

Адриана МИНОВИЋ

Марко МАТОВИЋ

ОДГОВОРНОСТ ПРУЖАОЦА УСЛУГА ИНФОРМАЦИОНОГ ДРУШТВА У ЕЛЕКТРОНСКОЈ ТРГОВИНИ НА НИВОУ ЕВРОПСКЕ УНИЈЕ

Резиме

Аутори овог рада истичу да све већи и експанзивнији развој нових технологија и интернету ишче у великој мери на све сфере живота, а поштово на тржиште и начин одвијања међународних трансакција. Стога електронска трговина због својих значајних предности и присвојачности почиње да заузима доминантно место у светским трансакцијама. Међутим, најнај технологишки развој има и своје мане, а то је дефинитивно могућности праћења и регулисања нових решења на овом плану. Као једно од најзначајнијих питања у области електронске трговине аутори виде одговорности пружаоца услуга информационе друштва. Иако се на ово питање, наравно, примењују већ присвојни правни принципи и правила у вези са одговорношћу, ипак треба имати у виду специфичности ове активности што захтева и посебан сет правила само за њу. Сигурно најзначајнији покушај регулисања електронске трговине на нивоу Европске уније представља Директива о електронској трговини 2000/31/ЕС која је посебну пажњу посветила баш правилима о одговорности пружаоца услуга информационе друштва кад наступају као посредници.

Директива предвиђа такозвани режим „сигурне луке“ који прописује да пружаоци услуга, кад врше чисте посредничке услуге, привремено складиштење података или трајно складиштење података, ако

исцрпљивају одређене услове прописане у члановима 12, 13 или 14 Директиве нису одговорни за садржај који преносе, нићи имају обавезу да контролишу садржај који преносе. Иако их ова правила ограничавају одговорности и накнаде штете, они су ипак дужни да оној пренутика кад стекну сазнање о нелегалном садржају или кад приме налој од стране надлежној тела, реајују скидањем или блокирањем садржаја или неким друим начином онемоућавања присутног садржаја. Начин на који се сајту ставља до знања присуство нелегалног садржаја варира од земље до земље и није јединствено уређен на нивоу ЕУ, али је дефинитивно један од механизма који се најчешће прејоручује процедура скидања сорној материјала након обавештења (енгл. Notice and Take and Down Procedures). Иако има доста критика ове процедуре, ипак она поставља значајан ниво извесности што је веома битно за предвидивост и сигурност пословања. Проблем који се јавља код ових мера забране је у вези са могућношћу да се претворе у мере обавезној мониторинга, ако се поред намењања обавезе скидања незаконитој материјала намеће и обавеза да и убудуће срече јојављивање тој материјала.

Аутори закључују да, поред тога што дефинитивно постоји неопходност ревизије Директиве и преиспитивање постојећих решења у складу са новим развојем технологија, иакоје треба бити и одрезан приликом прописивања оваквих механизма који се тичу мера забране. Свакако ревизија је неопходна ради премошћивања неуједначене примене решења из Директиве.

Кључне речи: електронска трговина, одговорност, пружалац услуга информационој друштва, принцип сигурне луке, мере забране.

I Основи одговорности/врсте одговорности

Савремено доба у коме живимо нам непрестано доноси иновације и напретке у развоју цивилизације. Свакако једна од највећих окосница XXI века је свеопшта дигитализација, значај и присуство интернета као свакодневнице већине светске популације. Интернет је постао место на којем се проводи све више времена, помаже у долажењу до потребних информација, информисе нас о актуелним дешавањима, преко интернета се послује и користе се разни забавни садржаји. Како је интернет свеприсутан у животу људи, неопходно је да постоје одређена правила преточена у закон која се односе на општу комуникацију на интернету, као и на податке и услуге које омогућавају пружаоци услуга информационог друштва.

Кад је реч о регулацији интернета, постоје становишта одређених група да је интернет универзални простор који припада свима, те да као такав, он не би требало да буде уопште регулисан законом, а поготово не законом на нивоу сваке државе засебно.¹ Међутим, сматра се да управо због домаћаја интернета, доступности и значаја у свакодневном животу људи јесте неопходно да исти буде законом регулисан како би се уредили односи субјеката који оперишу у оквиру њега и да би у случају злоупотребе и повреде права могло адекватно да се одговори.

Један од веома важних аспеката интернета и електронских комуникација се односи на појаву електронске трговине која је својом све учесталијом присутношћу и великим обимом, поставила питање њене све детаљније регулације. Питање пословања у виртуелном простору и његове размере, па самим тим и уређење на међународном нивоу све више се поставља.² Једно од најзначајнијих питања у светлу ове проблематике је питање одговорности пружаоца услуге информационог друштва (тј. електронског трговца) које је од изузетне важности за предвидивост пословања и пружање правне сигурности. Али, пре него што се пређе на специфичности овог режима одговорности у вези са електронском трговином, треба констатовати да се на њу подједнако примењују и општи правни принципи.

Правна теорија разликује више критеријума поделе од којих бисмо скренули пажњу на следећа два. Са становишта степена могуће одговорности пружаоца услуга информационог друштва разликујемо две врсте одговорности: 1) систем стриктне одговорности (енгл. *strict liability system*) који је и најригорознији кад је у питању одговорност пружаоца услуга информационог друштва и он лежи у наметању обавезе пружаоцу услуге информационог друштва да надгледа сав материјал постављен на интернету; 2) систем заснован на субјективној одговорности тј. кривици (енгл. *with fault liability system*) у оквиру којег је нагласак на намери да се повреди нечије право.³ Тако се у оквиру њега разликују два подсистема од којих један полази од знања пружаоца услуга информационог друштва за постојање материјала који доводи до директног кршења неког права, до ситуације у којој би пружалац услуга информационог друштва требало да претпостави да ће одређени материјал довести до кршења неког права.

