Др Видоје Спасић,*
Ванредни професор Правног факултета,
Универзитет у Нишу

ОРИГИНАЛАН НАУЧНИ ЧЛАНАК
doi:10.5937/zrpfni1674203S

UDK: 347.78:004

Рад примљен: 30.09.2016.
Рад прихваћен: 25.10.2016.

ТЕХНОЛОШКЕ МЕРЕ У ФУНКЦИЈИ КОНТРОЛЕ КОРИШЋЕЊА АУТОРСКИХ ДЕЛА У ИНФОРМАТИЧКОМ ДРУШТВУ**

Апстракт: Информатичко друштво проширило је могућности за коришћење ауторских дела и другог заштићеног садржаја. Самим тим, дигитална технологија је повећала и могућности за неовлашћено коришћење заштићеног садржаја. Наиме, у дигиталном окружењу носиоцима права је наметнут појачан ризик од неовлашћеног коришћења њихових интелектуалних творевина. Носиоци права све мање могу да контролишу коришћење својих творевина, а заштита коју пружају правне норме се у друштву брзе размене информација може показати као недовољно ефикасна. Стога се у пракси све чешће постављају физичке препреке дигиталном коришћењу ауторских дела, генерично назване технолошке мере заштите.

У раду ће бити обрађена питања која се односе на мере превентивне заштите ауторских дела путем технолошких механизма. Међутим, примена оваквих мера изазива одређене последице у ауторскоправним односима. Тако, оне намећу поновно преиспитивање односа између приватних интереса титулара права и јавног интереса да друштво користи и усавршава интелектуална добра. Такође, оне доводе у питање успостављену равнотежу интереса свих учесника у ауторскоправном односу: носилаца права, корисника и уживаоца дела, као и свих осталих субјеката.

Кључне речи: заштићени садржај, технолошке мере заштите, контрола коришћења, заобилажење технолошких мера.

* vidza@prafak.ni.ac.rs

** Рад је резултат истраживања на пројекту „Усклађивање права Србије са правом ЕУ“, који финансира Правни факултет Универзитета у Нишу у периоду 2013–2018. године.

1. Увод

У информатичком друштву повећане су могућности за искоришћавање ауторских дела, односно број имовинскоправних овлашћења која припадају аутору.¹ Међутим, с друге стране, повећане су и латентне опасности од повређивања ауторскоправних овлашћења. Стога се пред ауторе поставио проблем како пронаћи адекватне начине да заштите своја овлашћења, а да то не иде на уштрб легитимних интереса других субјеката или јавног интереса. Решење за наведену ситуацију опет се нуди технологија, односно одговарајуће технолошке мере. У том смислу, главни изазов је унапређење заштите ауторских права у новом окружењу.

Данас техничка заштита ауторских права није више предвиђање или сан, и многа ауторска дела се дистрибуирају у заштићеном формату: музички CD-и користе уграђене *anti-copy* механизме, DVD-јеви садрже сложену техничку заштиту која спречава копирање, „пуштање“ на недозвољеним уређајима или обезбеђује географску дистрибуцију филмова, електронске књиге не могу се копирати, модификовати или се користи на одређени начин.

Непосредна реакција ауторских индустрија на информатичко окружење била је да се технолошке мере укључе у заштиту дигиталних дела, како би се осигурало да просечан корисник не може неовлашћено да користи ауторскоправно заштићене садржаје. Међутим, пракса, а такође и неколико истраживања, показали су да технологије заштите (првенствено засноване на шифровању и сличним методима), не могу да гарантује потпуну сигурност заштите, јер компјутерски научници и талентовани корисници могу да заобиђу ове технологије у релативно кратком року.

Осим изреченог, технолошке мере, саме по себи, нису довољне и оне захтевају одговарајућу правну заштиту од њиховог заобилажења или злоупотребе.

На крају, треба истаћи да установљење и примена технолошких мера заштите у коришћењу ауторскоправног садржаја, изазива и одређена подозрења и контроверзе, па чак ствара и одређене проблеме у ауторскоправним односима. Ово, првенствено, што технолошке мере могу доћи у сукоб са постојећим нормама ауторског права, јер стварају одређени дисбаланс у успостављеној равнотежи интереса учесника у ауторскоправним односима.

1 У односу на друга субјективна права, ауторско право, без сумње, састоји се од највећег броја појединачних овлашћења, посебно имовинскоправних.

2. Појам и улога технолошких мера

У дигиталном свету, безбедност и приватност се имплементирају коришћењем разних криптографских алгоритама и протокола. На самом крају ланца, дигитални садржај се приказује у аналогној форми на тај начин што се дигитална слика трансформише у светло путем дисплеја, док се дигитални звук трансформише у акустичке таласе. При томе, увек је могућа поновна дигитализација ових аналогних сигнала.

Под технолошким мерама подразумева се било која технологија, уређај или компонента која у свом редовном функционисању спречава или ограничава радње коришћења (укључујући и приступ делу) заштићеног добра, за чије предузимање не постоји овлашћење аутора или титулара другог права.² Изражавање ауторских дела у дигиталном формату омогућава различите начине контроле њиховог коришћења. Стога су разноврсне и технолошке мере којима се таква контрола остварује.

