

**ОСВРТ НА ОДГОВОРНОСТ ИНТЕРНЕТ СЕРВИС
ПРОВАЈДЕРА (ИСП) У МЕЂУНАРОДНОМ
И УПОРЕДНОМ ПРАВУ**

Апстракт: На интернету се као активни учесници, са различитим улогама појављује више субјеката. Један од најзначајнијих учесника је интернет сервис провајдер (ИСП). Под ИСП-ом се подразумева сваки јавни или приватни субјект који омогућује корисницима сервиса комуникацију уз помоћ компјутерског система, као и било које друго тело које помаже при обради или складиштењу тако стечених података у име и за рачун корисника.

Одговорност ИСП-а за предузете радње на интернету, у међународном и упоредом праву, детерминисана је помоћу два кључна фактора. Као прво, узима се у обзир околност да ли је ИСП пасиван учесник (нпр. код е-mail-а), или активан учесник на мрежи (нпр. смештај или омогућавање приступа). Као друго, узима се у обзир чињеница да ли је ИСП свестан, односно има сазнање да учествује у некој недозвољеној радњи. Генерално, ИСП може бити одговоран само за дела у којима је он активно учествовао и био свестан да се преко њега одвијају незаконите делатности, а ништа није предузео да спречи њихово вршење.

Кључне речи: интернет, интернет сервис провајдер (ИСП), услуге ИСП-а, одговорност ИСП-а.

1. ИНТЕРНЕТ СЕРВИС ПРОВАЈДЕР (ИСП) - ЗНАЧАЈАН УЧЕСНИК НА МРЕЖИ

Кретање информација на интернету обухвата више врста радњи и активности, од којих су најзначајније: емитовање информација, пренос или трансмисија информација, стављање на располагање информација на интернету, пријем и коришћење информација. У том ланцу активности учествују различита лица: аутори порука-информација, издавачи web сервиса, провајдери, сервери за смештај или web сервери, приређивачи on-line сервиса, web администратори, оператори на телекомуникацијама, модератори мреже. Сви они имају различите функције и сходно томе морају бити спремни да прихвате и одређени степен своје одговорности.

У најопштијем смислу, интернет сервис провајдер (ИСП) или омогућавач приступа интернету, представља посредника у пружању интернет услуга. У остваривању мисије посредништва провајдер се појављује у различитим функцијама. Стога, питање одговорности провајдера, постаје још сложеније и изазива доста полемика. Пре свега, провајдер поступа као сервер за смештај. Осим тога, он може имати и функцију обичног преносиоца информација, као и функцију релеја или преносне станице са форума за дискусију (дискусионих форума) на news сервере, са web сајтова на релејне сервере или у кеш и порука постављених од његових корисника. Провајдер може, такође, стокирати, односно складиштити информације на својим серверима. Ова функција складиштења представља део функције транспорта. Стављање у службу једног news сервера, који је инхерентан техници Useneta, омогућава кориснику врло брзо и неометано приступање форумима за дискусију на мрежи. Што се тиче web сервиса, провајдери активирају релејне сервере (тзв. проксије), на којима копирају најтраженије сајтове и где складиште информације које су већ биле коришћене. То је тзв. кеширање (caching), које корисницима знатно смањује време потребно за трансмисију, уз избегавање закрчења на мрежи.

Осим наведеног, провајдер, такође, преноси поруке емитоване и примљене од својих корисника, било да се ради о електронској пошти (e-mail) или о порукама емитованим у њузгрупама (newsgroups). Провајдер је, у свим овим случајевима, само

транспортер информација, па сагласно томе, не може бити одговоран за понашање његових корисника, дакле за садржај информација које се преносе и којима омогућава приступ. Овакво схватање се имплементира и кроз комерцијалне уговоре између провајдера и њихових корисника.

Ипак, треба истаћи да, за разлику од обичног транспортера информација, провајдер, теоријски, има техничке могућности контроле садржаја информација које преко њега транзитирају, али он неће бити у могућности да то реализује, имајући у виду количину пренетих информација, као и различиту јурисдикцију, с обзиром на међународни карактер интернета. Такође, ни један пропис експлицитно не налаже провајдерима вршење једне такве контроле. Међутим, генерално, кад је провајдер обавештен о недопуштеном садржају неке информације, он је може укинути или обуставити са свог сервера, али од њега се никако не може очекивати да буде арбитар у сукобима између различитих интереса. У сваком случају, одговорност провајдера мора се анализирати са аспекта функције коју он обавља.¹

2. ДЕЛАТНОСТ ИСП-А (ИНТЕРНЕТ СЕРВИС ПРОВАЈДЕРА) НА МРЕЖИ

Као што је већ истакнуто, провајдер се у оквиру свога деловања на мрежи појављује у различитим улогама, односно са различитим функцијама које, саме по себи, имају кључну улогу у сагледавању и дефинисању његове одговорности за своје радње.

¹ Тако, нпр. у чл. 4 Општих услова сервиса Клуб интернет стоји да: "Сервис за приступ није један информациони или телематски сервис, већ само један сервис за конекцију између опреме и серверског центра у циљу трансмисије података између мрежа у крилу интернета.". Слично прописује и чл. 9 Општих услова сервиса Wanadoo: "Француски интерактивни Телеком, неће моћи, ни у ком случају, бити одговоран за садржај тражених сервиса, природу испитиваних, пренетих и уопште на било који начин консултованих информација од стране претплатника".