1 Juan Carlos Riofrio Martinez-Villalba, *Principles of Liability of Internet Service Providers*, Ecuador, 2006, доступно на адреси: <http://www.internationallawoffice.com/newsletters/detail.aspx?g=2b4a44e5-0223-db11-8a10-00065bfd3168>.

2 *E-commerce Proposal Causes Liability Jitters*, 2012, доступно на адреси: <http://www.euractiv.com/infosociety/commerce-proposal-causes-liabili-news-510099>.

3 Pablo Baistrocchi, „Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce“, *Santa Clara Computer & High Technology Law Journal*, Vol. 19, 1/2003, стр. 114.

С друге стране, одговорност можемо поделити и на основу следећег критеријума:⁴ 1) грађанска одговорност – примарна компонента да би постојала грађанска одговорност јесте постојање штете. У оквиру цивилне одговорности, кад је реч о електронској трговини, и кад је реч о споровима који се воде поводом исте, може се направити подела на уговорну одговорност и на деликтну одговорност; 2) управна одговорност – кад говоримо о управној одговорности, неопходно је истаћи да до управне одговорности долази услед кршења управних прописа или других чињеница.⁵ Код управне одговорности прави се разлика у односу на субјект који крши управни пропис, па се тако разликује кршење од стране физичких лица, правних лица, институција и других организација и са друге стране кршење управних прописа од стране државних органа; 3) кривична одговорност – главна карактеристика код кривичне одговорности се огледа у регулисању одговорности кад је реч о електронској трговини од случаја до случаја. Законодавац појединачно прописује одређено понашање као кривично дело и за њега прописује одређене казне. Тако нпр. у САД се сматра федералним злочином скидање, поседовање и примање заштићене информације у трговини без дозволе овлашћеног лица.⁶

Ово су само неке од подела које познаје правна доктрина код питања одговорности генерално, а које се подједнако примењују и на одговорност пружаоца услуга информационог друштва. Поред ових правила, електронска трговина познаје и себи својствена правила која само представљају додатни систем заштите у односу на већ постојеће механизме.

II Системи/приступу регулисању одговорности

Кад се говори уопштено о системима регулисања одговорности пружаоца услуга информационог друштва, издвајају се три значајна система: процедура скидања спорног материјала након обавештења (енгл. *Notice and Take and Down Procedures*, у даљем тексту: НТД), само-регулација и ко-регулација.⁷

НТД процедура се сматра једним од најефикаснијих метода заштите права од спорног материјала који се објављује или дистрибуи-

4 Zheng Qin, *Introduction to E-Commerce*, Beijing, 2009, стр. 195–201.

5 Z. Qin, *нав. дело*, стр. 199.

6 Katie Matison, *Liability for Breach of E-Commerce Security Standards*, Washington, 2001, стр. 5.

7 Студија ЕУ из 2007. године – *EU Study on the Liability of Internet Intermediaries*, даље у фуснотама: *EU Study from 2007*, European Commission's Information Society and Media Directorate – General, стр. 106–116.

ра на интернету. Такође, поменути метод је уједно и мета многих критика које почивају на становишту да та процедура угрожава слободу информисања. Процедура скидања спорног материјала је присутна у законодавствима земаља ЕУ, али је неопходно истаћи да није на исти начин и у истој мери кодификована. Она се огледа у скидању спорног материјала тек по пријему обавештења. НТД процедура је најпотпуније регулисана у финском законодавству где је читав поступак од обавештења пружаоца услуга информационог друштва о спорном садржају, па до скидања истог садржаја до детаља разрађен и кодификован.⁸ Поменута процедура је намењена заштити ауторских права искључиво. У мађарском законодавству је НТД процедура такође присутна, али само у сврху заштите права интелектуалне својине. Најшире постављена НТД процедура је у Литванији, где се поред заштите ауторских права, НТД примењује и у било којој ситуацији појаве материјала за који неко лице сматра да не треба да буде објављен или дистрибуиран.⁹

Систем само-регулације је присутан у скоро свим земљама ЕУ где пружаоци услуга информационог друштва самостално креирају методе контроле садржаја који се дистрибуира/складишти на интернету. Пример једног програма који је признат као ефикасан у тој сврси је програм који је лансирао *e-Bay*, тзв. *VeRo* програм. *VeRo* програм је у свим земљама у којима се појављује намењен заштити права интелектуалне својине.¹⁰ Белгија (енгл. *Belgacom*) је развила врло ефикасан систем заштите, где пружалац услуге информационог друштва неколико дана после примљеног обавештења шаље обавештење директно јавном тужиоцу који наставља даљу процедуру. У Великој Британији, такође, постоји само-регулација као метод заштите. Може се приметити да је доста институција у Великој Британији прихватило овај систем (енгл. *Direct Marketing Association, ICSTIS, The Internet Watch Foundation*), па су тако они самостално кодификовали одређене принципе по којима ће поступати у случају да дође до обавештења о спорном садржају који се налази на интернету.¹¹ Орган који је задужен да касније настави са испитивањем навода у обавештењу је омбудсман.

