

САДРЖАЈ

ОСНОВИ КОМПЈУТЕРСКОГ ПРАВА	1
Увод	1

Глава I

КОМПЈУТЕРСКО ПРАВО	4
1. Појам и предмет компјутерског права	4
2. Историјски развој компјутерског права	8
3. Извори компјутерског права	9
4. Однос компјутерског права и других грана права	11
4.1. Компјутерско право и право информационе технологије	11
4.2. Компјутерско право и информатичко право	12
4.3. Компјутерско право и информационо право	12
4.4. Компјутерско право и телекомуникационо право	13

Глава II

ПРАВНА ЗАШТИТА КОМПЈУТЕРСКИХ СИСТЕМА	15
ЗАШТИТА ПОДАТАКА	15
1. Уводне напомене о заштити података	15
1.1. Објекти заштите	17
2. Посебно о заштити права приватности	20
3. Инструменти заштите података	21
3.1. Правни инструменти заштите података	23
4. Посебно о заштити података у електронској размени податка	30
4.1. Европски модел EDI Споразума	35
5. Национални инструменти заштите података	36
5.1. Инструменти заштите података у праву Србије	39
ЗАШТИТА КОМПЈУТЕРСКИХ ПРОГРАМА И СОФТВЕРА	41

1.	Уопште о заштити компјутерских програма и софтвера	41
2.	Компјутерски програм и патентноправна заштита	42
3.	Компјутерски програми и заштита жигом	45
4.	Компјутерски програми и заштита од нелојалне конкуренције	48
5.	Компјутерски програми и ауторскоправна заштита	50
6.	Компјутерски програми и заштита <i>sui generis</i> правом.....	53
7.	Компјутерски програми и заштита пословне тајне	54
ЗАШТИТА БАЗА ПОДАТАКА		58
1.	Опште напомене о заштити база података	58
2.	Правна заштита база података.....	59
3.	Базе података и ауторскоправна заштита.....	60
3.1.	Базе података и регулисање заштите од нелојалне конкуренције	61
4.	Базе података и међународна заштита.....	61
4.1.	Нова <i>sui generis</i> заштита база података	64
5.	Правна заштита база података по нашем праву	65
ЗАШТИТА ТОПОГРАФИЈЕ ИНТЕГРИСАНИХ КОЛА		67
1.	Правна заштита топографије интегрисаних кола у упоредном и међународном праву	67
2.	Заштита топографије интегрисаних кола у нашем праву	69

Глава III

ЗАШТИТА ОД КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА		71
1.	Опште напомене о заштити од компјутерског криминалитета.....	71
2.	Појам и обележја компјутерског криминалитета	72
3.	Компјутерска кривична дела	74
3.1.	Прављење и убацивање компјутерских вируса	76
3.2.	Хакинг	79
4.	Остала типична компјутерска кривична дела	87
4.1.	Компјутерска крађа.....	87
4.2.	Компјутерске преваре.....	87
4.3.	Компјутерске саботаже и тероризам.....	88
4.4.	Софтверска „пиратерија“	88

5.	Правне мере заштите од компјутерског криминалитета	91
5.1.	Правне мере заштите у националним прописима	91
5.2.	Компјутерски криминалитет и међународноправна заштита ...	93
5.3.	Правна заштита од компјутерског криминалитета у нашем праву.....	96

Глава IV

ЕЛЕКТРОНСКА ЕКОНОМИЈА, ЕЛЕКТРОНСКА ТРГОВИНА И УГОВОРИ У ЕЛЕКТРОНСКОЈ ФОРМИ.....100

1.	Електронска економија	100
2.	Електронска трговина.....	101
2.1.	Кратак историјски развој електронске трговине	103
3.	Правне претпоставке развоја електронске трговине.....	106
3.1.	Општа правила о уговорима	107
4.	Специфичности уговора у електронском облику	114
4.1.	Нека општа правила о закључењу уговора у електронском облику	114
4.2.	Специфичности коришћења интернета у процесу закључења уговора	116
5.	Web уговори	117
5.1.	Уопште о изјави воље на Web страници.....	118
5.2.	Специфичности Web уговора.....	119
5.3.	Web уговори као формуларни уговори	122
5.4.	Click wrap и browse wrap уговори	123
5.5.	Потврда склапања уговора.....	129
5.6.	Место одашиљања и пријема електронске поруке.....	130
6.	E-mail уговори.....	131
7.	Електронско плаћање – електронски пренос средстава.....	134
7.1.	Уводне напомене о електронском плаћању	134
7.2.	Електронско банкарство.....	136
7.3.	Правни инструменти заштите у вези са електронским преносом средстава.....	139

