestavljen iz različnih sestavnih delov, ki niso novi, ampak gre za starejše tehnične rešitve, ki so v izumu sestavljene na nov način. Kopiranje nepatentiranih delov patentiranega izuma zato še ni kršitev patenta na celotnem izumu. Dopustna je izdelava nadomestnih delov za patentirano napravo, pri čemer pa se lahko reproducirajo samo posamezni deli patentiranega predmeta, ne pa tudi predmet kot celota. Meja med popravilom in reprodukcijo izdelka je v praksi pogosto nejasna in njena določitev bo v dobi 3D-tiskanja najbrž povzročala precej težav.[56]

Za domačo rabo 3D-tiskanja bo odločilna določba 19. člena ZIL-1, po kateri se pravice iz patenta ne nanašajo na dejanja, storjena zasebno in za negospodarske namene ter na raziskave in poskuse vseh vrst, ki se nanašajo na predmet patenta, ne glede na njihov končni namen. Podobno kot smo ugotovili že za avtorsko pravo, tudi v patentnem pravu velja, da zasebno reproduciranje varovanih predmetov s 3D-tiskanjem ni kršitev patenta, če se ne uporablja za gospodarske namene. Prav tako ne gre za kršitev, če je 3D-tiskanje namenjeno raziskavam in poskusom v zvezi s predmetom patenta, ne glede na njihov končni namen (na kar se lahko sklicuje tudi gospodarska družba). Takšni izjemi sta sicer v evropskih pravnih redih običajni in so ju vsebovali tudi vsi dosedanji poskusi poenotenja materialnega patentnega prava v EU.[57] Patentno pravo ZDA pa ne

[54] Brean, str. 788.

[55] Weinberg, str. 5.

[56] Weinberg, str. 8. Podrobneje o razmejevanju med popravilom in rekonstrukcijo v ameriški sodni praksi glej Wilbanks, str. 1158–1165.

[57] Kur, Dreier, str. 118–119.

pozna izjeme za domačo ali osebno rabo in zato tudi vsako zasebno izdelavo patentiranega predmeta obravnava kot kršitev patenta, kar bo precej zožilo krog pravno dopustnega domačega 3D-tiskanja tehničnih izdelkov v ZDA (četudi je izvajanje učinkovitega nadzora nad takšno dejavnostjo v praksi neizvedljivo).[58]

ZIL-1 ne definira pojmov zasebna raba in negospodarski namen, pa tudi pravna teorija ju ne obravnava tako podrobno, kot so obravnavani pogoji za prosto zasebno rabo na področju avtorskega prava. Enako lahko štejemo, da je krog oseb, ki še spadajo v zasebno rabo, omejen na krog ožjih sorodnikov in znancev. Bolj problematično je vprašanje, ali je mogoča tudi analogija s fotokopirnico: ali ponudnik, ki stranki po njenem naročilu in za njeno zasebno rabo proti plačilu natisne tridimenzionalno kopijo patentiranega izdelka, še spada v okvir zasebne negospodarske rabe ali pa gre pri tem že za kršitev patenta? Na podlagi besedila 19. člena ZIL-1, ki se glede samih pogojev proste rabe bistveno ne razlikuje od 50. člena ZASP, bi bilo mogoče argumentirati, da mora biti položaj enak kot na področju avtorskega prava. Vendar se zdi verjetneje, da bodo sodišča na področju industrijske lastnine glede tega vprašanja zavzela restriktivnejšo razlago in štela, da ponudnik 3D-tiskanja, ki po naročilu tiska patentirane izdelke, ni samo pomočnik pri izvrševanju proste rabe v okviru 19. člena ZIL-1, ampak tudi sam gospodarsko izkorišča izum z izdelovanjem in prodajo patentiranih izdelkov.[59] Zakon namreč očitno ni predvideval, da bi v okviru pogojev iz 19. člena ZIL-1 lahko prihajalo do množične proizvodnje patentiranih izdelkov, medtem ko je ZASP za fotokopiranje uvedel celo posebno nadomestilo avtorjem. ZIL-1 tudi ne določa števila dopustnih kopij, zasebne rabe ne omejuje na fizične osebe in ne določa izjem od proste uporabe. Če bi lahko vsakdo, ki bi želel dobiti patentirani izdelek, preprosto naročil njegovo izdelavo pri ponudniku 3D-tiskanja, ne glede na patent, bi to lahko povsem razvrednotilo gospodarski namen patenta. Komercialni spletni ponudniki 3D-tiskanja, kot na primer Shapeways, se torej glede patentiranih predmetov najbrž ne morejo zanašati, da je njihova dejavnost na podlagi 19. člena ZIL-1 izvzeta iz dosega patentne zaščite. To še zlasti velja za primere, ko ponudnik na spletni strani sam objavlja modele CAD patentiranih izdelkov in strankam ponuja njihovo 3D-tiskanje, saj že ponujanje patentiranega izdelka v prodajo lahko krši pravice iz patenta.

[58] Weinberg, str. 8, Wilbanks, str. 1155–1156, Brean, str. 789. Pravilo o *fair use* velja samo na področju avtorskega prava. O potrebi po njegovi širitvi tudi na patente razpravlja Maureen A. O'Rourke, Towards a Doctrine of Fair Use in Patent Law. *Columbia Law Review,* let. 100 (2000), št. 5, str. 1177–1250.

[59] Primerjaj Osterrieth, robna št. 278, ki zagovarja ozko razlago pojma zasebne uporabe.

3.3. Model

Imetnik modela ima izključno pravico, da zaščiteni videz izdelka uporablja in tretjim osebam, ki nimajo njegovega soglasja, prepreči, da ga uporabljajo. Omenjena uporaba obsega zlasti izdelovanje, ponujanje, dajanje na trg, uvažanje, izvažanje ali uporabljanje izdelka, na katerega se videz nanaša, ali skladiščenje takega izdelka v te namene (37. člen ZIL-1). Pravice iz modela Skupnosti so na skoraj identičen način opredeljene v 19. členu Uredbe 6/2002. Pri neregistriranem modelu Skupnosti gre za kršitev samo pri dejanskem kopiranju zaščitenega videza, medtem ko gre pri registriranem modelu za kršitev tudi, če je podoben videz izdelka razvit neodvisno.[60] 3D-tiskanje in nadaljnja uporaba izdelkov, katerih videz je zavarovan z modelom, torej lahko krši pravice iz modela. Varstvo z modelom je celo nekoliko strožje kot pri avtorski pravici in patentu: obseg varstva vključuje vsak videz izdelka, ki pri seznanjenem uporabniku ne ustvari drugačnega celotnega vtisa. Zato gre za kršitev modela tudi, če se zaščiteni videz v načrtu CAD deloma modificira, tako da ni identičen zaščitenemu videzu. Prav tako gre za kršitev, če je videz izdelka razvit brez kopiranja, vendar z zgledovanjem po zaščitenem videzu, tako da ustvari enak celotni vtis kot zaščiteni videz. Vendar pa gre za kršitev modela lahko samo, če je kopirana zunanja oblika izdelka, medtem ko je reproduciranje notranje zgradbe izdelka dopustno, če se bistveno spremeni zunanji videz izdelka, kot bo redno viden končnemu uporabniku.

Za pravice iz modela je v ZIL-1 in v Uredbi 6/2002 določena enaka izjema od pravne zaščite za zasebno negospodarsko rabo ter za raziskave in poskuse, kot velja za patente. Zasebno nekomercialno 3D-tiskanje izdelkov, zaščitenih z modelom, ali njihovo reproduciranje za raziskave in poskuse torej ni kršitev modela.[61] Glede kroga oseb, ki še spadajo v pojem zasebne rabe, veljajo enake ugotovitve kot pri patentni zaščiti. Ponudnik 3D-tiskanja, ki bi odplačno po naročilu reproduciral z modelom zaščitene izdelke, se najbrž ne bi mogel uspešno sklicevati na to, da gre za dopustno zasebno rabo naročnika tiskanja.

3.4. Znamka

Imetnik znamke je upravičen preprečiti tretjim osebam, da brez njegovega soglasja v gospodarskem prometu uporabljajo znamki enak znak za enako blago ali storitve, ki so obseženi z znamko, ter enak ali podoben znak za enako ali podobno blago, če obstaja verjetnost zmede v javnosti zaradi povezovanja med znakom in znamko. Imetnik ugledne znamke lahko prepove uporabo enakega ali podobnega znaka tudi za blago ali storitve, ki niso podobni tistim, ki so obse-

[60] Smith, str. 26.

[61] Austin, Grewal, Caddy, str. 24.

ženi z znamko, če bi uporaba takega znaka brez upravičenega razloga izkoristila ali oškodovala naravo ali ugled znamke. V primerih, ko je z znamko zaščitena oblika izdelka samega oziroma njegove embalaže (tridimenzionalna znamka), gre torej pri 3D-tiskanju tovrstnega blaga oziroma njegove embalaže lahko za kršitev znamke, zlasti je blago enako ali podobno, kot je zaščiteno z znamko, v primeru slovečih znamk pa celo ne glede na vrsto blaga. Glede na to, da so merila za podeljevanje tridimenzionalnih znamk precej omejujoča, pa bo pogostejši položaj, ko je s 3D-tiskanjem kršena klasična znamka v obliki dvodimenzionalnega znaka oziroma napisa na izdelku, če je skupaj z izdelkom reproduciran tudi ta znak. Čeprav znamka ne vpliva na funkcionalnost izdelka, njegova tržna vrednost pogosto izvira prav iz ugleda znamke, zlasti pri različnih modnih izdelkih pa je grafični znak oziroma logotip proizvajalca pogosto neločljivo vključen v videz izdelka (na primer športni copati, ženske torbice, sončna očala), zato si lahko predstavljamo jasen motiv za reproduciranje tovrstnih grafičnih znakov na 3D-tiskanih izdelkih. Zakon sicer dovoljuje prosto uporabo znamke za označitev namena proizvoda ali storitve, zlasti za dodatke ali nadomestne dele, vendar pa ta izjema ne zajema opremljanja »glavnega« izdelka ali njegove embalaže z znakom, tako kot to počne originalni proizvajalec, ampak samo uporabo znamke za informativne namene, ki ne dajejo vtisa o povezavi z imetnikom znamke.[62]

Z vidika tu obravnavanega vprašanja 3D-tiskanja je ključnega pomena ugotovitev, da so pravice iz znamke omejene samo na *uporabo v gospodarskem prometu*. To jasno določajo definicije znamke v 47. členu ZIL-1, 5. členu Direktive 2008/95/ES in 9. členu Uredbe 207/2009. Za kršitev znamke torej v nobenem primeru ne zadošča samo reproduciranje z znamko zavarovanega znaka oziroma oblike blaga, ampak je treba znamko še uporabiti v gospodarskem prometu. Sodišče EU je v zadevi *Arsenal proti Reedu* zapisalo, da gre za uporabo znaka, ki je enak znamki, v gospodarskem prometu, če je uporaba v okviru gospodarske dejavnosti, ki je namenjena pridobivanju gospodarskih koristi, ne pa v zasebni sferi.[63] Če se izdelki, katerih oblika ali oznake so zaščiteni z znamko, tridimenzionalno tiskajo za lastno zasebno rabo in uporabljajo doma, tega ni mogoče razlagati kot uporabe v gospodarskem prometu, zato ne gre za kršitev znamke.[64] Vprašanje je, kako je z nadaljnjo prodajo takšnih izdelkov. Pravni redi držav članic EU so zavzeli različna stališča do vprašanja, ali gre za kršitev znamke že v primeru, da posameznik na internetu prodaja posamezno zasebno repliko z znamko zavarovanega izdelka, ali

[62] Primerjaj Kur, Dreier, str. 222–223. Glej tudi sodbo in sklep Vrhovnega sodišča RS III Ips 30/2010 z dne 29. 3. 2011.

[63] Sodba Sodišča v EU zadevi C 206/01, *Arsenal Football Club plc proti Matthewu Reedu* z dne 12. novembra 2002, 40. odstavek. Glej tudi mnenje generalnega pravobranilca v isti zadevi, točki 63 in 64.

[64] Weinberg, str. 8.

pa je za kršitev potreben večji obseg uporabe znamke v gospodarski dejavnosti.[65] V slovenski sodni praksi še ni jasnega stališča do tega vprašanja. Komercialni ponudnik 3D-tiskanja, ki bi za stranke po naročilu tiskal posamezne izdelke, označene z znamko, pa bi s tem znamko uporabljal v okviru svoje gospodarske dejavnosti in izdelke dajal v promet, zato bi s tem gotovo kršil pravice iz znamke.

3.5. Ugotovitve glede kršitve pravic s 3D-tiskanjem

Ne glede na to, s katero vrsto pravic intelektualne lastnine je varovan tridimenzionalni predmet, ga lahko fizična oseba s 3D-tiskanjem reproducira za zasebno nekomercialno rabo, ne da bi s tem kršila katero od izključnih pravic.[66] Zasebna uporaba mora biti nekomercialne narave in omejena na lastnika 3D-tiskalnika in ožji krog njegovih sorodnikov in znancev. Za avtorska dela je dopustna izdelava največ treh zasebnih kopij.

Pravne osebe so pri 3D-reproduciranju varovanih predmetov za lastne potrebe nekoliko bolj omejene. Na določbe o prostem lastnem reproduciranju avtorskega dela se lahko sklicujejo samo nekatere izobraževalne in znanstvene ustanove, če same že razpolagajo z zakonitim primerkom tega dela. Pri izdelkih, zaščitenih s patentom ali modelom, se lahko tudi gospodarske družbe sklicujejo zlasti na izjemo za raziskave in poskuse, lahko pa seveda reproducirajo tiste dele proizvoda, ki jih varstvo z izključno pravico ne zajema. Pravice iz znamke pa preprečujejo zlasti dajanje blaga v gospodarski promet, zato lastne uporabe z znamko označenih proizvodov kaj dosti ne omejujejo.

Izjema, ki omogoča prosto reproduciranje pravno varovanih predmetov za lastno oziroma zasebno uporabo, je pomembna, ker vzpostavlja razmeroma jasen in širok krog zakonite rabe nove tehnologije, tudi kadar je ta posebej primerna za reproduciranje komercialnih izdelkov (na primer različne kombinacije 3D-skenerja in tiskalnika). Zaradi te možnosti je namreč izključena potencialna odškodninska odgovornost proizvajalcev potrošniških 3D-skenerjev in tiskalnikov, ki bi temeljila na očitku napeljevanja oziroma pomoči potrošnikom pri kršitvi izključnih pravic, saj proizvajalcu ni mogoče očitati, da je napravo proizvedel in prodal vedoč, da bo uporabljena predvsem za kršitev izključnih pravic intelektualne lastnine.[67]

Če 3D-tiskanje pravno varovanih predmetov preseže okvire dopustne zasebne uporabe in se izvaja odplačno, za tretje osebe, je odgovor odvisen od vrste pravnega varstva. Reproduciranje avtorsko varovanih del po naročilu je dopustno, če

[65] Kur, Dreier, str. 196–197.

[66] Primerjaj Smith, str. 26.

[67] Primerjaj Austin, Grewal, Caddy, str. 23, Kuehn, str. 28.

ostane v okviru naročnikove zasebne rabe. Z vidika ponudnika tiskanja to pomeni predvsem, da ne sme natisniti več kot treh primerkov dela, saj izpolnjevanja drugih pogojev za zasebno rabo pri naročniku v praksi ne more preveriti. Pri izdelkih, ki so varovani (tudi) s pravicami industrijske lastnine, se bo reproduciranje celotnih izdelkov za tretje osebe vedno štelo za gospodarsko dejavnost, ki krši izključne pravice v zvezi z izdelkom. Tudi na tem področju pa obstaja dopustno polje 3D-tiskanja zlasti v zvezi s proizvodnjo nadomestnih delov za obstoječe komercialne proizvode.

4. Zakonitost izdelave in razširjanja načrtov za 3D-tiskanje

4.1. Razlog za preganjanje internetnih posrednikov

Tehnična in pravna možnost, da ljudje doma skenirajo in tridimenzionalno tiskajo reprodukcije uveljavljenih komercialnih izdelkov, z vidika originalnih proizvajalcev teh izdelkov sama po sebi še ne zbuja velikih skrbi. Čeprav nova tehnologija reproduciranje poenostavi, izdelava digitalnih modelov za zdaj zahteva nekaj tehničnega znanja, predvsem pa mora potrošnik najprej imeti originalni izdelek, da ga lahko kopira. Reprodukcijski potencial domačega 3D-tiskanja pa bistveno okrepi, če lahko uporabniki že izdelane modele CAD za tiskanje različnih izdelkov preprosto poiščejo na internetu. V takšnem primeru potrošniku originalnega izdelka nikoli ni treba kupiti, da bi ga kopiral, ampak ga samo še natisne. Če domači tiskalnik omogoča izdelavo primerljivo kakovostnega izdelka po nižji ceni od maloprodajne cene originala, klasična proizvodnja postane odveč.

Že omenjeno spletno mesto Thingiverse uporabnikom omogoča nalaganje in deljenje modelov CAD za uporabo s tiskalniki MakerBot. Zloglasni Pirate Bay je digitalne načrte 3D-predmetov razglasil za naslednjo veliko kategorijo množičnega potrošniškega kopiranja in jo na svoji spletni strani poimenoval *physibles*: podatkovni objekti, ki jih je mogoče (zlasti s 3D-tiskanjem) pretvoriti v fizične.[68] Verjetno se bo s širitvijo domačega 3D-tiskanja pojavljalo vse več spletnih mest, namenjenih izmenjavi modelov CAD med uporabniki. Sodeč po izkušnjah s področja »piratiziranja« glasbe in filmov bo na spletu tako kmalu mogoče z lahkoto priti do digitalnih modelov vseh omembe vrednih komercialnih izdelkov. Takšen razvoj jasno posega v gospodarske interese proizvajalcev fizičnih izdelkov, saj bi se ob širitvi domačega 3D-tiskanja lahko znašli v položaju, ko sami nosijo stroške razvoja in oblikovanja novega izdelka, z njegovo prodajo pa ne morejo več ustvarjati pričakovanih prihodkov. Podobno kot razmah interneta, ki je z možnostjo enostavnega razmnoževanja in razširjanja digitalnih del ogrozil

[68] *Evolution: New Category.* The Pirate Bay, 23. januar, 2012, http://thepiratebay.se/blog/203.

tradicionalne poslovne modele glasbene in filmske industrije, bo tudi digitalna distribucija modelov CAD zastavila vprašanja, povezana z neavtoriziranim 3D-tiskanjem fizičnih izdelkov.[69]

Pri preganjanju »piratstva« na področju digitalne glasbe in filmov so imetniki pravic v praksi spoznali, da sprožanje sodnih postopkov zoper množico končnih uporabnikov, ki brez dovoljenja razmnožujejo in razširjajo avtorska dela, zaradi razpršenosti malih kršiteljev in neugodnega medijskega odmeva ne daje ustreznih rezultatov. Namesto tega so se osredotočili na pregon internetnih posrednikov, ki uporabnikom omogočajo preprosto izmenjavo datotek. Pri 3D-tiskanju, kot smo videli, za preganjanje domačih uporabnikov največkrat niti ni prave pravne podlage, saj zasebno nekomercialno reproduciranje varovanih tridimenzionalnih predmetov sploh ne krši pravic intelektualne lastnine. Zato bo proizvajalcem fizičnih izdelkov za zaščito njihovih gospodarskih interesov pred grožnjo 3D-tiskanja ostalo na voljo le vlaganje prepovednih in odškodninskih zahtevkov zoper upravljavce spletnih mest za izmenjavo digitalnih modelov CAD, češ da ta dejavnost omogoča in spodbuja kršitve njihovih pravic.[70]

V nadaljevanju so obravnavane možne pravne podlage za uveljavljanje tovrstnih zahtevkov. Za vsako od relevantnih pravic je preučeno, ali bi lahko do njene kršitve prišlo še pred 3D-tiskanjem, in sicer s samim 3D-skeniranjem varovanega predmeta in dajanjem na voljo javnosti tako ustvarjenega digitalnega modela CAD. Jasno je, da pri slednjem sklicevanje na zasebno uporabo ne pride v poštev. Posebej je obravnavano vprašanje potencialne odgovornosti zaradi spodbujanja h kršitvi izključnih pravic.

4.2. Avtorska pravica

Z vidika avtorske pravice je odločilno vprašanje, ali je izdelavo digitalnega modela CAD že mogoče šteti za reprodukcijo obstoječega tridimenzionalnega avtorskega dela. Če gre za reprodukcijo, potem je tudi za njeno digitalno razmnoževanje in razširjanje potrebno dovoljenje avtorja, sicer pa ne. Kot je bilo že pojasnjeno, je pojem reproduciranja po ZASP širok. Tudi če je kopija drugačne velikosti, dimenzije ali materiala od izvirnika, gre za reproduciranje, lahko v kombinaciji s predelavo avtorskega dela. Tridimenzionalno delo se lahko razmnoži tudi dvodimenzionalno (na primer s fotografiranjem) in obratno. V vsakem primeru mora biti tudi reprodukcija izražena oziroma zapisana na tak način, da jo

[69] Weinberg, str. 5, Brean, str. 781.

[70] Weinberg, str. 12.

je mogoče zaznati s človeškimi čuti, četudi s pomočjo tehničnih sredstev. Oblika reproduciranja je zato tudi shranitev v elektronski obliki.[71]

Model CAD je digitalni zapis oblike tridimenzionalnega predmeta. Datoteka je čisti podatkovni predmet in sama ni niti dvo- niti tridimenzionalna, vendar lahko računalnik z ustreznim programom na podlagi datoteke CAD na zaslonu izriše sliko tridimenzionalnega predmeta (avtorskega dela) s kateregakoli zornega kota. Izpolnjen je torej pogoj zaznavnosti dela s človeškimi čuti, četudi je primarni namen digitalnega modela CAD le podajanje informacij 3D-tiskalniku. Vloga modela CAD pri 3D-tiskanju je podobna vlogi arhitekturnega načrta pri gradnji arhitekturnega objekta: model CAD je načrt za tiskanje tridimenzionalnega predmeta.[72] Izvedba arhitekturnega dela z gradnjo objekta se šteje za reprodukcijo načrta arhitekturnega dela (drugi odstavek 23. člena ZASP).[73] Po tej analogiji je treba tudi 3D-tiskanje na podlagi originalnega avtorskega modela CAD kvalificirati kot razmnoževanje tega avtorskega dela. Ista ugotovitev mora veljati, če postopek poteka v nasprotni smeri, torej če s skeniranjem primerka avtorskega dela ustvarimo model CAD: gre za digitalno reprodukcijo tridimenzionalnega avtorskega dela, za kar je načeloma potrebno avtorjevo dovoljenje.[74]

Fizične osebe se lahko seveda tudi v zvezi s 3D-skeniranjem sklicujejo na izjemo za prosto zasebno reproduciranje, javni arhivi, knjižnice, muzeji ter izobraževalne in znanstvene ustanove pa na prosto lastno reproduciranje v skladu s 50. členom ZASP. Gospodarskim družbam 3D-skeniranje avtorskih del potemtakem ni dovoljeno. Seveda pa skeniranje zgolj za lastne potrebe navzven tako rekoč ni zaznavno in nima večjega gospodarskega pomena. Kot smo videli, ima večje gospodarske posledice objava s skeniranjem ustvarjenih modelov CAD na internetu, tako da so dostopni neomejenemu krogu tretjih oseb – uporabnikov 3D-tiskanja. S tem je presežena meja proste zasebne ali lastne rabe. Če je model CAD reprodukcija tridimenzionalnega avtorskega dela, gre pri tem za poseg v avtorjeve materialne pravice, in sicer v pravico dajanja na voljo javnosti, ki jo 32.a člen ZASP definira kot izključno pravico, da se po žici ali brezžično delo naredi dostopno javnosti na način, ki omogoča posameznikom dostop do njega s kraja in v času, ki ju sami izberejo, ali da se delo pošlje posamezniku na podlagi ponudbe, ki je namenjena javnosti.

Javna dostopnost modela CAD avtorsko varovanega dela na spletni strani torej že sama krši avtorsko pravico. Za kršitev v prvi vrsti odgovarja uporabnik spletišča, ki je sporno datoteko dal na voljo javnosti. Od upravljavca spletnega

[71] Trampuž, Oman, Zupančič, str. 94, Schack, str. 199.

[72] Rideout, str. 168.

[73] Schack, str. 199.

[74] Austin, Grewal, Caddy, str. 24.

mesta pa lahko avtor (oziroma imetnik avtorske pravice) upravičeno zahteva, naj prepreči dostop do modela CAD, s katerim je digitalno reproducirano njegovo avtorsko delo in hkrati omogočeno njegovo nadaljnje reproduciranje s 3D-tiskanjem. Odškodninski odgovornosti se lahko upravljavec spletnega mesta izogne s sklicevanjem na 11. člen Zakona o elektronskem poslovanju na trgu (ZEPT),[75] po katerem (v skladu z Direktivo 2000/31/ES[76]) ponudnik storitev informacijske družbe ni odgovoren za podatke, shranjene na zahtevo prejemnika storitve, ki ne deluje v okviru njegovih pooblastil ali pod njegovim nadzorom, pod pogojem, da ponudnik storitev:

- ne ve za protipravno dejavnost ali podatek in mu v zvezi z odškodninsko odgovornostjo niso znana dejstva ali okoliščine, iz katerih izhaja protipravnost, ali
- nemudoma, ko mu je protipravnost znana, ukrepa tako, da podatke odstrani ali onemogoči dostop do njih (t. i. sistem *notice and takedown*).

Glede na to, da večina tridimenzionalnih predmetov ni avtorskopravno varovanih, bo upravljavec spletišča navadno lahko izkazal, da za kršitev avtorske pravice ni vedel.[77] Bistveno za izognitev odgovornosti bo torej, da bo na zahtevo imetnika avtorske pravice s spletne strani odstranil sporen model CAD. Breme nadzora nad kršitvami avtorske pravice tako nosi imetnik pravice. Prvič je bila tovrstna zahteva vložena leta 2011, ko je Ulrich Schwanitz od spletne strani Thingiverse zahteval odstranitev virtualnega modela, ki ga je izdelal eden od uporabnikov in z njim kopiral Schwanitzevo delo. Datoteka je bila umaknjena prostovoljno, zato ni prišlo do sodnega postopka, v katerem bi bil položaj natančneje pravno kvalificiran.[78]

4.3. Patent

Izključne pravice iz patenta obsegajo izdelavo, uporabo, ponujanje v prodajo, prodajanje in uvoz patentiranega proizvoda. Digitalnega 3D-skeniranja patentiranega izdelka ni mogoče kvalificirati kot eno od navedenih ravnanj, saj je rezultat skeniranja le datoteka CAD, torej le virtualni model patentiranega proizvoda, ne pa tudi tak proizvod sam. Prav tako datoteka CAD ni komponenta patentiranega

[75] Uradni list RS, št. 96/2009 – uradno prečiščeno besedilo.

[76] Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju).

[77] Lahko si sicer zamislimo drugačen položaj, na primer če bi šlo za spletno stran, specializirano za objavo modelov CAD sodobnih umetniških del.

[78] Rideout, str. 162, 165–166. Glej še http://arstechnica.com/tech-policy/2011/04/the-next-napster-copyright-questions-as-3d-printing-comes-of-age (23. 12. 2013).

izuma.[79] Do kršitve patenta lahko pride šele, če je patentirani proizvod tudi fizično izdelan s 3D-tiskanjem na podlagi takega modela CAD, medtem ko izdelava, razširjanje ali celo prodaja samih datotek digitalnega modela CAD niso zajeti s pravicami iz patenta.[80] Za kršitev patenta na proizvodu bi šlo, če bi imetnik 3D-tiskalnika javno ponujal, da na spletni strani predstavljeni model CAD po naročilu stranke natisne in ji ga dobavi. Vendar bi v takšnem primeru kršitev ne izhajala iz same izdelave ali razširjanja virtualnega modela proizvoda, ampak iz dejanja ponujanja v prodajo, ki je zajeto s pravicami iz patenta.

4.4. Model

Uporaba modela obsega zlasti izdelovanje, ponujanje, dajanje na trg, uvažanje, izvažanje ali uporabljanje izdelka, na katerega se videz nanaša, ali skladiščenje takega izdelka v te namene (prvi odstavek 37. člena ZIL-1). Ključen je torej pojem izdelka, ki je definiran v 33. členu ZIL-1 in 3. členu Uredbe 6/2002 kot industrijski ali obrtni izdelek, ki med drugim vključuje dele, namenjene za sestavo kompleksnega izdelka, embalažo, opremo, grafične simbole in tipografske znake, razen računalniških programov. Podatki v elektronski obliki ne tvorijo izdelka,[81] zato kakršnokoli ravnanje s samo datoteko CAD ne more kršiti pravic iz modela.

4.5. Znamka

Imetnik znamke ima izključno pravico do uporabe znamke v gospodarskem prometu za označevanje blaga oziroma storitev. Ta pravica med drugim obsega prepoved opremljanja blaga ali embalaže z znakom; ponujanja blaga, označenega s tem znakom, njegovega dajanja na trg ali skladiščenja v te namene oziroma ponujanja ali oskrbovanja s storitvami pod tem znakom; uvoza ali izvoza blaga pod tem znakom; uporabe znaka na poslovni dokumentaciji in v oglaševanju. Pri uporabi znamke more biti torej prisotna neka jasna povezava z blagom oziroma storitvami. Poudarek varstva je namreč na uporabi znamke za proizvode ali storitve, ne pa na sami uporabi znaka, ki tvori znamko.[82] Če je oblika blaga varovana s tridimenzionalno znamko (kar je redko) ali če je na blagu odtisnjena dvodimenzionalna znamka, virtualni načrt takšnega proizvoda – četudi vključuje znamko – vendarle še ni tudi blago samo, dokler ni tridimenzionalno natisnjen. Izdelovanje modelov CAD s 3D-skeniranjem fizičnih proizvodov in internetno razširjanje tovrstnih datotek zato ne more kršiti znamke. Če so digitalni modeli

[79] Brean, str. 796.

[80] Weinberg, str. 12, Brean, str. 790–793, 803.

[81] Eichmann/von Falckenstein, §1, robna št. 22.

[82] Austin, Grewal, Caddy, str. 24.

CAD na voljo brezplačno, pa tudi ne moremo govoriti o uporabi v gospodarskem prometu, kar je prav tako eden od nujnih elementov kršitve znamke.

4.6. Odgovornost zaradi spodbujanja kršitve pravic

Kot smo videli, internetno razširjanje (dajanje na voljo javnosti) modelov CAD lahko krši avtorsko pravico, če se virtualni model nanaša na avtorsko delo. Pri kršitvah pravic industrijske lastnine (patent, model, znamka) pa je položaj drugačen: do kršitve pravic lahko pride šele, če se predmet tudi fizično izdela, medtem ko samo razširjanje modela CAD na internetu ni protipravno. V takšnem položaju na prvi pogled ne more biti izpolnjen pogoj za odgovornost ponudnika storitev informacijske družbe iz 11. člena ZEPT, tj. protipravnost podatka ali dejavnosti uporabnika. Ker dostopnost načrtov CAD na internetu znatno olajša 3D-tiskanje obstoječih proizvodov, pa se zastavlja vprašanje, ali bi lahko upravljavcu spletišča za izmenjavo datotek očitali zavestno spodbujanje h kršitvi pravic, s čimer bi presegel tehnično nevtralno vlogo internetnega posrednika. Bi bil upravljavec spletne strani, ki omogoča izmenjavo datotek CAD med uporabniki, lahko odškodninsko odgovoren kot napeljevalec ali pomagač pri kršitvi pravic industrijske lastnine, če je vedel, da so med dostopnimi datotekami tudi načrti proizvodov, zaščitenih s patentom, modelom ali znamko?[83]

Obligacijski zakonik (OZ)[84] v drugem odstavku 186. člena določa, da napeljevalec in pomagač ter tisti, ki je pomagal, da se odgovorne osebe ne bi odkrile, odgovarjajo solidarno z njimi. Sodna praksa potrjuje, da v gospodarskem prometu v izključno pravico industrijske lastnine ne poseže samo tisti, ki neposredno krši imetnikovo pravico (storilec), temveč tudi tisti, ki pri tem sodeluje, mu pomaga ali ga napeljuje na kršitev.[85] Civilno pravo se sicer pri opredeljevanju udeležbe več oseb pri sopovzročitvi škode opira na pojmovno bolj izdelane kazenskopravne nauke.[86] Če za kršitev pravic industrijske lastnine smiselno uporabimo opredelitvi napeljevanja in pomoči iz 37. in 38. člena Kazenskega zakonika (KZ-1),[87] ugotovimo, da sta predpostavi kateregakoli zahtevka zoper napeljevalca ali pomagača:

- da je zaradi napeljevanja oziroma pomoči že prišlo do kršitve izključnih pravic (možnost ali verjetnost kršitve ne zadošča)[88] in

[83] Austin, Grewal, Caddy, str. 24.

[84] Uradni list RS, št. 83/2001, 32/2004, 28/2006 Odl. US: U-I-300/04-25, 29/2007 Odl. US: U-I-267/06-41, 40/2007, 97/2007 – UPB1, 30/2010 Odl. US: U-I-207/08-10, Up-2168/08-12.

[85] Sklep Vrhovnega sodišča RS III Ips 90/2004 z dne 26. 1. 2005, točka 3.3.

[86] Sodba Vrhovnega sodišča RS III Ips 82/2007 z dne 27. 10. 2009, točka 9.

[87] Uradni list RS, št. 50/2012 – uradno prečiščeno besedilo.

[88] Kršitev pravic je relevantna le kot objektivno dejstvo, ne glede na krivdo neposrednega povzročitelja. Glej sklep Vrhovnega sodišča RS III Ips 90/2004 z dne 26. 1. 2005, točka 2.2.

- da je napeljevalec oziroma pomagač ravnal naklepno (napeljevanje ali pomoč iz malomarnosti nista mogoča).

Obstoj obeh predpostavk mora dokazati tožnik. Dokazati, da je do dejanske kršitve pravice industrijske lastnine že prišlo, je mnogo težje kot pri kršitvah avtorske pravice. Dokaza ni mogoče pridobiti na daljavo, s sledenjem podatkovnemu prometu prek določenega spletnega mesta, saj sama digitalna reprodukcija in prenos modela CAD še ne kršita patenta, modela ali znamke. Prav tako za kršitev ne zadošča že dokaz, da je oseba, ki je s toženčeve spletne strani snela model CAD varovanega predmeta, ta predmet reproducirala s 3D-tiskanjem, ampak bi moral tožnik dokazati še, da je bil v konkretnem primeru s 3D-tiskanjem presežen okvir zasebne nekomercialne rabe oziroma raziskav in poskusov.[89] Tipično bo torej mogoče neposredno kršitev pravic dokazati le v primerih, ko uporabnik spornega modela CAD javno ponuja v prodajo proizvode, ki so tridimenzionalno natisnjeni na podlagi tega modela. V takšnem položaju je neposredni kršitelj že identificiran, zato bo imetnik pravic tožbo najbrž primarno naperil zoper njega. Mogoče pa je, da bi se zaradi generalno preventivnih razlogov vendarle odločil še za tožbo zoper izdelovalca modela CAD in internetnega posrednika, ki je neposrednemu kršitelju omogočil dostop do modela CAD. Pri dokazovanju obstoja neposredne kršitve bi tu prišla v poštev določba tretjega odstavka 121. člena ZIL-1, po kateri se v postopku proti osebi, katere storitve so bile uporabljene za kršitev pravice, obstoj te kršitve pa je že pravnomočno ugotovljen v postopku proti tretjemu, domneva, da je kršitev podana.[90]

Še na več težav bi tožnik naletel pri dokazovanju, da je imel upravljavec sporne spletne strani naklep, njene uporabnike napeljati na kršitev izključnih pravic ali jim pri tej kršitvi pomagati. Na podlagi pravila o obrnjenem dokaznem bremenu iz prvega odstavka 131. člena OZ se namreč domneva samo najmilejša stopnja krivde, torej navadna malomarnost, obstoj naklepa pa mora dokazati tožnik.[91] Pri tem ne zadošča dokaz o možnosti, da bo model CAD uporabljen za kršitev pravice, ampak je treba tudi dokazati, da se je napeljevalec ali pomagač zavedal, da zaradi njegovega ravnanja lahko pride do kršitve pravic industrijske lastnine, in je takšno kršitev bodisi hotel povzročiti bodisi vsaj privolil, da do nje pride (primerjaj 29. člen KZ-1). Odškodninsko bi torej odgovarjal razširjevalec modela CAD samo, če bi bilo razumni osebi očitno, da bo datoteka uporabljena za kršitev izključne pravice industrijske lastnine.[92] Tak položaj je redek. Večina tridimen-

[89] Primerjaj Weinberg, str. 12, Doherty, str. 361.

[90] Za avtorsko pravico vsebuje identično določbo tretji odstavek 167. člena ZASP.

[91] Sodba in sklep Vrhovnega sodišča RS II Ips 34/2009 z dne 18. 5. 2009, točka 10.

[92] Austin, Grewal, Caddy, str. 24. Tudi po ameriškem pravu velja, da gre za napeljevanje samo, kadar nekdo napelje drugega h kršitvenemu ravnanju in se pri tem zaveda, da ravnanje, h kateremu napeljuje, pomeni kršitev patenta. Glej Brean, str. 794, Doherty, str. 361.

zionalnih predmetov sploh ni zaščitenih s katero od pravic industrijske lastnine, in tudi kadar so zaščiteni, to navzven največkrat ni očitno. Poleg tega bi morale biti podane posebne okoliščine, zaradi katerih bi bilo očitno, da bodo obiskovalci spletne strani načrte CAD uporabljali na način, ki presega okvire dovoljenega. Glede na širok krog zakonitega domačega 3D-tiskanja pravno zaščitenih proizvodov (na primer za zasebno nekomercialno rabo in za raziskave in poskuse) takšna očitnost kršitve praviloma ne bo podana. Zgolj dejstvo, da domače 3D-tiskanje določenega proizvoda posega v gospodarske interese njegovega izvirnega proizvajalca, pa seveda še ne pomeni tudi protipravnosti takega ravnanja. Upravljavcu spletnega mesta za izmenjavo datotek CAD bo torej v praksi zelo težko dokazati zavedanje vseh elementov, ki so potrebni, da bi odškodninsko odgovarjal kot napeljevalec ali pomagač.

5. Posledice za sistem prava intelektualne lastnine

Tehnologija 3D-tiskanja bo omogočila domačo proizvodnjo tridimenzionalnih predmetov in izdelkov v mnogo večjem obsegu, kot si je to kdo predstavljal v času, ko so se oblikovala temeljna pravila sedanjega prava intelektualne lastnine. Za zasebno nekomercialno reproduciranje pravno varovanih tridimenzionalnih predmetov je določenih le malo omejitev, razširjanje virtualnih modelov varovanih predmetov pa zajame samo avtorska pravica. Najbrž je odsotnost strožje regulacije posledica tega, ker se ni pričakovalo, da bi lahko takšna dejavnost resneje posegala v gospodarske interese imetnikov pravic. Bo torej 3D-tiskanje s spreminjanjem ustaljenega gospodarskega razmerja med proizvajalci in potrošniki, na podlagi katerega je bil veljavni sistem zgrajen, povzročilo nov pretres za pravo intelektualne lastnine? Gotovo, vendar lahko napovemo, da bo ta pretres manj sunkovit od tistega, ki ga je povzročila digitalna revolucija v prejšnjem desetletju. Pri dobrinah, ki jih je mogoče pretvoriti v elektronsko obliko – glasbi, filmih, računalniških programih –, je namreč klasično distribucijo na fizičnih nosilcih v le nekaj letih nadomestilo internetno razširjanje, ki ga odlikujejo nični mejni stroški razmnoževanja in prenosa podatkov ter identičnost izvirnika in kopije. Pri 3D-tiskanju stroški vhodnih surovin ostajajo. Zaradi ekonomije obsega bo množična proizvodnja mnogih enostavnih predmetov najbrž vedno cenejša s klasičnimi proizvodnimi metodami kot pa s 3D-tiskanjem, poleg tega vsaj pri potrošniškem 3D-tiskanju kakovost kopije še ne dosega izvirnika. Zato tudi najbolj optimistični evangelisti poceni 3D-tiskanja priznavajo, da so domači gospodinjski 3D-tiskalniki v široki uporabi oddaljeni še leta, če ne desetletja.[93]

[93] Bradshaw, Bowyer, Haufe, str. 31.

Pravni sistem bo tako imel več časa za prilagoditev spremembam proizvodnih razmerij.

Veljavna pravna ureditev zagotavlja razmeroma jasen položaj osebam, ki se s 3D-tiskanjem ukvarjajo le za zasebno rabo, medtem ko komercialnim ponudnikom 3D-tiskanja ne zagotavlja popolne varnosti pred zahtevki imetnikov pravic, tem pa ne ponuja učinkovitega pravnega varstva. Meje pravne dopustnosti reproduciranja komercialnih izdelkov za namene, ki presegajo zasebno nekomercialno rabo, bo treba v prihodnje jasneje začrtati, vendar menim, da lahko to nalogo vsaj v začetni fazi zadovoljivo opravi sodna praksa. S prenagljenim reformiranjem zakonodaje bi lahko ponavljali napake s področja avtorskega prava, kjer so se nova pravila oblikovala na podlagi zmotnih predpostavk o nadaljnjem razvoju digitalnega razširjanja avtorskih del. Z ukrepi, kot je na primer pravno varstvo tehnoloških ukrepov za varstvo avtorske pravice (*digital rights management*), se je skušalo čim bolj omejiti potencial nove tehnologije, zato da bi z njim zaščitili stare proizvodne modele. Lahko pričakujemo, da bodo imetniki pravic, zlasti proizvajalci fizičnih proizvodov, kakršne je mogoče v celoti ali deloma reproducirati s 3D-tiskanjem, tudi na tem področju skušali prepričati zakonodajalca, naj zaostri pravila prava intelektualne lastnine na primer tako, da bi zožil obstoječe izjeme za zasebno rabo varovanih predmetov ali da bi razširil izključne pravice iz patenta, modela ali znamke, tako da bi zajemale tudi izdelavo in uporabo virtualnih modelov varovanih predmetov. Vendar vsaka takšna razširitev proizvajalčevega zakonskega monopola posega v lastninsko pravico uporabnikov takšnih izdelkov, na primer z omejitvijo možnosti popravila izdelka in izdelave nadomestnih delov. Za utemeljitev ustavnosti takšnega posega ne bi smelo zadostovati zgolj sklicevanje na dejstvo, da nova tehnologija ogroža obstoječe proizvodne in poslovne modele.

Kot poudarja Michael Weinberg, sposobnost reproduciranja tridimenzionalnih predmetov resda omogoča kršitev pravic intelektualne lastnine, vendar po drugi strani številnim posameznikom omogoča tudi ustvarjanje in inoviranje na podlagi obstoječega znanja. Podobno kot pri tiskarskem stroju, fotokopirni napravi, videorekorderjih in osebnih računalnikih bodo nekateri gledali na 3D-tiskanje predvsem kot na grožnjo, drugi pa ga bodo dojemali kot prebojno orodje za širitev znanja in ustvarjalnosti. Bistveno je, da tisti, ki se bojijo, ne ustavijo tistih, ki jih nova tehnologija navdihuje.[94]

[94] Weinberg, str. 4, primerjaj tudi Doherty, str. 371.

Literatura in viri

Austin, Helen, Grewal, Randeep, Caddy, Lorna: 3D Printing is Here to Stay. *Intellectual Property Magazine*, april 2013, str. 22–24.

Bradshaw, Simon, Bowyer, Adrian, Haufe, Patrick: The Intellectual Property Implications of Low-Cost 3D Printing. *SCRIPTed,* 2010, let. 7, št. 1, str. 5–31.

Brean, Daniel Harris: Asserting Patents to Combat Infringement via 3D Printing: It's No »Use«. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 2013, let. 23, št. 3, str. 771–814.

Doherty, Davis: Downloading Infringement: Patent Law as a Roadblock to the 3D Printing Revolution. *Harvard Journal of Law & Technology*, 2012, let. 26, št. 1, str. 353–373.

Dolžan, Judita: Zavrnitev zahteve za registracijo tridimenzionalnega znaka zaradi neobstoja razlikovalnega učinka. *Pravna praksa*, 2012, let. 31, št. 23, str. 24–25.

Eichmann, Helmut, Von Falckenstein, Roland Vogel: *Geschmacksmustergesetz, 4. Auflage*. München: Verlag C. H. Beck, 2010.

Jacobs, A. J.: Dinner is Printed. *The New York Times*, 21. 9. 2013. http://www.nytimes.com/2013/09/22/opinion/sunday/dinner-is-printed.html (23. 12. 2013).

Kraßer, Rudolf: *Patentrecht, 6. Auflage*. München: Verlag C. H. Beck, 2009.

Kuehn, Cliff: Change as Quick as a Bullet. *Intellectual Property Magazine*, april 2013, str. 27–28.

Kur, Annette, Dreier, Thomas: *European Intellectual Property Law: Texts, Cases & Materials.* Cheltenham: Edward Elgar Publishing, 2013.

Prinsley, Mark: A Sticky Subject: Additive Manufacturing and IP. *Intellectual Property Magazine*, 31. 10. 2013.

Osterrieth, Christian: *Patentrecht.* München: Verlag C. H. Beck, 2010.

Puharič, Krešimir: *Zakon o industrijski lastnini (ZIL-1-UPB1) s komentarjem.* Ljubljana: GV Založba, 2003.

Rideout, Brian: Printing the Impossible Triangle: The Copyright Implications of Three-Dimensional Printing. *Journal of Business, Entrepreneurship & the Law*, 2011, let. V, št. 1, str. 161–177.

Schack, Haimo: *Urheber- und Urhebervertragsrecht, 4. Auflage.* Tübingen: Mohr Siebeck, 2007.

Skubic, Zoran: Preprosta geometrična oblika z banalnimi detajli (še) ne zadostuje za znamko Skupnosti. *Pravna praksa*, 2013, let. 32, št. 4, str. 27.

Smith, Shireen: See in 3D. *Intellectual Property Magazine*, april 2013, str. 25–26.

Trampuž, Miha, Oman, Branko, Zupančič, Andrej. *Zakon o avtorski in sorodnih pravicah (ZASP) s komentarjem.* Ljubljana: Gospodarski vestnik, 1997.

Weinberg, Michael: *It Will Be Awesome if They Don't Screw it Up: 3D Printing, Intellectual Property, and the Fight Over the Next Great Disruptive Technology.* Public Knowledge (november 2010). http://publicknowledge.org/it-will-be-awesome-if-they-dont-screw-it-up (22. 12. 2013).

Wilbanks, Kelsey B.: The Challenges of 3D Printing to the Repair-Reconstruction Doctrine in Patent Law. *George Mason Law Review*, 2013, let. 20, št. 4, str. 1147–1181.

3D printing. V: Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/Additive_manufacturing (23. 12. 2013).

III.
Procesna vprašanja v internetnem okolju

Elektronsko poslovanje in mednarodna pristojnost za potrošniške spore

dr. Aleš Galič

1. Uvod

V vse bolj pogostih primerih, ko potrošnik stopa v pravno razmerje s tujim trgovcem, je zelo pomembno vprašanje, pred sodiščem v kateri državi se bo reševal morebitni spor iz tega razmerja. Če bo namreč potrošnik moral pravno varstvo uveljavljati pred sodiščem tuje države, je utemeljen strah, da bo to praktično pomenilo onemogočitev pravnega varstva – še višji grozeči stroški, nepoznavanje tujega prava in okolja, izguba časa zaradi poti na sodišče ... Če bo šlo pri tem za državo sedeža trgovca, bo dejanska neenakopravnost med strankama še bolj izrazita. Uredba št. 44/2001 o pristojnosti ter priznanju in izvršitvi sodnih odločb v civilnih in gospodarskih zadevah (t. i. Bruseljska uredba – v nadaljevanju BU) zato zagotavlja posebno procesnopravno varstvo potrošnikov (podobno kot tudi za delavce in upravičence iz zavarovalnih pogodb). Gre za izraz želje po varstvu šibkejše stranke v pravnih razmerjih, za katere je tipična dejanska neenakopravnost strank.[1] Posebno varstvo se odraža v štirih smereh: določena je dodatna, posebej ugodna pristojnost po prebivališču tožnika za tožbe, v katerih kot tožnik nastopa potrošnik (prvi odstavek 16. člena[2]); določena je omejitev, da je potrošnik, kadar je tožen, lahko tožen le v kraju svojega prebivališča (drugi odstavek 16. člena); močno je omejena možnost sklenitve prorogacije oziroma dogovora o pristojnosti (17. člen); kršitev omenjenih pravil o pristojnosti pa lahko povzroči odklonitev priznanja tuje sodne odločbe (35. člen BU). Bruseljska uredba se sicer uporablja le v primeru, da ima toženec prebivališče v državi članici EU. Če ta pogoj ni izpolnjen, se za določitev mednarodne pristojnosti uporabi Zakon o mednarodnem zasebnem pravu in postopku.[3] Ta zakon potrošnikom ne daje

[1] Glej na primer sodbo Sodišča Evropske unije (SEU) z dne 14. marca 2013 v zadevi C-419/11, *Česká spořitelna, a.s. proti Geraldu Feichterju,* ter sodbo SEU z dne 5. decembra 2013 v zadevi C-508/12, *Walter Vapenik proti Josefu Thurnerju*.

[2] Bruseljska uredba se sicer uporablja le v razmerjih s čezmejnim elementom. Opozoriti pa velja, da glede potrošniških sporov (kot tudi glede nekaterih drugih pristojnosti) poleg mednarodne pristojnosti neposredno ureja tudi krajevno pristojnost.

[3] Uradni list RS, št. 56/1999 (ZMZPP). Glede mednarodne pristojnosti posebno in za potrošnika ugodno (čeprav precej nedodelano) določbo vsebuje le v 52. členu, ki določa, da v pravnem razmerju s potrošnikom ni dopusten dogovor o pristojnosti tujega sodišča.

takšnega varstva, kot ga zagotavlja Bruseljska uredba. Vendar to kmalu ne bo več pomembno. Prenovljena Bruseljska uredba (Uredba št. 1215/2012),[4] ki se začne uporabljati 1. januarja 2015, za potrošniške spore uveljavlja načelo univerzalne veljave. Od omenjenega dne se torej za pristojnost v potrošniških sporih (tistih, ki jih zajema opredelitev v 15. členu BU oziroma 17. členu prenovljene BU) ZMZPP ne uporablja več.

2. Vrste potrošniških sporov, za katere veljajo pravila Uredbe

V 15. členu Uredba definira potrošniški spor. Za tak spor gre, *kadar je predmet postopka pogodba ali zahtevek iz pogodbe, ki jo določena oseba – potrošnik – sklepa za namene, ki jih ni mogoče pripisati njeni poklicni ali obrtni dejavnosti*.[5] Vendar določbe Bruseljske uredbe ne pridejo v poštev za vse spore iz pravnih razmerij s potrošniki, ki ustrezajo navedeni definiciji, temveč le:

- če gre za pogodbo o prodaji premičnih stvari z obročnim plačilom;
- če gre za pogodbo o najemu posojila z obročnim odplačevanjem oziroma pogodbo, na katero je vezan kakšen drug kreditni posel in katere namen je plačilo nakupa premičnih stvari,
- v vseh drugih primerih, če je bila pogodba sklenjena z osebo, ki opravlja gospodarsko ali poklicno dejavnost v državi članici, v kateri ima potrošnik stalno prebivališče, ali če na kakršenkoli način usmerja to svojo dejavnost v to državo članico ali v več držav, vključno s to državo članico, pogodba pa spada v okvir te dejavnosti.

Posebno procesno varstvo potrošnika v Bruseljski uredbi torej ne gre tako daleč, da bi potrošnik že brez nadaljnjega v sporu iz potrošniške pogodbe trgovca lahko tožil v kraju svojega prebivališča. Sestavljavci Bruseljske uredbe so namreč ocenili, da je odstop od splošnih pravil o pristojnosti po prebivališču oziroma sedežu toženca upravičen le, če so podani posebej utemeljeni razlogi. Ti so lahko v tem, da gre za pogodbe, ki po izkušnjah za potrošnika pomenijo največje tveganje in so tudi po materialnem pravu podvržene številnim jamstvom v korist potrošnika (obročni nakup po prvi alineji in nakup s kombinacijo kredita za ta nakup po drugi alineji), ali pa v tem, da je pogodba rezultat neke komercialne aktivnosti prodajalca v državi prebivališča potrošnika (tretja alineja) – v slednjem primeru je namreč prodajalec očitno računal na to, da bodo njegovo blago kupovali tudi kupci iz te države.

[4] Uredba (EU) št. 1215/2012 Evropskega parlamenta in Sveta z dne 12. decembra 2012 o pristojnosti in priznavanju ter izvrševanju sodnih odločb v civilnih in gospodarskih zadevah (prenovitev).

[5] O tem glej več v: A. Galič, str. 125.

3. Poslovanje prek interneta kot usmerjanje komercialnih aktivnosti

S komercialno aktivnostjo v državi potrošnikovega prebivališča je mišljeno predvsem oglaševanje, prav tako pa opravljanje poslov na primer po posredniku ali agentu, ki mu je zaupano sklepanje pogodb.[6] Vprašanje pa je, kaj določba o »usmerjanju komercialnih aktivnosti v določeno državo« pomeni v zvezi s posli, sklenjenimi prek interneta, oziroma posli, sklenjenimi s trgovci, ki svojo dejavnost oglašujejo tudi na internetu. Jasno je, da vsaka internetna stran še ne pomeni, da se komercialne aktivnosti usmerjajo v druge države, tj. v praktično vse države sveta (oziroma v kontekstu BU: v vse države EU). Problem pa je, kako obravnavati internetne strani, ki omogočajo sklenitev pogodbe na daljavo ali vsaj vabijo k sklenitvi takšne pogodbe. Včasih je prevladovalo stališče, da tudi takšna internetna stran sama po sebi še ne pomeni, da gre za usmerjanje komercialnih aktivnosti v tujo državo; štelo se je, da je bilo treba ugotoviti namen trgovca, za to pa so bili upoštevni različni indici, med drugim jezik, ki je uporabljen, valute, ki so označene … Takšno stališče je bilo sprejeto tudi v Razlagalnem poročilu Giuliana in Legarda[7] ob sprejemu Rimske konvencije,[8] ko se je isto vprašanje pojavljalo glede določitve merodajnega prava za potrošniške pogodbe. Tedaj se te dileme seveda niso postavile v zvezi z internetom, temveč v zvezi s klasičnimi mediji; na primer, ker je bilo televizijski ali radijski program mogoče spremljati tudi v sosednji državi, se je postavljalo vprašanje, ali objavljanje reklam v takšnem programu pomeni usmerjanje komercialnih aktivnosti v drugo državo.

Razvoj je šel nato v nasprotno smer. Evropski svet in Evropska komisija sta izdali skupno izjavo, ki sicer potrjuje, da »samo dejstvo, da je internetna stran dostopna v tujini, še ne zadošča za uporabo čl. 15 BU«, tj. za sklep, da gre za usmerjanje komercialnih aktivnosti v tujo državo. Poleg tega je potrebno še, da ta spletna stran vabi k sklepanju pogodb na daljavo in da je bila na tak ali drugačen način pogodba dejansko sklenjena na daljavo. V tej izjavi je med drugim še izrecno povzeto, da jezik ali valuta, uporabljena na spletni strani, nista pomembna elementa.[9] Poudariti pa je treba, da pri navedenem ni šlo za stališče Evropskega sodišča, le za stališče Sveta in Komisije. Dodatno težo tej skupni izjavi pa vendarle daje okoliščina, da jo je evropski zakonodajalec povzel tudi v uvodni

[6] Več prav tam.

[7] Giuliano/Lagarde Report, I. *Official Journal C 282,* 31. 10. 1980, str. 0001–0050.

[8] Konvencija o uporabi prava v pogodbenih obligacijskih razmerjih, na voljo za podpis 19. junija 1980 v Rimu.

[9] A joint statement by the Council and the Commission on Articles 15 and 73 of the Brussels I Regulation. Objavljeno na: http://ec.europa.eu/civiljustice/homepage/homepage_ec_en_declaration.pdf (14. 1. 2014).

izjavi 24 Uredbe Rim I.[10] Za zanesljivo stališče glede predstavljene problematike pa je bilo treba počakati na odločitev SEU (pred Lizbonsko pogodbo Sodišče Evropskih skupnosti – SES).

4. Sodba SEU v združenih zadevah *Pammer* in *Hotel Alpenhof*

Na stališče SEU je bilo treba čakati do leta 2010. Tedaj je SEU odločilo v dveh zadevah, ki ju je zaradi sorodnosti problematike združilo v skupno obravnavanje.[11] V zadevi *Pammer* je avstrijski potrošnik prek posredniške agencije, ki je dejavnost trgovca oglaševala po internetu, stopil v stik ter nato sklenil pogodbo z nemškim ladjarjem za prevoz s tovorno ladjo iz Trsta na Daljni vzhod. Ker je po ogledu ladje ugotovil, da pogoji na ladji niso takšni, kot je bilo oglaševano, je odstopil od pogodbe in zahteval vračilo celotnega vplačanega zneska. Tožbo je vložil v Avstriji, toženi trgovec pa je ugovarjal, da svojih komercialnih aktivnosti ni usmerjal v Avstrijo, zato avstrijsko sodišče ni pristojno. V zadevi *Hotel Alpenhof* je nemški trgovec na podlagi oglaševanja avstrijskega hotela na internetu po elektronski pošti s tem hotelom sklenil pogodbo. Ker opravljenih storitev ni plačal, ga je trgovec tožil v Avstriji. Toženi potrošnik je ugovarjal, da bi smel biti tožen le v državi svojega prebivališča, saj je trgovec z internetnim oglaševanjem usmerjal svoje komercialne aktivnosti v Nemčijo. Ker je bila odločitev v obeh zadevah odvisna od tega, ali trgovčevo poslovanje prek interneta pomeni usmerjanje komercialnih aktivnosti v drugo oziroma druge države in ali je zato potrošnik varovan s posebnim režimom pristojnosti po Bruseljski uredbi, je SEU obe zadevi združilo.

SEU je najprej postavilo omejitev, da zgolj okoliščina, da ima trgovec (ali njegov posrednik[12]) spletno stran in da je ta dostopna v državi, v kateri ima potrošnik stalno prebivališče, ne zadostuje za sklep, da trgovec usmerja svoje komercialne aktivnosti v to državo. Potrošnik uživa varstvo v skladu z Uredbo, vendar to ne pomeni, da je to varstvo absolutno. SEU je poudarilo, da je s prisotnostjo na internetu, ki je po naravi globalen, oglaševanje trgovca na spletni strani

[10] Uredba (ES) št. 593/2008 Evropskega parlamenta in Sveta z dne 17. junija 2008 o pravu, ki se uporablja za pogodbena obligacijska razmerja (Rim I).

[11] Sodba SEU (veliki senat) z dne 7. septembra 2010 v združenih zadevah C-585/08, *Peter Pammer proti Reederei Karl Schlüter GmbH & Co KG,* in C-144/09, *Hotel Alpenhof GesmbH proti Oliverju Hellerju.*

[12] Pomembno je stališče SEU, da okoliščina, da gre za spletno stran posredniške družbe, in ne za trgovca, ne preprečuje ugotovitve, da trgovec usmerja svojo dejavnost v druge države članice, vključno z državo članico stalnega prebivališča potrošnika, če ta družba ravna v imenu in za račun navedenega trgovca. Nacionalno sodišče mora preveriti, ali je ta bil oziroma ali bi moral biti seznanjen z mednarodnim obsegom dejavnosti posredniške družbe in kako je bila ta družba povezana s tem trgovcem. Glej prav tam.

načeloma dostopno v vseh državah in zato v celotni EU brez nujnega nastanka dodatnih stroškov. Zato takšno oglaševanje še ne kaže na voljo trgovca, da bi ciljal na potrošnike zunaj ozemlja države članice, v kateri ima sedež.[13]

Prav tako ni dovolj, da na tej spletni strani navede svoj elektronski naslov in druge kontaktne podatke, na primer telefonsko številko (brez mednarodne kode). Navajanje teh informacij, po ugotovitvi SEU, namreč ne kaže na to, da trgovec usmerja svojo dejavnost v eno ali več držav članic, saj so tovrstne informacije v vsakem primeru nujne, da lahko potrošnik s stalnim prebivališčem v državi članici, v kateri ima ta trgovec sedež, z njim naveže stik. Navedbo informacij o identiteti trgovca pa zahtevajo tudi direktive EU.[14]

Po stališču SEU torej zgolj dejstvo, da je spletna stran dostopna, ni dovolj za uporabo člena 15(1)(c) Uredbe št. 44/2001. Ni tudi bistveno razlikovanje med »aktivnimi« in »pasivnimi« internetnimi stranmi. Treba pa je preveriti, ali je – pred morebitno sklenitvijo pogodbe s potrošnikom – iz teh spletnih strani in celotne dejavnosti trgovca razvidno, da je nameraval poslovati s potrošniki s stalnim prebivališčem v eni ali več državah članicah, vključno s tisto, v kateri ima ta potrošnik stalno prebivališče, in sicer tako, da je bil pripravljen na sklenitev pogodbe z njimi. Vendar odločilen kriterij pri tem ni izključno ugotavljanje subjektivne volje trgovca. Zato se je treba opreti na indice. Med indice, da je dejavnost »usmerjena v« državo članico, v kateri ima potrošnik stalno prebivališče, spada vsako očitno izražanje volje po poslovanju s potrošniki iz te države članice.[15]

SEU je ob tem načelnem stališču v oporo uporabi v praksi navedlo neizčrpni seznam indicev, ki lahko nacionalnemu sodišču pomagajo pri presoji, ali je izpolnjen bistveni pogoj glede gospodarske dejavnosti, usmerjene v državo članico, v kateri ima potrošnik stalno prebivališče.[16] Ti so (primeroma) mednarodni obseg dejavnosti, navedba poti iz drugih držav članic do kraja sedeža trgovca, uporaba jezika ali valute, ki se običajno ne uporablja v državi članici, v kateri ima trgovec sedež, z možnostjo rezervacije oziroma potrditve rezervacije v tem drugem jeziku, navedba telefonske številke z mednarodno klicno kodo, izdatki za storitev internetnega referenciranja, da bi se potrošnikom s stalnim prebivališčem v drugih državah članicah olajšal dostop do spletne strani trgovca ali do spletne strani njegovega posrednika, uporaba domenskega imena najvišje ravni, ki ni domensko ime države članice, v kateri ima trgovec sedež, in omemba

[13] Prav tam.
[14] Prav tam.
[15] Prav tam.
[16] Prav tam.

mednarodnih strank s prebivališčem v različnih državah članicah.[17] Vsekakor pa so ta merila le orientacijska in nacionalno sodišče mora sámo preučiti cilje in učinke poslovne strategije trgovca ali ponudnika storitev.[18] Trgovcu tudi ostanejo načini, kako zagotoviti, da bo jasno razvidno, da s potrošniki iz določenih držav ne želi poslovati (na primer z navedbo, za katere države ponudba ne velja, ali z zahtevo, da stranka vpiše državo prebivališča, njene države pa spletna stran ne »ponuja«).[19]

Zanimivo je, da SEU enakega pristopa glede dejanj, storjenih prek interneta, ni uporabilo pri opredelitvi kraja škodnega dogodka pri kršitvi osebnostnih pravic z vsebinami, objavljenimi na spletnem mestu (pristojnost po tretjem odstavku 5. člena BU). V zadevi *eDate Advertising* je zavrnilo predloge, da bi bilo treba tudi v tem kontekstu – tako kot pri ravnanjih trgovca – ugotavljati, ali je imela oseba, ki je prek interneta razširjala določene informacije, namen usmerjati svojo aktivnost v tujino.[20] Kriteriji pri določanju pristojnosti za spore glede deliktov, storjenih preko interneta, so torej drugačni kot kriteriji za določanje pristojnosti za spore iz potrošniških pogodb, sklenjenih prek interneta.

5. Sodba SEU v zadevi *Mühlleitner:* ali omenjena pravila veljajo le za pogodbe, sklenjene na daljavo?

V sodbi v zadevah *Pammer in Hotel Alpenhof* je SEU na več mestih omenilo, da gre za pogodbo, sklenjeno na daljavo (prek interneta ali prek elektronske pošte na podlagi informacij in oglaševanja na internetu), in je v tem kontekstu ocenjevalo pomen trgovčevega poslovanja prek interneta. Tudi prej omenjena skupna izjava Komisije in Sveta, ki je povzeta v uvodni izjavi k Rimski uredbi, izrecno govori o sklepanju pogodb na daljavo.[21] Zato ni bilo povsem jasno, ali

[17] Podobno sklepni predlogi generalne pravobranilke Verice Trstenjak (predstavljeni 18. maja 2010), ki je kot pomembne dejavnike za presojo štela zlasti vsebino spletne strani, dosedanje poslovanje osebe, ki opravlja gospodarsko ali poklicno dejavnost, vrsto uporabljene internetne domene in uporabo možnosti spletnega ali siceršnjega oglaševanja.

[18] Za obširen komentar sodbe v zadevah *Pammer in Hotel Alpenhof* glej A. Furrer, A. Glarner, v: F. Dasser, P. Oberhammer, str. 295–296.

[19] Glej prav tam.

[20] Sodba SEU z dne 25. oktobra 2011 C-509/09 in C-161/10 v združenih zadevah *eDate Advertising GmbH v X in Olivier Martinez, Robert Martinez v MGN Limited*. Skladno s t. i. formulo mozaika lahko vloži tožbo pri sodiščih vsake države članice, na ozemlju katere je ali je bila na spletu objavljena vsebina dostopna. Vendar so ta sodišča pristojna za odločanje zgolj glede škode, storjene na ozemlju države članice sodišča, ki odloča. Če pa želi tožnik z eno tožbo zajeti celotno škodo, mora tožiti bodisi v državi, kjer ima objavitelj teh vsebin sedež, bodisi pri sodiščih države članice, kjer je težišče oškodovančevih interesov.

[21] Za stališče (iz časa pred sodbo SEU v zadevi *Mühlleitner*), da omenjena pravila glede trgovcev, prisotnih na svetovnem spletu, veljajo le za pogodbe, sklenjene na daljavo, glej M. Bogdan, str. 220.

je *a contrario* mogoče sklepati, da je pri pogodbah, ki niso sklenjene na daljavo, položaj drugačen. Na to vprašanje je SEU odgovorilo v zadevi *Mühlleitner.* [22] Tu je šlo za primer, ko je avstrijska potrošnica na svetovnem spletu iskala vozilo nemške znamke, ki ga je želela kupiti za svoje zasebne potrebe. Ko se je povezala na nemški iskalnik www.mobil[e].de, je izbrala znamko in model želenega vozila in tako pridobila seznam vozil, ki so ustrezala posebnim lastnostim. Ko je izbrala vozilo, ki je najbolj ustrezalo njenim iskalnim merilom, je bila napotena na ponudbo toženih strank, nemškega prodajalca rabljenih avtomobilov (*Autohaus Yussufi*). Po nadaljnji komunikaciji po elektronski pošti in telefonu je odpotovala v Nemčijo, tam pregledala ponujeno vozilo in sklenila prodajno pogodbo. Ko je tožnica vložila tožbo (za razveljavitev pogodbe in vračilo kupnine) v Avstriji, sta tožena trgovca, brata Yussufi, ugovarjala, da svojih komercialnih aktivnosti nista usmerjala v Avstrijo in da je bila pogodba sklenjena na njunem sedežu v Nemčiji. Menila sta, da je potrošnika v skladu s stališči iz sodbe v zadevah *Pammer in Hotel Alpenhof* treba zavarovati, kadar zaradi trgovčeve internetne ponudbe sklene pogodbo na daljavo.

SEU temu stališču ni pritrdilo. Ocenilo je, da je sklenitev potrošniške pogodbe na daljavo zgolj »kazalnik povezanosti pogodbe« s poslovno ali poklicno dejavnostjo trgovca ali ponudnika storitev, ki je usmerjena v državo članico, v kateri ima potrošnik stalno prebivališče. SEU je zato izreklo, da člen 15(1)(c) Uredbe št. 44/2001 pride v poštev tudi v primerih, ko pogodba med potrošnikom in podjetnikom ni bila sklenjena na daljavo. Pri tem se je oprlo tako na gramatikalno razlago kot tudi na namen določbe – učinkovito varstvo potrošnikov. Iz člena 15(1)(c) izhajata le dva pogoja: prvič, podjetnik mora opravljati gospodarske in poklicne dejavnosti v državi članici, v kateri ima potrošnik stalno prebivališče, ali na kakršenkoli način usmerjati te dejavnosti v to državo članico ali v več držav, vključno s to državo članico, in drugič, sporna pogodba mora spadati v okvir takšnih dejavnosti.[23]

Sklenitev pogodbe na daljavo torej ni pogoj za sklepanje, da trgovec usmerja komercialne aktivnosti v drugo državo.[24] Lahko pa je indic za sklepanje o trgovčevem namenu čezmejnega poslovanja. Pomen sodbe v zadevi *Mühlleitner* je tudi v tem, da se seznam indicev, opredeljenih v sodbi v zadevah *Pammer in Hotel Alpenhof*, dopolnjuje. Med indice, ki lahko dokazujejo, da je pogodba povezana z dejavnostjo, usmerjeno v državo članico, v kateri ima potrošnik stalno prebi-

[22] Sodba SEU z dne 6. septembra 2012 v zadevi C-190/11, *Daniela Mühlleitner proti Ahmadu in Wadadu Yussufiju*.

[23] Prav tam.

[24] Za enaka stališča v literaturi že pred to sodbo SEU glej na primer A. Staudinger, v: T. Rauscher, str. 395.

višče, torej spadata tudi »navezava stika na daljavo« in »sklenitev potrošniške pogodbe na daljavo«.[25]

6. Sodba SEU v zadevi *Emrek:* ali omenjena pravila veljajo le, če obstaja vzročna zveza med trgovčevo prisotnostjo na internetu in sklenjeno pogodbo?

V zadevi *Emrek* je SEU odgovorilo na vprašanje, ali člen 15(1)(c) Bruseljske uredbe zahteva ugotovitev obstoja vzročne zveze med gospodarsko ali poslovno dejavnostjo, usmerjeno v državo članico, v kateri ima potrošnik stalno prebivališče, in potrošnikovo odločitvijo za sklenitev pogodbe.[26] Dejansko stanje ima kar nekaj podobnosti s prej opisano zadevo *Mühlleitner.* Šlo je za nemškega potrošnika, ki je v sosednjem mestu v Alzaciji v Franciji pri profesionalnem prodajalcu rabljenih avtomobilov g. Sabranovicu (ta posluje pod firmo *Vlado Automobiles Import-Export*) kupil rabljen avtomobil. Posebnost tega primera je, da nemški potrošnik sploh ni vedel, da francoski trgovec oglašuje tudi prek interneta – do njega je namreč prišel zato, ker so mu ga priporočili znanci, ki so s tem trgovcem že poslovali. Da ima trgovec spletno stran in da je ta takšne narave, da izkazuje tudi trgovčevo namero poslovanja s kupci iz Nemčije, je potrošnik izvedel šele kasneje, po nastanku spora. Zato je vložil tožbo v Nemčiji. Toženi trgovec je ugovarjal, da med njegovim oglaševanjem prek interneta in sklenjeno pogodbo očitno ni podana vzročna zveza in da se zato potrošnik ne more sklicevati na člen 15(1)(c) Bruseljske uredbe.

Takšna so bila pred odločitvijo SEU pretežno tudi stališča v teoriji (vsaj v nemško govorečih okoljih).[27] Tudi nemško Zvezno sodišče je izreklo, da je spletna stran podjetja morala potrošnika vsaj motivirati k sklenitvi pogodbe.[28] Vendar SEU temu stališču ni pritrdilo. Zavzelo je stališče, da člen 15(1)(c) Uredbe št. 44/2001 ne zahteva vzročne zveze med načinom usmerjanja gospodarske ali poklicne dejavnosti v državo članico, v kateri ima potrošnik stalno prebivališče, in sicer s spletno stranjo, ter sklenitvijo pogodbe s tem potrošnikom. Pri tem se je oprlo na gramatikalno razlago omenjene določbe, ki takšnega pogoja izkaza-

[25] Sodba SEU z dne 6. septembra 2012 v zadevi C-190/11, *Daniela Mühlleitner proti Ahmadu in Wadadu Yussufiju*.

[26] Sodba SEU z dne 17. oktobra 2013 v zadevi C-218/12, *Lokman Emrek proti Vladu Sabranovicu.*

[27] A. Staudinger, v: T. Rauscher, str. 398, P. Mankowski, Muss zwischen …, str. 333, A. Schwartze, v: T. Simons, R. Hausmann, str. 371 (ki povzema tudi prakso avstrijskega Vrhovnega sodišča), nekoliko bolj zadržano (z zavzemanjem za obrnjeno dokazno breme) A. Furrer, A. Glarner, v: F. Dasser, P. Oberhammer, str. 294.

[28] P. Mankowski, Neues zum …, str. 258.

nosti vzročne zveze ne vsebuje.[29] Poleg tega bi zahteva po izkazu vzročne zveze tudi nasprotovala cilju učinkovitega varstva potrošnikov, saj bi bilo pogosto težko dokazovati, da je potrošnik v času pred sklenitvijo pogodbe obiskal spletno stran trgovca.[30]

Vendar pa SEU dodaja, da čeprav navedena vzročna zveza ni nezapisan pogoj, od katerega bi bila odvisna uporaba navedenega člena 15(1)(c), je kljub temu lahko pomemben indic (enakovreden sklenitvi pogodbe na daljavo), ki ga nacionalno sodišče lahko upošteva pri odločanju o tem, ali je dejavnost dejansko usmerjena v državo članico, v kateri ima potrošnik stalno prebivališče. Seznam indicev iz sodbe v zadevah *Pammer* in *Alpenhof* se torej tudi s tem dopolnjuje in (čeprav to najbrž ni bil namen SEU) širi.[31]

Odločitev SEU v zadevi *Emrek* je predmet številnih kritik. Nekateri dvomijo že o pravilnosti stališča, da drugačnega sklepa gramatikalna razlaga čl. 15(1)(c) Bruseljske uredbe ne omogoča. Ta določba namreč govori o tem, da trgovec (…) na kakršenkoli način usmerja svojo dejavnost v to državo članico ali v več držav, vključno s to državo članico, *pogodba pa spada v okvir te dejavnosti.* Nekateri ta zapis, ko gre za internet, razumejo tako, da je z »*dejavnostjo*« mišljeno elektronsko poslovanje ali oglaševanje trgovca na internetu.[32] Vendar je to stališče zgrešeno. Ne gre za to, da mora pogodba spadati v okvir tega, da trgovec posluje prek interneta. Dovolj je, da se po vsebini nanaša na dejavnosti (tj. blago, storitve, tip pogodbe …), ki jih trgovec oglašuje ali opravlja tudi prek interneta. Bolj tehten je vsebinski pomislek o praktičnih posledicah, prav tako pa pomislek, da je stališče v nasprotju z uvodno izjavo št. 25 k Uredbi Rim I.[33] Res je sicer, da je SEU omenjeno stališče zavzelo ob presoji Bruseljske uredbe, vendar to tudi – kot bo razvidno iz naslednjega poglavja – ni brez pomena za presojo Rimske uredbe.

[29] Sodba SEU z dne 17. oktobra 2013 v zadevi C-218/12, *Lokman Emrek proti Vladu Sabranovicu*.

[30] Glej tudi sklepne predloge generalnega pravobranilca Cruza Villalóna z dne 18. julija 2013, ki meni, da bi se ta dokaz lahko spremenil v *probatio diabolica*, zaradi katerega bi posebna pristojnost iz členov 15 in 16 Uredbe št. 44/2001 postala neuporabna. Če bi po drugi strani zadoščalo, da se potrošnik zgolj sklicuje na vzročno zvezo, pa sploh ne bi šlo za pravi pogoj.

[31] Ta seznam pa se dopolnjuje še z naslednjim: v obravnavani zadevi za trgovca, ki sicer posluje v drugi državi, vendar na obmejnem območju, ki je del aglomeracije mesta Saarbrücken v Nemčiji. Okoliščina, da podjetnik uporablja tudi telefonsko številko druge države članice, ki jo daje na voljo potencialnim strankam s stalnim prebivališčem v tej državi, s čimer jim omogoča prihranek stroškov mednarodnega klica, je prav tako indic, ki dokazuje, da je njegova dejavnost »usmerjena v« to drugo državo članico.

[32] G. Ruehl, str. 1.

[33] Prav tam.

7. Pomen predstavljene judikature za določitev merodajnega prava v potrošniških pogodbah

Predstavljena stališča so bila sprejeta v zvezi z določanjem mednarodne pristojnosti po Bruseljski uredbi. Vprašanje pa je, ali imajo kakšen pomen tudi za razlago Uredbe Rim I.[34] Ta uredba določa kolizijska pravila za določitev merodajnega prava za pogodbena razmerja, pri čemer za potrošniške pogodbe uveljavlja podobne kriterije, kot jih Bruseljska uredba uveljavlja za določitev mednarodne pristojnosti.[35] Pravo države, v kateri ima potrošnik običajno prebivališče, se uporabi pod pogojem, da podjetnik izvaja svoje poslovne ali poklicne dejavnosti v državi, v kateri ima potrošnik običajno prebivališče, *ali na kakršenkoli način usmerja take dejavnosti v to državo ali več držav, vključno s to državo*, in da pogodba spada v okvir takih dejavnosti.[36] Skladno z drugim odstavkom 6. člena Uredbe Rim I je tudi v teh primerih sicer dopustna avtonomija strank, vendar izbira prava druge države potrošnika ne sme prikrajšati za zaščito, ki mu jo zagotavljajo določbe, od katerih ni dovoljeno odstopanje z dogovorom po pravu države prebivališča potrošnika.[37] Pogoj »usmerjanja dejavnosti« je pravzaprav isti kot v členu 15(1)(c) Bruseljske uredbe. SEU je že večkrat (v različnih kontekstih) izreklo, da je iste pojme, ki se pojavljajo v obeh uredbah (Rimski in Bruseljski), treba tolmačiti enako. [38] Zato je mogoče predvidevati, da se bo SEU glede vprašanja, kaj to pomeni glede trgovcev, prisotnih na svetovnem spletu, zavzelo za uporabo pravil iz sodb v zadevah *Pammer in Hotel Alpenhof*, *Mühlleitner* ter *Emrek* tudi pri razlagi Uredbe Rim I. To sicer ni povsem neproblematično, saj se uvodna izjava št. 24 k tej uredbi, kot je že bilo povedano (glej 3 poglavje), sklicuje

[34] Uredba (ES) št. 593/2008 Evropskega parlamenta in Sveta z dne 17. junija 2008 o pravu, ki se uporablja za pogodbena obligacijska razmerja (Rim I).