Технолошка решења, данас, знатно повећавају могућности заштите дигиталних дела. У том смислу, постоје технолошке могућности за спречавање или ограничавање приступа делу; ограничавање или контролу приступа одређеним изворима дела; ограничавање умножавања, адаптације, дистрибуције, јавног саопштавања или приказивања дела; идентификовање својстава и власништва над делом; као и лакше добијање ауторских лиценци.

Функционално посматрано, постоје три групе мера: технолошке мере контроле приступа, технолошке мере контроле искоришћавања и технолошке мере заштите интегритета дела (Koelman, K.J, Helberger, N: 2000: 166). У прву групу спадају оне технолошке мере чији је циљ да онемогуће неовлашћени приступ информацијама садржаним у ауторском делу. Такве су, примера ради, лозинке, или скрембловање. Скрембловање представља поступак промене редоследа података у току преношења тако да они немају никакво значење ако их прими неко коме нису намењени (Tasić, V. Bauer, I: 1989: 333). Криптовање (криптографија) представља начин шифровања претварањем текста у кодиране поруке које могу да протумаче само корисници који имају кључ (Tasić, V. Bauer, I: op. cit: 93).

Технолошке мере контроле недозвољеног коришћења материјала усмерене су на спречавање неовлашћених лица да предузимају одређене радње које улазе у корпус искључивих ауторскоправних овлашћења. Најчешће је реч о контроли умножавања. Тако нпр. лице које је прибавило примерак

² Чл. 6(3) DIRECTIVE 2001/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Official Journal of the European Communities, L 167, 22. 6. 2001).

ауторског дела у дигиталном облику (нпр. музички CD), може да употребава ауторско дело, али захваљујући уграђеним блокадама (физичким препрекама), не може да сачињава копије истих. У ширем смислу, у ову групу би могле да се уврсте и технолошке мере чији примарни циљ није да онемогуће корисника у искоришћавању дела, већ да прате учесталост и обим дозвољеног искоришћавања на основу чега се касније обрачунава лиценцна накнада. Мере усмерене на заштиту интегритета дела имају за примарну сврху онемогућавање лица која користе ауторско дело да врше било какве измене на делу. Иако се и овим мерама постиже контрола коришћења, с обзиром на то да је реч о неимовинском овлашћењу, сврстане су у посебну групу.

Упоредо са стварањем и применом ових технолошких мера одвија се процес проналажења начина за њихово заобилажење. Стога, делотворност технолошких механизма зависи управо од питања њихове правне заштите коју данас познаје већина савремених правних система. Ипак, нормативна решења нису уједначена. Постојеће разлике заправо одражавају проблеме у проналажењу адекватног облика заштите, који највише произлазе из чињенице да се санкционисањем заобилажења (или претходних радњи) технолошких мера доводи у питање циљ ауторског права уопште.

Два међународна акта тзв. *интернет уговори* регулишу ову материју: WIPO Уговор о ауторском праву и WIPO Уговор о интерпретацијама и фонограмима, оба из 1996. године. Према члану 11 Уговора о ауторском праву, односно чл. 18 Уговора о интерпретацијама и фонограмима, уговорне стране треба да обезбеде одговарајућу правну заштиту и ефикасна правна средства против уклањања ефикасних технолошких мера које аутори, на основу овог Уговора или Бернске конвенције, користе у вези са искоришћавањем својих права; и да у вези са њиховим делима ограниче такве поступке које сами аутори нису одобрили или који нису допуштени законом.

На нивоу ЕУ за предметну материју значајне су две директиве. Најпре, реч је о Директиви о правној заштити рачунарских програма.³ Ова Директива забрањује стављање у промет или држање у комерцијалне сврхе било ког средства чија је једина сврха да олакша недозвољено уклањање или неутрализацију било ког техничког механизма евентуално направљеног у циљу заштите рачунарског програма. Дакле, *stricto sensu*, не сматра се повредом сам акт заобилажења технолошких мера. Такође, није санкционисана ни производња уређаја за заобилажење.

3 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs (Official Journal of the EU L 122, 17/05/1991 p. 42).

Директива о хармонизацији извесних аспеката ауторског права и сродних права у информацијском друштву,⁴ исправила је недостатке претходне Директиве. У том смислу, овом Директивом се обавезују државе чланице да на адекватан начин санкционишу заобилажење било које ефективне технолошке мере, као и производњу, увоз, дистрибуицију, продају, изнајмљивање, оглашавање или поседовање у комерцијалне сврхе уређаја, производа или компоненти који су намењени заобилажењу, односно пружању услуга заобилажења технолошких мера.

Српски Закон о ауторском и сродним правима (ЗАСП)⁵ у чл. 208 и 208а, детаљно је регулисао питање технолошких мера заштите. Под „технолошким мерама“, у смислу ЗАСП-а, подразумева се свака технологија, уређај или део који је конструисан да током своје наменске употребе онемогући или ограничи радње коришћења у вези са ауторским делом или другим предметом заштите, за које носилац ауторског или сродног права није дао сагласност. Технолошке мере сматрају се ефикасним када носиоци права коришћење својих заштићених садржаја ограничавају путем контроле приступа или путем заштитног поступка као што су енкрипција, деформација или друга трансформација заштићеног садржаја или путем механизма за контролу умножавања којима се постиже циљ заштите.