2.1. Провајдер као обичан транспортер информација

Провајдер се, пре свега, може наћи у улози обичног преносиоца информација, што је нарочито случај са електронском поштом (e-mail). Тајност комуникација и неповредивост писама, не дозвољавају провајдеру чак ни да се упозна са садржајем порука, а камоли да предузима било какве мере. Дакле, провајдер је дужан, у овом случају, да се придржава обавезе неутралности, какве год биле поруке емитоване или примљене, пошто није могуће строго разлучити да ли је једна порука намењена непосредној кореспонденцији или је упућена неодређеном броју лица.

2.2. Провајдер као релеј (преносна станица) порука својих претплатника

Провајдер се може појавити и у улози стручног преносиоца (релеја) одређених порука. Тако, нпр. за учествовање у њуз групама (newsgroups) и другим форумима за јавну дискусију, корисници шаљу своје поруке на сервере својих провајдера, који ће их затим пренети другим серверима, исте природе, а ови ће их, потом, даље дистрибуирати потенцијалним примаоцима. Дакле, полазна тачка или станица јавног ширења порука почиње од сервера провајдера. Да би смо боље и потпуније сагледали одговорност провајдера размотрићемо неке значајне случајеве из савремене судске праксе.

Међу сервисима које својим претплатницима пружа провајдер CompuServe, фигурира приступ различитим јавним форумима, од којих је један посвећен новинским публикацијама. Једна од публикација - Rumorville USA, садржала је клеветничке информације. У спору који је поводом тога настао, суд је изрекао став да се није могло очекивати од CompuServe-а да прегледа сваку публикацију коју преноси, да би открио евентуалне клеветничке поруке.²

У другом примеру, радило се о објављивању клеветничких порука на један од форума Prodigy-а. Он се представио јавности са сопственом политиком издавачке контроле на својим форумима за јавну дискусију, путем специјалних софтвера за посебну филтражу

² Афера Cubby.Inc.v. CompuServe (776 F. Supp. 135 (SDNY 1991), Valérie Sedallian : Le contrôle de flux information - Le responsabilité des acteurs dans les flux des informations: <<http://argia.fr/lij/livre/respect.html>>, 17. 09. 1998. године.

протока информација. Кад је дошло до спора због клеветнички порука, суд је Prodigy-а огласио одговорним, упркос његовој одбрани да није могао контролисати 60.000 порука дневно послатих од његових претплатника.³

У Холандији је вођен поступак, јер је извесни Spaink постао на интернет документа заштићена ауторским правом. Овлашћени носиоци ауторског права тужили су 22 холандска провајдера, јер су имали активну улогу у дистрибуцији спорних докумената. Холандски суд је сматрао да провајдери нису били одговорни за дела фалсификата. Провајдер би могао бити одговоран само ако би фалсификат био очигледан и ако је провајдер знао за фалсификат.⁴

Анализирајући наведене судске пресуде, могу се приметити одређене тенденције. Пре свега, сама чињеница да неки корисник емитује недопуштене информације на интернету није довољна за активирање одговорности провајдера тог корисника. Такође, "издавач", у начелу, нема никакву дужност вршења "издавачке" контроле порука својих претплатника. Међутим, од тренутка када је провајдер сазнао или је морао сазнати да је нека порука недопуштена или повређујућа, а он није предузео ништа да спречи њено даље ширење, његова одговорност се не може више доводити у питање. При том, појам сазнања остаје фактичко питање које ће се тумачити у конкретним случајевима.⁵

Ако прихватимо став да о одговорности провајдера можемо говорити тек од момента сазнања за недопуштени садржај, чини се разумним ограничити ову одговорност на случај када се недопуштени карактер очигледно манифестује, било о каквој повреди да је реч. Уз све то, обим провајдерове одговорности треба процењивати у функцији његове управљачке власти и техничких могућности

³ Афера Statton Oakmont, Inc. v. Prodigy (NY Sup.Ct.N~ 31063/94,25. 5. 1995; Видети: Jonathan Rosenoer, Online Defamation, Cyberlaw, <http://www.cyberlaw.com>, 1995.

⁴ Scinetology b. Access providers and Karin Spaink : Le Conférence : Les autorutes de l information et le multimedia, Monaco 3, 03.05.1996. <http://www.iway.fi/groupecx/uae/Beerepoot.html>

⁵ Тако, нпр. у афери Netcom, обична нотификација титулара права о повреди његовог ауторског права, упућена провајдеру, за суд није била довољна за квалификовање "сазнања" о фалсификату.

којима располаже, да би спорну поруку "скинуо" са мреже или блокирао приступ њој или онемогућио њену даљу дифузију.

Након судских непријатности са црквом, Netsom је у опште услове закључења уговора о провајдерству инкорпорисао одредбу која забрањује коришћење постојећих сервиса преко њега за противзакониту дистрибуцију докумената заштићених правима интелектуалне својине. Netsom је, такође, разрадио читаву мини процедуру, која ће се применити, ако је обавештен да порука неког од његових претплатника наноси повреду ауторског права трећих лица.

Што се тиче Useneta-a, појављује се један други проблем. С обзиром на велику брзину ширења порука на Usenet-у, чим је једна порука послата она се налази, врло брзо, на свим news серверима, које емитује група на коју се порука односи. У том смислу, евентуална интервенција провајдера за поништавање неке поруке или ограничења њеног ширења, може се вршити само накнадно - а posteriori.