[35] Uredba Rim I velja univerzalno (2. člen), torej že zdaj v celoti nadomešča določbe ZMZPP. Določba 22. člena ZMZPP, ki določa upoštevno pravo za presojo pogodbe o zaposlitvi, praktično več ne velja, čeprav ni bila izrecno razveljavljena.

[36] Za starejša stališča glede vprašanj mednarodnega zasebnega prava glede potrošniških pogodb, sklenjenih prek interneta, glej D. Možina, str. 321 in nasl.

[37] Poseben režim za potrošniške pogodbe pa skladno s tretjim odstavkom 6. člena Uredbe Rim I ne velja za (1) pogodbe o opravljanju storitev za potrošnika, ki se v celoti opravijo zunaj države potrošnikovega prebivališča, (2) za prevozne pogodbe, razen za pogodbe o paketnih potovanjih, (3) za pogodbe, katerih predmet je stvarna pravica na nepremičnini ali najemna pravica na nepremičnini, razen za *time-sharing* pogodbe, (4) za pravice in obveznosti, ki tvorijo finančni instrument, ter pravice in obveznosti, ki tvorijo pogoje, ki urejajo izdajanje ali javne ponudbe in javne prevzemne ponudbe prenosljivih vrednostnih papirjev ter vpis in odkup enot v kolektivnih naložbenih podjemih, kolikor te dejavnosti ne predstavljajo finančnih storitev, ter (5) za pogodbe, sklenjene v okviru večstranskega sistema, ki združuje ali omogoča združevanje več nakupnih in prodajnih interesov tretjih oseb v zvezi s finančnimi instrumenti.

[38] Na primer sodba SEU (veliki senat) z dne 15. marca 2011 v zadevi C-29/10, *Heiko Koelzsch proti Velikemu vojvodstvu Luksemburg.*

na omenjeno izjavo Sveta in Komisije, v kateri so bila stališča nekoliko drugačna, uvodna izjava št. 25 pa izrecno govori tudi o tem, da mora obstajati zveza med sklenitvijo pogodbe in dejavnostjo trgovca na internetu (»pod pogojem, da je bila potrošniška pogodba sklenjena kot rezultat opravljanja gospodarskih in poklicnih dejavnosti podjetnika v tej državi«). To pa ni združljivo s stališčem SEU v zadevi *Emrek*. Predvsem zaradi tega je za dokončno rešitev vprašanja, v kolikšni meri je stališča iz omenjenih judikatov mogoče uporabiti tudi za razlago Uredbe Rim I, treba počakati na odločitev SEU.

8. Sklep

SEU je v obdobju med letoma 2010 in 2013 v treh pomembnih judikatih (*Pammer in Hotel Alpenhof*, *Mühlleitner, Emrek)* zavzelo nekaj pomembnih stališč v zvezi s potrošniškimi pogodbami, sklenjenimi s trgovci, ki poslujejo oziroma oglašujejo prek interneta. Domet varstva potrošnikov v Bruseljski uredbi se s tem širi: ne gre več le za pogodbe, sklenjene prek interneta, in tudi ne le za pogodbe, sklenjene na daljavo, ki so v zvezi s potrošnikovim predhodnim obiskom trgovčeve spletne strani. Pomembna razširitev je tudi, da vse napisano velja tudi za trgovce, prisotne na spletnih straneh posrednikov (na primer hotel, ki ga je mogoče rezervirati prek posrednika booking.com). Nova pomembna razširitev pa bo nastopila 1. januarja 2015, ko bo sistem Bruseljske uredbe glede varstva potrošnikov brez omejitev veljal tudi za trgovce iz tretjih držav (kar pa seveda ne pomeni, da je zagotovljeno, da bodo sodbe iz držav članic EU tudi priznane v tretji državi, kjer ima sedež – in premoženje – trgovec).

Stališče, da za aktiviranje varovalnih pristojnosti v korist potrošnika ni dovolj že sama okoliščina, da je trgovec prisoten na svetovnem sklepu, je razumljivo. Prav tako je sprejemljivo stališče, da subjektivne volje trgovca skoraj ni mogoče ugotavljati, pač pa je treba presojati različne indice. Vendar pa je seznam teh indicev v praksi SEU tako širok, da je vprašanje, ali sploh še gre za praktično relevantno omejitev. Poudariti tudi velja, da ne gre le za pogodbe, sklenjene prek interneta (elektronsko poslovanje v ožjem smislu), temveč je domet judikatov SEU bistveno širši. Kjer je potrošnikov obisk trgovčeve spletne strani povezan s sklenitvijo pogodbe (na primer, ker je tam dobil telefonsko številko ali elektronski naslov trgovca), to ni sporno. Ni sporno tudi v primeru, ko je nato do sklenitve pogodbe prišlo v prostorih trgovca in ne gre za sklenitev pogodbe na daljavo. Bolj problematično pa je, da se na okoliščino, da trgovec ima internetno stran, s katero usmerja svoje aktivnosti v tujino, lahko sklicuje tudi potrošnik, ki za to spletno stran sploh ni vedel (ali morda – na to mora SEU še odgovoriti – v času, ko je potrošnik sklenil pogodbo, niti še ni obstajala, obstaja pa v času, ko je vložena tožba pred sodiščem). Ker je vse več trgovcev prisotnih na svetovnem

spletu (in ker izpolnjujejo vsaj enega od indicev, da s tem usmerjajo aktivnosti v tujino), omejitve iz 15. člena BU počasi izginjajo. Nasprotno namenu evropskega zakonodajalca se bodo potrošniki tako rekoč neomejeno lahko oprli na pristojnost po svojem prebivališču v sporih proti trgovcem. Potrošniku gre vsekakor svetovati, da preden vloži tožbo proti trgovcu, ne glede na način, kako je prišel v stik s tem trgovcem, preveri, ali je prisoten na svetovnem spletu (bodisi z lastno spletno stranjo bodisi prek posrednikov). Če bo odgovor pozitiven (in bodo podani še kakšni indici iz sodbe *Pammer in Hotel Alpenhof*), bo potrošnik vzpostavil pristojnost sodišč v svoji državi (in tudi uporabo kogentnih predpisov materialnega potrošniškega prava svoje države). Pri tem pa se ne sme pozabiti, da trgovci niso le velike multinacionalne družbe, za katere je pravdanje v tujini zanemarljivo breme. Za majhne trgovce[39] je pravdanje v tujini lahko veliko breme. Še toliko večje breme pa je nevarnost, da se s tem v skladu s 6. členom Uredbe Rim I (kjer je problematika tako rekoč ista kot v Bruseljski uredbi) izpostavijo kogentnim predpisom potrošniškega prava v tuji državi, ki so morda drugačni kot v njihovi državi.

Glede indicev, ki kažejo, da je trgovec usmerjal aktivnosti specifično (!) v državo prebivališča potrošnika, se lahko kot najbolj problematičen izkaže jezik spletne strani (čeprav je ravno ta na prvi pogled najbolj razumen). Če se bo to stališče SEU razlagalo dobesedno, lahko pripelje do hude diskriminacije tako trgovcev kot tudi potrošnikov iz držav EU z »manjšimi jeziki«. Za trgovca seveda sklep o tem, da usmerja svoje aktivnosti v tujino, pomeni breme izpostavljanja pristojnosti tujih sodišč. Vendar se – glede pogoja jezika – britanski (ali irski) trgovec, čigar internetna stran je v angleščini, temu tveganju ne izpostavi. Vendar ali res drži sklep, da britanski (ali irski) trgovec, ki ima spletno stran v angleščini, ne računa na stranke iz tujine? Ali ne gre morda le za to, da računa, da večina potencialnih tujih strank razume angleško? Britanski trgovec torej lahko (s spletno stranjo v angleškem jeziku) pridobiva tuje stranke, ne da bi se izpostavil pristojnostim tujih sodišč. Na primer za slovenskega trgovca pa to ne velja. S spletno stranjo le v svojem jeziku tujih strank ne bo pridobival. Še bolj problematično je lahko vprašanje jezika kot indica na strani potrošnikov. Le upamo lahko, da SEU stališča, da mora biti iz indicev (tj. med drugim jezika) razvidno, da trgovec usmerja komercialne aktivnosti prav na državo potrošnika, ne razume tako, da obstaja vez le med uporabljenimi tujimi jeziki in državami, v katerih so ti jeziki domači. Hudo diskriminacijo potrošnikov iz držav z »majhnimi jeziki« bi povzročilo, če bi na primer za švedskega trgovca, čigar spletna stran poleg švedskega omogoča še uporabo angleškega, francoskega in nemškega jezika, šteli,

[39] Kot so v obravnavanih primerih brata Yusuffi in Vlado Sabranovic (oziroma samostojna podjetnika firm *Autohaus Yusuffi* in *Vlado Automobiles Import-Export).*

da svoje komercialne aktivnosti usmerja le v države, kjer so ti jeziki domači (tj. v okviru EU v Veliko Britanijo, Irsko, Francijo, Belgijo, Luksemburg, Nemčijo in Avstrijo), ne pa tudi v druge države članice. To bi pomenilo, da le potrošniki iz omenjenih držav švedskega trgovca lahko tožijo v kraju svojega prebivališča, potrošniki iz preostalih držav pa ugodnosti iz Bruseljske uredbe ne bi bili deležni. Takšen sklep ne bi ustrezal resničnosti. Okoliščina, da omenjeni švedski trgovec ne ponuja spletne strani tudi v slovenščini, ne pomeni, da ne računa na stranke iz Slovenije (in drugih držav) – računa pač na to, da bo veliko strank iz Slovenije (in drugih držav) razumelo vsaj enega od omenjenih (zanje tujih) jezikov. Menim, da je zato nujen sklep, da trgovec, ki na spletni strani uporablja (vsaj) angleščino kot jezik, ki je v svetovnem merilu močno razširjen kot tuj jezik, s tem svoje komercialne aktivnosti usmerja v vse tuje države, ne le v države z angleščino kot domačim jezikom.

Literatura

Bogdan, Michael: Contracts in Cyberspace and the Regulation »Rome I«, *Masaryk University Journal of Law and Technology,* 2009, vol. 3:2, str. 219–225.

Dasser, Felix, Oberhammer, Paul: *Lugano-Übereinkommen*, Zweite Auflage, Stämpfli Verlag, Bern 2001.

Galič, Aleš: Mednarodna pristojnost za reševanje potrošniških sporov v pravu EU, v: Seliškar Toš, M. (ur.), *Mednarodna konferenca, Slovensko pravo in gospodarstvo ob vstopu Slovenije v Evropsko unijo*, Pravna fakulteta, Ljubljana 2004, str. 125.

Giuliano, Mario, Lagarde, Paul: Report on the Convention on the law applicable to contractual obligations by Mario Giuliano, Professor, University of Milan, and Paul Lagarde, Professor, University of Paris I. *Official Journal C 282,* 31. 10. 1980, str. 0001–0050.

Hess, Burkhard: *Europäisches Zivilprozessrecht*, C. F. Müller Verlag, Heidelberg, 2010.

Mankowski, Peter: Muss zwischen ausgerichteter Tätigkeit und konkretem Vertrag bei Art. 15 Abs. 1 lit. c EuGVVO ein Zusammenhang bestehen? (OLG Karlsruhe, S. 348), *IPRax*, 2008, št. 4, str. 333–334.

Mankowski, Peter: Neues zum »Ausrichten« unternehmerischer Tätigkeit unter Art. 15 Abs. 1 lit. c EuGVVO (BGH); *IPRax*, 2009, št. 3, str. 258–259.

Mayr, Peter: *Europäisches Zivilprozessrecht*, Facultas wuv, Dunaj, 2011.

Možina, Damjan: Internet in varstvo potrošnikov v mednarodnem zasebnem pravu. *Pravnik*, 2000, let. 55, št. 4-5, str. 321–345.

Rauscher, T.: *Europäisches Zivilprozess- und Kollisionsrecht, Kommentar,* Brüssel I-VO, LugÜbk 2007, Sellier, München, 2011.

Ruehl, Giesela: CJEU rules on Art. 15 (1) lit. c) Brussels I-Regulation, Conflict of Laws blog, posted: October 19, 2013, objavljeno na: http://conflictoflaws.net/2013/cjeu-rules-on-art-15-1-lit-c-brussels-i-regulation (30. 12. 2013).

Simons, Thomas, Hausman, Rainer: *Brüssel I – Verordnung, unalex Kommentar, Deutsche Sprachausgabe*, IPR Verlag, München 2012.

Mednarodna pristojnost in kolizijsko pravo EU za internetne kršitve zasebnosti in osebnostnih pravic

dr. Jerca Kramberger Škerl

1. Uvod

Kršitve pravice do zasebnosti in osebnostnih pravic, to že v izhodišču občutljivo materialnopravno področje, so postale z razvojem množičnih medijev, kot so časopisi in televizija, tudi velik problem mednarodnega zasebnega prava. Za temeljna vprašanja, ki si jih ta pravna veja zastavlja, torej v kateri državi naj se vodi postopek, katero pravo naj se uporabi in v katerih državah lahko sodbe učinkujejo, so bile že sprejete različne bolj ali manj posrečene rešitve in predlogi rešitev.

Nato pa je prišel internet in problematika je postala še kompleksnejša. Naenkrat je mogoče izjave in mnenja (brezplačno) objavljati hkrati po vsem svetu (z vse boljšimi spletnimi prevajalniki tudi jezik več ni problem), bistveno olajšano je tudi »deljenje« oziroma posredovanje informacij prek spleta, poleg potencialnega občinstva pa se je močno razširil tudi krog potencialnih storilcev dejanj, ki posegajo v človekovo osebno sfero. To niso več samo identificirane (vsaj urednikom znane) osebe, ki so se »prebile« skozi uredniško politiko različnih medijev in za katere v materialnih pravih posameznih držav obstajajo jasna pravila o odgovornosti za povzročeno škodo. Na internetu lahko objavlja vsakdo, celo skrit za psevdonimom, kar ob pomanjkanju izobrazbe glede potencialnih pravnih problemov in ob nejasnih ali neobstoječih sankcijah privede do eksponentnega povečanja števila žaljivih izjav in razširjanja dejstev iz posameznikove zasebnosti. Vse več je tako tožb zoper blogerje in osebe, ki so sporne vsebine objavljale na socialnih omrežjih, na primer Facebooku in Twitterju.[1]

Krog storilcev se ne širi le številčno, temveč bi lahko rekli, da nastajajo nove kategorije storilcev. S tem vprašanjem se sicer mednarodno zasebno pravo ne ukvarja, njegova pravila se namreč načeloma uporabljajo enako za uveljavljanje zahtevkov zoper kateregakoli odškodninskega zavezanca – te določa materialno pravo, ki ga je treba v konkretnem primeru uporabiti. Kljub temu lahko krog

[1] Glej na primer Ardia.

pravno priznanih storilcev vpliva na tožnikovo odločitev o izbiri foruma, saj bo ta nato odločilna za izbiro materialnega prava, ki ga je treba uporabiti. Za ponazoritev naj omenim, da se poleg sodb zoper avtorje in urednike spletnih strani že pojavljajo sodbe zoper lastnike spletnih iskalnikov, ki med rezultati iskanja ponujajo sporne vsebine (čeprav se ponujene vsebine generirajo avtomatično, brez posameznikovega nadzora)[2] ali pa s takimi vsebinami samodejno dopolnjujejo iskalne nize (*auto-completion*), kar je odvisno od tega, kaj so ljudje največkrat vpisali kot iskalni niz, ki se začne z enako besedo (in ne glede na to, kaj bi določena oseba, urednik, določila kot pomembno, v javnem interesu ipd.).[3] V Združenem kraljestvu je sodišče sprejelo svojo pristojnost v sporu zoper Google s sedežem v ZDA zaradi kršitve pravice do zasebnosti, ker je podjetje na podlagi zbiranja podatkov o posameznikovi uporabi spletnih aplikacij oblikovalo reklamne ponudbe, ki jih je nato predvajalo na njegovih napravah.[4] Oktobra 2013 je Evropsko sodišče za človekove pravice (v nadaljevanju ESČP) razsodilo, da lastnik novičarske spletne strani odgovarja tudi za žaljivo vsebino, ki jo v komentarjih pod posameznimi članki objavijo anonimni komentatorji.[5] Februarja 2014 je bila zadeva sicer predana v odločanje velikemu senatu, tako da omenjena sodba ni dokončna.

Poleg težavnega odkrivanja storilcev in uveljavljanja njihove odškodninske odgovornosti tudi kontinentalno pojmovanje civilne odškodnine kot satisfakcije oškodovancu (medtem ko anglosaški sistemi omogočajo tudi t. i. kaznovalne odškodnine) ne pripomore k večji skrbnosti potencialnih storilcev. To pojmovanje je problematizirano v številnih nacionalnih pravih evropskih držav in nekatere so v primeru kršitev osebnostnih pravic od njega vsaj delno odstopile (ali pa to nameravajo).[6]

---

[2] Nekdanji šef Formule 1 Max Mosely je s tako tožbo uspel zoper Google.fr v Franciji (Tribunal de grande instance, Pariz, sodba z dne 6. 11. 2013) in zoper Google.de v Nemčiji (Landgericht Hamburg, sodba z dne 24. 1. 2014).

[3] Nemško zvezno vrhovno sodišče je maja 2013 razsodilo, da upravljavec (nem. *Betreiber*) spletnega iskalnika ni odgovoren, dokler ga oškodovanec ne opozori na samodejno dopolnjevanje, ki krši njegovo pravico do zasebnosti; ko pa ga oškodovanec na to opozori, mora upravljavec tako samodejno dopolnjevanje preprečiti, sicer je odškodninsko odgovoren. Glej Bundesgerichtshof, sodba št. VI ZR 269/12 z dne 14. 5. 2013.

[4] Tožniki so trdili, da ni sporno le zbiranje podatkov, temveč prikazane ponudbe te njihove podatke razkrivajo, da jih lahko vidijo tudi tretje osebe, ki bi gledale ali uporabljale iste naprave. Britansko sodišče je sprejelo svojo pristojnost za tožbo britanskih tožnikov zoper Google s sedežem v ZDA (Google.uk ni bil vpleten), zato sodišče ni uporabilo uredbe Bruselj I. Lahko bi torej uporabilo doktrino *forum non conveniens*, vendar je menilo, da to ne bi bilo utemeljeno. Glej High Court, *Vidal-Hall and Others v Google Inc* [2014] EWHC 13 (QB).

[5] ESČP, *Delfi AS proti Estoniji*, sodba z dne 10. 10. 2013. Podrobneje o sodbi in njenemu vplivu na slovensko pravo glej Mežnar 2013, str. 6–8. Zanimivo je, da je sodišče menilo, da je medij odškodninsko odgovoren, čeprav je žaljive komentarje po oškodovančevem opozorilu nemudoma umaknil.

[6] Obširno o tem vprašanju v slovenski teoriji Mežnar 2008 in Mežnar 2006.

Prek interneta je mogoče povzročiti škodo tudi s kršitvami drugih pravnih pravil, predvsem prava intelektualne lastnine in konkurenčnega prava. Zaradi razpršenosti škode je takšna povzročitev škode primerljiva tudi na primer z okoljsko škodo. Vendar pa se problematika kršitev osebnostnih pravic in pravice do zasebnosti od vseh naštetih primerov tudi pomembno razlikuje, zato jo je treba obravnavati ločeno.

V nadaljevanju obravnavam rešitve prava Evropske unije (v nadaljevanju EU) s področja mednarodne pristojnosti in kolizijskega prava v primerih kršitev zasebnosti in osebnostnih pravic prek interneta. Kot zanimivost pa velja omeniti, da se je obravnavana tematika kršitev osebnostnih pravic in zasebnosti pokazala za problematično tudi na tretjem klasičnem področju mednarodnega zasebnega prava, torej pri priznanju in izvršitvi tujih sodnih odločb. Če navedem le najočitnejši primer: številne države, ki ne poznajo civilnih odškodnin s kaznovalnim ali preventivnim namenom, so zadržane pri priznavanju in izvrševanju tujih sodb, ki take odškodnine prisojajo. Nemalokrat je učinkovanje tuje sodbe (delno) zavrnjeno na podlagi pridržka javnega reda, saj gre za trk temeljnih pravic do svobode izražanja in pravice do zasebnosti oziroma človekovega dostojanstva, ki ju države skušajo uravnotežiti na različne načine. Na ravni EU se je zadrega jasno pokazala pri sprejemanju prenovljene uredbe Bruselj I, ki naj bi po predlogu Komisije EU (v nadaljevanju Komisija) odpravila možnost zavrnitve izvršitve sodne odločbe iz druge države članice na podlagi razlogov t. i. vsebinskega javnega reda (kamor bi lahko spadala tudi zavrnitev izvršitve kaznovalnega dela civilne odškodnine). Komisija je namreč v predlogu iz tega mehanizma želela izvzeti prav sodbe v sporih zaradi kršitev osebnostnih pravic in zasebnosti (ter sodbe na podlagi t. i. skupinskih tožb).[7] V končnem besedilu prenovljene uredbe, sprejete leta 2012,[8] je bil uzakonjen enak režim za vse civilne in gospodarske sodbe, pridržek javnega reda pa je ostal nedotaknjen.

2. Forum shopping in libel tourism

Pred obravnavo mednarodne pristojnosti in kolizijskih pravil za navedene kršitve je treba pojasniti pojma *forum shopping* (»trgovanje s sodišči«) in *libel tourism* (»obrekovalni turizem«), ki se pogosto pojavljata v diskusijah o iskanju najboljših pravil.

[7] Predlog Uredbe Evropskega parlamenta in Sveta o pristojnosti in priznavanju ter izvrševanju sodnih odločb v civilnih in gospodarskih zadevah (Prenovitev), Bruselj, 14. 12. 2010, COM(2010) 748 končna, točka a tretjega odstavka 37. člena.

[8] T. i. uredba Bruselj I bis: Uredba (EU) št. 1215/2012 Evropskega parlamenta in Sveta z dne 12. decembra 2012 o pristojnosti in priznavanju ter izvrševanju sodnih odločb v civilnih in gospodarskih zadevah (prenovitev), UL L 351 z dne 20. 12. 2012.

Izraz *forum shopping*, ki se je tudi v slovenski teoriji uveljavil v angleški različici, pomeni premišljeno tožnikovo izbiro enega od pristojnih sodišč, pred katerim si lahko obeta najlažje in najuspešnejše pravdanje. Glede predvidenega uspeha v pravdi bo najpomembnejše ugotoviti, katero materialno pravo bo določeno sodišče uporabilo. Če ima tožnik po veljavnih predpisih izbiro, mu seveda ne moremo očitati, da je ravnal nedopustno, če se je vnaprej pozanimal, kje bo imel največ koristi. Nasprotno, bilo bi neodgovorno, če tega ne bi storil. Vendar pa nastane težava, če se rezultat tega premisleka preveč oddalji od temeljnega namena zakonodajalca, ki ni uzakonil več pristojnosti zato, da bi tožnik lahko izbiral po svojih osebnih preferencah, temveč zato, da bi bili vključeni vsi forumi, ki bi lahko bili s sporom v najtesnejši zvezi, in bi bilo tako postopek predvsem zaradi bližine dokazov tam najlažje izpeljati.[9] Pri tem ne smemo pozabiti, da je pristojnost po kraju škodnega dogodka, ki se uporablja za civilne delikte, posebna pristojnost, ki je izjema od splošne pristojnosti po prebivališču toženca, zato bi jo bilo treba razlagati restriktivno.[10] Anglosaški sistemi se takim težavam skušajo izogniti z uporabo instituta *forum non conveniens*, ki pristojnemu sodniku omogoča, da zavrne svojo pristojnost, če meni, da bi bilo bolje, da o konkretnem sporu odloča drugo sodišče. T. i. kontinentalni pravni sistemi tega instituta ne poznajo, prav tako pa ga zaradi zagotavljanja predvidljivosti Sodišče EU (v nadaljevanju SEU) ne dovoli pri uporabi uredbe Bruselj I.[11]

Izraz *libel tourism* ima podoben pomen, ki pa se nanaša neposredno na tožbe zaradi obrekovanja – tožnik, žrtev obrekovanja, toži v državi, kjer si lahko obeta najboljši rezultat postopka, torej zmago v sporu in čim višjo odškodnino. Po »prijaznosti« do tožnikov v primerih obrekovanja sta dolgo slovela Anglija in Wales, zato so tožniki v razmerjih s tujim elementom izbirali njuna sodišča, če so le imeli to možnost.[12] Angleško pravo je bilo namreč do žrtev takih dejanj zelo zaščitniško in je zato poželo številne mednarodne kritike. Ker je bila omenjena praksa tudi v Angliji in Walesu zaznana kot problematična, se je zakonodajalec odločil, da je čas za prenovitev prava varstva osebnostnih pravic. Leta 2013 je sprejel novi Zakon o obrekovanju (*Defamation Act*), ki je začel veljati januarja 2014 in se uporablja za kršitve, storjene po tem datumu.[13] Prehodno obdobje, ko

[9] Glej na primer Ten Wolde, Knot, Weller, str. 254, 255.

[10] Prav tam, str. 255.

[11] SEU, C-281/02, *Andrew Owusu proti N. B. Jacksonu*, z dne 1. 3. 2005.

[12] Znana je na primer zadeva *Berezovsky proti Michaels* [2000] UKHL 25; [2000] 1 WLR 1004; [2000] 2 All ER 986; [2000] EMLR 643, v kateri je House of Lords (nekdanje vrhovno sodišče Združenega kraljestva) dovolilo tožbo ruskih tožnikov zoper ameriško revijo pred sodiščem v Londonu, čeprav je bila ogromna večina naročnikov revije iz ZDA, domnevno žaljive izjave pa so se nanašale na dejavnosti tožnikov v Rusiji.

[13] Zakon je dostopen na primer na spletni strani http://www.legislation.gov.uk/ukpga/2013/26/contents/enacted (22. 3. 2014).

angleška sodišča uporabljajo staro zakonodajo, še vedno traja, vendar se bo sčasoma končalo. Novi zakon uvaja strožje materialnopravne pogoje za uveljavljanje odškodninske odgovornosti, ureja pa tudi mednarodno pristojnost za take spore. Določa namreč, da se, zunaj uporabe uredbe Bruselj I in Luganske konvencije, angleško sodišče lahko izreče za pristojno v sporu zoper tujega toženca le, če je očitno, da je najprimernejše, da v tem sporu izmed vseh sodišč v državah, kjer je bila žaljiva izjava objavljena, odloči ravno to sodišče.[14]

Znan je tudi primer (kazenske) tožbe izraelske znanstvenice Karine Calvo-Goller zoper urednika spletnega pravnega časopisa European Journal of International Law Josepha H. H. Weilerja, ker je bil zavrnjen umik nelaskavega komentarja njene knjige na spletnem portalu tega časopisa (pri čemer dr. Weiler ni bil avtor tega komentarja). Ker ima tožnica tudi francosko državljanstvo, obdolženec pa je imel v času vložitve tožbe stalno prebivališče v ZDA (tožnica je sicer izbrala kazenski pregon namesto civilne tožbe, vendar tudi za civilne tožbe obstaja pristojnost francoskih sodišč za tožbe, ki jih sprožijo francoski državljani),[15] je po francoskem pravu lahko postopek sprožila v Franciji. Sodišče je njeno ravnanje tudi na podlagi njene lastne razlage, da je to sodišče izbrala, da bi imela s postopkom najmanj stroškov, da bi hitro prišla do sodbe in ker je menila, da z zahtevkom lahko uspe samo v Franciji, ocenilo kot tipični *forum shopping* in *libel tourism*, torej kot zlorabo pravic, in je tožbo zavrglo, obdolžencu pa celo prisodilo odškodnino.[16]

Večina držav v svoji zakonodaji pozna pridržek javnega reda, s katerim se lahko onemogočita priznanje in izvršitev sodbe iz države, ki bi za odločanje v sporu uporabila pravila, nezdružljiva s temeljnimi načeli države, v kateri se zahteva učinkovanje te sodbe. Vendar pa je javni red pravni standard, ki ga sodišče napolni v vsakem konkretnem primeru, in je pogosto nemogoče z gotovostjo trditi, kako bo sodišče odločilo. Zato je zanimiv odziv Združenih držav Amerike na pojav *libel tourism*. V tej državi je svoboda govora izredno močno zavarovana[17] in se ji na primer (donedavni) angleški standardi za odškodninsko odgovornost zaradi obrekovanja zdijo do storilca odločno prestrogi. Zaradi tega ZDA niso

[14] Defamation Act, 9. člen.

[15] Francoski Civilni zakonik v 14. členu sicer dobesedno določa pristojnost francoskih sodišč za francoske tožnike v pogodbenih zadevah, vendar je Kasacijsko sodišče to pravilo razširilo na skoraj vse vrste tožb, tudi tožbe glede neposlovne odškodninske odgovornosti. Prvi civilni senat, sodba z dne 27. 5. 1970, *Weiss*, št. 68-13643.

[16] Vse informacije o poteku postopka in besedilo sodbe so dostopni na primer na spletni strani http://www.ejiltalk.org/in-the-dock-in-paris-%E2%80%93-the-judgment-by-joseph-weiler-2/ (21. 3. 2014).

[17] Prelomen primer pri vzpostavljanju strogih standardov za tožbe javnih oseb je bil *New York Times Co. proti Sullivan*, 376 U.S. 254 (1964).

pretirano priljubljen forum za obravnavane tožbe in tožniki so pogosto tožili na primer v Angliji, nato pa želeli priznati in izvršiti sodbo v ZDA. Leta 2008 je nato država New York (čeprav je bil že uzakonjen »splošni« pridržek javnega reda) sprejela zakon, popularno poimenovan kar Zakon za zaščito pred obrekovalnim terorizmom (The Libel Terrorism Protection Act). Ta je ameriškim tožencem, ki so bili zaradi obrekovanja toženi v tujini, omogočal, da pridobijo izjavo, da bo morebitna obsodilna sodba tujega sodišča v ZDA neizvršljiva. Sledile so tudi druge zvezne države, leta 2010 pa je predsednik Obama podpisal zvezni Zakon o govoru (The Speech Act). Ta zakon naj bi »preprečeval priznanje in izvršitev tujih sodb glede obrekovanja in nekaterih tujih sodb zoper ponudnike interaktivnih računalniških storitev«.[18]

Nedopustni, fravdulozni *forum shopping* (torej taka izbira sodišča, ki lahko pomeni zlorabo pravic) in *libel tourism* sta problema, ki se ju (ob zavrnitvi instituta *forum non conveniens*) da zajeziti na dva načina. Eden je omejevanje števila potencialno pristojnih sodišč, kar bo opisano v nadaljevanju, drugi, še učinkovitejši, pa je poenotenje kolizijskega prava. Če bo katerokoli od pristojnih sodišč v EU na podlagi poenotene kolizijske norme uporabilo isto materialno pravo, potem tožniki foruma ne bodo več izbirali glede na to, kje se jim obeta največ možnosti za uspeh in hkrati najvišja odškodnina, temveč glede na razloge, ki naj bi sploh upravičevali več možnih pristojnosti, torej glede na to, kje bo postopek (sicer še vedno predvsem s tožnikovega vidika) procesno lažje izpeljati. Kljub sprejemu uredbe Rim II[19] opisana problematika ostaja pa pri deliktih in kvazideliktih, ki niso zajeti v področje uporabe *ratione materiae* te uredbe. Eno od njih je tudi področje kršitev zasebnosti in osebnostnih pravic. Obstaja pa seveda tudi tretja, najboljša rešitev, vendar se zdi še zelo oddaljena: poenotenje materialnega prava na obravnavanem področju.

3. Mednarodna pristojnost za kršitve osebnostnih pravic prek interneta: uredba Bruselj I

Pravila o mednarodni pristojnosti določajo, v kateri državi se lahko vodi postopek glede določenega spora z mednarodnim elementom. Za stranki je to zelo pomembno. Ne gre samo za praktične razloge, povezane s stroški, časom, znanjem jezika itd., temveč predvsem pravne razloge: pristojno sodišče bo namreč uporabilo svoje kolizijsko pravo, ki mu bo povedalo, katero materialno pravo je treba uporabiti. Nacionalni materialnopravni predpisi pa se razlikujejo, predvsem

[18] O tem razvoju več Little 2013, str. 23–27.

[19] Uredba (ES) št. 864/2007 Evropskega parlamenta in Sveta z dne 11. julija 2007 o pravu, ki se uporablja za nepogodbene obveznosti (»Rim II«), UL L 199 z dne 31. 7. 2007.

na odškodninskopravnem področju so razlike zelo velike že v EU, tako glede temelja odškodninskopravne obveznosti kot glede višine dosojenih odškodnin. Mednarodna pristojnost je tako lahko odločilnega pomena ne le za višino odškodnine, temveč celo za pozitiven ali negativen izid spora za posamezno stranko.

V EU mednarodno pristojnost sodišč držav članic ureja Uredba št. 44/2001 o pristojnosti in priznavanju ter izvrševanju sodb v civilnih in gospodarskih zadevah, t. i. uredba Bruselj I.[20] V tretjem odstavku 5. člena ta uredba določa tudi mednarodno pristojnost v sporih zaradi neposlovne odškodninske odgovornosti. Omenjena določba pa se ne omejuje le na mednarodno pristojnost (kot je to pri pravilih o mednarodni pristojnosti običajno in velja tudi za večino določb uredbe Bruselj I), temveč določa tudi krajevno pristojnost in s tem izključuje uporabo nacionalnih predpisov o krajevni pristojnosti.[21] Enako določbo vsebuje v drugem odstavku 7. člena tudi prenovljena uredba, t. i. uredba Bruselj I bis, ki se bo začela uporabljati 10. januarja 2015.[22]

Podobno kot slovenski Zakon o mednarodnem zasebnem pravu in postopku (ZMZPP)[23] tudi uredba Bruselj I določa izbirno pristojnost po kraju škodnega dogodka. Pravi namreč, da je oseba s stalnim prebivališčem v državi članici lahko tožena v drugi državi članici v zadevah v zvezi z delikti ali kvazidelikti »*pred sodišči kraja, kjer je prišlo ali kjer grozi škodni dogodek*«.[24] Pristojnost zaradi nepogodbene odškodninske odgovornosti je izbirna,[25] kar pomeni, da je tožniku na voljo poleg splošne pristojnosti po stalnem prebivališču toženca iz 2. člena uredbe Bruselj I.[26]

Določba tretjega odstavka 5. člena uredbe se uporablja za vse spore v zvezi z nepogodbeno odškodninsko odgovornostjo – ker se razlaga pojmov delikt in kvazidelikt v posameznih državah razlikuje, domet obravnavane določbe avtonomno določa SEU. To šteje, da gre za delikte ali kvazidelikte vedno, kadar se uveljavlja toženčeva odgovornost, ki ni vezana na pogodbo (tudi pojem pogodbe

[20] Uredba Sveta (ES) št. 44/2001 z dne 22. decembra 2000 o pristojnosti in priznavanju ter izvrševanju sodnih odločb v civilnih in gospodarskih zadevah, UL L 12 z dne 16. 1. 2001.

[21] O tem podrobneje Galič, str. 10. Napačno je Višje sodišče v Ljubljani štelo, da omenjeni člen uredbe ureja le mednarodno in ne tudi krajevne pristojnosti: sklep VSL I Cp 3289/2010 z dne 2. 2. 2011 (šlo je za kršitev osebnostnih pravic s tujo televizijsko oddajo, predvajano v Sloveniji).

[22] Uredba (EU) št. 1215/2012 Evropskega parlamenta in Sveta z dne 12. decembra 2012 o pristojnosti in priznavanju ter izvrševanju sodnih odločb v civilnih in gospodarskih zadevah (prenovitev), UL L 351 z dne 20. 12. 2012.

[23] Uradni list RS, št. 56/99 in 45/08.

[24] Navedena je uradna različica besedila, ki bi se pravilneje glasila: »*pred sodišči kraja, kjer se je zgodil ali kjer grozi škodni dogodek*«.

[25] Da je pristojnost izbirna oziroma posebna (izraza sta na področju pristojnosti sinonima), izhaja iz naslova Oddelka 2 (Posebne pristojnosti), v katerega spada 5. člen.

[26] Tožnik se lahko torej še vedno odloči, da bo vso nastalo škodo uveljavljal pred sodiščem v državi toženčevega stalnega prebivališča.

SEU avtonomno razlaga v okviru prvega odstavka 5. člena).[27] Mednje spadajo tudi spori zaradi kršitve zasebnosti ali osebnostnih pravic.[28] Nacionalna sodišča držav članic so tretji odstavek 5. člena uredbe uporabljala tudi za internetne delikte, pravilnost te razlage pa je potrdilo SEU leta 2011.[29]

Vprašanje, ali je sploh prišlo do delikta ali kvazidelikta, je pomembno tako za določitev pristojnosti kot za vsebinsko odločitev o zahtevku – gre za t. i. dvojno relevantno dejstvo (*Doppelrelevante Tatsache*), pri čemer je za določitev pristojnosti dovolj zatrjevanje tožnika, da je bil delikt storjen.[30]

SEU je že v primeru *Bier* iz leta 1976[31] odločilo, da je kraj škodnega dogodka iz tretjega odstavka 5. člena *tako kraj, kjer je bilo storjeno škodno dejanje, kot tudi kraj, kjer je nastala škodna posledica*. Gre torej (kot v ZMZPP, v katerem je to izrecno razvidno že iz besedila določbe prvega odstavka 55. člena) za t. i. *forum loci delicti commissi vel laesionis*. V primeru *Shevill* je SEU zapisalo, da »ta kraja lahko pomenita pomembno povezavo z vidika sodne pristojnosti, saj je glede na okoliščine za vsakega od njiju mogoče ugotoviti zelo koristne razloge za dokazovanje in organizacijo postopka«.[32] Za uporabo tretjega odstavka 5. člena uredbe Bruselj I ni pomembno, kako je delikt storjen – lahko torej tudi po internetu, kot je SEU razsodilo leta 2011.[33] Tretji odstavek 5. člena se izrecno uporablja tudi za grozečo škodo, pri čemer pa je posebej pomembno, da tožnik izkaže, da med forumom in grozečo škodo obstaja tesna vez.[34]

SEU je torej nekatera bistvena vprašanja že rešilo. Še vedno pa sta s stališča tako mednarodne pristojnosti kot uporabe prava pri internetnih deliktih problematični opredelitvi kraja storitve škodnega dejanja in predvsem kraja nastanka škodne posledice, zato podrobneje poglejmo razvoj teorije in sodne prakse v zvezi s tema dvema naveznima okoliščinama.

---

[27] SEU, 189/87, *Athanasios Kalfelis proti Bankhaus Schröder in drugim*, z dne 27. 9. 1988. Za vsebinsko presojo dejanja pa je treba nato uporabiti pravo, na katero napotujejo ustrezne kolizijske norme. V zvezi z razmejevanjem med pogodbenimi in deliktnimi obveznostmi je SEU pred kratkim izdalo novo pomembno sodbo: SEU, C-548/12, *Brogsitter proti Fabrication de Montres Normandes EURL*, z dne 13. 3. 2014.

[28] SEU, C-68/93, *Shevill in drugi proti Presse Alliance SA,* z dne 7. marca 1995.

[29] SEU, združeni zadevi C-509/09 in C-161/10, *eDate Advertising GmbH proti X* in *Olivier Martinez in Robert Martinez proti MGN Limited*, z dne 25. 10. 2011; sodna praksa nacionalnih sodišč držav članic EU navedena na primer v Ten Wolde, Knot, Weller, str. 260, opomba 56.

[30] O tem več Galič, str. 24, 25.

[31] SEU, 21/76, *Handelskwekerij G. J. Bier BV proti Mines de potasse d'Alsace SA*, z dne 30. 11. 1976.

[32] SEU, C-68/93, *Shevill in drugi proti Presse Alliance SA*, z dne 7. marca 1995, točki 20 in 21.

[33] SEU, združeni zadevi C-509/09 in C-161/10, *eDate Advertising GmbH proti X* in *Olivier Martinez in Robert Martinez proti MGN Limited*, z dne 25. 10. 2011.

[34] Ten Wolde, Knot, Weller, str. 255.

3.1. Kraj storitve škodnega dejanja

Pri internetnih deliktih določitev kraja storitve škodnega dejanja povzroča nekaj težav, vendar drugače kot pri kraju nastanka škodne posledice potencialnih krajev škodnega ravnanja ni nešteto in je to navezno okoliščino zato lažje opredeliti.

Kljub temu je potreben dogovor, kateri kraj se bo štel za kraj delovanja storilca. Pri tiskanih medijih je to glede na sodbo SEU v že omenjenem primeru *Shevill* kraj, kjer ima sedež založba, ki časopis izdaja. Pri internetu bi bil ustreznica sedeža založbe lahko kraj, kjer stoji strežnik, prek katerega so sporne vsebine dostopne javnosti, ker pa je to lahko kjerkoli na svetu (in lahko nepredvidljivo oziroma neznano tudi za storilca), taka navezna okoliščina za pristojnost ni ustrezna. Tako je leta 2012 odločilo SEU v zadevi *Wintersteiger*.[35] Strinjati se je treba z mnenjem, da je kot kraj škodnega dejanja primerneje določiti kraj, kjer je dejansko (fizično) deloval storilec, torej kraj, kjer je bil storilec, ko je sporno vsebino naložil na splet.[36] Ni torej pomembno, kje je storilec sporno vsebino izdelal oziroma sestavil ali kje je bila izdelana internetna stran, na kateri je storilec vsebino objavil.[37] Ker je pogosto težko ugotoviti, kje je bil storilec v trenutku nalaganja na internet, pa teorija predlaga določitev ovrgljive domneve, da je storilec ravnal v kraju svojega prebivališča oziroma sedeža.[38] Če je tožen upravitelj internetne strani, ki je po materialnem pravu lahko tudi odškodninsko odgovoren, se za kraj škodnega dejanja spet šteje sedež ali prebivališče toženca.[39]

3.2. Kraj nastanka škodne posledice

Pri internetnih deliktih je predvsem težko določiti kraj nastanka škode oziroma, bolje rečeno, razumno omejiti nabor pravno relevantnih krajev nastanka škode. Gre namreč za t. i. razpršene delikte (nem. *Streudelikte*),[40] pri katerih škoda nastane na več različnih krajih hkrati, v primeru interneta govorimo kar o vseprisotnosti oziroma ubikviteti nastale škode. Kje bo škoda dejansko nastala, večinoma tudi ni pod storilčevim nadzorom (odvisno je od tega, kdo bo dostopal do spornih vsebin, kako se bodo širile po internetu s pošiljanjem povezav, citiranjem itd.).

---

[35] SEU, C-523/10, *Wintersteiger AG proti Products 4U Sondermaschinenbau GmbH*, z dne 19. 4. 2012, točka 36.

[36] Glej na primer Možina 2002, str. 516–517, Ten Wolde, Knot, Weller, str. 269 in tam navedeni avtorji.

[37] Možina 2002, prav tam.

[38] Možina 2002, str. 517.

[39] Ten Wolde, Knot, Weller, str. 269.

[40] Glej na primer Ten Wolde, Knot, Weller, str. 255.

Zaradi posebnosti interneta (internet je tudi bistveno drugačen medij od na primer časopisov in televizije) se je torej že zgodaj zastavilo vprašanje, ali pri internetnih deliktih za utemeljitev mednarodne pristojnosti v določeni državi ne bi bilo treba postaviti še kakšnega dodatnega kriterija. Po kriterijih, ki se uporabljajo za »običajne« delikte, bi namreč lahko bila pristojna sodišča vseh držav sveta, kar pa gotovo ni v skladu z načeli, ki jim pri določanju mednarodne pristojnosti sicer sledi pravo. Ta načela so predvidljivost (tako za storilca kot za oškodovanca),[41] koneksiteta[42] (povezanost sodišča s škodnim dogodkom in posledico, a tudi bližina dokazov, možnost izvršitve sodbe itd.), preprečevanje zlorabe procesnih pravic (v tem kontekstu sta se mednarodno uveljavila obrazložena izraza *forum shopping* in *libel tourism*).

Delno se je obravnavana problematika seveda izrazila že pri tiskanih medijih in televiziji. V nekaterih nacionalnih sodnih praksah se je že v sedemdesetih in osemdesetih letih razvil *koncept usmerjenega razširjanja*: če je storilec lahko predvidel, da bodo v neki državi nastale posledice njegovega ravnanja, potem so za obravnavo tega ravnanja pristojna sodišča te države.[43] Tudi pri informacijah, objavljenih na internetu, bi se lahko spraševali o usmerjenem razširjanju – iz vsebine, jezika ipd. bi se pogosto dalo razbrati ciljno občinstvo za posamezne vsebine. Vendar pa teorija opozarja, da kriterij ni splošno uporaben. Primer, v katerem ta kriterij ni ustrezen, je denimo internetna stran v angleščini z informacijami, ki zanimajo širši krog ljudi.[44]

Znana je tudi teorija t. i. globalne škode. Po 13. členu Dunajske konvencije o odgovornosti tretjim na področju jedrske energije[45] so pristojna le sodišča v

[41] Enajsta uvodna izjava k uredbi Bruselj I določa: »Pravila o pristojnosti morajo biti čim bolj predvidljiva in morajo temeljiti na načelu, da se pristojnost praviloma določa po stalnem prebivališču toženca, pri čemer mora taka pristojnost vedno obstajati, razen v nekaterih točno opredeljenih primerih, v katerih je zaradi predmeta pravde ali avtonomije strank upravičena druga navezna okoliščina […]« Glej tudi na primer SEU, C-256/00, *Besix SA proti Wasserreinigungsbau Alfred Kretzschmar*, z dne 19. 2. 2002 (obveznost opustitve), in SEU, C-168/02, *Rudolf Kronhofer proti Marianne Maier in drugim*, z dne 10. 6. 2004 (relevantnost prvega kraja, kjer je nastala škoda, in ne vseh nadaljnjih krajev, kjer oškodovanec trpi posledice).

[42] SEU je v že navedenih zadevah *eDate Advertising* in *Martinez* zapisalo: »V skladu z ustaljeno sodno prakso velja, da pravilo o posebni pristojnosti, ki je kot odstopanje od načela določitve pristojnosti na podlagi kraja stalnega prebivališča tožene stranke določeno v členu 5, točka 3, Uredbe, temelji na obstoju posebno tesne zveze med sporom in sodiščem kraja, v katerem je prišlo do škodnega dogodka, ki upravičuje podelitev pristojnosti temu sodišču zaradi učinkovitosti sodstva in načela procesne ekonomije.«

[43] Podrobneje Možina 2002, str. 513, 514.

[44] Podrobneje Možina 2002, str. 519.

[45] Konvencija o odgovornosti tretjim na področju jedrske energije z dne 29. julija 1960, dostopna na primer na spletni strani http://www.iaea.org/Publications/Documents/Conventions/liability.html (22. 3. 2014).

državi, kjer je prišlo do dogodka, zaradi katerega je nastala škoda. Tudi komentatorji tretjega odstavka 5. člena uredbe Bruselj I menijo, da v primeru, ko tožnik uveljavlja t. i. globalno škodo, pristojnost kraja škodne posledice odpade, ostaneta le splošna pristojnost po prebivališču toženca in pristojnost po kraju, kjer je bilo storjeno škodno dejanje.[46] Vendar pa bi bila taka rešitev za internetne kršitve osebnostnih pravic neuravnotežena, saj bi bila preveč v prid storilcu. Kot v zvezi s kolizijsko normo za obravnavane obveznosti opozarja Mežnarjeva, bi lahko z uporabo omenjene teorije povzročili, da bi medijski lastniki sedeže preselili v zanje pravno najugodnejše okolje,[47] s čimer bi neposredno vplivali na mednarodno pristojnost, posredno pa tudi na to, katero materialno pravo bo uporabljeno za obravnavo morebitnih kršitev.

Poleg tega, kot opozarja Galič v zvezi s t. i. čisto premoženjsko škodo (*pure economic loss*),[48] se je tudi pri obravnavanih kršitvah nujno sporazumeti o kraju nastanka škodljive posledice med drugim zato, ker je to običajna navezna okoliščina v kolizijskem pravu. Res je, kot bo pojasnjeno v nadaljevanju, da kolizijske norme za kršitve zasebnosti in osebnostnih pravic v EU še niso poenotene, vendar potekajo priprave na uzakonjenje skupne norme in treba je poskrbeti za čim večjo usklajenost (razlage) zakonodaje o pristojnostih in kolizijskih pravilih.

Vprašanje predvidljivosti nastanka škode na določenem kraju pri internetnih deliktih je deloma retorično: težko je namreč zanikati, da je storilec vedel oziroma moral vedeti, da bo vsebina (razen če jo bo ustrezno zavaroval z gesli ipd.) dostopna po vsem svetu. Vedel je tudi, da sam praviloma ne bo imel vpliva na to, kje bodo ljudje do vsebine dejansko dostopali. Drugače lahko na primer pri časopisih, televizijskih in radijskih oddajah ugotavljamo, kam so bili distribuirani, in lažje ugotovimo, da je na primer časopis le po naključju »zašel« na neki kraj. Kljub temu menim, da se tudi pri internetu lahko sprašujemo o določenem razumnem pričakovanju, kje lahko nastane relevantna škoda in kje ne, in nanj vežemo pravila o pristojnosti, v to smer pa so šla tudi razmišljanja, ki bodo predstavljena v nadaljevanju.

3.2.1. Primer Shevill (1995)

SEU je v prelomnem primeru *Shevill*[49] *iz leta 1995 z razlago Bruseljske konvencije (predhodnice uredbe Bruselj I) v zvezi s kršitvami osebnostnih pravic prek tiska vzpostavilo t. i. mozaični sistem*: toženec lahko uveljavlja odškodnino v vseh

[46] Ten Wolde, Knot, Weller, str. 275.

[47] Mežnar 2004, str. 25.

[48] Galič, str. 20.

[49] SEU, C-68/93, *Fiona Shevill in drugi proti Presse Alliance SA*, z dne 7. 3. 1995.

državah, v katerih je bila publikacija razširjana (gre za t. i. orientacijsko teorijo, ki jo tudi pri internetnih deliktih izrecno upošteva na primer francosko kasacijsko sodišče)[50] in v katerih je tožnik znan, vendar lahko v vsaki državi uveljavlja le škodo, ki je nastala tam, celotno škodo pa lahko uveljavlja v državi toženčevega prebivališča ali v kraju, kjer je bilo storjeno škodno dejanje.

Mozaični sistem je bil gotovo dobrodošel korak v smeri krčenja števila možnih pristojnosti in preprečevanja fravduloznega *forum shoppinga*, ko bi tožnik iztožil celotno škodo v državi, kjer je morda nastal minimalen del škode, vendar pa bo tam uporabljeno zanj najugodnejše materialno pravo.[51] Ker se pravila o odškodninski odgovornosti po državah razlikujejo, je po logiki SEU najbolje vsaki državi prepustiti odločanje o škodi, ki je nastala na njenem ozemlju. Po drugi strani pa teorija opozarja na pomanjkljivosti te rešitve, predvsem na nepraktičnost za tožnika, če bi želel škodo uveljavljati v državah, v katerih je nastala škodljiva posledica, in bi moral tako vložiti več tožb. Avtorji so se spraševali tudi o smiselnosti in možnosti razčlenitve nepremoženjske škode na več delov ter o upravičenosti pogoja, da je moral biti oškodovanec v kraju nastanka škode znan pred spornim dejanjem.[52]

3.2.2. Primera eDate in Martinez (2011)

Očitno je, da je pri internetu pravni problem bistveno večji in tudi dodatna pravila iz primera *Shevill* ne zadostujejo, poleg tega pa ima mozaični sistem že opisane pomanjkljivosti. Do spornih vsebin na internetu drugače kot pri tiskanih medijih lahko praviloma dostopi vsakdo takoj in brezplačno povsod po svetu, zato so lahko tudi posledice kršitev bistveno hujše, kraj nastanka škodne posledice pa je še težje določiti.

SEU se je s problematiko kršitev osebnostnih pravic prek interneta prvič srečalo v zadevah *eDate Advertising* in *Martinez* ter leta 2011 izdalo dolgo pri-

[50] Glej na primer sodbo gospodarskega senata Kasacijskega sodišča, z dne 29. 3. 2011, v zadevi *Ebay Inc, Ebay Europe in Ebay France proti Maceo*. Sodišče je zapisalo, da »dostopnost internetne strani na francoskem ozemlju sama po sebi ni dovolj za utemeljitev pristojnosti francoskih sodišč«, treba je raziskati, ali so bili francoski uporabniki interneta ciljno občinstvo te strani. Znani sta tudi odločbi prvostopenjskega sodišča (Tribunal de grande instance) v Parizu iz leta 2000 (22. 5. in 10. 11.) v primeru *LICRA proti Yahoo! France in Yahoo! Inc.*, v kateri se je sodišče izreklo za pristojno (in uporabilo francosko pravo) tudi zoper ameriškega toženca, saj je svoje zavedanje, da do njegovih strani dostopajo tudi francoski uporabniki spleta, pokazal s tem, da je takrat prikazoval francoske oglase. V ZDA odločb nato ni bilo mogoče izvršiti, saj bi to bilo v nasprotju z ameriškim pojmovanjem pravice do svobode govora.

[51] Tudi če toženec v tej državi nima premoženja, iz katerega bi se tožnik lahko poplačal, je namreč sodbo pogosto mogoče izvršiti v drugih državah, čeprav se rezultat, ki ga je tožnik dosegel v tujini, razlikuje od rezultata, ki bi ga lahko dosegel v meritornem postopku v državi izvršitve.

[52] O tem več Možina 2002, str. 515.

čakovano sodbo, s katero je postavilo nov mejnik pri določanju mednarodne pristojnosti za te delikte.[53] Ugotovilo je namreč, da »se objava vsebine na spletnem mestu razlikuje od razširjanja na določenem ozemlju, kot je med drugim značilno za tiskane medije, ker načeloma pomeni vseprisotnost te vsebine. Do te ima takoj dostop nedoločeno število spletnih uporabnikov po vsem svetu, neodvisno od kakršnegakoli namena objavitelja, da bi bila ta vsebina dostopna zunaj države članice, v kateri ima sedež, in brez njegovega nadzora. Tako se zdi, da splet zmanjšuje uporabnost merila glede razširjanja, ker je domet razširjanja po spletu objavljene vsebine načeloma neomejen. Poleg tega s tehničnega vidika ni vedno mogoče z gotovostjo in zanesljivostjo opredeliti obsega tega razširjanja za vsako državo članico niti posledično oceniti škode, ki je nastala v tej državi članici.«[54]

SEU je zato mozaični sistem nadgradilo tako, da je celotno škodo mogoče uveljavljati tudi (torej poleg države stalnega prebivališča toženca in kraja škodnega dejanja) v kraju, kjer je *težišče spora*, torej težišče konflikta med pravico do informacije in pravico do zasebnosti (navadno tam, kjer ima domnevni oškodovanec središče življenja in aktivnosti), tj. tam, kjer je sporna vsebina »posebej relevantna in so tako tožnikovi interesi tam posebej prizadeti«.[55]

SEU je kraj težišča oškodovančevih interesov opisalo takole: »Okolje, v katerem je težišče interesov neke osebe, je na splošno kraj njenega običajnega prebivališča. Vendar je lahko težišče interesov osebe tudi v državi članici, v kateri običajno ne prebiva, če je na podlagi drugih indicev, kot je opravljanje poklicne dejavnosti, mogoče ugotoviti obstoj posebno tesne povezave s to državo.«[56] Pristojnost sodišča v tem kraju pa je utemeljilo takole: »Pristojnost sodišča kraja, v katerem je težišče interesov domnevne žrtve, je v skladu s ciljem predvidljivosti pravil o pristojnosti […] tudi glede tožene stranke, ker objavitelj škodljive vsebine ob objavi po spletu lahko pozna težišča interesov oseb, ki so predmet te objave. Tako je treba ugotoviti, da merilo težišča interesov tožeči stranki omogoča, da brez

[53] SEU, združeni zadevi C-509/09 in C-161/10, *eDate Advertising GmbH proti X* in *Olivier Martinez in Robert Martinez proti MGN Limited,* z dne 25. 10. 2011.

[54] Točki 45 in 46 sodbe.

[55] Ten Wolde, Knot, Weller, str. 256. SEU je zapisalo, da »[…] lahko v primeru zatrjevane kršitve osebnostnih pravic z vsebino, objavljeno na spletnem mestu, oseba, ki meni, da je oškodovana, vloži tožbo zaradi ugotovitve odgovornosti glede celotne škode bodisi pri sodiščih države članice, v kateri ima objavitelj te vsebine sedež, bodisi pri sodiščih države članice, v kateri je težišče njenih interesov. Ta oseba lahko namesto tožbe zaradi ugotovitve odgovornosti glede celotne škode vloži tudi tožbo pri sodiščih vsake države članice, na ozemlju katere je ali je bila po spletu objavljena vsebina dostopna. Ta sodišča so pristojna za odločanje zgolj glede škode, storjene na ozemlju države članice sodišča, ki odloča.«

[56] Točka 49 sodbe.

težav ugotovi, na katero sodišče se lahko obrne, toženi stranki pa, da razumno predvidi, pred katerim sodiščem je lahko tožena […]«[57]

Še vedno je torej pomembno, da kraja težišča interesov tožnika ne enačimo samodejno s krajem tožnikovega prebivališča,[58] vendar pa je hkrati res, kot priznava tudi SEU, da ta dva kraja najpogosteje sovpadata. Situacija namreč ni enaka kot pri t. i. nadaljevani škodi, na primer nepremoženjski škodi, ki jo oškodovanec utrpi pri prometni nesreči, pri čemer velja, da bo pristojno le sodišče v kraju prometne nesreče in ne morebiti tudi sodišče oškodovančevega prebivališča, kjer je (praviloma) dejansko pretrpel večino telesnih in duševnih bolečin.[59] Škoda zaradi kršitve zasebnosti in osebnostnih pravic namreč nastane v oškodovančevem socialnem in poklicnem okolju. Medtem ko bi poškodovanec enake bolečine trpel kjerkoli, kamor bi po nesreči odšel, pa žrtev kršitve osebnostnih pravic utrpi škodo v domačem okolju in le redko tudi (ali samo) drugje. V tej smeri lahko razumemo tudi kriterij iz zadeve *Shevill*, da mora biti tožnik v kraju, kjer naj bi nastala škoda, znan že pred storjenim deliktom.

Tako kot bo v praksi kraj storitve škodnega dejanja pri internetnih deliktih navadno kar kraj toženčevega prebivališča ali sedeža, bo torej kraj nastanka škodljive posledice najpogosteje kraj tožnikovega prebivališča (ali, če je po materialnem pravu oškodovanec lahko tudi pravna oseba, sedeža).

Vezave pristojnosti za celotno škodo v kraju težišča kršitve si ni izmislilo SEU. Nekateri avtorji so to navezno okoliščino predlagali že pred leti,[60] uporabilo pa jo je že tudi ameriško Vrhovno sodišče v zadevi *Calder proti Jonesu* leta 1984.[61]

---

[57] Točka 50 sodbe.

[58] Pristojnost po kraju tožnikovega prebivališča namreč načeloma velja za pretiran temelj pristojnosti (glej tudi prilogo št. I k uredbi Bruselj I, ki kot pretirano pristojnost opredeljuje 14. in 15. člen francoskega Code civil). O tem podrobneje Galič, str. 17, 18.

[59] Po splošno uveljavljenem pravilu se kot kraj nastanka škode šteje le prvi kraj, kjer je nastala škoda zaradi določenega ravnanja ali dogodka, ne pa tudi vsi nadaljnji kraji, kjer nastanejo nadaljnje posledice. SEU, C-364/93, *Antonio Marinari proti Lloyds Bank plc in Zubaidi Trading Company*, z dne 19. 9. 1995.

[60] Nekateri nemški avtorji, ki so rešitev predlagali v devetdesetih letih 20. stoletja, so navedeni v Možina 2002, str. 520, opomba 53. V slovenski teoriji se je za to rešitev glede mednarodne pristojnosti zavzel Damjan Možina, glej Možina 2002, str. 522, glede kolizijske norme pa se je za kraj običajnega prebivališča oškodovanca v času nastanka kršitve kot kraja nastanka škode zavzela Špelca Mežnar, glej Mežnar 2004, str. 26.

[61] *Calder proti Jones*, 465 U. S. 783 (1984). Sodišče je v sodbi, ki jo je napisal sodnik Rehnquist, zapisalo, da je kalifornijsko sodišče pristojno zato, ker je bil časopis usmerjen h kalifornijskemu občinstvu, ker je storilec (odgovorni urednik časopisa) vedel, da ima oškodovanka prebivališče v Kaliforniji in da bo škoda za njeno kariero nastala v Kaliforniji (v časopisu so zapisali, da je Jonesova alkoholičarka). Zanimivo je, da je Vrhovno sodišče istega leta odločilo tudi v primeru *Keeton proti Hustler Magazine Inc.*, 465 U. S. 770 (1984), v katerem pa je tožnica tožila v zvezni državi, kjer je bil časopis distribuiran, vendar sama tam ni živela (to državo je izbrala le zato, ker je njeno pravo edino določalo dovolj dolg zastaralni rok, da je tožbo še lahko vložila, in ker si je lahko tam obetala

Prav tako ni nova kombinacija mozaičnega sistema in pristojnosti po težišču kršitve, saj je podobno normo vseboval že predlog Haaške konvencije o mednarodni pristojnosti in tujih sodnih odločbah v civilnih in gospodarskih zadevah iz devetdesetih let 20. stoletja, ki je bila projekt Haaške konference o mednarodnem zasebnem pravu.[62] Predlog je sicer drugače kot omenjena sodba SEU vseboval še varovalko, da pristojnost po kraju težišča kršitve ni bila podana, če je bil ta kraj za storilca nepredvidljiv.

V dostopni slovenski sodni praksi je že pred sprejetjem sodbe v primerih *eDate* in *Martinez* leta 2011 Višje sodišče v Ljubljani sprejelo podobno razlago tretjega odstavka 5. člena uredbe.[63] V primeru, ko je šlo za kršitev osebnostnih pravic tožnika s prebivališčem v Ljubljani s televizijsko oddajo, ki je bila prikazana v Sloveniji, kamor je bila (načrtno) distribuirana, se je sodišče sicer sklicevalo na primer *Shevill*, a tudi na omenjeni predlog Haaške konvencije, in zapisalo: »Pravilna pa je razlaga prvostopenjskega sodišča, da je sodišče v Ljubljani pristojno tudi zato, ker je bilo s sporno oddajo po trditvah tožnika poseženo v njegove osebnostne pravice, škodljiva posledica je torej nastala v njegovi zasebni sferi, tj. v kraju njegovega stalnega prebivališča.«

4. Pravo, ki ga je treba uporabiti za kršitve osebnostnih pravic prek interneta: EU na poti k enotni ureditvi

Kolizijsko pravo mora sodniku dati odgovor na vprašanje, katero materialno pravo naj uporabi za rešitev določenega pravnega problema. V nasprotju s pravili o pristojnosti, ki lahko dopuščajo več možnosti, med katerimi bo izbiral tožnik, pa mora kolizijsko pravilo dati enoznačen odgovor – izbira prava, ki ga bo v konkretnem primeru uporabil, namreč ne more biti prepuščena sodnikovi diskreciji.[64]

---

najvišjo odškodnino). Vrhovno sodišče je (spet soglasno) odločilo, da tožnica lahko tam zahteva odškodnino za celotno škodo (tudi tisto, ki je nastala v drugih zveznih državah), ker je bil časopis tam distribuiran. Kljub tej odločitvi se za najpomembnejšo odločitev ameriškega Vrhovnega sodišča šteje primer *Calder* in sodišča še danes sprejemajo svojo pristojnost na podlagi treh kriterijev: (1) toženec je storil dejanje namenoma; (2) dejanje je bilo izrecno usmerjeno v državo sodišča; (3) povzročena je bila škoda, za katero je toženec vedel, da bo verjetno nastala v državi sodišča. Več v: Little, str. 7.

[62] Glej na primer Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters, adopted by the Special Commission and Report by Peter Nygh and Fausto Pocar, avgust 2000, http://www.hcch.net/upload/wop/jdgmpd11.pdf (26. 2. 2014). Zaradi prevelikih težav pri iskanju skupnih rešitev za tako široko pravno področje je bil projekt kasneje (vsaj začasno) opuščen, Haaška konferenca pa se je usmerila v sprejetje Konvencije o sporazumih o pristojnosti iz leta 2005.

[63] Sklep Višjega sodišča v Ljubljani, št. Cp 3289/2010, z dne 2. 2. 2011.

[64] Seveda je mogoča uporaba mehanizmov t. i. posteriorističnega navezovanja, kot sta na primer izključitvena klavzula in pridržek javnega reda, vendar mora biti v predpisu jasno določena hierarhija naveznih okoliščin in pogoji za uporabo navedenih mehanizmov.

Kot je že bilo poudarjeno, ni vseeno, katero pravo se uporabi glede kršitev zasebnosti in osebnostnih pravic. Že na ravni EU, sploh pa širše, namreč države zelo različno določajo, katere pravice so varovane, v kolikšnem obsegu so varovane (tehtanje med svobodo izražanja in pravico do zasebnosti), s katerimi sredstvi, kdo so lahko oškodovanci in kdo storilci ter kakšen je v posameznem pravu namen civilne odškodnine in kolikšna je njena običajna višina. Zato bi bilo še toliko pomembneje, da se v EU določi enotno kolizijsko pravilo za obravnavane kršitve. Kot bo opisano v nadaljevanju, so bila prizadevanja za doseganje soglasja glede ustrezne norme zaenkrat žal neuspešna, tako da sodišča v državah članicah uporabljajo svoja nacionalna kolizijska pravila, ki se med seboj razlikujejo.

Pri tem je treba opozoriti tudi na problem kvalifikacije, ki je v mednarodnem zasebnem pravu pogost. Omenjeno je že bilo, da SEU pojma delikta in kvazidelikta iz tretjega odstavka 5. člena uredbe Bruselj I razlaga avtonomno, torej neodvisno od pravnih redov posameznih držav članic. Ker ni skupnega kolizijskega pravila, pa se lahko zgodi, da bodo sodišča v neki državi pristojna za obravnavo določenega dejanja, ki se po razlagi SEU šteje za delikt, pri uporabi nacionalnih kolizijskih pravil pa se to isto dejanje ne bo štelo za delikt in ne bo uporabljena kolizijska norma za deliktne obveznosti (to je sicer odvisno od načina, na katerega to nacionalno pravo rešuje vprašanje kvalifikacije v mednarodnem zasebnem pravu).[65] Lahko se zgodi tudi, da bo uporabljena kolizijska norma za delikte, vendar materialno pravo, na katero bo norma napotovala, takega dejanja ne šteje za delikt, tako da bo vsebinska presoja temeljila na drugih pravnih pravilih.

Čeprav se zdi poenotenje materialnega prava, ki ureja pravico do zasebnosti in osebnostne pravice, daleč, pa v okviru Sveta Evrope, katerega članice so vse države članice EU, smernice za enotnejšo materialnopravno obravnavo teh pravic določa Evropsko sodišče za človekove pravice (v nadaljevanju ESČP) v svoji sodni praksi s področja 8. (pravica do zasebnosti) in 10. člena (svoboda izražanja) Evropske konvencije o človekovih pravicah (EKČP). Prav tako so obravnavane pravice varovane z Listino EU o temeljnih pravicah. Razlaga posameznih človekovih pravic pred ESČP spada v (mednarodni) javni red držav članic, ki morajo uporabo tujega prava, neskladnega z usmeritvami ESČP, na podlagi pridržka javnega reda (ki ga vsebuje večina nacionalnih zakonodaj) zavrniti (tudi same pa morajo svoje notranje pravo uskladiti s standardi ESČP, če ne želijo tvegati obsodb pred tem sodiščem). Pomemben akt Sveta Evrope je na obravnavanem

[65] Glede problema kvalifikacije v mednarodnem zasebnem pravu glej Cigoj, str. 120–130.

področju tudi Konvencija Sveta Evrope št. 108 o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov iz leta 1981.[66]

V zvezi z internetnimi delikti je treba omeniti še Direktivo EU 2000/31 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju).[67] Določa namreč, da za ponudnika storitev elektronskega poslovanja v drugi državi članici ne smejo veljati strožje zahteve, kot so določene v materialnem pravu, ki velja v državi članici, v kateri ima ta ponudnik sedež.[68] V navedenih primerih *eDate Advertising* in *Martinez* iz leta 2011 je SEU odgovorilo na vprašanje o morebitnem vplivu omenjene direktive na kolizijskopravno urejanje področja internetnih kršitev osebnostnih pravic. Zapisalo je, da je treba »člen 3 Direktive razlagati tako, da ne zahteva prenosa v obliki posebnega kolizijskega pravila. Kljub temu morajo države članice glede koordiniranega področja zagotoviti, da – če ne gre za odstopanja, ki so dovoljena pod pogoji iz člena 3(4) Direktive – za ponudnika storitev elektronskega poslovanja ne veljajo strožje zahteve od tistih, ki so določene v materialnem pravu, ki velja v državi članici, v kateri ima ta ponudnik sedež.«[69] Domača teorija ocenjuje, da gre za »polkompromisno odločitev Sodišča«, ki bo sodiščem povzročala številne težave.[70]

4.1. Uredba Rim II

Na področju kršitev osebnostnih pravic kolizijske norme v EU torej niso poenotene. Uredba (ES) št. 864/2007 o pravu, ki se uporablja za nepogodbene obveznosti, t. i. uredba Rim II,[71] je sicer poenotila kolizijske norme za neposlovne obveznosti, vendar točka g drugega odstavka 1. člena določa, da se uredba ne uporablja za nepogodbene obveznosti, ki izvirajo iz kršitev zasebnosti in osebnostnih pravic, vključno z obrekovanjem.[72] V postopku sprejemanja uredbe se je namreč izkazalo, da je ta tematika preveč problematična, da bi bilo mogoče določiti enotno pravilo.

---

[66] Dostopna na spletni strani http://www.svetevrope.si/sl/dokumenti_in_publikacije/konvencije/108/ (22. 3. 2014).

[67] UL L 178, z dne 17. 7. 2000, str. 0001–0016.

[68] Drugi odstavek 3. člena direktive.

[69] SEU, že navedena sodba v primerih *eDate in Martinez*, št. 68.

[70] Skubic, str. 25.

[71] Uredba (ES) št. 864/2007 Evropskega parlamenta in Sveta z dne 11. julija 2007 o pravu, ki se uporablja za nepogodbene obveznosti (»Rim II«), UL L 199, z dne 31. 7. 2007.

[72] V angleščini: *»non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation«*.

Zanimivo pa je dogajanje, ki je vodilo do tega rezultata. Komisija kot predlagatelj te uredbe si je namreč prizadevala, da bi uredba vsebovala tudi kolizijsko normo za kršitve zasebnosti in osebnostnih pravic, saj je ugotovila, da se kolizijsko pravo držav članic na tem področju zelo razlikuje, poleg tega pa bi bilo treba kolizijsko normo uskladiti z že obstoječimi pravili in sodno prakso SEU v zvezi z uredbo Bruselj I (na primer z rešitvami iz že omenjenih primerov *Mines de Potasse* in *Shevill*). Pri tem pa bi se bilo treba izogniti težavnemu distributivnemu navezovanju, ko bi na primer sodišče v kraju toženčevega stalnega prebivališča, ki bi bilo po uredbi Bruselj I pristojno za celotno škodo, za vsak del škode moralo uporabiti pravo države, v kateri je ta del škode nastal. V leta 2002 objavljenem osnutku predloga nove uredbe[73] je Komisija tako predlagala, da bi se za kršitve zasebnosti in osebnostnih pravic uporabljalo pravo običajnega prebivališča oškodovanca. Ta predlog je imel številne zagovornike,[74] ni pa odveč omeniti, da se ta navezna okoliščina praviloma uporablja tudi v ZDA (kjer pa sodišča sicer sprejemanju pristojnosti zoper tožence iz drugih držav v splošnem niso naklonjena).[75]

Vendar pa je predlog naletel tudi na kritike, predvsem iz dveh razlogov. Pri slavnih osebnostih naj bi bilo včasih težko določiti običajno prebivališče (na primer formalna določitev prebivališča v določeni državi zaradi davčnih razlogov), založniški lobiji pa so ostro ugovarjali predvsem ureditvi, po kateri bi bili lahko v državi svojega sedeža obsojeni za ravnanja, ki so v tej državi sicer dopustna, v državi, katere pravo bi moralo sodišče uporabiti, pa ne.[76]

Tako je Komisija v predlogu uredbe iz leta 2003[77] osnutek spremenila in predlagala, da bi uredba v 6. členu določala, da se za obravnavane kršitve uporabi splošno pravilo, torej pravo države nastanka škodne posledice ali, če imata stranki običajno prebivališče v isti državi, pravo te države ali, če je zadeva tesneje povezana z drugo državo, pravo te druge države. V primeru, ko bi bilo na tej podlagi treba uporabiti pravo, ki bi bilo v nasprotju s temeljnimi načeli foruma glede svobode izražanja in pravice do informacije, pa bi uporabilo pravo foruma. Gre torej za

[73] Dostopen na primer na http://ec.europa.eu/justice/news/consulting_public/rome_ii/news_hearing_rome2_en.htm (21. 3. 2014).

[74] Na primer Hamburg Group for Private International Law, str. 25, ki je hkrati predlagala tudi možnost uporabe izključitvene klavzule (glej str. 14). V Sloveniji na primer Špelca Mežnar, glej Mežnar 2004, str. 26.

[75] O tem več Little, str. 5–18.

[76] Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-contractual Obligations (»Rome II«), Bruselj, 22. 7. 2003, COM(2003) 427 final, Explanatory Memorandum, str. 18.

[77] Predlog je citiran v prejšnji opombi.

izrecno varstvo omenjenih pravic kot dela javnega reda držav članic.[78] Za pravico do odgovora in podobne ukrepe pa bi se uporabilo pravo države, v kateri ima običajno prebivališče tisti, ki je sporno vsebino objavil oziroma razširjal.

Tudi ta predlog je naletel na številne kritike in Komisija je leta 2006 objavila še dodatno spremenjeni predlog.[79] Ugotovila je, da glede kršitev zasebnosti in osebnostnih pravic prek medijev ni mogoč kompromis z amandmaji, ki jih je predlagal Parlament, tako da je bolje te kršitve iz uredbe izključiti, za kršitve, ki niso bile storjene prek medijev, pa naj bi se uporabljalo splošno pravilo o državi nastanka škode.[80] V končnem besedilu uredbe, sprejete leta 2007, pa sta zakonodajalca celo v celoti izključila iz uporabe te uredbe kršitve zasebnosti in osebnostnih pravic, ne glede na to, kako so nastale (točka g drugega odstavka 1. člena).

Ob zavedanju, da je to velika pomanjkljivost uredbe, je evropski zakonodajalec v 30. členu uredbe določil, da mora Komisija najkasneje do decembra 2008 predložiti študijo o razmerah na področju prava, ki se uporablja za nepogodbene obveznosti, izhajajoče iz kršitev zasebnosti in osebnostnih pravic, ob upoštevanju pravil o svobodi tiska in svobodi izražanja v medijih, ter kolizijskopravnih vprašanj v zvezi z Direktivo 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.[81] Že ob sprejetju uredbe je torej bilo predvideno nadaljnje delo v smeri poenotenja kolizijskih pravil tudi na obravnavanem področju.

Na podlagi naročila Komisije je bila leta 2009 izdelana primerjalnopravna študija o pravu, ki se uporablja za kršitve zasebnosti in osebnostnih pravic v državah članicah, ter možnostih za ureditev tega področja na ravni EU.[82] Komisija je na podlagi 30. člena uredbe Rim II avgusta 2012 tudi izdala vprašalnik o uporabi te

[78] Uredba Rim II tudi na splošno ureja pridržek javnega reda v 26. členu, 32. uvodna izjava k uredbi pa celo določa: »Upoštevanje javnega interesa upravičuje, da lahko sodišča držav članic v izjemnih okoliščinah uporabijo izjeme na podlagi javnega reda in prevladujočih obveznih določb. Zlasti uporaba določb prava, kakor to določa ta uredba, ki bi povzročila dodelitev nesorazmerne eksemplarične ali kazenske odškodnine, odvisno od okoliščin primera ali pravnega reda države članice sodišča, kjer je bila vložena tožba, bi lahko veljala za nasprotujočo si z javnim redom (*'ordre public'*) pristojnega sodišča.«

[79] Amended proposal for a European Parliament and Council Regulation on the Law Applicable to Non-contractual Obligations (»Rome II«), COM(2006) 83 final.

[80] Prav tam, Explanatory Memorandum, str. 6.

[81] UL L 281, z dne 23. 11. 1995, str. 31.

[82] Comparative Study on the Situation in the 27 Member States as Regards the Law Applicable to Non-contractual Obligations Arising out of Violations od Privacy and Rights Relating to Personality, JLS/2007/C4/028. Final Report, februar 2009, dostopna na spletni strani http://ec.europa.eu/justice/civil/files/study_privacy_en.pdf (23. 3. 2014).

uredbe v državah članicah, v katerem se eno vprašanje nanaša tudi na nadaljnje ukrepe za ureditev obravnavanega področja v EU.[83]

Aktiven pa je tudi Evropski parlament, ki je maja 2012 sprejel resolucijo, s katero je podal predlog za spremembo uredbe Rim II, tako da bi bila dodana uvodna izjava št. 32a in novi člen 5a.[84] Nova uvodna izjava naj bi se glasila: »Ta uredba ne preprečuje državam članicam, da uporabijo svoja ustavna pravila v zvezi s svobodo tiska in svobodo izražanja v medijih. Zlasti uporaba določb prava, določenega s to uredbo, ki bi povzročila znatno omejitev področja uporabe teh ustavnih pravil, bi lahko glede na okoliščine primera ali pravnega reda sodišča, ki mu je bil primer dodeljen, veljala za nasprotujočo si z javnim redom (*ordre public*) pristojnega sodišča.«

Novi, 5.a člen pa naj bi imel naslov Zasebnost in osebnostne pravice in naj bi določal:

»1. Pravo, ki se uporabi za nepogodbene obveznosti, ki izhajajo iz kršitev zasebnosti ali osebnostnih pravic, vključno z obrekovanjem, je pravo države, v kateri nastopi(-jo) ali bi lahko nastopil(-i) najbolj bistveni element(-i) izgube ali škode.