Прилог

Закон о заштити података о личности	144
Директива савета европске заједнице о правној заштити компјутерских програма	169
Закон о ауторским и сродним правима	177
Конвенција о високотехнолошком криминалу	179
Кривични законик републике србије	205
Закон о електронској трговини	207

ОСНОВИ КОМПЈУТЕРСКОГ ПРАВА

Увод

Изузетно брз развој глобалне информационо технолошке инфраструктуре и њено увођење у безмало све сфере људских активности суштински су утицали на укупан развој модерне цивилизације с краја 20-ог и почетка 21-ог века. Само у последњих неколико година број интернет корисника се у свету повећао више десетина пута, а трендови улагања у усавршавање компјутерских технологија и даље бележе узлазне путање. Компјутери, интернет и модерна средства телекомуникација занимљиви су, корисни али и неопходни људима свих генерација (деци, њиховим родитељима, бабама и дедама), различитих професија (политичарима, судијама, полицији, трговцима, домаћицама...) и коначно незамењиви и незаобилазни у свим људским делатностима (државним службама, војсци, саобраћају, образовању, медицини, економији, индустрији, науци...).

Као уосталом и увек у историји масовно коришћење нових техничких достигнућа пружа људима до тада незамисливе погодности али, у исто време, наговештава и неопходност промишљене правне регулативе. У овој области се нужност таквог правног регулисања, више него и у једној другој раније, испољава и као нужност успостављања јасних, хармонизованих и кохерентних међународних „правила игре“. Јер ако су савремена информационо-комуникациона технолошка средства од света заиста направила „глобално село“ било је неопходно у том „селу“ утврдити правила понашања једнака за све. Додатни разлог за то врло брзо постају и јасно уочљиве могућности злоупотребе и криминала које се непосредно или посредно везују за компјутерске технологије. Мада аргументе за овакве тврдње и није потребно наглашавати ево неколико најважнијих:

- више десетина хиљада персоналних компјутера свакодневно бива увучено у тајне мреже које шире вирусе и друге штетне програме који представљају опасност како за саме рачунаре тако и за податке у њима потхрањене;

- уз помоћ рачунара и интернета интелектуална својина још обухватније наставља да се суочава са високим нивоом пиратства на кључним тржиштима широм света, а економска штета настала на овај начин мери се десетинама милијарди долара;
- према подацима из прве половине 2005. године само у САД је употребом односно злоупотребом компјутерских технологија и интернета злоупотребљено близу 50 милиона кредитних картица као и других персоналних података и информација;
- нека истраживања рађена такође у САД показују да је више од 20 % испитаника на неки начин било жртва преваре или крађе кроз злоупотребу персоналних информација и компјутерске технологије;
- нова форма трговине, тзв електронска трговина, која свој развој дугује управо погодностима које пружа компјутерска и интернет технологија такође је озбиљно угрожена пре свега потенцијалним опасностима од цурења и злоупотребе података односно информација;
- нове технолошке претње постоје и у области тероризма. Мада терористи и даље користе традиционалне методе напада извесно је да ће у будућности методологија њиховог деловања бити све чешће базирана на компјутерским технологијама. Ово посебно имајући у виду да је велики део светске инфраструктуре рањив на такве нападе управо због њихове високе зависности од тих технологија;
- све се озбиљније схватају упозорења о опасности избијања тзв. сајбер рата (*cyber war*) обзиром да се у војној индустрији широм света огромна средства издавају за војне потребе и нарочито у сврху коришћења *cyber* технологија као моћног оружја.

Примери које смо претходно навели само су један кратак приказ постојећих и потенцијалних проблема са којима се човечанство суочава или се може суочити обзиром на све ширу и супстанцијалну зависност од коришћења компјутерских и других информационих технологија. Разуме се, историја се не може зауставити нити се време може вратити у назад, све и да за тако нешто постоји потреба. Погодности које пружа коришћење интернета

и других модерних технологија права су свих људи. Али је са друге стране неопходно, баш као што је претходно и наглашено, правно регулисати и уредити ову широку област како би се предупредиле опасности и злоупотребе права које прете да обесмисле ову важну тековину човечанства.

