

Pregledni znanstveni članek
347.56:004.738.5:338.46

Odškodninska odgovornost internetnih posrednikov

DR. MATIJA DAMJAN,
raziskovalec na Inštitutu
za primerjalno pravo
pri Pravni fakulteti Univerze v Ljubljani

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 zahteve, so npr.:

- 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 (npr. 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 na-

¹ O tehnični zasnovi sodobnega interneta gl. Murray, str. 23–26.

stane tudi škoda.² Do kakšne odškodnine ali nadomestila je oškodovanec upravičen, je poleg splošnih pravil odškodninskega prava odvisno od specialnih pravil posameznega področja (npr. 168. člen ZASP³ 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 (npr. 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 zanj 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

² Murray, str. 47–48.

³ Zakon o avtorski in sorodnih pravicah (ZASP) (Uradni list RS, št. 21/95, 9/01, 30/01, 85–01 – Skl.US: U-I-149/98-36, 43/04, 58/04 – Odl. US: U-I-200/02-12, 94/04-UPB1, 17/06, 44/06 – UPB2, 139/06, 16/07 – UPB3, 68/08).

⁴ Pogosto je ponudnik internetnih storitev označen kar s kratico ISP, ki izvira iz angleškega izraza *internet service provider*. Prim. 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.

s preverjanjem vsebin uporabnikov grobo posegala v zasebne podatke oziroma 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, npr. 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 je v Evropski uniji Direktiva 2000/31/

⁷ Prim. 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).

ES o elektronskem poslovanju¹¹ 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.

Zakon torej ne ureja samo odgovornosti tradicionalnih ponudnikov internetnih storitev (ISP), temveč precej širšega razpona akterjev, udeleženih pri ponujanju blaga ali storitev na internetu (npr. spletne trgovine), pri ponujanju spletnih informacijskih ali iskalnih orodij (npr. Google), pa

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. 57/00, 30/01, 25/04, 73/04 – ZN-C, 98/04 – UPB1, 61/06 – ZEPT.

¹⁴ Uradni list RS, št. 61/06, 45/08 – ZArbit, 79/09.

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.

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, npr. 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 npr. za vsebino spletnega portala ponudnika internetnih storitev, ki jo ponudnik sam ureja (npr. www.siol.net). Bolj zanimivo pa je vprašanje odgovornosti ponudnika storitev za podatke, ki jih *zagotovi prejemnik njegove storitve*. Zakon za te podatke ponudniku 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.

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.«

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

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

¹⁸ Tičar, Makarovič, str. 263–264.

¹⁹ 42. uvodna izjava Direktive o elektronskem poslovanju.

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 strežniku. Sem spada npr. 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

²⁰ Tičar, Makarovič, str. 267–268.

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 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.

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

²² Mazziotti, str. 168.

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 (npr. 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, npr. pred protipravnimi posegi v osebne 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 (npr. 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

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

²³ Edwards, str. 66–67.

v politične ali poslovne namene (npr. 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 (npr. 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 oz. 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 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.

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>>

Gl. tudi Nas, *The Multatuli Project ISP Notice & take down*.

- 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 npr. 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?

Odgovornost za drugega zakon predpisuje v primerih, ko neposredni povzročitelj škode dejavnost opravlja za nekoga drugega (npr. 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

²⁶ Prim. Tičar, Makarovič, str. 271.

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

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 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 (npr. 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. Upravljevec 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 vedenje 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.

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

²⁹ Edwards, str. 67. Vsebinsko 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.

V zadevi *Louis Vuitton Moët Hennessey (LVMH) v. 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 v. 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 informacijske 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 npr. 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 bojzani 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. Vzpostavljane povezav na druga spletna mesta ne konstituira gostiteljstva in z njim povezane odgovornosti v smislu Direktive o elektronskem poslovanju

³⁰ Edwards, str. 69.

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.

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 npr. prikazani rezultati iskanja s katerimkoli od internetnih iskalnikov (npr. 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 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 vrsti 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 npr. prebere samo naslov in nekaj vrstic z izbrane strani (npr. Yahoo! News) ali primerja cene (npr. 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, npr. 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 (upravljavalec spletnega mesta) nima nadzora nad legalnostjo oziroma ilegalnostjo vsebin. Odškodninske odgovornosti ni mogoče utemeljevati zgolj s spodbujanjem uporabe protokola

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. Gl. 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. Gl. Murray, str. 228–233.

P2P, saj gre pri tem za vsebinsko nevtralnno tehnologijo prenosa podatkov, ki omogoča povsem zakonite prenose velikih datotek in se v ta namen pogosto tudi uporablja (npr. 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 strani, 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 npr. 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 npr. 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.

³⁶ Edwards, str. 79. Gl. tudi Klun, str. 21. V primeru *Bumal/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. Gl. Murray, str. 247–248.

³⁷ Tičar, Makarovič, str. 281.

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 terjaja 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 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-naslava 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 Prim. Edwards, str. 82. Gl. 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 presteči, 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.