2. Vendar pa je pravo, ki se uporablja, pravo države, v kateri ima tožena stranka običajno prebivališče, če ta oseba v razumnih okvirih ni mogla predvideti znatnih posledic njenega dejanja v državi, določeni v odstavku 1.

3. Če kršitev izhaja iz objave tiskane publikacije ali oddaje, je država, v kateri nastopi(-jo) ali bi lahko nastopil(-i) najbolj bistveni dejavnik(-i) škode, država, kateri naj bi bila publikacija ali oddaja prvenstveno namenjena, oziroma, če to ni očitno, država, v kateri se izvaja uredniški nadzor, in pravo te države je pravo, ki se uporablja. Država, kateri je publikacija ali oddaja namenjena, se določi zlasti na podlagi jezika publikacije ali oddaje ali na podlagi obsega prodaje oziroma velikosti občinstva v tej državi ali na podlagi deleža celotne prodaje oziroma velikosti občinstva ali na podlagi kombinacije teh dejavnikov.

4. Pravo, ki se uporablja za pravico do odgovora ali podobne ukrepe in za kakršne koli preventivne ukrepe ali sodne prepovedi zoper objavitelja ali predvajalca zaradi vsebine publikacije ali oddaje ali zaradi kršitve zasebnosti ali

[83] Questionnaire to the Member States on the Application of Regulation (EC) No 864/2007 on the Law Applicable to Non-contractual Obligations (Rome II), dostopen na primer na spletni strani http://www.dgpj.mj.pt/sections/relacoes-internacionais/eventos/consultas-publicas/revisao-do-regulamento/downloadFile/attachedFile_f0/Rome_II_questionnaire_-_EN_version.pdf?nocache=1350662648.03 (23. 3. 2014).

[84] Resolucija Evropskega parlamenta z dne 10. maja 2012 s priporočili Komisiji o spremembi Uredbe (ES) št. 864/2007 o pravu, ki se uporablja za nepogodbene obveznosti (Rim II) (2009/2170(INI))

osebnostnih pravic pri obdelavi osebnih podatkov, je pravo države, v kateri ima objavitelj ali predvajalec ali oseba, ki obdeluje podatke, običajno prebivališče.«

Podobno besedilo je Parlament sicer predlagal že kot amandma k predlogu uredbe Rim II iz leta 2003,[85] vendar ga je Komisija takrat zavrnila z utemeljitvijo, da je preveč v korist povzročiteljem škode.[86]

Očitno je torej, da EU ni opustila namena, da tudi na področju kršitev zasebnosti in osebnostnih pravic pride do enotne rešitve, vendar pa v času pisanja tega prispevka še ni jasno, kdaj in na kakšen način bo taka rešitev dosežena. Kakor je mogoče razumeti iz obsežne dokumentacije v zvezi z uredbo, je večji problem kot velike razlike med materialno in kolizijskopravnimi ureditvami tega področja med državami članicami iskanje kompromisne rešitve, ki bo upoštevala tako predvidljivost za potencialne povzročitelje škode kot varnost za oškodovance.

Malo je verjetno, da bi v nadaljevanju procesa sprejemanja novega kolizijskega pravila prišlo do kakšnega revolucionarnega predloga, ki bi zadovoljil vse države in vse vpletene stranke. Kljub temu menim, da je mogoč optimističen zaključek, saj je bil opravljen temeljit in konstruktiven razmislek o obravnavanem vprašanju. Tako razmišljanja o normi o pristojnosti kot še težavnejše iskanje optimalne kolizijske norme (težavnejše zato, ker ni mogoč nabor več enakopravnih norm) pravzaprav vodijo v smer določitve kraja nastanka škode v kraju, kjer je težišče kršitve. S tako navezno okoliščino večinoma pridemo do uporabe kraja oškodovančevega prebivališča, ne da bi se bilo treba ukvarjati s težavami pri odkrivanju in kvalifikaciji oškodovančevega prebivališča. Hkrati rešitev omogoča tudi dovolj fleksibilnosti, da se lahko zadovoljivo rešijo tudi situacije, ko oseba glavnino škode utrpi zunaj kraja svojega prebivanja. Ta rešitev tudi zadovoljivo varuje toženca, saj bo praviloma vedel oziroma bi moral vedeti, kje bo nastala glavnina škode. Kljub temu bi bilo dobro dodati toženčevo možnost dokazovanja, da ni mogel predvideti, kje bo nastalo težišče škode.[87] Toženec bo s tem ugovorom predvidoma redko uspel (dokazno breme bi vsekakor moral nositi on), seveda pa se zastavlja vprašanje, katero pravo naj se uporabi, kadar bi mu uspelo dokazati, da je bil kraj težišča nastanka škode zanj nepredvidljiv. Naj bo to avtomatično pravo države storilčevega sedeža ali pa je mogoče najti boljšo rešitev?

[85] Stališče Evropskega parlamenta, sprejeto na prvi obravnavi dne 6. julija 2005 z namenom sprejetja Uredbe (ES) št. .../2005 Evropskega parlamenta in Sveta o pravu, ki se uporabi za nepogodbene obveznosti (»Rim II«), P6_TC1-COD(2003)0168.

[86] Pojasnilo komisije glede amandmaja št. 57 v navedenem spremenjenem predlogu uredbe Rim II iz leta 2006.

[87] S tem se pravzaprav na področju kolizijskega prava približujemo rešitvi iz omenjenega predloga Haaške konvencije o mednarodni pristojnosti in tujih sodnih odločbah v civilnih in gospodarskih zadevah.

Strahovi potencialnih tožencev so omiljeni tudi s pridržkom javnega reda, tako na podlagi uredbe Rim II kot na podlagi uredb Bruselj I in Bruselj I bis. Če bi moralo sodišče v državi njihovega prebivališča ali sedeža uporabiti tuje pravo, ki bi bilo povsem v nasprotju s temeljnimi vrednotami foruma, sodišču tega prava ne bo treba uporabiti in bo lahko uporabilo *lex fori*. Če bi bila sodba izdana v drugi državi, pa bo država prebivališča ali sedeža toženca, kjer je praviloma večina premoženja, iz katerega bi se tožnik lahko poplačal, lahko zavrnila priznanje in izvršitev take sodbe. Odprava pridržka javnega reda na kateremkoli od navedenih področjih se ne zdi blizu.

4.2. ZMZPP

V Sloveniji se torej za določitev prava, ki ga je treba uporabiti, za zdaj uporablja ZMZPP, ki v 30. členu določa kolizijsko normo za nepogodbeno odškodninsko odgovornost:

»(1) Za nepogodbeno odškodninsko odgovornost se uporabi pravo kraja, kjer je bilo dejanje storjeno. Če je za oškodovanca ugodnejše, se namesto tega uporabi pravo kraja, kjer je nastopila posledica, vendar le, če je povzročitelj kraj posledice mogel in moral predvideti.

(2) Če pravo, določeno po prvem odstavku tega člena, nima z razmerjem tesnejše zveze, pač pa je podana očitna zveza z nekim drugim pravom, se uporabi to pravo.«

To normo je sicer nadomestila uredba Rim II, vendar ne glede kršitev zasebnosti in osebnostnih pravic.

Zanimiva je primerjava med normo ZMZPP o pristojnosti in kolizijsko normo tega zakona za nepogodbeno odškodninsko odgovornost. Pri pristojnosti (ZMZPP določa le, kdaj so pristojna sodišča Republike Slovenije) ima tožnik (poleg splošne pristojnosti po tožencevem stalnem prebivališču) na izbiro kraj škodnega ravnanja in kraj nastanka škode, kolizijska norma pa sodniku postavlja dva kriterija, glede na katera bo lahko ugotovil, ali naj uporabi pravo kraja škodnega ravnanja ali pravo kraja nastanka škode. Ta kriterija sta predvidljivost za storilca in ugodnost predpisa za oškodovanca. Le če sta izpolnjena oba pogoja, bo sodnik uporabil kraj nastanka škode.

Drugače kot po uredbi Rim II je torej primarna navezna okoliščina kraj storilčevega delovanja, ki je pri internetnih deliktih bistveno lažje določljiv kot kraj nastanka škode, kot je že bilo pojasnjeno. Čeprav gre za uporabo nacionalnega akta, lahko slovenska sodišča črpajo iz sodne prakse in komentarjev uredbe Bruselj I, ki se nanašajo na razlago te navezne okoliščine, seveda le kot vir tehtne argumentacije, ki ji ni treba obvezno slediti.

Verjetno pa bo zelo pogosto uporabljena druga navezna okoliščina, in sicer kraj nastanka škode. Če bo to za oškodovanca ugodneje (ugotavljanje tega je sicer lahko tudi zapleteno), bo imelo sodišče še težjo nalogo, in sicer ugotoviti, ali je bil določen kraj nastanka škode za povzročitelja predvidljiv. Spet se torej vračamo k istemu vprašanju – kaj lahko oziroma mora storilec predvidevati, ko gre za objavo na internetu? In ali 30. člen omogoča distributivno navezovanje v primeru škode, nastale v različnih državah? Vrhovno sodišče je leta 2010 zapisalo: »Določbe 30. člena ZMZPP ni mogoče več razumeti v smislu, da je odstop od načela *lex loci delicti commissi vel laesionis* dovoljen le izjemoma, ampak jo je treba razlagati v smislu, naj se uporabi pravo, s katerim je podana najtesnejša vez.«[88] Primarna navezna okoliščina naj bi torej postala koneksiteta. A s katerim pravom je podana najtesnejša vez? Je to pravo države prebivališča povzročitelja ali države prebivališča oškodovanca, morda kako tretje pravo? Ali stališče Vrhovnega sodišča pomeni, da je treba za celotno škodo, o kateri ima sodišče pristojnost odločati, uporabiti eno pravo, ali pa je mogoče distributivno navezovanje, če je slovensko sodišče tisto, ki lahko odloča o celotni škodi (ker je na primer v kraju, kjer je storilec deloval)? Iz teoretičnih zapisov bi lahko razbrali, da distributivno navezovanje v ZMZPP ni omejeno na primere, ki so izrecno določeni v zakonu,[89] vendar pa naj bi načelo najtesnejše zveze praviloma vodilo do uporabe prava ene države, poleg tega pa je distributivno navezovanje problematično s stališča predvidljivosti in težav sodišča pri uporabi več (tujih) prav.

5. Sklep

Splošni problemi pri čezmejnem uveljavljanju kršitev zasebnosti in osebnostnih pravic v množičnih medijih so pri storitvi kršitev prek interneta močno poudarjeni. V EU kombinacija več možnih pristojnosti po uredbi Bruselj I in zaradi odsotnosti skupne kolizijske norme oškodovanca postavlja v nesorazmerno boljši položaj, za »neposredne storilce« in njihove posrednike pa pomeni omejeno možnost predvidevanja (ne)dovoljenosti in morebitnih posledic njihovih objav na spletu. Res je tožnik kot (domnevni) oškodovanec tradicionalno obravnavan kot šibkejša stranka odškodninskih sporov, vendar kljub temu ni dopustno povsem zanemariti legitimnih interesov toženca kot domnevnega storilca kršitve. V nasprotju z »običajnimi« odškodninskimi spori je pri sporih, v katerih se na strani tožene stranke pogosto znajdejo mediji, ki imajo v družbi izredno pomembno vlogo (t. i. četrta veja oblasti), posebno pomembno poiskati ustrezno ravnovesje pravnih položajev obeh strank.

[88] Sklep VS, opr. št. II Ips 1001/2007 z dne 16. 12. 2010.

[89] Glej na primer Geč Korošec, str. 78, 79.

Popolno predvidljivost je v pravnih razmerjih z mednarodnim elementom nemogoče zagotoviti. Občutno pa se toženčev procesni položaj lahko uravnovesi s tožnikovim že, če se omeji nabor možnih forumov, tako da je mogoče tožiti le pri sodiščih v državi in kraju, ki sta s sporom pomembno povezana. To je gotovo najprej sodišče v državi toženčevega stalnega prebivališča, ki je v obravnavanih sporih splošno pristojno. Pri kriterijih zveze s sporom in predvidljivosti pa je treba pri internetnih deliktih s posebno skrbnostjo razmejevati med forumi, za katere je smiselno, da o sporu odločajo, in forumi, na območju katerih je sicer bilo mogoče dostopati do sporne internetne vsebine in glede katerih je storilec tudi lahko vedel, da bo to mogoče (nihče se namreč ne more izgovarjati, da ni vedel, da bo na internetu objavljena vsebina dostopna po vsem svetu), vendar ni smiselno, da bi bili pristojni. SEU je k tem ciljem pomembno pripomoglo s svojo razlago uredbe Bruselj I.

Seveda pa je pomembno tudi, da se v okviru EU najde kompromis glede skupne kolizijske norme za obravnavane kršitve. Čeprav se nacionalne ureditve odškodninskega prava med državami članicami EU precej razlikujejo,[90] je poglavitna težava v iskanju kompromisa med več zainteresiranimi skupinami, zlasti med založniki in uredniki spletnih medijev, ki si prizadevajo predvsem za določitev kolizijske norme po prebivališču oziroma sedežu storilca, saj bi tako najlažje ocenili dovoljenost in morebitne posledice svojih objav, ter oškodovanci, ki bi želeli uporabo prava nastanka škodne posledice, torej presojanje dejanj po pravu države, v kateri so sami utrpeli škodo.

V zadnjih letih je bila prisotna tudi ideja, da bi kršitve zasebnosti in osebnostnih pravic prek množičnih medijev in interneta izvzeli tudi iz urejanja tretjega odstavka 5. člena uredbe Bruselj I ter problematiko pristojnosti, kolizijskega prava ter priznavanja in izvrševanja tujih sodb na tem področju uredili v posebnem aktu. Videti pa je, da je razvoj usmerjen k ohranjanju urejanja omenjenih kršitev na »matičnih« področjih, torej v okviru ustreznega razvoja razlage tretjega odstavka 5. člena uredbe Bruselj I in dopolnitve uredbe Rim II z ustrezno kolizijsko normo. Dolgoročno pa bi bilo seveda za vse stranke v postopkih najbolje, da bi na ravni EU poenotili kar materialno pravo.

[90] Glej na primer Comparative Study on the Situation in the 27 Member States as Regards the Law Applicable to Non-contractual Obligations Arising out of Violations od Privacy and Rights Relating to Personality, JLS/2007/C4/028. Final Report, februar 2009, dostopna na spletni strani http://ec.europa.eu/justice/civil/files/study_privacy_en.pdf (23. 3. 2014).

Literatura

Ardia, David S.: Freedom of Speach, Defamation, and Injunctions, *William and Mary Law Review*, vol. 55, avgust 2013, št. 1, str. 0–59 (dostopno tudi na spletni strani SSRN: http://ssrn.com/abstract=2307744).

Basedow, Jürgen in drugi (Hamburg Group for Private International Law): Comments on the European Commission's Draft Proposal for a Council Regulation on the Law Applicable to Non-Contractual Obligations. *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 67, 2003, str. 1–56.

Cigoj, Stojan: *Mednarodno pravo osebnih in premoženjskih razmerij (Prva knjiga, Splošni nauki)*. Časopisni zavod Uradni list SRS, Ljubljana 1984.

Galič, Aleš: Pristojnost v nepogodbenih odškodninskih sporih. *Pravni letopis 2012,* Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani, 2012, str. 9–27.

Geč Korošec, Miroslava: *Mednarodno zasebno pravo, splošni del* (1. knjiga). Uradni list Republike Slovenije, Ljubljana 2001.

Little, Laura E.: Internet Defamation, Freedom of Expression, and the Lessons of Private International Law for the United States. *Yearbook of Private International Law*, Sellier, vol. 14, 2012, str. 1–36 (dostopno tudi na spletni strani SSRN: http://ssrn.com/abstract=2187449).

Mežnar, Špela: Predlog uredbe o kolizijskih pravilih za nepogodbene obligacijske obveznosti (t. i. Rimska II uredba). *Evro Pravna praksa*, leto 2, 2004, št. 4, str. 23–28 (priloga, str. I–VI).

Mežnar, Špela: Odškodnina kot kazen na primeru medijskih kršitev – zakaj (ne)?. V: Seliškar Toš, Mojca (ur.). *Izbrane teme civilnega prava*: zbornik Inštituta za primerjalno pravo pri Pravni fakulteti v Ljubljani. Inštitut za primerjalno pravo pri Pravni fakulteti, Ljubljana 2006, str. 77–91.

Mežnar, Špela: Začetek konca spletnih komentarjev?: ob sodbi ESČP v zadevi Delfi proti Estoniji. *Pravna praksa*, leto 32, 2013, št. 46, str. 6–8.

Mežnar, Špela: Novejši trendi v odškodninskem pravu. V: *Podjetje in delo*, let. 34, 2008, št. 6-7, str. 1284–1293.

Možina, Damjan: Persönlichkeitsverletzungen im Internet – die internationale Zuständigkeit. *Slovenian Law Review*, let. 1, 2004, št. 1-2, str. 77–92.

Možina, Damjan: Forum delicti commissi v internetu. *Pravnik*, let. 57 (119), 2002, št. 9-10, str. 509–532.

Skubic, Zoran: Čezmejna kršitev osebnostnih pravic z objavo na spletu: kje tožiti? *Pravna praksa*, 2011, št. 44, str. 25.

Ten Tolde, Mathijs, Knot, Jan-Ger, Weller, Mathias: Art. 5 Nr. 3. V: Simons, Thomas, Hausmann, Rainer (ur.). *Brüssel I-Verordnung, Kommentar zur VO (EG) 44/2001 und zum Übereinkommen von Lugano*. IPR Verlag GmbH, München 2012, str. 252–275.

Elektronsko vročanje*

Neža Pogorelčnik

1. Uvod

Razvoj informacijske tehnologije in tehnike ter posledično čedalje pogostejša uporaba interneta sta sprožila zahtevo po pravni ureditvi vse širšega spektra dejavnosti[1] našega vsakdanjega življenja, elektronskega poslovanja.[2] Pravno urejanje področja se je razvijalo od sprejetja prvih aktov na mednarodni in evropski ravni do prenašanja in vnašanja pravil v zakonodaje posameznih držav.

Medtem ko so sprva akti urejali pravila elektronskega poslovanja na splošno, so sčasoma prešli na regulacijo specifičnih delov, hkrati pa se elektronska oblika na vse več področjih pojavlja kot vzporedna in enakovredna klasični. Kot je v komentarju Zakona o elektronskem poslovanju in elektronskem podpisu (ZEPEP)[3] napisal Marko Pavliha,[4] bodo elektronske oblike dejavnosti počasi prevzemale klasične in nekoč bomo pridevnik elektronsko mirno izpustili, saj bo to postalo vsakdanja oblika poslovanja.

2. Razvoj pravne ureditve elektronskega poslovanja na mednarodni in evropski ravni

Komisija Združenih narodov za mednarodno trgovinsko pravo[5] je že leta 1985 izdala dokument z izvirnim naslovom Legal Values of Computer Records,[6]

---

* Prispevek je bil prvič objavljen v: Pravni letopis 2011, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani.

[1] Sem spadajo elektronsko bančništvo, plačevanje prek interneta, spletno trgovanje na borzi, delo in študij na daljavo … Spekter je širok, specifične lastnosti vsakega od njih pa zahtevajo različne ureditve.

[2] Slovenski izraz elektronsko poslovanje zajema dva angleška pojma, in sicer *electronic business* in *electronic commerce*. Prvi je širši in opredeljuje vsako ravnanje subjektov v informacijskem okolju, drugi pa je ožji in se prevaja kot elektronsko trgovanje. S. Matas, v: M. Pavliha, B. Jerman Blažič in drugi, Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem, GV Založba, Ljubljana 2002, str. 24.

[3] Uradni list RS, št. 57/2000, s spremembami in dopolnitvami.

[4] M. Pavliha, v: M. Pavliha, B. Jerman Blažič in drugi, Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem, GV Založba, Ljubljana 2002, str. 10.

[5] United Nations Commission on International Trade Law (UNCITRAL).

[6] Dostopen na: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1985Recommendation.html (9. 5. 2011).

katerega namen je bil spodbuditi nadzor zakonskih določb glede računalniških zapisov. Po naslednjem desetletju razvoja informacijske tehnologije je UNCITRAL leta 1996 sprejel Vzorčni zakon za mednarodno trgovinsko pravo o elektronskem poslovanju,[7] leta 1997 pa oblikoval skupino IV, ki pokriva področje elektronskega poslovanja (angl. *electronic commerce*). Leta 2001 je bil sprejet še Vzorčni zakon o elektronskem podpisu,[8] leta 2005 pa Konvencija Združenih narodov o uporabi elektronskih komunikacij v mednarodnih pogodbah.[9]

Na ravni EU je bilo na področju elektronskega poslovanja sprejetih več aktov, med temi je najpomembnejši Direktiva 2000/31/ES o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju).[10]

Elektronskega vročanja evropska zakonodaja ne ureja. Področje vročanja s čezmejnim elementom sicer zajema Uredba (ES) 1393/2007 o vročanju sodnih in izvensodnih pisanj v civilnih ali gospodarskih zadevah v državah članicah (vročanje pisanj) in razveljavitvi Uredbe Sveta (ES) 1348/2000,[11] a elektronske oblike ne predvideva. Pri urejanju elektronskega vročanja slovenski zakonodajalec tako ni vezan na predpisane evropske cilje.

Pomembna pa je tudi Direktiva 1999/93/ES o okviru Skupnosti za elektronski podpis,[12] saj Zakon o pravdnem postopku[13] (ZPP) kot pogoj za veljavno elektronsko vročitev v civilnem pravdnem postopku zahteva uporabo varnega elektronskega podpisa. Ureditev direktive je v slovenski pravni red prenesel ZEPEP, ki pa se uporablja tudi pri elektronskem vročanju v civilnih sodnih postopkih.[14]

---

[7] Vzorčni zakon sicer nima pravne veljave, a služi kot model zakona za države, ko to področje urejajo v svojih zakonodajah. Dostopen na: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html (9. 5. 2011).

[8] Dostopen na: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html (9. 5. 2011).

[9] Dostopna na: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html (9. 5. 2011).

[10] Dostopna na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:25:32000L0031:SL:PDF (9. 5. 2011).

[11] UL L 324, z dne 10. 12. 2007, str. 79–120.

[12] UL L 13, z dne 19. 1. 2000, str. 12–20, dostopna na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:SL:NOT (9. 5. 2011).

[13] Uradni list RS, št. 26/1999, s spremembami in dopolnitvami.

[14] Člen 3 Pravilnika o elektronskem poslovanju v civilnih sodnih postopkih, Uradni list RS, št. 64/2010, s spremembo, objavljeno v Uradnem listu RS, št. 23/2011.

3. Ureditev elektronskega poslovanja v Sloveniji

V Sloveniji je elektronsko poslovanje na splošno urejeno z Zakonom o elektronskem poslovanju in elektronskem podpisu, s katerim je bila slovenska pravna ureditev prilagojena evropski Direktivi za elektronski podpis.[15] Kot pove že ime, ZEPEP ureja dve področji, elektronsko poslovanje in elektronski podpis, ki se sicer zahteva le pri nekaterih oblikah elektronskega poslovanja. Je prvi slovenski zakon, ki je definiral, da so podatki v elektronski obliki oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način,[16] ter določil, da elektronsko poslovanje zajema poslovanje v elektronski obliki z uporabo informacijske in komunikacijske tehnologije.[17] S tem je uvedel podlago za uvedbo elektronskega poslovanja[18] v sodne, upravne in druge postopke.

Elektronsko poslovanje, vključno z elektronskim vročanjem, je v postopek uvedel Zakon o splošnem upravnem postopku (ZUP),[19] in sicer leta 2004 z novelo ZUP-C,[20] prvotna ureditev pa je bila kasneje spremenjena z novelo ZUP-E.[21] Zgodnja ureditev področja in sodelovanje pri nadnacionalnih projektih za uvedbo elektronske uprave[22] sta najverjetneje prispevala k temu, da je danes v Sloveniji upravni postopek edini, v katerem elektronsko poslovanje v praksi deluje,[23] čeprav stranke in upravni organi v večini primerov še vedno raje uporabljajo klasični način za vlaganje vlog in vročanje pisanj.

Elektronsko poslovanje je bilo leta 2007 vpeljano še v pravdni postopek, in sicer z novelo ZPP-C (ureditev je kasneje malo spremenila novela ZPP-D),[24] leto kasneje pa še v kazenski postopek z novelo I[25] Zakona o kazenskem postopku (ZKP).[26] Medtem ko elektronsko poslovanje zavzema vse večji del našega vsakda-

[15] Sicer je na tem področju pomemben tudi Zakon o elektronskem poslovanju na trgu, Uradni list RS, št. 61/2006.

[16] Prva točka prvega odstavka 2. člena ZEPEP.

[17] Prvi odstavek 1. člena ZEPEP.

[18] Elektronsko poslovanje v postopku zajema elektronsko vlaganje vlog, videokonference, vodenje elektronskih spisov, elektronski vpogled v spis, elektronsko vročanje …

[19] Uradni list RS, št. 80/1999, s spremembami in dopolnitvami.

[20] Uradni list RS, št. 73/2004.

[21] Uradni list RS, št. 126/2007.

[22] Centre for eGovernance Development, dostopen na: http://www.cegd.eu/about_us.htm (9. 5. 2011), in STORK, dostopen na: https://www.eid-stork.eu/index.php?option=com_content&task=view&id=37&Itemid=61 (9. 5. 2011).

[23] Elektronsko poslovanje na področju uprave poteka prek portala e-uprava, dostopno na http://e-uprava.gov.si/e-uprava/portalStran.euprava?pageid=1 (9. 5. 2011).

[24] Novela ZPP-C, Uradni list RS, št. 52/2007, in novela ZPP-D, Uradni list RS, št. 45/2008.

[25] Uradni list RS, št. 68/2008.

[26] Uradni list RS, št. 63/1994, s spremembami in dopolnitvami.

njika in bi pričakovali, da bo razvoj potekal v smeri njegovega uvajanja v zakone na vseh področjih, pa je ponekod ravno nasprotno. Tako je državni zbor leta 2008 z Zakonom o osebni izkaznici[27] uvedel elektronske osebne izkaznice, z zadnjo novelo z dne 3. maja 2011 pa je to možnost izbrisal, ker v praksi zaradi cenovne nesprejemljivosti ni zaživela.

4. Elektronsko poslovanje v slovenskem sodstvu

Strategija razvoja Slovenije, ki jo je vlada sprejela 23. junija 2005, med drugim vsebuje projekt Modernizacija pravosodnega sistema e-pravosodje, ki predvideva popolno informatizacijo sodišč. Na podlagi tega je bila sprejeta Strategija informatizacije slovenskega pravosodnega sistema 2008–2013,[28] katere osrednji predmet je projekt *e-pravosodje*. Ta zajema 31 projektov, med drugimi tudi *e-vložišče*, katerega cilj je zagotovitev informacijske podpore za obvladovanje vseh procesov sodišč, povezanih z vlaganjem, prenosom, odpremo in vročanjem dokumentov. Delo pri projektu se je začelo leta 2009 in naj bi se predvidoma končalo leta 2014.[29] Njegov nosilec je Vrhovno sodišče RS, glede na podatke Ministrstva za pravosodje pa je projekt trenutno v fazi priprave.[30]

Strategija informatizacije slovenskega pravosodnega sistema določa tri elemente, ki morajo obstajati, da bo projekt e-pravosodje zaživel v praksi: institucionalni element, ki zajema sprejem pravne podlage, organizacijski, kamor spadajo postopki, standardi in načini delovanja posameznih pravosodnih institucij, ter najenostavnejši, tehnološki, ki zajema nenehno razvijajoče se tehnološke sisteme.

V institucionalnem elementu so zajete spremembe, s katerimi smo nekatere zakone že prilagodili informacijskemu razvoju, na primer Zakon o sodnem registru,[31] Zakon o izvršbi in zavarovanju,[32] Zakon o zemljiški knjigi,[33] Zakon o finančnem poslovanju zaradi insolventnosti in prisilnem prenehanju[34] ter ZPP, katerega določbe o elektronskem poslovanju, posebno o elektronskem vročanju, so predstavljene v nadaljevanju.

---

[27] Uradni list RS, št. 75/1997, s spremembami in dopolnitvami.

[28] Dostopna na http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/2005/PDF/publikacije/strategija_e-pravosodje_2008-2013.pdf (12. 5. 2011).

[29] Letno poročilo 2009 Vrhovnega sodišča, http://www.sodisce.si/mma_bin.php?static_id=2010081011355553 (12. 5. 2011).

[30] http://www.mp.gov.si/si/delovna_podrocja/e_pravosodje/projekti_pregled_statusov/ (12. 5. 2011).

[31] Uradni list RS, št. 54/2007, s spremembami in dopolnitvami.

[32] Uradni list RS, št. 51/1998, s spremembami in dopolnitvami.

[33] Uradni list RS, št. 58/2003, s spremembami in dopolnitvami.

[34] Uradni list RS, št. 126/2007, s spremembami in dopolnitvami.

5. Ureditev elektronskega poslovanja v pravdnem postopku

Pri urejanju elektronskega pravdnega postopka se je zakonodajalec opiral na ureditev, ki jo je nekaj let prej uvedel na upravnem področju, upoštevajoč specifično naravo državnega organa, ki se v pravdnem postopku razlikuje od tistega v upravnem. Tako je ZPP-C na štiri področja pravdnega postopka vzporedno s klasično uvedel še elektronsko pot poslovanja:

1. elektronsko vlaganje vlog (tožb in drugih listin), ki jih na sodišče vlagajo stranke,
2. elektronsko poslovanje sodišč[35] (elektronsko vodenje spisov, izdelava elektronskih sodb itd.),
3. elektronski vpogled v stanje vlog (spremljanje takih postopkov s strani strank, možnost pregledovanja in prepisovanja elektronskih spisov po elektronski poti itd.) ter
4. elektronsko vročanje aktov strankam s strani sodišča (vključno z vročanjem sodb, ki so najpomembnejši akt sodišča, ki se vroča strankam).

S temi dejavnostmi je pokrita večina dejanj v pravdnem postopku in ustvarjena podlaga, da postopek od začetka do konca poteka v elektronski obliki.[36]

5.1. Enakovrednost pisne in elektronske oblike

Osnovna oblika, ki jo za pravna dejanja in akte v pravdnem postopku zahteva ZPP, je pisnost. Uvedbo elektronskega poslovanja in nadomeščanje pisne oblike z elektronsko (tudi pri vročanju) omogoča načelo enakovrednosti obeh in prepoved diskriminacije elektronske oblike glede na pisno, ki je klasična in splošno sprejeta.

Načelo je vsebovala že Direktiva za elektronski podpis,[37] na nacionalni ravni ga vsebuje ZEPEP (v 4. in 13. členu), posredno ali neposredno pa izhaja tudi iz vseh treh postopkovnih zakonov, ki predvidevajo elektronsko poslovanje.[38] Brez tega načela bi vsaka uvedba tega v zakon ostala zgolj črka na papirju. Elektronska

[35] V civilnem postopku je informatizacija najbolj razvita v izvršilnem postopku, v katerem od leta 2008 deluje Centralni oddelek za verodostojno listino. Na oddelek je mogoče elektronsko vložiti predlog za izvršbo, za vsak oddani predlog pa subjekt lahko prejme elektronsko sporočilo. Postopek teče v elektronski obliki, sklepe o izvršbi pa izdaja informacijski sistem samodejno.

[36] Pri tem še vedno ostaja pravilo fizične izvedbe glavne obravnave na sodišču, možnost videokonference pa je predvidena kot izjema, s soglasjem strank in dovoljenjem sodišča, pod pogojem, da je zagotovljen zvočni in slikovni prenos iz kraja, na katerem se opravlja narok, v kraj, na katerem se nahajajo stranke in pooblaščenci, ter obrnjeno (114.a člen ZPP).

[37] Direktiva v členu 5(2) določa enakost varnega elektronskega podpisa in podpisa v pisni obliki.

[38] Torej ZUP (tretji odstavek 63. člena), ZPP (16.a člen) in ZKP (drugi odstavek 117. člena).

oblika pisanj, tako tistih, ki jih na sodišča pošiljajo stranke, kot tudi tistih, ki potujejo v nasprotni smeri, ter vsa dejanja elektronskega poslovanja imajo torej enake učinke in enako vrednost kot klasična oblika oziroma pot, seveda pod pogojem, da so izpolnjeni zahtevani zakonski pogoji.

5.2. Zakonski pogoji za enakovrednost pisne in elektronske oblike

ZEPEP v 13. členu za enakovrednost elektronske in pisne oblike zahteva, da so podatki v elektronski obliki *dosegljivi* in *primerni* za kasnejšo uporabo. Iz tega so izvzeti nekateri pomembnejši pravni posli,[39] pri katerih je zagotovljena višja zaščita strank.

Zakon tako omejuje enakovrednost obeh oblik le na »navadne« pravne posle, s čimer kaže na to, da so stranke pri sklepanju pravnih poslov v elektronski obliki očitno manj skrbne in bolj ranljive ter zato bolj podvržene zlorabam sopogodbenikov.

Dosegljivost iz prvega odstavka 13. člena komentator zakona razlaga kot zahtevo, da so sporočila berljiva in jih je mogoče interpretirati, hkrati pa kot zahtevo po programski opremi, ki bo tako sporočilo lahko prikazala. Dokument mora biti prav tako primeren za kasnejšo uporabo, kar pomeni, da mora biti dosegljiv, nespremenljiv in obstojen tudi v daljšem časovnem obdobju.[40]

ZPP poleg tega zahteva še, da so podatki v elektronski obliki primerni za obdelavo na sodišču,[41] za kar je na vseh sodiščih nujno potrebna tehnična in programska oprema.

Poleg enakovrednosti pisne in elektronske oblike ZEPEP določa enakovrednost tudi za elektronski podpis, varen elektronski podpis[42] in elektronsko vlaganje vlog, pri čemer je za to postavljen dodaten pogoj, da je vloga podpisana z varnim elektronskim podpisom, ki je overjen[43] s kvalificiranim potrdilom.

---

[39] To so pravni posli, s katerimi se prenaša lastninska pravica na nepremičnini ali s katerimi se ustanavlja druga stvarna pravica na nepremičnini, oporočni posli, pogodbe o urejanju premoženjskih razmerij med zakoncema, pogodbe o razpolaganju s premoženjem oseb, ki jim je odvzeta poslovna sposobnost, pogodbe o izročitvi in razdelitvi premoženja za čas življenja, pogodbe o dosmrtnem preživljanju in sporazumi o odpovedi neuvedenemu dedovanju, darilne obljube in darilne pogodbe za primer smrti, kupne pogodbe s pridržkom lastninske pravice in drugi pravni posli, za katere zakon določa, da morajo biti sklenjeni v obliki notarskega zapisa.

[40] V. Rijavec, v: L. Ude, N. Betetto, A. Galič, V. Rijavec, D. Wedam Lukić in J. Zobec, Pravdni postopek, zakon s komentarjem spremenjenih členov, 4. knjiga, GV Založba in Uradni list Republike Slovenije, Ljubljana 2010, str. 25.

[41] Člen 16a ZPP.

[42] Člena 14 in 15 ZEPEP.

[43] Zakon je pri tem nedosleden, saj se s potrdilom podpis ne overi, ampak se preveri njegova pristnost.

6. Pošiljanje elektronskih sporočil

ZEPEP ureja pošiljanje elektronskih sporočil med strankama (ne pa med sodiščem in stranko kot ZPP ali med upravnim organom in stranko kot ZUP). Pri tem se elektronsko pisanje šteje za odposlano, ko vstopi v informacijski sistem zunaj nadzora pošiljatelja, če ni dogovorjeno drugače.[44] ZEPEP pa določa tudi, kdaj se pisanje šteje za prejeto:[45]

- če je pošiljatelj v vnaprejšnjem dogovoru ali naknadno zahteval, da naslovnik prejem sporočila potrdi s potrdilom,[46] je trenutek prejetja sporočila pogojen s tem, ali naslovnik pošiljatelju potrdi njegov prejem;[47]
- če prejem ni pogojen s povratnim potrdilom, se za čas prejema elektronskega sporočila šteje trenutek, ko elektronsko sporočilo vstopi v prejemnikov informacijski sistem.[48]

7. Elektronsko vročanje v pravdnem postopku

Novela ZPP-C je poleg drugih možnosti vročanja uvedla tudi elektronsko vročanje,[49] ki je v skladu s 16.a členom ZPP enakovredno klasičnemu. Pravilnik o elektronskem poslovanju v civilnih sodnih postopkih[50] (v nadaljevanju: Pravilnik) definira elektronsko vročitev kot vročitev po varni elektronski poti po ZPP.

7.1. Kdaj elektronsko vročanje namesto klasičnega

Sodišče vroči pisanje po elektronski poti:

- če mu stranka sporoči, da želi ta način vročanja, ter v vlogi navede naslov svojega varnega elektronskega predala ali
- če stranka uporabi elektronsko pot za vložitev svoje vloge, razen če sodišču hkrati sporoči, da ne želi elektronske vročitve pisanja.

---

[44] Člen 9 ZEPEP.

[45] ZEPEP je ureditev 7. člena povzel po vzorčnem zakonu UNCITRAL.

[46] Člen 7 ZEPEP.

[47] ZEPEP prejema ne dojema kot pasivno dejanje, ampak aktivno, saj zahteva, da prejemnik oblikuje potrdilo, s katerim potrdi, da je pisanje prejel. Pri tem pa potrdilo o prejemu ne pomeni tudi, da naslovnik sprejema ponudbo, vsebovano v pisanju. Drug sistem je pasivno potrjevanje prejetja, pri čemer informacijski sistem, pri katerem ima prejemnik odprt varen elektronski predal, ob prevzemu elektronskega pisanja informacijskemu sistemu pošiljatelja sam pošlje elektronsko vročilnico. Matas, v: Pavliha, Jerman Blažič, str. 54.

[48] Člen 10 ZEPEP.

[49] Prvi odstavek 132. člena ZPP.

[50] Uradni list RS, št. 64/2010, 23/2011.

Za »navadne« subjekte[51] se tako elektronska pot vročanja nikoli ne domneva. Za elektronsko vročanje pisanja mora subjekt sodišču vedno dati pobudo, bodisi da sodišču sporoči svojo željo po vročanju po elektronski poti bodisi da tako pot uporabi sam ob vložitvi vloge.[52]

Drugačen pristop je zakonodajalec uporabil za vročanje državnim organom, odvetnikom, notarjem, izvršiteljem, sodnim izvedencem, sodnim cenilcem, sodnim tolmačem, stečajnim upraviteljem in drugim, za katere se predvideva večja zanesljivost. Tem se namreč vedno in obvezno vroča po elektronski poti v varen poštni predal, ki ga morajo imeti. Vrhovno sodišče mora določiti in objaviti seznam oseb in organov, za katere je odprtje varnega elektronskega predala obvezno, česar pa do zdaj še ni storilo.

Če stranka zahteva elektronsko vročitev, pa ta ni mogoča, se pisanje vroči v fizični obliki.[53]

7.2. Katera pisanja se vročajo elektronsko

Tako kot se lahko pisanje v elektronski obliki vroči fizično[54] ali po varni elektronski poti,[55] je mogoče tudi obrnjeno. Po elektronski poti se lahko poleg pisanj v elektronski obliki vročajo tudi pisanja, katerih izvirnik je v fizični obliki. Tega sodišče optično prebere, v dokaz istovetnosti pa ga mora podpisati z varnim elektronskim podpisom, overjenim s kvalificiranim potrdilom.[56]

Elektronsko je mogoče vročati pisanja, za katera je predpisana osebna in neosebna (navadna) vročitev, določitev natančnega seznama pisanj, ki se bodo lahko vročala po varni elektronski poti, pa je ZPP prepustil podzakonskemu urejanju, pri čemer Pravilnik o elektronskem poslovanju v civilnih sodnih postopkih, ki je bil sprejet na podlagi ZPP, tega ni uredil.

---

[51] S pojmom »navaden« subjekt mislim na vse subjekte, razen tistih, navedenih v sedmem odstavku 132. člena ZPP.

[52] Ta ureditev se razlikuje od tiste po ZUP, po kateri je elektronska vročitev mogoča tudi, če stranka ne sporoči, da želi vročanje po elektronski poti, in sama ne vloži pisanja v elektronski obliki, vendar organ lahko zanesljivo ugotovi, da ima stranka varni elektronski predal (83. člen ZUP).

[53] Peti odstavek 132. člena ZPP.

[54] Obstaja več načinov fizičnega vročanja: po pošti, po delavcu sodišča, na sodišču ali na drug način, določen z zakonom (132. člen ZPP).

[55] Pri elektronskem vročanju sodne odločbe se pošlje odpravek elektronske sodne odločbe kot elektronski dokument (drugi odstavek 7. člena Pravilnika).

[56] Deveti odstavek 141.a člena ZPP.

Vročanje po elektronski poti v ZPP ni predvideno le za vročanje s strani sodišč, ampak se bo, potem ko bo vzpostavljeno, lahko uporabljalo tudi pri vročanju pisanj neposredno med pooblaščenci.[57]

7.3. Instrumenti, potrebni za elektronsko vročanje

Elektronsko vročanje na strani pošiljatelja, to je sodišča, poteka prek informacijskega sistema[58] e-sodstvo,[59] ki ga upravlja Center za informatiko na Vrhovnem sodišču.[60] Ta informacijski sistem ima v civilnih sodnih postopkih podobno vlogo kot v upravnem postopku enotni informacijski sistem za sprejem vlog, vročanje in obveščanje, ki ga je uvedel ZUP in ustanovilo Ministrstvo za javno upravo.

Na strani naslovnika pa vročitev poteka prek informacijskega sistema za varno vročanje, ki omogoča izvedbo postopkov elektronske vročitve v skladu z ZPP in Pravilnikom, upravlja pa ga oseba, ki opravlja storitve varnega elektronskega vročanja in je sklenila ustrezno pogodbo s Centrom za informatiko.[61]

Stranka, ki želi s sodiščem komunicirati elektronsko (torej elektronsko vlagati vloge ali od sodišča zahtevati, da ji pisanja vroča elektronsko) ali pa spada v skupino oseb, za katere je to obvezno, mora najprej odpreti varen elektronski predal. Ponudnika teh sta v Sloveniji (v času pisanja prispevka) Pošta Slovenije (www.moja.posta.si) in Eius, d. o. o. (www.vep.si).

ZEPEP sicer vsebuje definicije najpomembnejših pojmov, ki se navezujejo na elektronsko poslovanje in elektronski podpis, pri tem pa ne zajema enega najpogosteje uporabljenih terminov pri elektronskem vročanju, to je pojma »varni poštni predal« oziroma »varni elektronski predal«. To sta namreč izraza, ki se v ZPP, ZUP in ZKP uporabljata za elektronski naslov, na katerega se naslovniku pošiljajo pisanja po elektronski poti.

Za civilne sodne postopke ta pojem definira šele Pravilnik o elektronskem poslovanju v civilnih sodnih postopkih. Hkrati popravlja nejasno uporabo ZPP, ki

[57] Člen 139a ZPP.

[58] ZEPEP vsebuje splošno definicijo informacijskega sistema, in sicer ga definira kot programsko, strojno, komunikacijsko in drugo opremo, ki deluje samostojno ali v omrežju in je namenjena zbiranju, procesiranju, distribuciji, uporabi in drugi obdelavi podatkov v elektronski obliki (11. točka 2. člena).

[59] Informacijski sistem e-sodstvo vključuje štiri module, in sicer modul z varnostno shemo, modul za podporo izvajanju elektronskih opravil v civilnih sodnih postopkih (modul e-opravila), modul za podporo vodenja elektronskega vpisnika (modul e-vpisnik) in elektronskega spisa v civilnih sodnih postopkih (modul e-spis) ter modul za podporo poslovanja sodišč pri vročanju (modul e-poštna knjiga) (2. člen Pravilnika).

[60] Člen 2 Pravilnika.

[61] Ureditev iz tretjega odstavka 141.a člena ZPP je podrobneje urejena v drugem odstavku 7. člena Pravilnika.

enkrat govori o varnem elektronskem predalu in drugič varnem poštnem predalu. Tako Pravilnik določi termin varen elektronski predal in ga definira kot elektronski naslov uporabnika v informacijskem sistemu za varno elektronsko vročanje, ki ga upravlja izvajalec storitev varnega elektronskega vročanja ali državni organ in pomeni enako kot varen poštni predal po ZPP.[62]

Čeprav je kljub terminološki nedoslednosti zakonska ureditev jasna in je iz določb razvidno, da gre za varen elektronski predal,[63] bi bilo ustrezneje, da bi ob naslednji spremembi omenjenih treh zakonov izrazje poenotili še na zakonski ravni.

Poleg varnega elektronskega predala mora oseba pridobiti varno (tudi kvalificirano) digitalno potrdilo,[64] ki ji omogoča registracijo na spletnem portalu e-sodstvo. To potrdilo pri elektronskem poslovanju povezuje podatke za preverjanje elektronskega podpisa z določeno osebo ter potrjuje njeno identiteto, trenutno pa jih izdajajo[65] overitelj na Ministrstvu za javno upravo (Sigen-CA[66] in Sigov-CA[67]), Halcom, d. d. (Halcom CA), AC NLB in Pošta Slovenije, d. o. o. (Pošta®ca).[68]

Elektronsko potrdilo skupaj z elektronskim podpisom[69] dokazuje identiteto subjekta. Samo navaden elektronski podpis nima takega učinka. Člen 15 ZEPEP namreč določa, da je (le) varen elektronski podpis, overjen s kvalificiranim potrdilom, glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu

---

[62] Deveti odstavek 7. člena Pravilnika.

[63] V prispevku sem uporabljala izraz varen elektronski predal, razen ko sem povzemala točno določen zakonski člen, ki sem ga v opombi na koncu posamezne povedi tudi navedla.

[64] ZEPEP definira kvalificirano potrdilo kot potrdilo, ki ga je izdal overitelj, ki deluje v skladu z ZEPEP, in iz katerega morajo biti razvidne te sestavine: navedba, da gre za kvalificirano potrdilo, ime ali firma in država stalnega prebivališča ali sedeža overitelja, ime oziroma psevdonim imetnika potrdila z obvezno navedbo, da gre za psevdonim, dodatni podatki o imetniku potrdila, ki so predpisani za namen, za katerega se bo potrdilo uporabljalo, ki pa ne smejo biti v nasprotju z namenom uporabe psevdonima, podatki za preverjanje elektronskega podpisa, ki ustrezajo podatkom za elektronsko podpisovanje pod nadzorom imetnika potrdila, začetek in konec veljavnosti potrdila, identifikacijska oznaka potrdila, varen elektronski podpis overitelja, ki je potrdilo izdal, morebitne omejitve v zvezi z uporabo potrdila in morebitne omejitve transakcijskih vrednosti, za katere se potrdilo lahko uporablja (28. člen).

[65] Tretji odstavek 40. člena ZEPEP določa, da register overiteljev vodi ministrstvo. Po ukinitvi Ministrstva za informacijsko družbo ga vodi Ministrstvo za visoko šolstvo, znanost in tehnologijo. Register je dostopen na http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/pdf/informacijska_druzba/REGISTER_OVERITELJEV_V_RS_ver26__05.01.2011-podpisan.pdf (10. 5. 2011).

[66] Posebna in spletna kvalificirana digitalna potrdila za poslovne subjekte in fizične osebe.

[67] Posebna in spletna kvalificirana digitalna potrdila za državne organe.

[68] Pogoje in način delovanja overiteljev določata ZEPEP ter Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje, Uradni list RS, št. 77/2000, 2/2001, 86/2006.

[69] ZEPEP definira elektronski podpis kot niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika (3. točka 2. člena).

ter ima zato enako veljavnost in dokazno vrednost. Na podlagi takega podpisa je omogočeno ugotavljanje istovetnosti subjekta, saj je povezan izključno s podpisnikom, ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom, in povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.[70]

Subjekt, ki torej podpiše dokument z varnim elektronskim podpisom, tega ne more zatajiti, hkrati pa je mogoče razbrati, kakšna je bila vsebina dokumenta, ko ga je podpisal (ne glede na morebitne kasnejše spremembe).

»Navaden subjekt«[71] se na e-sodstvu registrira in kasneje prijavlja kot registrirani uporabnik, subjekt iz skupine, navedene v sedmem odstavku 132. člena ZPP, pa kot zunanji kvalificirani uporabnik. Registracijo subjekta v skupino zunanjih kvalificiranih uporabnikov mora potrditi administrator posamezne kvalificirane skupine,[72] k čemur ga pozove varnostna shema portala. Po njegovi potrditvi (za kar ima administrator tri dni časa) je subjekt obveščen o registraciji v sistem in lahko začne uporabljati spletni portal e-sodstvo. Subjekt v varnostno shemo vstopi z elektronskim naslovom in geslom, ki ju je določil ob registraciji.

Trenutno je na portalu e-sodstvo sicer mogoče dostopati le do modula elektronske zemljiške knjige[73] (eZK) in nekaterih insolvenčnih opravil (eIns), v prihodnosti pa bo komunikacija s sodišči mogoča na ta način tudi v civilnih sodnih postopkih.

7.4. Potek elektronskega vročanja

Sodišče vroča pisanja po elektronski poti prek informacijskega sistema e-sodstvo, ki dokument podpiše s kvalificiranim digitalnim potrdilom, ga časovno žigosa in pošlje informacijskemu sistemu za varni elektronsko vročanje (SVEV), pri katerem ima naslovnik odprt svoj varen elektronski predal. Skupaj s pisanjem pošlje e-sodstvo tudi sporočilo s podatki o sodišču, ki je pošiljatelj, o oznaki elektronskega dokumenta (ki se določi na portalu e-sodstvo) in o varnem elektronskem predalu naslovnika, v katerega naj SVEV vloži dokument.

Če SVEV po prejemu elektronskega pisanja ugotovi, da naslovnikovega naslova v njegovem sistemu ni, pošlje na sodišče obvestilo o vrnjeni pošiljki.

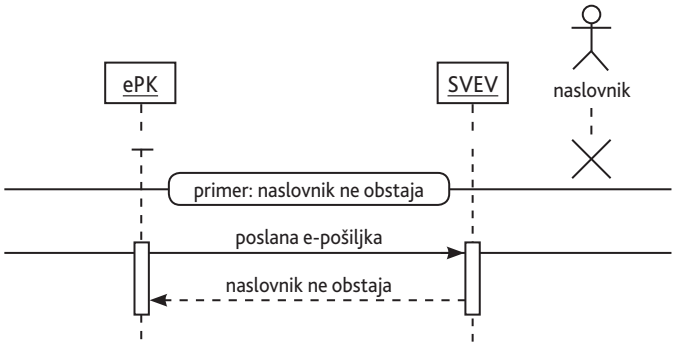
---

[70] Četrti odstavek 2. člena ZEPEP.

[71] Podrobnejša uporabniška navodila za registrirane uporabnike portala e-sodstvo so dostopna na https://evlozisce.sodisce.si/esodstvo/index.html (10. 5. 2011).

[72] Administrator za skupino notarjev je Notarska zbornica Slovenije, za skupino odvetnikov Odvetniška zbornica Slovenije, za skupino izvršiteljev Zbornica izvršiteljev Slovenije (11. člen Pravilnika).

[73] Od 1. 5. 2011 je vlaganje zemljiškoknjižnih predlogov mogoče le še elektronsko.



ePK: modul e-poštna knjiga[74]
SVEV: informacijski sistem za varno elektronsko vročanje[75]

Shema 1: Elektronsko vročanje v primeru, ko naslovnik ne obstaja[76]

SVEV potrdi e-sodstvu prejem pisanja v postopek vročanja, preveri veljavnost varnega elektronskega podpisa in časovnega žiga na njem ter pošlje pisanje naslovniku v varen elektronski predal. Hkrati mu na elektronski naslov pošlje elektronsko obvestilo o prispeli elektronski pošiljki, ki vsebuje podatke o pošiljatelju (sodišču), navodilo, da jo mora prevzeti v 15 dneh, ter opozorilo o posledicah v primeru neprevzema pošiljke.

Naslovnik prevzame pisanje iz varnega elektronskega predala s kvalificiranim potrdilom, s katerim dokaže istovetnost, presname elektronski dokument iz varnega elektronskega predala in elektronsko podpiše vročilnico z varnim elektronskim predpisom. Ne da bi podpisal vročilnico, naslovnik do pisanja v varnem elektronskem predalu ne more dostopati.

Vročitev se šteje za opravljeno z dnem, ko naslovnik prevzame pisanje.

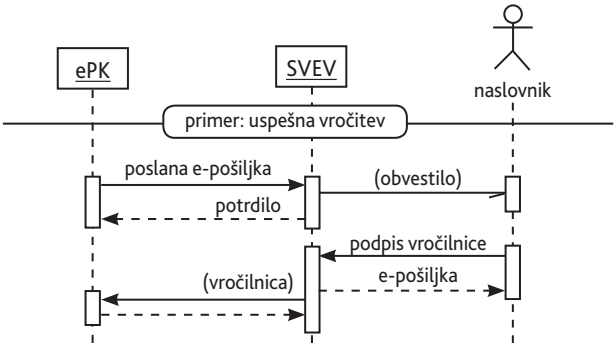
[74] Modul e-poštna knjiga je modul informacijskega sistema e-sodstvo, ki omogoča elektronsko vročanje elektronskih pisanj in vlaganje elektronskih vročilnic v e-spis, samodejno izdelavo pisnih odpravkov elektronskih sodnih pisanj in prepisov elektronskih vlog ali elektronskih prilog in njihovo odpravo po pošti ter podporo pretvarjanju pisnih vročilnic v elektronsko obliko in njihovemu vlaganju v e-spis (deseti odstavek 7. člena Pravilnika).

[75] Vzorci vseh pisanj, ki jih v postopku elektronskega vročanja opravlja informacijski sistem za varno elektronsko vročanje, so vsebovani v dokumentu Funkcionalne in tehnične zahteve informacijskega sistema za varno elektronsko vročanje v civilnih sodnih postopkih.

[76] Shema je povzeta po dokumentu Centra za informatiko Vrhovnega sodišča RS z naslovom Funkcionalne in tehnične zahteve informacijskega sistema za varno elektronsko vročanje v civilnih sodnih postopkih, str. 5, dostopno na https://evlozisce.sodisce.si/esodstvo/index.html (10. 5. 2011).

SVEV po prevzemu pisanja e-sodstvu pošlje elektronsko vročilnico,[77] podpisano z naslovnikovim varnim elektronskim podpisom. Na tak način je sodišče, ki je vročanje odredilo, obveščeno o opravljeni vročitvi.[78]

Elektronske oblike vročilnice ZPP pred uvedbo elektronskega vročanja ni poznal, zato je novela ZPP-C določila, da njeno vsebino in obliko določi minister za pravosodje.[79] V skladu s Pravilnikom mora elektronska vročilnica vsebovati podatke o sodišču, ki pisanje pošilja, podatke o naslovniku in besedilo: »Naslovnik potrjujem, da sem dne … (datum elektronskega podpisa vročilnice) sprejel pošiljko z oznako … (oznaka dokumenta, ki jo je ob odpravi določil informacijski sistem e-sodstvo).«



Shema 2: Elektronsko vročanje v primeru, da naslovnik pisanje prevzame[80]

Problem teka 15-dnevnega roka, v katerem mora naslovnik pisanje prevzeti iz varnega elektronskega predala

Že od uvedbe elektronskega vročanja v pravdni postopek velja pravilo, da je naslovnik z informativnim obvestilom na elektronski naslov obveščen, da je v informacijskem sistemu pisanje, ki ga mora prevzeti v 15 dneh od dne, ko mu je bilo pisanje poslano v njegov varni poštni predal, ter opozorjen na posledice, če tega ne bo storil. To obvestilo naj bi bilo v skladu s petim odstavkom 141.a člena ZPP naslovniku poslano sočasno z vročitvijo pisanja v njegov varni elektronski predal, kar bi pomenilo, da je naslovnik obveščen o čakajočem pisanju v istem trenutku, ko se začne 15-dnevno čakanje pisanja na prevzem v varnem

[77] Osmi odstavek 141.a člena ZPP.

[78] Členi 25 do 28 Pravilnika.

[79] Člen 149 ZPP.

[80] Shema je povzeta po dokumentu Centra za informatiko Vrhovnega sodišča RS z naslovom Funkcionalne in tehnične zahteve informacijskega sistema za varno elektronsko vročanje v civilnih sodnih postopkih, str. 5.

elektronskem predalu. Če bi med pošiljanjem informativnega sporočila na elektronski naslov naslovnika prišlo do napake in ta sporočila ne bi prejel, bi šlo to v njegovo škodo, saj bi 15-dnevni rok tekel (in se iztekel) od prispetja pisanja v varni elektronski predal. Tudi pridevnik »informativno« obvestilo potrjuje, da obvestilo nima pravnih učinkov in začetek teka oziroma tek roka nanj ni vezan. V skladu z zakonsko ureditvijo ZPP se tako rok, ki ga ima naslovnik za prevzem pisanja, v vsakem primeru izteče v 15 dneh od dne, ko je pisanje prispelo v njegov varni poštni predal, imetniki teh pa imajo obveznost rednega preverjanja, saj se ne morejo zanesti, da bodo o morebitnem prispetju pisanja tako ali tako obveščeni z informativnim sporočilom.

Drugače pa določa prvi odstavek 28. člena Pravilnika o elektronskem poslovanju v civilnih sodnih postopkih, ki je bil sprejet na podlagi ZPP in z namenom njegovega podrobnejšega urejanja. Omenjeni člen namreč določa, da pride do učinka fikcije vročitve, če naslovnik elektronske pošiljke ne prevzame v 15 dneh od dne, ko je prejel obvestilo o prispeli elektronski pošiljki. Razlika v ureditvah ni problematična, če je hkrati z vročitvijo pisanja v varni elektronski predal naslovniku poslano informativno sporočilo, ki dejansko prispe na njegov elektronski naslov. V tem primeru niti ni pomembno, ali štejemo tek roka od prvega ali drugega dejanja, saj sta oba umeščena v isti časovni trenutek.

Problem pa nastane, kadar hkrati z vročitvijo pisanja v varni elektronski predal na naslovnikov elektronski naslov informativno sporočilo bodisi ni poslano bodisi je poslano, a zaradi kakršnihkoli ovir oziroma razlogov ne prispe do naslovnika ali pa do njega prispe kasneje, kot je bilo pisanje vročeno v varen elektronski predal. Po zakonski ureditvi bo namreč 15-dnevni rok, v katerem ima naslovnik čas prevzeti pisanje, tekel od prispetja tega v varni elektronski predal, po podzakonski pa od prispetja informativnega sporočila na naslovnikov elektronski naslov.

Pravilnik v drugem odstavku 26. člena določa to besedilo, ki ga mora vsebovati informativno obvestilo naslovniku pisanja:

Obveščamo vas, da je v vaš varni elektronski predal dne _____ <*datum posredovanja obvestila*> prispela pošiljka, z oznako _____ <*oznaka dokumenta, ki jo je ob odpravi določil informacijski sistem e-sodstvo*>.

Pošiljko lahko prevzamete v roku 15 dni v vašem varnem elektronskem predalu na naslovu _____ <*naslov s povezavo za dostop*>. Rok za prevzem začne teči od dne _____ <*datum posredovanja obvestila*>. Če v tem roku pošiljke ne boste prevzeli, se bo po sedmem odstavku 141.a člena ZPP s potekom tega roka vročitev štela za opravljeno.

Isto določbo predvideva tudi vzorec obvestila, objavljen v dokumentu Funkcionalne in tehnične zahteve informacijskega sistema za varno elektronsko vročanje v civilnih in sodnih postopkih, ki ga je izdal Center za informatiko Vrhovnega sodišča RS.

Naslovnik bo torej obveščen o dnevu, ko je pisanje prispelo v njegov varni elektronski predal, a tudi opozorjen, da 15-dnevni rok teče od dneva prejema tega obvestila.

Ustava RS določa, da morajo biti podzakonski predpisi v skladu s splošno veljavnimi načeli mednarodnega prava, z veljavnimi mednarodnimi pogodbami, ustavo in zakoni.[81] Kadar na nezakonit oziroma protiustaven podzakonski predpis pri odločanju naleti redno sodišče, uporabi možnost, da odkloni uporabo podzakonskega predpisa (*exceptio illegalis*), saj je pri odločanju vezano zgolj na ustavo in zakone.[82] S tem pa podzakonski predpis še ne neha veljati. O njegovi skladnosti z ustavo in zakoni odloča Ustavno sodišče, ki ga lahko razveljavi ali odpravi.

Podzakonski akti so namenjeni določitvi izvrševanja zakonsko določenih razmerij. Tako Pravilnik določa izvrševanje elektronskega poslovanja v civilnih sodnih postopkih, kar je v pravdni postopek uvedel ZPP. Ureditev v Pravilniku, ki je neskladna z zakonom, je treba spremeniti in določiti, da se tek 15-dnevnega roka, v katerem lahko naslovnik prevzame pisanje, šteje od njegovega prispetja v varni elektronski predal.

Če pa bi zakonodajalec ugotovil, da je primernejša trenutna ureditev pravilnika, je treba spremeniti določbo petega odstavka 141.a člena ZPP. V tem primeru bodo morali biti informacijski sistemi za varno elektronsko vročanje, pri katerih bodo imeli subjekti odprte varne elektronske predale, povezani z elektronsko pošto naslovnikov ter se bo moral šteti rok za prevzem pisanja (in posledično zablokirala možnost prevzema pisanja) po 15 dneh od prispetja informativnega obvestila na elektronski naslov.

Naslovniku prijaznejša je ureditev, ko rok teče od trenutka, ko je bil obveščen, da ga pisanje čaka v varnem elektronskem predalu, torej od trenutka, ko je obvestilo o tem prispelo na njegov elektronski naslov, vendar se s tako ureditvijo ne strinjam. Subjekt, ki odpre varen elektronski predal, ima dolžnost redno preverjati njegovo vsebino, ne glede na to, ali na elektronski naslov prejme kakšno obvestilo ali ne. Primernejša se mi tako zdi ureditev, ki jo vsebuje ZPP, zato je treba ureditev nezakonitega Pravilnika spremeniti.

Fikcija vročitve

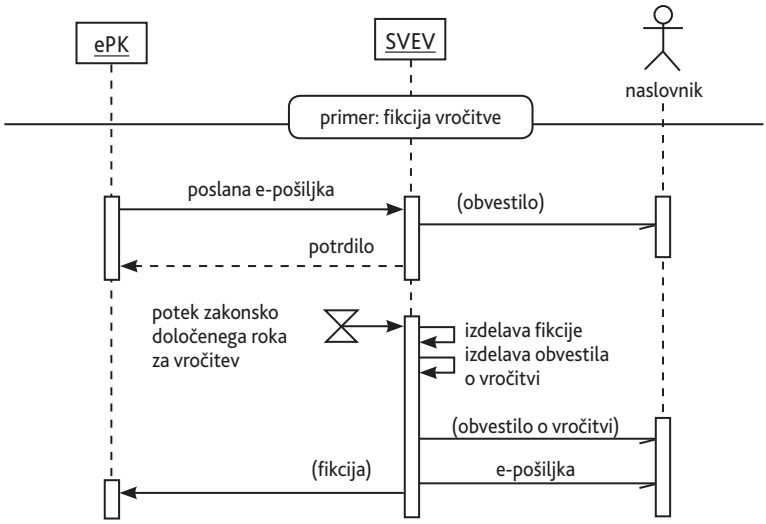
Če naslovnik pisanja ne prevzame v 15 dneh (po zakonski ureditvi od dne, ko je pisanje prejel v varni elektronski predal, po podzakonski pa od dne, ko je prejel informativno sporočilo o pisanju), informacijski sistem pisanje izbriše, naslovniku pa pošlje obvestilo, da je pisanje izbrisano ter da ga lahko prevzame

[81] Člen 153 Ustave RS.

[82] Člen 125 Ustave RS.

pri sodišču, ki je vročitev odredilo.[83] Hkrati informacijski sistem o tem obvesti sodišče, ki je vročitev odredilo.

Novela ZPP-C je ob uvedbi elektronskega vročanja določila, da če naslovnik pisanja ne prevzame v roku, velja vročitev za opravljeno z dnem, ko je informacijski sistem samodejno poslal naslovniku pisanje v njegov varni elektronski predal. Novela ZPP-D je ureditev spremenila in določila, da v primeru neprevzema pisanja v 15-dnevnem roku velja vročitev za opravljeno z dnem poteka tega roka.[84]



Shema 3: Elektronsko vročanje v primeru fikcije vročitve[85]

Prejšnja ureditev je bila skladna z ureditvijo neosebnega načina klasičnega vročanja, pri katerem je bila fikcija vročitve postavljena v trenutek, ko je vročevalec v predalčniku pustil obvestilo o tem, da se pisanje nahaja pri sodišču ter da ima naslovnik rok petnajstih dni, da ga prevzame, česar ta ni storil. Tako se je tudi pisanje, vročeno po elektronski poti, štelo za vročeno takoj, ko je prispelo v varen elektronski predal, če ga naslovnik v roku 15 dni ni prevzel. Pri tem je bilo elektronsko vročanje pisanj, ki so se sicer vročala osebno, za naslovnike slabša možnost, saj jim informacijski sistem pisanja ni poskušal vročiti dvakrat, ampak je 15-dnevni rok tekel že od vložitve pisanja v njihov varen elektronski predal.

[83] Sedmi odstavek 141.a člena ZPP.

[84] Sedmi odstavek 141.a člena ZPP.

[85] Shema je povzeta po dokumentu Centra za informatiko Vrhovnega sodišča RS z naslovom Funkcionalne in tehnične zahteve informacijskega sistema za varno elektronsko vročanje v civilnih sodnih postopkih, str. 5.

ZPP-D je spremenil ureditev tako za navadno kot tudi za elektronsko vročanje.

V primeru neuspešne neosebne vročitve vročevalec pisanje pusti v predalčniku. Šteje se, da je bila vročitev s tem opravljena. V primeru neuspešne osebne vročitve pa vročevalec v predalčniku pusti obvestilo o tem, kje je pisanje, in opozori na 15-dnevni rok za prevzem. V primeru neprevzema pisanja se trenutek fikcije vročitve premakne za 15 dni, torej s trenutka vložitve pisanja v predalčnik na trenutek poteka 15-dnevnega roka.

Medtem ko je bila fikcija vročitve v prejšnji ureditvi elektronskega vročanja primerljiva z ureditvijo neosebnega vročanja po klasični poti, so nekateri[86] opozorili, da zdaj, postavljena v pretečeni petnajsti dan, povzroča podaljševanje časa in poti do naslovnika. Ta ureditev namreč ni več primerljiva z neosebnim načinom vročitve pisanja, pri katerem se vročitev šteje za opravljeno z dnem, ko je bilo pisanje puščeno v predalčniku, ampak z osebnim načinom, pri katerem je trenutek fikcije vročitve postavljen v pretek petnajstdnevnega roka, ki ga je imel naslovnik na voljo, da bi pisanje prevzel.

Glede na to, da pri osebnem načinu klasičnega vročanja naslovnik uživa višjo stopnjo zaščite kot pri neosebnem, elektronski način vročanja pa velja kot osebna in neosebna vročitev, se mi zdi smiselno, da je naslovnik pisanja, ki se vroča osebno, te zaščite deležen tudi pri elektronski poti. Če bi se pisanje po elektronski poti štelo za vročeno z dnem, ko bi naslovnik pisanje prejel v varni elektronski predal,[87] bi bil naslovnik, ki bi mu bilo pisanje, ki se sicer vroča osebno, vročeno po elektronski poti, v slabšem položaju kot tisti, ki bi se mu isto pisanje vročilo po pošti. Taka ureditev bi bila diskriminatorna, zaradi česar je stranke v postopku ne bi želele in je ne bi predlagale sodišču. Institut elektronske vročitve se v praksi tako ne bi uporabljal. Bolje je, da je v situacijah, v katerih je predvidena enaka ureditev za pisanja, ki se vročajo na osebni in neosebni način, poskrbljeno za večjo zaščito naslovnikov in je trenutek fikcije vročitve premaknjen.

Druga možnost je seveda vzpostavitev dvojnega sistema elektronskega vročanja. Tako bi se za pisanja, ki se vročajo osebno, v primeru njihovega neprevzema iz varnega elektronskega predala štelo, da so vročena s potekom petnajstega dne, za pisanja, ki se vročajo neosebno, pa, da so naslovniku vročena s trenutkom, ko prispejo v njegov varni elektronski predal. Tak sistem bi bil sicer najbolj pravičen, saj bi popolnoma ustrezal ureditvi, ki jo ZPP predvideva za primer vročitve po pošti, ter ne bi pozitivno diskriminiral naslovnikov, ki jim je po elektronski

[86] V. Rijavec, v: L. Ude, N. Betetto, A. Galič, V. Rijavec, D. Wedam Lukić in J. Zobec, Pravdni postopek, zakon s komentarjem spremenjenih členov, 4. knjiga, GV Založba in Uradni list Republike Slovenije, Ljubljana 2010, str. 120.

[87] Kot je bila v ZPP ureditev pred novelo ZPP-D.

poti poslano pisanje, ki se vroča neosebno, a ga ne prevzamejo. Vendar pa bi taka ureditev seveda pomenila večjo zapletenost sistema, ki bi moral omogočati dve različni poti vročanja, hkrati pa bi zahtevala višjo stopnjo skrbnosti od sodnikov oziroma zaposlenih na sodiščih, ki bi pisanja pošiljali v informacijski sistem e-sodstvo, pri čemer bi morali označiti, ali se pisanje vroča na osebni ali neosebni način.

Res je, da sedanja ureditev destimulira elektronsko vročanje, saj bo pisanje, za katero se ne zahteva osebno vročanje, vročeno po klasični poti, veljalo za vročeno takoj, ko ga bo vročevalec pustil v predalčniku, medtem ko bo v varnem elektronskem predalu čakalo na potek petnajstdnevnega roka.[88] Vendar se mi zdi potrebno zaščititi naslovnika pisanja, ki se vroča osebno, četudi bodo (ker velja enotni sistem elektronskega vročanja) zato pozitivno diskriminirani prejemniki drugih. Fikcija vročitve, postavljena v trenutek preteka roka 15 dni, se mi tako zdi ustrezna.

7.5. Čas vročanja

Ker vročitev pisanja v elektronski predal naslovnika ne moti, se lahko opravi kadarkoli in tako ni vezana na urnik od 6. do 22. ure, ki ga za fizično vročanje določa 139. člen ZPP.

7.6. Kraj vročanja

Naslov varnega elektronskega predala se šteje za enakovrednega naslovu prebivališča oziroma sedežu stranke.[89] Naslov sodišču sporoči stranka (bodisi ob vložitvi svoje vloge po elektronski poti bodisi v vlogi v fizični obliki ob zahtevi, da se ji pisanja vročajo po elektronski poti), naslovi varnega elektronskega predala oseb oziroma organov iz sedmega odstavka 132. člena ZPP pa so na seznamu, ki ga objavi Vrhovno sodišče na svoji spletni strani.

Elektronsko vročanje odpravi vse probleme glede kraja vročanja pisanja. Naslov elektronskega vročanja je znan, v nasprotju z naslovom pri navadnem vročanju, pri katerem ga navede nasprotna stranka (na primer tožeča za toženo stranko) ali ga sodišče pridobi iz registra.

Če naslovnik naslov za elektronsko vročanje spremeni oziroma ga ukine, bo informacijski sistem pri elektronskem vročanju to zaznal in vročitev ne bo mogoča. Da je bil naslov spremenjen, bo tako razvidno takoj in ne bo takih težav kot

[88] Tako tudi A. Galič, Vročanje pravnim osebam, podjetnikom in odvetnikom, Pravna praksa, št. 5/2010, priloga, str. V.

[89] Četrti odstavek 132. člena ZPP.

pri navadnem vročanju, ko je pisanje puščeno v hišnem predalčniku naslovnika, za katerega se šele kasneje ugotovi, da se je s tega naslova odselil. Naslovnik se lahko poljubno seli, elektronska komunikacija s sodiščem (tudi elektronsko vročanje) pa ves ta čas poteka nemoteno, dokler ima naslovnik seveda dostop do računalnika, na katerem ima naloženo varno digitalno potrdilo.

8. Stanje v praksi

Za popoln zagon elektronskega vročanja v civilnih sodnih postopkih so, kot je bilo omenjeno že v 4. poglavju, potrebni trije elementi, in sicer institucionalna ureditev, organizacijski okvir ter tehnološka oprema. Medtem ko je institucionalna ureditev s sprejetimi spremembami zakonov in podzakonskih aktov v teorijo uvedla pravno podlago za elektronsko vročanje, pa se v praksi še čaka, da se sodišča tehnološko opremijo in v svoje postopke začnejo vnašati elektronska dejanja. Pomembno vlogo pri začetku elektronskega vročanja pa bodo igrale tudi zakonsko določene kvalificirane skupine oseb in organov, za katere sta odprtje varnih elektronskih predalov in registracija na informacijskem portalu e-sodstvo obvezna, saj se bo vročanje njim avtomatsko izvajalo po elektronski poti.

Glede na podatke Vrhovnega sodišča je projekt e-vložišče (kamor spada elektronsko vročanje) v fazi priprave, konec celotnega projekta e-pravosodje pa je predviden za leto 2014.

9. Ureditev vročanja v nekaterih evropskih državah

Elektronsko vročanje se je kot način vročanja v civilnem pravdnem postopku že uveljavilo v nekaj drugih evropskih državah.

Nemčija ima v svojem zakonu o pravdnem postopku (Zivilprozessordnung[90]) predvideno možnost elektronskega vročanja, in sicer se osebam oziroma organom z višjo stopnjo zaupanja, med katerimi eksemplifikatorno našteva odvetnike, notarje, sodne izvršitelje in davčne svetovalce, pisanja *lahko* vročajo elektronsko. Prav tako se elektronsko lahko vroča tudi drugim strankam, ki so se s tem načinom vročanja izrecno strinjale. Dokument, posredovan po elektronski poti, mora vsebovati elektronski podpis in biti zaščiten pred nepooblaščenim dostopom tretjih oseb. Naslovnik pa mora kot dokaz o prejemu pisanja na sodišče poslati potrdilo o prejemu pisanja z navedenim datumom, podpisano s kvalificiranim elektronskim podpisom.

[90] Dostopen na http://www.gesetze-im-internet.de/zpo/__174.html (11. 5. 2011).

Elektronsko vročanje sodnih pisanj je mogoče tudi v *Angliji,*[91] in sicer se mora stranka oziroma njen odvetnik s tem predhodno strinjati v vlogi ter pri tem navesti elektronski naslov, na katerega naj bo pisanje poslano. Če je v vlogi stranke naveden elektronski naslov, se to šteje kot soglasje k elektronskemu načinu vročanja.

Elektronsko vročanje je pod določenimi pogoji veljavno tudi na Finskem,[92] Češkem, v Franciji,[93] Španiji, Italiji, Avstriji …[94]

10. Ureditev elektronskega vročanja v drugih postopkih

Elektronsko vročanje je bilo, hkrati z nekaterimi drugimi dejanji elektronskega poslovanja, najprej uvedeno v upravni postopek (leta 2004),[95] čez tri leta še v pravdni postopek, leto kasneje pa še v kazenski.

Ureditev je v vseh treh postopkih podobna.

Medtem ko je pogoj za elektronsko vročanje v pravdnem in kazenskem postopku enak, tj. stranka sodišču sporoči, da želi vročitev pisanja v varni elektronski predal, oziroma sama pošlje pisanje na sodišče po tej poti, je v upravnem postopku še dodatna možnost. Upravni organ lahko po elektronski poti vroči pisanje tudi, če sam zanesljivo ugotovi, da ima stranka varen elektronski predal. Taka ureditev strankam vsiljuje elektronsko vročanje tudi, če same niso dale pobude za to. Ko oseba enkrat odpre varni elektronski predal, ne da bi za to vedela, zanjo velja zakonska domneva ZUP, da se ji pisanja v upravnem postopku vročajo po elektronski poti.

Tako kot v pravdnem je tudi v kazenskem postopku določena skupina oseb oziroma organov, pri katerih se domneva večja zanesljivost, zaradi česar se pisanja vedno vročajo v varni elektronski predal. V to nezaključeno skupino spadajo državni tožilec in drugi državni organi, odvetniki, sodni izvedenci, sodni cenilci, sodni tolmači ter morebitni drugi, za katere se domneva zadostna zanesljivost.

Tudi v upravnem postopku so državni organi, organi samoupravnih lokalnih skupnosti ter pravne in fizične osebe, registrirane za opravljanje dejavnosti, glede

[91] Točki 4.1 Direction 6A in 6.3 d v Civil Procedure rules, dostopen na http://www.justice.gov.uk/guidance/courts-and-tribunals/courts/procedure-rules/civil/index.htm (11. 5. 2011).

[92] Glej http://www.finlex.fi/pdf/saadkaan/E0030013.PDF (15. 5. 2011).

[93] Code de Procedure Civile, 21. naslov 1. knjige. Vir: http://www.legifrance.gouv.fr/affichCode.do;jsessionid=9E8EB0C872B17F1E8F6293E61AF202F5.tpdjo11v_1?idSectionTA=LEGISCTA000006117246&cidTexte=LEGITEXT000006070716&dateTexte=20110516 (16. 5. 2011).

[94] Glej http://ec.europa.eu/civiljustice/serv_doc/serv_doc_ec_en.htm (12. 5. 2011).

[95] Področje na podzakonski ravni ureja Uredba o upravnem poslovanju, Uradni list RS, št. 20/2005 s spremembami in dopolnitvami.

vročanja postavljeni v poseben položaj, in sicer se jim pisanja praviloma vročajo na elektronski način, če varnega elektronskega predala nimajo, pa po fizični poti. Zanje torej ne velja obveznost odprtja varnega elektronskega predala, kot je to določeno za nekatere skupine v pravdnem in upravnem postopku, kljub temu pa obstaja tendenca elektronskega vročanja, če je to seveda mogoče.