Глава I

КОМПЈУТЕРСКО ПРАВО

1. Појам и предмет компјутерског права

Израз компјутерско право почиње се употребљавати крајем 70-их и почетком 80-их година прошлога века најпре у САД и то примарно међу правницима практичарима који су се у то време све више суочавали са широком лепезом правних проблема везаних за употребу и коришћење рачунара. Имајући у виду да су компјутери изузетно брзо продирали у све сфере друштвеног живота такви проблеми су се најпре повезивали са питањима интелектуалне својине, нелојалне конкуренције, уговора, електронске обраде података, информатиче приватности, електронског преноса података...

Тешкоће узроковане непостојањем посебних правила и прописа који уређују правне односе настале употребом компјутера и компјутерске технологије решаване су у почетку најчешће применом правне аналогије. Тако су рецимо компјутерске крађе третиране као класичне крађе, компјутерски обрађени и складиштени подаци подвођени су под право приватности, а софтвер под ауторско право. И међу еминентним правницима све до краја прошлога века нису била ретка мишљења да заправо и не постоји нешто што би се могло назвати компјутерским правом односно да је оно што се популарно тако назива заправо тек еkleктичан скуп норми настао коришћењем појмова и правила из већ раније фомираних правних области који се примењују на релативно нове технологије везане за компјутерске хардвере и софтвере, електронску пошту и интернет.¹ Овакав приступ је у практичном смислу могао бити ефикасан док се број и врста правних односа

¹ Не постоји таква ствар која би се могла назвати компјутерско право, изјавио је познати амерички судија Френк Истербрук (Frank Easterbrook) 1996. године док је његов колега Герхард Каспер (Gerhard Casper) нешто раније рекао да не постоји „право на коњу“ (*law of the horse*), мислећи при томе управо на компјутерско право. Наведено према: What is Computer Law, Ronald B. Standler, www.rbs2.com/cdefn.htm .

у које су компјутерске технологије инволвиране, било као предмет или средство размене информација, нису до те мере усложнили да је многе од њих било немогуће подвести под неке већ познате правне принципе. Из тог разлога бројне државе поступно почињу да мењају постојеће или доносе посебне прописе који за предмет имају искључиво нека од питања која су везана за употребу или статус компјутера или компјутерских технологија. Овакве тенденције јављају се и на нивоу важних међународних и струковних организација и тела, а у вези прописа које оне доносе.

Упоредо са изменама позитивних законских прописа односно са доношењем нових прописа на националном и на међународном нивоу и правна наука постаје све више заинтересована за ову област увиђајући бројне њене специфичности. Додуше, као што је претходно и наглашено, теоријске расправе и недоумице о томе да ли постоји довољно елемената за издвајање онога што је предмет компјутерског права у посебну грану права постојале су и постоје. Важно је међутим констатовати да су сличне контраверзе и дилеме пратиле и стварање многих других правних дисциплина односно да пут њиховог стварања никада није био ни једноставан ни брз.

У општем смислу компјутерско право се може одредити као скуп правних норми, институција и принципа којима се регулишу односи који настају развојем и применом компјутерских технологија. Сваки покушај доласка до неке садржајније дефиниције подразумевао би претходно дефинисање појма „компјутерска технологија“ у ком погледу међутим не постоји јединствен став. Наиме, у упоредној стручној литератури уочљива су с тим у вези два схватања: прво, уже – које полази од тога да је компјутерска технологија она која је искључиво везана за компјутере, технике и принципе по којима они функционишу; друго – шире, према којем компјутерске технологије обухватају још и средства која се на њима базирају (али не телекомуникациона), средства помоћу којих се информације преносе као и методе и технике које за тај пренос служе. Но у сваком случају и независно од претходно изнете дилеме везане за одређење појма компјутерске технологије чини се да је компјутерско право сврсисходније дефинисати на начин који би „покривао“ сталне и у будућности очекиване новине у области компјутерских технологија, али и свих других технологија подобних за обраду информација у електронској форми. Ово и по цену извесних преклапања са такође новим правним дисциплинама као што су рецимо информатичко или информационо право.