Израз „информација о правима“ означава сваку информацију која потиче од носиоца права и која идентификује ауторско дело или предмет сродноправне заштите, аутора, односно носиоца права, или информацију о условима коришћења дела или предмета сродноправне заштите, или било који број или шифру која представља такву информацију.

У складу са ЗАСП-ом, повреду права представљају следеће радње:

3) производња, увоз, стављање у промет, продаја, давање у закуп, рекламирање у циљу продаје или давања у закуп или држање у комерцијалне сврхе уређаја, производа, саставних делова, рачунарских програма, који су превасходно конструисани, произведени или прилагођени да омогуће или олакшају заобилажење било које ефикасне технолошке мере, и који немају другу значајнију сврху осим наведене;

4) заобилажење било које ефикасне технолошке мере или пружање или рекламирање услуге којом се то омогућава или олакшава;

4 Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society (Official Journal of the European Communities, L 167, 22. 6. 2001).

5 „Сл. гласник РС“, бр. 104/2009, 99/2011, 119/2012 и 29/2016 – одлука УС.

5) уклањање или измена електронске информације о правима или стављање у промет, увоз, емитовање или на други начин јавно саопштавање ауторског дела или предмета сродноправне заштите са којег је електронска информација о правима неовлашћено уклоњена или измењена, а да при том починилац зна или има основа да зна да тиме подстиче, омогућује, олакшава или прикрива повреду ауторског права или сродног права.

Технолошким мерама заштите посвећена је секција 1201. америчког Закона о ауторском праву дигиталног доба из 1998. године.⁶ У основи у овом пропису разликују се две групе технолошких мера: оне које су усмерене на контролу приступа заштићеном делу и оне којима се онемогућава недозвољено вршење ауторских права у вези са заштићеним делом (као нпр. умножавање и јавно саопштавање легално прибављених примерака ауторских дела). Тако, према овом акту, за заобилажење технолошких мера којима се ефективно контролише приступ заштићеном делу; стављање у промет, увоз, нуђење или рекламирање производа и уређаја (и пружање услуга) конструисаних или произведених у сврху заобилажења технолошких мера којима се ефективно штите права аутора, одговорном лицу се могу изрећи грађанскоправне и кривичне санкције.

У смислу наведеног, под заобилажењем се подразумева избегавање, деактивирање, померање или на било који други начин уклањање технолошких мера, а када је реч о контроли приступа, нарочито, дескрембловање и декрипција без сагласности титулара права.

3. Врсте технолошких мера и њихово функционисање у заштити интернет садржаја

Носиоци ауторскоправног заштићеног садржаја ослањају се на разноврсне технолошке мере ради контроле његове употребе, односно заштите од неовлашћених употреба производа и услуга, сачињених од информација различитог типа. Све ове мере се деле у две основне генералне групе: мере хардверског и мере софтверског типа.

3.1. Хардверске и софтверске мере

Мере хардверског типа обухватају различите врсте физичких препрека које се уграђују у техничке уређаје за коришћење и/или умножавање ауторских дела и предмета сродних права. Овакве препреке функционално омогућавају коришћење заштићеног садржаја само у оној мери и на онај

6 Digital Millenium Copyright Act of 1998. – DMCA.

начин који је у складу са оним што је уговорено, односно допуштено. Тако, нпр. у америчком Акту о кућном аудио-снимању⁷ захтева се од произвођача уређаја за дигитално аудио-снимање и дигитално аудио-међуповезивање, уграђивање таквих перформанси које ће ограничавати серијско копирање. Ово се постиже тако што је хардвер програмиран тако да чита информацију која се кодира и која је садржана у „каналу за дигитално поткодирање“ дигиталних звучних снимака и емитовања. На основу информације коју прочита, струјно коло хардвера може дозволити копирање, али ће означити шифрама копије које прави да би се ограничило даље копирање или потпуно онемогућило умножавање. Систем за остваривање серијског умножавања дозвољава неограничено умножавање прве генерације дигиталног оригиналног примерка, као што су CD-и који дистрибуирају компаније које их снимају, али спречава даље дигитално умножавање ових примерака.

Слични системи могу се имплементирати путем хардвера, софтвера или оба заједно користећи одговарајуће концепте. Тако, на пример, фајлови који садрже дела могу обухватити инструкције које се једино користе за управљање или контролисање дистрибуције дела. Ова информација могла би се ставити у одељак за тај део фајла или у други део фајла. Заједно са хардвером или софтвером који је прима, информација се, било да је у заглављу било у неком другом делу, може употребити да ограничи употребу оригинала или копије фајла који садржи дело. Она може ограничити употребу дела само на гледање или слушање. Такође, могуће је ограничити колико се пута делу може приступити, тј. колико се пута оно може „отворити“ или умножити.