Elektronska pot vročanja je v vseh treh postopkih enaka, torej prek informacijskega sistema (v upravnem postopku je to poseben informacijski sistem za sprejem vlog, vročanje in obveščanje) s posredovanjem organizacije, ki opravlja elektronsko vročanje kot svojo dejavnost. Hkrati s pisanjem se v varni elektronski predal v vseh treh postopkih o tem pošlje na naslovnikov elektronski naslov informativno obvestilo. Naslovnik ima 15-dnevni rok, ki teče od prispetja pisanja v varni elektronski predal. V tem roku mora pisanje prevzeti, kar stori tako, da z uporabo kvalificiranega elektronskega potrdila dokaže svojo istovetnost, z elektronskim podpisom podpiše vročilnico in presname pisanje. Vročitev v vseh treh postopkih velja za opravljeno z dnem, ko naslovnik prevzame pisanje, o čemer se pošiljatelj obvesti z elektronsko vročilnico. Če ga ne prevzame, velja pisanje v upravnem in pravdnem postopku za vročeno s potekom petnajstega dne, le da se v pravdnem postopku pisanje nato izbriše, naslovnik pa obvesti, da ga lahko prevzame na sodišču, v upravnem postopku pa lahko naslovnik po poteku roka še vedno dostopa do pisanja v varnem elektronskem predalu. V kazenskem postopku je ureditev v primeru neprevzema pisanja drugačna. Po preteku roka informacijski sistem pisanje izbriše, naslovnika in sodišče pa obvesti, da se bo pisanje vročalo ponovno, in sicer po fizični poti. Ureditev je smiselna, saj je kazenski postopek po naravi navadno bolj obremenjujoč za subjekt vročanja in je zato treba poskrbeti za to, da bo pisanje zagotovo vročeno.[96]

Elektronsko vročanje je do zdaj zaživelo le v upravnem postopku, kjer je bilo tudi najprej uvedeno, na njegovo uporabo v sodnih postopkih pa bo treba še počakati.

11. Sklep

Elektronsko vročanje v sodnih postopkih bo poslovanje sodišč poenostavilo, vročanje naredilo preglednejše, hitrejše in bolj zanesljivo (poleg tega je še bolj ekološko). Ker ima velik delež strank v postopkih pooblaščenca (odvetnika), za katere bo elektronsko vročanje obvezno, hkrati pa je čedalje večji del prebivalstva vešč dela z internetom, se bo število klasičnih vročitev zmanjšalo, kar bo vročanje hkrati pocenilo. Prednosti elektronske oblike vročanja je tako veliko, šele ko bo zaživelo v praksi, pa se bodo pokazale slabosti.

[96] Členi 117 in 117a ZKP in 83 do 91 ZUP.

V želji po čimprejšnjem doseganju vseh teh prednosti, ki jih bo elektronsko poslovanje sodstva prineslo, pa je treba pri ureditvi in izvajanju vseh treh komponent, organizacijske, tehnološke in institucionalne, vedno upoštevati načela pravne varnosti in predvidljivosti, pravičnosti, enakosti pred zakonom in ekonomičnosti.

IV.
Informacijske tehnologije na področju javnega prava

Domet pravne ureditve spletnih iger na srečo

dr. Katarina Zajc, Neža Muhič in Luka Markelj

1. Uvod

Igre, v katerih je izid igre odvisen od naključja oziroma negotovega dogodka, so že od nekdaj priljubljene in so postale del človeške kulture. Igre na srečo lahko razdelimo na dve veliki skupini – klasične igre na srečo, ki pomenijo fizično prirejanje iger na srečo na določeni lokaciji (*land-based* ali *off-line gaming*), in spletne igre na srečo (*on-line gaming*), pri čemer so predmet obravnave v tem prispevku slednje. Z razvojem informacijske tehnologije, ki omogoča prirejanje iger na srečo brez neposrednega stika prireditelja in igralca, so igre na srečo pridobile nov zagon. V okvir spletnih iger na srečo uvrščamo vse oblike prirejanja iger na srečo na daljavo, kot so trenutno na primer preko osebnega in prenosnega računalnika, mobilnega telefona in tabličnega računalnika ali preko interaktivne televizije, z razvojem tehnologije pa se razvijajo vedno novi informacijski kanali. Upoštevaje splošen trend prodaje pametnih mobilnih telefonov in tabličnih računalnikov v prihodnosti pričakujemo zlasti rast mobilnih spletnih iger na srečo. Po oceni Evropske komisije[1] so leta 2011 prihodki sektorja iger na srečo znašali 84,9 mrd EUR z letno stopnjo rasti 3 odstotke, od tega prihodki spletnih iger na srečo kar 9,3 mrd EUR, njihova letna stopnja rasti pa znaša 15 odstotkov. Močna rast spletnih iger na srečo se odraža tudi na predvidenih prihodkih spletnih iger na srečo leta 2015, ki so ocenjeni na 13 mrd EUR. Velikost evropskega trga spletnih iger na srečo je ocenjena na okoli 6,8 milijona potrošnikov. Močan socialni in ekonomski pomen iger na srečo in tudi spletnih iger na srečo se odslikava v pravni regulaciji tega področja v posameznih državah ter hkrati v dejstvu, da (spletne) igre na srečo niso predmet harmonizacije na ravni Evropske unije.

Predmet tega dela je pravna analiza omejevanja ponudbe iger na srečo, ki je v skladu z evropsko sodno prakso, ter izzivov, ki jih predstavlja čezmejno prirejanje spletnih iger na srečo, torej problematike, ko prireditelj spletnih iger na srečo načeloma, ali pa tudi ne, razpolaga z dovoljenjem za prirejanje iger na

[1] Evropska komisija, Gambling, http://ec.europa.eu/internal_market/gambling/index_en.htm (15. 11. 2013).

srečo v posamezni državi članici EU ali tretji državi, ne razpolaga pa z dovoljenjem za prirejanje spletnih iger na srečo tiste države, v kateri dejansko prireja spletne igre na srečo – državljani katere vplačujejo za udeležbo v igrah na srečo. Pravna ureditev področja (spletnih) iger na srečo je v nacionalnih ureditvah sicer zelo različna, a hkrati jasna in v osnovi prepoveduje prirejanje (spletnih) iger na srečo brez dovoljenja nacionalnih organov. Problem je vprašanje, na kakšen način se lahko sankcionira in prepreči nadaljnje prirejanje spletnih iger na srečo, saj sta nadzor nad ilegalnimi prireditelji spletnih iger na srečo in onemogočanje delovanja teh izredno težavna. Ne pomaga niti dobra tehnologiji ali pa je težava ravno v njej. Problem pa ne obstaja le na območju EU. Potrošniki so izpostavljeni tudi prevaram in zlorabam prireditelјev spletnih iger na srečo s sedežem zunaj EU.[2] Svetovni splet je v obliki, kot ga poznamo, globalni medij brez centralnega organa upravljanja, zato je popolni nadzor iluzija, poleg tega pa je nadzor (cenzura) interneta v zahodni civilizaciji sporen z vidika človekovih pravic in zato nesprejemljiv tudi iz tega razloga. Nacionalni nadzorni organi so postavljeni v nezavidljiv položaj, ko bolj ali manj (ne)uspešno izvršujejo nacionalno zakonodajo na področju spletnih iger na srečo.

Po uvodu je v drugem delu obravnavana pravna ureditev prirejanja iger na srečo v EU, tretji del pa predstavi pravno ureditev prirejanja spletnih iger na srečo v Sloveniji, s posebnim poudarkom na možnostih sankcioniranja nelegalnih prireditelјev igre na srečo in pregledom sedanje predlagane ureditve, temu pa sledi sklepni del.

2. Pravna ureditev iger na srečo v Evropski uniji

Veliko vprašanje je, ali naj bodo spletne igre na srečo dovoljene, v kakšnem obsegu in koliko naj jih regulirajo države članice ter ali naj bo regulacija spletnih iger tudi v pristojnosti EU.

Ker se na področju predpisov o igrah na srečo pojavljajo moralna, verska in kulturna razhajanja in ker ni dovolj političnega konsenza, to področje na ravni EU ni enotno urejeno. Na področju iger na srečo morajo države članice na podlagi lastne lestvice vrednot presojati zahteve za varstvo zadevnih interesov (*Henn and Darby*,[3]

[2] Poudariti je treba, da se potrošnik običajno niti ne zaveda oziroma ga ne zanima, da je udeležen v igrah na srečo pri tujem prireditelju, ki nima dovoljenja za prirejanje iger na srečo v njegovi državi, saj so spletne strani v nacionalnih jezikih, pa tudi sicer potrošnika ne prizadenejo dodatni transakcijski stroški (na primer bančni stroški, stroški poštnine) v primerjavi z nacionalnimi prireditelji iger na srečo.

[3] Sodba Sodišča v zadevi 34/79, *Regina proti Maurice Donald Henn in John Frederick Ernest Darby* (1979).

točka 15; *Schindler*,[4] točka 32; *Jany in drugi*,[5] točka 56 in 60; *Placanica*,[6] točka 47; *Liga Portuguesa*,[7] točka 57; *SIA Garkalns*,[8] točka 36). V teh okvirih države članice presojajo, ali je za dosego cilja treba omejiti igralniško dejavnost oziroma ali je treba prepovedati igralniško dejavnost deloma ali v celoti in ali je treba sprejeti kontrolne mehanizme, upoštevajoč, da omejitve ne smejo biti diskriminatorne (*Schindler*, točka 61; *Läärä*,[9] točka 14 in 35; *Zenatti*,[10] točka 15; *SIA Garkalns*, točka 37).

Države članice same odločajo o organiziranosti sektorja iger na srečo, morajo pa biti nacionalne ureditve skladne z zakonodajo EU, načeli in pravili notranjega trga ter prakso Sodišča Evropske unije (v nadaljevanju Sodišče).[11] Države imajo kar nekaj diskrecije za varstvo upravičenih ciljev javnega interesa, skladno s Pogodbo o delovanju Evropske unije (PDEU).[12] Sodišče je v zadevah *Schindler, Läärä* in *Zenatti* zavzelo stališče, da so omejitve igralniške dejavnosti lahko upravičene z nujnimi razlogi v splošnem interesu. Vendar morajo biti omejitve na podlagi razlogov v splošnem interesu in razlogov javnega reda primerne za dosego ciljev in morajo služiti omejevanju igralniških priložnosti dosledno in sistematično (*SIA Garkalns*, točka 41, 42, 43) ter morajo v zvezi z njihovo sorazmernostjo[13] izpolnjevati pogoje, ki izhajajo iz ustaljene prakse Sodišča (*Placanica*,[14] točka 48). Upravičeni cilji javnega interesa so predvsem varstvo potrošnikov, javni red in financiranje dejavnosti v javnem interesu.

---

[4] Sodba Sodišča v zadevi C-275/92, *Her Majesty's Customs and Excise proti Gerhart Schindler and Jörg Schindler* (1994).

[5] Sodba sodišča v zadevi C-268/99, *Aldona Malgorzata Jany in drugi proti Staatssecretaris van Justitie* (2001).

[6] Sodba Sodišča v združenih zadevah C-338/04, C-359/04 in C-360/04, v postopkih zoper Massimiliana Placanico, Christiana Palazzeseja in Angela Sorricchia (2007).

[7] Sodba v zadevi C-42/07, *Liga Portuguesa de Futebol Profissional in Bwin International Ltd, formerly Baw International Ltd proti Departamento de Jogos da Santa Casa da Misericórdia de Lisboa* (2009).

[8] Sodba Sodišča v zadevi C-470/11, v postopku *SIA Garkalns proti Rīgas dome* (2012).

[9] Sodba sodišča v zadevi C-124/97, *Markku Juhani Läärä, Cotswold Microsystems Ltd in Oy Transatlantic Software Ltd proti Kihlakunnansyyttäjä (Jyväskylä) in Suomen valtio* (finska država) (1999).

[10] Sodba Sodišča v zadevi C-67/98, *Questore di Verona proti Diego Zenatti* (1999).

[11] Evropska komisija, Sporočilo komisije Evropskemu parlamentu, Svetu, Ekonomsko-socialnemu odboru in Odboru regij z naslovom Celovitemu evropskemu okviru za spletne igre na srečo naproti z dne 19. decembra 2012, str. 5.

[12] Uradni list C 326, 26. 10. 2012 str. 0001–0390.

[13] S testom sorazmernosti Sodišče najprej preveri, ali obstajajo nujni razlogi v javnem interesu ali pa razveljavitveni razlog, ki zagotavlja legitimnost cilja. Drugo, kar Sodišče presoja pri testu sorazmernosti, je primernost ukrepa. Nazadnje pa Sodišče presoja, ali je ukrep nujen in ali se morebiti da ukrep doseči z milejšimi sredstvi.

[14] Sodba Sodišča v združenih zadevah C-338/04, C-359/04 in C-360/04, v postopkih zoper Massimiliana Placanico, Christiana Palazzeseja in Angela Sorricchia (2007).

Nenadzorovano prirejanje iger na srečo je lahko negativno za posameznika, ki se prostovoljno udeleži iger na srečo, in za širšo družbeno okolico. Sem spadajo negativne posledice za družine vseh odvisnikov od iger na srečo, zapravljanje denarja, povečanje kriminala in drugih kaznivih dejanj.[15] Še bolj to velja za spletne igre na srečo, saj so postale posameznikom dostopne brez večjih stroškov in omejitev. Vse to na trgu povzroča negativne eksternalije, ki jih trg sam ne more odpraviti. Tako je naloga države, da omeji svobodno konkurenco in vzpostavi ureditev, ki bo v največji meri odpravila negativne posledice prisotnosti iger na srečo na trgu.[16]

V EU je prisoten tako črni trg spletnih iger na srečo (nezakonite stave in igre na srečo brez licence) in sivi trg, kjer ponudniki spletnih iger sicer imajo licenco za ponujanje spletnih iger v eni ali več državah članicah, vendar pa ne tudi v državi, kjer jih ponujajo.[17] Proti nezakonitim ponudnikom storitev lahko države izvajajo ukrepe, ki se jim zdijo primerni in potrebni, pri tem pa morajo vselej upoštevati temeljna načela Pogodbe EU. Zakonodaja mora biti sorazmerna, dosledna, pregledna in nediskriminatorna.[18]

2.1. Sodna praksa Sodišča Evropske unije

Ker za sekundarno zakonodajo[19] ni dovolj soglasja, saj so vrednote v posameznih državah članicah tako različne, je večja težnja po doslednem izvajanju primarne zakonodaje. Tako so spletne igre na srečo predmet številnih postopkov pred Sodiščem, kjer se preverja omejevalna zakonodaja znotraj držav članic in skladnost omejitev s primarno zakonodajo Evropske unije.[20] Sodišče je zdaj uvedlo že serijo usmerjevalnih načel in številne države, proti katerim je Komisija začela postopke za ugotavljanje kršitev, so začele z reformami na področju spletnih iger. Študija o igrah na srečo na notranjem trgu EU švicarskega inštituta za primerjalno pravo (2006) je pokazala, da je notranji trg na tem področju zelo omejen in da države članice zelo pogosto določajo omejitve za čezmejno prire-

[15] Kot so na primer nezakonito ponujanje spletnih iger na srečo, nedovoljene spletne igre na srečo, ki jih ponuja ponudnik, ki sicer ima licenco, davčne utaje (Evropska komisija, Zelena knjiga o spletnih igrah na srečo na notranjem trgu z dne 24. 3. 2011, str. 29).

[16] Zajc, Markelj: Ekonomski in pravni pogled na prirejanje spletnih iger na srečo – zakaj je monopol lahko boljši kot prosti trg (2011).

[17] Evropska komisija, Zelena knjiga o spletnih igrah na srečo na notranjem trgu z dne 24. 3. 2011.

[18] Evropski parlament, Poročilo o spletnih igrah na srečo na notranjem trgu z dne 11. 6. 2013, str. 8.

[19] Spletne igre niso predmet urejanja sekundarne zakonodaje in so izvzete v smislu storitev iz veliko direktiv (dejavnosti iger na srečo so izključeno na primer iz direktive o storitvah (2006/123/ES), direktive o elektronskem poslovanju (2000/31/ES) (vir: Poročilo o neoporečnosti iger na srečo)).

[20] Povzeto po Evropska komisija, Zelena knjiga o spletnih igrah na srečo na notranjem trgu z dne 24. 3. 2011.

janje spletnih iger na srečo. Študija je zaznala okoli 600 zadev pred nacionalnimi sodišči, ki kažejo na pravno negotovost.[21]

2.1.1. Splošno o spletnih igrah na srečo

PDEU zagotavlja štiri svoboščine. To so prost pretok blaga, prosto gibanje delavcev, prost pretok storitev in svoboda ustanavljanja ter prost pretok kapitala in plačil. Vse te svoboščine tvorijo skupni notranji trg EU. Temeljno načelo notranjega trga EU je svoboda opravljanja storitev, ki jih države članice ne smejo omejiti. PDEU v 56. členu prepoveduje omejitev svobode opravljanja storitev za državljane držav članic, ki imajo sedež v eni od držav članic, vendar ne v državi osebe, ki so ji storitve namenjene. Dopustne omejitve zajema že sama PDEU. Država članica lahko omeji to svobodo opravljanja storitev, če za to obstaja legitimen cilj. To so lahko javni red, javna varnost in javno zdravje (52. člen PDEU). Iz svobode opravljanja storitev države članice lahko izvzamejo tiste dejavnosti, ki so v tej državi povezane, četudi občasno, z izvajanjem javne oblasti (51. člen PDEU). Druge dopustne omejitve pa naprej določa sodna praksa Sodišča EU.

Igre na srečo so storitve v smislu PDEU. Sodišče je v sodbi *Schindler* zapisalo, da se določba o svobodi opravljanja storitev iz 56. člena PDEU nanaša na dejavnosti, v kateri se uporabniku v zameno za plačilo dovoli sodelovanje v igri, če je vsaj en ponudnik teh storitev ustanovljen v drugi državi članici, kot je država, kjer se storitve ponujajo. Te storitve imajo nadnacionalni značaj, tudi če je posrednik v isti državi članici kot uporabnik storitev (*Zenatti*, točki 24 in 25). Zato uživa tako potrošnik kot tudi prireditelj iger na srečo svobodo opravljanja storitev (*Liga Portuguesa*, točka 51).

Potrošnika se želi zavarovati pred zasvojenostjo, goljufijami, želi se preprečiti pranje denarja in druga kazniva dejanja, ohraniti integriteto športa, preprečiti vnaprej dogovorjene športne izide in zaščititi javni red. Sodišče v ta namen dovoljuje omejitve svobode opravljanja storitev in svobode ustanavljanja, zaradi splošnega interesa.[22] V zadevi *Gambelli*[23] je odločilo, da morajo biti te omejitve upravičene z nujnimi ukrepi v splošnem interesu, biti morajo primerne za dosego cilja in ne smejo iti čez mejo, ki je potrebna za dosego cilja, ter morajo biti uporabljene nediskriminatorno (*Gambelli,* točka 65). Navedeno stališče dopolnjuje Sodišče EFTA s stališčem, da mora biti omejevalni ukrep skladen s podobnimi

[21] Evropska komisija, Zelena knjiga o spletnih igrah na srečo na notranjem trgu z dne 24. 3. 2011, COM (2011) 128 konč., str. 10, 11.

[22] Povzeto po: Poročilo o neoporečnosti spletnih iger na srečo z dne 17. 2. 2009.

[23] Sodba Sodišča v zadevi C-243/01, v postopku zoper Piergiorgia Gambellija in druge (2003).

že sprejetimi ukrepi in država ne sme sprejeti, omogočiti ali dopuščati ukrepov, ki bi nasprotovali v omejevalni zakonodaji sprejetim ciljem.[24]

Sodišče je v zadevah *Schindler* (točke 57 do 60), *Läärä in drugi* (točki 32 in 33), *Zenatti* (točki 30 in 31) in *Gambelli* (točka 67) priznalo kot nujni razlog v splošnem interesu varstvo potrošnikov, preprečevanje goljufije in preprečevanje spodbujanja državljanov k čezmerni porabi pri igranju in preprečevanje vznemirjanja družbenega reda na splošno.[25] Nadalje je Sodišče v zadevi *Liga Portuguesa*[26] potrdilo, da je lahko nujni razlog v splošnem interesu, s katerim je mogoče opravičiti omejitve, tudi boj proti kaznivim dejanjem. Sodišče meni, da je prednost omejenega dovoljevanja iger na srečo na podlagi izključne pravice to, da usmerja prirejanje iger na srečo v nadzorovane okvire in preprečuje, da bi se igre na srečo prirejale v goljufive in kaznive namene (*Läärä in drugi*, točka 37; *Zenatti,* točka 35; *Liga Portuguesa*, točka 64). Sodišče v zadevi *Liga Portuguesa*[27](točka 69) pravi: »... da država članica lahko upravičeno meni, da samega dejstva, da gospodarski subjekt, kot je družba Bwin, prek interneta zakonito ponuja storitve iz tega sektorja v drugi državi članici – kjer ima sedež in kjer zanjo načeloma že veljajo pravni pogoji in jo nadzorujejo pristojni organi te države – ni mogoče šteti za zadostno jamstvo, da bodo nacionalni potrošniki zavarovani pred nevarnostjo goljufije in kaznivih dejanj, če se upoštevajo težave, ki jih lahko imajo v takih okoliščinah organi države članice, v kateri je sedež, pri presoji poklicne usposobljenosti in poštenosti gospodarskih subjektov«. Sodišče je v tej zadevi zaključilo, da 49. člen Pogodbe o Evropski skupnosti (v nadaljevanju PES; zdaj 56. člen PDEU) ne nasprotuje predpisom države članice, s katerimi je gospodarskim subjektom s sedežem v drugih državah članicah, kjer zakonito ponujajo podobne storitve, prepovedano ponujati igre na srečo preko interneta na ozemlju navedene države članice. Navedeno stališče je Sodišče utrdilo tudi v poznejših zadevah *Ladbrokes*,[28] *Sporting Exchange*,[29] *Carmen Media*,[30] *Markus Stoß*.[31]

[24] Sodba Sodišča EFTA, zadeva E-3/00, *Nadzorni organ EFTA proti Kraljevini Norveški* (2001).

[25] Vir: *Placanica in drugi*, 360/04, točka 46.

[26] Sodba Sodišča v zadevi ECJ C-42/07, *Liga Portuguesa de Futebol Profissional in Bwin International Ltd.* (2009).

[27] Prav tam, točka 69.

[28] Sodba Sodišča v zadevi C-258/08 *Ladbrokes Betting & Gaming Ltd in Ladbrokes International Ltd proti Stichting de Nationale Sporttotalisator* (2010).

[29] Sodba Sodišča v zadevi C-203/08 Sporting Exchange Ltd, ki posluje pod imenom *»Betfair«, proti Minister van Justitie* (2010).

[30] Sodba Sodišča v zadevi C-46/08, *Carmen Media Group Ltd proti Land Schleswig-Holstein, Innenminister des Landes Schleswig-Holstein* (2010).

[31] Sodba Sodišča v združenih zadevah C-316/07, od C-358/07 do C-360/07, C-409/07 in C-410/07, *Markus Stoß in drugi proti Wetteraukreis* in *Kulpa Automatenservice Asperg GmbH in drugi proti Land Baden-Württemberg* (2010).

2.1.2. Prepoved ponujanja iger na srečo na ozemlju druge države članice kot omejevalni ukrep

V nekaterih državah članicah so spletne igre na sreče prepovedane za vse vrste iger ali za določene vrste iger na srečo kot na primer poker, kazino igre (Nemčija in Nizozemska). Ponekod lahko spletne igre na srečo ponujajo le subjekti, ki jim je država podelila izključno pravico, monopol za prirejanje iger na srečo (Finska, Portugalska, Švedska). Monopol imajo lahko javni subjekti ali zasebne družbe. Ponekod se z ustanovitvijo licenčnega sistema omogoča prirejanje iger na srečo več subjektom (Danska, Italija, Španija, Estonija, Francija).[32] V skoraj dveh tretjinah držav članic je na področju loterij vzpostavljen monopolni sistem oziroma sistem izključnih pravic, ki se dodelijo državnim upravljavcem ali zasebnim subjektom, ki so pod strogim nadzorom javnega organa (na primer Slovenija).[33] Širše gledano obstajata večinsko trenutno dva modela nacionalnih ureditev. Eden temelji na ponudnikih z licenco, ki opravljajo storitve znotraj reguliranega trga, drugi pa temelji na monopolni ureditvi, ki je strogo nadzorovana s strani nadzornih organov držav članic.[34]

Glede opravljanja čezmejne dejavnosti iger na srečo in stav prav tako obstajajo različne ureditve. Ponekod je izrecno določeno, da dodeljene licence, koncesije in dovoljenja veljajo le za ozemlju države članice. Drugje teh omejitev in prepovedi ni. Ponekod lahko upravljavci iz druge države članice zaprosijo za dovoljenje ali licenco države članice, kjer želijo opravljati storitev. Upravljavci, ki so pridobili licenco, koncesijo ali dovoljenje v državi članici, lahko tako storitve ponujajo tudi v drugi državi članici, če država, v kateri imajo registriran sedež, tega ne preprečuje v okviru nadzora nad upravljavci. Ponekod obstajajo med državami dvostranski dogovori. Večinoma pa države članice, ki imajo monopolno ureditev ali izključne pravice, ovirajo konkurenčno dejavnost in preprečujejo ter prepovedujejo, da bi ponudnik, registriran v drugi državi članici, opravljal storitev na njenem ozemlju.

Sodišče je že v zadevi *Gambelli* povedalo, da je nesporno, da predpis države članice, ki ponudnikom s sedežem v drugi državi članici prepoveduje ponujanje storitev na ozemlju obravnavane države članice prek interneta, pomeni omejitev svobode opravljanja storitev, ki jo zagotavlja 49. člen PES (zdaj 56. člen PDEU) tako ponudniku kot tudi prebivalcem te države. Sodišče je navedlo, da je treba preučiti, ali je omejitev dovoljena na temelju razveljavitvenih ukrepov iz 45. in

[32] Evropska komisija, *Online gambling in the Internal Market – Frequently asked questions*, 23/10/2012. Dostopno na http://europa.eu/rapid/press-release_MEMO-12-798_en.htm (27. 11. 2013).

[33] Svet EU, Igre na srečo in stave: pravni okvir in politike v državah članicah evropske unije z dne 27. 11. 2008.

[34] Evropska komisija, Zelena knjiga o spletnih igrah na srečo na notranjem trgu z dne 24. 3. 2011, str. 3.

46. člena PES (zdaj 51. in 52. člen PDEU), tj. na temelju javnega reda, javne varnosti in javnega zdravja, ali na podlagi sodne prakse z nujnimi razlogi v splošnem interesu.[35]

V državah članicah se pravne ureditve iger na srečo zelo razlikujejo. Razlike se pojavljajo glede števila prireditelјev iger na srečo, glede načinov in oblik državnega nadzora, glede tehničnih zahtev za igralni sistem, ki se ga ponuja preko spleta, glede ravni preverjanja identitete igralcev in ravni zaščite mladoletnih igralcev, glede obremenitev z dajatvami, glede sistemov in stopenj obdavčevanja spletnih iger, glede bolj ali manj strogih pogojev za pridobitev licenc, glede ravni legalizacije spletnih iger.[36] Če se ne spoštujejo omejitve ponujanja spletnih iger na srečo znotraj države sedeža prireditelja in drugi pogoji, določeni z nacionalno zakonodajo, in vdirajo tuji ponudniki z milejšimi pogoji za prirejanje iger in slabšim nadzorom s strani nacionalnih organov, se s tem izničuje zakonodaja in onemogoča njen namen, ki je ravno v večji zaščiti potrošnikov in ranljivih skupin[37] države članice.

2.1.3. Monopol kot omejevalni ukrep držav članic

Eden od omejevalnih ukrepov držav je vzpostavitev monopola na nacionalni ravni. Gre za ureditev, ki močno posega v svobodo opravljanja storitev in prav tako krši temeljna pravila konkurenčnega prava. Za tak ukrep morajo biti izpolnjeni pogoji, ki jih glede omejevanja prostega pretoka storitev določata PDEU in sodna praksa Sodišča. Gre za zelo pogost ukrep držav članic, zato je njegovo skladnost s PDEU Sodišče že večkrat preizkušalo.

Podelitev monopola je po mnenju Sodišča primeren ukrep. Država članica ima pravico podeliti dovoljenje za prirejanje iger na srečo le enemu subjektu (*Läärä*, točka 37; *Zenatti*, točka 35; *Anomar*, točka 74). Izbira sistema izključne pravice, ki se podeli samo enemu subjektu, spada v diskrecijsko pravico države (*Läärä,* točki 35 in 39; *Zenatti*, točka 33; *Anomar,* točka 87).[38] V zadevi *Liga Portuguesa* Sodišče pove, da podeljevanje izključnih pravic za prirejanje iger na srečo prek interneta samo enemu gospodarskemu subjektu, ki je pod strogim

[35] *Placanica*, točka 45.

[36] Odgovori RS Evropski komisiji na vprašanja Zelene knjige o spletnih igrah na srečo na notranjem trgu z dne 25. 7. 2011.

[37] Vidnejše skupine teh so mladoletniki, igralci z nizkimi dohodki, neizkušeni igralci, osebe, ki so imele v preteklosti težave z odvisnostjo in zasvojenostjo, povezano z uživanjem kemičnih snovi ali vedenjem, osebe, ki imajo enostaven dostop do iger na srečo (na primer zaposleni pri ponudniku spletnih iger na srečo), ali druge osebe, ki so pogosto izpostavljene igram na srečo (Zelena knjiga Evropske komisije, str. 25).

[38] Sklepni predlogi generalnega pravobranilca Yvesa Bota, predstavljeni 17. decembra 2009 v zadevah C-203/08 in C-258/08, točki 55 in 56.

nadzorom javne oblasti, lahko omogoča prirejanje iger na srečo v nadzorovanih okvirih in je primerna omejitev za varstvo potrošnikov pred goljufijami gospodarskih subjektov. Ta ukrep po mnenju Sodišča ustreza pojmu legitimnosti (*Liga Portuguesa*, točka 67).

Sodišče v zadevi *Läärä* pravi, da dejstvo, da država iger na sreči ni v celoti prepovedala, ne kaže na to, da namen nacionalne zakonodaje ni dejansko doseganje javnega interesa. Izključna pravica omogoča omejevanje želje po igranju in izkoriščanja igralništva v nadzorovanih okoliščinah, preprečuje tveganje goljufij in kaznivih dejanj ob takem izkoriščanju ter omogoča izkoriščanje dobičkov za dejavnosti v javnem interesu (*Läärä,* točki 37 in 38). Država članica je tista, ki se odloči, ali bo za doseganje tega cilja izbrala izključno pravico ali sprejela strožjo ureditev s predpisanimi obveznostmi za organizatorje, vendar ta odločitev ne sme biti nesorazmerna z zastavljenimi cilji (*Läärä*, točka 39). Nacionalni organi imajo diskrecijsko pravico, da sami določijo zahteve, ki izhajajo iz varstva potrošnikov in družbenega reda, in če so izpolnjeni pogoji, določeni v sodni praksi, mora država članica presoditi, ali je v okviru legitimnih ciljev, ki jih uresničuje, treba v celoti ali delno prepovedati dejavnost iger na srečo in prirejanje stav, ali jih je treba zgolj omejiti in predvideti bolj ali manj strog nadzor (*Stoß in drugi,*[39] točka 9, *Carmen Media Group*,[40] točka 58).

Tudi Sodišče EFTA v zadevi E-1/06[41] sklene, da je utemeljeno domnevati, da bo monopolni operater igralnih avtomatov, ki bo pod učinkovitim nadzorom državne oblasti, bolj težil k zmanjševanju zasvojenosti z igrami na srečo kot bi zasebni operater ali druga humanitarna organizacija, katere obstoj bi bil odvisen od dohodkov od igralnih avtomatov. Po mnenju sodišča je utemeljeno pričakovati, da država učinkoviteje nadzoruje in usmerja državno podjetje kot pa zasebne ponudnike. Države članice monopol pogosto podelijo državnim ustanovam ali državnim podjetjem. Sodišče meni, da je utemeljeno pričakovati, da lahko država učinkoviteje nadzoruje in usmerja državno podjetje, ki je v celoti v državni lasti, kot zasebne ponudnike, saj lahko pri tem deluje kot javna oblast in tudi kot lastnik.

[39] Sodba Sodišča v združenih zadevah C-316/07, C-358/07, C-359/07, C-360/07, C-409/07 in C-410/07, v postopkih *Markus Stoß* (C-316/07), *Avalon Service Online Dienste GmbH* (C-409/07), *Olaf Amadeus Wilhelm Happel* (C-410/07) *proti Wetteraukreis in Kulpa Automatenservice Asperg GmbH* (C-358/07), *SOBO Sport & Entertainment GmbH* (C-359/07), *Andreas Kunert* (C-360/07) *proti Land Baden Württemberg* (2010).

[40] Sodba Sodišča v zadevi C-46/08, *Carmen Media Group Ltd proti Land Schleswig-Holstein, Innenminister des Landes Schleswig-Holstein* (2010).

[41] Sodba Sodišča EFTA, zadeva E-1/06, *Nadzorni organ EFTA proti Kraljevini Norveški* (2007).

Sodišče vselej presoja, ali ukrepa ni mogoče doseči z manj restriktivnimi sredstvi (*Läärä*, *Zenatti*, *Anomar*,[42] *Gambelli*, *Lindman*[43]). Treba je oceniti, ali je monopol potreben za dosego cilja in ali se ne da cilja doseči tudi z manj omejujočimi ukrepi, kot je na primer licenčni sistem. Nujnost ukrepa zahteva, da uvedba monopola vodi v učinkovitejše doseganje ciljev kot manj omejevalni ukrepi (*Läärä*, točki 41 in 42).

2.1.4. Licenčni sistem in vzajemno priznavanje licenc kot omejevalni ukrep?

V nekaterih državah se od ponudnikov spletnih iger na srečo zahteva, da za opravljanje iste vrste spletnih iger v različnih državah članicah zaprosijo za licenco v vsaki državi članici. Nekatere države članice priznavajo licence, izdane ponudnikom v drugih državah članicah, ko jih ti priglasijo (bela listina). Nekatere države upoštevajo licence drugih držav članic pri izdajanju svojih licenc in tako uveljavljajo dvojni režim podeljevanja licenc.[44]

Načelo vzajemnega priznavanja licenc v tej panogi ni primerno. V zadevi *Markus Stoß in Dickinger*[45] je Sodišče izrecno pojasnilo, da ni obveznega medsebojnega priznavanja dovoljenj, izdanih v drugi državi članici (*Markus Stoß*, točka 112; *Dickinger*, točka 96), ter da vsaka država posebej sama presoja priznavanje dovoljenj, izdanih v drugih državah. Sodišče je presodilo, da ob upoštevanju široke diskrecijske pravice držav članic glede ravni varstva potrošnikov in ciljev, ki jih nameravajo doseči, ter neobstoja kakršnekoli usklajenosti pri igrah na srečo na ravni EU pri sedanjem pravu Unije ne more obstajati obveznost medsebojnega priznavanja dovoljenj, ki jih izdajo različne države članice (*Biasci in drugi*,[46] točka 40). Če pa država članica odpre spletni trg iger na srečo, mora zagotoviti model licenciranja, ki bo pregleden in bo omogočal nediskriminatorno konkurenco.[47]

Vsaka država članica ima pravico določiti, da mora gospodarski subjekt, ki želi ponujati igre na srečo potrošnikom na njenem ozemlju, pridobiti dovoljenje pristojnih organov, čeprav ima ta subjekt že dovoljenje, ki ga je izdala druga država članica (*Biasci*, točka 41). Sodišče pravi, da je to potrebno predvsem zato, ker

---

[42] Sodba Sodišča v zadevi C-6/01, *Associação Nacional de Operadores de Máquinas Recreativas (Anomar) and Others proti Estado português* (2003).

[43] Sodba Sodišča v zadevi C-42/02, v postopku na zahtevo Diane Elisabeth Lindman (2003).

[44] Evropska komisija, Zelena knjiga o spletnih igrah na srečo na notranjem trgu z dne 24. 3. 2011, COM(2011) 128 konč., str. 15.

[45] Sodba Sodišča v zadevi C-347/09, *Kazenski postopek proti Jochenu Dickingerju in Franzu Ömerju* (2011).

[46] Sodba Sodišča v združeni zadevi C-660/11 in C-8/12, *Daniele Biasci in drugi proti Ministero dell'Interno in Questura di Livorno* (C-660/11), in *Cristian Rainone in drugi proti Ministero dell'Interno in drugi* (2013).

[47] Resolucija Evropskega parlamenta z dne 15. 11. 2011 o spletnih igrah na srečo na notranjem trgu.

različne države članice ne razpolagajo z enakimi sredstvi za nadzor nad igrami na srečo in glede tega ne izberejo vedno enakih rešitev. Neka država članica lahko uporablja napredne tehnike nadzora in spremljanja, torej doseže določeno raven varstva potrošnikov. To ne pomeni, da lahko druge države članice, ki s temi sredstvi ne razpolagajo ali niso izbrale enake rešitve, dosežejo enako raven varstva. Država članica lahko poleg tega upravičeno spremlja gospodarsko dejavnost, ki se izvaja na njenem ozemlju. To bi bilo nemogoče, če bi morala zaupati nadzorom, ki so jih opravili organi druge države članice z nadzornim sistemom, s katerim sama ne razpolaga (*Biasci*, točka 42). Sodišče nadalje pravi, da je člena 43 in 49 PES (zdaj člena 49 in 56 PDEU) treba razlagati tako, da pri sedanjem stanju prava Unije to, da ima gospodarski subjekt v eni državi članici, kjer ima sedež, tudi dovoljenje, ki mu dopušča ponujanje iger na srečo, ne nasprotuje temu, da druga država članica ob upoštevanju zahtev prava Unije določi, da mora tak subjekt za ponujanje storitev potrošnikom, ki so na njenem ozemlju, imeti dovoljenje, ki ga izdajo njeni organi (*Biasci*, točka 43).

2.1.5. Finančni cilji in omejevalni ukrepi

Igre na srečo so v večini držav članic obdavčene, te prihodke pa države uporabljajo za različne socialne, kulturne, dobrodelne namene, za razvoj športa in konjeniške dejavnosti. Pogosto se kaže težnja, da države sprejmejo omejevalne ukrepe zaradi finančnih ciljev. Igre na srečo so izredno dobičkonosna dejavnost, države pa preko obremenitve prireditelјev iger na srečo z različnimi dajatvami (davki, koncesijske dajatve) pridobijo veliko sredstev. Zato se kaže velik interes držav po omejevanju vstopa tujih ponudnikov spletnih iger na srečo, ki niso registrirani na njenem ozemlju, saj od takih subjektov sama nima finančnih koristi, hkrati pa ustvarjajo konkurenco in posledično nižajo zaslužke domačih prireditelјev iger na srečo.

V zadevi *Schindler* Sodišče pravi, da ni nerelevantno, da igre na srečo lahko znatno prispevajo k financiranju družbeno koristnih ciljev, kar pa ne more biti samostojen razlog za opravičilo omejevalnega ukrepa. Taka omejitev je dovoljena le, če res služi predvsem cilju zmanjševanja priložnosti igralništva in je financiranje družbeno koristih dejavnosti le naključna koristna posledica, in ne dejanski razlog za omejevalno politiko (*Zenatti*, točka 36, *Schindler, Gambelli*).

Prav tako je Sodišče v zadevi *Zenatti* glede omejevalnega ukrepa monopola odločilo, da ta ni nezakonit, če sledi tudi ekonomskim ciljem. Sodišče EU omejevalni ukrep v zadevi *Zenatti* sprejme kot legitimen, saj poleg ekonomskih ciljev sledi predvsem cilju zmanjševanja odvisnosti z zmanjševanjem priložnosti za igranje iger na srečo in z eliminacijo dobičkov zasebnikov. V zadevi *Zenatti* Sodišče poudari, da zagotavljanje sredstev družbenim organizacijam v zadevnem

primeru ni bil dejanski cilj omejevalnega ukrepa, pač pa zgolj koristna in naključna posledica, ki je postranskega pomena.

Sodišče EFTA v zadevi E-1/06 proti Norveški[48] določi, da je treba cilje ocenjevati kot celoto in da v konkretnem primeru prevladujeta cilj zaščite potrošnikov ter cilj zagotavljanja javnega reda, kot prevladujoča cilja v javnem interesu (nujna razloga v splošnem interesu). Navede, da to, da loterije in druge igre na srečo precej prispevajo k financiranju dobrodelnih in družbeno koristnih dejavnosti, ne more biti samo po sebi zadostno objektivno opravičilo za omejevanje temeljne svoboščine, in sicer prostega gibanja storitev. Finančni razlog je lahko zgolj naključna in koristna posledica ukrepa, katerega prvoten cilj sta zmanjševanje priložnosti za igre na srečo in zmanjševanje zasvojenosti z njimi.

2.2. Delovanje Evropske komisije na področju spletnih iger na srečo (*soft law*)

V zadnjem času se s spletnimi igrami na srečo vse več ukvarja tudi Evropska komisija. Prizadeva si za krepitev upravnega sodelovanja in učinkovito izvajanje, skrbi za varstvo potrošnikov, mladoletnikov in drugih ranljivih skupin. Eden pomembnejših dokumentov Evropske komisije je Zelena knjiga o spletnih igrah na srečo.[49] Cilj Zelene knjige je bil ugotoviti najboljše vzpostavljene prakse in oceniti, ali je različna urejenost znotraj držav članic na tem področju še mogoča, primerna in učinkovita.

Iz držav članic prihaja skoraj soglasen poziv za ukrepanje k politiki na ravni EU in določitev prednostnih področij, kjer so potrebni ukrepi in spremembe. Komisija je 23. oktobra 2012 izdala Sporočilo komisije Evropskemu parlamentu, Svetu, Ekonomsko-socialnemu odboru in Odboru regij z naslovom Celovitemu evropskemu okviru za spletne igre na srečo naproti. V sporočilu Komisija opredeli ključne izzive, ki jih predstavljajo različni nacionalni sistemi na ravni EU in njihov soobstoj. Cilj sporočila je bil predlagati ukrepe na ravni EU in ravni držav članic ob upoštevanju dobrih praks EU in držav članic. Komisija se v dokumentu osredotoča predvsem na spletne igre zaradi hitre rasti trga spletnih iger in predvsem v zvezi s prostim pretokom storitev (56. člen PDEU) in pravico do ustanavljanja (49. člen PDEU).[50]

---

[48] V zadevi E-1/06 *nadzorni organ EFTE proti Norveški* poda zahtevo za razglasitev, da je sprejetje Zakona o loteriji, ki določa monopol državnega podjetja za igralne avtomate na Norveškem, v nasprotju z 31. in 36. členom pogodbe EEA (31. člen določa svobodo ustanavljanja, 36. člen pa svobodo opravljanja storitev).

[49] Evropska komisija, Zelena knjiga o spletnih igrah na srečo na notranjem trgu z dne 24. 3. 2011.

[50] Evropska komisija, Sporočilo komisije Evropskemu parlamentu, Svetu, Ekonomsko-socialnemu odboru in Odboru regij z naslovom Celovitemu evropskemu okviru za spletne igre na srečo naproti z dne 23. 10. 2012, str. 4.

2.3. Preventivni izvršilni ukrepi, blokade

Evropska komisija šteje kot pomembne izvršilne ukrepe, ki zmanjšujejo stik državljanov s čezmejnimi igrami na srečo, ki niso skladne z zakonodajo v državi članici, kjer se ponujajo. Pravi, da imajo lahko odzivni izvršilni ukrepi, kot sta omejevanje dostopa do teh spletnih mest, strani, kjer se ponujajo nezakonite igre na srečo, ali blokada plačil med igralcem in ponudnikom igre na srečo, tako dobre kot slabe posledice. Zato morajo biti ti ukrepi vselej skladni s temeljnimi svoboščinami PDEU. Komisija si prizadeva za jasnejšo opredelitev postopkov. Po njenem bi bilo mogoče izboljšati sodelovanje preko mreže, vzpostavljene z Uredbo o sodelovanju na področju varstva potrošnikov, ki omogoča čezmejne ukrepe za izvrševanje.[51]

Ponudniki plačilnih in telekomunikacijskih storitev imajo za omejevanje nedovoljenih spletnih iger na srečo oziroma spletnih iger na srečo, ki jih ponujajo ponudniki, ki za to nimajo pravice in jih ponujajo nelegalno različne metode. Dostop do teh spletih strani lahko onemogočijo z metodo filtriranja domen (DNS). S to metodo se prepreči igranje iger na srečo na nedovoljenih spletnih mestih z določenega seznama ali se jih preusmeri na drugo spletno mesto na podlagi seznama internetnih naslovov (imen domen). Druga metoda je blokiranje internetnega protokola (IP), ki prepreči povezavo med strežnikom (spletnim mestom) in določenimi naslovi IP. Tretja metoda, ki jo lahko uporabijo, pa je blokiranje plačil, temelji pa na posebni kodi ponudnika storitev (MMC – Merchant Category Codes).[52]

Vse države članice bi morale tudi izvajati dosledno politiko na področju kazenskih sankcij. Proti nereguliranim igram bi bilo treba ukrepati tudi na ravni EU.[53] Evropski ekonomsko-socialni odbor (v nadaljevanju EESO) predlaga, da naj se oblikuje nacionalni zakonodajni okvir načel, ki bo zagotavljal zakonitost in preglednost spletnih strani, uvrstitev teh na črne in bele sezname, prenehanje, zaseg, blokiranje ali odstranitev nezakonitih spletnih strani, zamrznitev finančnih tokov na te strani, prepoved reklamnih sporočil in oglaševanja nezakonitih spletnih iger na srečo.[54] EESO tudi poudarja, da bi bilo treba ustanoviti nacionalne regulativne organe, ki bodo skrbeli za izvajanje evropskih in nacionalnih predpisov za varstvo potrošnikov in boj proti nezakonitim igram na srečo. Zato

[51] Prav tam, str. 10.

[52] Evropska komisija: Zelena knjiga o spletnih igrah na srečo na notranjem trgu z dne 24. 3. 2011, str. 35, 36.

[53] Evropski parlament: Poročilo o spletnih igrah na srečo na notranjem trgu, str. 22.

[54] Mnenje Evropskega ekonomsko-socialnega odbora o sporočilu Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij z naslovom Celovitemu evropskemu okviru za spletne igre na srečo naproti z dne 23. 10. 2012, str. 271/52, točka 4.2.5.

predlaga, da države članice od vseh ponudnikov, ki imajo dovoljenje za prirejanje spletnih iger na srečo, zahteva, da številko dovoljenja in oznako regulativnega organa objavijo na vidnem mestu na spletu, kjer igre ponujajo.[55]

3. Pravna ureditev prirejanja iger na srečo v Republiki Sloveniji

Leta 2012 so v Sloveniji[56] bruto prihodki od iger na srečo (BPI)[57] znašali 339,7 mio EUR, pri čemer je BPI klasičnih iger na srečo znašal 79,1 mio EUR in posebnih iger na srečo 260,6 mio EUR. V Sloveniji je v tem letu delovalo 9 igralnic in 31 igralnih salonov. Na področju prirejanja iger na srečo je bilo skupaj zabeleženih 123,6 mio EUR dajatev, od tega pri klasičnih igrah na srečo 34,5 mio EUR in pri posebnih igrah na srečo 89,1 mio EUR (igralnice 45,3 mio EUR in igralni saloni 43,8 mio EUR). V času sestave prispevka sta v registru prireditelјev iger na srečo, ki ga vodi Ministrstvo za finance, vpisana dva imetnika koncesije za trajno prirejanje klasičnih iger na srečo, 9 koncesionarjev za prirejanje posebnih iger v igralnicah in 30 koncesionarjev za igralni salon.

Jasen dokaz o tveganjih, poveznih s (spletnimi) igrami na srečo, ponujata raziskavi Fakultete za uporabne družbene študije v Novi Gorici (FUDŠ). Raziskava FUDŠ iz leta 2008,[58] v kateri je bil v okviru telefonske ankete zajet 10.001 anketiranec, ugotavlja da ima v Sloveniji 0,46 odstotka odrasle slovenske populacije probleme z igranjem.[59] Delež igralcev posamezne igre na srečo, ki imajo probleme pri spletnih igrah na srečo, znaša 9,9 odstotka, sicer pa je največji pri igrah s kartami v igralnici (13,9 odstotka), igralnih avtomatih v salonih (13,3) in v igralnicah (9,7 odstotka) ter najnižji pri lotu (1 odstotek). Bolj zaskrbljujoče podatke kaže raziskava FUDŠ iz leta 2010, opravljena med dijaki višjih letnikov srednjih šol v goriški in dolenjski regiji,[60] v kateri je sodelovalo 1.113 anketirancev. Medtem ko je v celotni slovenski populaciji spletne igre na srečo igralo 0,62 odstotka, je ta delež med dijaki znašal nad 16 odstotkov. Glede na raziskavo je 10,61 odstotka dijakov goriške regije spletne igre na srečo igralo nekajkrat letno, 4,84 odstotka nekajkrat mesečno in 1,3 odstotka skoraj vsak dan. Veliko večji je med dijaki tudi delež problematičnih igralcev, ki v celotni slovenski populaciji znaša 0,46

[55] Prav tam, str. 53, točka 4.3.7.

[56] Vir: Davčna uprava RS – Zbirni podatki o igrah na srečo v Sloveniji v obdobju 2005–2013 (januar–junij).

[57] Bruto prihodek od iger predstavljajo skupaj vplačila, zmanjšana za izplačane dobitke.

[58] Rončević in drugi, 2009.

[59] Uporabljen je bil test *South Oaks Gambling Screen* (SOGS), ki se kot mednarodni standard največkrat uporablja za ugotavljanje problemov z igrami na srečo.

[60] Fakulteta za uporabne družbene študije, 2010.

odstotka, med goriškimi dijaki 2,57 odstotka in med dolenjskimi dijaki celo 3,37 odstotka. Navedeni raziskavi potrjujeta, da je med mlajšim prebivalstvom večji delež problematičnih igralcev in da so spletne igre na srečo bolj priljubljene med mlajšimi osebami.

3.1. Pravna ureditev iger na srečo

3.1.1. Aktualna pravna ureditev po Zakonu o igrah na srečo

Ureditev področja iger na srečo v Sloveniji je predmet Zakona o igrah na srečo (ZIS),[61] ki je bil sprejet leta 1995 in pozneje večkrat noveliran. Cilji pravne ureditve iger na srečo so definirani v 1. členu ZIS, in sicer so to zlasti varstvo potrošnikov, preprečevanje kriminalitete (kaznivih dejanj), varstvo javnega reda in javne varnosti, varstvo javnega zdravja in preprečevanje zasvojenosti ter predvsem zaščita mladoletnih oseb in drugih občutljivih skupin. Prirejanje iger na srečo je izključna pravica Republike Slovenije, zato lahko igre na srečo na območju Slovenije prirejajo zgolj gospodarske družbe, ki pridobijo koncesijo Vlade Republike Slovenije. Prepovedano je tudi sprejemanje ali posredovanje vplačil, oglaševanje ali opravljanje drugih storitev v zvezi s prirejanjem na srečo za osebe, ki nimajo koncesije Vlade (6. člen ZIS). Igre na srečo se delijo na klasične igre na srečo in posebne igre na srečo. Obseg je strogo omejen že na ravni zakona, in sicer določba petega odstavka 3. člena ZIS na območju Slovenije dovoljuje največ dva prireditelja trajnih klasičnih iger na srečo, 15 koncesij za prirejanje posebnih iger na srečo v igralnicah ter 45 koncesij za igralne salone. Koncesije za trajno prirejanje iger na srečo podeljuje po prostem preudarku Vlada Republike Slovenije, upoštevaje merila, določena v ZIS, na podlagi vloge zainteresiranega prireditelja (t. i. pasivni koncesijski sistem[62]). Koncesija se lahko podeli delniški družbi s sedežem v Sloveniji za obdobje 10 let z možnostjo podaljševanja za 5 let. Osebam, mlajšim od 18 let, je prepovedana udeležba pri posebnih igrah na srečo ter spletnih igrah na srečo (3.a in 83. člen ZIS). Zakonski institut samoprepovedi igralcu omogoča, da se mu na podlagi lastne izjave za obdobje od šestih mesecev do treh let onemogoči udeležba pri posebnih in spletnih igrah na srečo, pri čemer igralec v obdobju veljavnosti te svoje izjave ne more preklicati (9. člen ZIS). Hkrati so tudi koncesionarji dolžni igralce opozoriti na tveganja in jim zagotoviti informacije o tem, kje poiskati pomoč v primeru zasvojenosti (8. člen ZIS), ter skrbeti za izobraževanje svojih zaposlenih glede odgovornega prirejanja iger na srečo.

[61] Uradni list RS, št. 27/1995, s spremembami in dopolnitvami.

[62] Cizelj, 2008.

3.1.2. Predlog novega Zakona o igrah na srečo

Besedilo predloga Zakona o igrah na srečo (ZIS-1)[63] je Ministrstvo za finance objavilo in posredovalo v javno obravnavo 24. septembra 2013. Predlog zakona temelji na leta 2010 sprejeti Strategiji razvoja iger na srečo v Sloveniji, ki med drugim predvideva tudi pripravo novih zakonskih in podzakonskih rešitev, s ciljem, da Republika Slovenija postane država s sodobnim in kakovostnim prirejanjem iger na srečo, kjer se igre prirejajo v urejenem in nadzorovanem okolju ter v takšnem obsegu in strukturi, ki dolgoročno zagotavlja čim večje koristi za družbo, obenem pa so varovane določene vrednote, predvsem gre za varstvo šibkejših družbenih skupin, kot so otroci in mladoletniki, varstvo potrošnikov, zmanjševanje in odpravljanje kaznivih dejanj ter odvisnosti od iger na srečo.[64]

Instituta odgovornega prirejanja iger na srečo in varstva mladoletnih oseb sta s predlogom zakona okrepljena. Cilji pravne ureditve iz ZIS ostajajo v predlogu zakona nespremenjeni. Opuščena je delitev iger na srečo na klasične in posebne igre na srečo ter v skladu z delitvijo v večini evropskih držav uvedena delitev na loterijske igre, stave in igralniške igre. Predlog ohranja na zakonski ravni določeno največje število koncesij, in sicer po eno koncesijo za loterijske igre in stave ter največ 30 koncesij za prirejanje igralniških iger.[65] Predlog zakona sledi evropskim zahtevam po transparentnosti in določa podeljevanje koncesij za stave in igralniške igre na podlagi javnega razpisa za obdobje petih let, medtem ko za loterijske igre na srečo uvaja zakonski monopol Loterije Slovenije, d. d. Odgovornemu prirejanju iger na srečo je v predlogu namenjeno 2. poglavje z naslovom Zaščita igralcev in drugih občutljivih oseb. Predlog uvaja splošno prepoved sodelovanja oseb, mlajših od 18 let, ter prepoveduje postavitev vplačilnih mest za loterijske igre in stave na oddaljenosti bližje kot 300 m od vzgojno-izobraževalnih ustanov (7. člen ZIS-1). Predlog ohranja institut samoprepovedi ter prireditelјem iger na srečo nalaga dolžnost obveščanja in zavezuje k aktivnemu ukrepanju za zaščito igralcev pred zasvojenostjo (8. in 9. člen ZIS-1). Zakon uvaja pravno regulacijo oglaševanja (odgovorno oglaševanje) ter prepoveduje zavajajoče oglaševanje in dodatno ščiti mladoletnike tako glede sodelovanja v oglaševanju kot glede usmerjenosti oglaševanja na mladoletne osebe. S ciljem preprečevanja goljufij in varstva integritete športa je uvedena prepoved udeležbe pri stavah osebam, ki bi lahko vplivale na izid dogodka (59. člen ZIS-1).

[63] Predlog Zakona o igrah na srečo, objavljen dne 24. 9. 2013 pod oznako EVA 2013-1611-0041.

[64] Vlada RS, 2010, str. 27.

[65] Predlog zakona v prehodnih in končnih določbah predvideva uskladitev števila koncesij za prirejanje igralniških iger najpozneje do 1. 1. 2018 (132. člen ZIS-1).

3.2. Pravna ureditev spletnih iger na srečo

3.2.1. Aktualna pravna ureditev

Spletne igre na srečo niso bile predmet regulacije Zakona o igrah na srečo iz leta 1995, prvič jih je pravno uredil leta 2001 sprejeti Zakon o spremembah in dopolnitvah zakona o igrah na srečo (ZIS-A).[66] Skladno z ureditvijo po noveli ZIS-A, ki je začela veljati dne 30. oktobra 2001, je bilo spletno prirejanje iger na srečo dovoljeno imetnikom koncesije za trajno prirejanje iger na srečo in koncesije za prirejanje posebnih iger na srečo v igralnicah. Zakon o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-C),[67] ki je začel veljati 27. februarja 2010, je prirejanje spletnih iger dodatno omejil zgolj na tiste igre na srečo, ki se kot take določijo v koncesijski pogodbi, ter prepovedal udeležbo mladoletnim osebam.

Trenutno veljavni ZIS definira spletne igre na srečo kot igre na srečo, ki se prirejajo prek interneta in drugih telekomunikacijskih sredstev (prvi odstavek 3.a člena ZIS), vendar spletnih iger na srečo ne opredeljuje kot posebne vrste iger na srečo, ampak zgolj kot poseben način prirejanja le-teh. Izključna pravica države do prirejanja iger na srečo je s 3.a členom ZIS razširjena tudi na internet in druga telekomunikacijska sredstva. Spletne igre na srečo lahko prireja le delniška družba, ki ima koncesijo za trajno prirejanje klasičnih iger na srečo ali koncesijo za prirejanje posebnih iger na srečo v igralnicah (ne pa imetnik koncesije za igralni salon), in to le tistih iger na srečo, ki so določene v koncesijski pogodbi (prvi odstavek 3.a člena ZIS). Preko spleta se lahko prirejajo klasične igre na srečo in posebne igre na srečo, z izjemo stav, pri čemer je treba izpostaviti, da so športne stave umeščene med klasične igre na srečo in se lahko prirejajo kot spletne igre na srečo.

Enako kot koncesionarje posebnih iger na srečo zakon zavezuje tudi prireditelje spletnih iger na srečo, da informacijski sistem, na katerem prirejajo spletne igre na srečo, povežejo v informacijski sistem DURS in mu zagotovijo bralni dostop do aplikacij, podatkov in sistemskih zapisov (drugi odstavek 3.a člena ZIS). S stališča odgovornega igralništva je treba izpostaviti institut samoprepovedi, ki zavezuje tudi prireditelje spletnih iger na srečo (šesti odstavek 9. člena ZIS), ter institut prepovedi udeležbe v spletnih igrah na srečo osebam, mlajšim od 18 let (tretji odstavek 3.a člena ZIS). Za podrobnejšo ureditev prirejanja spletnih iger na srečo ZIS v zadnjem odstavku 3.a člena napotuje na podzakonski akt, in sicer Pravilnik o prirejanju iger na srečo preko interneta oziroma drugih telekomunikacijskih sredstev (Pravilnik).[68] Pred udeležbo v spletnih igrah na srečo

[66] Uradni list RS, št. 85/2001.

[67] Uradni list RS, št. 10/2010.

[68] Uradni list RS, št. 42/2008, s spremembami in dopolnitvami.

se mora igralec registrirati in odpreti igralni račun pri koncesionarju (18. člen Pravilnika), kjer mora igralec koncesionarju posredovati osebne podatke, med katerimi je tudi datum rojstva. Koncesionarji, ki prirejajo spletne igre na srečo, so hkrati zavezanci[69] po Zakonu o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT)[70] in so tako dolžni pred sklenitvijo poslovnega razmerja opraviti pregled stranke, v okvir katerega spada ugotavljanje in preverjanje istovetnosti stranke. Nadzor države nad prireditelji spletnih iger na srečo, ki so nujno sočasno tudi prireditelji *land-based* iger na srečo, je enak kot nad klasičnimi prireditelji iger na srečo, in sicer neposreden, posreden in preko nadzornega sveta. Pooblaščena oseba nadzornega organa ima na podlagi določbe 109. člena ZIS pravico pregledati poslovne prostore in vse procese, povezane z igrami na srečo, ter naprave in pripomočke za prirejanje iger na srečo. Zato je logična zahteva Pravilnika v 6. členu, ki poleg ustreznega varovanja spletnega igralnega sistema in zgradbe, kjer se nahajata programska in strojna oprema spletnega igralnega sistema, zahteva tudi, da se zgradba in spletni igralni sistem (programska in strojna oprema) nahajata na območju Slovenije.

3.2.2. Predlog novega Zakona o igrah na srečo

Nedavno objavljeni predlog ZIS-1 ohranja obstoječi koncept spletnih iger na srečo, kot poseben način prirejanja iger na srečo. Prav tako kot obstoječi zakon tudi predlog v tretjem odstavku 17. člena napotuje na podzakonsko ureditev, ki v času priprave prispevka še ni objavljena. Spletne igre na srečo lahko prirejajo zgolj koncesionarji za prirejanje loterijskih iger[71] in stav[72] ter imetniki koncesije za igralniško zabaviščni center in igralnico, ob izpolnitvi določenih dodatnih pogojev.[73] Osnovni pogoji za prirejanje spletnih iger na srečo so določeni v 17. členu, kjer zakon od koncesionarja, ki sprejema vplačila za udeležbo pri igrah na srečo, izplačuje dobitke ali prireja igre na srečo, zahteva povezavo spletnega igralnega sistema v informacijski sistem nadzornega organa, da pred začetkom poslovnega razmerja ugotovi istovetnost igralca po zakonu, ki ureja preprečevanje pranja denarja in financiranja terorizma, ter da za igralca odpre igralni račun. Predlog zakona ob izpolnjevanju splošnih pogojev za prirejanje spletnih iger na srečo dovoljuje spletno prirejanje loterijskih iger in stav. Za spletno prirejanje igralniških iger je treba dodatno pridobiti dovoljenje ministra, pristojnega za finance, ter zagotoviti, da se strojna oprema spletnega igralnega sistema nahaja

[69] Glej 14. točko prvega odstavka 4. člena ZPPDFT.

[70] Uradni list RS, št. 60/2007, s spremembami in dopolnitvami.

[71] 29. člen ZIS-1.

[72] 57. člen ZIS-1.

[73] 79. člen ZIS-1.

v igralnem prostoru in da igralniška družba vplačila lahko sprejema zgolj od rezidentov.

3.3. Ukrepi proti nezakonitemu prirejanju spletnih iger na srečo

Evropske države[74] v boju proti nezakonitim prirediteljem spletnih iger na srečo poleg upravnih, prekrškovnih in kazenskih ukrepov uporabljajo ali načrtujejo tudi ukrep blokiranja finančnih transakcij z nepooblaščenimi spletnimi mesti (Belgija, Nemčija, Estonija, Finska, Francija, Litva, Nizozemska) ter ponudnikom informacijske tehnologije nalagajo obvezno opozorilo uporabnikom ob priključku na nezakonito spletno mesto (Belgija, Estonija, Francija, Nizozemska) oziroma blokado teh spletnih mest (Nemčija, Estonija, Finska, Italija). Skladno s stališčem Sodišča so izvedbeni ukrepi nacionalne ureditve (izvršitveni ukrepi) nepogrešljiv element pri varstvu, ki ga država članica želi zagotavljati na svojem ozemlju pri igrah na srečo, zato se izvršitvenih ukrepov ne more šteti za dodatno omejitev glede na tisto, kar izhaja neposredno iz določb ZIS. Izvršitveni ukrepi ne predstavljajo dodatne omejitve na trgu, ampak samo zagotavljajo polni učinek nacionalne ureditve – brez izvršitvenih ukrepov prepoved, ki jo določa ZIS, ne bi imela nobenega učinka, saj bi tudi osebe brez koncesije lahko prirejale igre na srečo na ozemlju Slovenije (tako Sodišče v zadevi *Ladbrokes*, točke 43–50).

Že Zakon o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-A), ki je začel veljati 30. oktobra 2010, je predvidel, da nadzorni organ z odločbo prepove prirejanje iger na srečo, če se le-te prirejajo brez koncesije, vendar zakon ni uredil načina izvršitve izdane prepovedne odločbe, če je kršitelj ni prostovoljno izvršil. Zato je Urad za nadzor prirejanja iger na srečo (UNPIS) v obdobju do leta 2010 omejitev dostopa do spletnih strani ponudnikom storitev informacijske družbe oprl na 6. člen ZIS, ki je prepovedoval opravljanje drugih storitev v zvezi s katerokoli igro na srečo za tuje osebe v Republiki Sloveniji. Zakon o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-C),[75] ki je začel veljati 27. februarja 2010, je uredil vprašanje načina izvršitve prepovedne odločbe tako, da je nadzorni organ ponudniku storitev informacijske družbe naložil omejitev dostopa do spletnih strani, preko katerih so se prirejale igre na srečo brez koncesije. Z Zakonom o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-D),[76] ki je začel veljati 11. januarja 2011, je bila pristojnost omejevanja dostopa do spletnih strani prenesena na Upravno sodišče RS, ki o tem odloča na predlog nadzornega organa. Dodatno je novela ZIS-D izrecno določila, da mora biti v predlogu nad-

[74] Svet EU, 2008, str. 23.

[75] Uradni list RS, št. 10/2010.

[76] Uradni list RS, št. 106/2010.

zornega organa določen obseg omejitve in način njene izvršitve, upoštevaje načela sorazmernosti in tehničnih možnosti, ter da se omejitev dostopa do spletnih strani izvrši le v obsegu, ki je nujno potreben za izvršitev odločbe o prepovedi prirejanja iger na srečo, in na način, ki je najmanj obremenjujoč za ponudnika informacijske družbe. Resnična novost novele ZIS-D je v prenosu pristojnosti na sodišče, medtem ko je zahteva po določitvi obsega in načina izvršitve omejitve, upoštevaje načelo sorazmernosti, pred uveljavitvijo novele ZIS-D izhajala iz določbe 7. člena Zakona o inšpekcijskem nadzoru (ZIN),[77] zahteva po določenosti načina izvršitve pa iz določbe 279. člena Zakona o splošnem upravnem postopku (ZUP).[78] S prenosom pristojnosti odločanja na sodišče pa je bilo treba to materijo dodatno urediti v samem ZIS, ker sodišče ni zavezano z ZIN in ZUP. Kot je razvidno iz obrazložitve Predloga zakona o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-D),[79] je do prenosa pristojnosti na sodišče prišlo zaradi mnenja Informacijskega pooblaščenca, Direktorata za informacijsko družbo, ureditve v Zakonu o elektronskem poslovanju na trgu (ZEPT),[80] ki le sodišču daje pristojnost odrediti odstranitev nezakonitih vsebin ali onemogočanje dostopa do njih, ter ker gre za poseg, povezan z omejevanjem svobode interneta in svobode izražanja, in je treba pristojnost omejevanja dostopa do spletne strani prenesti na sodišče. Ne glede na predhodno spremembo zakonodaje Vrhovno sodišče RS pri presoji odločb, izdanih s strani UNPIS, ni videlo neustavnosti v dejstvu, da je ukrep omejitve dostopa do spletne strani izrekel upravni organ, in ne, kot ga mora po ZEPT, sodišče, ker se ta zakon izrecno ne uporablja za področje iger na srečo. Iz enakega razloga po mnenju sodišča tudi ni prišlo do kršitve načela *mere conduit* iz Direktive 2000/31/ES, ker se na to področje direktiva ne nanaša (tako Vrhovno sodišče RS v sklepu opr. št. I Up 77/2011 z dne 16. 2. 2011).

Aktualna ureditev določa, da Upravno sodišče RS na predlog DURS, kot nadzornega organa iger na srečo, ponudniku storitev informacijske družbe odredi omejitev dostopa do spletne strani, prek katere se prirejajo spletne igre na srečo brez koncesije vlade, če le-ta prostovoljno ne izvrši odločbe o prepovedi prirejanja iger na srečo. Zakon veže omejitev dostopa do spletnih strani na obseg, ki je nujno potreben za izvršitev odločbe o prepovedi prirejanja iger na srečo, in na način, ki je najmanj obremenjujoč za ponudnika storitev informacijske družbe. O predlogu DURS mora Upravno sodišče RS odločiti v sedmih dneh, zoper odločbo

[77] Uradni list RS, št. 56/2012, s spremembami in dopolnitvami.

[78] Uradni list RS, št. 80/1999, s spremembami in dopolnitvami.

[79] Predlog zakona o spremembah in dopolnitvah Zakona o igrah na srečo, EVA 2010-1611-0084 z dne 28. 10. 2010.

[80] Uradni list RS, št. 61/2006, s spremembami in dopolnitvami.

ima ponudnik storitev informacijske družbe pravico v treh dneh vložiti pritožbo, o kateri odloči Vrhovno sodišče RS najpozneje v petnajstih dneh.

Omejitev dostopa do določenih spletnih strani je tehnično mogoče izvršiti na štiri načine,[81] in sicer z blokado prometa glede na ciljni naslov IP, spreminjanjem tabel za usmerjanje prometa, preusmerjanjem s pomočjo lažnih odgovorov DNS in tehnologijo DPI (*Deep Packet Inspection)*. Blokada naslova IP prekine spletni promet, ki je namenjen na določen spletni naslov IP. Metoda spreminjanja tabel za usmerjanje prometa pomeni, da se v usmerjevalne table vnese lažne podatke, ki uporabniku, ki želi dostopati na določen spletni naslov, vrne podatek, da se ta spletna stran nahaja na primer na strežniku DURS. Pri metodi podtikanja lažnih odgovorov DNS strežniki DNS ponudnika dostopa do interneta pri poizvedbi za določeno spletno mesto vrnejo napačen IP naslov (na primer naslov IP spletnega mesta DURS). Najbolj invazivna in z ustavnega vidika nesprejemljiva pa je metoda *Deep Packet Inspection*, ki temelji na vpogledu v vsebino spletne komunikacije.

Upoštevajoč dostopno sodno prakso sta UNPIS[82] oziroma po uveljavitvi novele ZIS-D Upravno sodišče RS kot način izvršitve onemogočitve dostopa do spletne strani ponudnikom informacijske družbe naložila onemogočitev pretvorbe tekstovnega spletnega naslova, na katerem so se prirejale igre na srečo, v pripadajoči naslov IP oziroma onemogočitev pretvorbe tekstovnih spletnih naslovov v pravi naslov IP tako, da je strežnik DNS vrnil naslov IP spletne strani na www.infounpis.si. Ustaljena sodna praksa sprejema oba načina izvršitve, tako onemogočitev pretvorbe tekstovnega spletnega naslova kot tudi preusmeritev na spletno stran UNPIS. Takšen način izvršitve prepovedne odločbe je Vrhovno sodišče RS v sklepu op. št. I Up 66/2012 z dne 16. 2. 2012 štelo za sorazmernega, za najbolj enostavnega in z najmanj stranskimi učinki, v primerjavi z drugimi načini, kot so filtriranje paketov prometa po naslovu IP ali filtriranje paketov IP po vsebini (enako sklep Vrhovnega sodišča RS, opr. št. I Up 54/2012 z dne 16. 2. 2012). Glede učinkovitosti ukrepa je Vrhovno sodišče RS realno in je v sklepu opr. št. I Up 54/2012 z dne 16. 2. 2012 zapisalo, da se z izvršitvijo ukrepa doseže to, da je večina uporabnikov pri vsakodnevni uporabi interneta pri poskusu dostopa do spletne strani nezakonitega prireditelja iger na srečo preusmerjena na spletno stran UNPIS, na kateri bo obveščena o neuspešnem poskusu dostopa do spletne strani z nezakonito ponudbo iger na srečo ter z razlogi za preusmeritev (enako sklep Vrhovnega sodišča RS, opr. št. I Up 66/2012 z dne 16. 2. 2012). Po mnenju Vrhovnega sodišča RS se s tem doseže osnovni namen ukrepa, ob sočasnem

[81] Božič, 2010.

[82] Prirejanje iger na srečo je do 1. 1. 2013 nadzoroval Urad za nadzor prirejanja iger na srečo (UNPIS), z Zakonom o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-E, Uradni list RS, št. 108/2012) pa je nadzor prenesen na Davčno upravo Republike Slovenije (DURS).

zavedanju, da je ukrep mogoče obiti. Vrhovno sodišče se je opredelilo tudi do vprašanja poseganja tega ukrepa v ustavne pravice ter je v sklepu opr. št. I Up 77/2011 z dne 16. 2. 2011 pojasnilo, da izvrševanje ukrepa, ki ga je z dokončnim upravnim aktom odredil državni organ, pristojen za nadzor nad prirejanjem iger na srečo, ne pomeni poseganja v pravico ponudnika informacijske družbe kot ponudnika sredstva komunikacije, če ureditev posega v ustavne pravice uporabnikov, pa to opravičuje varovanje javnega reda, preprečevanje kaznivih dejanj, zaščita potrošnikov pred škodljivimi posledicami igranja iger na srečo (enako Vrhovno sodišče RS v sklepu opr. št. I Up 90/2011 z dne 17. 2. 2011 ter opr. št. I Up 54/2012 z dne 16. 2. 2012).

V postopku omejitve dostopa do spletnih strani kot specialne oblike izvršbe po drugih osebah na podlagi izrecne določbe 107. člena ZIS nastopa kot stranka ponudnik informacijske družbe. Zaradi tehničnih značilnosti medija (svetovnega spleta) omejitve dostopa ni mogoče izvesti drugače kot z naložitvijo ukrepa ponudniku storitev informacijske družbe, zato takšen ukrep ne krši ustavnih pravic le-teh, kljub dejstvu, da je s prepovedno odločbo prirejanje spletnih iger na srečo prepovedano drugi osebi (tako Upravno sodišče RS, sodba I U 2000/2010 z dne 21. 12. 2011). Na drugi strani v postopku omejitve dostopa do spletnih strani nezakoniti prireditelji spletnih iger na srečo, ki jim je bilo prirejanje spletnih iger na srečo s pravnomočno odločbo, ki se z v tem sporu obravnavano odločbo izvršuje, prepovedano, nimajo položaja stranskega intervenienta, ker za to nimajo pravnega interesa (tako Vrhovno sodišče RS, sklep opr. št. I Up 321/2012 z dne 30. 8. 2012, sklep I Up 169/2012 z dne 11. 7. 2012 ter sklep I Up 177/2012 in I Up 176/2012 z dne 12. 7. 2013).

3.3.1. Izvršilni ukrepi omejevanja iger na srečo po ZIS-1

Dne 24. 9. 2013 objavljen predlog ZIS-1 v 114. členu ohranja blokado spletnih strani in v 115. členu dodatno uvaja prepoved izvrševanja plačilnih transakcij. Prvi odstavek 114. člena ZIS-1 ponudnika storitev informacijske družbe zavezuje, da ne sme omogočiti dostopa do spletnih strani, preko katerih se igre na srečo prirejajo brez koncesije vlade. Pristojnost odločanja o omejitvi dostopa so spletnih strani je ponovno prenesena na upravni organ, in sicer DURS, ki kot nadzorni organ vzpostavi in vodi seznam spletnih strani, na katerih se prirejajo igre na srečo brez koncesije. Predlog DURS zavezuje k javni objavi seznama in pošiljanja le-tega ponudnikom storitev informacijske družbe, ki so dolžni najpozneje v 24 urah onemogočiti dostop do spletnih strani s preusmeritvijo zahteve na spletno stran nadzornega organa. Novost pri preprečevanju nezakonitega prirejanja iger na srečo je v 115. členu ZIS-1 uvedena prepoved plačilnih storitev. Plačilna institucija z dovoljenjem Banke Slovenije za opravljanje plačilnih storitev ne sme

izvršiti transakcije v dobro prireditelja ali v dobro uporabnika, če je iz transakcije razvidno, da se nanaša na igre na srečo brez koncesije, pri čemer podatke o prireditelji in številko transakcijskega računa plačilnim institucijam sporoča nadzorni organ. Za nadzor nad izvajanjem blokade spletnih strani je pristojna Agencija za pošto in elektronske komunikacije, za nadzor nad izvajanjem blokade finančnih transakcij pa Banka Slovenije.

V zvezi s predlagano spremembo prenosa pristojnosti odločanja glede omejitev dostopa do spletnih strani na DURS je v predlogu zakona kot razlog za spremembo sedanje ureditve navedena njena neučinkovitost. Vendar v predlogu ni obrazloženo, kako naj bi se spremenile okoliščine, ki so obstajale ob sprejemu novele ZIS-D. Prenos pristojnosti odločanja glede omejitve dostopa do spletnih strani na sodišče z novelo ZIS-D je utemeljil na okoliščini, da ureditev v ZEPT takšno pristojnost podeljuje zgolj sodišču, in dejstvu, da gre za omejevanje svobode interneta in svobode izražanja po 39. členu Ustave RS (URS)[83] ter je zato takšno pristojnost primerneje zaupati sodišču. Okoliščine, ki so botrovale prenosu pristojnosti na sodišče, se po mnenju avtorjev niso spremenile, glede na kratek rok, v katerem sta zavezana odločiti Upravno sodišče RS in Vrhovno sodišče RS, pa tudi ni mogoče govoriti o neučinkovitosti trenutne ureditve. S tehničnega vidika ukrep omejevanja dostopa do spletnih strani ostaja nespremenjen in že iz tega razloga enako (ne)učinkovit kot po sedanji ureditvi. Zato glede na navedeno ni mogoče sprejeti obrazložitve za ponoven prenos pristojnosti s sodišča nazaj na upravni organ. Poleg tega je predlog zakona pomanjkljiv, saj ne ureja postopka in meril umestitve spletne strani na seznam ter določitve prepovedanih plačilnih transakcij (na primer, ali mora biti predhodno izdana odločba o prepovedi prirejanja iger na srečo) in morebitnega pravnega varstva prireditelja iger na srečo ali tretje osebe, katere spletna stran oziroma transakcijski račun bo umeščen na seznam, ali ponudnika storitev informacijske družbe oziroma plačilne institucije. Zato ni jasno, katerim osebam bo šlo pravno varstvo in po katerih postopkovnih določbah, glede na potrebo po hitri odločitvi pa ne bi bilo primerno, da se pravno varstvo osebam v tem primeru zagotavlja v upravnem sporu.[84] Omejevanje dostopa do spletnih strani z vidika posameznika nedvomno pomeni poseg države v posameznikovo sfero svobodnega ravnanja, ki ga Ustava RS varuje v 39. členu v okviru svobode izražanja, ob določenih načinih izvrševanja omejevanja dostopa do spletnih strani pa lahko pride tudi do posega ustavno zajamčeno pravico do tajnosti občil iz 37. člena Ustave RS, zato smo avtorji mnenja, da je pristojnost

[83] Uradni list RS, št. 33/1991-I, s spremembami in dopolnitvami.

[84] Določba prvega odstavka 4. člena Zakona o upravnem sporu (ZUS-1, Uradni list RS, št. 105/2006, s spremembami in dopolnitvami) zagotavlja subsidiarno varstvo zakonitosti posamičnih aktov in dejanj, s katerimi organi posegajo v človekove pravice in temeljne svoboščine posameznika, če ni zagotovljeno drugo sodno varstvo.

za odločanje o tako pomembnem vprašanju primerneje zaupati sodišču. Iz enakih razlogov avtorji pozdravljamo odločitev, da je seznam spletnih strani javno objavljen, pri čemer naj se spletna stran na seznam, ki ga vodi nadzorni organ, uvrsti na podlagi pravnomočne sodne odločbe. Javna objava seznama spletnih strani na preprost način omogoča nadzor javnosti nad delovanjem države in je najmočnejše jamstvo, da se na seznam pod pretvezo prirejanja nedovoljenih iger na srečo ne bodo umestile tudi spletne strani z drugimi vsebinami.