Поента ко-регулације лежи у сарадњи компанија, институција са државним органима по питању регулисања и процедуре у случајевима кад се укаже на неки недозвољени садржај на интернету. Пример успешне сарадње на том пољу је протокол о сарадњи који су потписали

8 *EU Study from 2007*, стр. 106.

9 *EU Study from 2007*, стр. 108–109.

10 Доступно на адреси: <http://pages.ebay.com/help/community/vero-aboutme.html>.

11 *EU Study from 2007*, стр. 113.

белгијска *Internet Service Provider Association*, Министарство правде и Министарство телекомуникација, који предвиђа периодично информисање о недозвољеном садржају и то тако што ће се подаци о томе складиштити у *Federal Crime Computer Unit*, после чега ће се разматрати даље прослеђивање јавном тужиоцу.¹²

III Правила о одговорности у Директиви о електронској трговини

Најзначајнији покушај да се питање одговорности пружаоца услуге информационог друштва регулише на међународном нивоу је Директива о електронској трговини која је првенствено донета у циљу стварања правног оквира који ће омогућити слободно кретање услуга информационог друштва између земаља чланица.¹³ Директива треба да поспеши развијање услуга информационог друштва, обезбеди правну сигурност кроз координацију националних правних режима и појасни правне аспекте електронске трговине како би се обезбедило правилно функционисање унутрашњег тржишта ЕУ. Посебно, код регулисања питања одговорности пружаоца услуга информационог друштва Директива тежи да поспеши развој међународног пословања и да отклони дисторзије у конкуренцији кроз хармонизацију националних одредби у вези са одговорношћу пружаоца услуга информационог друштва у улози посредника.¹⁴

Питање одговорности пружаоца услуге информационог друштва у улози посредника је од нарочите важности имајући у виду да због природе услуге коју обављају они имају врло мало сазнања о томе које информације преносе или чувају, и због тога, регулисање њиховог односа и односа субјеката који постављају информације, које они даље преносе, може бити веома проблематично код питања одговорности за недопуштен материјал. Стога, иако питања одговорности пружаоца услуге информационог друштва, у вези са недопуштеним материјалом, потичу од њихових корисника, сами пружаоци услуга су много атрактивнији за наметање одговорности због тога што их је лакше лоцирати и због финансијске јачине која је погодна за намирење.¹⁵ Управо због тих раз-

12 *EU Study from 2007*, стр. 114.

13 *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market („Directive on electronic commerce“)*.

14 P. Baistrocchi, *нав. дело*, стр. 122.

15 Студија ЕУ из 2009. године – *EU study on the Legal analysis of a Single Market for the Information Society – Liability of online intermediaries*, даље у тексту: *EU Study from*

лога Директива препознаје специфичну улогу пружаоца услуга информационог друштва када наступају као посредници и, стога, тежи да регулише то питање изједначавајући њихове обавезе у свим земљама чланцима.

1. Дефинисање пружаоца услуге информационог друштва, *safe harbor* принцип и основи за изузеће од одговорности

Директива уводи посебан сет правила одговорности које се односе на пружаоце услуга информационог друштва, али само кад наступају као посредници пружајући одређене врсте услуга које су дефинисане у члановима 12, 13 и 14 Директиве о електронској трговини. Принцип садржан у овим члановима се назива у доктрини режим „сигурне луке“ (енгл. *safe haven, safe harbor*) који омогућава да, док год су испуњени услови из поменутих чланова, пружалац услуге информационог друштва не може бити одговоран за незаконит садржај.¹⁶ Пре свега, потребно је обратити пажњу на саму дефиницију услуга информационог друштва, јер се у складу са њима дефинише и сам пружалац поменутих услуга.

Директива их дефинише као услуге које се „регуларно пружају на основу накаде, на даљину, електронским средствима на индивидуалан захтев примаоца услуге“,¹⁷ у чему се виде два битна елемента, а то је накнада и да је пружена електронским средствима.¹⁸ Поред испуњавања овог основног услова, да би могли да буду заштићени овим принципом, пружаоци услуга информационог друштва морају да, или врше чист аутоматски посреднички пренос података (енгл. *mere conduit*), или привремено складиштење (енгл. *caching*) или трајно складиштење (енгл. *hosting*), под тачно одређеним условима које ћемо у наредном делу детаљно образложити.¹⁹ Оно што треба приметити је да Директива уводи хоризонтални режим одговорности који значи да се он примењује на три тачно одређене врсте услуга, независно од врсте одговорности за коју се терете (тј. небитно је да ли је у питању кршење права интелектуалне својине, клевета, итд.).²⁰

2009, European Commission's Information Society and Media Directorate – General, стр. 3.

16 *EU Study from 2009*, стр. 7.

17 *Directive 2000/31/EC*, рецитал 17.

18 *EU Study from 2009*, стр. 11.

19 P. Baistrocchi, *нав. дело*, стр. 118.

20 *EU Study from 2009*, стр. 9; Trevor Cook, „Online Intermediary Liability in the European Union“, *Journal of Intellectual Property Rights*, N. 17/2012, стр. 158.