3.2. Серверска контрола и контрола на нивоу фајла

У информатичком друштву технологија ће играти централну улогу у имплементацији контроле приступа и употребе заштићених дела на нивоу фајла и сервера.⁸ Дистрибуција дигиталних дела може бити регулисана, првенствено контролом приступа изворима заштићеног садржаја. Приступ овим серверима може варирати од неограниченог (цео садржај сервера на располагању је без икаквих ограничења), преко делимично контролисаног (неограничен приступ дозвољен је само извесним подацима на серверу, а другима не), до потпуно контролисаног приступа (није допуштен никакав неконтролисан приступ, у било којој форми). Контрола приступа

7 The Audio Home Recording Act of 1992. – AHRA.

8 О безбедности на мрежи види шире у: Спасић, В: Онлајн безбедност: Зборник радова Правног факултета у Нишу: 55: 2010: 77–101.

остварује се кроз употребу процедуре идентификације и аутентификације која забрањује приступ серверу неовлашћеним клијентима, у целини или појединим информацијама. Скоро сви провајдерски сервиси, укључујући комерцијалне онлајн сервисе и сервере присутне на интернету, контролишу приступ својим системима.

У пракси, неки провајдери дозвољавају потпуно неограничен приступ информацијама садржаним на њиховим главним серверима, а контролу користе само да би задовољили физичка ограничења својих главних сервера, односно да би ограничили број истовремених корисника. Остали даваоци информација ограничавају приступ непријављеним клијентима. Тако нпр. користећи „ftp“ сервис, клијент може често да се повеже са удаљеним серверима на мрежи, као „н.н.“ лице, али ће моћи нормално да приступи само неким посебним подацима у централном серверу. Наравно, давалац информације може одлучити да не дозволи неконтролисани приступ, и одобрити само овлашћеним лицима да „уђу“ на главни сервер. Контрола приступа главном серверу, који садржи заштићена дела, представља типично средство, односно најчешће ће представљати први ниво заштите коју ће власник садржаја тражити пре него што своја заштићена дела учини доступним на мрежи преко главног сервера.

Други ниво контроле приступа и употребе заштићених дела може се спровести путем контролних мера повезаних са електронским датотекама (фајловима), које садрже дело.

Рестрикције приступа на нивоу фајла могу се спровести користећи одређене карактеристике „помоћног“ софтвера (односно програма за тумачење тзв. „рендеринг“ софтвера). Носилац права, односно власник садржаја, може израдити специјализоване софтверске производе или остварити такве карактеристике софтверских производа за општу примену, које би контролисале ко и у којој мери може користити заштићено дело. Овакве рестрикције могле би се остварити коришћењем својстава поменутог „помоћног“ софтвера јединственог формата фајла, или карактеристика у утврђеном формату фајла, или комбинацијом оба формата. „Контролне“ мере такође би се могле спровести да одреде да ли је власник садржаја дозволио извесне употребе дела, као и неке мере за контролу степена до кога би затим клијент могао да „манипулише“ делом.⁹

Помоћни софтвер, такође, може бити конципиран на начин да оспорава општи приступ делу ако фајл који садржи дело није довољно аутентич-

⁹ Тако, нпр., помоћни софтвер могао би корисника који није добио одговарајућу дозволу од власника садржаја, или који користи неодобрену или застарелу лозинку, спречити да користи податке.

на копија (тј. фајл је измењен у односу на верзију коју је дистрибуирао власник садржаја). Овакве карактеристике омогућавају одређивање која информација, довољна у погледу овлашћене употребе, може бити повезана с фајлом који садржи софтверски производ.

4. Појам и значај криптографије за ауторскоправне односе

4.1. Скривено значење – енкрипција (шифровање)

Функционисање интернета заснива се на технологији комутације пакета, што представља систем код кога поруке пролазе кроз много различитих пунктова, односно компјутера који се налазе на различитим местима и могу бити поседовани и контролисани од стране различитих лица.

Етимолошки, криптографија значи писање тајним знацима, симболима.¹⁰ Криптограм је текст, писмо, спис сачињен тајним знацима, тј. шифрама. Криптографија је грана математике која изучава математичку заснованост криптографских метода. Криптографија или шифровање представља поступак транскрипције (превођења) јасне и разумљиве информације у неразумљив облик применом тајног договора, при чему је такво дејство реверзибилно.

Француско законодавство¹¹ дефинише делатност криптологије као *све радње усмерене на трансформисање јасних информација или знакова у информације, или знакове нејасне за трећа лица помоћу тајних споразума, или на реализовање обратних операција, захваљујући опреми, материјалу или компјутерском програму замишљеним са тим циљем*. Реч је о једној општој дефиницији која, такође, обухвата и стеганографију, вештину тајног писања, која се састоји у скривању једне поруке у другој поруци у ублаженијој форми.

У криптографској терминологији порука се шаље у облику пуног текста (*plaintext*), или јасног, разумљивог текста (*cleartext*). Формирање (*encoding*) садржаја поруке на начин који скрива његов садржај назива се енкрипција (*encryption*).¹² Енкрипција и декрипција обично подразумевају употребу кључа, а метод кодирања је такав да декрипција може бити извршена само уз познавање тачног кључа.