Kot potencialno uspešen način omejevanja prirejanja nezakonitih spletnih iger na srečo avtorji štejemo ukrep prepovedi bančnih transakcij, saj ta izniči motiv nezakonitih prirediteljev iger na srečo in hkrati pomeni manjši poseg v ustavne pravice posameznika. Vendar tudi pri tem ukrepu ni mogoče mimo prej navedenih nedorečenosti predlagane zakonske ureditve. Glede na dejstvo, da ta ukrep manj posega v ustavno varovane svoboščine, bi bil zanj lahko pristojen upravni organ, vendar avtorji menimo, da bi bilo z vidika spletnih iger na srečo predvsem iz razloga ekonomičnosti postopka in tudi višje ravni varstva ustavnih svoboščin smotrno, da bi tudi o tem ukrepu odločalo sodišče na predlog nadzornega organa, in sicer sočasno z odločanjem o omejitvi dostopa do spletne strani.

4. Namesto sklepa

Upoštevaje analizirano sodno prakso sodišča je obstoječa pravna ureditev skladna s pravnim redom EU, morda z izjemo zahteve po sedežu koncesionarja na območju Slovenije ter potencialno problematičnega t. i. pasivnega[85] koncesijskega sistema.[86, 87] Prav tako so skladne z zahtevami EU kaznovalne sankcije, in sicer prekršek prirejanja iger na srečo brez dovoljenja ali koncesije po 110. členu ZIS in kaznivo dejanje organiziranja denarnih verig in nedovoljenih iger na srečo po drugem odstavku 212. člena Kazenskega zakonika (KZ-1).[88, 89, 90] Novi predlog ZIS-1, objavljen 24. septembra 2013, kot že rečeno odpravlja pomanjkljivosti sedanjega zakona in slovensko pravno ureditev še bolj približuje zahtevam pravnega

[85] Cizelj, 2008.

[86] Glej zlasti sodbe Sodišča v zadevah *Engelmann*, *Sporting Exchange*, *Carmen Media* in v teh sodbah citirano sodno prakso Sodišča.

[87] Sladič, 2008, Cizelj, 2011, in Hojnik, 2010.

[88] Uradni list RS, št. 55/2008, s spremembami in dopolnitvami.

[89] Skladnost kazenskih sankcij je Sodišče presojalo na primer v zadevah *Gambelli* in *Placanica*, v katerih je sicer presodilo, da so kazenske sankcije v nasprotju s pravom EU, vendar iz razloga, ker je Italija omejevala prirejanje iger na srečo v nasprotju s pravom EU. Če pa je kazenska sankcija zgolj izvedbeni ukrep za izvrševanje z EU pravom skladne omejitve iger na srečo, sama ne pomeni dodatne omejitve in ni predmet presoje Sodišča (tako sodba Sodišča v zadevi *Placanica*, točki 68 in 69, ter podobno v zadevi *Ladbrokes*, točka 50).

[90] Cizelj, 2010.

reda EU. Predlog zakona odpravlja zahtevo po sedežu koncesionarja na ozemlju Slovenije, ohranja pa zahtevo po statusni obliki delniške družbe, pri čemer je Sodišče v zadevah *Engelmann*[91] in *Dickinger* dopustilo omejitve glede statusne oblike imetnika koncesije.[92] Prav tako je s pravnim redom EU skladnejši način podelitve koncesij za stave in igralniške igre, ki se po predlogu zakona podeli na podlagi javnega razpisa za obdobje petih let, kar je z vidika načela transparentnosti nedvomno primernejši način podeljevanja koncesij.

Sodišče v ustaljeni sodni praksi šteje, da igre na srečo, ki so dostopne prek interneta, zaradi neobstoja neposrednega stika med potrošnikom in gospodarskim subjektom vključujejo drugačna in večja tveganja v zvezi z morebitnimi goljufijami gospodarskih subjektov v škodo potrošnikov, kot jih vključujejo enake igre na srečo, ki niso ponujene preko interneta (*Liga Portuguesa*, točka 70; *Carmen Media*, točka 102; enako je stališče Sodišča v zadevah *Ladbrokes* in *Sporting Exchange*). Značilnosti ponujanja iger na srečo prek interneta se torej lahko izkažejo kot izvor drugačnih in večjih nevarnosti na področju varstva potrošnikov, zlasti pa v zvezi z mladimi in osebami, ki so posebej nagnjene k igram na srečo ali pri katerih obstaja verjetnost, da se to nagnjenje razvije, kot jih te igre vključujejo na zanje običajnih trgih. Poleg navedenega neobstoja neposrednega stika med potrošnikom in ponudnikom sta tudi posebno lahka in stalna dostopnost iger na internetu ter morebiten povečan obseg in pogostost take mednarodne ponudbe v okolju, v katerem je igralec tudi izoliran in za katerega sta značilni anonimnost in neobstoj družbenega nadzora, dejavnika, ki pripomoreta k razvoju zasvojenosti z igrami na srečo in k z njimi povezani čezmerni porabi ter lahko zato povečata s tem povezane negativne družbene in moralne posledice, kot so poudarjene v ustaljeni sodni praksi (*Carmen Media*, točka 103). Zato je glede na navedeno na področju spletnih iger na srečo ključno vprašanje, ali je država sposobna izvrševati svojo suvereno oblast na svetovnem spletu in uresničevati zastavljene cilje.

Predlog zakona je odpravil zahtevo po sedežu koncesionarja na ozemlju Slovenije, zato se glede spletnih iger na srečo postavlja vprašanje izvrševanja učinkovitega nadzora nad imetniki koncesije, če bodo ti zunaj ozemlja Slovenije imeli tako sedež kot tudi spletni igralni sistem.[93] Vsaka država lahko izvaja suve-

[91] Sodba Sodišča v zadevi C-64/08, v kazenskem postopku proti Ernstu Engelmannu (2010).

[92] V zadevah *Engelmann* in *Dickinger* je Sodišče zaradi preprečevanja pranja denarja in goljufij štelo za dopustne zahteve po statusnopravni obliki imetnika koncesije (*Engelmann*, točka 30, in *Dickinger*, točka 76).

[93] Sodišče je v 84. točki sodbe v zadevi *Dickinger* prepustilo presojo nacionalnemu sodišču, ki naj presodi, ali je mogoče enako raven nadzora, kot je mogoča za subjekte s sedežem na ozemlju države članice, doseči na manj omejevalen način (kot z obveznim sedežem v državi članici) tudi za prireditelje iger na srečo s sedežem v drugih državah članicah.

reno oblast zgolj na svojem ozemlju, zato si ob ustaljeni sodni praksi Sodišča ni mogoče predstavljati, kako naj bi se v teh primerih izvrševal učinkovit nadzor, saj Sodišče samo priznava, da ne obstaja obveznost medsebojnega priznavanja dovoljenj za prirejanje iger na srečo ter da se države članice ne morejo zanesti na nadzor nad prireditelјem iger na srečo v drugi državi članici (glej *Liga Portuguesa*, točka 69; *Ladbrokes*, točka 54; *Sporting Exchange*, točka 33; *Dickinger*, točki 96 in 98; *Biasci*, točki 41 in 42). Pri tem stališču Sodišča moramo dodatno upoštevati, da se nanaša na države članice EU, v katerih je dosežen določen standard pravne države, medtem ko imajo prireditelji spletnih iger na srečo svoj sedež lahko tudi v tretjih državah, kjer sta pojma pravne države in pravne kulture šele v začetnih fazah razvoja.

Zato mora država kot suverena oblast, če želi svojo suverenost izkazovati tudi na spletnem področju in dejansko izvrševati zastavljene cilje na področju iger na srečo, zagotoviti učinkovite mehanizme nadzora zakonitih prireditelјev iger na srečo ter mehanizme preprečevanja nedovoljenega prirejanja spletnih iger na srečo na svojem ozemlju, saj so drugače vse zakonske omejitve in zapovedi le mrtva črka na papirju. Vendar kljub vsej regulativi in mehanizmom preprečevanja prirejanja nezakonitih iger na srečo država ne sme pozabiti na državljane, na ozaveščanje in izobraževanje državljanov, saj so le-ti tisti, ki ustvarjajo povpraševanje po (ne)zakonitih igrah na srečo. Namesto dokončnega odgovora je tako treba ugotoviti, da bodo ukrepi proti nezakonitemu prirejanju iger na sreče v posamezni državi članici odvisni od uspešnosti implementacije kombinacije preventivnih in izvršilnih ukrepov omejevanja iger na srečo. Zaradi varstva ustavnih svoboščin posameznikov ni sprejemljiva uvedba cenzure ali drugačna oblika omejevanja svobode interneta, ki bi v večji meri posegla v posameznikove svoboščine, zato se kot potencialno učinkovit izvršilni ukrep kaže prepoved plačilnih transakcij, ki manj posega v svoboščine posameznikov in hkrati izniči motiv nezakonitih prireditelјev iger na srečo. Kljub različnim ureditvam (spletnih) iger na srečo med posameznimi državami članicami EU bi bilo na ravni EU treba ob upoštevanju različnih pravnih ureditev po državah članicah sprejeti določene minimalne standarde (na primer standard elektronske identifikacije posameznikov) ter vzpostaviti sistem sodelovanja med nadzornimi organi držav članic, v okviru katerega bi si države članice izmenjevale dobre prakse glede izvršilnih ukrepov ter podatke o spletnih mestih in plačilnih poteh, ki se uporabljajo za nezakonito prirejanje iger na srečo.

Literatura in viri

Barnier, Michel: *Online Betting and Gambling in Europe:* from Consultation to Action, 27. 6. 2012.

Yves, Bota: *Sklepni predlogi generalnega pravobranilca Yvesa Bota* v zadevah C-203/08 in C-258/08, točki 55 in 56, z dne 17. 12. 2009.

Božič, Gorazd: *Problemi blokiranja spletnih mest.* http://hr-cjpc.si/pravokator/index.php/2010/01/06/problemi-blokiranja-spletnih-mest/ (15. 11. 2013).

Charif, Marcos: European Union Law and Online Gambling, The European Legal Outlook, oktober 2010.

Charif, Marcos: European Union Law, Online Gambling and Emerging Markets, pocket guide.

Cizelj, Dženeta: Koncesijska politika kot predmet morebitne spremembe Zakona o igrah na srečo. *Pravna praksa* 27 (2008) 28, str. 9–10.

Cizelj, Dženeta: Novela Zakona o igrah na srečo prinesla poskusne spremembe? *Pravna praksa* 29 (2010) 10, str. 18–19.

Cizelj, Dženeta: Sporno širjenje iger na srečo ob deklarativni skrbi za javno zdravje: nauki za Slovenijo iz zadeve Sodišča EU Carmen Media. Pravna praksa 30 (2011) 3, str. 13–14.

Ferčič, Aleš, Hojnik, Janja, Tratnik, Matjaž: *Uvod v pravo Evropske unije.* Ljubljana: GV Založba, 2011.

Hojnik, Janja. Komu po novem koncesije za prirejanje iger na srečo?. *Pravna praksa* 29 (2010) 43, str. 8–10.

Kupic, Gašper, Kovač, Mitja: Pravno ekonomska analiza spletnih iger na srečo: zaključna strokovna naloga Visoke poslovne šole Ljubljana 2013.

Rončević, Borut, Makarovič, Matej, Macur, Mirna: *Igre na srečo med prebivalci Slovenije.* Nova Gorica: Fakulteta za uporabne družbene študije (FUDŠ), 2009.

Schettini, Kearney: *The Economic Winners and Losers of Legalized Gambling* (2005). http://www.brookings.edu/~/media/research/files/papers/2005/2/gambling/200502kearney.pdf (10. 12. 2013).

Sladič, Jorg: Novejša praksa Sodišča ES glede javnih koncesij. *Podjetje in delo* (2008) 7, str. 1066–1078.

Vandall, Frank: Why We Are Outraged, An Economic Analysis of Internet Gambling.

Vatovec, Katarina: Konec monopola nad prirejanjem iger na srečo v Nemčiji?. *Pravna praksa,* 29 (2010) 36, str. 26–27.

Zajc, Katarina, Markelj, Luka: Ekonomski in pravni pogled na prirejanje spletnih iger na srečo: zakaj je monopol lahko boljši kot prosti trg. *Zbornik znanstvenih razprav* (2011), letnik 51, str. 237–258.

Commission staff working document. Online gambling in the Internal Market, accompanying the document: Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Com-

mittee of the Regions, Towards a comprehensive framework for online gambling. Strasbourg, 23. 10. 2012.

Davčna uprava RS. Register koncesionarjev in prirediteljev klasičnih iger na srečo, igralnic in igralnih salonov. http://www.durs.gov.si/si/storitve/storitve_v_zvezi_z_nadzorom_prirejanja_iger_na_sreco/registri_in_javne_evidence/ (15. 11. 2013).

Davčna uprava RS. Zbirni podatki o igrah na srečo v Sloveniji v obdobju 2005–2013 (januar–junij).

Direktorat za informacijsko družbo. Stališče Direktorata za informacijsko družbo k Zakonu o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-C), dne 13. 1. 2010. http://www.arhiv.mvzt.gov.si/nc/si/medijsko_sredisce/novica/article/101/6430/ (15. 11. 2013).

European commission. Commission will do all it can to help tackle match-fixing and corruption in sport, says Vassiliou, 18. 3. 2013.

European commission, Online gambling in the Internal Market – Frequently asked questions, 23. 10. 2012.

European commission, Directorate General Internal Market and Services, minutes, workshop on online gambling: 1. Protection of consumers of gambling services and 2. Responsible gambling advertising, 13. 6. 2013.

European commission. Recommendation on best practices in the prevention and combatting of betting related match fixing, december 2012.

Evropska komisija. Gambling. http://ec.europa.eu/internal_market/gambling/index_en.htm (15. 11. 2013).

Evropska komisija. Sporočilo komisije Evropskemu parlamentu, Svetu, Ekonomsko-socialnemu odboru in Odboru regij z naslovom Celovitemu evropskemu okviru za spletne igre na srečo naproti (23. 10. 2012).

Evropska komisija. sporočilo za medije: Komisija predstavila akcijski načrt za spletne igre na srečo, Bruselj, 23. 10. 2012.

Evropska komisija. Zelena knjiga o spletnih igrah na srečo na notranjem trgu z dne 24. 3. 2011.

Evropski parlament. Resolucija o spletnih igrah na srečo na notranjem trgu z dne 15. 11. 2011.

Evropski parlament. Poročilo o spletnih igrah na srečo na notranjem trgu z dne 11. 6. 2013.

Evropski parlament. Resolucija o vnaprejšnjem dogovarjanju o izidih tekem in korupciji v športu št. 2013/2657 z dne 14. 3. 2013.

Fakulteta za uporabne družbene študije (FUDŠ). Igranje na srečo med dijaki višjih letnikov srednjih šol, primerjava med goriško in dolenjsko regijo. Nova Gorica: FUDŠ, 2010.

Gambling industry code for socially responsible advertising, august 2007.

Informacijski pooblaščenec. Predlog zakona o spremembah in dopolnitvah zakona o igrah na srečo – mnenje Informacijskega pooblaščenca, št. 007-48/2009/4, dne 20. 4. 2010.

Informacijski pooblaščenec. Stališče Informacijskega pooblaščenca do pripomb Ministrstva za šolstvo in šport glede Zakona o spremembah in dopolnitvah zakona o igrah na srečo – ZIS-D (EVA 2010-1611-0084), št. 007-8/2010/10, dne 20. 10. 2010.

Informacijski pooblaščenec. Blokiranje internetnih strani zaradi iger na srečo, št. 0712-29/2010, dne 25. 1. 2010.

Informacijski pooblaščenec. Predlog Informacijskega pooblaščenca za spremembo Zakona o spremembah in dopolnitvah zakona o igrah na srečo – ZIS-C, št. 007-8/2010/2, dne 16. 2. 2010.

Informacijski pooblaščenec. Predlog zakona o igrah na srečo – Mnenje Informacijskega pooblaščenca, št. 007-84/2013/, dne 22. 10. 2013.

Ministrstvo za finance. Predlog za nujno spremembo Zakona o igrah na srečo, št. 007-139/2009/167, dne 9. 3. 2010.

Mnenje Evropskega ekonomsko-socialnega odbora o sporočilu Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij: Celovitemu evropskemu okviru za spletne igre na srečo naproti, 23. 10. 2012.

Odgovori RS Evropski komisiji na vprašanja Zelene knjige o spletnih igrah na srečo na notranjem trgu, 25. 7. 2011.

Poročevalec DZ. Predlog zakona o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-C) – prva obravnava – EPA 553-V, EVA: 2007-1611-0009, št. 00712-56/2009/8, Ljubljana, 27. 8. 2009.

Poročevalec DZ. Predlog zakona o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-D), skrajšani postopek, EPA 1366-V, EVA: 2010-1611-0084, št. 00712-57/2010/9, Ljubljana, 28. 10. 2010.

Poročilo o neoporečnosti spletnih iger na srečo, 17. 2. 2009.

Predlog Zakona o igrah na srečo, objavljen dne 24. 9. 2013; EVA 2013-1611-0041, <http://e-uprava.gov.si/e-uprava/zakonodajaIskanje.euprava?zadeva_id=3759> (15. 11. 2013).

Spletne igre na srečo v Evropi: vabilo na razpravo, Bruselj, 24. 3. 2011.

Svet EU. Igre na srečo in stave: pravni okvir in politike v državah članicah Evropske unije, št. 16022/08, Bruselj, dne 27. 11. 2008.

Upravno sodišče RS, sodba, opr. št. I U 2000/2010 z dne 21. 12. 2011.

Urad RS za prirejanje iger na srečo. Poročilo o delu, 2010.

Urad RS za prirejanje iger na srečo. Poročilo o delu, 2011.

Sodba Sodišča EFTA, zadeva E-1/06, *Nadzorni organ EFTA proti Kraljevini Norveški* (2007).

Sodba Sodišča EFTA, zadeva E-3/00, *Nadzorni organ EFTA proti Kraljevini Norveški* (2001).

Sodba Sodišča v zadevi C-64/08, v kazenskem postopku proti Ernstu Engelmannu (2010).

Sodba Sodišča v zadevi C-258/08 *Ladbrokes Betting & Gaming Ltd in Ladbrokes International Ltd proti Stichting de Nationale Sporttotalisator* (2010).

Sodba Sodišča v zadevi 34/79, *Regina proti Maurice Donald Henn in John Frederick Ernest Darby* (1979).

Sodba Sodišča v zadevi C-46/08, *Carmen Media Group Ltdb proti Land Schleswig-Holstein,* Innenminister des Landes Schleswig-Holstein (2010).

Sodba Sodišča v zadevi C-470/11, *SIA Garkalns proti Rīgas dome* (2012).

Sodba Sodišča v zadevi C-124/97, *Markku Juhani Läärä, Cotswold Microsystems Ltd in Oy Transatlantic Software Ltd proti Kihlakunnansyyttäjä (Jyväskylä) in Suomen valtio* (finska država) (1999).

Sodba Sodišča v zadevi C-203/08 *Sporting Exchange Ltd, ki posluje pod imenom »Betfair«, proti Minister van Justitie* (2010)

Sodba Sodišča v zadevi C-243/01, v postopku zoper Piergiorgia Gambellija in druge (2003).

Sodba Sodišča v zadevi C-268/99, *Aldona Malgorzata Jany in drugi proti Staatssecretaris van Justitie* (2001).

Sodba Sodišča v zadevi C-275/92, *Her Majesty's Customs in Excise proti Gerhart Schindler in Jörg Schindler* (1994).

Sodba Sodišča v zadevi C-42/02, v postopku na zahtevo Diane Elisabeth Lindman (2003).

Sodba Sodišča v zadevi C-6/01, *Associação Nacional de Operadores de Máquinas Recreativas (Anomar) in drugi proti Estado português* (2003).

Sodba Sodišča v zadevi C-67/98, *Questore di Verona proti Diego Zenatti* (1999).

Sodba Sodišča v zadevi C-42/07, *Liga Portuguesa de Futebol Profissional in Bwin International Ltd.* (2009).

Sodba Sodišča v združeni zadevi C-660/11 in C-8/12, *Daniele Biasci in drugi proti Ministero dell'Interno in Questura di Livorno* (C-660/11) in *Cristian Rainone in drugi proti Ministero dell'Interno in drugi* (2013).

Sodba Sodišča v združenih zadevah C-338/04, C-359/04 in C-360/04, v postopkih zoper Massimiliana Placanico, Christiana Palazzeseja in Angela Sorricchia (2007).

Sodba Sodišča v združenih zadevah C-316/07, od C-358/07 do C-360/07, C-409/07 in C-410/07, *Markus Stoß in drugi proti Wetteraukreis* ter *Kulpa Automatenservice Asperg GmbH in drugi proti Land Baden-Württemberg* (2010).

Vlada RS. Strategija razvoja iger na srečo v Sloveniji, št. 46100-2/2010/9 z dne 16. 12. 2010.

Vrhovno sodišče RS, sklep, opr. št. I Up 66/2012 z dne 16. 2. 2012.

Vrhovno sodišče RS, sklep, opr. št. I Up 169/2012 z dne 11. 7. 2012.

Vrhovno sodišče RS, sklep, opr. št. I Up 177/2012, enako tudi I Up 176/2012 z dne 12. 7. 2013.

Vrhovno sodišče RS, sklep, opr. št. I Up 321/2012 z dne 30. 8. 2012.
Vrhovno sodišče RS, sklep, opr. št. I Up 54/2012 z dne 16. 2. 2012.
Vrhovno sodišče RS, sklep, opr. št. I Up 77/2011 z dne 16. 2. 2011.
Vrhovno sodišče RS, sklep, opr. št. I Up 77/2011 z dne 16. 2. 2011.
Vrhovno sodišče RS, sklep, opr. št. I Up 90/2011 z dne 17. 2. 2011.

Kazenski zakonik, KZ-1, Uradni list RS, št. 55/2008, s spremembami in dopolnitvami.
Ustava Republike Slovenije, URS, Uradni list RS, št. 33/1991-I, s spremembami in dopolnitvami.
Zakon o elektronskem poslovanju na trgu, ZEPT, Uradni list RS, št. 61/2006, s spremembami in dopolnitvami.
Zakon o igrah na srečo, ZIS, Uradni list RS, št. 27/1995, s spremembami in dopolnitvami.
Zakon o inšpekcijskem nadzoru, ZIN, Uradni list RS, št. 56/2012, s spremembami in dopolnitvami.
Zakon o preprečevanju pranja denarja in financiranja terorizma, ZPPDFT, Uradni list RS, št. 60/2007 s spremembami in dopolnitvami.
Zakon o splošnem upravnem postopku, ZUP, Uradni list RS, št. 80/1999, s spremembami in dopolnitvami.
Zakon o spremembah in dopolnitvah Zakona o igrah na srečo, ZIS-A, Uradni list RS, št. 85/2001.
Zakon o spremembah in dopolnitvah Zakona o igrah na srečo, ZIS-C, Uradni list RS, št. 10/2010.
Zakon o spremembah in dopolnitvah Zakona o igrah na srečo, ZIS-D, Uradni list RS, št. 106/2010.
Zakon o spremembah in dopolnitvah Zakona o igrah na srečo, ZIS-E, Uradni list RS, št. 108/2012.
Zakon o upravnem sporu, ZUS-1, Uradni list RS, št. 105/2006, s spremembami in dopolnitvami.
Pravilnik o prirejanju iger na srečo preko interneta oziroma drugih telekomunikacijskih sredstev, Uradni list RS, št. 42/2008, s spremembami in dopolnitvami.

Nekateri pravnoekonomski vidiki navideznih valut[1]

dr. Meta Ahtik

1. Uvod

V zadnjem obdobju se pojavlja čedalje več t. i. navideznih oziroma virtualnih valut. Njihov nastanek je mogoče šteti za naravno pot razvoja digitalnega sveta, čeprav so zasebne valute obstajale tudi v sistemu papirnate valute. Žalosten konec sistema svobodnega bančništva v ZDA je svojevrstno opozorilo in hkrati izraža nujo po regulaciji tega področja, ki pa za zdaj precej zaostaja za njegovim razmahom.

Šele v zadnjem obdobju se pojavljajo nekateri regulativni ukrepi. Najpogosteje sicer države v poslovanje s temi valutami posegajo na davčnem področju, vendar pa pravni status teh valut večinoma ostaja precej nejasen.

Navidezne valute bodo umeščene v teorije o pravni naravi denarja, predstavljeni bodo tudi njihov trenutni ekonomski pomen in lastnosti. Prikazana bo porajajoča se pravna ureditev v izbranih državah in v Evropski uniji. Na koncu bo predstavljena tudi veljavna slovenska ureditev.

2. Pravna in ekonomska definicija denarja[2]

O denarju je mogoče govoriti samo v blagovnem gospodarstvu; če ni blaga, ni menjave in denar kot posrednik menjave ni potreben. Sprva se je menjala le ena vrsta blaga za drugo; splošnega menjalnega posrednika še ni bilo. Sčasoma se je zaradi poenostavitve trgovanja pojavilo blago, ki so ga ljudje splošno sprejemali v plačilo; nastal je splošni menjalni posrednik – denar. Pojavil se je tudi splošni ekvivalent – neko blago se je splošno uporabljalo kot merilec vrednosti vseh vrst blaga. Obe funkciji je lahko opravljala ena vrsta blaga, lahko pa sta bili ločeni.[3] Sčasoma so ljudje začeli hraniti svoje premoženje v nekem blagu

[1] Stališča, zapisana v tem prispevku, so osebna stališča avtorice in ne odražajo stališč Evropske centralne banke, v kateri je zaposlena.

[2] Poglavje je v glavnem povzeto po Ahtik, Monetarna …

[3] Ribnikar, 2003, str. 7–9.

(funkcija zaklada), ki se je zaradi svoje obstojnosti in trajne vrednosti izkazalo za najbolj praktično.[4]

Ekonomski pogled, po katerem je denar vsaka stvar, ki opravlja prej opisane funkcije denarja, pravno ni povsem sprejemljiv. Vloge na vpogled, ki ekonomsko gledano spadajo v denarni agregat M1,[5] pravno niso denar, ampak dolgovi. Podobno velja za denarna agregata M2[6] in M3;[7] v slednjem so celo vrednostni papirji. S pravnega vidika je med ekonomskimi funkcijami denarja poglavitna vloga splošnega menjalnega posrednika, ki je navadno tudi sestavni del pravne opredelitve denarja.[8] Obstajajo tri glavna pravna pojmovanja denarja.

Po **metalističnem razumevanju** je denar potrošna, zamenljiva, deljiva in premična plemenita kovina, zlasti zlato ali srebro, ki se ji zaradi njenih naravnih in ekonomskih lastnosti pripisujejo lastnosti denarja. Metalisti menijo, da je vloga države in prava le v tem, da s svojim žigom in avtoriteto jamči, da kos plemenite kovine, ki funkcionira kot plačilno sredstvo, vsebuje določeno količino kovine določene kvalitete. Država in pravo imata zgolj deklarativno vlogo. Tovrstno pojmovanje denarja je lahko vzdržalo le, dokler je gospodarsko življenje obvladoval stvarni denar. Ko je vlogo plačilnega sredstva prevzel zamenljivi papirni denar, je takšna opredelitev postala neprimerna. Če bi se držali metalistične opredelitve, danes denarja v pravnem pomenu sploh ne bi bilo.[9]

Državnopravno pojmovanje denarja je bilo v pravni literaturi vzpostavljeno v 17. stoletju, podrobneje pa ga je razčlenil nemški pravnik in ekonomist Knapp.[10] Pravica pravnega urejanja monetarnih zadev je bila sicer zgodovinsko gledano bistveni element vladajoče oblasti že prej.[11] Po državnopravnem pojmovanju je denar premična stvar, izdana po zakonskem (pravnem) pooblastilu, imenovana je po obračunski enoti in je univerzalno plačilno sredstvo v državi, ki je denar izdala.[12] Državnopravna teorija ima dva vidika. Menjalni posrednik postane denar le, če je ustvarjen po pooblastilu države oziroma druge oblasti, ki je nosilec suve-

[4] Hubbard, str. 18.

[5] V skladu z definicijo Evropske centralne banke (ECB, 1999, str. 35) obsega gotovino v obtoku in vloge čez noč.

[6] M2 po definiciji ECB obsega M1, vezane vloge do vključno dveh let in vloge na odpoklic z odpoklicem do vključno treh mesecev (prav tam, str. 35).

[7] V skladu z definicijo ECB obsega M2, repo pogodbe, delnice oziroma točke skladov denarnega trga ter dolžniške vrednostne papirje z dospelostjo do vključno dveh let (prav tam, str. 35).

[8] Mann, str. 5.

[9] Stranjak in drugi, str. 16.

[10] Prav tam, str. 16.

[11] Mann, str. 16.

[12] Prav tam, str. 8.

renosti, hkrati pa izgubi svoje lastnosti le s formalno demonetizacijo.[13] Država kot nosilec suverene oblasti in s tem tudi monetarne suverenosti in monetarnopravnega monopola je pooblaščena za izdajanje denarja in njegovo določitev za zakonito plačilno sredstvo. S tem določena premična stvar postane sestavni del monetarnega sistema in denar v pravnem smislu.[14] Izdajanje lastnega denarja je eden od zunanjih znakov suverenosti. Vsebina monetarne suverenosti pa se kaže v vodenju samostojne monetarne in fiskalne politike.[15] Kot ugotavlja Zimmermann, v sodobnem času vsebina monetarne suverenosti dobiva širše razsežnosti, saj lahko na primer zajema tudi regulacijo področij, kakršni sta finančna stabilnost in finančna integriteta (preprečevanje pranja denarja ipd.), hkrati pa zaradi globalizacije in nastanka regionalnih ekonomskih povezav potrebuje redefinicijo.[16]

Družbeno teorijo denarja večinoma zagovarjajo ekonomisti pa tudi nekateri pravniki, ki se zavzemajo za definicijo denarja, veljavno tako v pravni kot tudi v ekonomski znanosti. Osnove te teorije je postavil Savigny s trditvijo, da javno mnenje ne odloča le o tem, ali je nekaj denar, ampak tudi, v kolikšnem obsegu ima to lastnost. Za definiranje denarja je odločilno mišljenje ljudi, ki denar uporabljajo v vsakdanjem življenju. Denar so le tiste premične stvari in pravice, ki se splošno uporabljajo kot sredstvo menjave in ki jim državljani zaupajo. Pojem denarja ni vezan na državo, prav tako ni bistveno, ali je denar v materialni ali nematerialni obliki. Neka stvar postane denar, ko se med ljudmi vzpostavi zaupanje, da bo z njim mogoče danes ali v prihodnosti kupiti neke druge stvari. Obstajati mora splošno prepričanje, da bo ta stvar sposobna opravljati tudi funkcijo splošnega ekvivalenta. Če bi se uporaba posamezne navidezne valute zadostno razmahnila, bi v skladu s to teorijo taka valuta postala denar.

Mann meni, da bi bila ta teorija pravno relevantna le, če bi bila združljiva z državnopravno teorijo in bi lahko razložila pomen kriz za pravno definicijo denarja ter pokazala vsaj en sodoben primer, v katerem je denar v pravnem smislu pridobil ali izgubil svoje lastnosti po volji skupnosti, a proti volji neke vrhovne pravne ali dejanske oblasti. Vsebinsko bi to pomenilo, da bi bila država prisiljena sprejemati denar, ki ga ni določila za zakonito plačilno sredstvo. Proctorjeva teorija se od Mannove razlikuje po tem, da ves denar, ki ekonomsko gledano spada v M1, vključi v opredelitev denarja v pravnem pomenu z obrazložitvijo, da imajo depoziti pri bankah lahko dvojno vlogo in so torej lahko hkrati terjatev do banke in denar.[17]

[13] Mann, str. 19–20.
[14] Stranjak in drugi, str. 15–16.
[15] Mann, str. 15.
[16] Zimmermann, str. 24–31.
[17] Proctor, str. 35–37.

Ob upoštevanju opisanih teorij je **denar pravno** mogoče opredeliti kot deljivo, premično, zamenljivo, potrošno, telesno ali netelesno stvar oziroma pravico *sui generis*, ki opravlja družbeno funkcijo splošnega menjalnega posrednika in izraža vrednost vseh drugih dobrin. Za pravno pojmovanje denarja je bistven tudi element oblastnosti – denar dobi atribut državne suverene oblasti in postane edino obvezno plačilno sredstvo v neki državi. Denar lahko obstaja brez suverene oblasti, vendar takrat ni denar v pravnem pomenu. To lastnost mu daje obveznost uporabe, ki jo lahko predpiše samo suverena oblast. Seveda pa neka stvar ali pravica ne more biti denar v nasprotju z voljo uporabnikov denarja. Pravo, ki je povsem v nasprotju z družbeno prakso, ne more obstati. Prej ali slej se mora spremeniti. Denar v zgodovini ni izgubil ali pridobil svojih lastnosti proti volji oblasti le zato, ker so te pravočasno uvidele, da je potrebna sprememba, in jo tudi izvedle, navadno zato, ker je to koristilo tudi sami oblasti. V nasprotnem primeru bi konkurenca med denarnimi oblikami prav gotovo privedla do izrinjenja zakonitega plačilnega sredstva – če ne v celoti, pa vsaj v pretežnem delu transakcij. Če bo katera od virtualnih valut začela ogrožati tradicionalne valute, bodo denarne oblasti verjetno poskrbele, da se na neki način vključi v njihovo poslovanje.

Zakonito plačilno sredstvo, ki ga določa *lex monetae*, je tisti denar, ki ga nihče ne more odkloniti. Od treh uveljavljenih vrst denarja v obtoku so bankovci neomejeno zakonito plačilno sredstvo, kovanci so v večini držav zakonito plačilno sredstvo v omejenem obsegu,[18] knjižni denar, ki ga je največ, pa ni zakonito plačilno sredstvo. Zakon o plačilnih storitvah in sistemih (ZPlaSS)[19] med denarna sredstva šteje bankovce, kovance, knjižni denar in elektronski denar. Čeprav zahteva po plačevanju s knjižnim denarjem upnike izpostavlja kreditnemu tveganju,[20] Uredba ES 974/98 določa, da »omejitve plačil v bankovcih in kovancih, ki so jih iz javnih razlogov določile države članice, niso nezdružljive s statusom bankovcev in kovancev evra kot zakonitega plačilnega sredstva, pod pogojem, da so na razpolago druga zakonska sredstva za poravnavo monetarnih dolgov«.[21]

Vedno pa je med strankami mogoč drugačen dogovor – da se obveznost poravna v plačilni obliki, ki ni zakonito plačilno sredstvo v neki državi, na primer v tuji ali navidezni valuti. Za tovrstne transakcije lahko veljajo ustrezna pravila

[18] Upnik je dolžan pri posameznem plačilu sprejeti omejeno število (50) kovancev (11. člen Uredbe ES/974/98 o uvedbi eura.)

[19] Uradni list RS, št. 58/2009, s spremembami.

[20] Ribnikar, 2005, str. 75.

[21] Sem bi utegnila spadati tudi določba Pravilnika o izvajanju Zakona o davčnem postopku (23.a člen), ki izplačevalcem dohodkov nalaga, da morajo dohodke (obstajajo izjeme) nakazovati na transakcijski račun drugega subjekta. Bolj navadno bi sicer bilo, da bi se taka obveznost predpisala z zakonom, kakršna je tudi sicer praksa v drugih državah. Kaj se zgodi, če prejemnik zaradi stečaja kreditne institucije ne more priti do izplačanega dohodka?

davčnega, civilnega, gospodarskega prava in drugih pravnih panog pa tudi zakonodaja, ki ureja preprečevanje pranja denarja.[22]

3. Svobodno bančništvo[23]

Navidezne valute z marsikatero svojo lastnostjo spominjajo na sistem svobodnega bančništva, ki ima dolgo teoretično, hkrati pa precej kratko in manj uspešno praktično zgodovino. Prav ta je lahko opozorilo, kaj se s temi valutami lahko zgodi.

Svobodno bančništvo je ureditev, v kateri zasebne banke konkurenčno izdajajo bankovce brez znatnih pravnih omejitev. V takem sistemu ni centralne banke, ki bi imela monopol za izdajo bankovcev.[24] Banke v tako zasnovanem sistemu izdajajo neobrestovana potrdila (certifikate) in odpirajo račune na podlagi svojih registriranih blagovnih znamk. Različne banke torej izdajajo različna potrdila – različne valute. Z gotovino različnih bank se trguje po različnih menjalnih tečajih. Konkurenca in maksimiranje dobička bi vodila do ravnotežja, v katerem bi obstale le banke, ki bi na svoje obveznosti zagotavljale konkurenčne donose. Ker ta potrdila ne prinašajo obresti, je osnovna zahteva sistema zagotavljanje stabilne kupne moči denarja. Banke, ki si ne bi ustvarile tovrstnega ugleda, bi izgubile stranke, zato bi jih konkurenca izrinila s trga.

Mnoge države so pred uvedbo centralne banke poznale sistem svobodnega bančništva. Nastal je, ker kovanci niso zadostovali za povpraševanje po denarju in so potrebe po dodatnem denarju zadovoljile banke z izdajanjem bankovcev. Centralne banke so se oblikovale šele čez čas. Večina meni, da je bilo svobodno bančništvo le vmesna stopnja do nastanka ureditve s centralno banko, le nekaj pa je tistih, ki menijo, da denarni sistem brez centralne banke pomeni »naravno stanje stvari«.

Tudi v Sloveniji je ob osamosvajanju zaživel Zavod Lipa, ki je izdajal zasebni denar. Edini natisnjeni bankovec (za eno lipo) so sprejemali v okrog osemdeset podjetjih.

Poglavitni problem v sistemu prostega izdajanja denarja so sicer emisijske banke, ki želijo na trgu ostati le nekaj časa – toliko, da poberejo dobičke. Tako so delovale nekatere banke v Združenih državah Amerike (t. i. *wildcat* bančništvo), ki so izdale bankovce, nato pa so se umaknile v divjino (k divjim mačkam), da

[22] http://ec.europa.eu/economy_finance/euro/cash/legal_tender/index_en.htm.

[23] Poglavje je večinoma povzeto po Ahtik, Izdajanje …

[24] Monografijo o tej tematiki je izdal Hayek.

jih ne bi nihče iskal in zahteval menjave za rezerve.[25] Seveda podobno tveganje obstaja tudi pri izdajateljih navideznih valut.

4. Navidezne valute

4.1. Definicija

Za zdaj ne obstaja pravno relevantna definicija navideznih valut.[26] Glede na prakso njihove rabe pa obstaja več definicij.

ECB navidezno valuto definira (s pripombo, da bo razvoj uporabe morda zahteval spremembo definicije) kot »vrsto nereguliranega, digitalnega denarja, ki jo izdajajo in običajno tudi nadzorujejo njeni razvijalci ter je v rabi med člani neke navidezne skupnosti«.[27] GAO jo opredeljuje kot digitalni menjalni posrednik, ki nima podlage v zakonitem plačilnem sredstvu,[28] FinCEN pa kot menjalni posrednik, ki v nekaterih okoljih deluje kot valuta, a nima vseh lastnosti prave valute.[29] EBA jo je v opozorilu, izdanem decembra 2013, opredelila kot obliko nereguliranega digitalnega denarja, ki ga centralna banka ne izda ali zanj ne jamči in se lahko uporablja kot plačilno sredstvo.[30]

Navidezno valuto je navadno mogoče pridobiti na dva načina: z nakupom, z uporabo pravega denarja, po prej določenem menjalnem tečaju ali z vnaprej določenimi aktivnostmi (sodelovanje v promocijskih akcijah, spletnih raziskavah).[31]

Razlikovati je mogoče tri vrste navideznih valutnih shem:[32]

- **zaprte navidezne valutne sheme** brez povezave z realnim gospodarstvom, pri katerih lahko uporabnik po plačilu določene pristojbine kupuje navidezne dobrine in storitve le znotraj navidezne skupnosti (na primer World of Warcraft Gold);
- **navidezne valutne sheme z enostranskimi tokovi**, pri katerih je navidezno valuto mogoče kupiti s »pravim« denarjem po določenem menjalnem tečaju, a je ni mogoče zamenjati nazaj; te valute omogočajo nakupe navideznih,

[25] Ribnikar, 2003, str. 343.

[26] Uporabljata se tudi izraza virtualna valuta in kriptovaluta (za digitalne valute, temelječe na kriptografiji).

[27] ECB, str. 13.

[28] Government Accountability Office (GAO), str. 3.

[29] Financial Crimes Enforcement Network, FIN-2013-G001, str. 1.

[30] EBA, str. 1.

[31] ECB, str. 13.

[32] Osnovni kriterij delitve sta raven interakcije s pravim denarjem in možnost nakupov dobrin in storitev v nevirtualnem svetu (prav tam, str. 13, BIS, str. 50).

včasih pa tudi realnih dobrin in storitev (na primer Amazon coins, programi zvestobe – na primer v letalskem prometu (*frequent flier)*[33]);

- **navidezne valutne sheme z dvostranskimi tokovi**, pri katerih je navidezno valuto mogoče po veljavnem menjalnem tečaju spreminjati v »pravi« denar in ki omogočajo nakup tako navideznih kot realnih dobrin in storitev (bitcoin, lindenski dolarji v virtualnem svetu Second life).[34]

Očitno je, da taka valuta ne more biti zakonito plačilno sredstvo. Postavlja pa se vprašanje, ali in koliko neka navidezna valuta izpolnjuje prej opisane (ekonomske) funkcije denarja. Najverjetneje je odgovor, vsaj znotraj neke navidezne skupnosti, pritrdilen, ko gre za menjalni posrednik,[35] morda pa (odvisno od stabilnosti tečaja) tudi pri obračunski enoti oziroma merilcu vrednosti. Pogosto pa zaradi nihanj v vrednosti navidezna valuta ni uporabna kot obračunska enota, še manj pa kot hranilec vrednosti (zaklad).[36]

Navidezne valute druge in zlasti tretje predhodno opisane vrste se torej uporabljajo zlasti za izvedbo plačil. Podobno kot sicer imajo tudi v navideznem gospodarstvu vse transakcije dva elementa poravnave – dobavo navideznih ali realnih dobrin oziroma storitev ter prenos sredstev. Navidezne valutne sheme so podobne plačilnim sistemom[37] majhnih vrednosti (*retail payment system*), čeprav vanje niso vključeni finančni posredniki. Plačilni sistem deluje po naslednji poti: plačilni instrument je sredstvo avtorizacije in vložitve plačila, sledita obdelava in kliring, ki pomenita izmenjavo plačilnega naloga med upnikom in dolžnikom, nato pa pride do poravnave – knjiženja na računih obeh uporabnikov. V primeru navideznih valut bančni posredniki niso vključeni, prav tako ni tretjih subjektov, ki bi izvedli plačilo (kliring, poravnavo). Računa obeh, upnika in dolžnika, sta znotraj organizacije, ki upravlja shemo. Navadno gre za plačila majhne vrednosti (*retail*), ki se poravnavajo po bruto načelu, vsako plačilo se namreč poravna posamično.[38]

Dne 1. 2. 2014 je tržna kapitalizacija navideznih valut znašala 13,5 milijarde dolarjev. V primerjavi s količino denarnega agregata M3, ki je v obtoku v evrskem območju, ta znesek zajema zgolj 0,1 % evrskega M3. Vrednost navideznih

[33] Vrednost teh programov je že leta 2005 presegla količino dolarskih bankovcev in kovancev v obtoku.

[34] ECB, str. 13–14.

[35] Razsežnost te lastnosti je seveda odvisna od števila uporabnikov.

[36] Prav tam, str. 11.

[37] Plačilni sistem je mogoče definirati kot sklop instrumentov, pravil in procedur za prenos sredstev med udeleženci.

[38] ECB, str. 17–18.

valut sicer precej niha[39] – na primer v 24 urah je ena od prikazanih navideznih valut pridobila kar 129 % vrednosti prejšnjega dne, druga pa izgubila 19 % svoje vrednosti.

Tržna kapitalizacija 82 navideznih valut na dan 1. 2. 2014

	Tržna kapitalizacija	**Tečaj glede na USD**	**Količina v obtoku**
Bitcoin	10.350.213.639	838,85	12.338.575
Ripples	2.074.178.989	0,0210	98.770.428.048
Litecoin	570.680.840	22,520	25.341.067
Peercoin	124.446.252	5,9000	21.092.585
Nxt	63.643.421	0,0640	994.428.453
DogeCoin	62.225.963	0,0015	41.483.975.333
MasterCoin	48.506.930	86,130	563.183
Namecoin	44.563.088	5,6300	7.915.291
Quark	22.211.614	0,0900	246.795.711
ProtoShares	18.078.098	12,850	1.406.856
druge (72 valut)	125.166.106	0,0002	749.661.366.602
SKUPAJ	13.503.914.940	0,0152	891.225.651.704

Vir: http://coinmarketcap.com.

Yermack ugotavlja, da se tečaj najpomembnejše navidezne valute, bitcoina, obnaša podobno kot internetne delnice konec devetdesetih let, kar ga po naložbenih lastnostih približuje špekulativni naložbi. Njegov tečaj se torej ne obnaša tako kot menjalni tečaji tujih valut.[40]

Na vprašanje, kako dolgo bodo posamezne navidezne valute trajale, je težko odgovoriti. Vsekakor pa je precej takih valut že propadlo (na primer e-gold).

4.2. Bitcoin

Že leta 1999 je v pogovoru za National Taxpayers Union Foundation valuto z lastnostmi, ki povsem ustrezajo bitcoinu, napovedal Milton Friedman.[41] Samo navidezno valuto bitcoin pa je v članku leta 2008 zasnoval Satoshi Nakamoto,[42]

[39] Več v poglavju 4.2.

[40] Yermack, str. 2.

[41] http://www.youtube.com/watch?v=6MnQJFEVY7s.

[42] Ime je psevdonim, poleg tega ni znano, ali gre za posameznika ali skupino.

ki jo je tudi uveljavil. Predlagal je alternativni plačilni sistem brez posrednika, ki je sicer običajen člen pri izvajanju kakršnihkoli transakcij. Izvajanje spletnih transakcij brez posrednika je seveda cenejše. Ustrezno uporabo plačilnega sredstva omogoča kriptografski zapis, ki nadomesti zaupanje, ki ga sicer zagotavlja izvajanje transakcij prek plačilnih posrednikov. Elektronski kovanec je Nakamoto definiral kot verigo digitalnih podpisov. Vsak imetnik kovanec iz svoje elektronske denarnice z elektronskim podpisom podatkov o predhodno izvedenih transakcijah in podpisom javnega dela ključa naslednjega lastnika kovanca prenese v elektronsko denarnico prejemnika. Ta lahko preveri verigo lastništev.[43] Računalniški algoritmi torej zagotavljajo zaščito pred goljufijami, kakršna je na primer dvojno plačilo z istimi bitcoini. Izvedbe plačila ni mogoče naknadno preklicati, kar ščiti prodajalca.[44]

Bitcoinov ne izdaja neka centralna oblast, prav zato v povezavi z njimi tudi ni mogoče vodenje denarne politike. Ta je na neki način vgrajena v sam sistem njihovega nastajanja, saj se v skladu z računalniškim algoritmom bitcoini sproščajo v obtok z vnaprej opredeljivo hitrostjo.[45]

Idejna zasnova in tudi dejanske lastnosti valute v marsičem sledijo lastnostim, ki jih je kot denar izkazovalo zlato, čeprav je za mnoge sporno, da nima nikakršne notranje vrednosti.[46, 47] Tako kot zlato ima tudi deflacijske težnje – končna količina bitcoinov v obtoku je namreč omejena na 21 milijonov, kar pomeni, da njihova količina v obtoku (ob predpostavki gospodarske rasti) ne bo mogla slediti proizvedeni količini dobrin in storitev. Zato se bo njihova vrednost povečevala, cene blaga, denominirane v bitcoinih, pa zniževale. S tem pa upada tudi motivacija za trošenje. Ne nazadnje asociacijo na zlato vzbuja tudi eden od načinov pridobivanja bitcoinov – »rudarjenje«.

Uporabnik bitcoinove mreže mora na svoj računalnik najprej naložiti brezplačen odprtokodni program. Pridobivanje bitcoinov je mogoče na tri načine: »rudarjenje«, nakup z uporabo »pravega« denarja in prodaja dobrin ali storitev s plačilom v bitcoinih.

»Rudarjenje« je uporaba moči računalniškega procesorja za reševanje kompleksnih matematičnih problemov. Uspešni uporabnik je nagrajen s (trenutno) 25 bitcoini.[48] Verjetnost, da bo računalnik rešil matematični problem, je soraz-

[43] Nakamoto, str. 1–2.

[44] Nakamoto, str. 1.

[45] Jeong, str. 2.

[46] Notranja vrednost denarja je vrednost materiala, iz katerega je denar narejen (Bajt in Štiblar, str. 434).

[47] Matonis, http://themonetaryfuture.blogspot.de/2011/06/why-are-libertarians-against-bitcoin.html.

[48] Prav tam, str. 4.

merna z močjo njegovega grafičnega procesorja, kar pomeni, da je pri navadnem računalniku praktično zanemarljiva. Hitrost pridobivanja bitcoinov je mogoče napovedati. Njihova količina je omejena na 21 milijonov – to številko naj bi dosegli leta 2140.[49]

Nakup bitcoinov je mogoč z običajnimi valutami (dolar, evro itd.). Cena je določena z interakcijo ponudbe in povpraševanja[50] ter trenutno (1. 2. 2014) znaša 838,85 dolarja za bitcoin.[51] Nihanja v ceni so sicer izjemno velika – Yermack navaja, da je med 1. 1. 2013 in 29. 11. 2013 volatilnost[52] bitcoina znašala 133 %, medtem ko menjalni tečaji običajnih valut nihajo med 8 in 12 %, volatilnost zelo tveganih delnic pa se zgolj približuje 100 %.[53]

Uporabnik lahko bitcoine pridobi tudi tako, da jih sprejme v zameno za dobrino ali storitev.

Bitcoine je mogoče hraniti v elektronski denarnici na lastnem računalniku (oziroma pametnem telefonu) ali na strežniku. Oba načina hrambe sta povezana s tveganjem.[54] Pride lahko do okvare ali hekerskega napada na strežnik.[55]

Prednosti uporabe bitcoinov kot plačilnega sredstva sta brezplačnost transakcij in višja raven zasebnosti, medtem ko so ključne pomanjkljivosti neuživanje statusa zakonitega plačilnega sredstva, majhno število uporabnikov, veliko nihanje menjalnega tečaja glede na prave valute in deflacijsko tveganje. Pojavljajo se tudi hekerski napadi, katerih žrtve so tako borze kot elektronske denarnice posameznih uporabnikov.[56] Bitcoinska mreža naj bi izkazovala celo nekatere lastnosti Ponzijeve sheme (denarne piramide) – iz nje je namreč mogoče izstopiti le, če obstaja nekdo, ki je od izstopajočega uporabnika bitcoine pripravljen odkupiti.[57]

Uporaba bitcoinov je priljubljena pri računalniških zanesenjakih, libertarcih, ki nasprotujejo centralnemu izdajanju denarja,[58] pa tudi pri kriminalcih, saj jim zaradi (relativne)[59] anonimnosti lajša trgovino s prepovedanim blagom in pranje denarja.

---

[49] Elwell in drugi, str. 2.

[50] Prav tam, str. 2.

[51] http://coinmarketcap.com.

[52] Odstotkovna sprememba dnevnega menjalnega tečaja, preračunana na letno raven.

[53] Yermack, str. 7.

[54] Podobno seveda velja za hrambo gotovine, ki jo lahko uniči požar, ukrade tat ipd.

[55] EBA, str. 2.

[56] Elwell in drugi str. 6–8.

[57] ECB, str. 27.

[58] Obsežno analizo problema je podal Hayek, 1990.

[59] Transakcije so natančno zabeležene in jim je mogoče slediti.

Kljub osnovni ideji plačilnega sistema brez posrednikov je bilo ustanovljeno veliko število borz, na katerih se trguje z bitcoini. Po podatkih iz aprila 2013 je moralo prenehati delovati 45 % borz, vsaj 5 od 18 propadlih trgovalnih platform pa svojih uporabnikov ni poplačalo.[60] Opozorilo o tveganjih, povezanih s platformami za hrambo ali menjavo navideznih valut, je decembra 2013 dala tudi EBA.[61]

4.3. Pravni status navideznih valut

Za rabo zasebnega denarja ne velja *lex monetae*, veljajo pa lahko pravila številnih drugih pravnih panog. Regulacija tehnološkemu razvoju navadno sledi šele čez nekaj let. Tako so se navidezne valutne sheme v ZDA pojavljale že ob koncu devetdesetih let, medtem ko je do prvega regulativnega posega prišlo šele leta 2006.[62] Na vprašanje, kakšna je pravna narava navideznih valut, pa še ni odgovora, čeprav se s tem vprašanjem ukvarjajo (zlasti davčniki) v številnih državah. Odgovor je seveda odvisen od države, vendar pa bi globalna narava navideznih valut zahtevala koordinacijo med državami.

Sledi pregled do zdaj podanih stališč o statusu navideznega denarja (oziroma bitcoinov, saj se ureditev v mnogih državah nanaša samo nanje) v različnih državah oziroma povezavah držav.

4.3.1. Združene države Amerike

V ZDA (podobno kot drugod po svetu) največjo pozornost namenjajo navidezni valuti z največjim tržnim deležem – bitcoinu.

Zanimivo je, da (drugače od mnogih držav, ki so se najprej lotile davčnih vidikov navideznih valut) Internal Revenue Service (IRS) še ni opredelila davčnega statusa navideznih valut, čeprav se s tem vprašanjem ukvarja že od leta 2007.[63]

FinCEN je marca 2013 izdal navodilo, v skladu s katerim so subjekti, vpleteni v izdaje navidezne valute in njene umike iz obtoka, in subjekti, ki navidezne valute menjajo za pravi denar ali druge navidezne valute, podjetja, ki izvajajo denarne storitve (*money service business*), natančneje prenos denarja in plačilne storitve (*money transmitters*).[64] Definicija te dejavnosti je sicer odvisna od zvezne države, a je v mnogih državah dovolj ohlapna, da omogoča podreditev pravnim pravilom za nekatere subjekte, ki se ukvarjajo z bitcoini. Na podlagi navodila FinCENa je že bilo izvedenih nekaj ukrepov (opozorila, zaprtje računov ipd.).

[60] Moore in Christin, str. 13.
[61] EBA/WRG/2013/01.
[62] ECB, str. 43.
[63] Rubin in Dougherty.
[64] FIN-2013-G001, str. 1.

Celo Mt.Gox, največja trgovalna platforma z bitcoini, ki je opravila okrog 80 %[65] vseh transakcij,[66] se je po številnih pritiskih junija 2013 registrirala kot podjetje, ki izvaja denarne storitve, in je s tem podvržena zakonodaji s področja preprečevanja pranja denarja.[67]

Pred sodiščem (United States District Court, Eastern District of Texas, Sherman Division) se je do zdaj znašel le spor med SEC (Securities and Exchange Commission) ter Trendonom T. Shaversom in Bitcoin & Savings and Trust.[68] Shavers naj bi reklamiral investicije v finančne produkte, vezane na bitcoin. Investitorjem je ponujal 1 % oziroma kasneje celo 3,9 % dnevne obresti, in sicer, dokler ne dvignejo sredstev oziroma dokler so njegovi posli donosni (*either you withdraw the funds or my local dealings dry up and I can no longer be profitable*). Investitorji so tako izgubili 1,8 milijona dolarjev glavnice (merjeno po cenah na dan nakupa bitcoinov) oziroma več kot 23 milijonov dolarjev, merjeno po menjalnem tečaju bitcoinov v času odločanja. Sodišče je odločalo, ali so Shaversovi finančni produkti vrednostni papirji (in s tem zadeva spada v regulatorno pristojnost SEC) ali ne. Shavers je trdil, da ni tako, saj bitcoini niso denar. V okviru poslov naj bi torej ne bilo nikakršnih denarnih transakcij. Sodišče se je oprlo na uveljavljeno definicijo investicijske pogodbe, ki obsega kakršnokoli pogodbo, transakcijo ali shemo, ki vključuje (1) investicijo denarja, (2) v skupni podjem (3) s pričakovanjem dobička, ki ga bo ustvaril subjekt, ki promovira investicijo, ali kdo tretji.

Za pravni status bitcoina je ključna prva točka. Ali torej bitcoini pomenijo investicijo denarja? Sodišče je odločilo, da je jasno, da jih je mogoče uporabljati kot denar, saj se z njimi lahko kupujejo dobrine in storitve. Edina omejitev je dejstvo, da so plačilno sredstvo le v omejenem obsegu – pri subjektih, ki so jih pripravljeni sprejemati. Poleg tega jih je mogoče zamenjati za običajne valute. Sodišče je zaključilo, da so bitcoini valuta oziroma oblika denarja, investicija, izvedena z njimi, pa izpolnjuje prvi navedeni pogoj.

Dejstvo, da je FBI zaprl nezakonito internetno tržnico Silk Road, kjer so se bitcoini uporabljali za plačevanje prepovedanih drog in druge prepovedane posle, ter zasegel tudi bitcoine v tedanji vrednosti okoli štirih milijonov dolarjev,[69] pa spet opozarja na morda največjo pomanjkljivost navideznih valut.

---

[65] Deloma tudi zaradi tega se je njen tržni delež potem precej zmanjšal (http://www.coindesk.com/mt-gox-registers-with-fincen-as-a-money-services-business/).

[66] Koncentracija trga na področju trgovanja z bitcoini je torej zelo visoka.

[67] Sparshot, http://online.wsj.com/news/articles/SB10001424127887323873904578574000957464468.

[68] Case No. 4:13-CV-416, 8. 6. 2013.

[69] Kodrič, str. 34.

Dosedanji oblastveni ukrepi v ZDA kažejo, da bi bitcoini (pa tudi nekatere druge navidezne valute) utegnili biti oblika denarja.

4.3.2. Kitajska

Kitajska centralna banka je decembra 2013 finančnim ustanovam in izvajalcem plačilnih storitev prepovedala uporabo bitcoinov, medtem ko ga drugi subjekti lahko uporabljajo. Bitcoini po stališču centralne banke niso valuta v pravem pomenu besede in tudi nimajo takega pravnega statusa. Razlog za prepoved sta zlasti ovirano izvajanje kapitalskih kontrol, ki so v veljavi na Kitajskem, ter tveganje za finančno stabilnost.[70]

Bitcoin je na Kitajskem postal zelo priljubljen, kar je prispevalo k dvigu njegovega tečaja v zadnjem letu. Tečaj je po prepovedi uporabe za finančne institucije precej upadel.[71]

4.3.3. Evropska unija

Najprej bo predstavljena skupna ureditev na ravni Evropske unije oziroma evrskega območja, ki seveda zadeva tudi Slovenijo. Države evropske denarne unije uporabljajo skupno valuto – evro, zato zanje velja skupen *lex monetae*, ki ga sestavljata prvi odstavek 128. člena PDEU[72] (status bankovcev) in 11. člen Uredbe ES/974/98[73] (status kovancev). Od tod jasno izhaja, da navidezne valute niso zakonito plačilno sredstvo. V vseh državah Evropske unije oziroma Evropskega gospodarskega prostora pa veljajo tudi nekateri drugi predpisi, ki bi lahko veljali za navidezne valute.

Nekatere lastnosti navideznih valut tako govorijo v prid dejstvu, da bi lahko šlo za posebno vrsto elektronskega denarja (njegovo izdajo ureja Direktiva 2009/110/ES),[74] ki se uporablja za transakcije na spletu, vendarle pa je med navideznimi valutnimi shemami in shemami za izdajo elektronskega denarja precej razlik. Elektronski denar v skladu z direktivo pomeni denarno vrednost, shranjeno v elektronski obliki, ki pomeni terjatev do izdajatelja, izdano na podlagi prejema denarnih sredstev za namen izvrševanja plačilnih transakcij, in ki jo sprejme fizična ali pravna oseba, ki ni izdajatelj elektronskega denarja.

[70] Bloomberg News.

[71] Vrednost bitcoina je zgolj v nekaj urah upadla s približno 1.220 na dobrih 900 dolarjev (Konda).

[72] Pogodba o delovanju EU, UL C 83/47, 30. 3. 2010.

[73] Uredba sveta (ES) št. 974/98 o uvedbi eura.

[74] Direktiva o začetku opravljanja in opravljanju dejavnosti ter nadzoru skrbnega in varnega poslovanja institucij za izdajo elektronskega denarja ter o spremembah direktiv 2009/110/ES.

Sheme elektronskega denarja so nadzorovane in uživajo jamstvo, sredstva je, kot zahteva 11. člen Direktive 2009/110/ES mogoče dobiti nazaj po njihovi nominalni vrednosti (*par value*). Nasprotno pa se menjalni tečaj navideznih valut v razmerju do tradicionalnih valut oblikuje glede na ponudbo in povpraševanje ter lahko precej niha, kar pomeni, da pogoj iz 11. člena Direktive ni izpolnjen. »Izdajatelj«[75] bitcoinov na primer sploh ni zavezan izplačati protivrednosti v pravi valuti. Tako elektronski denar kot navidezna valuta sta sicer izdana v digitalni obliki, vendar pa elektronski denar temelji na tradicionalnih valutah, ki imajo status zakonitega plačilnega sredstva, medtem ko je pri navideznih valutah obračunska enota valuta brez statusa zakonitega plačilnega sredstva. Elektronski denar je reguliran, izdaja ga regulirana institucija za izdajo elektronskega denarja, navidezne valute so neregulirane, pogosto jih izdaja nefinančna gospodarska družba, ki ni podvržena običajni regulaciji finančnega sektorja. V prvem primeru je ponudba denarja omejena, v drugem pa neomejena, saj temelji na izdajateljevi odločitvi. Elektronski denar je večinoma povezan le z operativnim tveganjem (nevarnost okvare sistema, na katerem je shranjen), navidezne valutne sheme pa tako s pravnim (zaradi pomanjkanja regulacije in nevarnosti goljufij), kreditnim, likvidnostnim kot tudi operativnim tveganjem.[76] Ugotoviti je torej mogoče, da navidezne valute niso elektronski denar.

ECB je tudi zapisala, da izdajatelj bitcoina v skladu z Direktivo 2007/64/ES[77] ne pride v poštev kot plačilna institucija, saj naj plačilne institucije ne bi smele izdajati elektronskega denarja. Kot je bilo ugotovljeno v predhodnem besedilu, pa navidezne valute sploh niso elektronski denar. Glede na to, da naj bi direktiva urejala pravila za izvrševanje plačilnih transakcij, pri katerih so sredstva v obliki elektronskega denarja, pa je vendarle očitno, da subjekti, ki opravljajo plačila z virtualnimi valutami, ne morejo biti podvrženi tej direktivi.

Problematična je tudi pravna podlaga za delovanje bitcoinskega plačilnega sistema. ECB tako navaja naslednje pomanjkljivosti: pomanjkanje ustrezne pravne podlage za delovanje plačilnega sistema pa tudi pomanjkanje jasne definicije pravic in obveznosti strank, zlasti kdaj pride do dokončnosti poravnave.[78] Avtorji oziroma uporabniki največje virtualne denarne sheme (bitcoinov) sicer trdijo, da

[75] Je pa vprašanje, kdo sploh je izdajatelj – avtor ideje bitcoinov, ki (razen po vzdevku) sploh ni znan, posameznik, ki »narudari« bitcoine, ali kdo tretji?

[76] ECB, str. 16–17.

[77] Direktiva 2007/64/ES Evropskega parlamenta in Sveta o plačilnih storitvah na notranjem trgu in o spremembah direktiv 97/7/ES, 2002/65/ES, 2005/60/ES in 2006/48/ES ter o razveljavitvi Direktive 97/5/ES.

[78] ECB, str. 40.

je vsako izvedeno plačilo, ko je enkrat potrjeno, dokončno,[79] seveda pa gre tu zgolj za eno stran transakcije.

EBA opozarja, da ob uporabi virtualne valute za plačilo blaga in storitev drugače kot pri prenosih z običajnega bančnega ali drugega plačilnega računa ni pravice do povračila. Nedovoljene ali nepravilne bremenitve iz digitalne denarnice navadno ni mogoče razveljaviti. Poleg tega so virtualne valute zasebni denar, kar pomeni, da jih gospodarski subjekti sprejemajo povsem prostovoljno (medtem ko je zakonito plačilno sredstvo vsakdo dolžan sprejeti) in se lahko kadarkoli odločijo, da jih bodo prenehali sprejemati.[80]

4.3.4. Danska

Danski finančni regulator je zavzel stališče, da v danskem pravnem redu ni pravne podlage, ki bi omogočala regulacijo poslov, povezanih z bitcoini. Njihova uporaba je torej povsem prosta.[81]

4.3.5. Finska

Finska centralna banka je odločila, da bitcoin ne ustreza niti definiciji valute niti definiciji plačilne oblike. Definicija slednje namreč zahteva izdajatelja, ki je odgovoren za njeno delovanje. Bitcoine je torej klasificirala kot blago.[82] Podobno možno rešitev omenjajo (sicer za ZDA, ki pa so v svoji definiciji očitno krenile v drugo smer) tudi Elwell in soavtorji.[83]

Uporaba bitcoinov je povsem prosta, na Finskem deluje celo prvi bankomat (verjetno bi ga bilo bolje imenovati prodajni avtomat?), na katerem je mogoče kupiti bitcoine. Kapitalski dobički iz trgovanja z bitcoini so obdavčeni, čeprav morebitnih izgub ni mogoče odbiti. Za »narudarjene« bitcoine morajo Finci plačati dohodnino.[84]

4.3.6 Francija

Banque de France je v zadnji decembrski številki glasila Focus podala ugotovitev, da bitcoini niso niti zakonito plačilno sredstvo niti elektronski denar. Utemeljitev slednjega sledi razlagi, ki jo je bila podala ECB. Posebej so poudarili dejstvo, da bitcoini (drugače od elektronskega denarja) niso v kateremkoli tre-

[79] Nakamoto, str. 1.
[80] EBA, str. 2.
[81] Schwartzkopff in Levring.
[82] Pohjanpalo.
[83] Elwell in drugi, str. 16.
[84] Pohjanpalo.

nutku zamenljivi za pravi denar po nominalni vrednosti.[85] Ta navsezadnje sploh ni določena.

Francoski nadzorni organ (L'Autorité de contrôle prudentiel et de résolution – ACPR), ki deluje v okviru centralne banke, pa je podal uradno stališče, da menjava bitcoinov za denar, ki je zakonito plačilno sredstvo, in stalna dejavnost posredovanja med kupci in prodajalci bitcoinov, pomenita obliko plačilnih storitev, za katere je potrebno dovoljenje nadzornega organa. Storitve lahko opravljajo kreditna institucija, družba za izdajo elektronskega denarja ali plačilna institucija. Pogoj za izdajo dovoljenja so zagotovitev ustreznega obsega kapitala, strukture financiranja in obsega lastnih sredstev ter ustrezno vodenje družbe. Družba, ki se ukvarja s to dejavnostjo, mora zagotoviti notranji nadzor in izvajati ukrepe za preprečevanje pranja denarja in financiranja terorizma.[86]

4.3.7. Italija

Italija je ena prvih držav, v katerih je bila predlagana celo zakonska ureditev bitcoinovega statusa, kar pa seveda še ne pomeni, da bo predlog sprejet.

Predlog spremembe zakona (gre za zakon, namenjen izvajanju ukrepov načrta Direzione Italia,[87] ki sicer ureja precej raznolika področja, kot so na primer znižanje tarif za električno energijo in plin, internacionalizacijo, razvoj in digitalizacijo poslovanja podjetij, javna dela in EXPO 2015) v skladu z usmeritvijo zakona (promocija digitalizacije) tako predlaga ureditev, po kateri se kriptovalute na spletu uporabljajo kot dopolnilni menjalni posrednik brez funkcije hranilca vrednosti. Predvidena je obvezna identifikacija strank ob transakcijah, ki presegajo vrednost 1000 evrov. Za plačila z bitcoini naj bi v skladu s predlogom veljala zakonodaja, ki ureja preprečevanje pranja denarja.[88]

4.3.8. Nemčija

Nemško finančno ministrstvo je podalo stališče, da bitcoini niso niti domače niti tuje zakonito plačilno sredstvo.[89] Prav tako niso elektronski denar, saj niso izdani na podlagi prejetega denarnega zneska (eden od že opisanih pogojev za

[85] Banque de France, str. 1.

[86] ACPR, str. 1.

[87] Interventi urgenti di avvio del piano »Destinazione Italia«, per il contenimento delle tariffe elettriche e del gas, per la riduzione dei premi RC-auto, per l'internazionalizzazione, lo sviluppo e la digitalizzazione delle imprese, nonche' misure per la realizzazione di opere pubbliche ed EXPO 2015, 23 dicembre 2013, n. 145.

[88] Besedilo predloga zakona ni na voljo na parlementarni spletni strani, ga pa povzema Tamburrino.

[89] Ministrstvo je pojasnilo podalo v odgovoru na poslansko vprašanje (Bundesministerium, str. 1–2).

obstoj elektronskega denarja, naveden v Direktivi 2009/110/ES), ampak na podlagi uporabe »računalniške moči«.

Ministrstvo jih je naposled razglasilo za obračunske enote (*Rechnungseinheiten*) oziroma zasebni denar, saj se uporabljajo kot plačilno sredstvo na podlagi pogodbenih dogovorov – torej na podlagi zasebnega prava.[90]

Za vse »obračunske enote« tudi velja, da spadajo med finančne instrumente (podobno velja na primer za tuje valute; finančni instrumenti pa so seveda tudi delnice in obveznice). Trgovanje s finančnimi instrumenti zahteva dovoljenje in nadzor pristojnega nadzornega organa – v Nemčiji je to *Bundesanstalt für Finanzdienstleistungsaufsicht* oziroma BaFin.[91] Za dovoljenje za poslovanje je tako na primer že zaprosila banka Fidor. BaFinovi posegi pa niso potrebni pri »rudarjenju« bitcoinov in plačevanju z njimi.[92]

Trgovanje z bitcoini je podvrženo (običajni) obdavčitvi kapitalskih dobičkov po dohodninski zakonodaji, a le, če se prodaja zgodi v prej kot enem letu po pridobitvi bitcoinov.[93] Ker bitcoini niso zakonito plačilno sredstvo, za prihodke od njihove prodaje ne velja sicer običajna oprostitev plačila davka na dodano vrednost.[94]

4.3.9. Slovenija

Mediji so poročali, da je Banka Slovenije (BS) bitcoin že obravnavala z vidika plačilnih storitev in izdajanja elektronskega denarja ter ugotovila, da valuta po zakonu ni denarno sredstvo (torej ne spada med bankovce, kovance, knjižni denar ali elektronski denar). V BS so tudi opredelili, da trgovanje oziroma poslovanje z bitcoini ni regulirana dejavnost v okviru nadzora BS. Sheme virtualnih valut imajo nekaj podobnih značilnosti kot plačilne storitve in plačilni sistemi, zato naj bi BS razvoj te sheme spremljala tudi v prihodnje. Ker gre za neregulirano dejavnost, BS uporabnikom bitcoinov svetuje previdnost pri trgovanju in poslovanju z njimi.[95] Na svoji spletni strani je slovenska centralna banka objavila tudi že predstavljeno opozorilo EBA.

Obvestilo pravnim in fizičnim osebam, ki v Republiki Sloveniji opravljajo posle v zvezi z dejavnostjo izdajanja in upravljanja drugih plačilnih sredstev, pri katerih ne gre za plačilno storitev v skladu z zakonom, ki ureja plačilne storitve

[90] Prav tam, str. 1.
[91] Leonhardt.
[92] Nestler.
[93] Leonhardt.
[94] Prav tam, str. 2.
[95] Ugovšek.

in sisteme, pa je izdal tudi Urad za preprečevanje pranja denarja.[96] Zakon o preprečevanju pranja denarja in financiranja terorizma[97] namreč tudi zanje določa, da pri svoji dejavnosti (ki obsega tudi trgovanje z bitcoini oziroma izdajanje[98] virtualne valute) izvajajo ukrepe za poznavanje stranke,[99] sporočajo predpisane in zahtevane podatke ter uradu predložijo dokumentacijo v skladu z zakonom, imenujejo pooblaščenca in namestnike pooblaščenca ter jim omogočijo delo, skrbijo za redno strokovno usposabljanje, pripravijo seznam indikatorjev, zagotovijo varstvo in hrambo podatkov, izvajajo ukrepe odkrivanja in preprečevanja pranja denarja in financiranja terorizma v podružnicah in hčerinskih družbah v večinski lasti v tretjih državah ter izvajajo druge naloge in obveznosti, ki jih določajo ZPPDFT in na njegovi podlagi sprejeti predpisi.[100]

Bitcoinov se je dotaknila tudi Davčna uprava Republike Slovenije (DURS) in izdala pojasnilo z naslovom Davčna obravnava poslovanja z virtualno valuto po ZDOH-2 in ZDDPO-2.[101]

Ministrstvo za finance[102] (ki ga je DURS prosil za pomoč) je podobno kot Banka Slovenije pojasnilo, da virtualna valuta bitcoin ne velja za denarno sredstvo po 7. točki 4. člena ZPlaSS. Prav tako se bitcoin ne šteje za finančni instrument.[103] Jasno je torej, kaj bitcoin ni, medtem ko odgovora na vprašanje, kaj po slovenskem pravu je, še nimamo.

Davčna obravnava dohodka, doseženega pri takem trgovanju oziroma poslovanju ali v taki obliki, je po stališču DURS odvisna od okoliščin posameznega primera. Odvisna je od tega, kdo dosega dohodek in za kakšne vrste dohodek v posameznem primeru gre (dohodek iz kreiranja bitcoinov, iz kupovanja in prodajanja bitcoinov, izplačilo drugega dohodka v bitcoinih).

DURS v skladu z Zakonom o dohodnini[104] razlikuje med primerom, ko dohodek dosega fizična oseba, in primerom, ko dohodek dosega fizična oseba v okviru opravljanja dejavnosti. V skladu s 15. členom ZDoh-2 se kakršenkoli

[96] Urad RS za preprečevanje pranja denarja, str. 1.

[97] Točka 16c 4. člena ZPPDFT (Uradni list RS, št. 60/2007, s spremembami).

[98] V praksi bo sicer verjetno prišlo v poštev zgolj trgovanje z bitcoini, saj je izdajanje bitcoinov prej opisana aktivnost »rudarjenja«, ki z vidika pranja denarja ne bi smela biiti sporna.

[99] Ta ukrep je v skladu z 8. členom ZPPDFT na primer obvezen v primeru, da transakcija oziroma verjetno povezan sklop transakcij presega vrednost 15.000 evrov.

[100] Člen 5 ZPPDFT.

[101] Pojasnilo DURS, št. 4210-11634/2013, 23. 12. 2013.

[102] Ministrstvo za finance je prejelo celo pobudo uporabnika, da naj se bitcoin uvrsti med tuje valute, a jo je zavrnilo (Ministrstvo za finance).

[103] Te sicer v 7. členu opredeljuje Zakon o trgu finančnih instrumentov, Uradni list RS, št. 67/2007, s spremembami.

[104] Zakon o dohodnini (ZDoh-2), Uradni list RS, št. 13/2011 – UPB7, s spremembami.

dohodek, ki ga fizična oseba dobi izplačanega v bitcoinih, obdavči kot dohodek, prejet v naravi. To pomeni, da se dohodek preračuna v evre po tečaju, ki je veljal, ko je bil dohodek prejet.

Po 15. členu ZDoh-2 se obdavčujejo dohodki fizične osebe, pridobljeni oziroma doseženi v davčnem letu, ki je enako koledarskemu letu. Dohodki so vsi dohodki in dobički, ne glede na vrsto, če ni s tem zakonom drugače določeno. Za dohodek se šteje vsako izplačilo oziroma prejem dohodka, ne glede na obliko, v kateri je izplačan oziroma prejet. Dohodek, prejet v naravi, se določi na podlagi primerljive tržne cene, če ni z zakonom drugače določeno. Dohodek je pridobljen oziroma dosežen v davčnem letu, v katerem je prejet (razen če zakon določa drugače). Šteje se, da je dohodek prejet, ko je izplačan fizični osebi ali ji je kako drugače dan na razpolago.

Skladno z navedenim se kakršenkoli dohodek, ki je obdavčljiv v skladu s prej opisano določbo, a ga fizična oseba doseže v bitcoinih, obdavči kot dohodek, prejet v naravi. Višina dohodka v evrih se določi ob upoštevanju vrednosti bitcoina v evrih v času, ko je bil dohodek prejet.

Zanimivo je, da kapitalski dobiček, dosežen pri trgovanju z bitcoini, ni obdavčljiv. DURS je to utemeljil z določbo 32. člena ZDoh-2, da se dohodnina ne plača od dobička iz kapitala od odsvojitve premičnin (razen izjem, med katere pa bitcoin ne spada). Bitcoin po interpretaciji DURS torej spada med premičnine. Če bi to interpretacijo razširili na druga pravna področja, bi lahko sklepali, da v skladu s 15. členom SPZ[105] bitcoin pomeni stvar – obliko energije ali valovanja, ki jo človek lahko obvladuje.[106]

Dohodek, ki ga fizična oseba doseže z »rudarjenjem«, se obdavči kot drugi dohodek po 105. členu ZDoh-2. Višina dohodka v evrih se določi ob upoštevanju vrednosti bitcoina v evrih v času, ko je bil dohodek prejet.

Če fizična oseba bitcoinski dohodek ustvari pri opravljanju dejavnosti, se dobiček iz poslov trgovanja z bitcoini ali dohodek iz »rudarjenja« obdavčuje kot dohodek iz dejavnosti po določbah ZDoh-2. Za ugotavljanje prihodkov in odhodkov se sicer uporabljajo predpisi o obdavčitvi dohodkov pravnih oseb. DURS ugotavlja, da ZDDPO-2[107] nima izrecne določbe za davčno obravnavo dohodkov, povezanih s poslovanjem oziroma trgovanjem z bitcoini. Uporabljale pa naj bi se siceršnje določbe ZDDPO-2 o dobičku, ki pomeni presežek prihodkov nad odhodki. Te torej veljajo tudi za bitcoine. Računovodska obravnava naj bi bila tako odvisna od okoliščin posameznega primera.