У вези са питањем одговорности провајдера када се налази у функцији релеја, треба истаћи једну значајну могућност злоупотребе, везану за ову активност, која се доста појављује у пракси. Постоји могућност да се при прослеђивању порука (relay), као аутор поруке, појави неовлашћено лице, које може да се пријави под лажним именом, или измењеним налогом (просто као н. н. корисник). Или, још флагрантнији пример, када се неко лице конектује "освајањем рачунара", и тада се не може открити сервер, са кога је порука стварно послата, а камоли лице које је послало недопуштену поруку. У том случају, је одговоран систем администратор out going mail сервера. Он треба да забрани прослеђивање порука са рачунара које нису под његовом јурисдикцијом, односно под његовим доменом, што је технички изводљиво.

2.3. Одговорност провајдера у вези са форумима за дискусију

Заједница њузгрупа (newsgroups) нарасла је данас у свету на неколико стотина хиљада. Свакодневно се на ове форуме шаље на хиљаде порука. Поступак ширења порука између news сервера је аутоматски. Али, ретки су провајдери који реемитују форуме у потпуности (интегрално). Провајдер може да бира да ли ће реемитовати или не поједину њузгрупу (newsgroup). Али, кад

прихвати неку newsgroup, провајдер не врши контролу порука постављених на форум и не проверава да ли порука одговара тематици форума. Провајдер у овој функцији није одговоран за садржај порука послатих на форум које он реемитује на свој news сервер. Али, ако је обавештен да се преко његовог канала емитују недопуштене или повређујуће поруке, а он ништа не предузима, постоји његова одговорност.

3. АСПЕКТИ МЕЂУНАРОДНОГ КРИВИЧНОГ ПРАВА

Осим већ изнетих, интернет поставља и један други тип проблема. Пошто се ради о међународној мрежи, неки документи или поруке могу бити законити у земљи емитовања, али недопуштени у земљи пријема.⁶

Француски Кривични закон (Code penal), предвиђа да ће се његове одредбе применити на дела учињена у иностранству, ако је дело кажњиво истовремено и по француском и по страном праву и ако је то констатовано правноснажном судском пресудом. Такође, француски закон је примењив и на деликте учињене од Француза у иностранству, ако постоји дуплицитет инкриминације. Исти закон прецизира да је повреда учињена на територији Француске ако је бар један од елемената везан за ову територију. Питање примене домаћег закона на web сајтове лоциране у иностранству, такође би могло да се постави. Истина, начин приступа web сајтовима је другачији од начина приступа па news. Садржај једног web сајта може бити директно репатриран преко корисника без транзитирања преко сервера провајдера, док код newsa постоји преспајање са news серверовог провајдера на провајдер корисника. Отуда, када говоримо о одговорности провајдера велику опасност и искушење представља "окретање" против провајдера, као једино познатог и једино "ухватљивог" актера у немогућности да се "ухвате" аутори порука и издавачи инкриминисаних сајтова.

На крају, изнећемо неколико мишљења неких институција о одговорности провајдера. Тако, у једном извештају Федералне

⁶ Нпр. креирање једног сајта или емитовање порука које негирају холокауст, недопуштени су у Француској, док се у САД-у и Канади оваква тематика сматра само једном врстом мишљења, која нису, а priori, недопуштена.

управе правосуђа Швајцарске,⁷ истиче се да се одговорност провајдера не може посматрати, сходно одговорности директора публикације, где је, по принципу супсидијарне одговорности, у крајњој линији провајдер одговоран за дешавања на мрежи.

На сличном становишту је и Међуминистарска Мисија о интернету⁸, која је истакла да би одговорност провајдера требало подвргнути систему општег права.

Британски Закон о клеветатама (Defamation law Act), од 1996. године, садржи одредбу која дозвољава провајдерима да се екскулпирају одговорности у случају клеветничких порука.

Најзад, амерички Закон о пристојној комуникацији (The Communication Decency Act), од 1996. године, прописује да провајдер не може бити одговоран за дифузију непристојних информација, способних да буду виђене од малолетника, за било коју активност на интернету (омогућавање приступа, трансмисија, посредничко складиштење, софтверски приступ и др.), ако таква активност не укључује стварање информационог садржаја.

На крају, сматрамо да у недостатку међународне регулентације, најбољи начин да се одговори захтевима за увођење одговорности за проток информација на интернету јесте промо-висање система уговорне регулације и подстицање усвајања система ауторегулације, односно аутоконтроле (нпр. софтверски филтери, ме-дијатори, етички кодекси и слично).

4. МЕЂУНАРОДНИ И УПОРЕДНОПРАВНИ ПРЕДГЛЕД ОДГОВОРНОСТИ ИСП-А (ИНТЕРНЕТ СЕРВИС ПРОВАЈДЕРА)

Интернет представља глобално подручје у којем се данас спреплићу озбиљни пословни интереси и захтеви за поштовањем приватности, тајности и неповредивости личне комуникације, с једне стране, и бројне могућности злоупотребе и сиве зоне правно нерегулисаних или контрадикторно регулисаних питања. Приступ контроли садржаја на интернету и одговорности за поступање на

⁷ Извештај из маја 1996. године, расположив ва интернету: <<http://www.admin.ch/ejpd/d/bj/internet/indearbf.htm>>. Скуп је одржан од 16.3.-16.6.1996. г. у Француској.

⁸ Скуп је одржан од 16.3.-16.6.1996. године у Француској.