Генерално посматрано, криптографија је уметност или наука држања података тајним. Криптоанализа јесте уметност, вештина прекидања

10 Спомине се још у античко доба код Херодота и Плутарха.

11 Члан 28, Закона 90-1170, са изменама од 29. 12. 1990. године.

12 Енкриптована порука назива се шифрованим текстом (*ciphertext*). Поступак стварања *plaintext*-а из *ciphertext*-а назива се декрипцијом (*decryption*).

(„разбијања“) шифре (нпр. стварање пуног текста без познавања тачног кључа). Криптографија је повезана са свим аспектима сигурног, безбедног информисања и преношења порука, аутентификације (оверавања), дигиталних потписа и електронских плаћања.¹³

4.2. Функције криптографије

Метод енкрипције и декрипције назван је шифровањем, а производ тих поступака се назива шифром. Неке криптографске методе се ослањају на тајанственост алгорита. Међутим, сви модерни алгоритми користе кључ за контролу енкрипције и декрипције. Порука може бити декриптована само ако се зна тачан кључ, односно ако постоји подударност између кључева за енкрипцију и декрипцију.

Постоје два велика, основна типа криптографије: симетрична и асиметрична криптографија.

Код симетричне криптографије исти кључ се користи за шифровање и дешифровање информација. Проблем ове методе је како наћи средство безбедног преноса кључа на кореспондента.

Код асиметричне криптографије се једним кључем скрива а другим открива поруку. Корисник поседује један приватни и један јавни кључ. Он дистрибуира свој јавни кључ, а чува скривеним тајни, односно приватни кључ. У овом случају, теоријски, неограничени број лица може писати кориснику уз помоћ јавног кључа, али само ће корисник моћи да дешифрира поруке својим приватним кључем. Криптографија овде обезбеђује веродостојност података који се преносе путем мреже. Подаци су пренети једино уз знање овлашћених лица.

Други, или исти пар кључева користи се да би се обезбедио идентитет емитера поруке (пошиљаоца). То је поступак аутентификације (оверавања). Корисник криптира (шифрира) поруку својим приватним кључем. Сви корисници моћи ће да дешифрирају поруку јавним кључем, који се подудара са пошиљачевим.

Спој поступака аутентификације пошиљаоца и провере интегритета његове поруке омогућава стварање правих електронских потписа, које је у пракси веома тешко фалсификовати, као и поступак потписивања руком. Информатичка техника омогућава израђивање алатки за производњу

13 Види шире у: Спасић, В: Улога криптографије у трансферу и приступу информацијама на интернету – правни аспекти: Симпозијум о рачунарским наукама и информационим технологијама; Зборник радова YUINFO – Niš: 2001: CD-ROM: електронска публикација.

кључева и коришћење система криптографије на начин препознатљив за корисника.

Да би систем био поуздан, неопходно је да кључеви за коришћено шифровање буду довољно сигурни.¹⁴ Приликом кодирања сигурност кључа произилази из његове дужине. Међутим, што је кључ дужи, то ће трансакција или комуникација бити спорија у смислу времена потребног да се изврши прорачун. Тако, оно што је добијено у смислу сигурности, губи се у погледу брзине и ефикасности.

Да би се дешифровао један документ, без поседовања кључа, потребно је располагати компјутером способним да изврши велики број операција у секунди. Поузданост система зависи од способности рачунара потребног за предузимање радњи за „разбијање“ шифре. Да би операција имала смисла, трошак потребан за „разбијање“ шифре мора бити пропорционалан вредности заштићене информације. Данас, да би се „разбио“ („провалио“) један кључ реда величине 1024 бита, потребно је више милијарди година рачунања компјутером. Међутим, овај систем зависи и од стања технике које еволуира веома брзо. Алгоритам који се данас сматра неразрешивим, не значи да ће такав бити и за неколико година.

4.3. Систем електронског управљања ауторским правима – *Digital Rights Management (DRM)*

Нека данашња технолошка истраживања везана су за стварање дигиталних дела чија је карактеристика отежано копирање, а олакшано добијање дозвола за коришћење. Овакве технологије се називају заједничким именом – *Digital Rights Management (DRM)*. Најједноставнији систем у оквиру ове технологије базира се на „сигурном преносу (трансмисији)“ дигиталног материјала између пошиљаоца и примаоца. Већи степен заштите може бити креиран централизованим извором приступа садржају заштићеним ауторским правом. У том смислу, клијент (уживалац) може добити приступ неким целовитим комплексним подацима, као што су роман или филм, али са приступом само у циљу коришћења дела док је „конектован“ на изворни сајт.

Систем DRM треба да омогући компромис између безбедности материјала, коју захтева власник права; приватности крајњег корисника, као и цене система који ће бити коришћен између учесника у том ланцу. Задати циљеви се постижу употребом различитих криптографских мера.

¹⁴ Најславнији поступак криптовања и један од најсигурнијих, према речима специјалиста, који поставља стандард поступања на интернету, где га је лако прибавити, јесте програм PGP, базиран на систему RSA, који је пронашао Американац Phil Zimmerman.