а) Чист аутоматски посреднички пренос података (енгл. *mere conduit*)

Чист аутоматски пренос података постоји онда када се ради или о пружању услуге приступа мрежи или пружању услуге преноса података. У складу с тим пружалац услуга који преноси електронске податке које му је предао корисник услуге, није одговоран за садржај послатих података и њихово упућивање ако није: иницирао пренос, извршио одабир података, изменио податке и одабрао примаоца преноса. Ово укључује и аутоматско, посредничко и привремено складиштење пренетих података, али они морају бити складиштени само у периоду који је неопходан за њихов пренос.²¹ Овде је заправо реч о традиционалним провајдерима који пружају приступ интернету преко *dial up* модема, кабла, фиксних линија, итд. и провајдерима који врше интерконекију и оно што им је заједничко је то да преносе огромну количину података на захтев својих корисника. Стога, у светлу њиховог изузећа од одговорности веома је важно да су пасивно укључени у пренос података.²²

б) Привремено складиштење (енгл. *caching*)

Привремено складиштење података се односи на привремено и аутоматско складиштење у сврху омогућавања даљег преношења података на најефикаснији начин. Овде се најчешће говори о такозваним прокси серверима (енгл. *proxy server*) који чувају копије информација о посећеним веб сајтовима од стране њихових корисника. Кад се један сајт посећује изнова и изнова прокси сервер омогућава испоруку локално сачуване копије сајта, што омогућава да се избегне ситуација да оригинални веб сервер мора бити контактиран поново, и тиме се смањује загушење интернет саобраћаја и убрзава процес испоруке информације. Да би овакав пружалац услуга био изузет од одговорности, мора да испуни одређене услове. Мора се радити о аутоматском, посредничком и привременом складиштењу које служи само за ефикаснији пренос података тражених од стране других корисника услуга, ако пружалац услуге: не мења податке, уважава услове за приступ подацима, поступа у складу са правилима за ажурирање података, делује у складу са дозвољеном применом технологија за прикупљање података и ако укљони или онемогући приступ подацима које је чувао одмах након сазнања да су подаци укљонени из првобитног преноса посредством мреже или је онемогућен приступ до њих, као и када је суд, односно други надлежни орган наредио њихово уклањање или онемогућавање приступа (чл.

21 *Directive 2000/31/EC*, чл. 12.

22 *EU Study from 2009*, стр. 7.

13 Директиве). Као што можемо приметити, за разлику од претходног услова који се сводио на чисто објективне елементе за оцену изузећа од одговорности, овде имамо и субјективни елемент који се односи на сазнање у вези са незаконитим подацима и применом дужне пажње у том погледу.²³

Кад је у питању судска пракса, привремено складиштење података није изазивало много недоумица до сада. Један од интересантнијих случајева се односио на кршење права интелектуалне својине кроз *Google*-ово објављивање чланака, а који су објављени од стране трећих лица (новинских кућа), и који су били копирани захваљујући тужениковом кеш систему и тиме били доступни *Google*-овим корисницима. Централни проблем је овде био потенцијално кршење права интелектуалне својине од стране туженог, кроз копирање садржаја трећих лица. Белгијски суд је у овом случају одбио да примени изузетке од одговорности на *Google*.²⁴

в) Трајно складиштење (енгл. *hosting*)

Кад је у питању овај услов, реч је о чувању тачно одабраних података и њиховом постављању од стране корисника услуге, који су намењени да буду чувани у неодређеном временском периоду. Типичан пример је веб хостинг компанија која пружа простор на интернету својим корисницима који желе да поставе веб сајт. Стога су услови за њихово изузеће од одговорности да само складиште податке пружене од стране корисника услуге на захтев корисника услуга и то под условом да не знају за недопуштено деловање корисника услуга или за садржај податка, као ни за чињенице или околности на основу којих би недопуштена активност корисника била очигледна и ако благовремено закон сазнања да се ради о недопуштеном деловању или податку уклоне или онемогуће приступ том податку. Ове одредбе се неће примењивати на случајеве у којима је корисник услуга лице које је на било који начин зависно од пружаоца услуга (чл. 14 Директиве). Овде треба напоменути да постоје два различита степена свести у зависности од захтева који се могу упутити против пружаоца услуга (у даљем тексту: хостинг провајдер): први се односи на то да није свестан чињеница и околности које се тичу недопуштеног податка или деловања и то ако се ради о грађанскоправним захтевима за накнаду штете и други, који се односи на стварно сазнање о недопуштеном деловању / податку кад је реч о свим осталим захтевима.

23 Р. Baistrocchi, *нав. дело*, стр. 118.

24 *Copie Press v. Google*, Tribunal de Premiere instance de Bruxelles, 13.2.2007.

У пракси судова земаља чланица се досад показало да највише нејасноћа изазива баш овај члан и одређивање пружаоца услуга као хостинг провајдера што је доста тешко имајући у виду развој нових технологија. Иако није неуобичајено да судови различито одлучују у сличним стварима, одлуке судова које су биле у вези са *eBay* су нарочито интересантне, јер су имале везе са питањем да ли је тужени уствари хостинг провајдер, али су судови у својим одлукама користили различите приступе приликом тумачења овог питања. Стога је трговински суд у Паризу у три одвојена случаја против *eBay* заузео исти став и одбио да примени правила о изузећу за трајно складиштење података на туженог наводећи да се аукцијска услуга *eBay* не састоји само од услуга које се односе на трајно складиштења података и да то није најбитнија услуга коју нуди тужени и да се стога не може на њега применити режим за хостинг провајдере.²⁵ Међутим, други француски суд је ова правила применио на туженог само у одређеном делу и то на услуге које су повезане са аукцијским услугама, сматрајући да његову комерцијалну активност треба поделити у више активности и да се режим изузећа може применити само на оне активности које испуњавају услове за то.²⁶ На крају, Белгијски суд је одбио да примени ова правила о изузећу на *eBay*.²⁷ Међутим, у Великој Британији разлика се прави на основу тога да ли пружалац услуга само олакшава нелегалне активности треће стране или их и одобрава,²⁸ а у Грчкој је довољно да је само нека активност за складиштење података присутна како би се неко оквалификовао као хостинг провајдер.²⁹