[105] Stvarnopravni zakonik, Uradni list RS, št. 87/2002, s spremembami.

[106] Vprašanje je sicer, ali bi ta interpretacija v fizikalnem smislu zdržala.

[107] Zakon o davku od dohodkov pravnih oseb (Uradni list RS, št. 117/2006, s spremembami).

DURS bo »narudarjene« bitcoine sicer lahko zaznal le prek ugotavljanja povečanja premoženja.

V Sloveniji je nekaj časa poslovala druga največja trgovalna platforma Bitstamp,[108] pozneje pa je sedež prestavila v London. Ne glede na to bi bilo koristno vzpostaviti pravno podlago, ki bi poslovanje z bitcoini obravnavala na podoben način, kot sta to storili na primer Nemčija in Francija, kar pomeni, da bi profesionalno ukvarjanje s prodajo in nakupi bitcoinov zahtevalo posebno dovoljenje, vezano na izpolnjevanje določenih standardov.

5. Sklep

Navidezne valute so pričakovan korak v razvoju digitalnega sveta. Obstaja več oblik teh valut, kot morebitna konkurenca običajnemu denarju so zanimive zlasti t. i. navidezne valutne sheme z dvostranskimi tokovi, pri katerih je navidezno valuto mogoče po veljavnem menjalnem tečaju spreminjati v »pravi« denar, omogočajo pa nakup tako navideznih kot realnih dobrin in storitev. Po t. i. družbeni teoriji denarja, ki v pravni teoriji sicer še ni povsem nadomestila državne teorije, bi tovrstni shemi ob večjem razmahu lahko priznali status denarja. Mnogi ekonomisti (med njimi sta bila tudi Hayek in Friedman) sicer zagovarjajo že več kot stoletje staro idejo svobodnega bančništva, v skladu s katero lahko denar izdajajo zasebni subjekti, posamezne denarne oblike pa si med seboj konkurirajo. Navidezne valute v marsičem pomenijo udejanjenje te ideje, zato so blizu libertarcem.

Izdajanje in uporaba navideznih valut v večini držav nista regulirana. Prvi regulatorni posegi se nanašajo večinoma na (za zdaj) najuspešnejšo virtualno valuto – bitcoin. Ponekod ima bitcoin status zasebnega denarja, drugod status stvari, najpogosteje pa njegov status ostaja nedefiniran, znano je le, kaj bitcoin ni. Ureditev (kolikor je pač obstaja) se med državami precej razlikuje – ponekod je uporaba navideznih valut povsem prosta, drugod so za dejavnost trgovanja z bitcoini potrebna dovoljenja. Skoraj povsod pa je poslovanje z navideznimi valutami na neki način obdavčeno in zahteva izvajanje ukrepov za preprečevanje pranja denarja in financiranja terorizma.

V Sloveniji so se na pojav bitcoina odzvali Banka Slovenije, DURS in Urad za preprečevanje pranja denarja. Prva je podala stališče, da bitcoini ne spadajo med denarna sredstva in da ni pristojna za izvajanje nadzora nad njimi. DURS je pojasnila davčne obveznosti subjektov, ki poslujejo z bitcoini, UPP pa jih je

[108] https://si.bitstamp.net.

opomnil na obveznosti, ki jih imajo v skladu z Zakonom o preprečevanju pranja denarja in financiranja terorizma.

V skladu s podobno prakso v Nemčiji in Franciji bi bilo v primeru, da uporaba bitcoinov ali drugih virtualnih valut doseže večje dimenzije, koristno izvajati nadzor nad subjekti, ki se ukvarjajo z dejavnostjo trgovanja z virtualnimi valutami.

Ne glede na to, ali bodo obstoječe navidezne valute zgolj muhe enodnevnice ali pa bodo dobile trajni prostor v svetu denarja, bo njihov vpliv na razvoj denarja verjetno dolgoročnejši.

Literatura in viri

Ahtik, Meta: *Izdajanje denarja v sistemu neomejenih bank.* 2005, mimeo.

Ahtik, Meta: Monetarna suverenost in Banka Slovenije po uvedbi evra. *Zbornik znanstvenih razprav*, 2005a, let. 65, str. 29–51.

Bajt, Aleksander in Štiblar Franjo: *Ekonomija. Ekonomska analiza in politika.* Ljubljana: GV Založba, 2004.

Elwell, Craig K., Murphy, Maureen M. in Seitzinger, Michael V.: Bitcoin: Questions, Answers, and Analysis of Legal Issues. CRS Report prepared for Members and Committess of Congress, 20. 12. 2013. http://www.fas.org/sgp/crs/misc/R43339.pdf (2. 2. 2014).

Hayek, Friedrich A.: *Denationalisation of Money: The Argument Refined.* 3. izdaja. London: The Institute of Economic Affairs, 1990.

Hubbard, Glenn, R.: *Money, the Financial System and the Economy,* Reading: Addison-Wesley, 1996.

Jeong, Sarah: The Bitcoin Protocol as Law, and the Politics of a Stateless Currency. May 2013. http://ssrn.com/abstract=2294124 or http://dx.doi.org/10.2139/ssrn.2294124 (2. 2. 2014).

Kodrič, Sandi: Prihodnost denarja ali peskovnik za špekulante? *Pravna praksa,* 2013, let. 32, št. 46, str. 34.

Konda, Uroš: Kitajska centralna banka: Navadni ljudje smejo uporabljati bitcoine, *Finance,* 5. 12. 2013.

Leonhardt, Pia. Bitcoin under German law. 2013 http://www.e-comlaw.com/e-finance-and-payments-law-and-policy/hottopic.asp?id=1379 (2. 2. 2014).

Mann, Frederic Alexander: *The legal aspect of money.* Oxford: Clarendon Press, 1992.

Matonis, Jon: Why Are Libertarians Against Bitcoin?, 26. 6. 2011. http://themonetaryfuture.blogspot.de/2011/06/why-are-libertarians-against-bitcoin.html (2. 2. 2014).

Moore, Tyler in Christin, Nicolas: *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk.* Proceedings of Financial Cryptography 2013. Okinawa, 2. 4. 2013. http://fc13.ifca.ai/proc/1-2.pdf (2. 2. 2014).

Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. https://bitcoin.org/bitcoin.pdf (2. 2. 2014).

Nestler, Franz: Deutschland erkennt Bitcoins als privates Geld an. 16. 8. 2013. http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-waehrung-deutschland-erkennt-bitcoins-als-privates-geld-an-12535059.html (3. 2 . 2014).

Pohjanpalo, Kati: Bitcoin Judged Commodity in Finland After Failing Money Test. 20. 1. 2014. http://www.bloomberg.com/news/print/2014-01-19/bitcoin-becomes-commodity-in-finland-after-failing-currency-test.html (2. 2. 2014).

Proctor, Charles: *Mann on the legal aspect of money.* Oxford, New York: Oxford University Press, 2005.

Ribnikar, Ivan: Denar v obtoku in denar kot zakonito plačilno sredstvo. *Bančni vestnik,* 2005, let. 54, št. 1-2, str. 74–76.

Ribnikar, Ivan: *Monetarna ekonomija I.* Ljubljana: Ekonomska fakulteta v Ljubljani, 2003.

Rubin, Richard in Dougherty, Carter: Clear Bitcoin Tax Rules Needed, Taxpayer Advocate Says. 9. 1. 2014 http://www.bloomberg.com/news/2014-01-09/clear-bitcoin-tax-rules-needed-taxpayer-advocate-says.html (2. 2. 2014).

Schwartzkopff, Frances in Levring, Peter: Bitcoins Spark Regulatory Crackdown as Denmark Drafts Rules. 18. 12. 2013 http://www.bloomberg.com/news/2013-12-17/bitcoin-rules-drafted-in-denmark-as-regulator-warns-against-use.html (2. 2. 2014).

Selgin, George: Synthetic Commodity Money. 2013 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118 (2. 2. 2013).

Sparshot, Jeffrey: Bitcoin Exchange Makes Apparent Move to Play by U. S. Money-Laundering Rules.The Wall Street Journal, 28. 6. 2013. http://online.wsj.com/news/articles/SB10001424127887323873904578574000957464468 (2. 2. 2014).

Stranjak, Asim, Jovanovski, Tihomir, Dautbašić, Ismet in Konjhodžić Halid: Monetarne finansije i monetarno pravo, Sarajevo: »Svjetlost« OOUR Zavod za udžbenike i nastavna sredstva, 1981.

Tamburrino, Claudio: Anche l'Italia si accorge di Bitcoin. 21. 1. 2014. http://puntoinformatico.it/3977384/PI/News/anche-italia-si-accorge-bitcoin.aspx, 5. 2. 2014.

Ugovšek, Jure: Ali lahko eksplozija IT-valute bitcoin spremeni vaše poslovanje? *Finance*, 9. 4. 2013.

Yermack, David: Is Bitcoin a real currency? NBER Working Paper 19747. December 2013, http://www.nber.org/papers/w19747, 2. 2. 2014.

Zimmermann, Claus D: A Contemporary Concept of Monetary Sovereignty. Oxford: Oxford University Press, 2013.

L'Autorité de contrôle prudentiel et de résolution. Position de l'ACPR relative aux opérations sur Bitcoins en France. 29. 1. 2014, http://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/registre-officiel/201401-Position-2014-P-01-de-l-ACPR.pdf (4. 2. 2014).

Banque de France: Les dangers liés au développement des monnaies virtuelles: l'exemple du bitcoin, *Focus*, let. 2013, št. 10, http://www.banque-france.fr/fileadmin/user_upload/banque_de_france/publications/Focus-10-stabilite-financiere.pdf (4. 2. 2014).

BIS. Innovations in retail payments. Report of the Working Group on Innovations in Retail Payments. May 2012, http://www.bis.org/publ/cpss102.pdf (2. 2. 2014).

Bloomberg news. China Bans Financial Companies From Bitcoin Transactions. 5. 12. 2013. http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html, 2. 2. 2014.

Bundesministerium der finanz, 2013/0752711.

Crypto-Currency Market Capitalizations, http://coinmarketcap.com, 1. 2. 2014.

European Banking Authority (EBA). Opozorilo uporabnikom v zvezi navideznimi valutami, EBA/WRG/2013/01 (12. 12. 2013).

European Central Bank (ECB). Euro area monetary aggregates and their role in the Eurosystem's monetary policy strategy. Monthly Bulletin, 1999, št. 2, str. 29–46.

European Central Bank (ECB). Virtual currency schemes. 2012 www.ecb.europa.eu/pub/pdf/.../virtualcurrencyschemes201210en.pdf (2. 2. 2014).

European Commission. Euro legal tender. http://ec.europa.eu/economy_finance/euro/cash/legal_tender/index_en.htm (2. 2. 2014).

Governemnt Accountability Office (GAO). Virtual economies and currencies. Report to the Committee on Finance, U. S. Senate. May 2013. www.gao.gov/assets/660/654620.pdf (2. 2. 2014).

Guidance FIN-2013-G001 of the Financial Crimes Enforcement Network. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. 18. 3. 2013.

Interventi urgenti di avvio del piano »Destinazione Italia«, per il contenimento delle tariffe elettriche e del gas, per la riduzione dei premi RC-auto, per l'internazionalizzazione, lo sviluppo e la digitalizzazione delle imprese, nonche' misure per la realizzazione di opere pubbliche ed EXPO 2015. *Gazzetta Ufficiale,* 23 dicembre 2013, n. 145.

Ministrstvo za finance. Predlagam.vladi.si Predlog 5344-8: Bitcoin na postane uradno tuja valuta. 20. 1. 2014 http://www.predlagam.vladi.si/webroot/files/5344_PVS%205344%20MF.pdf (5. 2. 2014).

National Taxpayers Union Foundation. Intervju z Miltonom Friedmanom. 1999. http://www.youtube.com/watch?v=6MnQJFEVY7s (4. 2. 2014).

Pojasnilo DURS, št. 4210-11634/2013, 23. 12. 2013.

Securities and Exchange Commission vs. Trendon T. Shavers and Bitcoin Savings and Trust, Case No. 4:13-CV-416, 6. 8. 2013.

Urad RS za preprečevanje pranja denarja. Virtualna valuta bitcoin – obvestilo za zavezance. 22. 1. 2014. http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/dokumenti/Bitcoin_obvestilo.pdf (5. 2. 2014)

Stvarnopravni zakonik, Uradni list RS, št. 87/2002, s spremembami.

Zakon o davku od dohodkov pravnih oseb, Uradni list RS, št. 117/2006, s spremembami.

Zakon o dohodnini, Uradni list RS, št. 13/2011 – UPB7, s spremembami.

Zakon o plačilnih storitvah in sistemih, Uradni list RS, št. 58/2009, s spremembami.

Zakon o preprečevanju pranja denarja in financiranja terorizma, Uradni list RS, št. 60/2007, s spremembami.

Zakon o trgu finančnih instrumentov, Uradni list RS, št. 67/2007, s spremembami.

Pravilnik o izvajanju Zakona o davčnem postopku, Uradni list RS, št. 141/2006 s spremembami.

Pogodba o delovanju EU, UL C 83/47, 30. 3. 2010.

Uredba sveta (ES) št. 974/98 o uvedbi eura, UL L 139, 11. 5. 1998.

Direktiva 2007/64/ES Evropskega parlamenta in Sveta o plačilnih storitvah na notranjem trgu in o spremembah direktiv 97/7/ES, 2002/65/ES, 2005/60/ES in 2006/48/ES ter o razveljavitvi Direktive 97/5/ES, UL L 319/1, 5.12. 2007.

Direktiva 2009/110/ES Evropskega parlamenta in Sveta o začetku opravljanja in opravljanju dejavnosti ter nadzoru skrbnega in varnega poslovanja institucij za izdajo elektronskega denarja ter o spremembah direktiv 2009/110/ES, UL L 267/7, 10. 10. 2009.

Uporabnik mobilne naprave – žrtev ali storilec kaznivega dejanja?

dr. Sabina Zgaga, Blaž Markelj

1. Uvod

Uporaba mobilne naprave, še posebej v poslovnem okolju, je lahko relevantna tudi z vidika kazenskega prava. Na to v zadnjem času vplivajo predvsem vse večja uporaba mobilnih naprav, vse večja ogroženost teh naprav in dostopanje z mobilno napravo do vrste občutljivih podatkov, shranjenih v informacijskem sistemu organizacije.[1]

Pri presojanju kazenske odgovornosti uporabnika mobilne naprave, s katero dostopa do informacijskega sistema organizacije in do zaščitenih podatkov, pri tem pa jo uporablja na način, ki krši pravila organizacije, in s tem povzroči neupravičeno razkritje ali dostop do teh podatkov, je kot vedno treba ugotoviti, ali so izpolnjeni elementi splošnega pojma kaznivega dejanja (bit inkriminacije, protipravnost, krivda). V zvezi s tem bo treba odgovoriti tudi na vprašanja, ali se je uporabnik zavedal groženj, ki grozijo mobilni napravi, ali se je zavedal, kako in na kakšen način je dolžan ravnati z mobilno napravo, da bo njena uporaba varna, vključno z vidika podatkov, do katerih se dostopa s to mobilno napravo, ali pa podatkov, ki so že na mobilni napravi, oziroma ali je bilo varno ravnanje z mobilno napravo sploh predpisano. S tem se na dejanski ravni ugotovi obstoj kaznivega dejanja, predvsem izpolnjenost definicije kaznivega dejanja in krivde storilca.

Prispevek v prvem delu zato predstavlja vidik informacijske varnosti pri uporabi mobilnih naprav in se pri tem predvsem osredotoča na vprašanje razširjenosti uporabe mobilnih naprav, namen uporabe mobilnih naprav, poznavanje groženj informacijski varnosti mobilnih naprav in poznavanje ter uporabo ustreznih varnostnih zaščit.

V drugem, prevladujočem delu pa prispevek analizira potencialno kazensko odgovornost takega uporabnika preko splošnega pojma kaznivega dejanja in

[1] V prispevku se uporablja splošnejši izraz organizacija, ki zajema tako gospodarske družbe kot tudi druge pravne osebe javnega in zasebnega prava, pa tudi fizične osebe, ki opravljajo določeno dejavnost in imajo s tem namenom vzpostavljen informacijski sistem.

njegovih elementov. S tega vidika predstavlja relevantna kazniva dejanja, odnos med njimi, predpisano dolžnostno ravnanje glede varne uporabe mobilne naprave, presojo uporabnikove krivde glede neupravičenega razkritja ali dostopa do podatkov in relevantnost potencialne pravne zmote uporabnika glede dovoljenosti določenih načinov uporabe naprave. Prav presoja oblik krivde in obstoja ustreznih zmot bosta bistveni za iskanje odgovora na vprašanje, ali je uporabnik žrtev ali storilec kaznivega dejanja.

2. Informacijsko varnostni vidik

Informacijska tehnologija je postala nepogrešljiv element našega življenja. Omogoča nam, da opravimo stvari hitreje in bolj učinkovito. Z vedno hitrejšim tempom življenja je prišla namreč tudi potreba po hitrem, neprestanem dostopu v kibernetski svet, kar nam omogočajo vedno naprednejše informacijske rešitve. Priča smo vedno večji razširjenosti spleta in posledično raznovrstnih naprav, ki omogočajo povezavo vanj. Za dostopanje do spleta smo v preteklosti uporabljali preproste računalnike, ki jih v današnjem času čedalje pogosteje nadomeščajo mobilne naprave.

Med mobilne naprave uvrščamo predvsem naprave, ki imajo prilagojen operacijski sistem, kot so iOS, Android, BlackBerry OS, Windows mobile, in so prenosljive (mobilni telefoni, tablični računalniki, itd.). V to kategorijo se lahko uvrsti vse naprave, ki se lahko prenašajo in pri katerih je dostop v internet mogoč brez fizične povezave (tudi prenosniki, prenosne igralne konzole, industrijski čitalci, itd.), medtem ko v skupino mobilnih telefonov sodijo tako mobilni telefoni, ki so namenjeni zgolj klicanju in pisanju kratkih sporočil, kot tudi pametni mobilni telefoni, ki predstavljajo sodobno komunikacijsko napravo, saj poleg klicanja preko mobilnih omrežij omogočajo še kopico dodatnih funkcij, ki so podobne funkcijam osebnega računalnika.

Po raziskavi Microstoft Tag (2011) naj bi do leta 2014 mobilni dostopi do interneta prehiteli dostope, opravljene prek namiznih računalnikov.[2] Slovenija tukaj ne zaostaja, ravno nasprotno. Po raziskavi CEE Telco Industry Report (2011), ki je zajela 15 držav Srednje in Vzhodne Evrope, je Slovenija po uporabi pametnih mobilnih telefonov v samem vrhu, saj 27,8 odstotka uporabnikov mobilne telefonije uporablja pametni mobilni telefon.[3]

[2] Microsoft Tag. *Infographic: MobileStatistics, Stats&Facts 2011,* http://www.digitalbuzzblog.com/2011-mobile-statistics-stats-facts-marketing-infographic/ (2. 2. 2013).

[3] GfK Group. *CEE Telco Industry Report 2011,* http://www.gfk.com/group/press_information/press_releases/008894/index.en.html (6. 6. 2013).

Hkrati s povečanjem uporabe mobilnih naprav pa je treba opozoriti tudi na obstoj ter zavedanje glede groženj in posledic, ki pretijo uporabnikom mobilnih naprav. Mobilna naprava je namreč lahko tarča delčkov programske opreme, ki se namestijo nanjo s pomočjo programskih oprem *malware*, *spyware* in *botnet* ali s povezavo *bluetooth* in sodelovanjem v socialnih omrežjih.[4] Rezultati raziskav kažejo, da se je v zadnjih šestih mesecih leta 2011 zelo povečalo število groženj, temelječih na aplikacijah programa *malware*, predvsem v primerjavi s programi *spyware*.[5] Obstaja verjetnost, da se pri nalaganju programske opreme »okuži« od 1 do 4 odstotki mobilnih naprav. Poročilo, ki ga je izdelalo podjetje Juniper (2011), navaja, da se je od poletja 2010 naprej število mobilnih naprav, ki delujejo na platformi Android in so se okužile s programi *malware*, povečalo za 400 odstotkov.[6] V poročilu lahko tudi preberemo, da ima kar 85 odstotkov uporabnikov na svojem mobilnem telefonu neuporabno zaščito. Nepoznavanje programske opreme in vseh zmožnosti, ki jih programska oprema mobilne naprave omogoča, pa lahko uporabnike mobilnih naprav pripelje tudi v položaj, ko z uporabo mobilne naprave izvršijo zakonske znake kaznivih dejanj.

Tudi poročilo Treat Assessment, ki ga je izdal Europol (2011), kot eno od možnosti naraščajočih priložnosti kibernetskega kriminala navaja mobilnost podatkov,[7] kar lahko razumemo tudi kot uporabo mobilnih naprav, saj so le-te vedno bolj razširjene, ravno tako pa jih je zaradi njihove neprestane mobilnosti težje nadzorovati in varovati.

V mesecu decembru 2011 je bila med študenti narejena raziskava z naslovom »Zavedanje groženj mobilnim napravam«. Namen raziskave je bil ugotoviti, koliko se mladi zavedajo nevarnosti oziroma groženj, ki jim pretijo, in kakšne varnostne rešitve že uporabljajo. Zanimiva je ugotovitev, da mladi, kljub poznavanju številnih nevarnosti, še vedno ne verjamejo, da se lahko grožnja zgodi tudi njim. To posledično pomeni, da vsakršno nevarnost zavestno zanemarijo. Cilji raziskave so bili pridobiti podatke o namenu, načinu in vrsti uporabe mobilnih naprav ter posledično o poznavanju načina uporabe, groženj in zaščit. S stališča poznavanja groženj in varnega upravljanja z mobilnimi napravami lahko sklepamo tudi na uporabnikovo dovzetnost in poznavanje kibernetske kriminalitete.

---

[4] Leavitt, Neal. *Mobile Security: Finally a Serious Problem?,* Largo: University of Maryland, 2011, http://www.computer.org/portal/web/computingnow (7. 9. 2013).

[5] Lookout. *Lookout Mobile Threat Report,* https://www.mylookout.com/mobile-threat-report (10. 9. 2013).

[6] Juniper Networks. *Malicious Mobile Threats Report 2010/2011,* http://www.juniper.net/us/en/dm/interop/go (10. 9. 2013).

[7] Europol. *Organised Crime Threat Assessment,* https://www.europol.europa.eu/content/press/europol-organised-crime-threat-assessment-2011-429 (6. 12. 2013).

Raziskava je bila narejena s pomočjo spletnega vprašalnika, ki je bil objavljen na spletnem portalu »1ka« (www.1ka.si). Vprašalnik je sestavljen tako, da je mogoče ugotoviti, kdo in s kakšnim namenom uporablja mobilne naprave in katere vrste mobilnih naprav ter programskih rešitev so mu ljubše. V drugem delu vprašalnika pa so vprašanja postavljena tako, da iz rezultatov dobimo vpogled v uporabnikovo poznavanje in uporabo varnostnih rešitev ter poznavanje in zavedanje groženj, ki pretijo ob uporabi mobilnih naprav.

Iz rezultatov raziskave je razvidno, da je največji odstotek tistih, ki istočasno uporabljajo klasični mobilni telefon (ti danes v veliki meri tudi omogočajo povezavo v splet) ter prenosni računalnik oziroma da so vprašani veliki uporabniki ne samo ene, ampak več mobilnih naprav hkrati.

Pomemben je tudi namen uporabe mobilne naprave. Več kot polovica vprašanih uporablja mobilne naprave v zasebne namene, medtem ko je četrtina takih, ki mobilne naprave uporablja sočasno tako v zasebne kot tudi v službene namene. Podatki so skoraj pričakovani, glede na populacijsko strukturo vprašanih (študentje). Vsekakor pa je skrb vzbujajoče dejstvo, da je še vedno dokaj visok odstotek tistih, ki uporabljajo mobilne naprave za zasebne in službene potrebe, še posebno če je to ista mobilna naprava. Problem nastane, ko s kombinirano zasebno in službeno rabo mobilne naprave ne usklajujemo zadostno tudi z zagotavljanjem ustrezne stopnje informacijske varnosti.

Predpogoj zavedanja potrebe po zagotavljanju zadostne stopnje informacijske varnosti pri uporabi mobilnih naprav pa je zagotovo poznavanje in zavedanje glede groženj, ki pretijo uporabnikom mobilnih naprav. Ni presenetljivo, da rezultati raziskave kažejo, da je kraja med vsemi naštetimi grožnjami na prvem mestu s skoraj 90 odstotki. Vsekakor pa je presenetljivo in skrb vzbujajoče, da so grožnje, kot na primer *malware* in *spyware* ter okužbe z *rootkitom,* zelo slabo znane med vprašanimi, predvsem upoštevajoč dejstvo, da raziskave opozarjajo na veliko povečanje možnosti tovrstnih okužb.[8]

Na podlagi poznavanja groženj se uporabnik lahko odloči za ustrezno zaščito svoje mobilne naprave. Raziskava je pokazala, da uporabniki mobilnih naprav največ uporabljajo PIN-kodo za SIM-kartico, kar je tudi pričakovano. Tako varnostno rešitev vgradi v SIM-kartico že mobilni operater. Skrb vzbujajoče pa je dejstvo, da zelo veliko vprašanih pozna varnostno PIN-kodo za dostop do posameznih aplikacij na pametnem telefonu, vendar je ne uporablja, čeprav pametni mobilni telefoni to že samodejno omogočajo. Kot varnostno rešitev obravnavamo tudi oddaljeno brisanje vsebine mobilnega pametnega telefona. To rešitev lahko uporabimo v primeru izgube ali kraje mobilnega pametnega telefona. Vendar

[8] Kot sta že omenjeni raziskavi Lookout in Juniper, obe iz leta 2011.

samo 40 odstotkov vprašanih to varnostno rešitev pozna, pa še ti je kljub temu ne uporabljajo, 52 odstotkov vprašanih pa te varnostne rešitve sploh ne pozna.

Opravljena raziskava torej prikazuje realno stanje zavedanja glede groženj in možnih zaščit uporabe mobilnih naprav pri določeni skupini uporabnikov mobilnih naprav, kar predstavlja izhodišče za kazenskopravno analizo.

3. Kazenskopravni vidik kibernetskih groženj in posledic

3.1. Uporabnik mobilne naprave – žrtev ali storilec kaznivega dejanja?

Zaradi neskrbne uporabe mobilne naprave je lahko zoper njenega uporabnika v določenih primerih sprožen tudi kazenski postopek. Zaradi nezavedanja glede groženj in/ali neuporabe ustreznih oblik zaščite mobilne naprave je le-ta namreč lahko zlorabljena za neupravičeno pridobitev ali odtujitev podatkov, ki se hranijo na tej ali drugi mobilni napravi ali drugje v informacijskem sistemu, do katerega dostopa uporabnik preko svoje mobilne naprave. Situacija je posebej varnostno občutljiva takrat, kadar uporabnik s svojo mobilno napravo dostopa do informacijskega sistema organizacije, ki ima dostop do občutljivih podatkov, za katere zakonodaja določa, da imajo status določene vrste podatkov. Odtujitev podatka ali njegovo neupravičeno razkritje, če je tak podatek mogoče opredeliti kot osebni ali tajni podatek, poklicno ali poslovno skrivnost, je v skladu s Kazenskim zakonikom (KZ-1)[9] tako lahko kaznivo dejanje.[10]

Poleg tega KZ-1 opredeljuje še dve relevantni kaznivi dejanji, pri katerih pa zavarovana dobrina ni varovanje tajnosti določenih vrst podatkov, ampak nedotakljivost informacijskega sistema[11] (napad na informacijski sistem)[12] oziroma področja gospodarskega poslovanja (zloraba informacijskega sistema).[13] Odvisno od naklepa uporabnika mobilne naprave oziroma potencialnega storilca kaznivega dejanja pa bi bila lahko relevantna tudi druga kazniva dejanja, kot je na primer tatvina,[14] poneverba in neupravičena uporaba tujega premoženja,[15] izsiljevanje,[16] terorizem[17] itd.

[9] Uradni list RS, št. 50/2012 – UPB2.
[10] Glej 142., 143., 236. in 260. člen KZ-1.
[11] Predlog Kazenskega zakonika (KZ-1), EVA 2007-2011, str. 175.
[12] Člen 221 KZ-1.
[13] Predlog novele KZ-1B, EVA 2010-2011-0006, str. 11; 237. člen KZ-1.
[14] Člen 204 KZ-1.
[15] Člen 209 KZ-1.
[16] Člen 213 KZ-1.
[17] Člen 108 KZ-1.

Uporabnika mobilne naprave lahko v takem primeru štejemo bodisi za žrtev kaznivega dejanja bodisi za njegovega storilca. V primeru, ko pride »le« do odtujitve uporabnikove mobilne naprave ali pa do odtujitve podatkov, ki se nahajajo na tej mobilni napravi, in gre za podatke, ki se nanašajo le na uporabnika mobilne naprave, je uporabnik mobilne naprave le žrtev kaznivega dejanja.

Ko pa odtujitev uporabnikove mobilne naprave ali podatkov na njej poseže tudi v pravice[18] in dobrine drugih oseb, saj gre za podatke, ki se nanašajo tudi na druge osebe, in ne le na uporabnika, za podatke, ki jih je uporabnik dolžan varovati, ali pa za podatke, na podlagi katerih je mogoče priti do podatkov, ki se nanašajo na druge posameznike in jih je uporabnik dolžan varovati, ali pa tretja oseba s pomočjo uporabnikove mobilne naprave vdre oziroma neupravičeno vstopi v druge mobilne naprave ali druge dele informacijskega sistema organizacije, postane relevantno tudi vprašanje, ali je mogoče uporabnika mobilne naprave šteti tudi za storilca relevantnega kaznivega dejanja. Na to vprašanje je mogoče odgovoriti le z obravnavo vseh elementov splošnega pojma kaznivega dejanja v skladu s KZ-1.

3.2. Pojem informacijskega sistema in mobilne naprave z vidika slovenske kazenske zakonodaje

KZ-1 (in pred njim tudi že Kazenski zakonik – KZ po noveli iz leta 2004[19]) uporablja v zvezi z določenimi kaznivimi dejanji zakonski znak informacijski sistem. Za subsumpcijo ravnanja uporabnika mobilne naprave pod kaznivi dejanji iz 221. (napad na informacijski sistem) in 237. člena KZ-1 (zloraba informacijskega sistema) je nujen predpogoj sklep, da zakonski znak informacijski sistem pokriva tudi mobilno napravo.

Zgodovinska primerjava ustreznih različic 225. člena KZ,[20] ki ustreza sedanjemu 221. členu KZ-1, kaže na postopno širjenje zakonskega znaka, ki opredeljuje varstveni objekt oziroma predmet napada v konkretnem primeru. V skladu s KZ iz leta 1995 tako to kaznivo dejanje ščiti le podatke ali programe, namenjene za računalniško obdelavo ali uporabo, naslednja različica iz leta 1999 (KZ-A)[21] upo-

[18] Na primer pravica do zasebnosti, ki jo z več vidikov varuje tudi Ustava Republike Slovenije (Uradni list RS, št. 33/1991-I, 42/1997, 66/2000, 24/2003, 69/2004, 68/2006 in 47/2013), predvsem relevanten pa je 37. člen, ki ureja komunikacijsko zasebnost.

[19] KZ-B, Uradni list RS, št. 95/2004 – UPB1.

[20] Pojavljajo se tudi različna poimenovanja tega kaznivega dejanja: poškodovanje računalniških podatkov in programov po KZ (Uradni list RS, št. 63/1994), neupravičen vstop v zaščiteno računalniško bazo podatkov po KZ-A (Uradni list RS, št. 23/1999) in neupravičen vstop v informacijski sistem po KZ-B (Uradni list RS, št. 40/2004).

[21] Uradni list RS, št. 23/1999.

rablja že širši zakonski znak zaščitena računalniška baza podatkov in šele različica iz leta 2004 (KZ-B)[22] vsebuje najširši zakonski znak do zdaj; informacijski sistem. S tem se je KZ odmaknil od računalnika kot edinega možnega tehničnega nosilca podatkov, ki je zaščiten s tem kaznivim dejanjem in proti kateremu je mogoče izvršiti to kaznivo dejanje.[23]

Vlada se je kot predlagatelj sprememb v predlogu KZ-B sklicevala na Konvencijo Sveta Evrope o kaznivih dejanjih v kibernetskem prostoru,[24] ki uporablja izraz računalniški sistem. Ta naj bi predstavljal vsako napravo ali skupino med seboj povezanih ali soodvisnih naprav, od katerih ena ali več samodejno obdeluje podatke s pomočjo programa.[25] Čeprav je samo poimenovanje iz konvencije z današnjega vidika ozko (*računalniški* sistem), pa je njegova vsebinska opredelitev dovolj široka in ustreza današnji, saj govori splošneje o napravah, in ne zgolj računalnikih. Dotedanji zakonski znak v KZ (tj. zaščitena računalniška baza podatkov) tako ni ustrezal temu zakonskemu znaku in njegovi opredelitvi iz konvencije Sveta Evrope, zato je vlada predlagala razširitev ustreznega zakonskega znaka v KZ iz zaščitene računalniške baze podatkov v informacijski sistem, ki se primerno uporablja tudi v 221. členu KZ-1.

Podobno je potekal razvoj 237. člena KZ-1 (zloraba informacijskega sistema), kjer je ustrezno kaznivo dejanje v KZ najprej vsebovalo zakonske znake računalniški podatek, program oziroma računalniški sistem,[26] nato pa od leta 2004 naprej ustrezni širši zakonski znak informacijski sistem. Enako velja za 237. člen KZ-1. To kaznivo dejanje sicer ureja t. i. gospodarsko špijonažo,[27] kar zoži možnost njegove uporabe v praksi. Gre namreč za kaznivo dejanje zoper gospodarstvo, kar pomeni, da je treba dokazati, da je prišlo do izvršitve tega kaznivega dejanja v okviru gospodarske dejavnosti, kakor jo definira 99. člen KZ-1.[28]

---

[22] Uradni list RS, št. 95/2004.

[23] Več o tem Završnik, str. 248 in naslednje.

[24] Angl. ETS 185 – *Council of Europe Convention on Cybercrime*, podpisana v Budimpešti 23. 11. 2001.

[25] Alineja a prvega odstavka 1. člena Konvencije Sveta Evrope o kaznivih dejanjih v kibernetskem prostoru.

[26] Člen 242 KZ: vdor v računalniški sistem.

[27] Predlog Kazenskega zakonika (KZ-1), EVA 2007-2011, str. 177.

[28] Vsaka dejavnost, ki se opravlja proti plačilu na trgu, in vsaka dejavnost, ki se za dogovorjeno ali predpisano plačilo opravlja poklicno ali organizirano. Za opravljanje gospodarske dejavnosti oziroma gospodarsko poslovanje po KZ-1 se štejejo tudi izvajanje, upravljanje, odločanje, zastopanje, vodenje in nadziranje v okviru gospodarske dejavnosti ter upravljanje nepremičnin, premičnin, denarnih sredstev, dohodkov, terjatev, kapitalskih naložb, drugih oblik finančnega premoženja ter drugih sredstev pravnih oseb javnega ali zasebnega prava, razpolaganje s temi sredstvi in nadzorstvo nad njimi. Glej deseti in enajsti odstavek 99. člena KZ-1.

Vsebina in zgodovinska širitev relevantnega zakonskega znaka kaznivih dejanj iz 221. in 237. člena KZ-1 sta relevantni zato, ker uporabniku mobilne naprave ne moremo očitati teh kaznivih dejanj, če mobilne naprave, ki je bila zlorabljena ali uporabljena za izvršitev kaznivega dejanja, ne moremo subsumirati pod zakonski znak informacijski sistem.

Če informacijski sistem na podlagi pravil informacijske vede in mednarodnih pogodb razumemo kot skup strojne in programske opreme, ki omogoča učinkovit način za zbiranje, shranjevanje, obdelavo, urejanje, upravljanje, iskanje in prikaz podatkov,[29] potem je mobilna naprava del informacijskega sistema določene pravne ali fizične osebe. Hkrati jo lahko razumemo tudi kot celovit in samostojen informacijski sistem, saj vsebuje tako strojno kot tudi programsko opremo za shranjevanje, obdelavo, urejanje, upravljanje, iskanje in prikaz podatkov. Del informacijskega sistema delodajalca ali druge organizacije je na primer mobilna naprava, ki jo uporabnik dobi od organizacije v službene namene in jo tudi uporablja. Vsak uporabnik pa lahko mobilno napravo uporablja tudi kot samostojni informacijski sistem, saj ima na njej shranjene določene službene ali zasebne podatke in jo s tem namenom tudi uporablja.

Po drugi strani za odgovornost za ustrezna kazniva dejanja neupravičene pridobitve in/ali razkritja določenih vrst podatkov (osebni, tajni podatek, poslovna ali poklicna skrivnost) ni relevantna vrsta nosilca podatkov, saj KZ-1 ne določa, na kakšnem nosilcu oziroma kje se mora tak podatek nahajati, da gre za določeno vrsto podatka. Nasprotno – pomembna je njegova vsebina. KZ-1 tako našteva le vrste podatkov in ravnanje, ki predstavlja izvršitveno ravnanje kaznivega dejanja. Pri določenih kaznivih dejanjih KZ-1 opredeljuje tudi samo vsebino podatka, pri večini pa vsebino oziroma opredelitev določene zaščitene vrste podatkov prepušča področni zakonodaji, pri tem pa vrsta nosilca podatkov ni relevantna niti po KZ-1 niti po področni zakonodaji. Relevanten zaščiten podatek se tako lahko nahaja tudi na mobilni napravi, pomembno je le, da gre za določeno vrsto oziroma vsebino podatka. KZ-1 tako v skladu s tem določa kaznivo dejanje izdaje in neupravičene pridobitve poslovne skrivnosti,[30] izdajo tajnih podatkov,[31] neupravičeno izdajo poklicne skrivnosti[32] in zlorabo osebnih podatkov.[33]

Ker lahko določen podatek subsumiramo pod več vrst zaščitenih podatkov, bi na ravni biti inkriminacije storilec lahko odgovarjal za več kaznivih dejanj

[29] http://www.lkn.fe.uni-lj.si/gradiva/IS_VS/Informacijski%20sistemi%2002%20-%20Infrastruktura%20-%20Strojna%20oprema.pdf (27. 3. 2013).

[30] Člen 236 KZ-1.

[31] Člen 260 KZ-1.

[32] Člen 142 KZ-1.

[33] Člen 143 KZ-1.

neupravičenega dostopa in/ali razkritja zaščitenih podatkov, kar odpira vprašanje stekov[34] med temi kaznivimi dejanji, predvsem vprašanje, ali storilec odgovarja za vsa kazniva dejanja (pravi stek) ali pa katero kaznivo dejanje izgubi samostojnost (navidezni stek).[35] Kaznivo dejanje neupravičene izdaje poklicne skrivnosti je tako splošno kaznivo dejanje, da po našem mnenju v primeru, če gre za razkritje podatka, ki je hkrati poklicna skrivnost in poslovna skrivnost ali tajni podatek, storilec odgovarja za specialno kaznivo dejanje izdaje poslovne skrivnosti ali tajnega podatka,[36] in ne pa tudi za izdajo poklicne skrivnosti.[37] Razmerje med podatki tako določa tudi razmerje med kaznivimi dejanji, pri tem pa je treba seveda upoštevati tudi težo kaznivega dejanja in odnos konsumpcije, v skladu s katero je treba presoditi, ali je z določeno definicijo kaznivega dejanja pokrito celotno nepravo ravnanja.[38]

3.3. Izvršitveno ravnanje in protipravnost uporabnikovega ravnanja

Vsako kaznivo dejanje je sestavljeno iz treh elementov, ki morajo biti podani v vsakem primeru, da lahko govorimo o kazenski odgovornosti; ravnanje, ki izpolnjuje bit inkriminacije (tj. ravnanje storilca, ki izpolnjuje vse zakonske znake kaznivega dejanja), protipravnost ravnanja in storilčeva krivda.[39]

Najpomembneje je, definicija katerega kaznivega dejanja je relevantna zaradi neskrbnega ravnanja z mobilno napravo in do katerih podatkov se s to napravo dostopa. Skoraj vsa omenjena kazniva dejanja neupravičenega dostopa in/ali razkritja določene vrste podatkov vsebujejo zakonski znak, ki opredeljuje dispozicijo teh kaznivih dejanj kot blanketno. Za blanketno dispozicijo kaznivega dejanja gre namreč takrat, ko zakonodajalec ne opredeli natančno vseh zakonskih znakov kaznivega dejanja že v kazenskem zakonu, ampak prepusti opredelitev posameznega zakonskega znaka področni zakonodaji ali drugim predpisom.[40]

KZ-1 tako v povezavi z omenjenimi kaznivimi dejanji največkrat uporablja zakonski znak »neupravičeno«,[41] »v nasprotju s svojimi dolžnostmi«[42] in podobno. Kadar gre torej za neupravičen dostop ali razkritje oziroma za dostop ali razkritje v nasprotju z dolžnostmi storilca, imamo potencialno opravka s kaznivim

[34] Bavcon in drugi, str. 210.
[35] Prav tam, str. 210.
[36] Deisinger, str. 146.
[37] Prav tam, str. 146.
[38] Bavcon in drugi, str. 213. Glej tudi Markelj, Zgaga, str. 95.
[39] Bavcon in drugi, str. 152.
[40] Prav tam, str. 193.
[41] Člen 142 KZ-1.
[42] Člen 260 KZ-1.

dejanjem. Tako sam KZ-1 spet ne določa, kdaj je razkritje ali pridobitev podatkov neupravičena in na kakšen način je posameznik dolžan ravnati, da zaščiti podatke, do katerih ima dostop in ki jih je dolžan varovati, vključno s podatki, ki jih ima na mobilni napravi ali do katerih dostopa s pomočjo mobilne naprave, ki je del informacijskega sistema organizacije. Vse to je ali naj bi vsaj bilo določeno s področnimi predpisi in/ali notranjimi akti organizacije, ki ji pripada informacijski sistem, do katerega dostopa mobilna naprava.

Tako KZ-1 na primer ne določa, kako mora biti varovana poslovna skrivnost in kdo jo je dolžan varovati. To določi gospodarska družba s sklepom, s katerim tudi določi, kateri podatek sploh je poslovna skrivnost. V tem sklepu bi morala družba urediti tudi vidik informacijske varnosti, vključno z mobilnimi napravami, ki jih uporabljajo tisti posamezniki, ki so upravičeni do poznavanja poslovne skrivnosti in z njimi dostopajo do tega podatka (tudi) preko mobilne naprave. KZ-1 pa določa, kaj je poslovna skrivnost, in sicer vse listine in podatki, ki so z zakonom, statutom, pravili ali drugim splošnim aktom ali odredbo pristojnega organa ali druge upravičene osebe razglašeni za industrijsko, bančno ali drugo poslovno skrivnost in so tako pomembni, da so z njihovo izdajo očitno nastale ali bi lahko nastale hujše škodljive posledice.[43]

Zakon o tajnih podatkih[44] in številni podzakonski predpisi določajo, kaj je tajen podatek in na kakšen način ga morajo osebe, ki imajo dostop do teh podatkov, varovati.[45] Tajni podatek je tako opredeljen kot dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, sisteme, naprave, projekte in načrte, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije, znanstvene, raziskovalne, tehnološke, gospodarske in finančne zadeve, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije, ki ga je treba zaradi razlogov, določenih v tem zakonu, zavarovati pred nepoklicanimi osebami in ki je v skladu s tem zakonom določeno in označeno za tajno. Bistveno je torej, da je podatek določen za tajnega s strani pooblaščene osebe, ker je tako pomemben, da bi z njegovim razkritjem nepoklicani osebi nastale ali bi očitno lahko nastale škodljive posledice za varnost države ali za njene politične ali gospodarske koristi.[46]

---

[43] Peti odstavek 236. člena KZ-1. Pred tem se je KZ skliceval na ureditev Zakona o gospodarskih družbah.

[44] Uradni list RS, št. 50/2006 – UPB2, 9/2010 in 60/2011.

[45] Na primer Uredba o varovanju tajnih podatkov, Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih itd.

[46] Členi 2, 10, 11 Zakona o tajnih podatkih.

Vsaka organizacija mora vnaprej sprejeti predpise, ki urejajo ustrezne sisteme in postopke varovanja tajnih podatkov, ki ustrezajo določeni stopnji tajnosti, in onemogočajo njihovo razkritje nepoklicanim osebam.[47] Posebej relevanten predpis za mobilne naprave je Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih,[48] ki ureja vidik informacijsko-komunikacijske varnosti tajnih podatkov, kamor zagotovo spada tudi mobilna naprava in dostopanje do podatkov preko nje. Uredba ureja fizične, organizacijske in tehnične ukrepe ter postopke varovanja tajnih podatkov, katerih namen je, da se vzpostavi sistem minimalnih standardov, postopkov in tehničnih ukrepov, ki ustreza stopnji tajnosti tajnih podatkov v komunikacijskih in informacijskih sistemih ter onemogoča njihovo razkritje nepooblaščenim osebam.[49]

Način varovanja poklicne skrivnosti, ki jo KZ-1 opredeljuje kot podatek, ki ga oseba pridobi pri opravljanju poklica,[50] prav tako ni določen v KZ-1, ampak v področnih predpisih, ki urejajo določene poklice. V zdravstvu na primer dolžnost in način varovanja poklicne skrivnosti določajo številni predpisi,[51] vključno z Zakonom o zdravstveni dejavnosti (ZZDej),[52] v skladu s katerim so zdravstveni delavci in zdravstveni sodelavci ter osebe, ki so jim podatki dosegljivi zaradi narave dela, dolžni varovati kot poklicno skrivnost podatke o zdravstvenem stanju posameznika in o vzrokih, okoliščinah in posledicah tega stanja,[53] pri tem pa se zakon tudi ne omejuje na določeno vrsto nosilca podatkov.

In ne nazadnje, Zakon o varstvu osebnih podatkov (ZVOP-1)[54] ureja način varovanja osebnih podatkov. Osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ki je določena ali določljiva fizična oseba, fizična oseba pa je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa ne glede na obliko, v kateri je izražen.[55] ZVOP-1 tudi določa, da so upravljavci osebnih podatkov in pogodbeni obdelovalci dolžni zagotoviti zavarovanje osebnih podatkov ter v svojih aktih

[47] Člena 38 in 40 Zakona o tajnih podatkih.

[48] Uradni list RS, št. 48/2007 in 86/2011.

[49] Prvi odstavek 2. člena Uredbe o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih.

[50] Člen 142 KZ-1.

[51] Glej na primer Korošec, str. 61.

[52] Uradni list RS, št. 23/2005 – UPB2, 15/2008, 23/2008, 58/2008, 77/2008, 40/2012, 14/2013.

[53] Člen 51 ZZDej.

[54] Uradni list RS, št. 86/2004, 113/2005 – ZInfP, 51/2007 – ZUstS-A in 67/2007.

[55] Člen 6 ZVOP-1.

predpisati postopke in ukrepe za zavarovanje osebnih podatkov in določiti osebe, ki so odgovorne za določene zbirke osebnih podatkov, ter osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke.[56] Ti akti morajo zajemati tudi vidik informacijske varnosti, vključno z zaščito osebnih podatkov na mobilnih napravah, saj ZVOP-1 določa, da je osebni podatek katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen,[57] tako da ta opredelitev pokriva tudi podatke na mobilni napravi.

Na normativni ravni torej zakon, drug predpis ali akt organizacije predpiše, na kakšen način morajo posamezniki, ki imajo dostop do določene vrste podatka in so ga zato dolžni tudi varovati, ravnati, da podatka ne razkrijejo. To velja tudi za dolžnost varovanja podatkov pri uporabi mobilnih naprav, na katerih so taki podatki ali s katerimi se dostopa do takih podatkov. To vključuje uporabo določenih kanalov komuniciranja, protivirusnih programov, gesel in drugih šifrirnih ključev, nezaklenjenih oziroma nezavarovanih brezžičnih omrežij itd., kar pač organizacija v skladu s področnimi predpisi določi v svojih notranjih aktih kot zavezujoč standard varovanja podatkov, do katerih se dostopa z mobilno napravo.

Dolžnostno ravnanje glede skrbnega varovanja podatkov, ki ga določajo zavezujoči področni predpisi ali akti organizacije, je tako opredeljeno v obliki standardov skrbnosti ali zavezujočih pravil ravnanja in upravljanja z informacijskim sistemom na splošno in mobilno napravo posebej. Zavezujoči predpisi po uveljavitvi veljajo za vse naslovnike predpisa (splošni in abstraktni pravni akti).[58]

Tudi za pravne akte o načinih zaščite in varovanja podatkov, ki jih sprejme sama organizacija, velja, da so splošni in da veljajo za vse potencialne naslovnike akta. Kadar so ti akti zavezujoči, gre v skladu z delovnopravno zakonodajo (Zakon o delovnih razmerjih, ZDR-1)[59] za splošne akte delodajalca, s katerimi lahko delodajalec določa organizacijo dela ali določa obveznosti, ki jih morajo delavci poznati zaradi izpolnjevanja pogodbenih in drugih obveznosti.[60] Delodajalec mora tako pred sklenitvijo pogodbe o zaposlitvi kandidata seznaniti z delom, pogoji dela ter pravicami in obveznostmi delavca in delodajalca, ki so povezane z opravljanjem dela, za katero se sklepa pogodba o zaposlitvi.[61] Posledično mora delavec upoštevati zahteve in navodila delodajalca v zvezi z izpolnjevanjem pogodbenih in drugih obveznosti iz delovnega razmerja, med katere lahko sodi-

[56] Člen 25 ZVOP-1.

[57] Prvi odstavek 6. člena ZVOP-1.

[58] Pavčnik, str. 198.

[59] Uradni list RS, št. 21/2013 in 78/2013.

[60] Člen 10 ZDR-1.

[61] Sedmi odstavek 28. člena ZDR-1.

jo tudi pravila o pravilnem ravnanju z mobilnimi napravami v informacijskem sistemu delodajalca oziroma organizacije.[62]

Kadar torej delodajalec, ki ima organiziran informacijski sistem, katerega del je tudi uporabnikova (službena ali zasebna) mobilna naprava, določi način varovanja podatkov v tem informacijskem sistemu s pravno zavezujočim pravnim aktom, kršitev tega pravnega akta pomeni, da uporabnik ravna »neupravičeno« oziroma »v nasprotju s svojo dolžnostjo varovati podatek«. S tem je uporabnik izpolnil bit inkriminacije relevantnega kaznivega dejanja iz KZ-1. Organizacija lahko določi enako dolžnost tudi za druge posameznike – uporabnike mobilnih naprav, s katerimi organizacija sodeluje na drugih pravnih podlagah, in ne nujno na podlagi delovnega razmerja.[63]

Ti predpisi tako določajo raven skrbnosti, ki jo uporabnik mobilne naprave mora upoštevati pri uporabi mobilne naprave. Če uporabnik ravna v skladu s temi predpisi, je pravilno varoval določene podatke. V nasprotnem primeru gre za kršitev dolžnostnega ravnanja oziroma za pravno kršitev, ki ji lahko sledijo različne negativne posledice. Ravnanje, ki je kršitev dolžnosti varovanja podatka na način, kot ga predpisujejo splošni predpisi in/ali organizacija sama, v skrajnem primeru lahko predstavlja izvršitveno ravnanje ustreznega kaznivega dejanja iz KZ-1, hkrati pa tudi podlago za civilnopravno (odškodninsko) tožbo, disciplinsko ukrepanje ali celo prekrškovni postopek[64] zoper uporabnika mobilne naprave.

Pri vsakem izvršitvenem ravnanju mora biti podana ne le določena uporabnikova storitev ali opustitev, ki predstavlja kršitev dolžnostnega ravnanja, ampak tudi prepovedana posledica, kakršno predvideva relevantna definicija kaznivega dejanja iz KZ-1, in vzročna zveza med njima.[65] Prepovedana posledica, ki nastane z neupoštevanjem pravil o pravilnem varovanju podatkov v konkretnem primeru, je neupravičen dostop tretje osebe do teh podatkov oziroma neupravičeno razkritje teh podatkov. Čeprav uporabnik podatkov, ki jih ima na mobilni napravi, najpogosteje ni aktivno razkril, je njegovo nespoštovanje pravil o varovanju podatkov oziroma njegova opustitev dolžnega ravnanja povzročila neupravičeno razkritje podatkov, kar je mogoče subsumirati pod prepovedano posledico ustreznih kaznivih dejanj po 142., 143., 236. ali 260. členu KZ-1. Podobno velja za kaznivo dejanje iz 236. člena KZ-1.

Seveda je v vsakem konkretnem primeru treba sprejeti sklep, da je prav uporabnikova opustitev določenega dolžnega ravnanja povzročila neupravičeno

[62] Člen 34 ZDR-1.

[63] Na primer civilna podjemna pogodba ali avtorska pogodba.

[64] Če je seveda določen prekršek v ustreznem zakonu, uredbi vlade ali odloku občine v skladu z Zakonom o prekrških (ZP-1, Uradni list RS, št. 29/2011 – UPB8 in 21/2013).

[65] Bavcon in drugi, str. 159–186.

razkritje podatkov na mobilni napravi ali podatkov, do katerih se dostopa s pomočjo mobilne naprave; da je torej med uporabnikovo storitvijo ali bolj pogosto opustitvijo dolžnega ravnanja in nastalo prepovedano posledico podana vzročna zveza. Dokazati je treba tako vzročno zvezo med opustitvijo uporabe ali namestitve predpisane zaščite oziroma drugo kršitvijo dolžnostnega ravnanja na eni strani in nastalo grožnjo varnosti mobilne naprave na drugi strani kot tudi vzročno zvezo med nastalo grožnjo oziroma varnostnim dogodkom in neupravičenim razkritjem podatkov. V tem delu bo zelo pomembna vloga sodnih izvedencev za področje informacijske varnosti in tehnologije, ki bodo morali podati mnenje o vzročni zvezi, saj sodišče s takim strokovnim znanjem seveda ne razpolaga.[66]

S tem je izpolnjen šele prvi element kaznivega dejanja; voljno ravnanje, ki ga moramo subsumirati pod ustrezno opredelitev kaznivega dejanja iz KZ-1, potrditi pa je treba še obstoj protipravnosti in krivde. Četudi je lahko protipravnost ravnanja, ki se pri kaznivem dejanju domneva,[67] nesporna tudi v konkretnem primeru, bo največkrat sporno prav vprašanje zadnjega elementa kaznivega dejanja; uporabnikove krivde. Prav presoja njegove krivde in s tem njegove (ne)zadostne skrbnosti bo namreč razmejila situacijo, ko je uporabnik le žrtev kaznivega dejanja, od situacije, ko ga lahko štejemo za storilca kaznivega dejanja.

3.4. Uporabnikova krivda

3.4.1. Odgovornost uporabnika mobilne naprave za naklep

Za izpolnitev vseh elementov kaznivega dejanja mora biti torej v vsakem primeru dokazan tudi obstoj storilčeve oziroma uporabnikove krivde. Znotraj krivde se prištevnost domneva in je njeno odsotnost ali zmanjšanje treba utemeljevati v vsakem primeru posebej,[68] načeloma pa pri teh kaznivih dejanjih sama po sebi ni sporna.

Bolj bo relevantna presoja obstoja ustrezne oblike krivde in zavesti o protipravnosti. Namreč, kriv je le tisti storilec, ki je bil ob storitvi kaznivega dejanja prišteven in je ravnal z naklepom ali iz malomarnosti, pri tem pa se je zavedal ali bi se moral in mogel zavedati, da ravna v nasprotju s pravom, in če niso pri njem podani razlogi, ki izključujejo krivdo.[69]

Slovenski KZ-1 pozna dve obliki krivde: naklep in malomarnost. Kaznivo dejanje je izvršeno z naklepom, če se je storilec zavedal svojega dejanja in ga je

[66] Glej 248. člen Zakona o kazenskem postopku (ZKP – Uradni list RS, št. 32/2012 – UPB8 in 47/2013).

[67] Bavcon in drugi, str. 227.

[68] Prav tam, str. 262.

[69] Člen 24 KZ-1.

hotel storiti (direktni naklep), ali če se je zavedal, da lahko stori dejanje, in je v to privolil (eventualni naklep).[70] Kaznivo dejanje pa je izvršeno iz malomarnosti, če storilec ni ravnal s potrebno pazljivostjo, čeprav se je zavedal, da lahko stori dejanje, pa je lahkomiselno mislil, da se to ne bo zgodilo ali da bo to lahko preprečil (zavestna malomarnost), ali če se ni zavedal, da lahko stori dejanje, pa bi se bil po okoliščinah in po svojih osebnih lastnostih tega moral in mogel zavedati (nezavestna malomarnost).[71]

Omenjena kazniva dejanja so vedno kazniva, če so izvršena naklepno, le nekatera od njih pa so kazniva tudi, če so izvršena iz malomarnosti. Med te sodita kaznivi dejanji izdaje in neupravičene pridobitve poslovne skrivnosti[72] in izdaje tajnih podatkov.[73] Kadar je kaznivo dejanje v skladu s KZ-1 kaznivo iz malomarnosti, zadošča katera koli oblika malomarnosti, razen če bi bilo iz opredelitve kaznivega dejanja razvidno nasprotno.[74] Se pa pozneje intenzivnost krivde, ki ni relevantna za sam obstoj kaznivega dejanja, lahko upošteva pri odmeri kazni kot olajševalna ali obteževalna okoliščina.[75]

V primeru, če uporabnik mobilne naprave v informacijskem sistemu organizacije ne ravna dovolj skrbno in ne upošteva navodil organizacije o varni uporabi mobilnih naprav, posledično pa pride do tega, da se s podatki, ki bi jih sicer bil dolžan varovati, seznani neupravičena oseba, lahko zavrnemo obstoj naklepa pri takem uporabniku, s tem pa tudi subsumpcijo njegovega ravnanja pod definicije tistih kaznivih dejanj, ki so kazniva le v primeru, če so izvršena naklepno. Za kaznivo dejanje zlorabe osebnih podatkov ali neupravičene izdaje poklicne skrivnosti bi tako uporabnik mobilne naprave odgovarjal le, če naklepno ne bi uporabljal predpisanih zaščit, hkrati pa bi se zavedal groženj, nevarnosti in možnosti zaščit, saj bi želel, da pride do odtujitve podatkov, ali pa je v odtujitev podatkov vsaj privolil.

Kaznivi dejanji napada na informacijski sistem in zlorabe informacijskega sistema sta ravno tako kaznivi le takrat, ko sta izvršeni iz naklepa, zato v tem primeru prav tako ne prideta v poštev. Kaznivi bi bili tako le v primeru, ko uporabnik mobilne naprave naklepno ne bi uporabljal predpisanih zaščit, z namenom neupravičeno vstopiti ali vdreti v informacijski sistem ali to posredno omogočiti z opustitvijo uporabe ustreznih zaščit.

[70] Člen 25 KZ-1.
[71] Člen 26 KZ-1.
[72] Četrti odstavek 236. člena KZ-1.
[73] Četrti odstavek 260. člena KZ-1.
[74] Bavcon in drugi, str. 398.
[75] Prav tam, str. 398; 49. člen KZ-1.

3.4.2. Odgovornost uporabnika mobilne naprave za malomarnost

Pri kaznivem dejanju izdaje in neupravičene pridobitve poslovne skrivnosti in izdaje tajnih podatkov pa je relevantna tudi uporabnikova malomarnost. Če sodišče ugotovi obstoj malomarnosti, je mogoče govoriti o kazenski odgovornosti za ti dve kaznivi dejanji, v nasprotnem primeru pa ni krivde in s tem tudi ne kaznivega dejanja. V zvezi s presojo obstoja malomarnosti pri uporabniku mobilne naprave so tako relevantna naslednja dejstva, ki so bila tudi predmet opravljene ankete:

- (ne)zavedanje obstoja groženj informacijski varnosti mobilne naprave;
- (ne)poznavanje dostopnih rešitev za grožnje, ki so kot obvezne predpisane s strani organizacije;
- (ne)uporaba teh rešitev kljub poznavanju groženj in možnih rešitev ter obvezni uporabi le-teh.

Če se je uporabnik mobilne naprave zavedal možnosti konkretne varnostne grožnje mobilni napravi in s tem celotnemu informacijskemu sistemu, lahko govorimo o zavestni malomarnosti. Dokazati je treba, da uporabnik ni ravnal s potrebno pazljivostjo s tem, da je kršil predpisano dolžnostno ravnanje (da ni uporabljal predpisanih zaščit), čeprav se je zavedal, da lahko stori dejanje (da lahko pride zaradi njegove neuporabe predpisane zaščite do varnostne grožnje in posledično do neupravičenega razkritja poslovne skrivnosti ali tajnih podatkov), pa je lahkomiselno mislil, da se to ne bo zgodilo ali da bo to lahko še pravočasno preprečil s svojim ravnanjem ali s posredovanjem primera ustrezni službi znotraj informacijskega sistema ali drugi pristojni osebi.

Glede na rezultate opravljene ankete, ki kažejo, da se uporabniki mobilnih naprav bolj zavedajo klasičnih groženj mobilnim napravam, lahko ugotovimo, da bo pri teh grožnjah laže utemeljiti zavestno malomarnost uporabnika. Podatek, kako močno uporabnik mobilne naprave verjame, da se določena grožnja lahko zgodi tudi njemu, pa je relevanten za presojo zakonskega pogoja lahkomiselnosti, da ne bo prišlo do prepovedane posledice.

Enaka pravna posledica nastopi v primeru, ko se uporabnik zaveda groženj varnosti mobilne naprave, pa tudi dostopnih in predpisanih rešitve za te grožnje, saj tudi v tem primeru govorimo o zavestni malomarnosti. V zvezi s temi podatki ankete kažejo, da so nekatere vrste zaščit med uporabniki bolj znane, druge pa manj, da pa za skoraj vse oblike zaščit velja, da več kot 40 odstotkov uporabnikov, ki zaščito sicer pozna, te zaščite ne uporablja. Če se uporabnik zaveda groženj in pozna rešitve za odpravo oziroma preprečevanje teh groženj, ki jih je predpisala organizacija, pa jih ne uporabi, gre torej potencialno za primer zavestne malomarnosti.

Ko pa se uporabnik mobilne naprave ne zaveda potencialnih možnosti varnostnih groženj mobilni napravi, mu zavestne malomarnosti ne moremo očitati, saj se ni zavedal, da lahko stori kaznivo dejanje, tj. mu ne moremo očitati ravnanj s prepovedano posledico, kot sta določeni v definiciji kaznivega dejanja. Lahko mu kvečjemu očitamo, da ni ravnal s potrebno pazljivostjo (da ni uporabljal predpisanih zaščit za mobilno napravo), ker se ni zavedal, da lahko stori dejanje (da lahko zaradi neuporabe predpisanih zaščit pride do grožnje mobilni napravi in do neupravičenega razkritja poslovne skrivnosti ali tajnih podatkov), pa bi se bil po okoliščinah (objava načina uporabe mobilne naprave, izobraževanje o zaščitah in grožnjah, kakšno dolžnostno ravnanje glede upravljanja z mobilno napravo je imel konkretni uporabnik po pravilih organizacije itd.)[76] in po svojih osebnih lastnostih (individualne izkušnje z uporabo mobilnih naprav, položaj oziroma delovno mesto znotraj organizacije, lastnosti in sposobnosti konkretnega uporabnika mobilne naprave[77] itd.) tega moral in mogel zavedati.

V zvezi s tem so relevantni podatki ankete, v skladu s katerimi se uporabniki mobilnih naprav ne zavedajo novejših in bolj »sofisticiranih« groženj mobilnim napravam. V tem primeru torej uporabniku lahko očitamo kvečjemu le nezavestno malomarnost.

Enako velja v primeru, ko se uporabnik ne zaveda in ne pozna predpisanih rešitev za varno uporabo mobilnih naprav s strani organizacije, o čemer priča tudi opravljena anketa. To dejstvo je treba upoštevati pri presoji uporabnikove krivde.

Vprašanje, ali se je uporabnik resnično zavedal varnostnih groženj mobilni napravi ali ne, je dejansko vprašanje, ki ga bo sodišče moralo razrešiti v dokaznem postopku. Dejstvo pa je, da so predpisi, v katerih so določena pravila ravnanja s podatki in mobilnimi napravami, splošni in javno objavljeni, s splošnim aktom delodajalca pa je bil uporabnik v skladu z delovnopravno zakonodajo seznanjen s strani delodajalca v pisni ali ustni obliki. Za vprašanje obstoja storilčeve krivde bo to močan indic ali celo dokaz dejstva, da se je storilec zavedal groženj in predpisanih rešitev, ki pa ga bo tožilstvo v skladu z domnevo nedolžnosti seveda moralo dokazati v vsakem primeru posebej do stopnje prepričanosti sodišča.[78]

Po drugi strani pa je očitek, da bi se storilec po svojih osebnih okoliščinah in drugih okoliščinah tega moral in mogel zavedati, normativna ugotovitev, ki jo mora sprejeti sodišče na podlagi vseh okoliščin primera. Gre za očitek, da se uporabnik mobilne naprave ni zavedal možnosti grožnje in neupravičenega razkritja poslovne skrivnosti, čeprav bi se tega mogel glede na to, kakšno je bilo

[76] Bavcon in drugi, str. 291.
[77] Prav tam, str. 292.
[78] Drugi odstavek 3. člena ZKP.

njegovo objektivno dolžnostno ravnanje glede zaščite in varne uporabe mobilnih naprav, in glede na njegove osebne in subjektivne lastnosti. S tem bo sodišče določilo standard skrbnosti, ki se zahteva od uporabnika mobilne naprave, ki je del določenega informacijskega sistema, ki vsebuje zaščitene podatke.

V zvezi s predvidenimi zaščitami, ki omogočajo varno uporabo mobilne naprave znotraj informacijskega sistema, se zastavi vprašanje, kakšna je razlika v pravnem položaju storilca oziroma uporabnika mobilne naprave, če je predvidena zaščita predpisana ali le priporočena. Glede tega menimo, da v primeru, ko sta ravnanje in zaščita le priporočeni, in ne obvezno predpisani, ne moremo govoriti o objektivnem dolžnostnem ravnanju v konkretnem primeru, njegovi kršitvi in protipravnosti ravnanja, če ni način ravnanja predpisan že s kakšnim drugim predpisom. Na kratko: če želimo govoriti o kršitvi in protipravnem ravnanju ter posledično tudi odgovornosti, potem mora biti dolžnostno ravnanje predpisano.

Kazenskopravno je zanimivo tudi razkritje poslovne skrivnosti ali tajnega podatka neupravičeni osebi kljub uporabi predpisanih zaščit za mobilno napravo in kljub pravilnemu ravnanju z mobilno napravo. V tem primeru ni podana že bit inkriminacije, uporabnik torej ni izpolnil zakonskih znakov ustreznih kaznivih dejanj, ker je deloval v skladu s svojimi vnaprej določenimi dolžnostmi. Kaznivega dejanja in kazenske odgovornosti v takem primeru torej ni.

Zanimiv pa je tudi naslednji konkretni dejanski stan: uporabnik uporablja službeno mobilno napravo, vključeno v informacijski sistem organizacije, tako za službene namene, za katere mu je bila predana, pri čemer uporablja vse predpisane zaščite in jo uporablja za varen način, kot tudi za druge, neslužbene namene. Tukaj se lahko pojavi vprašanje kazenske odgovornosti, če pride do neupravičenega razkritja varovanih podatkov organizacije zaradi okužbe mobilne naprave z *malwareom* ali kakšno drugo grožnjo informacijski varnosti zaradi uporabe mobilne naprave s sicer vsemi predpisanimi zaščitami, a v času uporabe za neslužbeni namen. Če uporaba mobilne naprave v neslužbene namene ni dopustna, gre v tem primeru po našem mnenju tudi za kršitev akta organizacije, dolžnostnega ravnanja in za neupravičeno razkritje podatka. Hkrati je mogoče v delu, ko se mobilna naprava uporablja v neslužbene namene, govoriti o kaznivem dejanju poneverbe in neupravičene uporabe tujega premoženja iz 209. člena KZ-1. To seveda ne velja, če je neslužbena uporaba mobilnih naprav dovoljena.

To ugotovitev je treba povezati z rezultati ankete, ki kažejo na to, da več kot 40 odstotkov uporabnikov v ciljni populaciji uporablja mobilno napravo tako v službene kot tudi v neslužbene oziroma zasebne namene. Ta odstotek bi bil verjetno še višji v starejši populaciji, ki je bolj vključena v določeno organizacijo. Znotraj te populacije pa je, kot že rečeno, treba pravno razlikovati primere, ko je skupna uporaba iste mobilne naprave tako za službene kot tudi za zasebne

namene dovoljena z akti organizacije, in ko to ni dovoljeno. Samo v slednjem primeru lahko govorimo o potencialni kazenski odgovornosti.

3.4.3. Zavest uporabnika mobilne naprave, da ravna v nasprotju s pravili

Ob obstoju ustrezne oblike krivde je treba potem ugotoviti, ali se je storilec zavedal oziroma bi se moral in mogel zavedati, da ravna v nasprotju s pravom, ali ne.[79] Če želimo govoriti o kazenski odgovornosti uporabnika, mu je treba v konkretnem primeru namreč očitati, da se je zavedal, da ravna v nasprotju s pravom (v našem primeru torej v nasprotju s predpisanim ravnanjem z mobilno napravo), ali pa bi se tega vsaj moral in mogel zavedati. V slednjem primeru govorimo o neopravičljivi pravni zmoti, saj se uporabnik protipravnosti oziroma prepovedanosti svojega ravnanja ni zavedal, a glede na vse okoliščine zadeve lahko sprejmemo stališče, da takega nezavedanja ne moremo sprejeti in da bi se tega moral in mogel zavedati, zato bo kljub pravni zmoti odgovarjal za kaznivo dejanje.

Podrobnejše merilo, kdaj je uporabniku mogoče očitati, da bi se moral zavedati, da s svojim ravnanjem krši pravila organizacije o varni uporabi mobilne naprave, oziroma kdaj lahko govorimo o neopravičljivi pravni zmoti, določa tudi KZ-1, v skladu s katerim ni upravičenih razlogov za pravno zmoto in bi se uporabnik moral zavedati protipravnosti opustitve uporabe zaščitnih sredstev, če storilec ni vedel za pravna pravila, s katerimi bi se *lahko seznanil pod enakimi pogoji kot drugi v njegovem širšem okolju,* ali pa je *moral glede na svoje delo, vlogo ali siceršnji položaj* poznati posebna pravna pravila.

V našem primeru je zagotovo širše okolje storilca, ki je relevantno za to presojo, informacijski sistem organizacije oziroma organizacija in uporabnikovo službeno okolje. Za tako okolje pa zagotovo velja, da bi ga glede na svoje delo, vlogo ali siceršnji položaj moral poznati in da je imel za seznanitev z njimi enake možnosti kot drugi uporabniki mobilnih naprav v istem informacijskem sistemu, za katere velja isto dolžnostno ravnanje, ker so bili vsi skupaj naslovniki akta delodajalca, s katerim je le-ta predpisal, kako je treba ravnati z mobilno napravo. Čeprav je treba v skladu z domnevo nedolžnosti ta očitek dokazati v vsakem primeru posebej, menimo, da s tem ne bi smelo biti težav in da lahko v večini takih primerov govorimo o neopravičljivi pravni zmoti. Nasprotno trditev oziroma obstoj opravičljive pravne zmote bi bilo res težko utemeljiti s posebnostmi konkretnega primera, glede na to, da je bilo predpisano ravnanje vnaprej objavljeno, predpisano in sporočeno relevantnim naslovnikom.

[79] Člen 24 KZ-1.

4. Sklep

Mobilne naprave uporabljamo vse bolj pogosto, kar za študentsko populacijo dokazuje tudi opravljena raziskava, po kateri več kot četrtina vprašanih študentov uporablja klasični mobilni telefon in prenosni računalnik ali pametni telefon, to pa dokazujejo tudi poročila drugih organizacij. Mobilne naprave so poskrbele, da se je meja med zasebnim in poslovnim dodobra zabrisala, dober dokaz za to pa so tudi podatki iz raziskave, ki je bila v tem prispevku predstavljena. Vprašani namreč pametni telefon ne uporabljajo le v zasebne, ampak tudi v službene namene, in preko pametnega telefona, ki ga uporabljajo v zasebne namene, dostopajo tudi do službenih podatkov, ki lahko predstavljajo tudi poslovno ali poklicno skrivnost, osebni ali tajni podatek.

Tu pa uporabnost mobilnih naprav trči ob grozeče varnostne grožnje in njihove posledice. Osebe, ki imajo pooblaščen dostop do teh vrst podatkov, so jih dolžne varovati pred nepooblaščenim dostopom, tudi pred varnostnimi grožnjami, tako da mobilno napravo, s katero dostopajo do takih podatkov, uporabljajo na predpisan način.

Pri presojanju kazenske odgovornosti uporabnika mobilne naprave, ki je del informacijskega sistema organizacije, je treba ugotoviti, ali so izpolnjeni elementi splošnega pojma kaznivega dejanja (bit inkriminacije, protipravnost, krivda). Pri iskanju odgovora na to so pomembna prav dejstva, o katerih je bila opravljena omenjena raziskava. Ko namreč ugotavljamo, ali bo uporabnik mobilne naprave kazensko odgovarjal za to, da je preko njegove mobilne naprave prišlo do nepooblaščenega dostopa do določenega podatka na podlagi uresničitve varnostne grožnje in predhodne neuporabe varnostnih zaščit, moramo ugotoviti, ali se je uporabnik zavedal groženj, ki grozijo mobilni napravi, ali se je zavedal, kako in na kakšen način je dolžan ravnati z mobilno napravo, da bo njena uporaba varna, vključno z vidika podatkov, do katerih se dostopa s to mobilno napravo, ali pa podatkov, ki so že na mobilni napravi, oziroma ali je bilo varno ravnanje z mobilno napravo sploh predpisano. Z odgovori na ta vprašanja bomo na dejanski ravni ugotovili obstoj kaznivega dejanja, predvsem izpolnjenost znakov iz definicije kaznivega dejanja in obstoj krivde storilca.

KZ-1 sicer določa definicije ustreznih kaznivih dejanj, zakonske znake katerih uporabnik mobilne naprave lahko izvrši, ne določa pa, kdaj so razkritje in dostop do podatkov in s tem tudi ravnanje z mobilno napravo neupravičeni oziroma upravičeni. To je prepuščeno področnim predpisom in zavezujočim pravilnikom organizacije oziroma aktom delodajalca. Z vidika vzpostavljanja kazenske odgovornosti za neupravičeno razkritje takih podatkov je zato ključnega pomena zavezujoča določitev oziroma predpisovanje dolžnostnega ravnanja vseh uporabnikov mobilnih naprav, ki so vključene v informacijski sistem organizacije. Znotraj tega

dolžnostnega ravnanja se med drugim določi, katere zaščite je uporabnik dolžan uporabljati, na kakšen način lahko uporablja mobilno napravo oziroma za kakšne namene in kakšne grožnje pravzaprav grozijo mobilni napravi in podatkom znotraj informacijskega sistema. Če je dolžnostno ravnanje predpisano v aktu delodajalca ali drugem splošnem aktu organizacije, kršitev tega dolžnostnega ravnanja lahko predstavlja izpolnitev definicije kaznivega dejanja in s tem podlago za kazensko odgovornost. To olajša poznejše ugotavljanje kazenske, pa tudi drugih vrst pravne odgovornosti, hkrati pa izobražuje in obvešča uporabnike mobilne naprave, kako naj jo varno uporabljajo, in s tem deluje preventivno.

Opravljena raziskava in kazenskopravna analiza torej kažeta, da je poznavanje varnostnih groženj in rešitev slabo. To posledično pomeni, da je tveganje uresničitve katere od groženj večje. Ker je uporabnik mobilne naprave lahko kazensko odgovoren za odtujitev podatkov, do katerih dostopa z mobilno napravo, tudi v primeru, če se groženj in rešitev ne zaveda (v primeru nezavestne malomarnosti), menimo, da bi bilo treba zaradi izboljšanja informacijske varnosti in preprečevanja, pa tudi lažjega poznejšega uveljavljanja kazenske odgovornosti predpisati dovoljeno ravnanje z mobilno napravo in izboljšati poznavanje predvsem novejših groženj, tipičnih za mobilno napravo, ter varnostnih rešitev. Temu služijo v prvi vrsti že omenjeni pravilniki organizacij, pomembno pa je tudi stalno izobraževanje uporabnikov mobilnih naprav o njihovi varni uporabi v skladu s predpisi organizacije. Tako izobraževanje ravno tako preprečuje očitek, da se storilec ni mogel seznaniti s pravilno uporabo mobilne naprave ali da s tem ni bil seznanjen, preventivno učinkuje na kršitve pravilnega ravnanja in pojavljanje groženj mobilnim napravam, hkrati pa tudi olajša poznejši očitek storilcu, da je ravnal malomarno.

Literatura in viri

Bavcon, Ljubo, Šelih, Alenka, Korošec Damjan, Ambrož, Matjaž, Filipčič, Katja: (2013): *Kazensko pravo, splošni del*, Ljubljana: Uradni list, Ljubljana 2013.

Deisinger, Mitja: *Kazenski zakonik s komentarjem, Posebni del*. GV Založba, Ljubljana, 2002.

Korošec, Damjan: Poklicna skrivnost v slovenski kazenski zakonodaji – med prepovedjo in dolžnostjo izdaje podatka. V: Pavlović Z. (ur.), *Slabo ravnanje z otroki v Sloveniji: opažanje in obravnavanje.* Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani, 1997.

Leavitt, Neal: *Mobile Security: Finally a Serious Problem?,* Largo: University of Maryland 2011, http://www.computer.org/portal/web/computingnow (7. 9. 2013).

Markelj, Blaž, Zgaga, Sabina: Možnosti izgube podatkov in kazenskopravne posledice. V: Markelj, B., Bernik, I. (ur.), S*odobni aspekti informacijske varnosti.* Ljubljana: Fakulteta za varnostne vede, 2013, str. 95–109.

Pavčnik, Marijan. *Teorija prava: prispevek k razumevanju prava.* GV Založba, Ljubljana 2011.

Završnik, Aleš. Kibernetična kriminaliteta – (kiber)kriminološke in (kiber)viktimološke posebnosti »informacijske avtoceste«. V: *Revija za kriminalistiko in kriminologijo*, 2005, let. 56, št. 3, str. 248–260.

Europol. Organised Crime Threat Assessment, https://www.europol.europa.eu/content/press/europol-organised-crime-threat-assessment-2011-429 (6. 12. 2013).