Истовремено са развојем технолошких мера заштите тече и процес проналажења начина за њихово заобилажење. Стога, делотворност технолошких механизма контроле зависи управо од питања њихове правне заштите, коју данас познаје већина савремених правних система. Ипак, нормативна решења нису уједначена. Постојеће разлике заправо одражавају проблеме у проналажењу адекватног облика заштите, који највише произлазе из чињенице да се санкционисањем заобилажења (или претходних радњи) технолошких мера доводи у питање циљ ауторског права уопште.

У сваком случају, нормативном уређењу технолошких мера заштите мора се приступити са доста опреза. Обезбеђивањем правне заштите ових мера требало би заокружити и стабилизovati систем ауторскоправне заштите уопште. То значи да би се морала задржати неопходна равнотежа интереса свих релевантних субјеката. Технолошким мерама контроле коришћења ауторских дела морају се првенствено заштитити интереси ствараоца. Али, свакако се морају уважавати и легални и легитимни интереси корисника дела и публике (јавности), а нарочито института ограничења ауторског права у корист трећих лица.

4.4. Заштита путем видео-криптовања

Концепт испоруке аудио или видео-садржаја преко јавних мрежа ствара нове проблеме у области ауторског права. Наиме, треба обезбедити систем за прикупљање такси или процентуалне зараде, заштиту од дигиталне крађе, као и то који учесници у процесу су одговорни за обезбеђење сваке карике у том ланцу. Сви ти изазови се намећу пред техничким питањима како применити постојеће правне прописе у дигиталном окружењу.

Код дистрибуције дигиталног видеа до корисника стижу дигиталне копије високог квалитета и свака од њих ће бити једнако доброг квалитета. Међутим, преносом таквог материјала јавним мрежама долази до потенцијалне могућности крађе од стране пирата. Носиоци ауторских права интернет често доживљавају као медијум где је њихов материјал свима доступан онлајн. Крађа материјала са интернета је могућа, иако није баш једноставна. Један од начина да носиоци права буду убеђени у сигуран пренос је криптовање материјала при транзитну кроз мрежу и директно декриптовање пре његовог емитовања.

Поступак криптовања мора да задовољи комерцијалне захтеве за видео-сервисима, наведене захтеве сервера, као и захтеве корисника ауторских права. Систем треба да заштити видео-власништво од крађе при транзитну кроз мрежу, меморисању на серверу, као и приликом декодирања и прика-

зивања од стране корисника. Такође, потребно је обезбедити да квалитет видео-сигнала буде стално задржан.

Носилац ауторског права има право да постави низ захтева пред креаторе система за видео-сервисе како би били уверени да ће њихова инвестиција бити адекватно заштићена. Први захтев се односи на ауторизацију корисника и гаранцију за сигуран трансфер новчаних средстава ка носиоцу ауторског права. Други захтев носилаца ауторских права би се односио на активну заштиту њиховог власништва путем криптовања за све време транзита кроз јавну мрежу. Коначно, носиоци ауторског права могу захтевати да се видео декриптује само на уређајима крајњег корисника, и то тако да корисник нема директан приступ декриптованом видео-садржају, како га не би могао даље копирати. Ова ограничења се не односе само на систем за проток видеа, већ и за пројектовање алгоритма за видео-криптовање. Онлајн видео-сервис мора да обезбеди аутентификацију потрошача, као и могућности за несметано плаћање. Такође, захтева се да видео буде криптован од када напусти централни сервер, па све док не буде декриптован и декодован на страни корисничког уређаја за плејбек.

Широки опсег сервера подразумева различит хардвер, оперативне системе, као и софтвер, што значи да криптовани дигитални видео-сигнал мора да буде компатибилан са свим постојећим и будућим видео-серверским системима, односно платформама.

5. Закључак

Дигитално доба свакако је нова претња заштити ауторских права. Међутим, технологија би могла и да омогући обезбеђивање нових алата и средстава за заштиту ауторског дела у дигиталном окружењу. Врло брзо технолошка решења или помоћи били су осмишљени од стране индустрије ауторског права. „Одговор на машине је у машини“ (Clark, C: 2014).

Неке технолошке мере имају за циљ управљање лиценцама о употребама права и одредбе о делима у складу са правилима таквих употреба: оне се зову *Digital Rights Management* (DRM). Системи DRM базирани првенствено на криптографији развијени су у последњих неколико година с циљем да се позабаве питањем трновите заштите и управљања ауторским права у електронском окружењу. DRM може бити истовремено нова норма, паралелна оној за ауторско право. Технологија је допуна, односно акцесоријум уз ауторско право. Међутим, она прети да постане његова супституција која потенцијално може учинити ауторско право потпуно ирелевантним.

Истовремено са развојем примене ових мера тече и процес проналажења начина за њихово заобилажење. Упоредо са развојем DRM система, носиоци ауторских права су тражили и правну заштиту од таквих техничких помагала и баријера. Технологија може бити поражена од друге технологије, као што је то доказано у многим случајевима хаковања заштите DVD-ја и других DRM система. Стога, делотворност технолошких механизма зависи управо од питања њихове правне заштите, коју данас познаје већина савремених правних система. Због тога су донети прописи о забрани неовлашћеног заобилажења технолошких мера заштите ауторског дела на међународном и националном нивоу. Ипак, нормативна решења нису уједначена. Постојеће разлике заправо одражавају проблеме у проналажењу адекватног облика заштите, који највише произлазе из чињенице да се санкционисањем заобилажења (или претходних радњи) технолошких мера доводи у питање циљ ауторског права уопште.