Као што се може видети, иако се приступ у земљама чланицама разликује те је, стога, немогуће наћи јединствену дефиницију за овај принцип која би се једнако примењивала у свим случајевима, ипак треба приметити да у свим овим случајевима Директива захтева да се ради о пасивној посредничкој улози како би пружалац услуге информационог друштва могао имати користи од ових принципа ограничења одговорности. Али, тај степен пасивности варира у зависности од врсте услуге коју пружа и мора се ценити у сваком случају посебно. Тако, код пуког посредничког преношења садржаног у члану 12 Директиве захтева се највећи степен пасивности и пружаоци услуге не смеју имати

25 *Louis Vuitton Malletier / Christian Dior Couture and Parfums Christian Dior, Kenzo, Givenchy et Guerlain v eBay*, Commercial Court of Paris, First Chamber, 30.6.2008.

26 *Hermès International v. eBay*, T.G.I. Troyes, 4.6.2008.

27 *Border Mesures, Brussels Commercial Court agrees with NYSD Court about eBay*, доступно на адреси: <http://www.bordermeasures.com/spip.php?article144>.

28 *Bunt v. Tilley*, [2006] EWHC 407 (QB).

29 Greek case No 44/2008 of Rodopi Court of First Instance, published in Armenopoulos 2009/3, стр. 406.

никакву активну улогу. За разлику од њих, провајдери који привремено складиште податке могу имати активнију улогу, јер им се дозвољава да одаберу податке или примаоце услуге. А најмањи ниво пасивности имају хостинг провајдери којима се дозвољава да селектују, измене податке које чувају, као и да одаберу примаоца података.³⁰

2. Непостојање генералне обавезе мониторинга

Као што се може закључити из претходно објашњених изузећа од одговорности, пружаоци услуга информационог друштва неће се сматрати одговорним за недопуштен податак ако испуњавају услове из чланова 12, 13 или 14. У складу са тим произлази и општи принцип садржан у члану 15 Директиве,³¹ да пружаоци услуга информационог друштва који пружају претходно објашњене врсте услуга немају обавезу да врше мониторинг података које преносе или чувају, нити да активно траже чињенице или околности које би указале на неки незаконит податак или материјал. Међутим, они су свакако дужни да скину недопуштен податак онда кад у складу са претходно објашњеним члановима стекну сазнање о њему или када им то нареди суд или надлежни орган.³²

Иако су пружаоци услуга информационог друштва који пружају претходно објашњену врсту услуга генерално изузети од одговорности и немају обавезу да врше мониторинг података које преносе или чувају, то не значи да им се не може наложити да скину спорни садржај и прекину или предупреду радње које воде кршењу права трећих. У складу с тим, иако у тим ситуацијама не може да им се тражи накнада штете, јер нема основа за одговорност, свакако им се може наложити да независно од њихове одговорности прекину штетне радње.³³ Оно што се овде првенствено поставља као питање је, када се пружалац услуга информационог друштва сматра свесним незаконитих радњи и како и у којој форми, тј. на који начин, му се може тражити да скине одређени незаконит материјал.

а) Неопходни ниво свесности/знања о недопуштеном подацима/радњи

Без обзира на изузеће од одговорности, пружалац трајног или привременог складиштења података мора скинути или блокирати не-

30 *EU Study from 2009*, стр. 8.

31 *Directive 2000/31/EC*, чл. 15.

32 *EU Study from 2009*, стр. 9.

33 *EU Study from 2009*, стр. 9.

легалан садржај онда кад сазна за недопуштено деловање корисника услуга или за садржај податка, као и кад је свестан чињеница или околности на основу којих би недопуштена активност корисника била очигледна или када добије налог суда или другог надлежног органа да поступи тако. Наизглед најједноставнија је ситуација кад је процедура обавештења прописана националним законима и када пружалац услуга добије налог од надлежног органа, јер онда зна шта тачно треба да уради и има правно ваљан основ за то. Међутим, проблем се овде јавља са тумачењем стандарда кад неко има сазнање о незаконитом материјалу или чињеницама које чине тај материјал/активност очигледно незаконитим, а у ситуацијама кад процедура није прописана и кад није јасно по чијем обавештењу је пружалац услуге дужан да реагује и да ли по сваком обавештењу мора да реагује. У тој ситуацији се пружалац услуга ставља у незавидну улогу неког ко треба слободно да процени незаконитост одређеног материјала или радње и да ли ће и по чијем обавештењу реаговати.³⁴ Посебно је проблематично што сама директива не прецизира ове услове, него оставља земљама чланицама да пропишу детаљније услове, и као резултат тога постоје различити приступи у различитим земљама чланицама у вези са истим питањем.