мрежи различит је, зависно од правног система који је носилац контроле. Контрола садржаја, свакако, је блажа у земљама западне европске, односно америчке културе, док многе исламске и азијске земље имају стриктне прописе о забрањеним садржајима на серверима који припадају под њихову надлежност.⁹

Почетком деведесетих година двадесетог века започела је комерцијализација интернета и појавили су се први приватни пружаоци интернет услуга, како спајања на интернет (dial-up i leased line), тако и омогућавања простора на рачунарима (web hosting). Такви правни субјекти, деоничка друштва или друштва с ограниченом одговорношћу, познати су под америчким називом ISP/IPP (Internet Service Provider/ Internet Presence Provider). Неке од тих фирми су се на пружање интернет услуга преbacиле са пружања различитих BBS¹⁰ услуга, док су друге биле сасвим нове фирме. У том тренутку, постојало је више хиљада различитих пружаоца интернет услуга широм света. Велика већина њих своју делатност базира на неколико основних услуга о којима је већ било нешто речи:

- Омогућавање спајања клијената на интернет;
- Пружање услуге смештаја web страница и података;
- Различити облици едукације и популаризације кориштења интернета.

Кад корисници користе услуге ИСП фирме постоји могућност да ће неки од њих починити и неки од појавних облика рачунарског криминалитета, поготово оних који цветају на интернету. Због тога, многе ИСП фирме имају организовану службу која прима и обрађује пријаве различитих сигурносних инцидената везаних уз

⁹ Неке од тих земаља, попут Ирана и Кине, иду толико далеко да осим контроле садржаја на серверима у властитом домену, значи формалној “територији” унутар интернета, над којим имају надлежност, филтрирају промет властитих корисника према серверима у другим доменама, значи “слободном” интернету.

¹⁰ Bulletin Board System - врста једноставније рачунарске мреже популарне у Сједињеним државама, и Западној Европи, крајем седамдесетих и почетком осамдесетих година двадесетог века.

кориснике који користе њихове услуге и имају могућност таквим корисницима ускратити даљи приступ.¹¹

У задњих неколико година, у свету је на снагу ступило или је у поступку ступања на снагу неколико прописа који се, уз остала правна питања везана уз интернет и модерне информацијске и телекомуникацијске технологије, баве одговорношћу ИСП-а на интернету.

У том смислу, посебно место и пажњу заслужује Cybercrime Convention – Конвенција о кибернетском криминалу, потписана у Будимпешти 2001. године. Уз то, треба истаћи, да су у многим земљама донети национални прописи који регулишу ову материју. Тако, нпр., током 1997. године донети су немачки прописи Teledienstgesetz – TDG (Закон о телекомуникацијским услугама) и Mediendienstestaatsvertrag – MDStV. Велики утицај има, свакако, и француско право, а релевантан извор права у овом случају је Закон о емитовању аудиовизуелних садржаја, од 1986. године, допуњен одговарајућим амандманима 1998. године.¹²

Наравно, треба споменути и аустријско право, те осврт на рад др. Gabrielle Schmölder-а, посвећен интернету и казеном праву, у коме она посебан нагласак ставља на казнене одредбе аустријског Казненог закона (Ст.Г.Б.) и Закона о казеном поступку (Ст.Р.О).¹³

У тексту Конвенције о сајбер криминалу, након Преамбуле, дефинишу се основни појмови којима се Конвенција бави. У члану

¹¹ Такве службе (често назване “abuse” службама), у начелу, сарађују са истоврсним службама других ISP-а ради спречавања инцидента ширих размера, попут DDOS напада. Тако, данас постоје две главне категорије ISP-а, приватне фирме и различите установе, попут војске и образовних институција широм света. Начелно сви ИСП-и имају организовану службу за пријем и обраду сигурносних инцидента са овлашћењима да упозори кориснике-починиоце и ускрати им даљи приступ.

¹² То су тзв. Ammendments Fillon, од којих су два касније “срушена” након што је група сенатора предложила испитивање уставности закона (“Conseil Constitutionnel”), да испита усклађеност тих, од многих окарактерисаних као брзоплето донесених, амандмана.

¹³ Dr.sc. Gabrielle Schmölder: “Internet und Strafrecht”, “Strafrechtliche Probleme der Gegenwart”, cl. 25 1998.

Ревизија в1.1

CCERT-PUBDOC-2003- -

Страница 31/42

1, ст. 1, налази се дефиниција сервис провајдера.¹⁴ Под њим се подразумева сваки јавни или приватни субјект који омогућује корисницима сервиса комуникацију уз помоћ компјутерског система, као и било које друго тело које помаже при обради или складиштењу тако стечених података у име и за рачун корисника.

Са аспекта наше теме, свакако, је најважнији члан 12, ст. 2, који се бави одговорношћу правних лица.

Конвенција јасно захтева предузимање свих потребних радњи да се у правни поредак држава потписница унесу одредбе које омогућују вођење поступка, како против физичких, тако и против правних лица, како приватних тако и установа и државних организација. Зависно од природе почињеног дела тражи се могућност постојања казнене, грађанске и управноправне одговорности, како за правно лице тако и за одговорно лице.

Треба истаћи, да Cybercrime Конвенција представља дефинитивно остварење једног од "резон детр" Већа Европе, а то је рад на уједначењу легислативе чланица и припрему њихових правних поредака за будућност у ЕУ. Њене су одредбе дефинитивно у духу с временом, но правни поредак већине земаља је дефинитивно конзервативан, ретко кад креативан, и креће се по сопственој инерцији. Мало је симптоматична и никако похвална чињеница што је Конвенцију ратификовало тек неколико земаља. Томе у прилог иде и приличан број резерви (одредбе Конвенције које се могу, али не морају прихватити од стране држава потписница). Државе потписнице могу изреком изјавити неку од резерви, која се тада неће примењивати у њиховом правном систему, које је могуће у било које време нотификацијом истакнути (чл. 42.). Биће прилично тешко пратити у којем је тренутку која земља потписница истакла или повукла коју од резерви (а има их десетак). Тога су дефинитивно свесни и у телима Већа Европе, па су на web страницама Већа

¹⁴ "Service provider means:

- i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
- ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service."