GfK Group. *CEE Telco Industry Report 2011,* http://www.gfk.com/group/press_information/press_releases/008894/index.en.html (6. 6. 2013).

Informacijski sistemi – infrastruktura, Laboratorij za komunikacijske naprave, http://www.lkn.fe.uni-lj.si/gradiva/IS_VS/Informacijski%20sistemi%2002%20-%20Infrastruktura%20-%20Strojna%20oprema.pdf (4. 12. 2013).

Lookout. *Lookout Mobile Threat Report,* https://www.mylookout.com/mobile-threat-report (10. 9. 2013).

Microsoft Tag. *Infographic: MobileStatistics, Statse&Facts 2011,* http://www.digitalbuzzblog.com/2011-mobile-statistics-stats-facts-marketing-infographic (2. 2. 2013).

V.
Vpliv informacijskih tehnologij na pravni sistem

Dostop do interneta kot temeljna pravica*

dr. Matija Damjan

1. Pomen interneta v demokratični družbi

Internet postaja temelj informacijske in komunikacijske infrastrukture sodobne družbe, saj povezuje številne nekdaj ločene tehnologije in storitve prenosa informacij: pošte, telefonije, časopisov, radia, televizije. Elektronsko poslovanje postaja nepogrešljivo v trgovini in bančništvu, raste pa tudi njegova vloga v upravnih in sodnih postopkih. Virtualni prostor interneta tako postaja ekvivalent fizičnega prostora, v katerem se gibljemo in izražamo. Internet je zato tudi pomembno sredstvo (ali prostor) za uresničevanje človekovih pravic in temeljnih svoboščin. Prva pride na misel svoboda izražanja, ki jo zagotavlja 39. člen Ustave RS.[1] Internet drugače kot klasični mediji omogoča obojestranski pretok informacij, to pomeni, da lahko vsak uporabnik prejema informacije in se nanje odziva, pri čemer lahko svoja stališča izrazi na način, da so dostopna vsem uporabnikom interneta, na primer v spletnem dnevniku (na blogu) ali na spletnem forumu. Pri sodobnih hibridnih storitvah ni mogoče več strogo razlikovati med oddajanjem in tradicionalnim individualnim komuniciranjem.[2] Lahko rečemo, da je šele na internetu svoboda izražanja zaživela v popolnosti, saj so prvič tako izenačene tehnične možnosti za uresničevanje te pravice. V duhu Ustave na internetu vsakdo lahko svobodno zbira, sprejema in širi vesti ter mnenja. Svoboda izražanja je postala praktično dejstvo in svetovni fenomen za vsakogar z računalnikom ali mobilnim telefonom.

Svoboda komuniciranja, ki je trdno zakoreninjena v mednarodnem pravu človekovih pravic, tvori jedro internetnih svoboščin.[3] Evropsko sodišče za člo-

---

* Prispevek je bil prvič objavljen v: Pravni letopis 2011, Inštitut za primerjalno pravo pri Pravni fakultetei v Ljubljani.

[1] Ustava Republike Slovenije (Uradni list RS, št. 33/1991-I, 42/1997, 66/2000, 24/2003, 69/2004, 69/2004, 69/2004, 68/2006).

[2] K. H. Ladeur, *Legal Questions of Excluding Participants from Internet Discussion Groups: On the Guaranteeing of Freedom of Communication Through 'Network-Adapted' Private Law.* German Law Journal, let. 9 (2008), str. 965.

[3] R. Uerpmann-Wittzack, *Principles of International Internet Law.* German Law Journal, vol. 11 (2010), št. 11, str. 1247.

vekove pravice (ESČP) je potrdilo, da informacije in ideje, izražena na spletni strani, spadajo znotraj obsega 10. člena Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin (EKČP),[4] ki varuje svobodo govora in mišljenja.[5] Enako velja za internetne arhive.[6] Priljubljen internetni forum pa z vidika svobode medijev, ki jo sodna praksa izvaja iz svobode izražanja, uživa enako varstvo kot tiskani mediji.[7] Tudi Vrhovno sodišče ZDA je odločilo, da je internet medij, ki uživa popolno svobodo izražanja po prvem amandmaju, enako kot časopisi. Drugače kot radiodifuzni mediji (radio, televizija) se namreč internet ne srečuje z omejenostjo frekvenčnega spektra, zato ni razloga za kakršnokoli državno reguliranje ali cenzuro njegove vsebine. Vrhovno sodišče je pri tem o internetu govorilo kot o širokem demokratičnem forumu, o novem trgu idej, ki omogoča relativno neomejeno možnost poceni komunikacije in ki posamezniko dramatično lajša nagovarjanje širše javnosti. Internet omogoča, da so posamezniki tudi ustvarjalci vsebin, in ne samo njihovi pasivni sprejemniki, ter da so aktivni udeleženci v dialogu, in ne le njegovi opazovalci. Zato ima internet velik demokratični potencial.[8]

Internet se je že izkazal kot pomembno sredstvo pri razvoju demokracije in boju proti diskriminaciji. Razvita informacijska infrastruktura namreč državljanom olajša uveljavljanje njihovih demokratičnih pravic, zlasti z virtualnim uresničevanjem pravic svobodnega izražanja in svobodnega združevanja.[9] To je prišlo do veljave na primer pri letošnjih vstajah proti nedemokratičnim režimom v arabskem svetu, ki so bile večinoma organizirane prek internetnih socialnih omrežij. Za demokracijo pa je internet pomemben tudi kot orodje, prek katerega je mogoče v elektronski obliki izvesti različne postopke pravne države (e-pravosodje, e-uprava, e-volitve, dostop do elektronskih javnih registrov ipd.). Z omogočanjem dostopa do neslutenega obsega znanja (na primer v spletni enciklopediji Wikipedija ali digitalni knjižnici dLib.si) internet prevzema del tradicionalne vloge javnih knjižnic in postaja nepogrešljiv za uresničevanje ustavno zagotovljene svobode izobraževanja. Zaradi rastočih možnosti opravljanja dela na daljavo pa je internet relevanten tudi s stališča svobode dela in proste izbire zaposlitve.

[4] Uradni list RS – MP, št. 7/1994 (33/1994).

[5] Sodba ESČP v zadevi *Perrin proti Združenemu kraljestvu* z dne 18. oktobra 2005.

[6] Sodba ESČP v zadevi *Times Newspapers Ltd. proti Združenemu kraljestvu* z dne 10. marca 2009.

[7] Sodba ESČP v zadevi *Fatullayev proti Azerbajdžanu* z dne 22. aprila 2010, 95. odstavek.

[8] *Reno proti American Civil Liberties Union*, 521 U. S. 844 (1997).

[9] M. L. Best, *Can the Internet be a Human Right?*, Human Rights & Human Welfare, vol. 4 (2004), str. 24. Primerjaj Ladeur, nav. delo, str. 965.

Z ustavnega vidika je pomembno tudi varstvo komunikacijske zasebnosti in osebnih podatkov, ki so na internetu še posebej izpostavljeni zaradi hitre prenosljivosti digitalnih podatkov in številnih posrednikov, ki tehnično sodelujejo pri ponujanju informacijskih storitev. Sodna praksa ESČP potrjuje, da elektronska pošta nedvomno spada med zaščitene oblike korespondence,[10] pa tudi drugi podatki, ki se prenašajo prek interneta, spadajo v zasebno življenje lastnikov, če niso namenjeni javnemu dostopu.[11] Nedopustno lahko v zasebnost posežejo tako država kot tudi zasebni izvajalci storitev, na primer ponudniki internetnega dostopa, ki jim država naloži shranjevanje določenih podatkov o posameznikovi uporabi interneta ali ki tovrstne podatke zbirajo in obdelujejo sami zaradi poslovnih interesov (ciljano oglaševanje).[12]

Glede na to, da internet nadomešča oziroma prevzema vlogo različnih starejših tehnologij, je treba poskrbeti, da ob tem tehnološkem prehodu ne bi efektivno izumrle s temi tehnologijami povezane in tradicionalno uveljavljene pravice, kot sta svoboda tiska ter varstvo tajnosti pisem in drugih občil. Kot rečeno, sodna praksa že priznava varstvo izvrševanja teh pravic na internetu, podobno kot pri klasični, predinternetni obliki (elektronska pošta je izenačena s klasično pošto, internetni forum z mediji ipd.). Vendar ostaja vprašanje, ali je tak parcialen pristop dolgoročno zadovoljiv. Internet združuje in hkrati opravlja funkcije pošte, telekomunikacij, medijev in marsičesa drugega, zato omejujoč oblastni poseg v internet lahko prizadene izvrševanje vseh teh funkcij in s tem poseže v vrsto ustavno varovanih človekovih pravic. Presoja dopustnosti takega posega mora biti zato večdimenzionalna.

2. Pravica dostopa do interneta za posameznika

Internet postaja standardni način komuniciranja in dostopanja do različnih podatkov na daljavo, zato pridobiva internetni dostop podoben infrastrukturni pomen kot drugi komunalni priključki: vodovod in kanalizacija, elektrika, telefon. Izključitev od te tehnologije dejansko pomeni nekakšno izključitev iz sodobne družbe. Zato si države prizadevajo omogočiti enostavno dostopnost interneta čim širšemu delu prebivalstva, na primer tudi na odmaknjenih območjih. Estonija je na primer kot prva država določila, da ima vsakdo pravico dostopa do interneta, ki jo lahko brezplačno uresničuje tudi v javnih knjižnicah. Na Finskem pa od

[10] Glej sodbo ESČP v zadevi *Liberty et al. proti Združenemu kraljestvu* z dne 1. julija 2008, 52. odstavek.

[11] V zadevi C-275/06 *Promusicae proti Música de España* je Sodišče EU (SEU) štelo, da ima tudi IP-naslov naravo podatka, ki je zavarovan v skladu s 6. členom Direktive 2002/58/ES o zasebnosti in elektronskih komunikacijah.

[12] Uerpmann-Wittzack, nav. delo, str. 1252.

1. julija 2010 primerna internetna povezava velja za univerzalno storitev, ki jo morajo izbrani operaterji omogočiti vsem stalnim prebivalcem in podjetjem po razumni ceni in s sprejemnim tokom vsaj 1 Mbit.[13]

Po drugi strani pa se marsikje pojavljajo predlogi zakonodaje, ki kot sankcijo za (nekomercialne) kršitve pravic intelektualne lastnine z uporabo interneta (zlasti pretakanje »piratskih« kopij glasbe in filmov z uporabo tehnologij *peer-to-peer*) predvideva odklop posameznika od internetnega dostopa. Ker je zaradi prej prikazanih razlogov internetni dostop vse pomembnejši za uresničevanje različnih človekovih pravic, je oblastna prepoved dostopa do interneta hud poseg v pravice posameznika, ki ga ni mogoče odrediti brez ustreznih procesnih jamstev. To je leta 2009 potrdil francoski ustavni svet pri presoji zakona, znanega pod akronimom HADOPI,[14] ki je predvideval, da poseben upravni organ lahko po treh opozorilih po elektronski pošti odredi odklop interneta uporabniku, ki s snemanjem piratskih vsebin z interneta krši avtorske pravice. Ustavni svet je odločil, da je taka rešitev v nasprotju z več določbami francoske ustave o temeljnih pravicah, zlasti o svobodi izražanja in domnevi nedolžnosti, ter o delitvi oblasti. Poudaril je, da je internet sredstvo, prek katerega francoski državljani lahko izvršujejo svoje temeljne ustavne demokratične pravice in svoboščine. Pristojnosti novega upravnega organa lahko omejijo pravico katerekoli osebe do svobodnega izražanja in komuniciranja, zlasti s svojega doma. Zato je odklop naročnikov od dostopa do interneta dopusten samo na podlagi odločitve sodišča.[15] Tej odločitvi je francoski zakonodajalec sledil z ustrezno prilagoditvijo zakona, ki postopek odklopa bolj formalizira in zahteva sodelovanje sodišča.

Ostaja pa vprašljivo, koliko bo sankcija odklopa interneta dejansko učinkovita kot ukrep varstva avtorskih pravic. Odklop bo namreč lahko veljal samo za konkretnega naročnika, ne pa na primer za druge člane njegovega gospodinjstva. Če so ti poprej dostopali do interneta prek istega priključka, bo z odklopom poseženo tudi v izvrševanje njihovih pravic, ne glede na njihovo ravnanje. Po drugi strani bodo te osebe lahko same sklenile naročniško razmerje in v prihodnje

---

[13] N. Coulson, A. E. J. Hutchinson, *Should access to the internet be a fundamental right?*, E-Commerce Law & Policy, let. 12 (2010), št. 9, str. 12. *Access to a minimum of 1 Mbit Internet connection available to everyone in Finland by July 2010.* Sporočilo za javnost finskega ministrstva za promet in komunikacije z dne 16. 10. 2009, http://www.lvm.fi/web/en/pressreleases/view/920100. Glej tudi A. Linnervuo, T. Ruikka, *Finland: Universal broadband access: The Finnish experience.* E-Commerce Law & Policy, let. 11 (2009), št. 12.

[14] Gre za kratico novoustanovljenega urada za varstvo avtorskih del na internetu *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet.* Naslov zakona je Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.

[15] Décision n° 2009-580 DC du 10 juin 2009. Glej tudi F. Rizzuto, *European Union Telecommunications Law Reform and Combating Online Non-Commercial Infringements of Copyright: Seeing Through the Legal Fog.* Computer and Telecommunications Law Review, let. 17 (2011), št. 3, str. 78.

prek njega omogočale dostop kršitelju. Poleg tega je vstopnih točk v internet več: poleg kabelskega in DSL-dostopa je vse bolj razširjen tudi mobilni internet, ki je dostopen tudi anonimno, na predplačniški podlagi, dostop je mogoč tudi prek javno dostopnih brezžičnih omrežij in internetnih kavarn, zato je zgolj prekinitev posamezne naročniške pogodbe omejenega pomena, četudi je za posameznika lahko neprijetna.[16]

Pod vplivom razprav o kontroverznem francoskem zakonu se je za ureditev možnosti odklopa od interneta v istem obdobju odločil tudi Evropski parlament, ki je ravno sprejemal spremembe Direktive 2002/21/ES o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve.[17] Poudaril je, da je internet nujen za izobraževanje in dejansko uresničevanje svobode izražanja ter dostopa do informacij in bi moralo biti kakršnokoli omejevanje teh temeljnih pravic v skladu z EKČP.[18] V okvirno direktivo je bil tako vnesen nov, 3.a odstavek 1. člena, ki določa, da morajo ukrepi, ki jih države članice sprejmejo glede dostopa do in uporabe storitev in aplikacij prek elektronskih komunikacijskih omrežij s strani končnih uporabnikov, spoštovati temeljne pravice in svoboščine fizičnih oseb, zagotovljene z EKČP ter s splošnimi načeli prava Skupnosti. Tovrstni ukrepi, ki bi lahko omejili temeljne pravice ali svoboščine, se lahko naložijo le, če so ustrezni, sorazmerni in potrebni v demokratični družbi, za njihovo izvajanje pa veljajo ustrezni postopkovni zaščitni ukrepi v skladu z EKČP ter s splošnimi načeli prava Skupnosti, vključno z učinkovitim sodnim varstvom in predpisanim postopkom. Skladno s tem se ti ukrepi lahko sprejmejo le ob ustreznem spoštovanju načela domneve nedolžnosti in pravice do zasebnosti. Zagotovljen mora biti predhoden, pošten in nepristranski postopek, vključno s pravico do zaslišanja zadevne osebe ter do učinkovitega in pravočasnega sodnega nadzora.

Besedilo te določbe sicer izrecno ne omenja interneta, vendar je iz četrte uvodne izjave k Direktivi 2009/140/ES razvidno, da se novi odstavek nanaša predvsem na dostop do interneta, zato se jo v pravni literaturi poimenuje določba o internetni svobodi. Direktiva precej podrobno in izrecno določa načela ter postopkovne pravice, ki jih morajo države članice zagotoviti v svoji zakonodaji (zato je gotovo neposredno učinkovita). Tri postopkovna jamstva so: domneva

[16] Primerjaj Coulson, Hutchinson, nav. delo, str. 13.

[17] Direktiva Evropskega parlamenta in Sveta 2002/21/ES z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (okvirna direktiva), UL L 108 z dne 24. 4. 2002, spremembe: UL L 171, z dne 29. 6. 2007, str. 32, L 167, z dne 29. 6. 2009, str. 12, L 337, z dne 18. 12. 2009 str. 37.

[18] Četrta uvodna izjava Direktive 2009/140/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o spremembi direktiv 2002/21/ES o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve, 2002/19/ES o dostopu do elektronskih komunikacijskih omrežij in pripadajočih naprav ter o njihovem medomrežnem povezovanju in 2002/20/ES o odobritvi elektronskih komunikacijskih omrežij in storitev, UL L 337/37, z dne 18. 12. 2009.

nedolžnosti in pravica zasebnosti; predhodni pošten in neodvisen postopek; pravica do učinkovitega in pravočasnega sodnega nadzora. Poleg tega morajo biti ukrepi omejevanja dostopa do interneta v konkretnem primeru nujni, primerni in sorazmerni znotraj demokratične družbe. Določba je zasnovana podobno kot 6. člen EKČP, ki določa pravice v kazenskih postopkih in s tem implicitno varuje pravico dostopa do interneta podobno, kot so varovane človekove pravice in temeljne svoboščine.[19] Del pravne teorije zato ugotavlja, da gre ta določba onkraj tega, da bi varovala dostop do interneta samo kot sredstvo za uresničevanje drugih pravic, saj določa procesna jamstva za posege v dostop do interneta sam po sebi, ne glede na način njegove uporabe. S tem se dejansko priznava nemoten trajni dostop do interneta kot avtonomno pravico oziroma svoboščino po pravu EU, ki mora biti ustrezno pravno varovana.[20] Tudi pri konservativnejši razlagi, da je dostop do interneta zgolj sredstvo za uresničevanje različnih človekovih pravic, je praktični rezultat določbe enak, kot če bi varovali dostop. Seveda pa direktiva ne zahteva, da mora država zagotoviti posameznikom dostop do interneta, ampak samo, da vanj ne sme samovoljno posegati. Večina držav članic sicer z različnimi ukrepi spodbuja dostopnost interneta.[21]

Določba o internetni svobodi neposredno varuje samo pravice fizičnih oseb kot končnih uporabnikov interneta, zlasti ker sankcija odklopa internetnega dostopa grozi predvsem takim uporabnikom zaradi nekomercialnih kršitev avtorskih pravic. Vendar ESČP potrjuje, da svobodo izražanja na internetu uživajo tudi pravne osebe pri izvajanju komercialnih dejavnosti.[22] EKČP sicer posebej ne varuje svobode opravljanja poslovnih dejavnosti, pač pa se lahko v skrajnih primerih prizadeti sklicujejo na pravico do varstva premoženja iz 1. člena prvega protokola k EKČP,[23] v Sloveniji pa pride v poštev še varstvo na podlagi pravice do svobodne gospodarske pobude iz 74. člena Ustave.[24] Zato bi širša formulacija temeljne pravice internetne svobode morala obsegati tudi pravice pravnih subjektov, da nemoteno uporabljajo internet za opravljanje svoje dejavnosti.

[19] Rizzuto, nav. delo, str. 80–81.

[20] Rizzuto, nav. delo, str. 75–76.

[21] D. Dods, P. Brisby, R. Hubbard, K. Ollerenshaw, B. Ingram, *Reform of European Electronic Communications Law: A Special Briefing on the Radical Changes of 2009.* Computer and Telecommunications Law Review, let. 16 (2010), št. 4, str. 104–105.

[22] Sodba ESČP v zadevi *Times Newspapers Ltd. proti Združenemu kraljestvu* z dne 10. marca 2009.

[23] Glej na primer sodbo ESČP v zadevi *Megadat.com SRL proti Moldaviji* z dne 8. aprila 2008, odstavki 62–64.

[24] Primerjaj Uerpmann-Wittzack, nav. delo, str. 1247, 1249.

3. Blokiranje spletnih strani kot omejitev dostopa do interneta

3.1. Razlogi za blokiranje in veljavna ureditev

Doslej smo obravnavali pogoje, pod katerimi se lahko posamezniku prepreči, da bi dostopal do interneta. Mogoč pa je tudi obrnjen položaj: z blokiranjem posameznih spletnih mest oziroma IP-naslovov je mogoče preprečiti, da internet »pride« do posameznika. Rezultat je v marsičem podoben. Najbolj znan in najobsežnejši primer tovrstne cenzure interneta je »véliki kitajski požarni zid«, ki filtrira in samodejno blokira vse vsebine, ki so politično neprimerne, torej kakorkoli kritične do stališč kitajskih oblasti. Tak celovit sistem filtriranja dejansko pomeni delitev interneta, saj je bistvena tehnična lastnost interneta ravno njegova decentraliziranost in možnost vzpostavitve povezave med katerimikoli dostopnimi točkami (IP-naslovi), zaradi česar lahko vsak uporabnik dostopa do kateregakoli spletnega mesta.

Cenzura interneta je značilna predvsem za nedemokratične režime, ki vsebine blokirajo iz političnih razlogov. Vendar tudi razvite demokracije niso imune na rastoče želje po sistematičnem filtriranju interneta. S takim ukrepom se želi zlasti preprečiti širjenje vsebin, ki kršijo določene norme nacionalnega prava (kršitve avtorskih pravic, otroška pornografija, nacistična propaganda). Če se ponudniki teh vsebin oziroma njihovi strežniki nahajajo zunaj domače jurisdikcije, ukrepanje pri viru ni mogoče – namesto tega se izvede blokada pri posredniku, tj. ponudniku internetnega dostopa (ISP). V Avstraliji na primer lahko vladna agencija sestavi črno listo blokiranih tujih spletnih mest z neprimernimi vsebinami, zlasti povezanimi s pornografijo, promoviranjem terorizma ali drog, kršitvami avtorskih pravic ipd. Znotraj Evropske unije takih splošnih internetnih blokad (za zdaj) ni, čeprav se pojavljajo pobude o vzpostavitvi »virtualne schengenske meje«, na kateri bi se blokiralo nezakonite vsebine z neevropskih strežnikov na podlagi črne liste.[25]

Problematiko delno ureja Direktiva o elektronskem poslovanju,[26] ki jo v tem delu v slovenski pravni red prenaša Zakon o elektronskem poslovanju na trgu (ZEPT).[27] Kot temeljno načelo velja, da mora nadzor nad storitvami informacijske družbe zaradi zaščite ciljev javnega interesa potekati pri viru dejavnosti, v državi

[25] Glej zapisnik sestanka pri Svetu EU *Joint meeting of the Law Enforcement Working Party and the Customs Cooperation Working Party* z dne 17. februarja 2011, dostopen na: http://register.consilium.europa.eu/pdf/en/11/st07/st07181.en11.pdf.

[26] Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju), UL L 178, 17. 7. 2000.

[27] Uradni list RS, št. 61/2006, 45/2008 – ZArbit, 79/2009.

članici, kjer imajo storitve svoj izvor. Ne glede na to pa lahko države članice pod pogoji iz te direktive uvedejo ukrepe za omejitev prostega pretoka storitev informacijske družbe.[28] Direktiva naj bi bila ustrezna podlaga za razvoj hitrih in zanesljivih postopkov za odstranitev in blokiranje dostopa do nezakonitih podatkov, pri čemer se predvideva tudi možnost uporabe tehničnih sistemov za nadzor, ki jih omogoča digitalna tehnika. Vsi taki ukrepi pa morajo biti v skladu s pravili EU o varstvu osebnih podatkov in zasebnosti komunikacij.[29]

V 15. členu direktiva izključuje kakršnokoli splošno obveznost ponudnikov storitev informacijske družbe, da nadzirajo podatke, ki jih prenašajo ali shranjujejo za svoje stranke (uporabnike storitev). Prav tako ponudniki niso dolžni dejavno raziskovati okoliščin, nakazujočih na protipravnost podatkov, ki jih zagotavlja prejemnik storitve (enako tretji odstavek 8. člena ZEPT). Ponudnik torej niti ni dolžan nadzirati vsebine niti je zaradi varstva zasebnosti uporabnikov ne sme nadzirati. To splošno načelo pa ne izključuje možnosti, da sodišče ali drug organ ponudniku internetnega dostopa naloži, da odstrani ali onemogoči dostop do določenih nezakonitih podatkov, vendar je taka blokada lahko samo individualne narave. Direktiva torej razlikuje med splošno obveznostjo nadzora podatkov, ki je izključena, in konkretnimi obveznostmi nadzora, ki se lahko po nacionalni zakonodaji odredijo ponudnikom internetnih storitev.[30]

ZEPT v 18. členu vsakomur, ki meni, da ponudnik storitev krši katero njegovo pravico, omogoča, da pred pristojnim sodiščem zahteva izdajo začasne odredbe. Sodišče lahko z začasno odredbo zlasti prepove grozeče kršitve ali nadaljevanje začetih kršitev ali omeji opravljanje storitev informacijske družbe tako, da ponudniku storitve naloži, naj odstrani ali onemogoči dostop do podatkov, ki jih hrani.

Sodišče lahko izda začasno odredbo tudi brez zaslišanja nasprotne stranke, če predlagatelj izkaže za verjetno, da bi kakršnokoli odlašanje z izdajo začasne odredbe onemogočilo doseganje njenega namena ali povzročilo težko nadomestljivo škodo predlagatelju. V vsakem primeru pa mora predlagatelj začasne odredbe v določenem roku vložiti tožbo, s katero opraviči izdajo začasne odredbe.

Zakon o varstvu osebnih podatkov (ZVOP-1)[31] pri ureditvi ukrepov inšpekcijskega nadzora sledi izhodišču o ukrepanju pri viru podatkov. V drugem odstavku 54. člena namreč določa, da sicer predvidenih ukrepov zaradi kršitve osebnih podatkov (na primer prepoved obdelave, anonimiziranje, blokiranje, brisanje ali uničenje) ni mogoče odrediti zoper osebo, ki v elektronskem komunikacijskem

[28] Dvaindvajseta in štiriindvajseta uvodna izjava Direktive o elektronskem poslovanju.

[29] Štirideseta uvodna izjava Direktive o elektronskem poslovanju.

[30] Glej K. Tičar, B. Makarovič, Udeleženci internetne komunikacije, v: *Pravni vodnik po internetu* (ur. B. Makarovič, J. Toplišek), Ljubljana: GV Založba, 2007, str. 263–264.

[31] Uradni list RS, št. 86/2004, 113/2005 – ZInfP, 51/2007 – ZUstS-A, 67/2007, 94/2007 – UPB1.

omrežju opravlja storitve prenosa podatkov, vključno z začasnim shranjevanjem podatkov in drugimi delovanji v zvezi s podatki, ki so pretežno ali v celoti v funkciji opravljanja ali olajšanja prenosa podatkov po omrežjih, če ta oseba sama nima interesa, povezanega z vsebino teh podatkov, in ne gre za osebo, ki lahko sama ali skupaj z omejenim krogom z njo povezanih oseb učinkovito nadzoruje dostop do teh podatkov. Blokado teh podatkov na internetu je torej mogoče doseči samo na podlagi sodne odločbe, kot to predvideva v ZEPT, ne pa z odločbo inšpekcijskega organa.

Drugačen je bil pristop Zakona o igrah na srečo (ZIS).[32] Novela ZIS-C[33] iz leta 2010, ki je podrobneje uredila prirejanje internetnih iger na srečo, je v novem devetem odstavku 107. člena določila, da lahko Urad za nadzor prirejanja iger na srečo, če ugotovi, da se spletne igre na srečo prirejajo brez ustrezne koncesije, ponudniku storitve informacijske družbe naloži omejitev dostopa do spletnih strani oziroma drugih telekomunikacijskih povezav, prek katerih se take igre prirejajo. Urad je tak ukrep v praksi tudi uporabil. Taka ureditev pa ni veljala dolgo, saj je isto leto novela ZIS-D[34] navedeno določbo nadomestila z novim, 107.a členom, ki omogoča, da v primeru, če ponudnik spletnih iger na srečo brez koncesije prostovoljno ne izvrši prepovedne odločbe nadzornega organa, upravno sodišče na predlog urada ponudniku storitev informacijske družbe odredi omejitev dostopa do spletnih strani, prek katerih se take igre prirejajo. Ureditev je povzeta po ZEPT (ki sicer igre na srečo izključuje iz svoje uporabe). Obrazložitev predloga zakona je navajala, da gre pri vsakem omejevanju dostopa do spletnih strani za ukrepe, ki so povezani z omejevanjem svobode interneta in s tem svobode izražanja kot ustavno zagotovljene pravice, zato je primerno, da tudi o omejitvi dostopa do spletnih strani, prek katerih se prirejajo spletne igre na srečo brez koncesije, odloči sodišče.[35] Zakon predpisuje tudi načela, ki jih mora urad upoštevati v svojem predlogu (sorazmernost, upoštevanje tehničnih možnosti), in sestavine, ki jih mora vsebovati predlog (obseg omejitve, način izvršitve). Omejitev dostopa do spletnih strani je mogoča le v obsegu, ki je nujno potreben za izvršitev odločbe o prepovedi prirejanja igre na srečo, in na način, ki je najmanj obremenjujoč za ponudnika storitev informacijske družbe.

[32] Uradni list RS, št. 27/1995, 35/1997 – Skl. US: U-I-140/97 (43/1997 popr.), 22/2000, 22/2000, 22/2000, 85/2001, 54/2002 – Odl. US: U-I-50/00-18, 101/2003, 134/2003 – UPB1, 19/2004 – Odl. US: U-I-245/01-6, 132/2004 – Odl. US: U-I-3/02-25, 10/2010, 106/2010, 14/2011 – UPB3.

[33] Uradni list RS, št. 10/2010.

[34] Zakon o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-D) (Uradni list RS, št. 106/2010).

[35] Predlog Zakona o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-D), EVA 2010-1611-0084, EPA1366-V, str. 7.

3.2. Svoboda prejemanja informacij

Na blokiranje spletnih mest se običajno gleda samo kot na poseg v pravice imetnika takega mesta oziroma ponudnika vsebin na njem. Vendar je tako gledanje preozko, saj vsaka blokada interneta omeji tudi uporabnike zadevnega ponudnika internetnega dostopa, saj ti ne morejo več dostopati do kateregakoli dela interneta. Ta možnost je pomembna zlasti z vidika svobode izražanja. Best opozarja, da se ta pravica sicer pogosto formulira asimetrično: svoboda izražanja se vedno smatra za temeljno človekovo pravico, svoboda branja oziroma drugih oblik sprejemanja izraženih stališč pa se ne obravnava enako. Vendar iz pravice izražanja izhaja tudi potreba po poslušanju oziroma sprejemanju izraženega in s tem povezana potreba po dostopu do ustreznih informacijskih tehnologij, sicer izražanje izzveni v prazno.[36] Svoboda iskanja in sprejemanja informacij ter idej s kakršnimikoli sredstvi ter brez vmešavanja javnih oblasti je v okviru svobode izražanja izrecno izražena v 39. členu slovenske Ustave, tako kot tudi v 19. členu Splošne deklaracije človekovih pravic,[37] 10. členu EKČP in 11. členu Listine EU o temeljnih pravicah.[38] Ameriško vrhovno sodišče je že leta 1965 zapisalo, da svoboda govora in tiska ne vključuje samo pravice nekaj izreči ali natisniti, ampak tudi pravico to informacijo distribuirati, jo prejeti in jo prebrati. Vključuje pravico poizvedovati, svobodo misli in svobodo učenja.[39] ESČP pa je leta 2009 potrdilo, da ker svoboda izražanja obsega tudi svobodo pridobivanja informacij, zahteva po cenzuriranju spletnih mest ne zadeva samo ponudnikov vsebin, ampak tudi javnost kot uporabnika interneta.[40]

S tega stališča je jasno, da je blokiranje spletnih mest v demokratični družbi zelo občutljiv ukrep, po učinkih primerljiv na primer s prepovedjo izdaje časopisa in zaplembo natisnjene naklade. Tak ukrep je torej ustavno sprejemljiv samo kot *ultima ratio*, če je res nujen za zaščito drugih, pomembnejših ustavnih vrednot javnega interesa. Vprašljivo je, ali navaden premoženjski interes prizadete stranke lahko upraviči tako grob poseg v informacijsko in komunikacijsko svobodo interneta. Zato bo sodišče pri vsakokratnem odločanju o zahtevi za blokado spletnega mesta moralo tehtati ustavne vrednote na eni in drugi strani ter presoditi sorazmernost predlaganega ukrepa s stališča zastavljenega cilja. Blokada celotnega spletnega mesta oziroma internetnega naslova je lahko nesorazmerna,

[36] Best, nav. delo, str. 23 in 24.

[37] Sprejela in razglasila jo je Generalna skupščina Združenih narodov 10. decembra 1948 z resolucijo št. 217 A (III).

[38] Uradni list EU, C 83, 30. 3. 2010.

[39] *Griswold proti Connecticut*, 381 U. S. 479 (1965).

[40] Sodba ESČP v zadevi *Times Newspapers Ltd. proti Združenemu kraljestvu* z dne 10. marca 2009, 40. in 41. odstavek.

če so nezakonite samo nekatere vsebine, ki so na njem dostopne, večina pa je neproblematičnih in ni opravičljivega razloga za njihovo cenzuro. Sodišče bi torej moralo upoštevati, da pri vsakem odločanju o blokadi interneta odloča tudi o človekovih pravicah in o posegu v svobodo temeljne informacijske infrastrukture sodobne demokratične družbe.

Pomemben vidik, ki ga je treba pri presoji upoštevati, pa je tudi vprašanje učinkovitosti tovrstnega blokiranja. Blokado domenskega imena ali IP-naslova je namreč tehnično mogoče razmeroma preprosto obiti, na primer z uporabo posredovalnih (*proxy*) strežnikov, za kar ni potrebno posebno tehnično znanje. Zato je vprašljivo, ali je odreditev take blokade res primeren ukrep za dosego zastavljenih ciljev. Res učinkovita blokada je samo tista, ki temelji na t. i. *deep packet inspection,* torej na preverjanju vse vsebine, ki se pretaka prek strežnikov določenega ponudnika internetnih storitev. Glede na to, da pakete informacij, ki potujejo prek interneta, lahko obravnavamo analogno poštnim pošiljkam, bi bila tako zasnovana blokada enaka temu, da bi Pošti naložili, naj prebere vse pisemske pošiljke in izloči tiste z nezakonito vsebino (na primer s skeniranjem, prepoznavanjem besedila in samodejnim iskanjem ključnih besed). Zaradi ustavnega varstva zasebnosti in tajnosti pisemskih pošiljk je jasno, da bi bil tak ukrep pri klasični pošti nedopusten, in enako mora veljati tudi pri nadzoru internetnega prometa.

Podoben položaj obravnava Sodišče EU v zadevi C-70/10 *Scarlet Extended proti SABAM*, v kateri bo presojalo začasno odredbo, s katero je belgijsko sodišče naložilo ponudniku internetnega dostopa, podjetju Scarlet, vgraditev sistema za filtriranje vseh podatkovnih komunikacij, ki se pretakajo skozi njegovo omrežje, zaznavanje podatkov, ki kršijo avtorske pravice, in blokiranje tovrstnih komunikacij bodisi na strani pošiljatelja bodisi na strani prejemnika. Generalni pravobranilec Cruz Villalón je v svojem mnenju v tej zadevi izrazil stališče, da taka začasna odredba pomeni omejitev pravice do spoštovanja zasebnosti komunikacij in pravice do varstva osebnih podatkov, ki ju varuje Listina EU o temeljnih pravicah. Prav tako bi tak sistem filtriranja omejil svobodo izražanja in obveščanja, ki jo listina tudi varuje. Omejitve teh pravic so sicer mogoče, če za to obstajajo utemeljeni razlogi, vendar mora vsaka omejitev temeljiti na zakonu, ki je dostopen, jasen in predvidljiv. Po stališču generalnega pravobranilca zato pravo EU sodišču države članice prepoveduje odreditev sicer posamičnega ukrepa nadzora, s katerim pa bi se za neomejen čas vzpostavil sistem abstraktnega preventivnega nadzora in filtriranja vsega internetnega prometa.

4. Sklep

Uporabnik na internetu najde tako rekoč vsako vsebino, ki jo išče, redko pa proti svoji volji naleti na nekaj, česar sploh ni iskal. Pred neželenimi vsebinami

se lahko varuje tudi s programi za filtriranje, zato ni potrebe, da bi uporabnike pred tem »varovala« država z vzpostavitvijo cenzure interneta. Velja nasprotno: s cenzuro se poseže prav v pravice uporabnikov. Pri vsakem posegu države v internet je potrebna celovita presoja, kako ta poseg vpliva na svobodo interneta kot integralno svoboščino tehnične narave, in ne zadošča omejitev na konkretno kršitev oziroma pravico, ki se skuša z blokiranjem zavarovati. Glede na kvalitativno razliko med internetom in starejšimi informacijskimi tehnologijami smo vse bliže položaju, ko bo treba kot človekovo pravico varovati internet sam po sebi, in ne zgolj internet kot orodje za uresničevanje drugih pravic.[41]

[41] Best, nav. delo, str. 23 in 24.

Objavljanje sodnih odločb v internetnih podatkovnih bazah in vpliv na sodno prakso

dr. Lojze Ude

1. Uvod

Na Inštitutu za primerjalno pravo poteka raziskovalni program Pravni izzivi informacijske družbe. V okviru te raziskave je pomembno področje tudi oblikovanje modernih – internetnih podatkovnih baz in vpliv teh podatkovnih baz na sodno odločanje ter na oblikovanje sodne prakse na splošno. Internetne podatkovne baze, še posebej, če so v njih zajete vse sodne odločbe Vrhovnega sodišča RS in vseh višjih sodišč v Sloveniji, seveda vplivajo ne le na argumentacijo sodnih odločb, temveč tudi na vsebinsko odločanje sodišč. Ureditev revizije v veljavnem Zakonu o pravdnem postopku med kriterije za dopustnost revizije uvršča zlasti pojme v 367.a členu, kot so »zagotovitev pravne varnosti«, »enotna uporaba prava«, »razvoj prava preko sodne prakse«, »odstop od sodne prakse Vrhovnega sodišča«, »neobstoj sodne prakse« in »neenotnost sodne prakse Vrhovnega sodišča«. Namen tega sestavka ni spuščati se globlje v vsebino problematike o dopustnosti revizije. Že sama uporaba pojmov pa dokazuje, da je sodna praksa izredno pomembna za dopustnost tega izrednega pravnega sredstva.[1] Zaradi tega pa je tudi izjemnega pomena, da je objavljenih čim več sodnih odločb, na podlagi katerih je mogoče ugotoviti, ali je dopustna revizija. Isto velja tudi za druge pravne institute, ki jih sodišča uporabljajo pri odločanju.

V nadaljevanju se bom skliceval večinoma ali skoraj izključno na civilno pravno področje, predvsem na obligacijsko pravo, stvarno pravo in sodne postopke. Sklicevanje na druga pravna področja bi razširilo ta sestavek na obseg, ki bi ga bilo težje predstaviti, poleg tega pa avtor na drugih pravnih področjih ni deloval v enakem obsegu in enako poglobljeno kot na področju civilnega prava.

V sklepnem delu bo obravnavana tudi empirična raziskava s področja insolvenčnega prava, ki smo jo na inštitutu opravili leta 2013 in obsega prikaz 245

[1] Glej o tem L. Ude v komentarju Pravdni postopek, Zakon s komentarjem, 3. knjiga, GV Založba in Uradni list Republike Slovenije, Ljubljana 2009, str. 533–539.

sodnih odločb.[2] Insolvenčno pravo je bilo izbrano, ker zakon, ki ga ureja, zajema ekonomsko in pravno problematiko, pa tudi problematiko materialnega in procesnega prava. Sam insolvenčni postopek je sicer neke vrste nepravdni postopek, tako da revizija proti nekaterim pravnomočnim odločbam ni dovoljena, v številnih sporih v zvezi z insolvenčnimi postopki (v sporih zaradi prerekanja terjatev, izpodbijanja pravnih dejanj stečajnega dolžnika) pa potekajo pravde po določbah civilnega pravdnega postopka, seveda vključujoč pri tem tudi izredno pravno sredstvo revizije.

Navedena raziskava nikakor ni in ne more biti zaključena, saj sedanje stanje na področju objavljanja sodnih odločb ni zadovoljivo. Potrebujemo nadaljnji razvoj pravne doktrine in sodne prakse na področju internetnih podatkovnih baz, ki v modernem življenju zajemajo največje število objavljenih sodnih odločb.

2. Sodna praksa in objavljanje sodnih odločb pred osamosvojitvijo Slovenije

Pred osamosvojitvijo Slovenije je dolgo, na civilnem področju vse do leta 1978/1980, veljala nenavadna situacija. Številna pravna področja niso bila urejena z zakoni, tako da so obstajale številne »neprave« pravne praznine.[3] Ta ugotovitev je veljala za večji del obveznostnega (obligacijskega) prava, za večji del stvarnega prava in v tem okviru odškodninskega prava ter celo za izvršilni postopek. Do uveljavitve novih zakonov[4] je bilo treba zaradi obstoja t. i. pravnih praznin na podlagi 4. člena Zakona o razveljavitvi pravnih predpisov, izdanih pred 6. 4. 1941 in med sovražnikovo okupacijo, uporabljati stare pravne predpise kot pravna pravila, kadar niso bila v nasprotju z ustavo federacije in republik in pozitivnimi zakoni ter drugimi predpisi oziroma z načeli ustavnega reda federacije in republik. To je pomenilo, da so sodišča na teh področjih uporabljala celo take predpise, kot je bil Občni državljanski zakonik (ODZ iz leta 1811). Seveda so sodišča v takem pravnem položaju ustvarjala pravna pravila, saj na primer na področju odškodninskega prava Občni državljanski zakonik ni bil več primerna podlaga za odločanje, pa čeprav ne zaradi tega, ker so njegove določbe nasprotovale »pridobitvam revolucije in socialističnemu pravnemu redu«, temveč te določbe niso

[2] Pregled odločb s področja insolvenčnega prava vsebuje zbirka Insolvenčno pravo, izbor iz sodne prakse, oktober 2013, ki je bila pripravljena v okviru raziskave na Inštitutu za primerjalno pravo pri Pravni fakulteti v Ljubljani.

[3] Glej o tem R. Lukić, Uvod v pravo, Beograd 1973, L. Ude, Civilni pravdni postopek, Ljubljana 1988, str. 29 in 30.

[4] Zakon o obligacijskih razmerjih, ZOR, Uradni list SFRJ, št. 29/1978, Zakon o temeljnih lastninsko-pravnih razmerjih ZTLR, Uradni list SFRJ, št. 6/1980 in Zakon o izvršilnem postopku ZIP, Uradni list SFRJ, št. 20/1978.

več ustrezale pravi eksploziji odškodninskih primerov.[5] Tako na primer je ODZ poznal v paragrafih 1325 in 1326 dve obliki nepremoženjske škode – bolečine (pravna teorija in sodna praksa na območju veljavnosti ODZ je štela med te bolečine telesne in duševne bolečine, upoštevajoč pri tem tudi strah)[6] in skaženost kot posebno obliko duševnih bolečin. Sodna praksa je nato poleg dveh teh temeljnih oblik – odškodnine za bolečine in za skaženost – uvedla še nekatere druge oblike nepremoženjske škode oziroma je odškodnino za bolečine razčlenila v več ločenih postavk.[7]

Tako je mogoče trditi, da je sodna praksa imela celo kreativno funkcijo pri oblikovanju prava in nikakor ni le interpretirala zakonodaje in drugih splošnih pravnih predpisov.[8] Da je sodna praksa odločilno vplivala celo na zakonodajo, je mogoče razbrati iz ureditve različnih institutov v ZOR, ZTLR in ZIP, ki so na civilnem področju skušali napolniti nekatere neprave pravne praznine. Tudi zdaj veljavni zakoni, ki urejajo ta področja (Obligacijski zakonik, Uradni list RS, št. 53/2001 in nasl., OZ, Stvarnopravni zakonik, Uradni list RS, št. 87/2002 in nasl., SPZ, Zakon o izvršbi in zavarovanju, Uradni list RS, št. 51/1998 in nasl., ZIZ), pomenijo kontinuiteto na področju civilnega materialnega in procesnega prava ter zaradi tega povzemajo tudi pravno ureditev, ki jo je v precejšnjem delu izoblikovala sodna praksa.

V obdobju pred osamosvojitvijo Republike Slovenije je tedanje Vrhovno sodišče SRS imelo tudi izredno pogoste občne seje. Potekale so dva- do trikrat na leto in so obravnavale več deset stališč, izoblikovanih s sodnimi odločbami, ki jih je nato Vrhovno sodišče SRS objavljalo v Poročilu o sodni praksi Vrhovnega sodišča SRS. Ta stališča se niso nanašala samo na tista pravna vprašanja, ki niso bila urejena z novimi pravnimi predpisi, temveč tudi na vsa druga področja, ki so bila že desetletja urejena s pravnimi predpisi, kot je na primer področje civilnega pravdnega postopka. Pogostost občnih sej in s tem velik vpliv sprejetih mnenj in stališč na teh sejah poudarjam zaradi tega, ker Vrhovno sodišče RS takih sej nima več oziroma so tako redke in na njih sprejeta stališča tako osamljena, da nikakor ni več mogoče trditi, da njegove občne seje vplivajo na razvoj sodne prakse.

Poleg tega je pred osamosvojitvijo izšlo tudi mnogo komentarjev. Pisec tega sestavka je tako na primer skupaj z Jožetom Juhartom in Dragico Wedam Lukić

[5] Glej S. Cigoj, Odškodninsko pravo Jugoslavije, Ljubljana 1972, str. 2 in 3, L. Ude, J. Mlakar, J. Trajčev, Odškodninska odgovornost za nesreče pri delu, Ljubljana 1974, str. 5.

[6] Glej o tem M. Brkić, Neimovinske štete usled telesne povrede, Pravni život 1971, št. 5, str. 43, in isti pisec, O koncepciji neimovinske štete in novčane prestacije za tu štetu u našem pravu, Naša zakonitost, 1972, št. 4, str. 3.

[7] L. Ude, delo cit. v op. 4, str. 72.

[8] L. Ude, celo cit. v op. 2, str. 29 in 30.

leta 1974 izdal obsežen komentar z naslovom Pravdni postopek, izdal pa je tudi štiri komentarje Zakona o stanovanjskih razmerjih. Ti in drugi komentarji o različnih zakonskih ureditvah so tako kot v drugih kontinentalnih državah, ki temeljijo na legislativnem sistemu, ne na precedenčnem pravu, vplivali na oblikovanje sodne prakse in na uveljavljanje različnih interpretacij pravnih institutov in pravnih predpisov.

3. Sodna praksa in objavljanje sodnih odločb po osamosvojitvi Republike Slovenije

3.1. Novi pravni sistem in sodna praksa

Tudi v drugih državah v Evropi je objavljanje sodnih odločb obsežno. Tako nemška pravna doktrina poudarja, da vpliva objave sodnih odločb nikakor ni treba podcenjevati. Zaradi tega se izredno zaostrujeta vprašanji izbora objavljenih odločb in tudi njihove redakcijske obdelave. Postopki izbire, ki so po mnenju doktrine pogosto nepregledni, povzročajo neurejen položaj. Tak položaj pa na pravnem področju ustvarja negotovost, saj se na objavljene odločbe ni mogoče brez zadržkov zanašati. Zelo različen je tudi obseg objave odločb posameznih sodišč in sodnih senatov.[9] Sicer pa je v ZR Nemčiji objavljanje sodnih odločb zaradi uveljavitve načela javnosti sodnega odločanja celo obveznost sodišč. To stališče je zavzelo Zvezno upravno sodišče v odločbi z dne 26. 2. 1997.[10] Tudi v Švici zvezno in kantonalna sodišča objavljajo sodne odločbe, in sicer v uradnih publikacijah, internetnih bankah podatkov, pa tudi v strokovnih časopisih in celo drugih medijih. Vendar obveznost objavljanja ni tako jasno opredeljena kot v Nemčiji, dejansko pa je objavljanje uveljavljeno v širokem obsegu.[11]

Eden posebnih problemov v zvezi z objavljanjem je vprašanje anonimizacije sodnih odločb, se pravi vprašanje, ali naj se sodbe objavijo z imeni strank in sodnikov, ki so sodbo izdali. Pravna doktrina se večinoma zavzema za objavljanje imen strank. Eden izmed argumentov je, da je v pomembnih zadevah javnosti znano, kdo so udeleženci posameznih postopkov. To zlasti velja, kadar gre za področja, kot je na primer konkurenčno pravo. Seveda pa lahko zahteva po osebni, poslovni ali uradni tajnosti povzroči, da objava imen ni dopustna. Tudi navajanje imen

[9] Glej R. Walker, Die richterliche Veröffentlichungspraxis in der Kritik, JurPC Web-Dok. 34/1998, odst. 1–163.

[10] Glej sodbo Bundesverwaltungsgericht, BVerwG 6 C 3.96, OVG 10 L 5059/93, z dne 26. 2. 1997.

[11] P. Tschümperlin, Die Publikation gerichtlicher Entscheide, v: Kommentar zum Publikationscesetz des Bundes, Editions Weblaw, Bern 2011, str. 69–87.

sodnikov je dopustno.[12] Pravna doktrina tudi poudarja, da količina objavljenih odločb (popolnost prikaza sodne prakse) kaže tudi kakovost.[13]

3.2. Objavljanje sodnih odločb v Sloveniji

V Sloveniji tako kot v drugih državah s kontinentalnim pravnim sistemom sodišča zdaj objavljajo vse pomembnejše odločbe. To velja v celoti za Vrhovno sodišče RS, v zadnjem času pa tudi za višja sodišča v naši državi. Vendar objavljanje sodnih odločb ni pravno obvezno kot na primer v ZR Nemčiji. Sodne odločbe se objavljajo v komentarjih,[14] v zadnjih letih pa so vse sodne odločbe dostopne tudi na portalu IUS-INFO, tj. v urejenem pravnem in poslovnem informacijskem sistemu na internetu. Zanimivo je, da pri objavljanju sodnih odločb ni nobene selekcije in da tudi ni pravil, v kakšni obliki se objavljajo. Na internetnem portalu se je uveljavila oblika s poudarjenim jedrom sodne odločbe, v nadaljevanju pa je polno besedilo izreka in obrazložitve. Imena strank in imena sodnikov pa pri nas niso navedena. Tak je uveljavljeni način objavljanja sodnih odločb.

Problematiko objavljanja sodnih odločb in predvsem problematiko sodne prakse je največ preučeval Tilen Štajnpihler,[15] ki se je ukvarjal s temelji precedenčnega učinka sodnih odločb, s sodno odločbo kot virom prava, s sodno odločbo kot nosilko precedenčnega primera, z utemeljevanjem sodne odločbe s predhodnimi sodnimi odločbami, z argumentom precedensa in s precedenčnim učinkom sodnih odločb pri ustvarjanju prava.[16] V svojih delih se zavzema za velik obseg objavljanja sodnih odločb, poudarja pa vpliv sodne prakse na pravičnost sojenja v določenem obdobju in na uveljavljanje formalne enakosti. Opozarja tudi, da ustaljena sodna praksa ustvarja stabilnost pravnega sistema ter

[12] G. Knerr, Die Namensnennung bei der Publikation gerichtlicher Entscheidungen, JurPc Web-Dok. 73/2004, odst. 1–54, S. Ackermann, Veröffentlichung gerichtlicher Entscheidungen in juristischen Fachpublikationen in anonymisierter Form? JurPC 7/93, str. 2168–2174.

[13] W. Kuntz, Quantität gerichtlicher Entscheidungen als Qualitätskriterium juristischer Datenbanken, JurPc-Web-Dok. 0012/2006, str. 1–14.

[14] Glej M. Juhart, A. Berden, T. Kersteš, V. Rijavec, M. Tratnik, A. Vlahek in R. Vrenčur, Stvarnopravni zakonik s komentarjem, Ljubljana 2004, N. Plavšak, M. Juhart, V. Kranjc, D. Jadek Pensa, P. Grilc, A. Polajnar Pavčnik, M. Dolenc, M. Pavčnik, Obligacijski zakonik s komentarjem, Splošni del, 1. in 2. knjiga, Ljubljana 2003, L. Ude, N. Betetto, A. Galič, V. Rijavec, D. Wedam Lukić in J. Zobec, Pravdni postopek, Zakon s komentarjem, 1.–4. knjiga, Ljubljana 2005–2010.

[15] T. Štajnpihler, Precedenčni učinek sodnih odločb pri pravnem utemeljevanju, GV Založba, Ljubljana 2012.

[16] Isti avtor je nekatera vprašanja, ki so sicer zajeta v njegovi samostojni publikaciji, obravnaval tudi v člankih Smisel precedenčnega učinka sodnih odločb, Zbornik znanstvenih razprav Pravne fakultete v Ljubljani 2010, str. 255–284, Prispevek k interpretaciji načela enakega obravnavanja, Zbornik znanstvenih razprav Pravne fakultete v Ljubljani 2008, str. 233–259, in K vprašanju (ne)enotnosti sodne prakse v luči pravice do poštenega sojenja, Pravna praksa, št. 44/2011, str. 28.

utrjuje pravno državo in vladavino prava. Nekateri avtorji so se ukvarjali tudi z drugo problematiko, na primer z anonimizacijo sodnih odločb. Tako na primer D. Možina[17] poudarja, da je za javnost in tudi sama sodišča koristno objavljanje sodnih odločb le tedaj, kadar je iz objavljene odločbe razvidno, na katero dejansko stanje se nanaša, in da je brez povzetka bistvenega in relevantnega dejanskega stanja objavljena sodba manj pomembna in ima tudi manj vpliva. Kar zadeva anonimizacijo, pa se zavzema za čim popolnejše navajanje podatkov o strankah in sodnikih. Anonimizacija objavljenih sodnih odločb je včasih dopustna zaradi varstva osebnih podatkov, argumentov za brisanje imen sodnikov pa avtor ne najde. Sodnik, ki ga izvoli državni zbor in predstavlja neodvisno sodno vejo oblasti, se ne sme skrivati.

3.3. Kratka analiza empirične raziskave

Kot je bilo že rečeno, smo v okviru raziskovalnega programa opravili tudi empirično analizo sodne prakse v zvezi z uporabo insolvenčnega zakona. Na podlagi te analize je mogoče ugotoviti:

a) V razmeroma majhnem obsegu je objavljanje sodnih odločb pripeljalo do enotne sodne prakse, včasih tudi po razhajanju glede posameznih vprašanj, ki pa je zahtevalo poenotenje zaradi obravnavanja zadev z enako pravno problematiko:

- Tako se je na primer v sodnih odločbah uveljavilo stališče, da se tudi v primeru, ko Javni jamstveni in preživninski sklad RS nastopa kot upnik zoper preživninskega zavezanca, ker je namesto njega plačal preživninskim upravičencem, izvršilni postopek kljub uvedbi osebnega stečaja nadaljuje (tako v odločbah Vrhovnega sodišča RS, opr. št. II Ips 649/2001, z dne 7. 2. 2002, opr. št. I R 94/2007, z dne 25. 10. 2007, in opr. št. II Ips 170/2010, z dne 16. 12. 2010).
- Sodna praksa Vrhovnega sodišča RS je uveljavila tudi stališče, da obveznosti kapitalske gospodarske družbe, nad katero je bil opravljen postopek stečaja, z izbrisom iz registra ne prenehajo. Isto velja tudi tedaj pri izbrisu brez likvidacije. To stališče je pomembno predvsem zaradi obveznosti porokov ali hipotekarnih dolžnikov (tako odločba VS RS, opr. št. III Ips 121/2011, z dne 11. 6. 2013, in pravno mnenje občne seje VS RS, opr. št. 1/2013, z dne 21. 6. 2013).
- Po nekaterih različnih sodnih odločbah glede priznavanja nagrade stečajnega upravitelja (glej odločbo Višjega sodišča Maribor št. I Cpg 235/2009, z dne 31. 8. 2009, Višjega sodišča v Ljubljani št. Cst 42/2011, z dne 25. 5. 2011) je

[17] D. Možina, O vplivu javne dostopnosti in zgradbe sodnih odločb na kvaliteto prava, Pravna praksa, št. 45/2012, str. 6.

najprej Ustavno sodišče RS vplivalo na sodno prakso z odločbo št. U-I-185/10, Up-1409/10, z dne 2. 2. 2012, nato pa je sodno prakso uskladilo tudi Vrhovno sodišče RS z odločbo št. Cst 70/2012, z dne 5. 4. 2012. Zavzelo je stališče, da se stečajnemu upravitelju odmeri nagrada po predpisih, ki so veljali v času opravljanja nalog in pooblastil stečajnega upravitelja. V obdobju do 13. 6. 2009 je zato pravna podlaga za določitev nagrade odredba, ki je veljala do tega datuma, po tem datumu pa tedaj sprejeti pravilnik.

b) Precej pa je tudi neusklajenih odločb sodišč, tako da kljub njihovemu številu ne moremo govoriti o enotni sodni praksi. Tako imamo na primer različna stališča do vprašanj:

- Po mnenju nekaterih sodišč (glej na primer odločbo Višjega sodišča v Ljubljani, št. III Cpg 427/2010, z dne 19. 5. 2010) dolžnik nima pravice do ugovora proti sklepu o odpustu obveznosti pri osebnem stečaju. Zaradi tega je sodišče s citiranim sklepom tak ugovor oziroma pritožbo (formalno je bila vložena pritožba) zavrglo. Po mnenju drugih sodišč pa sta pritožba oziroma ugovor proti takemu sklepu dopustna, saj so nekatera sodišča pritožbo obravnavala vsebinsko (tako odločba Višjega sodišča Ljubljana št. Cst 254/2011, z dne 22. 9. 1011).
- Po stališču enega senata višjega sodišča (glej odločbo Višjega sodišča v Ljubljani št. Cst 254/2011, z dne 22. 9. 2011) v postopku osebnega stečaja, ko začetek stečajnega postopka predlaga dolžnik, ne velja domneva insolventnosti. Po stališču drugega senata istega sodišča (glej odločbo Višjega sodišča v Ljubljani št. III Cpg 841/2010, z dne 6. 7. 2010) pa tudi v primeru, ko začetek stečajnega postopka predlaga dolžnik, velja domneva insolventnosti.
- Tudi odločbe istega sodišča (verjetno različnih senatov) so glede drugih pravnih vprašanj pogosto različne. Tako je Višje sodišče v Ljubljani v odločbi št. I Cpg 849/2010, z dne 13. 10. 2010, sprejelo stališče, da ne morejo nastopiti učinki zaznambe izvršbe po tretjem odstavku 87. člena Zakona o zemljiški knjigi (ZZK-1), ker iz zemljiškoknjižnega izpiska ni razvidno, da bi zemljiškoknjižno sodišče sprejelo sklep o izvršbi oziroma o vpisu na podlagi sprejetega sklepa. Po odločbi Višjega sodišča v Ljubljani št. II Ip 2128/2011, z dne 25. 10. 2011, pa je dan zaznambe sklepa o izvršbi in s tem dan pridobitve zastavne in ločitvene pravice na nepremičninah odvisen od trenutka začetka učinkovanja vpisa, torej od trenutka, ko zemljiškoknjižno sodišče prejme listino za vpis na podlagi predloga ali po uradni dolžnosti. Upnik torej zastavno in s tem tudi ločitveno pravico pridobi z učinkom za nazaj.

Navedeni primeri torej kažejo, da sodna praksa glede uporabe posameznih institutov ali zakonskih določb pogosto ni usklajena. Zdi se, da objavljanje sodnih odločb, zlasti kadar število objavljenih odločb, v katerih je sodišče zavzelo eno

od možnih stališč, ni veliko, ne pripelje do poskusov poenotenja sodne prakse. Šele kadar je število objavljenih odločb večje, je mogoče govoriti o usklajeni sodni praksi, če je stališče v njih enako. Kadar pa številne odločbe vsebujejo različna stališča, gre za neusklajeno sodno prakso, kar naj bi bil predvsem znak za Vrhovno sodišče RS, da je treba ali v revizijskem postopku, če je to glede na ureditev revizije mogoče, ali pa s pogostejšim razpisovanjem občnih sej in sprejemanjem načelnih mnenj sodno prakso uskladiti. Vrhovno sodišče RS ne izpolnjuje svoje obveznosti usklajevanja sodne prakse, čeprav Zakon o sodiščih (Uradni list RS, št. 19/1994 in nasl.) v 108. členu določa, da vodi evidenco sodne prakse, v 109. členu pa, da to sodišče skrbi za enotno sodno prakso, in čeprav je v 110. členu istega zakona tudi določeno, da Vrhovno sodišče RS na občni seji sprejema načelna mnenja o vprašanjih, ki so pomembna za uporabo zakonov, sprejema pravna mnenja o vprašanjih sodne prakse in določa način spremljanja sodne prakse na sodiščih. Večja višja sodišča (zlasti Višje sodišče v Ljubljani) pa ne usklajujejo pravnih stališč niti med svojimi senati.

4. Sklep

Očitno je, da je objavljanje sodnih odločb in s tem stališč, ki so v njih zavzeta, koristno tako za uveljavljanje enakosti strank pred sodiščem po določbah 22. in 14. člena Ustave RS kot tudi za delovanje pravne države. Smiselno bi bilo, da bi bila vsaj na strokovni ravni sprejeta pravila, kako naj se sodne odločbe za objavo pripravijo in redigirajo. Očitno pa v Sloveniji ni potrebe, da bi tudi formalnopravno uvedli obveznost objavljanja sodnih odločb, ker se je v naši državi uveljavila praksa objavljanja vseh odločb Vrhovnega sodišča RS in višjih sodišč v državi.

Vrhovno sodišče RS svoje dolžnosti skrbeti za enotno sodno prakso ne opravlja učinkovito in v večjem nujno potrebnem obsegu. Večkrat bi moralo razpisati občno sejo in na njej sprejemati načelna pravna mnenja o uporabi zakonov in mnenja o vprašanjih sodne prakse.

Treba bi bilo natančneje preučiti vprašanje anonimizacije objavljenih sodnih odločb. Razen v primerih varovanja osebne, poslovne ali uradne tajnosti ni razlogov za črtanje imen fizičnih oseb ali pravnih oseb v sodnih odločbah, pripravljenih za objavo. V objavljenih sodnih odločbah bi morali biti navedeni vsi sodniki, ki so pri odločanju sodelovali.

Umetna inteligenca v pravu*

Andrej Grah Whatmough, Boštjan Koritnik

Avtorja sva v tem delu knjige najprej orisala velik gospodarski pomen (uspeh) interneta, najuspešnejši produkt na njem (spletni[1] iskalnik Google) in razlog za tak uspeh ter prizadevanja na področju umetne inteligence za (več kot le) nadgradnjo tovrstnih iskalnikov. Na prvi pogled povezava teh vsebin in prava gotovo ni očitna (razen običajnega pravno določenega okvira za posamezno od teh vsebin, npr. varstvo osebnih podatkov pri uporabi brskalnikov), a bo to morda zgolj potrdilo za v tem prispevku predstavljeni podjetniški projekt zatrjevano inovativnost in drznost, ki v podjetniškem procesu (raz)deli ekonomsko uspešne zgodbe od neuspešnih. V nadaljevanju bova predstavila projekt slovenskih podjetnikov inovatorjev, katerega cilj je uporaba na znanju temelječih informacijskih sistemov (torej takih »z« umetno inteligenco), ki bi korenito spremenili pravni sistem, predvsem v smeri večje objektivnosti v upravnih in sodnih postopkih ter s tem večje pravne varnosti. Razčlenitvi te ideje in možnostim, ki jih njena uresničitev ponuja, bova namenila večji del tega prispevka.

Gre torej za projekt s področja umetne inteligence v pravu, ki temelji na »strojnem razumevanju naravnega jezika«, zaradi te značilnosti pa je ta hkrati tudi cilj »dokončne« nadgradnje trenutno (še) najuspešnejšega internetnega produkta v zgodovini – spletnega iskalnika. Njegov uspeh je torej eden od kazalnikov gospodarskega potenciala predstavljenega projekta, ki pa je razmeroma majhen v primerjavi z vpeljavo umetne inteligence v pravo oziroma z njenim potencialom, da spremeni naša življenja.

1. Razvoj internet(neg)a (iskanja) – od znakovnih nizov do metapodatkov

Internet ne bo nikoli splošno uporabljan (t. i. *mainstream*), saj ni bil zasnovan za opravljanje (gospodarskih) poslov.[2] To je bil le eden od argumentov za tako

---

* Prispevek je spremenjen in dopolnjen. prvič je bil objavljen v: Pravna praksa, št. 10/2010, priloga.

[1] V prispevku izraza splet in internet uporabljava kot sopomenki.

[2] »*It was not designed for doing commerce*.« Glej K. Kelly: We Are the Web, v: Wired, št. 12.08, avgust 2005; na voljo je na www.wired. com/wired/archive/13.08/tech.html (10. 3. 2014).

stališče ameriške revije Time proti koncu leta 1994.[3] Dobrih deset let pozneje se je novinarju iste revije zapisalo, da internet še vedno ni povsem pripravljen (za »biznis«), da pa se koščki sestavljanke počasi že sestavljajo v celoto.[4] A če pogledamo razvoj v zadnjih dobrih 20 letih – do leta 1991 je bilo delovanje oziroma poslovanje s ciljem pridobivanja dobička na internetu celo strogo prepovedano![5] –, bi lahko rekli, da je internet predvsem (ne pa (še) zgolj) »velik biznis«.

Na eni strani je internet »medij« reklamiranja dobrin »stare ekonomije« in kanal njihove prodaje,[6] vse bolj pa je tudi prodajna dobrina oziroma so to njegove posamezne »značilnosti«. Z vse večjo penetracijo[7] pa ima tudi absolutno gledano vse večji pomen.

Prodor dokazuje tudi izredna rast vrednostnega obsega oglaševanja na spletu – kjer so potrošniki, tam je denar. Leta 1998 je denimo na internet odpadlo zgolj 0,1 odstotka vrednosti oglaševanja v Evropi, leta 2012 pa naj bi vrednost trga spletnega oglaševanja znašala več kot 44 milijard evrov.[8] Vrednostni obseg internetnega oglaševanja v prvi polovici leta 2013 je denimo v Veliki Britaniji dosegel vrednost skoraj 3,7 milijarde evrov, kar je dobrih 17 odstotkov več kot leto prej.[9]

Večina zgodb o uspehu (vsaj če in kolikor je merilo ekonomski uspeh) na internetu je tako ali drugače povezanih s prodajo – samega sebe ali drugih:[10] socialna omrežja (npr. Facebook, LinkedIn, Twitter), ponudniki e-poštnih storitev, portali za spremljanje video vsebin (npr. YouTube[11]) in fotografij (npr. Flickr.

---

[3] Prav tam. Še večji je bil (splošni) skepticizem ameriškega astrofizika in strokovnjaka za internet Cliffa Stola, in to »po dveh desetletjih *online*«. Glej C. Stol: The Internet? Bah!, v: Newsweek, 27. februar 1995; na voljo je na www.newsweek.com/clifford-stoll-why-web-wont-be-nirvana-185306 (10. 3. 2014).

[4] »*While the Net is still not entirely ready for business, the pieces are falling into place.*« Neznani avtor: Battle for the Soul of the Internet, v: Time.com, 18. marec 2005; na voljo je na http://content.time.com/time/magazine/article/0,9171,981132,%2000.html (10. 3. 2014).

[5] K. Kelly, nav. delo.

[6] »Primeri« so denimo eBay, Amazon.com, pri nas Bolha.com itd.

[7] Podatki so na voljo na www.internetworldstats.com/stats.htm, za Slovenijo pa na www.ris.org.

[8] E. Dwoskin: Study: Digital Marketing Industry Worth $62 Billion, The Wall Street Journal, 14. oktober 2013; na voljo je na http://blogs.wsj.com/digits/2013/10/14/study-digital-marketing-industry-worth-62-billion/ (10. 3. 2014). Za precej bolj pesimistične (dolgoročne) napovedi (in odzive nanje) glej E. Clemons: Why Advertising Is Failing On The Internet, v: TechCrunch, 22. marec 2009; na voljo je na http://techcrunch.com/2009/03/22/why-advertising-is-failing-on-the-internet/ (10. 3. 2014).

[9] Internet Advertising Bureau: 2013 H1 Digital Adspend Results; na voljo je na www.iabuk.net/research/library/2013-h1-digital-adspend-results (10. 3. 2014).

[10] Prek prihodkov od oglaševanja.

[11] Ta domena je bila registrirana šele februarja 2005, manj kot dve leti pozneje pa jo je družba Google odkupila za 1,65 milijarde ameriških dolarjev. Na prvi pogled ogromno, a se lahko na eni strani izkaže za poceni nakup, na drugi pa nosi tveganje usode ponudnika video vsebin broadcast.com, ki ga je Yahoo! leta 1999 kupil za 5,7 milijarde ameriških dolarjev, danes pa ne obstaja več.

com), ponudniki različnih informacij itd. Največji generatorji dobičkov so sicer (ob nezanemarjanju fenomena socialnh omrežij) »produkti«, ki so najbolj splošno uporab(lja)ni: spletni iskalniki.

Generiranje dobička je namreč (skoraj) naravna posledica generiranja obiska, med štirimi najbolj obiskanimi spletnimi stranmi pa sta v svetovnem merilu že več let dva iskalnika: daleč spredaj pred vsemi drugimi je bil in je še vedno Google[12] – že zadnjih nekaj let se giblje okrog 67-odstotnega tržnega deleža iskanj[13] –, sledi pa mu Yahoo, in sicer na četrtem mestu splošne lestvice.[14] Približno tako naj bi glede Googla tudi ostalo,[15] glavni argument za tako pričakovanje pa je že pregovorna inovativnost te družbe.[16]

Razlog za tak uspeh Googla naj bi bil sicer predvsem posledica najbolj dovršenega iskalnika (informacij, dokumentov itd.) v milijardah datotek na internetu.[17]

Glej J. Cloud: The YouTube Gurus, v: Time, 25. december 2006; na voljo je na http://content.time.com/time/magazine/article/0,9171,1570795,00.html (10. 3. 2014).

[12] Glej www.alexa.com/siteinfo/google.com (10. 3. 2014).

[13] Glej comScore: comScore Reports Global Search Market Growth of 46 Percent in 2009, sporočilo za javnost z dne 22. januarja 2010; na voljo je na www.comscore.com/Press_Events/Press_Releases/2010/1/Global_Search_Market_Grows_46_Percent_in_2009 (24. 3. 2014); www.comscore.com/Insights/Press_Releases/2013/11/comScore_Releases_October_2013_US_Search_Engine_Rankings (24. 3. 2014).

[14] Glej www.alexa.com/siteinfo/yahoo.com (24. 3. 2014). V zadnjih dobrih petih letih sta namreč Yahoo! prehitela Facebook (www.alexa.com/siteinfo/facebook.com (24. 3. 2014)) in YouTube (www.alexa.com/siteinfo/youtube.com (24. 3. 2014)), če pa gledamo samo trg v ZDA, je pred njim tudi že Bing. Glej D. Goodwin: Google Fails to Gain Search Market Share, Bing Steals From Yahoo, 14. november 2013; na voljo je na http://searchenginewatch.com/article/2307115/Google-Fails-to-Gain-Search-Market-Share-Bing-Steals-From-Yahoo (24. 3. 2014). Za previdnost glede tovrstnih podatkov – vsi so bili pridobljeni na dan 24. 3. 2014 – družbe Alexa glej denimo M. Arrington: Alexa Says YouTube Is Now Bigger Than Google. Alexa Is Useless, v: Techcrunch.com, 13. avgust 2007; na voljo je na http://techcrunch.com/2007/08/13/alexa-says-youtube-is-now-bigger-than-google-theyre-wrong/ (10. 3. 2014).

[15] Glej denimo J. Berfield: Future Trend on the Internet, v: EZineArticles, 13. oktober 2009; na voljo je na http://ezinearticles.com/?Future-Trend-on-the-Internet&id=3276890 (10. 2. 2014).

[16] Po oceni revije Fast Forward iz ZDA je Google, potem ko je bil denimo leta 2010 četrto najbolj inovativno podjetje na svetu, leto prej pa na drugem mestu (www.fastcompany.com/mic/2010 (10. 3. 2014)), zdaj že najbolj inovativno podjetje na svetu (R. Safian: The World's Most Innovative Companies 2014; na voljo je na www.fastcompany.com/3026098/most-innovative-companies-2014/the-worlds-most-innovative-companies-2014 (24. 3. 2014)). Glej tudi N. Pečenko: Fenomen Google, v: Monitor, september 2005; na voljo je na http://www.monitor.si/clanek/fenomen-google/121789/?xURL=301/ (10. 3. 2014); neznani avtor: The Secret To Google's Success, v: Businessweek, 6. marec 2006; na voljo je na www.businessweek.com/magazine/content/06_10/b3974071.htm (10. 3. 2014).

[17] Prav tam. N. Pečenko, nav. delo: »Z 10.000 iskanj na dan v prvih tednih je v prvi polovici leta 1999 naraslo na pol milijona in do konca leta na tri milijone iskanj. Sredi leta 2000 je bilo iskanj že 18 milijonov na dan, in ko je do konca tistega leta naraslo na 60 milijonov na dan, je postalo dokončno jasno, da je Google postal najpriljubljenejši iskalnik. Tistega leta je postal tudi največji, saj je imel v svojem stvarnem kazalu že več kot milijardo spletnih strani.« Za zanimiv komentar pri-

Ta storitev iskanja je res najuspešnejša, a morda se že obeta »boljša uporabniška izkušnja«.

Trenutno namreč iskalniki bolj ali manj[18] uporabljajo iskanje informacij po znakovnih nizih (dejansko ne iščejo želene informacije, temveč želene znakovne nize, med prvimi in drugimi pa ni nujno enačaja). Tako iskanje je seveda koristno, saj omeji nabor virov, še vedno pa ponudi poleg pravih tudi veliko takih, ki uporabnikom jemljejo dragocen čas.

Zato bi bila izredno učinkovita nadgradnja, če bi lahko iskalnik iskal ne le po zaporedju znakov (in izjemoma, ob uporabnikovih prizadevanjih, po nekaterih metapodatkih), temveč po pomenu posameznih zaporedij, s čimer bi vedno izločil vsebinsko neustrezne, čeprav po znakih ujemajoče se zadetke. Iskanje bi torej v takem primeru potekalo ob pomoči že omenjenih metapodatkov, kar dobesedno pomeni podatkov o podatkih.[19] Metapodatke lahko opredelimo kot »zbir (vsoto) vsega, kar lahko povemo o kateremkoli informacijskem objektu na katerikoli ravni kopičenja (agregacije)«.[20]

Verjetno bolj razumljiva pa je definicija, kakršno uporabljajo v Agenciji Republike Slovenije za okolje:

»Metapodatki vsebujejo podatke o podatkih; obsegajo podatke, ki se nanašajo na vsebino, strukturo, kakovost, lastništvo, distribucijo, tehnologijo, namen, uporabnost in druge elemente, ki so pomembni za pravilno interpretacijo oziroma uporabo podatkov.«[21]

Več ko je v iskanje vključenih (upoštevanih) tovrstnih (meta)podatkov, ustreznejši je rezultat iskanja s stališča uporabnikovih želja (s predpostavko, da zna ta svoje želje ustrezno ubesediti/zapisati). Lahko bi rekli, da so skrajna oblika pravzaprav že orodja (iskalniki) oziroma stroji, ki »razumejo«. S tem pa smo že na področju umetne inteligence (angl. *artificial intelligence* – AI).

---

merjave prenehanja uporabe Googla s prenehanjem kajenja glej T. Krazit: One week without Google, v: CNet News, 23. februar 2010; na voljo je na http://news.cnet. com/8301-30684_3-10457892-265.html?tag=nl.e703 (10. 3. 2014).

[18] Bolj ali manj zato, ker napredno iskanje pri različnih iskalnikih že vključuje tudi nekatere t. i. metapodatke (opredelitev v nadaljevanju), iskalnik na WebCrawler.com pa naj bi po besedah snovalcev »opredelil namen iskalčevega iskanja« (www.webcrawler.com/support/aboutus?qc=web&aid=8280dd9f-f4fd-4c60-bfcc-b29c4f8efe13&ridx=1 (10. 3. 2014)).

[19] A. Kavčič Čolić: Metapodatki za trajno ohranjanje elektronskih virov, v: Knjižnica, 48 (2004) 4, str. 97–119, str. 98; na voljo je na www.dlib.si/v2/StreamFile.aspx?URN=URN:NBN:SI:doc-1CZP9E8Z&id=99152c6b-c1a3-478f-bfc8-81e8dfd48f71&type=PDF (10. 3. 2014).

[20] A. J. Gilliland: Setting the Stage, v: T. Gill, A. J. Gilliland, M. Whalen in M. S. Woodley (ur. M. Baca): Introduction to Metadata. Spletna različica 3.0; na voljo je na www.getty.edu/research/publications/electronic_publications/intrometadata/index.html (10. 3. 2010).

[21] Glej www.arso.gov.si/vreme/poro%C4%8Dila%20in%20projekti/metapodatki.pdf (10. 3. 2014).

Na prvi pogled se zdi umetna inteligenca nekaj zelo oddaljenega, a gre v praksi za kombinacijo znanosti računalništva, psihologije in filozofije, katere korenine segajo v sredino 19. stoletja, raziskave na tem področju pa so omogočile denimo tudi »izdelavo« uporabnih računalniških vmesnikov in urejevalnikov besedil.[22] Ti so tudi dober primer za učinek umetne inteligence (angl. *AI effect*), ko mnogo »pojavnosti« umetne inteligence, ko so te enkrat zelo uporabne in splošno uporabljane, ni več označenih in razumljenih kot rezultat dela na področju umetne inteligence;[23] pogosto jih pač dojemamo kot še en dosežek informacijske tehnologije.[24]

(Splošna) javnost podobno razume tudi internetne iskalnike. Tudi ti so namreč delno rezultat prizadevanj raziskovalcev na področju umetne inteligence, predvsem pa to velja za njihove (želene) nadgradnje v orodja, ki razumejo. In tu pride do v nadaljevanju pojasnjene povezave med prizadevanji razvijalcev teh (internetnih) iskalnikov na eni in raziskovalci umetne inteligence (v pravu) na drugi strani: eno »izvirnih« področij raziskovanja (uporabe) umetne inteligence je ravno področje razumevanja naravnega jezika[25] (s strani orodij, konkretno tudi iskalnikov), pravo pa je – poleg denimo medicinske diagnostike, trgovanja z vrednostnimi papirji in nadzora robotiziranih sistemov – eno tistih področij, na katerih potekajo najobsežnejše raziskave s področja umetne inteligence in na katerih se tudi zelo veliko uporabljajo njihova dognanja.