Кад је у питању одређивање нивоа знања о незаконитим подацима/радњама, различите земље су заузеле различите ставове приликом тумачења. Немачки судови, на пример, траже ниво знања који одговара знању човека, а не вештачке интелигенције, тј. компјутера. Такође, ни евентуални умишљај, ни нехат нису довољни да се оквалификују као сазнање. Термин „сазнање“ се може односити само на сазнање о тачно одређеном садржају, јер је то неопходно да би се он могао и скинути. Стога, у складу са немачком праксом пружаоци услуга су одговорни само ако поступају у складу са грубом непажњом.³⁵ С друге стране, опште је прихваћен став да, кад је реч о очигледно незаконитом материјалу или активностима, ту се сматра да постоји сазнање о незаконитости радње / материјала. Аустријски судови су ту ситуацију окарактерисали на начин на који би и једном лаику, без икакве посебне истраге, било јасно да се ради о недозвољеном материјалу. Конкретан пример је био везан за неауторизовано регистровање домена истоветног називу најпознатије политичке партије у Аустрији.³⁶ Такође, Апелациони суд у Паризу је нашао да је ширење расистичког, антисемитистичког садржаја, као и текстова о ратним злочинима и педофилији представљало евидентно нелегално садржај.³⁷ Иако овај критеријум, наизглед, делује да је много

34 *EU Study from 2009*, стр. 17.

35 *EU Study from 2007*, стр. 37.

36 AU12. – OGH, 13/9/200, 4Ob 194/05s.

37 *EU Study from 2007*, стр. 39.

лакши, ипак треба имати у виду да питање очигледних незаконитости и није тако лако разграничити у свим ситуацијама (типа клевета).

На крају, као битно питање поставља се и проблем обавештења. Да ли пружалац услуга мора да реагује по сваком обавештењу и ако не, по чијем мора? Какво обавештење треба да буде и да ли мора да садржи одређене елементе?

б) Обавештење о недопуштеном податку/деловању и НТД процедура

У погледу самог обавештења веома се разликују критеријуми и приступи од земље до земље. Неке земље детаљно регулишу ово питање док друге немају никакву посебну регулацију у овом погледу и прихватају било какво обавештење. Приступ решавању овог проблема се генерално искристалисао у три правца у земљама чланицама.

Једна група земаља чланица нема формалне услове за процедуру обавештења о недопуштеном податку/деловању, него се ослања на различите критеријуме које је већ развила њихова судска пракса или доктрина. У Холандији, на пример, суд је заузео став да (на основу парламентарних преписки које се тичу концепта стварног сазнања) просто обавештење није довољно да би пружалац услуге реаговао, док је судски налог сасвим довољан основ. С друге стране, у Немачкој, кад је у питању кршење права интелектуалне својине ако обавештење нема све податке неће се реаговати по њему.³⁸

Друга група земаља, иако није установила посебне формалне услове за ову процедуру ипак има одређене прописане критеријуме који се морају испунити кад је у питању обавештење. У Португалији пружалац услуга није дужан да скине садржај само зато што се трећа страна жали на кршење права. У Великој Британији суд узима у обзир све релевантне околности, а посебно да ли је обавештење примљено на одређен начин, да ли има све неопходне податке (име и контакт податке пошиљаоца, детаље о локацији спорног садржаја и објашњење незаконите природе садржаја), итд.³⁹

На крају, трећа група земаља је у својим законима увела детаљно прописану НТД процедуру. Такав је случај у Шпанији где пружалац услуге реагује кад надлежно тело – суд или управни орган – наложе скидање или блокирање незаконитог материјала, прогласи тај материјал незаконитим или кад је већ констатовано да је штета настала. Мана овог приступа је што не мора да реагује по притужби странке којој је

38 *EU Study from 2009*, стр. 19.

39 *EU Study from 2009*, стр. 19.

право угрожено. Слично је и у Италији где се тражи да надлежне власти пошаљу обавештење. Финска је детаљно прописала ову процедуру, али само у погледу повреда ауторских права.⁴⁰ Она има три различита режима за различите врсте одговорности: пружалац услуга мора скинути или блокирати материјал кад обавештење добије од стране суда без обзира на врсту права која се крше; код кршења ауторских права примењује се процедура НТД; и на крају, за кривична дела довољно је било какво друго обавештавање, тј. имање сазнања.⁴¹

3. Мере забране (енгл. *injunction*)

Као што је већ напоменуто, принципи ограничења одговорности не утичу на то да се од пружаоца услуге може тражити да прекине или предупреди незаконите радње, а посебно да скине или блокира недопуштене активности/податке, без обзира на чињеницу да није одговоран за исте. Ко ће издати ову наредбу (суд или други државни орган) и на основу чега, зависи од земље до земље. У Аустрији, Француској и Италији су усвојене посебне одредбе које се односе на издавање оваквих забрана против пружаоца услуга, док с друге стране у већини земаља чланица црпи ову могућност из основних правила грађанског процесног права. Такође, и врста ових мера може бити различита: блокирање приступа одређеном сајту, блокирање конкретне адресе интернет протокола (енгл. *IP addresses*), филтрирање, откривање података о починиоцу незаконите радње итд.⁴² У вези са тим, Литванија, на пример, захтева од хостинг провајдера само да онемогуће приступ недопуштеном податку, али не и да уклони тај садржај. С друге стране, у Словачкој постоји само обавеза да се уклони незаконит податак, а не да се онемогући приступ. Док је у Шведској заступљена једна генералнија формулација која се односи на спречавање даљег ширења незаконитог материјала без улажења у сам начин остваривања.⁴³

Проблем код мера забране није у томе што оне налажу прекидање штетне радње, тј. скидање или блокирање садржаја, него у томе што се таква мера врло лако може претворити у обавезу мониторинга, јер налаже да се предупредује и будуће штетне радње такве врсте. Ако би се говорило о мери која има баш такав карактер, онда би се то директно косило са принципом да пружаоци услуга информационог друштва (који испуњавају услове из чланова 12, 13 или 14 Директиве) немају

40 *EU Study from 2009*, стр. 19.