Ревизија v1.1

CCERT-PUBDOC-2003- Страница 32/42

Европе посвећеним Конвенцији поставили таблицу потписа и ратификације, као и могућност означавања истакнутих резерви за сваког од потписника.

4.1. Стање одговорности ИСП-а у Француској

Као једна од водећих земаља континенталног правног система, али и технолошки авангардна нација, Француска се рано сусрела са проблемом регулације одговорности пружаоца интернет услуга. Пут којим је француски правни систем кренуо, састоји се у разликовању улоге фирме као пружаоца услуге спајања на интернет и улоге пружаоца простора серверима који ће нудити садржаје, које корисници поставе у облику web страница, датотека или огласних плоча (форума), заинтересованим на интернету.¹⁵

Крајем деведесетих година прошлог века, у Француској се догодио низ случајева у вези са одговорношћу ИСП-а, у којим су разна тела заузимала различите ставове.¹⁶ Коначан и заједнички закључак који је установљен је, да фирме које се баве пружањем услуга спајања на интернет нису у могућности пратити сав промет који пролази њиховим рачунарима.

Како француско казнено законодавство тражи за дела почињена помоћу рачунара намеру, то фирме пружаоци услуге спајања на интернет нису и не могу бити казнено нити грађанско-правно одговорне. Али, поставља се питање шта је с фирмама које пружају услугу простора web серверима? Ако је фирма, пружалац услуга, упозната са преступом, и не предузме мере у њеној надлежности да спречи ширење кажњивог садржаја, тада би могла бити одговорна. Горе наведени амандмани (Amendments Fillon) додали су две обавезе за фирме пружаоце интернет услуга. Фирме пружаоци су дужне својим корисницима пружити програме са могућношћу контроле приступа (parental lock), те блокирати приступ web-

¹⁵ Vallérie Sedallian: "Controlling Illegal Content over the Internet"; Излагање одржано на 26. International Bar Association Conference, у Берлину, 1996. године.

Ревизија v1.1

CCERT-PUBDOC-2003 -

Страница 33/42

¹⁶ (Union des Etudiants Juifs de France vs. Compuserve, затим Француска против FranceNet-a и WorldNet--a и други).

страницама и другим интернет садржајима, који садрже материјале који се могу подвести под неку од инкриминација из корпуса француског казненог права, у овом случају садржаног у одредбама казненог законика и већ наведеног Закона о емитовању аудиовизуалних садржаја, са припадајућим амандманима.

4.2. Немачка

И пре него је донесен Закон о телекомуникацијама (Teledienstgesetz – TDG), донесен, немачко је правосуђе заузело сличан став о одговорности провајдера, какав је превалентан и у француском правном поретку. Нема дилеме, да због нехата, пружалац интернет услуга не може бити кажњен. У доношењу решења за наведена питања и немачки законодавац се позива на природу и техничку страну посла фирме пружаоца услуга која му онемогућује да буде свестан садржаја свих информација, пренесених од стране корисника његове услуге. Слично, попут било ког телематског сервиса, када је улога пружаоца услуга само обичан пренос информација, он не мора бити свестан њиховог садржаја. Овде сада долазимо и до дихотомије садржане у немачком праву, у вези овог конкретног случаја. Наиме, изгледа да савезни закон, TDG, одступа од норми садржаних у Државном уговору о медијским услугама (Mediendienststaatsvertrag – MDStV), као изразу законодавне воље немачких савезних држава (Ländern). Реч је о дужности пружаоца услуга да, ако зна за постојање нелегалног садржаја и ако је онемогућивање садржаја за њега технички изводиво (а да не угрози своје дужности према својим другим клијентима), онемогући забрањен садржај. С друге стране, MDStV тражи обавезу блокирања садржаја, ако то затражи немачки орган надлежан за бригу и права младих. И немачки систем грађанско-правне и казнене одговорности разликује пружаоца интернет приступа и пружаоца услуга смештаја web страница.

За разлику од француског приступа и приступа из Cybercrime Конвенције, начелно је кроз опште прописе била предвиђена, осим одговорности за намеру, и одговорност за нехат (negligence). Ипак, и овде је присутан оправдани страх да је ефективна контрола и свест пружаоца услуге о садржају, због огромне количине информација практично немогућа, па су и TDG и MDStV искључили нехат и

концентрисали се само на намеру. Фирма, пружалац услуга може бити одговорна ако је свесна садржаја. У вези с тим, у немачкој судској пракси се, као накнадно, поставило питање када се може рећи да је фирма свесна садржаја, и да ли одговорност централе фирме, ако постоји сазнање да је неко од запослених у некој од подружница био свестан нелегалног садржаја. Федерални судови стоје на становишту, да у овом случају одговорност централних органа фирме постоји. Свако сазнање унутар фирме о садржају довољно је да постоји одговорност фирме за садржај који се путем њеног сервера нуди. Дакле, немачко право сматра да не постоји одговорност пружаоца услуга спајања (access provider), зато што по чл. 13, немачког Кривичног законика, не постоји дужност пружаоца услуга да пази какав је садржај који се емитује кроз његову опрему, односно мрежу.¹⁷

Што се тиче одговорности пружаоца услуга смештаја web страница, она постоји ако постоји његова намера.

4.3. Аустрија

У аустријском правном систему, одредбе о одговорности пружаоца интернет услуга садржане су у: Казненом законнику (St.GB), Законнику о казненом поступку (St.PO), Закону о телекомуникацијама (Telekommunikationsgesetz), Закону о штампи и другим средствима јавног саопштавања (1993.), као и у још неким, уско специјализованим законима.