У САД технолошке мере заштите од неовлашћеног коришћења имају значајну улогу у контроли коришћења заштићеног садржаја. Таква контрола назива се „резерва“ и прави се разлика између два основна облика резерве. Прва се назива тајна или интелектуална резерва, и она омогућава носиоцу да задржи непознате нематеријалне ствари од ометања или ограничавања. Друга, економска резерва, или резерва на тржишту, омогућава да ће дело или други заштићени садржај бити под његовом контролом, и то кроз преношење овлашћења на права интелектуалне својине или санкционисањем неких понашања правним средствима, нпр. путем нелојалне конкуренције (Mousseron, J. M, Vivant, M: 1989: 2–4). Резерва, дакле, резултира из комбинације DRM и одредбе о заобилажењу, и она је хибридна мешавина интелектуалне резерве и економске резерве.

Када носиоци права одлуче да обезбеде дигитални садржај неким дефинисаним правилима употребе, као нпр. укључивањем броја копија, броја дозвољених гледања, итд..., ова употреба постаје норма за примаоце и кориснике таквог садржаја, иако конкретна употреба тих дела у складу са законом може бити шири и мање ограничена.

Дусолије истиче да технолошка заштита постаје преширока и више субјективизирана него што је објективна (Dusollier, S.V: 2005: 163). У дигиталном свету посредници су нестали и носиоци ауторских права почели су да дистрибуирају своја дела директно јавности. Прибегавање технолошким мерама омогућава контролисање обеју страна преноса у ауторско-правном односу. Технолошка заштита ауторских права чини да приступ, коришћење, односно уживање дела улази сферу монопола носиоца ауторског права. Следствено томе, можемо рећи да је кôд закон, односно

да дигитални кôд успостављен од стране DRM-а делује као пропис који мења човеково културно и друштвено понашање према ауторскоправно заштићеном садржају. Овакво проширење контроле ауторске области није само допуштено техничким и чињеничним акцијама, већ је обезбеђено законом кроз одредбе о забрани заобилажења технолошких мера. Дакле, у САД и ЕУ технолошки капацитети сада диктирају правни оквир заштите ауторских права. Технолошке мере све више постају супституција/замена за ауторска права, иако се и даље широко представљају као његов обичан суплемент.

На тај начин, стварање правила о начину употребе информација постаје све више приватизовано, а правна моћ да дефинише границе јавног приступа информацијама је умањена. По самој својој природи, технологија би требало да има протетски карактер: да смањи и замени недостатке пре него да их допуни (комплетира). Технологија је створена с циљем да исправи одређене мањкавости, а не да би стварала нове сличне недостатке. Употреба технологије у ауторскоправним односима је решење, односно лек за недостатак ефикасне заштите ауторских права. Међутим, да би се остварило њено пуно дејство и моћ, она је створена у одсуству ауторских права или макар прикривањем ауторских права иза диктата технологије.

Враћање изворних принципа у законодавство о ауторском праву је једино решење да би се задржала прихватљива равнотежа интереса у ауторскоправним односима и да би се технологија користила као адекватан алат и помоћ. Циљ је да примена помоћне технологије у ауторском праву постане управљање односима између технологије и ауторскоправних прописа, а не замена једног другим. Коначно, закон мора да пронађе ефикасно и уравнотежено решење за очување свих законских изузетака у ауторском праву.

Резимирајући, можемо констатовати следеће. Употреба технолошких мера заштите ауторскоправно заштићеног садржаја, осим позитивних ефеката, изазива и одређене проблеме у ауторскоправним односима. Прва последица је да се применом оваквих мера фактички проширује садржина субјективног ауторског права установљена законом у корист носилаца права, а на штету других субјеката.

Уграђивањем технолошких мера којима се спречава неовлашћено коришћење, може се догодити да искоришћавање буде онемогућено и лицима која иначе имају овлашћење да предузимају поједине радње. При томе, када је реч о уговорном овлашћењу, проблем углавном није приметан, јер се овлашћена лица (корисници) најчешће снабдевају потребним средствима за уклањање заштитних механизма (нпр. лозинкама). Међутим, са за-

конским овлашћењима (тј. ограничењима субјективног ауторског права), ствари стоје посве другачије и велика категорија субјеката је онемогућена да користи своја законска овлашћења.

Апсолутна заштита технолошких мера постоји само када је реч о умножавању у приватне сврхе: физичком лицу је дозвољено умножавање примерака објављеног дела за личне некомерцијалне потребе, уколико такво умножавање не захтева заобилажење технолошких мера или пружање или рекламирање услуге којом се то омогућава (Чл. 46 (1) у вези са чл. 208 (1) (4) и (5) српског ЗАСП-а).