41 *EU Study from 2007*, стр. 40.

42 *EU Study from 2009*, стр. 21–22.

43 *EU Study from 2007*, стр. 35.

обавезу да врше мониторинг у складу са чланом 15 Директиве. У вези са тим, судска пракса земаља чланица је јако подељена те у Немачкој, на пример, Федерални суд је установио да пружалац услуге не само да треба да уклони незаконит материјал, него да и предузме све могуће и разумне мере да спречи даље такве повреде.⁴⁴ У једном аустријском случају наметнута је мера забране једном хостинг провајдеру интернет форума због клевете. Хостинг провајдер не само да је морао да скине материјал у вези са том клеветом, него и да пази да се у будућности не понови та клевета, јер аутор клевете је анониман, а очекивало се да ће их бити још, јер је сам садржај клевете позивао на њено даље ширење. Суд је нашао да је за ово праћење специфичне информације потребно мање труда него за генерални мониторинг.⁴⁵ С друге стране, британски суд је у једном случају везаном за клевету нашао да би оваква мера забране против провајдера који привремено складиште податке била непропорционална.⁴⁶

Кад је у питању пракса Суда правде ЕУ у случају *L'oreal SA v eBay* суд је нашао да на основу Директиве 2004/48⁴⁷ земље чланице не само да морају обезбедити да се не крше права интелектуалне својине, него да се путем мере забране нареди пружаоцу услуге да предузме мере у циљу прекидања кршења и спречавања даљег кршења права интелектуалне својине.⁴⁸ С друге стране, у другом случају *Scarlet v SABAM* исти суд је рекао да, иако национални судови могу изрећи меру забране, не могу да наметну пружаоцу услуге меру забране која би захтевала да инсталира, на недискриминаторној бази према свим својим корисницима, и на свој трошак, на неодређено време, систем филтрирања за целокупну комуникацију која пролази кроз његов систем.⁴⁹

Проблем са оваквим врстама мера забране је њихова неизвесност, која доводи до могућности наметања обавезе мониторинга. Иако пружалац услуге није одговоран, и стога се против њега не могу уперити захтеви за накнаду штете, изрицање овакве мере забране која се у ствари своди на мониторинг, доводи суштински до истих резултата, као и да

44 *RapidShare Cases: Oberlandesgericht, Hamburg, 2. July 2008; District Court of Düsseldorf, 23. January 2008; Regional Court of Hamburg, 12.6.2009.*

45 *Online-Gatebuch, AU5 – OGH, 21/12/2006, 6 Ob 178/04a.*

46 *Bunt v. Tilley & Others, UK1 – Queen's Bench Division, 10/03/2006, [2006] EWCH 407 (QB); [2006] ALL ER 336; [2006] EMLR 523.*

47 *Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights.*

48 *L'oreal SA v eBay, Case C-324/09, (CJEU, 12 July 2011).*

49 *Scarlet v SABAM, Case C-360/10, (CJEU 24 November 2011); T. Cook, нав. дело, стр. 159.*

је уперен захтев за накнаду штете, имајући у виду трошкове које може изазвати овакав мониторинг. Стога треба бити веома опрезан приликом одређивања ове обавезе и неопходно је бити добро упознат не само са чињеницама сваког случаја посебно, него и са самом инфраструктуром пружаоца услуге и могућих техничко-технолошких решења.

IV Закон о електронској трговини Републике Србије

Кад је реч о Закону о електронској трговини Републике Србије, он скоро у потпуности транспонује решења из Директиве.⁵⁰ У вези са одговорношћу пружаоца услуге информационог друштва закон дословно прати решења Директиве. Међутим, иако је смисао Директиве дословце преузет, оно што би се могло унапредити је сама терминологија, као на пример у одредбама о искључењу одговорности где уместо термина „електронска порука“ треба користити термин „податак“, јер је шири од тренутно прописаног у закону и у складу са Директивом.⁵¹ Кад се говори о трајном складиштењу порука, ту је потребно додати и део који се односи на сазнање о чињеницама или околностима на основу којих би недопуштена активност корисника била очигледна.⁵² Такође, потребно је прецизирати одредбе о обавештавању у складу са већ поменутом НТД процедуром. Што се тиче мера забране, оне се не прописују посебно у овом закону, него се примењују општа правила грађанског процесног права. На крају треба поменути да, за разлику од Директиве, Закон уређује и питање линкова и то по узору на режим за трајно складиштење података.⁵³ Све у свему, Закон је у претежној мери усклађен са Директивом и у његовим следећим изменама би само требало ускладити терминологију, прецизирати и прописати у овом закону неке већ постојеће механизме.

VI Закључак

Иако Директива представља најзначајнији покушај регулације овог питања на нивоу ЕУ до сада, ипак су многа питања остала нерешена и нерегулисана. Прво од тих питања је то што сем чистих посредника, пружаоца услуга привременог складиштења и хостинг провајдера (у

50 Закон о електронској трговини (*Службени гласник РС*, бр. 41/2009; даље у фуснотама: ЗЕТ).

51 ЗЕТ, чл. 16.

52 ЗЕТ, чл. 18.

53 ЗЕТ, чл. 19.