Слично немачком, и у аустријском систему важи став, да се, начелно, не може сматрати одговорним пружалац услуге за пружање услуга приступа интернету. Што се тиче пружања услуга смештаја web страница, ИСП је за такве радње, начелно, одговоран, али се може ослободити одговорности ако је поступао са дужном пажњом.¹⁸ С оваквим мишљењем се слаже и проф. Sieber који наводи још један пример из чл. 75, и чл. 104, ст.1, Telekomu-

¹⁷ Prof. Dr. Ulrich Sieber : Responsibility of Internet Providers , стр. 9.

Ревизија v1.1
CCERT-PUBDOC-2003- -
Страница 34/42

¹⁸ Gabrielle Schmörlzer : Интернет и казнено право, превод у Хрватском летопису за казнено право вол.4 2/97, стр. 895.

nikationsgesetz-a, где начелно постоји одговорност пружаоца услуга, али се изјавом пружаоци услуге спајања на интернет могу екскулпирати генералне одговорности, па тако произилази да фирме власници опреме за пружање интернет услуга не могу бити одговорни за њену злоупотребу у смислу почињења кривичних дела и прекршаја.¹⁹

Професор G. Schmölder, такође, у свом делу о односу Кривичног права и интернета наводи и одредбе аустријског правног поретка о одговорности за ширење национал-социјалистичке литературе и идеја, инкриминација по Закону о забрани Националсоцијалистичке немачке народне странке из 1945. године, новелираног 1952. године.

У аустријском правном систему постоји свест о кажњавању фирми пружаоца услуга, који знају за недопуштен садржај на њиховим рачунарским системима, а ништа не предузимају да се промет таквог садржаја блокира. С друге стране, ако фирме пружаоци услуга нису свесне постојања таквог садржаја, што због обима пренесених информација није незамисливо, тада начелно не постоји њихова одговорност.²⁰ По мишљењу G. Schmölder-a, у Аустрији још треба јасно законски утврдити дужност надзора и њених даљих ефеката.

4.4. САД

У САД-у, одговорност пружаоца интернет услуга регулисана је следећим прописима: Communications Decency Act, Child Online Protection Act, Online Copyright Infringement Liability Limitation Act, као и део Digital Millennium Copyright Act-a.

4.4.1. Према Закону о пристојној комуникацији, од 1996. године (**Communications Decency Act**), сматра се да не постоји одговорност пружаоца услуге ако он само пружа услугу приступа, или корисницима пружа софтвер који омогућује приступ, или одржава

¹⁹ Prof. Dr. Ulrich Sieber : Responsibility of Internet Providers, стр. 14.

²⁰ Gabrielle Schmölder : Интернет и казнено право; превод у Хрватском летопису за казнено право вол.4 2/97, стр. 897.

Ревизија v1.1

CCERT-PUBDOC-2003- -

Страница 35/42

системе везане уз техничко функционирање интернет везе (Проху системи, DNS системи). Наравно, одсуство одговорности не постоји када пружалац услуге сарађује са ауторима незаконитог садржаја, или је свестан постојања таквог садржаја, али не чини ништа да то спречи, односно такав садржај уклони.²¹

4.4.2. Када је 1998. године ступио на снагу **Закон о заштити деце на мрежи (Child Online Protection Act)**, пружаоци интернет услуга постали су законом обавезни да обавесте своје кориснике, приликом склапања уговора, да постоји софтвер са могућношћу филтрирања садржаја. Исто тако, тај је пропис донео и одредбу којом су одговорни они који учине доступним преко интернета, садржај који је штетан деци и малолетницима. Ова одговорност се, опет, не односи на пружаоце самог приступа, већ оне који смештају такав садржај на своје странице. Такви се пружаоци услуга могу оградити од одговорности, тако да заштите такве странице обавезном употребом идентификатора и лозинки, те истицањем обавештења када је реч о страницама забрањеним за малолетнике.

4.4.3. **Закон о ограничењу одговорности за онлајн повреде ауторског права (Online Copyright Infringement Liability Limitation Act)**, из 1998. године, садржи одредбе у погледу одговорности и ограничењу одговорности пружаоца интернет услуга за објављивање недозвољено умноженог или другог материјала који крши ауторска и сродна права. Ограничење одговорности односи се на случај када пружалац услуга, на основу информација о постојању материјала који крши ауторска и сродна права, без одлагања блокира приступ и одстрани такав садржај са сервера под својом надлежношћу. Овај пропис, такође, специфицира прилично формалан поступак којим се може од фирме, пружаоца услуге, захтевати скидање и блокирање приступа садржају који вређа ауторска и сродна права. Првенствено се, од фирме пружаоца услуга, тражи да именује “designated agent”, особу одређену да прима захтеве за

²¹ Проф. Др. Ulrich Sieber : Responsibility of Internet Providers, стр. 17
Ревизија v1.1
CCERT-PUBDOC-2003--
Страница 36/42

одстрањење одређеног садржаја. При том, од стране која сматра да су јој права повређена тражи се:

1) потписани захтев којим се тражи одстрањење спорног материјала;

2) довољно података да се може установити о каквој повреди права је реч;

3) потребни подаци да пружалац услуга може установити који је материјал објављен путем његовог рачунарског система споран;

4) лични подаци тужиоца да пружалац услуге може с њим ступити у контакт, и

5) изјаву да као тужилац наступа у доброј вери и да поседује права чију заштиту тражи.