Poudariti je treba, da tudi razmišljanja o informacijski tehnologiji in pravu – v primerjavi s preučevanjem uporabe umetne inteligence na področju prava – niso nova, ne v svetu[26] ne v Sloveniji.[27] Področje prava oziroma njegovi akterji so

[22] Glej http://library.thinkquest.org/2705/basics.html (10. 3. 2014).

[23] Nick Bostrom, direktor Inštituta za prihodnost človeštva (Future of Humanity Institute) na univerzi Oxford, v: neznani avtor: AI set to exceed human brain power, na: CNN.com, 9. avgust 2006; na voljo je na www.cnn.com/2006/TECH/science/07/24/ai.bostrom/ (10. 3. 2014).

[24] Informacijska tehnologija in umetna inteligenca sta sicer neločljivo povezani, ne moremo pa ju enačiti. Na umetno inteligenco lahko gledamo kot na vrsto informacijske tehnologije, ki postaja ključna v razvoju današnjih modernih računalniških aplikacij. Glej D. L. Waltz: Artificial Intelligence: Realizing the Ultimate Promises of Computing; na voljo je na www.cs.washington.edu/homes/lazowska/cra/ai.html (10. 3. 2014).

[25] J. McCarthy: What is Artificial Intelligence, razdelek Applications of AI, 12. november 2007; na voljo je na www-formal.stanford.edu/jmc/whatisai/node3.html (10. 3. 2014).

[26] V ZDA denimo sodniki že uporabljajo računalniške programe v postopku odmere kazni, in sicer tako, da v računalnik vnesejo vse relevantne parametre primera, računalniški program pa izračuna kazen. Glej A. Završnik: Ali želite, da vam sodi računalnik?, v: Pravna praksa, št. 12/2009, str. 3. Poudariti pa je treba, da to ni primer uporabe umetne inteligence v pravu, temveč gre za program, ki vsebuje bolj ali manj zapleteno formulo za izračun oblike in višine kazni (gre torej za obliko informacijske tehnologije v pravu, ne pa za umetno inteligenco).

[27] Že leta 2000 je v Bovcu na temo pravnih izzivov informacijske tehnologije potekal seminar evropskega združenja študentov prava ELSA (glej denimo I. Vovk: Elsa Ljubljana: Seminar – Pravni izzivi

tudi v Sloveniji že razmeroma zgodaj spoznali pasti in priložnosti, ki jih ponuja informacijska tehnologija. Inovacija, o kateri bova govorila v nadaljevanju, to le še potrjuje oziroma z vstopanjem na področje umetne inteligence nadgrajuje.

2. Zakaj umetna inteligenca v pravu?

Na prvi pogled morda preseneča, da so se raziskovalci oziroma snovalci umetne inteligence zatekali na področje prava, saj je to zelo kompleksno oziroma so taka pravna besedila. Vendar pa naj bi bila ta posebno primerna za apliciranje rešitev umetne inteligence.[28]

Eden osnovnih namenov pravnih besedil je namreč posredovanje pravnih pravil, ki vsebujejo dva dela: dispozicijo in pravno posledico.[29] Dispozicija je sestavljena iz primarne hipoteze in sekundarne dispozicije, pravna posledica pa iz sekundarne hipoteze in sankcije.[30]

Pri konkretnem odločanju je ključno, da pravnik na podlagi pravno relevantnih dejstev dejanskega stanu (konkretnega, življenjskega primera) poveže pravno pravilo in dejstva življenjskega primera, s čimer omogoči uporabo pravne posledice na življenjskem primeru. V primeru uporabe sankcije pa se ustvari še četrti element, in sicer vpliv posledice, kar pomeni spremembo dejstev in okoliščin, ki izhaja iz aplikacije okoliščin v primeru izvršitve sankcije.[31] Ko prepoznamo vse štiri sestavine, ki so zlasti očitne v sodnih odločbah in pravnih člankih,[32] pa je razvidna **informacijska vrednost** vsebin, ki jih je mogoče obdelati.

Prepoznavanje informacijske vrednosti vsebin na pravnem področju ponuja številne zanimive možnosti, predvsem pa povečuje zmožnost pridobivanja in

informacijske tehnologije, Pravna praksa, št. 36/2000, str. 39). Pa tudi sicer je bilo v zadnjih nekaj letih organiziranih razmeroma veliko kongresov in srečanj na temo informacijske tehnologije in prava, denimo konferenca o e-pravičnosti in e-pravu, ki je potekala v Portorožu junija 2008, ali konferenca Informatika in pravo, ki je v drugi polovici minulega desetletja nekaj let potekala v Mariboru.

[28] M. Lah: Why is legal content ideal for AI?; na voljo je na www.tomazic.info/Why%20is%20legal%20content%20ideal%20for%20AI.htm (10. 3. 2014).

[29] M. Pavčnik: Teorija prava: Prispevek k razumevanju prava. Cankarjeva založba, Ljubljana 2001, str. 43.

[30] Prav tam, str. 43 in 44. Če povzameva še naprej: obe sestavini dispozicije opisujeta primarni (želeni) način ravnanja. Neuresničitev tega vedenja in ravnanja je opisana v sekundarni hipotezi, ki predstavlja pravno kršitev. Sankcija pa opisuje sekundarno pravno posledico, ki naj zadene storilca pravne kršitve.

[31] M. Lah, nav. delo (Why is legal content …).

[32] To velja *a fortiori* za besedila s področja kazenskega prava, kjer je pravna posledica oziroma sankcija iz predpisa več kot očitna. Prvi poskusi aplikacije umetne inteligence v pravu so zato potekali prav na področju kazenskega prava. Glej denimo A. R. Lodder, A. Oskamp in M. J. A. Duker: AI & Criminal Law: Past, Present & Future, str. 2; na voljo je na www.jurix.nl/pdf/j98-05.pdf (10. 3. 2014).

prepoznavanja pravnih vsebin ter povezovanja posameznih enot pravnih vsebin, kar omogoča razvrščanje pravnih besedil v skladu z danimi kriteriji, pridobivanje novih podatkov iz obstoječih vsebin, ustvarjanje novih vsebin, iz katerih lahko izhajajo novi podatki, ter boljše predvidevanje in tudi sooblikovanje prihodnjega razvoja pravnih podatkov.[33]

3. Pravnikovo delo in pomen dela s podatki v pravu

Osnovno delo pravnika, ne glede na to, v kakšni funkciji nastopa oziroma kakšno delo opravlja,[34] je v tem, da konkretni dejanski stan primera, s katerim se sreča in ga rešuje, podredi najbolj primernemu abstraktnemu dejanskemu stanu, ki izhaja iz zakonodaje in drugih pravnih virov, in tako ugotovi pravno posledico, ki izhaja iz konkretnega dejanskega stanu.[35] Pri tem pa nujno potrebuje podatke – o dejanskem stanu (okoliščinah konkretnega primera) in o vsebini pravnega predpisa ali drugega pravnega vira. Tako kot na številnih drugih področjih velja tudi v pravu, da so podatki bistvo, s katerim vsi delamo, in temelj našega dela, pa tudi nas samih.[36]

Čeprav je ta lastnost pravnikovega dela najbolj razvidna v sodnih in upravnih postopkih, kjer se ugotavlja vsebina posameznikovih pravic in dolžnosti oziroma se celo odloča o uporabi prisilnih sankcij zoper posameznike (kazensko pravo), pa se nič manj ne uporablja v drugih vlogah. Ko hišni pravnik zavarovalnice ocenjuje zahtevek zavarovalca po izplačilu odškodnine, pravzaprav preverja, ali je nastopil tak dejanski stan (škodni dogodek), ki upravičuje izplačilo odškodnine (pravna posledica). Podobno tožilec ob prejemu ovadbe oceni, ali so podani znaki kaznivega dejanja, in sicer tako, da na podlagi lastnega pravnega znanja subsumira konkretni dejanski stan pod abstraktni dejanski stan na področju kazenskega prava. Če bo pri tem uspešen, bo tožilec ocenil, da ima dejanski primer znake kaznivega dejanja, in se bo na podlagi dodatnih okoliščin primera odločil, ali je smotrno podati obtožnico ali obtožilni predlog.

[33] M. Lah, nav. delo (Why is legal content …).

[34] Sodnik, uradna oseba v upravnem postopku, tožilec, odvetnik, pravobranilec, pripravljavec zakonodaje ali pravnik v gospodarski družbi (angl. *in-house lawyer*).

[35] Gre za normativno konkretiziranje splošnega in abstraktnega pravnega pravila, ki ga izluščimo iz formalnega pravnega vira. Pri tem zgornja premisa vsebuje abstraktni dejanski stan, ki je pogoj za nastop pravne posledice iz pravnega pravila. Pravnik abstraktnemu dejanskemu stanu podredi spodnjo premiso, ki vsebuje konkretni dejanski stan oziroma dejstva konkretnega (življenjskega) primera, in tako izvede sklep. M. Pavčnik, nav. delo, str. 297.

[36] M. Lah: Knowledge Extraction using Natural Language Analysis; na voljo je na http://presentations.ai-in-law.com/files/AI_Knowledge_Extraction_Using_NLA.pps (10. 3. 2014).

Poenostavljeno, v praksi pravnikovo delo torej obsega analizo konkretnega dejanskega stanu in ocenjevanje, katere okoliščine primera so pravno relevantne, iskanje in identificiranje tistih pravnih pravil, ki so lahko – glede na ugotovljena pravno relevantna dejstva – relevantna za odločitev v konkretnem primeru, ter iskanje najbolj primernega pravnega pravila in posledično apliciranje relevantne pravne posledice na konkreten primer.

Pravnikovo delo torej močno zaznamujejo analiziranje, sintetiziranje, razvrščanje in ocenjevanje podatkov. Pomen podatkov za pravnikovo delo potrjujejo številne baze, ki obsegajo zakonodajo, podzakonske predpise, zbirke pravne teorije in sodne ter upravne prakse. Čeprav te pravniku lajšajo iskanje relevantnih pravnih virov, pa je obseg relevantnih virov, ki jih bo ponudil informacijski sistem, odvisen od vhodnih podatkov, ki jih uporabnik (pravnik) vnese v obliki ključnih besed. Poleg tega, da ne more biti nikoli prepričan, da ne obstaja kakšen drug pravni vir, ki ga ni našel, a je relevanten za njegovo odločitev v konkretnem primeru, mora pravnik najdene vire še vedno ročno analizirati in oceniti njihovo relevantnost za konkreten primer.

Zato porabi veliko časa predvsem za analizo in ocenjevanje podatkov, ki tvorijo podlago za odločitev v konkretnem primeru, poleg tega pa mora svojo odločitev navadno tudi pisno utemeljiti, denimo v sodbi, odločbi ali (svetovalnem) mnenju. V svoji utemeljitvi mora pravnik pojasniti postopek odločanja in opisati potek svojega dela.[37]

4. Potencialne rešitve informacijske tehnologije – elektronska vloga in elektronski spis

Že danes informacijska tehnologija ponuja dve rešitvi, ki bi ju bilo mogoče uporabiti in s tem znatno poenostaviti (in delno tudi avtomatizirati) delo (predvsem) v upravnih in sodnih postopkih: elektronsko vlogo in elektronski spis. Smisel elektronskih dokumentov (med katere uvrščamo elektronsko vlogo in spis) je v tem, da je mogoče podatke, ki jih vsebujejo, takoj elektronsko obdelati in tudi uporabiti, uporabniku pa zato ostane več časa za vsebinsko delo oziroma za odločanje o zadevi.[38] Pri elektronski vlogi in spisu sicer ne gre za uporabo umetne inteligence v pravu, lahko pa bi ju z uporabo umetne inteligence dodatno razvili.[39]

[37] Katera dejstva konkretnega primera so pravno relevantna, katere predpise je uporabil pri svoji odločitvi in kako je okoliščine konkretnega primera podredil določbam uporabljenih predpisov.

[38] P. Luin: Prihodnost sodnih postopkov – izziv za sedanjost, str. 1; na voljo je na http://presentations.ai-in-law.com/files/AI_Pravosodje_SodniPostopki.pdf (10. 3. 2014).

[39] Velja pa tudi omeniti, da elektronski dokument v smislu tega odstavka ni le elektronska kopija fizičnega dokumenta, temveč dokument, ki se v celoti izpolni in vodi elektronsko, kar omogoča takojšno uporabo podatkov, ki jih ta vsebuje.

Zamislimo si primer elektronskega tožbenega zahtevka. Sodišče prejme tožbeni zahtevek prek informacijskega sistema v trenutku, ko uporabnik klikne gumb »pošlji«, namesto v nekaj dneh. Tožbenega zahtevka ni treba obdelati v vložišču sodišča, temveč vse potrebne postopke izvede informacijski sistem samodejno: zahtevek se samodejno evidentira v vpisniku, dodeli se vložna številka zadeve, opravi pa se tudi avtomatični predhodni preizkus zahtevka. V nekaj nadaljnjih sekundah se zadeva dodeli sodniku, ki bo vodil postopek. Ta prejme zahtevek v elektronski obliki in ga lahko tudi vsebinsko obdela v informacijskem sistemu (pri čemer bi lahko uporabljal rešitve umetne inteligence, ki jih bova opisala v nadaljevanju). Sodnik, ki vodi postopek, lahko celo vrsto drugih opravil – priprava elektronskega spisa, določanje morebitnih narokov in drugih procesnih dejanj, priprava in pošiljanje vabil ipd. – opravi povsem elektronsko in le v nekaj trenutkih.[40]

Elektronska vloga in spis torej nista le digitalizirani obliki obstoječih dokumentov, temveč novi obliki poslovanja s sodiščem ali upravnim organom, ki lahko prineseta pomemben prihranek časa in denarja za vse vpletene strani (sodišče oziroma organ, stranke). Ker je za organ delo z vlogo bistveno lažje in hitrejše, se lahko za elektronsko vložene zahtevke predpiše nižja taksa ali kako drugače spodbudi njihovo vlaganje.[41]

5. Mogoče smeri razvoja umetne inteligence v pravu

Potencial uporabe umetne inteligence v pravu je velik. Osnovne možnosti pa so:[42]

1. **identifikacija sestavin pravnega pravila** – računalnik oziroma aplikacija, ki tvori del informacijskega sistema, prepozna vsebino pravnega pravila in ga prikaže uporabniku. To ima za nadaljnje možnosti razvoja informacijskih sistemov v pravu dve pomembni posledici: na eni strani omogoča, da aplikacija poudari (označi) relevantne podatke in dejstva ter pravnika na te podatke opozori, na drugi pa omogoča, da aplikacija sama poišče relevantne pravne vire za konkretno vprašanje. Kot sva že omenila, so pravni viri podlaga za pravno odločanje, kar ponuja možnosti znatnih poenostavitev pravnikovega dela. Hkrati pa je ta najbolj osnovni način uporabe umetne inteligence v pravu lahko izhodišče za razvoj obeh v nadaljevanju opredeljenih oblik, ki sta veliko

[40] P. Luin, nav. delo, str. 1.

[41] Podoben sistem je v Sloveniji že vzpostavljen, denimo pri elektronskem predlogu za izvršbo na podlagi verodostojne listine.

[42] M. Lah, nav. delo (Why is legal content …).

bolj kompleksni ter omogočata tudi veliko bolj zanimive in revolucionarne možnosti uporabe;

2. **pravno odločanje ob pomoči umetne inteligence** – v tem postopku informacijski sistem pravnika ne zgolj napoti na relevantne pravne vire, temveč mu tudi predlaga (delno) vsebino končne odločitve, ki pa jo ta sprejme povsem neodvisno;
3. **samodejno sprejemanje odločitev** – to je nadgradnja pravnega odločanja ob pomoči umetne inteligence in hkrati (vsaj trenutno) tudi najdrznejša možnost uporabe umetne inteligence v pravu. Informacijski sistem bi tako na podlagi dejstev konkretnega primera našel ustrezne rešitve pravnega vprašanja in med vsemi mogočimi rešitvami povsem samostojno izbral najprimernejšo. V bližnji prihodnosti bi bilo samodejno sprejemanje odločitev mogoče le v najpreprostejših primerih ter ne brez ustreznih človeških posegov in nadzora, mogoče pa bi bilo tudi samodejno sprejemanje odločitev na prvi stopnji odločanja, pri čemer bi se pravnik v postopek vključil le v primeru nepravilnosti oziroma pritožbe.[43]

Vse te tri možnosti so inovacijski okvir, v katerem se giblje slovenska inovacijska skupina AI-in-Law. V nadaljevanju bova predstavila konkretno inovacijo – rešitev s področja umetne inteligence v pravu, ki jo razvija oziroma jo je razvijala[44] skupina AI-in-Law.

6. Inovacij(sk)a (skupina) AI-in-Law

Doslej sva poudarila predvsem pomembnost podatkov ter vlogo informacijske tehnologije in umetne inteligence v pravu. V nadaljevanju pa bova predstavila konkretno inovacijo, ki bo (tako predvidevava) že v bližnji prihodnosti revolucionarno spremenila način pravnikovega dela oziroma, natančneje, način, kako in na kakšni podlagi pravniki sprejemamo odločitve.

Inovacija obeta, da bo pravnikom ponudila danes nepredstavljive možnosti informacijske podpore pri delu in odločanju. Umetna inteligenca bo omogočila povsem nove informacijske sisteme, ki bodo temeljili na znanju oziroma na

[43] V bližnji prihodnosti lahko pričakujemo predvsem širšo uporabo prve možnosti, v bolj oddaljeni prihodnosti pa vsaj poskuse konkretizacije druge in tretje možnosti. Čeprav zahtevata slednji precejšen miselni (in tudi etični) preskok, pa z vidika zahtevane tehnologije ne prinašata bistvene nadgradnje prve možnosti.

[44] Gospodarske razmere zadnjih nekaj let so v mnogočem zadržale smele načrte te skupine, saj tovrstnih raziskav brez znatnih finančnih sredstev ni mogoče izvajati. Upava lahko, da gre res za zastoj in da se bo projekt nadaljeval z enako intenzivnostjo, kot se je začel. Uporabljene formulacije v sedanjiku se lahko tako pogojno, glede konkretno te skupine, berejo tudi v pretekliku. Gre pa vsekakor za idejo in metode, ki niso vezane zgolj nanjo, temveč na splošni napredek na tem področju.

možnosti iskanja in povezovanja po **pomenu** pojmov, in ne na podlagi zaporedij znakov, kakor je uveljavljeno danes. Potencial te inovacije je ogromen: pravni sistem se bo korenito spremenil, predvsem v smeri večje objektivnosti v upravnih in sodnih postopkih ter posledično večje pravne varnosti. Čeprav je sama inovacija namenjena predvsem pravnikom, pa se vsi dnevno srečujemo s pravnimi (upravnimi, sodnimi) postopki, zato bo zelo verjetno korenito posegla v življenja vseh, ki v kakršnikoli vlogi sodelujemo v pravnih postopkih.

7. Tehnološka rešitev umetne inteligence v pravu

Govorila sva že o možnostih, ki jih računalniško prepoznavanje vsebin pravnega pravila ponuja v pravu: zmožnost pridobivanja in prepoznavanja pravnih vsebin, povezovanja posameznih enot pravnih vsebin, razvrščanje pravnih besedil v skladu z danimi merili, pridobivanje novih podatkov iz obstoječih vsebin in ustvarjanje novih vsebin, iz katerih lahko izhajajo novi podatki, ipd. Te možnosti temeljijo na uporabi umetne inteligence v pravu, ki izhaja iz možnosti prepoznavanja vsebin pravnega pravila iz pravnega besedila (t. i. ekstrakcija znanja).

Prepoznavanje informacij v besedilu temelji na analizi naravnega jezika.[45] Naravni jezik je poglavitni način človeške komunikacije, saj je večina informacij posredovanih (zapisanih) v enem ali več naravnih jezikih. Če želimo določiti vsebino naravnega jezika, je treba besedilo analizirati, da prepoznamo in pridobimo relevantne informacije. Ročna analiza besedil je delovno intenziven, s tem pa tudi drag in dolgotrajen proces. Inovacija na področju umetne inteligence omogoča avtomatično analizo besedila, in sicer skorajda brez stroškov in v trenutku.[46]

Avtomatična (računalniška) analiza bo potekala na podlagi posebnega semantičnega modela, ki nastaja kot plod lastnega znanja inovacijske skupine,[47] temelji pa na gramatikalni analizi besedil. Ker je razlaga besedil ločena od njihove analize, je ta tehnologija tudi povsem neodvisna od jezika besedila, uporabiti pa je treba ustrezen jezikovni korpus oziroma vnaprej pripravljeno zbirko izrazov določenega jezika oziroma kulture.

[45] Razumevanje naravnega jezika je področje uporabe umetne inteligence, ki ni lastna samo pravu, temveč je uporabna na vseh področjih, kjer je treba razumeti vsebino besedila. Za razumevanje naravnega jezika pa ne zadostuje le prenos besedil v računalniško okolje in njihovo razčlenjevanje; računalniku moramo omogočiti razumevanje vsebine besedila, kar je največji izziv (J. McCarthy, nav. delo).

[46] M. Lah, nav. delo (Knowledge Extraction …).

[47] Inovacijsko skupino konkretnega projekta AI-in-Law bova predstavila v nadaljevanju.

Zlasti v poznejših fazah bo postopek prepoznavanja informacij v besedilu mogoče večinoma avtomatizirati, v zgodnjih fazah nastanka tehnološke rešitve pa bo treba za najvišjo stopnjo natančnosti zagotoviti tudi človeški nadzor.

Osnovna baza znanja bo zbirka informacij, izvedenih iz besedil pravnih virov (zakonov in predpisov), ki urejajo posamezno področje. V primerjavi z mogočim naborom konkretnih primerov (opisov dejanskega stanu) je obseg informacij iz pozitivnega prava bistveno manjši, pri tvorjenju baze znanja pa si lahko tako privoščimo več človeških posegov (rezultate analize pred uporabo preverijo strokovnjaki za izbrano pravno področje). Pripravljeno bazo znanja nato uporabimo za vrednotenje besedil iz konkretnih primerov tako, da v teh prepoznamo (morebitno) vsebinsko povezanost z zakoni in predpisi, zajetimi v bazi znanja. Udeležencem v procesu odločanja je tako na voljo bistveno boljši vpogled v dejansko stanje, saj so posamezne navedbe v opisih dejanskega stanja ovrednotene z vidika relevantnih pravnih pravil, izpostavljene so informacije posebnega značaja, prepoznane pa so tudi – za konkretni primer – nerelevantne informacije.

V kombinaciji z rešitvijo sinteze naravnega jezika je mogoče rezultate analize in vrednotenja uporabiti tudi v samodejni pripravi osnutka odločbe, v bolj preprostih postopkih (npr. v postopkih, v katerih se za opis dejanskega stanja uporabljajo pametni obrazci) pa je mogoče zagotoviti celo samodejno izvedbo odločitvenega procesa v celoti.[48]

8. Uporabnost in obeti inovacije

Čeprav je bilo v zadnjih desetletjih na področju umetne inteligence[49] in tudi njene uporabe v pravu mnogo raziskovalnih dejavnosti, so te potekale predvsem na akademski ravni. Malokdo je prepoznal možnosti uporabe umetne inteligence v praksi, številni so menili, da umetna inteligenca ni prava poslovna priložnost.[50] Inovacijska skupina AI-in-Law pa je prepoznala možnosti uporabe umetne inteligence v pravu v komercialne namene in zato dejavno razvija različne tehnike na tem področju, ki so razmeroma blizu komercialni uporabi.[51] V nadaljevanju so predstaviljena nekatera področja, na katerih bo imela umetna inteligenca še posebno velik vpliv na pravo.

[48] M. Lah, elektronsko sporočilo, z dne 24. februarja 2010.

[49] Glej denimo www.ischool.utexas.edu/~palmquis/courses/project98/ailaw/ailaw.htm (20. 3. 2014). Obstaja tudi mednarodno združenje za umetno inteligenco in pravo (International Association for Artificial Intelligence and Law), www.iaail.org/ (10. 3. 2014).

[50] A. Tomažič in drugi: AI-in-Law Future Technologies Business Initiative; na voljo je na www.tomazic.info/AI-in-Law.htm (10. 3. 2014).

[51] Prav tam.

Na najbolj osnovni ravni umetne inteligence v pravu lahko že v bližnji prihodnosti pričakujemo informacijske rešitve, ki bodo namesto pravnika poiskale za pravni problem relevantne predpise in sodno prakso.[52] S tem bo odpravljeno dolgotrajno iskanje relevantnih predpisov, ki so podlaga za pravnikovo odločanje, hkrati pa se pravnik ne bo srečeval z negotovostjo, ali je zbral vse potrebne (in za odločitev relevantne) vire, saj bo to storila informacijska rešitev. Ta bo torej prepoznala vsebino problema in poiskala relevantne predpise v informacijski bazi, kar bo trajalo nekaj sekund, pravnik pa bo lahko takoj začel postopek subsumpcije konkretnega primera pod zakonsko normo.[53]

9. Upravni in sodni postopki

Možnosti uporabe umetne inteligence v pravu so velike zlasti v upravnih in sodnih postopkih. V upravnih postopkih bo mogoče ob pomoči umetne inteligence glede na obravnavano zadevo hitro in preprosto identificirati relevantna pravna pravila, ki izhajajo iz zakonodaje, podzakonskih predpisov, sekundarnega prava (sodne prakse in prakse upravnih organov) in priporočil oziroma usmeritev organa, ki odloča o zadevi.[54] Ob tem ne gre zanemariti dejstva, da pravniku celovita informacijska rešitev omogoča jasen pregled nad dogajanjem med postopkom, kar mu lahko olajša sestavo končne odločbe brez tveganja nehotenega izpuščanja elementov, ki sestavljajo primer, oziroma določb, na katerih temelji odločitev.[55]

Zlasti v poznejših razvojnih stopnjah informacijske rešitve bo mogoča tudi popolna avtomatizacija procesa odločanja v upravnih zadevah, pri čemer bo tisti, ki v skladu z zakonom in javnimi pooblastili odloča v zadevi, računalniško pripravljeno odločbo pregledal, in če se bo z njeno vsebino strinjal, le podpisal in odposlal. Če se z vsebino odločbe ne bo strinjal, pa si bo z uporabo umetne inteligence v pravu nadaljnje delo lahko bistveno poenostavil.

V sodnih postopkih so možnosti uporabe umetne inteligence podobne kot pri upravnih postopkih, s pomembno razliko: (vsaj v bližnji prihodnosti) v demokratičnih državah iz moralnih razlogov ne bo sprejemljivo, da bi umetna inteligenca samodejno pripravila osnutek sodne odločbe, temveč bo namenjena predvsem pomoči sodniku pri odločanju in vodenju zadeve.

---

[52] P. Luin: Uporabiti znanje – praktični rezultati uporabe naprednih informacijskih (AI) rešitev v pravu, prispevek za konferenco e-Justice and e-Law, Portorož, 1.–3. junij 2008, str. 2; na voljo je na http://presentations.ai-in-law.com/files/AI_in_Law_prakticni_rezultati_in_moznosti.pdf (10. 3. 2014).

[53] Prav tam, str. 3.

[54] A. Tomažič in drugi, nav. delo.

[55] P. Luin, nav. delo, str. 4.

Že kmalu pa bo imela umetna inteligenca pomembno vlogo pri sodnikovem odločanju glede izvedbe predlaganih dokazov. Informacijska rešitev, podprta z umetno inteligenco, bo sodniku posredovala konkretne predloge o tem, katere dokaze bi bilo treba glede na pravno relevantna dejstva ter predpise in pravila izvesti v postopku.[56] Pomembna posledica tega – poleg prihranka časa – je večja objektivnost odločitve glede izvedbe dokazov, saj je zdaj odločitev, katere dokaze izvesti, prepuščena posamezniku in njegovi subjektivni analizi primera.[57] V praksi so rezultat te subjektivnosti precejšnja odstopanja med različnimi pravniki in za stranke večja negotovost pri odločanju o dokaznih predlogih. Ustrezna informacijska rešitev lahko tako pripomore k poenotenju sprejemanja dokaznih predlogov ter predvidljivosti njihovih mogočih učinkov in posledic za postopek, kar vse posamezniku zmanjšuje pravno negotovost oziroma povečuje pravno varnost.

10. Postopki mediacije

Umetna inteligenca ponuja presenetljive rešitve v postopkih mediacije, ki postaja v zadnjih letih vse bolj priljubljen in tudi uporabljan način za alternativno reševanje sporov (angl. *alternative dispute resolution* – ADR). Z elektronsko vlogo in elektronskim spisom bi bil postopek mediacije bistveno poenostavljen, stroški mediatorja pa precej nižji, saj bi mediator porabil veliko manj časa za pregledovanje spisa in opredelitev mogočih rešitev spora. Glede na vse večji pomen postopkov ADR v Sloveniji in v svetu je umetna inteligenca z informacijsko rešitvijo, temelječo na znanju, velik potencial za cenejše in hitrejše reševanje sporov, s tem pa tudi za razbremenitev sodišč. Ob tem ni odveč omeniti, da bi ob večjem razmahu umetne inteligence v pravu stranki lahko imeli večje zaupanje v rešitev, ki bi jo ponudila informacijska rešitev, saj bi se zavedali, da je predlog avtomatiziran in objektiviziran do razmeroma visoke stopnje, posledično pa bi bil predlog v mediaciji v veliki večini primerov enak ali vsaj podoben končni sodnikovi odločitvi, ki bi jo ta sprejel z uporabo umetne inteligence v sodnem postopku.

11. Priprava predpisov

Izboljšave na področju upravljanja pravnih podatkov lahko precej olajšajo pripravo učinkovitejših predpisov. Pri pripravi zakonodaje in drugih dokumentov (npr. podzakonskih predpisov) imajo pravniki lahko posebne težave. Od njih se pri tem predvsem pričakuje, da zagotovijo vsebinsko skladnost novega predpisa

[56] Prav tam, str. 3. in 4.

[57] Prav tam.

z obstoječim oziroma z višjim predpisom, npr. zakonom, da zagotovijo notranjo skladnost predpisa, da uporabljajo enotne termine ipd. Tako delo zahteva veliko časa in natančnosti, zato so ti dokumenti zaradi časovne stiske pravnikov, za katere to ni njihovo »redno delo«, pogosto pomanjkljivi, površni in vsebinsko neustrezni.

V prihodnje lahko pričakujemo razvoj informacijske rešitve, ki bo pripravljavcu omogočila vpogled v vse relevantne pravne vire s področja svojega dela in mu samodejno ponudila vsebinsko skladne predloge sprememb obstoječe ureditve. Lahko pa bi se tak sistem uporabljal za analizo različnih predpisov in ugotavljanje njihove morebitne vsebinske neskladnosti.

Rešitev bo imela predvidoma obliko posebnega urejevalnika pravnih besedil (ali dodatka za obstoječi urejevalnik besedil, kot je Microsoft Word). Tudi v teh besedilih se bodo skrivali metapodatki o subjektih in objektih pravne zaščite, o dispozicijah in sankcijah, o hierarhičnih razmerjih, o postopkih ter instancah, o sklicevanjih in vplivih ipd., kar bo olajšalo primerjavo in usklajevanje različnih pravnih sistemov. V take urejevalnike besedil bodo integrirane tudi normotehnične smernice, skupaj s sklicevanji, pravnimi podlagami in posledicami. Ključni potencialni kupci teh storitev so predvsem države in mednarodne organizacije s svojimi zakonodajnimi službami, pa tudi založniki pravne literature.

12. Pravno svetovanje in ponudba pravnih vsebin

Inovativne storitve oziroma rešitve AI-in-Law so namenjene tudi drugim ciljnim skupinam. Zanimivo področje uporabe je lahko v odvetniških pisarnah in pri notarjih ter drugih vrstah pravnih svetovalcev. Druga pomembna ciljna skupina so ponudniki pravnih vsebin, kamor prištevamo predvsem upravljavce baz s pravnimi viri (predpisi, sodna praksa in literatura). Ti bodo verjetno ena pomembnejših skupin strank, hkrati pa bodo ravno baze s pravnimi vsebinami ena pomembnejših priložnosti, prek katere bo lahko vsa zainteresirana javnost uporabljala nove informatizirane vsebine.

Pomembna skupina potencialnih kupcev takih produktov so tudi vsi upravljavci obstoječih pravnih informacijskih sistemov, ne glede na to, kdo so končni uporabniki teh sistemov. Iskanje po pomenu (vsebini) predpisov bo imelo, kot sva že zapisala, številne pozitivne vplive na pravnikovo delo, zato bo uporaba rešitev AI-in-Law za upravljavce informacijskih sistemov in ponudnike vsebin pomembna konkurenčna prednost.

Omenjeno iskanje po pomenu seveda ni vezano le na področje prava, zato bi taka tehnična rešitev omogočila tudi nadgradnjo obstoječih spletnih iskalnikov, o kateri sva govorila v uvodu. Gospodarski potencial udejanjene ideje skupine AI-in-Law je torej v povezavi z odjemalci teh rešitev izredno velik.

13. Upravljanje tveganj v družbah

V velikih podjetjih je rešitve, ki jih ponuja uporaba umetne inteligence v pravu, mogoče uporabiti tudi v postopkih inteligentnega upravljanja tveganj, pri čemer informacijski sistem nadomesti veliko večino človeškega dela. Informacijski sistem za upravljanje tveganj lahko družbo oziroma njene odgovorne tudi opozori na morebitna novonastala tveganja, ki so posledica sprememb v podatkih, ki so podlaga za določanje tveganja. Hkrati pa tak sistem omogoča učinkovito načrtovanje tveganj.

14. Trženjske poti in ciljne stranke inovacije

Ciljni uporabniki rešitev, ki jih ponuja umetna inteligenca v pravu, so tako različni kot njene rešitve. Rešitve, ki bodo omogočale lažje vodenje upravnih postopkov (in morda tudi povsem samodejno generiranje odločb), so namenjene predvsem upravnim organom držav. Njihove koristi so očitne, od prihranka časa in zlasti tudi denarja do večje pravne varnosti in manjšega tveganja za korupcijo, kar koristi tako tem državam kot tudi in predvsem njihovim prebivalcem.

Rešitve na področju sodnih postopkov so namenjene predvsem sodnim in pravosodnim organom. Koristi teh so podobne tistim upravnih organov, vendar pa vsaj v bližnji prihodnosti ne moremo pričakovati, da bo umetna inteligenca sama vodila postopek do izdaje odločbe, sodnik pa bo nastopil v vlogi nadzornika pravilnosti in zakonitosti odločitve, ki jo bo pravzaprav oblikoval računalnik. Ob dosegu take ravni razvoja pa bi koristi, poleg finančnih, izhajale predvsem iz poenotene in skladne sodne prakse ter manjše pravne negotovosti, kar je v sodnih postopkih še posebno pomembno.

15. Programska oprema kot storitev

Predmet razvoja podjema AI-in-Law so predvsem moduli umetne inteligence v pravu. Zanje ni predvideno, da bi bili predmet prodaje ali licenciranja, saj bodo pomenili večino kapitala njihovega ponudnika. Končni uporabnik jih tudi ne more neposredno uporabiti, temveč jih je treba vgraditi v novo ali obstoječo programsko opremo oziroma informacijski sistem.

Najustreznejši način trženja in prodaje rešitev umetne inteligence v pravu se zdi pristop programske opreme kot storitve (angl. *Software as a Service* – SaaS). Ker je to razmeroma nov pristop k trženju moderne programske opreme, si zasluži kratko predstavitev.

Na splošno lahko rečemo, da pomeni pristop SaaS predvsem spletni način dobave programske opreme. Namesto da bi stranka kupila licenco za programsko

opremo, ki bi jo namestila na svoje računalnike, kupi pravico dostopa do aplikacije na strežniku, ki ga upravlja podjetje, ki je programsko opremo razvilo in dobavilo.[58] Bistvene prednosti takega pristopa so med drugim v tem, da kupcu za vzdrževanje in nadgradnjo programske opreme ni treba storiti ničesar,[59] saj ima kupec vedno dostop do zadnje različice programske opreme, tj. tiste (takšne), kakršna je na spletnem strežniku prodajalca.

Bistvo tega tega trženjskega pristopa leži v ločevanju posesti in imetništva programske opreme od njene uporabe.[60] Pristop SaaS se torej ne usmerja na dobavo programske opreme, kar je značilnost klasičnih pristopov k trženju programske opreme, temveč na opravljanje storitev naročniku, prilagojeno njegovim specifičnim zahtevam. Pravzaprav gre za neoprijemljivo storitev, ki v običajnih razmerah ne vključuje prenosa lastninske pravice na kateremkoli proizvodnem dejavniku.[61]

Gre za inovativno področje ponujanja programske opreme, ki se v zadnjem desetletju naglo razvija. V raziskavi podjetja IDC iz leta 2005 je bilo predvideno, da bo do leta 2009 kar deset odstotkov trga programske opreme za podjetja zasnovano na čistem modelu SaaS.[62] Novejše raziskave kažejo trend še višje rasti trga, kot je bilo sprva pričakovano.[63]

Za uporabo načel SaaS pri trženju tovrstnih inovacij obstajajo prepričljivi argumenti. Najprepričljivejši je ta, da je kljub pravni zaščiti (patenti) modulov umetne inteligence, ki jih bo podjetje razvilo, mogoča kraja intelektualne lastnine, če bi bila programska oprema uporabniku na voljo prek klasičnih sredstev (namestitev programa pri uporabniku). Zato je nujno, da poteka trženje te inovacije prek oddaljenega dostopa, brez možnosti uporabnikovega vstopa v varovane module umetne inteligence.

Trženje inovacije v obliki storitev sprotne analize in vrednotenja besedil pravnih virov ob vsaki njihovi spremembi bi lahko denimo potekalo na dveh osrednjih ravneh:

---

[58] A. Dubey in D. Wagle: Delivering software as a service, v: The McKinsey Quarterly, maj 2007, str. 1; na voljo je na www.mckinsey.com/clientservice/bto/pointofview/pdf/delivering_software_service.pdf (10. 3. 2014).

[59] Prav tam, str. 2.

[60] M. Turner, D. Budgen in P. Brereton: Turning Software into a Service, v: Computer, 36 (2003) 10, str. 38–44, str. 38; na voljo je na http://courses.ischool.berkeley.edu/i243/s06/readings/software-to-service.pdf (10. 3. 2013).

[61] Prav tam, str. 2.

[62] International Data Corporation (IDC): Worldwide and US Software as a Service 2005–2009 Forecast and Analysis: Adoption for the Alternative Delivery Model Continues, marec 2005, v: A. Dubey in D. Wagle, nav. delo, str. 2.

[63] Glej denimo P. M. Parker: The 2009–2014 World Outlook for Software-As-A-Service (SaaS) Applications. Icon Group International, San Diego 2008.

- kot storitev, pri kateri se rezultati analize in vrednotenja vgradijo v uporabnikovo informacijsko rešitev, in
- kot storitev, pri kateri so rezultati analize na voljo v obliki spletne baze, do katere uporabnik dostopa, kadar želi »raziskovati« pozitivno ureditev specifičnega področja ali kadar želi ovrednotiti izbrani opis dejanskega stanu.

Prva rešitev je torej namenjena predvsem večjim strankam – državnim organom in sodiščem –, druga pa upravljavcem spletnih zbirk podatkov.[64]

16. Inovacijska skupina

Ob kompleksnosti in velikopoteznosti razvoja informacijskih rešitev, ki kažejo uporabo umetne inteligence v pravu, morda preseneča, da se je takega projekta lotila inovacijska skupina iz Slovenije. Poglobljen pregled vzrokov za nastanek inovacijske (in podjetniške) pobude AI-in-Law pa pokaže, da to niti ni tako presenetljivo oziroma da je ta projekt neke vrste logično nadaljevanje preteklih uspehov že ustaljene inovacijske skupine (tudi če morda trenutno ni več enako dejavna), ki jo sestavljajo inovatorji Anton Tomažič, Matija Lah in Peter Luin. V to ožjo inovacijsko skupino (v Sloveniji) so sicer vključeni tudi partnerji iz nekaterih drugih držav (Madžarska, Italija, Nizozemska, Avstrija itd.), s katerimi so se slovenski inovatorji spoznali na različnih mednarodnih konferencah o uporabi umetne inteligence v pravu.[65]

Hkrati pa tudi ne preseneča, da so se takega projekta lotili slovenski inovatorji, saj ponuja Slovenija primerno pravno okolje za razvoj in preskus napredne rešitve umetne inteligence v pravu. V primerjavi z nekaterimi drugimi državami, ki so podjetniško in inovacijsko prijaznejše, ima Slovenija dokaj visoko reguliran pravni sistem z razmeroma številnimi pravnimi predpisi. Sodišča v Sloveniji so zelo dejavna in zato nastaja tudi veliko sodne prakse, ki pa je – tudi zaradi obremenjenih sodišč in sodnih zaostankov – pogosto notranje neskladna in zato v procesu odločanja sodnika morda manj uporabna kot bolj koherentna sodna praksa drugih držav.

Finančna konstrukcija projekta je sicer temeljila na spoznanju, da bodo rešitve, ki jih ponuja uporaba umetne inteligence v pravu, uporabnikom (podjetjem in organom) prinesle številne koristi, navsezadnje tudi finančne. Namenjene so predvsem (pravnim) osebam in organizacijam s potrebo po obvladovanju velike količine podatkov (npr. državni organi, velike gospodarske družbe, velike odvetniške družbe) oziroma potrebo po zagotavljanju kakovosti podatkov posebnega

[64] M. Lah in A. Tomažič, elektronski sporočili z dne 24. februarja 2010.

[65] A. Tomažič, elektronska pošta z dne 1. marca 2010. Primeroma glej www.aaai.org/Conferences/AAAI/aaai07.php in http://ecai2006.fbk. eu/cda/aree/index.php.

pomena (poleg državnih organov denimo tudi odvetniki, notarji, zaposleni v (zasebnem) zdravstvu in drugi upravljavci »občutljivih« podatkov).[66]

Z vidika organizacije projekta je treba omeniti, da je bila krovna družba – AI-in-Law Future Technologies, Inc. – ustanovljena v ZDA. Glavni razlog za to je predvsem v lažji in učinkovitejši pravni zaščiti tehnologij.[67] Kot sva že omenila, so predmet razvoja moduli umetne inteligence, ti pa predstavljajo programsko kodo in algoritme, zato je bila odločitev za ustanovitev krovne družbe v ZDA več kot smiselna, saj je tako intelektualno lastnino lažje zaščiti v ZDA kot v nekaterih drugih državah, vključno s Slovenijo.[68]

Omenila sva že, da je ta inovacijska skupina v preteklosti predstavila nekaj drugih inovativnih projektov, ki so na neki način začetek projekta AI-in-Law. Prvi tak projekt je podjetje IUS SOFTWARE, d. o. o., ki se od ustanovitve leta 1989 ukvarja z obdelavo in distribucijo pravnih informacij v elektronski obliki in razvojem pravne informatike.[69] Leta 1997 je tako nastal spletni portal s pravnimi viri IUS-INFO,[70] ki pa je kot interaktivni pravni informacijski sistem deloval že od leta 1989.[71]

Drugi inovativni projekt te skupine je sistem pametnih elektronskih obrazcev, ki so ga razvili v podjetju INform, d. o. o.[72] Ta je neke vrste predhodnica ideje AI-in-Law, saj so pametni elektronski obrazci[73] primer najosnovneše uporabe umetne inteligence v pravu. Projekt je namenjen širši javnosti, predvsem tudi prava neveščim posameznikom, omogoča pa preprosto ustvarjanje različnih pravnih dokumentov in vlog.

Čeprav so pametni elektronski obrazci le predhodnica umetne inteligence v pravu, so lahko tudi odlična platforma za nadgradnjo v »inteligentne elektronske

[66] M. Lah, elektronsko sporočilo z dne 2. marca 2010. Glej tudi A. Tomažič in drugi, nav. delo.

[67] Prav tam. O pomembnosti izbire »prave« države za ustrezno zaščito (konkretno patentov) glej denimo M. Milič: Kako bo Jaka služil s svojo inovacijo, v: Moje finance, januar 2010.

[68] Prav tam. Enako tudi na omenjenem sestanku na sedežu družbe AI-in-Law 19. januarja 2010.

[69] Glej www.iusinfo.si/Ostalo/oPodjetju.aspx?Id=OSCom4 (10. 3. 2014).

[70] Prav tam.

[71] A. Tomažič, elektronska pošta z dne 1. marca 2010.

[72] Glej www.informiran.si/ (24. 3. 2014).

[73] Pametni elektronski obrazec je aplikacija, ki uporabnika vodi proti cilju (ustvarjanju dokumenta, kot so denimo vloga, oporoka, izjava) ob pomoči interaktivnega obrazca, postopkovnikov, navodil in pojasnil. Ko uporabnik izbere cilj, ki ga želi doseči (npr. ustvariti želi oporoko), mu sistem postavi niz obrazloženih vprašanj, prek katerih zazna njegove želje in potrebe, nato pa nadaljnji potek postopka prilagodi njegovim odgovorom. Rezultat je zato individualiziran dokument, ki je prilagojen posameznemu uporabniku. (www.informiran.si/portal.aspx?content=o_druzbi_inform&showMenu=1&showRightFrame=1 (10. 3. 2014).

obrazce«.[74] Do te nadgradnje pa bo prišlo, ko bo v elektronske obrazce vgrajena umetna inteligenca.[75]

17. Sklep

V tem delu sva predstavila primer tehnološke inovacije in njeno konkretno uporabnost v pravu.

Čeprav se zunanjemu opazovalcu, zlasti nepravniku, lahko zdi, da gre le za inkrementalno inovacijo,[76] pa gre za prebojno inovacijo v pravem pomenu besede. Taka inovacija bi v pravnem sistemu, predvsem v konkretnih procesih odločanja, namreč lahko povzročila pravo revolucijo.

Rezultate uporabe umetne inteligence v pravu bomo čutili vsi, ne le tisti, ki delujemo na področju prava. Fizične dokumente bodo zamenjale elektronske vloge, odločitve upravnih organov pa bodo takojšnje, saj bo računalniški sistem sam sprejel potrebno odločitev. Šele v primeru pritožbe bo odločitev preverila uradna oseba, seveda znova z uporabo informacijskega sistema.

Umetna inteligenca bo za uporabo v pravu precej bolj prelomna kot sistem »vse na enem mestu« oziroma e-VEM pri ustanavljanju podjetij in gospodarskih družb?, hkrati pa bo prodrla v vse pore družbenega in pravnega življenja. Z gotovostjo lahko trdiva, da pravo po implementaciji sistemov umetne inteligence nikoli več ne bo tako, kakršno je danes.

[74] A. Tomažič, M. Jamnik in P. Ličen: Environment and Tools for Creating Legal Documents Online, v: Palmirani, M., van Engers, T., Traunmueller, R.: The Role of Knowledge in e-Government. Wolf Legal, Tilburg 2005, str. 69–78.

[75] A. Tomažič, M. Jamnik in P. Ličen, nav. delo, str. 74.

[76] Gre za manjše inovacije, ki so pogosto rezultat krajših investicijskih in razvojnih ciklov, pri čemer je negotovost v zvezi z inovacijo manjša, cilji in rezultati predvidljivi, rezultati pa nastajajo enakomerno, brez daljših obdobij brez oprijemljivih rezultatov razvoja (R. Leifer in drugi: Radical innovation: how mature companies can outsmart upstarts. Harvard Business School Press, Harvard 2000, str. 19–20).

Law in Information Society

Summary

Foreword: The Position of Law in Information Society

Bojan Bugarič

Since the turn of the twenty-first century, the use of information technology has gradually spread to all areas of life. Computers have enabled digital recording and high-speed processing of a wide range of data while the Internet and mobile telecommunications permit rapid transfer and exchange of information over long distances. Almost every complex device now contains a microprocessor and connects to the Internet, at least to download software updates. This fundamental technological breakthrough has affected physical manufacturing, business services, personal and business communications, media, commerce, music and film industry. It has changed everything from the way people store family photos to the way they access services of the public administration. Information Society has emerged: a society in which information technology is essential for the economy, for the culture and for the private sphere, and in which the creation, transmission and management of information are becoming increasingly important cultural and economic activities.

Simplified remote communication, immediate availability of a wide range of information and interactive user interfaces have removed the technological obstacles to the exchange of information, which have dictated for centuries certain characteristics of social relations regulated by the law. The Internet, for example, has complicated the application of territorial rules of jurisdiction and blurred the line between telecommunications and media. Consequently, the law itself must adapt to the new realities of the emerging information society. The first phase of the law's adaptation to the new IT environment consisted mainly of solving problems and paradoxes that emerged when traditional legal norms first encountered the new technological circumstances. The prevailing normative approach was to apply the existing legal concepts to the new technology by analogy. Thus electronic form of documents, of communications and of signatures

has been accorded the same level of legal effectiveness as traditional written form; electronic reproduction of a copyrighted work has been equalised in legal consequences to its mechanical reproduction; the rules of classical registers of rights have been adapted for use with electronic registers; traditional rules of territorial jurisdiction have been applied mutatis mutandis to the regulation of the Internet; issuers of electronic media have been held responsible for their content in the same way as issuers of classic media, etc.

The process of adapting the law to new realities of the information society is not yet complete. The legal solutions adopted so far have often been based on (partially) incorrect assumptions about the further technological and economic development, and about the business methods to be developed on this basis. Establishing new regulation by analogy with traditional solutions is not appropriate when the *ratio* of the old normative regime is no longer relevant due to the new technologies. An essential feature of the new technological environment, which was initially often overlooked, is the tendency towards free and uncontrolled flow of all digital data, regardless of the type of information contained. By allowing direct peer-to-peer contact between any users, the Internet heralds a wide-reaching process of disintermediation. Traditional models of centralised creation and distribution of knowledge through publishers and media operators should no longer be taken for granted as they can be effectively replaced with new forms of collaborative creation and sharing. This is evident from the successful projects of open-source software development and by the spread of data transfer with P2P protocols. The decentralised nature of these phenomena goes against certain premises of the existing (monopoly-based) legal regulation; nevertheless, their use has quickly spread from a narrow circle of enthusiasts to major business and consumer users. An example of misguided legislative solutions is the enactment of legal protection of technological measures of protection of copyrighted works, as it only served to protect traditional business models of centralised distribution instead of encouraging the business to adapt to technological changes.

The possibilities for use of information technologies in the field of law have not yet been exhausted. A number of formal procedures in public administration and before courts could be simplified using electronic communications, which could enable the clients to perform various tasks remotely. The Internet can facilitate a wider and easier access to electronic registers of rights and legal facts, and to various official texts generated in the public sector, thereby increasing transparency in the functioning of state bodies. It should not be overlooked, however, that in addition to opportunities, the widespread use of information technologies also opens up new risks. Internet access to public databases, for example, increases the possibility of malicious intrusions and abuse of the collected personal data.

Over-reliance on the use of information technologies in official proceedings, e.g. by requiring that particular applications may only be submitted in electronic form, can raise pointless barriers to persons who lack technological knowledge or simply mistrust electronic form. In any case, the introduction of electronic procedures should not serve its own purpose, but should bring clear advantages, taking into account the potential risks and drawbacks. Apart from purely technical or legal challenges, the lack of trust into new technologies is also a relevant factor that should not be overlooked. This is particularly important in relation to electronic or Internet elections, where the technical possibilities for abuse and distortion of results are in fact more limited than with classical methods; however, they can only be detected by computer experts, while the traditional paper ballots could in principle be manually counted by any citizen, thus verifying the election result. To ensure democratic legitimacy of electronic or Internet election, an adequate level of public trust into such procedures and technologies needs to be reached first.

Completely new legal issues inherent to the new technological environment also arise in information society and are often covered only by self-regulation of information service providers. These include the regulation of the Internet and electronic communications as the basic information infrastructure, Internet domain name rights, the setting of Internet standards and protocols, and the exploitation of patents and technologies encompassed by such standards. Further legal issues relate to new phenomena and services that did not exist before the advent of the Internet, such as web search, cloud computing and software as service, social networks, online forums, virtual currencies, hacker attacks on closed systems and distributed denial-of-service attacks. An important issue concerns the rights of users in relation to Internet access providers on the one hand and the state on the other. Due to the growing impact of information technology on individuals' lives, the legal regulation in this area increasingly touches upon issues of human rights and the democratic structure of the society as a whole.

In order to exploit effectively all the opportunities of the information age, it is necessary to review constantly the adequacy of the existing regulation. However, legislative changes are not always necessary for the legal system's adaptation to new technological circumstances, since adequate solutions are often developed in the legal practice. For this reason, it is of paramount importance for the legal theory to detect the outstanding issues in time and to provide answers to them adopting a broader systemic view, which often eludes the everyday legal practice. Legal professionals, due to the nature of their profession, are usually somewhat conservative in their approach to new issues and try solving them by applying established legal solutions or avoiding altogether the issues they do not fully understand. A common preconception among legal scholars is that legal issues of

the information society encompass particularly the regulation of new technologies, especially the electronic communications and IT. However, as shown above, outstanding legal issues go beyond that, since the use of information technologies also raises new questions in the traditional fields of law. The present monograph provides an overview and an in-depth discussion of selected legal issues of the information society that have previously not yet been adequately studied in the Slovenian legal theory. Nevertheless, it is clear that we have only started unveiling the view of a broad field of legal challenges raised by the modern information society.

I. Private Law Issues of the Internet

The Liability of Internet Intermediaries
Matija Damjan

The content available on the Internet may violate various legal norms (e.g. intellectual property rights and personal rights) and thereby cause damage. Internet service providers and other Internet intermediaries, due to their technical role in the transmission and storage of information, have a certain degree of control over third parties' content. The key question is when and to what extent such intermediaries should bear the responsibility for the damage, and to what extent the liability should lie with the original content providers. The article discusses the main reasons for and against Internet intermediary liability. The general rules of European and Slovenian law on intermediary liability are presented, which distinguish between three types of information society services: mere conduit, caching and hosting. Certain open issues are discussed concerning the required speed of action, the validation of a takedown notice, the hyperlink liability and the new challenges posed by the Web 2.0.

Civil Liability for Anonymous Internet Comments in Slovenia
Špelca Mežnar

Recently, anonymous comments on the Internet have become a widespread and problematic phenomenon, requiring a clear and stricter legal regulation. Unfortunately, commenting on different Internet portals, blogs, forums and social networks is often misused to express frustration, hatred, prejudice, insult and accusations, as well as to spread hate speech. This raises the question who – in addition to anonymous Internet users themselves – should be held legally liable for the damage caused by anonymous commentators. The starting hypothesis is

that the legal responsibility for the Internet comments may be compared substantively to the responsibility for print media readers' letters. It is undisputed that the primary responsibility for the unlawful content is borne by the authors (web users) themselves. However, as it is currently almost impossible to identify anonymous writers of Internet comments, it is even more important, for the protection of the victims, to establish the potential liability of other persons who enable, promote or benefit from Internet comments: web editors, publishers and web site owners. The aim of this article is therefore to establish who, according to the Slovenian civil law, may be held jointly and severally liable for damage caused by unlawful commenting. To achieve this, the law and practice of Slovenian legal system is analysed. In addition, case law of the Court of Justice of the EU and the European Court of Human Rights is studied, with a special reference to 2013 Delfi judgment confirming the civil liability of news website publishers for anonymous user comments.

Certain Legal Aspects of (Misleading) Online Advertising

Peter Grilc

The web has brought about a series of new advertising practices, especially through expanded possibilities for interaction with the addressees of the ads. Apart from advertising, the web tackles a range of other areas of law, e.g.: private international law, copyright, antitrust, contract law, consumer law, the law of personal rights, criminal law, administrative law, regulation of various regulated markets and regulated products. The article is mainly focused on the issue whether online advertising should be treated differently than advertising in other media. Legislative models and methodologies in comparative law (an exhaustive list, a general clause, tort, passing-off), used separately or combined, are flexible enough to successfully enforce protection against misleading or other unfair advertising. Several types of online advertising increase the possibilities for unfair practices. Special legislation partly or wholly focused on web problems has already arisen in certain countries and it is likely to be upgraded in the future in order to regulate thus far unregulated areas of advertising, especially in relation to consumer protection. The article also stresses the importance of self- regulation.

Data Protection in the Online Environment

Maja Brkan

One of the biggest challenges of modern society is an effective protection of privacy and personal data of Internet users. Protection of personal data is one of the areas that has not only attracted the attention of lawyers, but also the general public, notably after Snowden's revelations of NSA activities as well as after

the reported spying on German Chancellor's mobile phone. A phrase "Google knows everything" is often used to express the omnipresence and the influence of this search engine on our everyday lives and of its knowledge about its users. For example, the search engine can create a profile of each consumer by virtue of the collection of personal data, which is then used for selective and targeted advertising. Hence, what is the price that we are paying for being constantly connected in an online world?

The article examines the legal bases for data protection currently in force in the EU and addresses the issues of necessity and the adequacy of the recently proposed reform of this legislation. The early case law of the Court of Justice of the EU in this regard (C-101/01, Lindqvist; C-524/06, Huber; C-553/07, Rijkeboer; C-73/07, Satakunnan Markkinapörssi and Satamedia) as well as the more recent case law of this court is analysed. Hence, the controversies around the legality of the Data Retention Directive as well as the much-debated cases C-293/12, Digital Rights Ireland, and C-594/12, Seitlinger et al. are discussed. The article also assesses the issues of privacy and data protection through the perspective of the currently pending case C-131/12, Google Spain and Google and puts this case into a broader perspective of fundamental rights protection.

II. Intellectual Property in Information Society

Digitalization and Orphan Works

Maja Bogataj Jančič, Jernej Pusser

Digitization enables easier access to world knowledge, which is available in libraries, museums, galleries, archives and other cultural heritage institutions. Not only is digitization an important means of ensuring access to world knowledge and its use, it can also, in some cases, be the only way to preserve world knowledge for future generations, and is thus of great importance. One of the main problems in digitization is the issue of copyright. Copyrights must be cleared, before a digitized work is published. This can be a great hurdle, if the copyright owners of a work cannot be found or identified; such works are called orphaned works. The European Commission, in its effort to encourage digitization and enable mass access to European cultural heritage, has enacted the Directive 2012/28/EU on certain permitted uses of orphan works, which not only does not solve the problem of orphan works, it also increases it. It sets conditions for the use of orphan works, which will cause enormous costs for institutions involved in their digitization as well as cause legal insecurity. The Directive does not

meet expectations and presents merely a bad compromise, which causes more problems then it solves.

Certain Copyright Issues Concerning the Establishment of a Digital Repository at the University of Ljubljana

Miha Juhart

University is an environment where new knowledge is being created continuously. The intellectual creations produced comply with all criteria of copyrighted work. The university's mission is to distribute knowledge and thus enhance the conditions for new creation. Online publication enables fast, easy and efficient access to scientific texts and thereby significantly alters the relationships previously based on printed publications, which have created a special position of publishers as economic operators with a monopoly on knowledge distribution. The principle of open access helps spread knowledge by providing scientific and research publications on the Internet without subscription or copyright restrictions. In the academic world, open access is implemented in the form of open scientific and professional journals as well as digital repositories that publish works of university lecturers and students. Such repositories are an excellent benchmark for quality of a university, since they reveal its entire scientific and research work. This is especially important for a public university, which fulfils its mission and justifies its social role through such presentation.

Two main methods of open access can be identified. The so-called green open access (or self-archiving) means that authors upload their contributions to the digital repository of their home institution prior to or simultaneously with its publication in a scientific journal, but the text becomes openly accessible only after an embargo period. Another method is the gold open access, under which the first publication of a scientific works already complies with the conditions of open access. For publication in open access mode, the copyright and related rights on the work in question have to be cleared first. The article discusses the problems of obtaining appropriate rights for open access publication in the system of University of Ljubljana and its digital repository (RUL). The copyright issues of RUL are closely linked to certain specific characteristics of the university's operation. A special legislative regulation of this area might be in place in order to find an appropriate balance between the interests of authors and the public, both in terms of access to knowledge as well as quality assurance in higher education. The purpose of university repositories to take on gradually the task of university libraries should be taken into account.

Legal Protection of Databases – Selected Legal Aspects

Jure Levovnik

In the European Union, legal protection of investments in the creation of databases is based on one of the most curious institutions of intellectual property law, the so-called *sui generis* right which comes into existence if the creation of a database has resulted from a substantial investment and which, to a certain extent and with certain limitations, prohibits third parties from taking actions that could unreasonably prejudice the database maker's legitimate interests related to such investment. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases introduced this exclusive right with the aim to foster investments in the production of databases as advanced information storage and processing systems. This article discusses, to a limited extent, some of the fundamental aspects of legal protection based on the *sui generis* right, namely: legal definition of a database, conditions for the emergence and ownership of the *sui generis* right and content and infringement of the *sui generis* right. As will be demonstrated, the regulation of the *sui generis* right is very vague in several respects and leaves a lot of room for different interpretations. For instance, the broad definition of the term 'database' could potentially allow for the protection of compilations, which are not understood as databases in common language. Furthermore, the condition for the right to become existent (substantial investment) is designed in a way that gives the courts a broad range of options to justify either existence of non-existence of the right and to take into account specific characteristics of a database at hand. A similar finding applies to the infringement test, as the existence of an infringement depends on whether or not the conduct of a third party causes detriment to the substantial investment of the rightholder. The article concludes with a short overview of certain practical aspects of the *sui generis* right enforcement in the context of which it also presents how diligence (and also ingenuity) of the database maker already in the phase of creation of a database can significantly affect the subsequent successfulness of proving the existence, ownership and infringement of the *sui generis* right.

Three-Dimensional Printing and Intellectual Property Rights

Matija Damjan

Three-dimensional (3D) printing is a manufacturing technology that significantly simplifies the production of various three-dimensional physical objects, including complex products with movable internal parts. The spread of low-cost 3D printers will enable the consumers to produce on their own many useful or artistic objects. The article discusses how the possibility of reproducing existing artworks or commercial products with 3D printing is compatible with the

protection of such objects under intellectual property (IP) law. None of IP rights (copyright, patent, design or trademark) applies to all types of three-dimensional objects, so we cannot speak of a general system of their legal protection. This differs from the situation with purely digital goods, such as e-books, music, films or computer programmes, which are all primarily subject to copyright (and may additionally be covered by other IP rights). Consequently, it has to be ascertained separately for each three-dimensional object whether it is legally protected at all and by which type of IP rights.

The exact scope of permitted reproduction of protected objects with 3D printing depends on the type of IP right in question. Nevertheless, a general conclusion is that a private individual may reproduce any object with 3D printing without breaching any IP rights, as long as its use is limited to private non-commercial purposes. Under copyright law, an individual may even engage a commercial provider of 3D printing to produce for him a private reproduction of a copyrighted object. Companies and other legal entities, on the other hand, face more restrictions in 3D reproduction of protected objects, even for their own purposes. Generally, the 3D reproduction of protected objects for commercial use, such as the sale of reproductions to consumers, is not permissible. However, the production of spare parts for commercial products is allowed under patent and industrial design law, subject to certain conditions. These exceptions set out a clear outline of legitimate use of the new technology, thus releasing the producers of 3D scanners and 3D printers of any liability for contributory infringement of IP rights in the reproduced objects.

A specific issue is the permissibility of digital dissemination of virtual CAD models that can be used for 3D printing of protected objects. In copyrighted objects, a CAD model can be considered a reproduction of the protected object and its dissemination may violate the author's making available right. In relation to patents, trademarks and industrial design, however, an infringement occurs only if the protected object is physically produced, while merely producing and disseminating CAD files does not violate the original manufacturers' exclusive rights. In case any right holders' claims are directed against the operator of a file-sharing website where CAD files are available, the operator can rely on the safe haven provision of Article 14 of the Electronic Commerce Directive. To establish the operator's liability based on the actual knowledge and active inducement of the infringement, the claimant would have to prove both that the violation of his rights by 3D printing has actually occurred and that the operator's intent was to bring about such an infringement. Due to the relatively wide scope of legitimate use of CAD models, the success of such claims seems unlikely.

III. Procedural Issues in the Internet Environment

E-commerce and International Jurisdiction over Consumer Disputes

Aleš Galič

The Brussels I Regulation protects the consumer, who is regarded as economically weaker and less experienced in legal matters than the other party to the contract, by rules of jurisdiction more favourable to his interests than the general rules of jurisdiction. The special jurisdictional protective regime, however, does not extend to all types of consumer contracts. In addition to contracts for sale on instalment credit terms or combined with a consumer credit, it applies only in cases where the trader pursues commercial or professional activities in the state of the consumer's domicile or directs such activities to that state by any means and the contract falls within the scope of such activities. This requirement gives rise to the question whether (and if, to what extent and under what conditions) it can be established that the trader who is (either directly or through intermediaries) present on the Internet "directs commercial or professional activities" to the country of the consumer's domicile.

In 2010, the Court of Justice of the European Union delivered a landmark decision in joint cases of Pammer and Hotel Alpenhof, in which it clarified this dilemma to a certain extent, but not fully. Inter alia, it clarified that the mere accessibility of the trader's or of the intermediary's website in the Member State where the consumer is domiciled is insufficient in order to establish that the trader directed commercial activities to the country of the consumer's domicile. It must be apparent from his (or the intermediary's) website and the trader's overall activity that the trader was envisaging doing business with consumers domiciled abroad. In order to enable such a conclusion, the CJEU provided a non-exclusive list of circumstances, which can be relied upon in order to establish such intent of the trader. The question however is whether this list is not so broad that at least one of the circumstances will inevitably be fulfilled in most cases of trader's presence in Internet.

Following the aforementioned CJEU judgment, numerous new dilemmas appeared. In the Mühlleitner judgment, the CJEU clarified that in order to establish that by engaging in marketing on the Internet the trader directed its activities to the Member State of the consumer's domicile, it is not necessary for the contract between the consumer and the trader to be concluded at a distance. Additionally, in a rather controversial judgment in the Emrek case, the CJEU extended the applicability of the aforementioned provisions and principles even if no causal link exists between the means used to direct the commercial or

professional activity to the consumers' Member State, and the conclusion of the contract (e.g. cases where the consumer wasn't even aware of the trader's presence on Internet in the time of conclusion of the contract).

By analysing of the aforementioned judgments of the CJEU, the author critically assesses whether the Court has not in fact extended the limits of consumer protection beyond what the drafters of the Brussels Regulation wanted (and perhaps beyond what is needed) and whether this will necessarily apply to the construction of the Rome I Regulation as well. Concerning the language of the website as an indication of the trader's intention to direct its commercial activities to the country of the consumer's domicile, a danger also exists that both the traders as well as the consumers from the Member States with "small languages" will be discriminated against.

Defamation and the Violations of Privacy via the Internet Under Eu Private International Law

Jerca Kramberger Škerl

In the article, defamation and the violations of privacy committed via the Internet are studied from the point of view of EU private international law. The author describes the current problems in this field arising from the fact that usually a number of courts have jurisdiction to decide such cases and, moreover, from the absence of a unified conflict of laws rule on the matter.

More than one court having jurisdiction over the same dispute is not unusual or per se problematic; on the contrary, this should enable the most appropriate court to decide the case. But in a situation where there is no common conflict of laws rule, each of the competent courts will apply their national conflict of laws rule to determine the applicable substantial law, according to which the dispute will be resolved. Plaintiffs are thus most likely to choose the court that will, under its national conflict of laws rule, apply the law under which the plaintiff is most likely to, firstly, win the case, and secondly, be awarded the highest damages. Such a situation is also called 'forum shopping', or, as regards defamation, 'libel tourism'.

Even though the damaged party usually enjoys special legal protection, a fair balance must be struck between the procedural (and consequentially substantive) rights of both parties. This balance is very hard to find in the field of defamation and privacy, since it is inseparably connected with striking a balance between freedom of speech, on one hand, and personality rights, on the other, all of them being fundamental rights protected by the constitutions of EU Member States, as well as the European Convention on Human Rights and the EU Charter of Fundamental Rights.

The jurisdiction of EU courts (in cases where the defendant is domiciled in the EU) is determined by the Brussels I Regulation, specifically by the rule on jurisdiction for non-contractual obligations. Over the years, the CJEU has devoted great effort to interpreting this rule in such a way that the particularities of violations committed via the Internet (or, before that, other 'mass media', such as television or the press) sought after. The ultimate solution would naturally be the unification of substantive rules, but this still seems to be very far away.

Electronic Service of Documents

Neža Pogorelčnik

The development of information technology and technical devices and, as a consequence, increased use of the Internet caused a requirement for legal regulation of electronic commerce and of electronic service delivery as a part of it. The article first presents the development of legal regulation of electronic commerce at the international, European and Slovenian level. The author discusses the regulation of electronic service delivery according to Slovenian Civil Procedure Act and its comparison to the relevant rules in criminal and administrative proceedings. Special attention is paid to the legal fiction of service, when the addressee does not pick up the electronic legal document waiting in the secure electronic system, and the problem of running 15-day period in which he or she has to do so. The introduction of electronic form of service into court proceedings will simplify the administration of the courts and will make the service more transparent, cheaper, faster and more reliable. On the first glance, there are many advantages of electronic form of service, but only after it is applied in practice, the disadvantages will be seen as well.

IV. Information Technology in the Field of Public Law

The Extent of Online Gambling Regulation

Katarina Zajc, Neža Muhič, Luka Markelj

Online gambling is the fastest growing service in the EU, with an annual growth rate of 15% and estimated 2015 revenues of 13 billion EUR. With the development of new technologies, especially the Internet, gambling has acquired a huge market, so that today online gambling is accessible to ordinary consumers of all segments of the population. With the availability, or better yet intrusion, of gambling into the homes of consumers, online gambling has been characterized as normal, acceptable and morally uncontested. However, gambling is not only

fun, but also a source of various risks, for example addiction, fraud, money laundering, etc. It is these very risks of (online) gambling that cause a need for strict legal regulation of gambling in individual countries. The aim of this article is to present legal regimes of online gambling in the EU Member States through the prism of the judgments of the Court of Justice of the European Union and the principles of the internal market with the application to the Slovenian regulation of online gaming, with a focus on issues arising from the implementation of the national legislation relating to the Internet.

Some Legal and Economic Aspects of Virtual Currencies

Meta Ahtik

In the recent period, several virtual money schemes have appeared. It is possible to treat them as a natural part of the development of digital and virtual world; however, it remains difficult to predict how long they will last. Anyhow, they will probably influence the development of money and legal theories of money. None of the virtual currencies fits into the prevailing legal theory of money, although they might, in case a certain scheme expands and its money becomes widely used, correspond to the social theory of money – a theory that has recently gained importance among legal scholars. Virtual currencies are close to the economic theory of free banking, according to which every bank can issue its own private money and the free market determines which one survives. Nevertheless, history has proven that free-riders wanting to benefit from the free-banking system of the 19th Century in the United States managed to destroy it.

Though gaining importance, virtual currency schemes encompass the amount of means that corresponds to only 0.1% of the euro area M3. Nevertheless, several law disciplines are affected by the use of virtual currencies, especially bitcoin, that remain most common subject of virtual currency regulation. Most countries have decided to tax the income from trading or acquiring bitcoins. Similarly, many countries demand from their companies to implement measures for prevention of money laundering and financing of terrorism, while licensing of bitcoin trade platforms remains less common. Slovenia has adopted first two solutions, while no a priori regulation of bitcoin exchanges exists so far. Warnings issued at the EU (European Banking Authority) and Slovenian (Bank of Slovenia) level should be preferably supplemented with a certain level of regulation, especially due to the fact that virtual currencies, namely bitcoin, exhibit several speculative patterns.

The User of a Mobile Device – A Victim of a Crime or Its Perpetrator?
Sabina Zgaga, Blaž Markelj

The use of mobile devices, especially in business environment, can also be relevant from the viewpoint of criminal law. This has become of even greater importance lately due to the increased use of mobile devices and thereby access to sensitive data and especially due to the exponent growth of threats to mobile security. The assessment whether a user of a mobile device should be considered a perpetrator or victim of a criminal act in a situation when he or she accesses the protected data in the information system of an organisation by not using the mobile in a proper and prescribed manner, and thereby potentially also causes unlawful access to protected data for others, should be made through the application of the elements of the general definition of a criminal act. As always in a case of criminal responsibility, it should be established whether in a concrete case the definition of a criminal act is fulfilled, whether the act is in fact unlawful and whether the perpetrator acted with guilt. To make this assumption, several questions should be answered, such as whether the user was aware of threats to mobile security and of the prescribed manner of use of the mobile device and whether there is any regulation on proper use of mobile devices inside the information system of the organisation at all.

First part of the article therefore presents the information security aspect and focuses on the growth of use of mobile devices, the different aims of using mobile devices and the awareness of threats to information security and proper protection. Based upon the first part, the second part of the article then discusses potential criminal responsibility and tries to draw a line between the victim and the perpetrator of a criminal act. In connection with this, it defines relevant criminal acts for which the user of mobile devices could be held criminally responsibly, the issue of merger of offences, the prescribed duty of action or omission of the user of mobile devices and especially the relevant forms of guilt and the relevance of his potential mistake of law.

V. The Influence of Information Technologies on the Legal System

Internet Access as a Fundamental Right
Matija Damjan

The Internet is fast becoming a cornerstone of the information and communication infrastructure of modern society; therefore, it is an important tool

for the exercise of human rights and fundamental freedoms. Any state-mandated limitation of an individual's Internet access thus interferes severely with the person's constitutional rights. The article deals with the conditions for admissibility of such measures in the light of the decisions in the French HADOPI case. The state can also interfere with the freedom of the Internet by blocking certain websites or IP-addresses. Blocking does not prejudice only the content providers' rights, but also limit the users, as they can no longer access any part of the Internet. Freedom of expression includes the freedom to receive information, so the censorship of websites affects not only content providers, but also the general public. The author finds that protecting the Internet just as a mere means for the realisation of human rights is not sufficient anymore. The freedom of the Internet itself should be constitutionally guaranteed as well.

Online Publication of Judicial Decisions and Its Impact on the Case Law

Lojze Ude

Internet databases of case law, especially if they contain all decisions of the Supreme Court and of all higher courts in Slovenia, affect not only the reasoning of judicial decisions, but also the very substance of judicial decision-making. The rules on revision as an extraordinary legal remedy in the current Civil Procedure Code list among the criteria for the admissibility of revision such terms as "to ensure legal certainty", "uniform application of the law", "development of the law through case law", "departure from the case law of the Supreme Court", "lack of case law" and "lack of uniformity in the Supreme Court's jurisprudence". This demonstrates that the case law is of the utmost importance for the admissibility of this extraordinary remedy. For this reason, it is also of utmost importance that as many court decisions are published as possible, as this allows the determination whether a revision is admissible in a particular situation.

Before 1978–1980, significant parts of civil law (e.g. obligations law, tort law, property law and even the enforcement procedure) were not regulated by valid legislation in Slovenia, thus there were a number of *quasi lacunae* that had to be filled by the courts. Thus jurisprudence exercised a creative function in the formation of the law and was not limited to its interpretation. After the adoption of new legislation, this role of jurisprudence was reduced. Nevertheless, the new regulation of extraordinary judicial review in combination with online databases of the courts' decision have once again increased the importance of case law. Currently, the Supreme Court publishes online all its decisions, while higher court publish only the important decisions. However, the publication of judicial decisions is not legally compulsory, as for example in Germany. The names of the parties and of the judges are not listed.

A study of current case law in the field of insolvency has shown that the case law regarding individual institutes or statutory provisions is often inconsistent. It seems that the publication of a small number of judicial decisions does not lead to attempts to unify the case law. It is therefore only possible to speak of coherent case law once the number of published decisions representing a certain interpretation of law increases. The Supreme Court should adopt a more active role in unifying the jurisprudence, either through extraordinary judicial review or by adopting an opinion of principle. It is clear that online publication of judicial decisions and following of the case law established therein is useful both to ensure the equality of parties before the law and the rule of law itself. However, some general rules on the manner of publication of judicial decisions are necessary. Except in cases personal, business or official secrecy, there is no reason to delete the names of natural or legal persons in judicial decisions prepared for publication. In any case, the names of all the judges who participated in the decision should be published.

Artificial Intelligence in Law

Andrej Grah Whatmough, Boštjan Koritnik

At the heart of every lawyer's job lies 'normative concretization of a general and abstract legal rule that can be discerned from the formal legal source' - subsuming facts of the case at hand to the most suitable abstract premise which is apparent from legislation and other legal sources, which enables the lawyer to determine the legal consequence(s) that result(s) from the facts of the case at hand. In doing this, the lawyer relies on data – data concerning the circumstances of the case at hand as well as the provisions of legal acts or other legal sources.

This paper deals with the project of a group of Slovenian innovators, the purpose of which is to use knowledge-based information systems to drastically change the legal system, especially with a view of providing greater objectivity in (legal) administrative and court procedures, and thus providing a greater degree of legal certainty.

As presented in the paper, the potential of using artificial intelligence in law is considerable. Namely, artificial intelligence could be used to (1) recognise the constituent components of legal provisions, as (2) an aid in legal decision-making, finally culminating in (3) automated decision-making – the boldest (for the time being at least) potential use of artificial intelligence in law.

In the near future we may in particular expect broader usage of the first possibility, while in more distant future, attempts, at least, at concretization of the second and third possibility. Although the latter two require a large mental

(and also ethical) leap, they do not, in terms of required technology, bring about substantial upgrade of the first possibility.

We believe that greater use of artificial intelligence in law has the potential to reduce the number of legal disputes, mainly due to two factors. First, disputes could be resolved early on by legal advisors and lawyers, who would, before submitting the dispute to the court, examine the solutions of the concrete question in the information system supported by artificial intelligence. Second, when disputes do emerge, mediators would be able to use the information system to search for the most suitable solution and suggest it to clients.

The benefits of artificial intelligence in law will be reaped by everyone, not merely those working in the field of law. Physical documents shall be replaced by electronic applications and administrative body decisions will be instant, as the computer system will reach the decision itself. Only in case of an appeal shall a lawyer, again using the IT system, review the decision.

PRAVO V INFORMACIJSKI DRUŽBI

Izdal in založil	IUS SOFTWARE, d. o. o., GV Založba
Direktorja	mag. Tomaž Iskra, Boštjan Koritnik
Odgovorni urednik	Boštjan Koritnik
Uredila	Vesna Fortuna
Lektorirala	Mateja Pogačar
Naslovnica in računalniški prelom	Anja Tavčar
Tisk	VB&S, d. o. o., Ljubljana
Prvi natis	300 izvodov Ljubljana 2014
Cena z DDV	38,00 EUR

IUS SOFTWARE, d. o. o.
Tivolska cesta 50, 1000 Ljubljana
E-pošta: zalozba@gvzalozba.si
Telefon: 01 30 91 820
Faks: 01 30 91 815

Spletna knjigarna:
www.gvzalozba.si