члановима 12, 13 и 14) Директива не регулише друге подједнако значајне посреднике као што су претраживачи и хиперлинкови / линкови. Неке земље су по угледу на правила прописана за посреднике у Директиви уредиле и ово питање, али свакако остаје чињеница да се Директива не бави овим питањем. Такође, питање се поставља и са дефинисањем пружаоца услуге информационог друштва који захтева елемент накнаде, имајући у виду да је већина данашњих услуга која се пружа на интернету бесплатна, јер се профит не остварује директном накнадом, него углавном кроз закуп рекламног простора или се циља на популарност сајта или неке компаније послују само због стварања *goodwill*-а. Такође, имајући у виду технолошки напредак поставља се и питање прецизности дефинисања улоге посредника у члановима 12, 13 и 14. Приметно је у том погледу да, у поређењу са системом у САД-у, на једној страни (у САД) имамо презаштићене пружаоце услуга информационог друштва док у ЕУ Директива махом штити „традиционалне“ пружаоце услуга информационог друштва (нпр. *caching* и *web hosting*), док су пружаоци услуга нових пословних модела (нпр. Веб 2.0 модели) мање заштићени, него у САД.⁵⁴

Једно од најважнијих питања које се јавило у вези са ревизијом Директиве јесте препозната потреба да се регулише НТД процедура. Оваква потреба је неопходна у циљу обезбеђивања правне сигурности, јер одсуство ове процедуре приморава пружаоце услуга да врше цензуру како би избегли одговорност, такође омогућава појаву злонамерних обавештења како би се онемогућила конкуренција и на крају прети угрожавању и слободи говора. За разлику од Директиве, амерички *Digital Millenium Copyright Act 2000* детаљно регулише НТД процедуру, и не само то, него и прописује одговорност особа које пошаљу лажно обавештење и такође, прописује и могућност враћања материјала који није требало да буде скинут.⁵⁵ Баш због пропуста Директиве да регулише ово питање, велики је раскорак и разлика међу законодавствима земаља ЕУ која су често врло различита и неуједначена. Примећено је у ранијем излагању да се нпр. НТД процедура другачије уређује од земље до земље, али што је још значајније и горе за цело стање је што се помнута процедура користи у различите сврхе. Управо је огромна дискрепанца у регулативи земаља ЕУ разлог неефикасности и неусклађености кад је реч о електронској трговини и одговорности пружаоца услуга информационог друштва.

Због свих ових разлога ЕУ је и покренула иницијативу за измену Директиве и завршила јавне консултације у вези са Директивом још

54 *EU Study from 2009*, стр. 11–34.

55 Р. Baistrocchi, *нав. дело*, стр. 130.

2010. године.⁵⁶ Решавање ових питања кроз измену Директиве би била неопходно како би се омогућила несметана електронска трговина и повећао обим њене размене.

Adriana MINOVIĆ

Marko MATOVIĆ

LIABILITY OF INFORMATION SERVICE PROVIDERS IN E-COMMERCE AT THE EUROPEAN UNION LEVEL

Summary

The authors of this article state that expansive and huge development of new technologies and the Internet affects all spheres of life in significant manner, especially the way in which markets and international transactions are conducted. Therefore, e-commerce due to its significant benefits and affordability begins to occupy a dominant position in the global transactions. However, the fast growing development of technology has its flaws such is a possibility of monitoring and regulating new solutions in this area. As one of the most important issues in the field of electronic commerce the authors see the question of liability of information service providers. Although this question is already regulated with existing legal principles and rules relating to liability, it should be borne in mind the specificity of this activity, which requires a special set of rules for it. Certainly the most significant attempt to regulate electronic commerce on the EU level is the Directive 2000/31/EC on electronic commerce which devoted special attention to the rules of liability of information service providers when they are acting as intermediaries.

Directive stipulates a so-called regime of “safe harbor” which requires that service providers when they are doing a mere conduct of intermediary services or acting as cashing or hosting, if they meet certain requirements set out in Articles 12, 13 and 14 of the Directive are not responsible for the content they carry, nor do they have an obligation to control the content that they transmit.

56 Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC), доступно на адреси: http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm; JF Bretonniere, *Liability for internet host providers in the European Union: time for a reform?*, France, 2011, стр. 31, доступно на адреси: <http://www.iam-magazine.com/issues/Article.ashx?g=f8e060f5-378c-4979-a1d5-0ef3a42f0c9c>.

Although these rules are exempting them from liability and damages, they are still bound to react by removing or blocking content or by other means of preventing access to illegal content, from the moment when they gain knowledge of illegal contents or when they receive an order from a competent body. The manner on which information service provider is informed about the illegal content varies from country to country and it is not uniquely designed at EU level, but definitely one of the most recommended mechanisms is "Notice and Take Down and Procedure". Although there are many critics of this procedure, however, it raises a significant level of certainty which is very important for the predictability and safety of business operations. The problem that arises in regard of these measures (injunctions), is related to the possibility that they may transform into mandatory monitoring measures, if in addition to the imposing obligations of removing illegal material imposes also an obligation to prevent dissemination of illegal material in the future. Therefore, authors conclude that despite the fact that there is definitely a need for revision of the Directive and a review of existing regime in accordance with the new technology development, also we should be very cautious in regard of prescribing the mechanisms related to the injunctions. Anyway the revision of Directive is necessary in order to overcome non harmonized application of the Directive.

Key words: *e-commerce, liability, safe harbor principle, injunction, information service provider.*