Наравно, сличним поступком регулисано је и право оног који је спорни садржај ставио на интернет, да реагује на захтев оштећеника, па и да истим путем затражи поновно постављање садржаја на интернет и омогућавање приступа, уколико се покаже да није дошло до повреда наведених од стране наводног оштећеника.

Даље одредбе, које су од важности за тему овог рада, односе се на додатно ограничење одговорности за универзитете као пружаоце интернет услуга. Закон јасно каже, да не постоји обавеза на страни пружаоца услуге да активно учествује и евалуира садржај објављен на својим серверима, у потрази за садржајем који би могао бити противан одредбама о заштити ауторских и сродних права. Сиебер даље сматра да је амерички законодавац овим прописом успоставио избалансирани компромис између интереса носиоца ауторских и сродних права, чија би права могла бити угрожена, и пружаоца услуга.

4.4.4. Digital Millennium Copyright Act - У САД-у је, 1998. године, донет Закон о ауторском праву дигиталног доба. Осим увођења начелне одговорности ИСП-а за свесно предузете радње на које су могли имати утицаја, овај Закон уређује и неке специфичне случајеве, односно искључује одговорност ИСП-а, у одређеним случајевима.

4.4.4.1. Активности на које се односи искључење одговорности

Искључење одговорности обухвата четири типа активности: а) обичан транспорт; б) кеширање (caching); в) смештај и г) претраживаче и хипертекстуалне везе.

а) Обичан пренос

Основна функција провајдера представља обичан пренос информација. Провајдер не може сносити одговорност ако се његова улога ограничава на просту трансмисију података, које он не модификује према примаоцима, које не селекционише. Искључење одговорности обухвата и посредничко складиштење и транзитирање података, под условом да ове активности произилазе из аутоматског поступка и да ускладиштени материјал не буде доступан другим лицима, осим оних којима је намењен. Овај случај покрива посредничко стокирање (складиштење) нужно везано за функцију транспорта информација. Тако, нпр., електронска пошта, пре него што ће бити подигнута од примаоца, нужно мора бити ускладиштена на сервер посредника. Дакле, обичан пренос представља један од основа за искључење одговорности провајдера који има улогу пасивног преноса информација. У три преостала случаја провајдер има и неке обавезе чињења.

б) Кеширање (Caching)

Провајдери могу ставити у службу сервере релеје (преносне станице) на којима праве копије најтраженијих сајтова и где складиште информације које су већ били тражене. Ова техника се назива кеширање. Она побољшава конекситет са сајтовима на мрежи уз избегавање закрчења мреже. Провајдер је ослобођен одговорности за овај кеш под извесним условима, а нарочито ако:

<информација буде пренесена последњем кориснику без модификације;

<посредник поштује инструкције са положаја одапиљача, које се тичу ажурирања информација, означених сагласно индустријским стандардима;

<посредник поштује услове приступа информацијама (накнада, password, лозинка и сл.);

<посредник се не уплиће у коришћену технологију у циљу добијања података о коришћеним информацијама;

<посредник ради промптно на повлачењу или блокирању приступа фалсификованим информацијама, по добијеној нотификацији, чим је информација била повучена са оригиналног сајта или је повлачење ове информације било наређено од суда.

в) Смештај

Ово ограничење тиче се функције смештаја, што ће рећи стокирања-складиштења и сређивања података на захтев корисника сервиса на систему посредника. Да би се користио овом врстом ослобађања обезбеђивач смештаја, пружалац интернет услуга, треба да испуни следеће услове:

<не сме знати за фалсификаторски карактер смештене информације, а такав карактер мора бити очигледан;

<мора брзо повући фалсификовану информацију, чим је за њу сазнао;

<не сме примити накнаду која директно проистиче из фалсификаторске активности, кад посредник има право и могућност да контролише такве активности.

Осим тога, од пријема нотификације (опомене) од стране титулара ауторског права, у законској форми, обезбеђивач смештаја мора поступати брзо ради повлачења или онемогућавања приступа фалсификованој информацији. Да би се користио овом врстом ослобађања, обезбеђивач смештаја мора означити једног пуномоћника за пријем нотификација који ће бити регистрован код Copyright Office-а. Нотификација наведена у закону мора обезбедити посреднику довољно прецизне информације о фалсификованом материјалу, његовој локацији и повређујућем делу садржаја.

г) Претраживачи и хипертекстуалне везе - хиперлинкови

Овај изузетак обухвата хиперлинкове, директоријуме, збирке, претраживаче и друга помоћна средства за локализовање информација расположивих на мрежи. За искључење одговорности провајдера поводом ових активности, сходно се примењују правила о смештају.

д) Налози-наредбе према посредницима

Амерички закон је установио, у корист титулара ауторског права, један скраћени поступак у циљу издејствовања налога од суда, против посредника, ради обезбеђивања елемената за идентификацију претпостављеног фалсификатора.

Налози за чињење - За активности обичног транспорта, посреднику може, само бити наређено да раскине, односно поништи претплатнички рачун клијента фалсификатора и предузме "разумне

мере" за блокирање приступа појединим сајтовима, који су идентификовани у вршењу недопуштеног преноса информација. За остале типове активности, посредницима може само бити наређено да раскину рачун претплатника фалсификатора или да повуку фалсификовани материјал са његовог система.

У свим случајевима, текст прецизира да судови, који издају налоге, морају да узму у обзир: техничке могућности за предузимање тражених мера блокаде, величину терета наметнутог посреднику, последице мера на приступ другим сајтовима који не садрже фалсификаторски материјал и штету коју би претрпео титулар ауторског права, кад мере не би биле предузете.