Заобилажење технолошких мера искључиво ради вршења овлашћења аутора сходно законским ограничењима, сем умножавања у личне некомерцијалне сврхе, представља основ искључења одговорности за повреду ауторског права (Радовановић, 2011: 399–411).

Из наведеног произлази да заобилажење технолошких мера заштите не представља увек повреду права, јер у одређеним случајевима постоји „овлашћење“ да се предузму такве радње. Ипак, уживаоци дела најчешће не располажу технолошким вештинама или средствима потребним за заобилажење технолошких мера, због чега је неопходно да користе услуге трећих лица или да прибаве адекватна средства. Дакле, производња и стављање у промет вишенаменских уређаја код којих је омогућавање заобилажења само једна (али не примарна) функција, нису стављени ван закона. Према томе, за пружање услуга заобилажења технолошких мера без позивања на изузетке постоји одговорност.

Литература

Dusollier, S.V: Droit d'auteur et protection des oeuvres dans l'univers numérique: Larcier: 2005.

Devèze, J. L, Frayssinet, J: Droit de l'informatique et de l'Internet: PUF: 2001.

Vivant, M. et al., Lamy Droit de l'informatique et des réseaux: Lamy: 2007.

Vivant, and Jean-Louis Navarro, L. J: Code de la Propriété intellectuelle: Paris: 2016.

Koelman, K.J, Helberger, N: Protection of Technological Measures, u: Copyright and Electronic Commerce – Legal Aspects of Electronic Copyright Management: Kluwer Law International (ed. P. Bernt Hugenholtz): The Hague, London, Boston: 2000.

Marković, M. S: Pravo intelektualne svojine i informaciono društvo, Beograd, 2014.

Macrez, F: Les cumuls de droits intellectuels sur les créations informatiques: Strasbourg: 2008.

Mousseron, M.J. & Vivant, M: « Les mécanismes de réservation et leur dialectique: Le «terrain» occupé par le droit », Semaine Juridique, Cahiers de Droit de l'Entreprise: 1989/1, 2–4.

Радовановић, С: Технолошке мере у систему заштите ауторског права: Зборник радова Правног факултета у Новом Саду: 1/2011: 399–411.

Спасић, В: Ауторска дела у дигиталном окружењу: Ниш: 2011.

Спасић, В: Дигитално управљање правима: Право и привреда: Београд: 2011: 4–6: 909–926.

Спасић, В: Онлајн безбедност: Зборник радова Правног факултета у Нишу: 55: 2010: 77–101.

Tasić, V. Bauer, I: Rečnik kompjuterskih termina: Beograd: 1989.

Herak, K.: Digital rights management (DRM): Zagreb: 2005.

Clark, C: „The answer to the machine is in the machine”: European Publishers Council, 2014. Retrieved 20. 6. 2016. from <http://copyright-debate.co.uk/?p=641>

Vidoje Spasić, LL.D.

Associate Professor,

Faculty of Law, University of Niš

TECHNOLOGICAL MEASURES FOR CONTROLLING THE USE OF COPYRIGHTED WORKS OF AUTHORSHIP IN THE INFORMATION SOCIETY

Summary

Information technology has given rise to the problem of controlling the use of copyrighted works of authorship from their unauthorized use. In this context, one of the effective solutions is the application of technological protection measures, which are aimed at a more efficient application of the protection measures prescribed by the law.

Technological protection measures imply the use of any technology, device or component which may be aimed at preventing or restricting an unauthorized use of a protected work of authorship, which has not been approved by the author or holder of some related right. Generally, all these measures may be classified into three basic groups: technological measures aimed at controlling access, technological

measured aimed at controlling exploitation, and technological measures aimed at protecting the integrity of the work of authorship. Considering their technical characteristics and mode of application, they may be hardware-based measures, software-based measures, or a combination thereof.

Modern technology has enabled the development of digital systems which entail a controlled use of copyrighted works and facilitate obtaining licences for their exploitation. They are commonly known as digital rights management (DRM). The DRM system should provide for a compromise between safeguarding the intellectual property rights of the copyright holder, the end user privacy, and system costs. The envisaged goals are achieved by employing various cryptographic measures.

The process of developing technological protection measures is accompanied by concurrent attempts to circumvent the application of these measures. Thus, the effectiveness of these measures primarily depends on their legal protection, which has been recognized by a vast majority of legal systems, we now know the most modern legal system. However, the normative solutions are not uniform. The observed differences actually reflect problems in finding adequate forms of protection, which mostly stem from the fact that sanctions for evasion of technological measures call into question the ultimate purpose of copyright law in general.

Yet, the regulation of technological protection measures must be approached with great caution. Envisaging relevant legal protection for these measures should contribute to providing a comprehensive and stable system of copyright protection. Moreover, it is essential to ascertain the necessary balance of interest of all relevant subjects involved in that process. Technological measures for controlling the use of copyrighted works of authorship should primarily protect the authors' rights and interests; however, they certainly must encompass the legal and legitimate interests of the end-users as well as the general public, particularly considering the statutory limitations to authorship rights in favour of third parties.

Keywords: *copyrighted work of authorship, technological protection measures, digital rights management, control of use; circumvention of technological protection measures.*