ђ) Неосноване нотификације

Закон садржи и одређене ограде за ограничавање неоснованих нотификација према посредницима. Одговорност посредника не може бити покренута од стране издавача садржаја из разлога што је могао повући спорну информацију или блокирати приступ њој. Међутим, да би се позвао на овај "имунитет" посредник мора:

<предузети све неопходне мере ради обавештавања претплатника, коме је повучен материјал или обустављен приступ односном материјалу;

<чим прими контранотификацију од издавача садржаја о спору, промисно информисати титулара ауторског права;

<вратити материјал у року од 10-14 радних дана, ако је информисан у том року, од стране титулара ауторског права, да је он покренуо судски поступак против издавача садржаја.

Анализирајући овај закон, чини се да он, ипак, фаворизује, па чак, и претерано штити провајдере, у односу на друге учеснике на мрежи, као и у односу на кориснике интернет услуга.

4.5. Одговорност посредника према Директиви ЕУ о електронској трговини

Једно од пет питања која третира Директива Европске Уније о електронској трговини, од 2000. године, представља одговорност посредника на мрежи. Посредничке активности карактерише чињеница да се жељене информације довлаче, складиште или преносе преко или на захтев прималаца сервиса. Израз "прималац

сервиса" подразумева не само потрошача информације, који ту конкретно има приступ, већ и свако друго лице, коме је потенцијално приступачна таква информација, било да иступа под личним или професионалним именом. Ова Директива је одговорности посредника приступила трансверзално, што значи без разлике између типова недопуштених активности. Тако, систем ограничења одговорности, установљен с циљем да се примени у материји нелојалне утакмице, тиче се подједнако грађанске и кривичне одговорности.

У смислу одредаба Директиве, технички посредници не морају себи наметати никакву општу обавезу надгледања информација које они преносе или складиште, нити какву дужност у поступку за активно истраживање радњи или околности које индицирају недопуштене активности. Оваква одредба не искључује само судску власт, која може захтевати од неког посредника да контролише одређени сајт у одређеном периоду у циљу превенције или детекције.

4.5.1. Активности на које се Директива односи

Директива регулише три типа активности које, под одређеним условима, представљају основ за искључење провајдерове одговорности. Да би се користио предвиђеним повластицама, провајдер мора за сваки тип активности да испуни услове прописане Директивом. У супротном, неће моћи да се позива на ослобађање одговорност по овој Директиви, већ ће се на њега применити национални закон.

а) Обичан пренос

Слично америчком закону, Директива установљава изузетак од провајдерове одговорности, када он поступа као обичан преносилац информација постављених од трећих лица или као обичан омогућавач приступа на телекомуникациону мрежу. Да би се користио наведеном погодношћу, посредник не сме бити на извору трансмисије, не сме селекционирати примаоца трансмисије и не сме селекционирати или модификовати информације које чине предмет трансмисије. При том, активности трансмисије обухватају аутоматско складиште, посредовање и транзит информација.

б) Кеш (Саш)

Посредник је искључен од одговорности за овај тип активности, под условом да:

<не модификује информацију;

<се управља према условима приступа информацијама;

<се придржава одредаба које се тичу ажурирања информација, означених на кохерентан начин према индустријским стандардима;

<се не уплиће у технологију у циљу добијања информација о коришћеним информацијама;

<делује промтно на повлачењу информација или враћању приступа који је био онемогућен, чим сазна да је информација повучена са оригиналног сајта или да је приступ овој информацији био онемогућен или да су њено повлачење или блокада били наређени од надлежне власти.

в) Смештај

Директива уводи ослобађање одговорности посредника за активности складиштења извршеног на захтев примаоца сервиса. Ово ослобађање ће имати дејство под условом да посредник није имао стварно сазнање да се неки корисник његовог сервиса бавио неком недопуштеном активношћу на мрежи, а за тужбе у грађанској одговорности, ако посредник није знао за чињенице и околности према којима се недопуштена активност појављује као очигледна. Међутим, није прецизирано шта значе појмови "имати стварно сазнање да је активност недопуштена" или "имати сазнање о чињеницама и околностима према којима је недопуштена активност очигледна", већ су та питања остављена да се решавају у конкретним случајевима.

У сва три случаја у којима се провајдер користи за ослобађање одговорности за предузимање наведених активности, искључене су тужбе за накнаду штете и камату, као и кривично гоњење, али нису искључене тужбе за обуставу ("action en cessation", "prohibitory injunction"). Наведене тужбе су имане у виду у циљу повлачења или блокирања недопуштене информације. Изван оквира ових тужби, Директива не намеће посреднику повлачење недопуштене информације или блокирање приступа, као у случају кеша или смештаја.

Vidoje Spasić, LLD, Assistant Professor

REVIEW TO RESPONSIBILITY OF ISP (INTERNET SERVICE PROVIDER) IN INTERNATIONAL AND COMPARATIVE LAW

Summary

As active participants, on the internet appear a lot of entities with different roles. On of the most important participants is the Internet Service Provider (ISP). Service provider means: any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service.

The responsibility of the ISP for undertaken activities to the internet, has been determined by two key factors. First, one we take into consideration the circumstance if the ISP is the passive participant on the web (for example - e-mail), or active participant on the web (for example - stocking or making the accesses possible). Second, one we take into consideration the fact if the ISP is conscious, actually if he has a knowledge to participate in one of the prohibited activities. Generally, the ISP can be responsible just for the acts, where he has active participated, and was conscious that according to him, the illegal activities were developing and did nothing to stop their executing.

Key words: *internet, internet service provider (ISP), services of ISP, responsibility of ISP.*