У упоредној литератури могу се међутим срести и другачија одређења појма компјутерског права. Према једном од њих под компјутерским правом се подразумева грана права која регулише технолошке аспекте информација односно право којим су регулисани различити аспекти обраде информација. Под појмом обраде информација се у овом смислу подразумева аутоматска обрада или пренос дигиталних информација независно од технологија које се при томе користе.² Ово практично значи да се под „капу“ компјутерског права могу подвести не само односи који су непосредно везани за обраду информација путем компјутера већ и путем свих осталих уређаја технолошки оспособљених да врше обраду дигиталних информација односно информација у електронској форми. Међу такве уређаје могли би се сврстати мобилни телефони али и они мање уобичајени уређаји као што су рецимо електронски тостери који садрже специјално уграђене полупроводничке чипове или машине за прање којима се може управљати путем интернета.

Две претходно изнете дефиниције компјутерског права се очигледно разликују али не суштински, ма како то на први поглед изгледало. Наиме, полазиште у одређењу појма компјутерског права у првој дефиницији су односи који настају развојем и применом компјутерских технологија, што су ван сваке сумње примарно односи који за предмет имају различите аспекте обраде информација у електронској форми. У другој дефиницији компјутерско право се опет одређује из угла природе односа које регулише (аутоматска обрада и пренос дигиталних информација односно информација у електронској форми), а независно од технологије која се при томе користи. При томе је несумњиво да се, када је реч о коришћеној технологији, овде пре свега мисли на компјутерске али и све друге њима компатибилне и сродне технологије. Отуда би једна синтетичка дефиниција компјутерског права могла гласити и овако:

Компјутерско право је грана права која за предмет има регулисање правних односа који извиру из различитих аспеката обраде и преноса информација у електронској форми и то пре свега применом компјутерских и њима сродних технологија.

² Reed C – Angel J: Computer Law, Oxford University Press, New York 2003, p. 2-3.

У најопштијем смислу предмет регулисања ове гране права одређен је врстом правних односа који су њоме регулисани. Имајући то у виду могло би се рећи да предмет компјутерског права између осталог обухвата:

- заштиту рачунарских програма, софтвера, корисничког интерфејса, продуката реверзибилног програмирања, компјутерски генерисаних дела, назива;
- заштиту топографије интегрисаних кола;
- заштиту база података;
- компјутерске уговоре;
- заштиту података, информација и права појединаца угрожених компјутерском технологијом (приватност пре свега);
- компјутерски криминалитет односно кривична дела везана за коришћење компјутерске технологије;
- одговорност за грешке које настају коришћењем компјутера, у програмирању, заштити података, прекограничним токовима, ЕДИ окружењу...;
- осигурање од разних облика ризика;
- техничке норме којима се регулишу разна питања софтвера, хардвера и стандарда;
- методологију прикупљања, обраде, чувања, трансфера и коришћења података и информација;
- легитимитет и аутентичност докумената и информација добијених применом компјутерске технологије.³

Мада претходно одређено као посебна и самостална грана права компјутерско право је у свакој држави део јединственог националног система права тако да се сва начела и појмови тог система протежу и на њега. У исто време оно је тесно повезано и са међународним нормама и гранама права које

³ Наведено према: Дракулић М: Основи компјутерског права, Београд 1996, стр.29-30.

регулишу међународне, посебно међународне пословне односе. Сматра се ипак да се компјутерско право, мада задире на посредан начин и у многе друге правне области, најтешње може везати за правна питања интелектуалне својине, компјутерског криминала, заштите података и компјутерских уговора односно електронског пословања.

2. Историјски развој компјутерског права

Видели смо претходно да је компјутерско право сасвим нова, још увек недовољно оформљена правна дисциплина. О њеном историјском развоју може се у најбољем случају говорити тек у контексту последњих неколико десетина година. Отуда би могли рећи да ова грана права, посебно ако је поредимо са историјом права уопште, тек треба да створи своју сопствену историју или, другим речима, да се њена историја управо дешава и ствара у времену чији смо савременици.

Настанак и развој компјутерског права се у првом реду доводи у везу са САД, државом у којој су се компјутерске технологије први пут појавиле и државом која је и данас светски лидер у њиховом развоју. Проблемима употребе, коришћења и промета компјутера и компјутерских технологија амерички правници се почињу спорадично бавити већ крајем 60-их година прошлога века када се јављају и први радови у којима се разматра проблематика везана за рачунаре, опрезно називана у општем смислу компјутерско право. Ипак свој прави и пуни развој ова грана права доживљава тек крајем 80-их и почетком 90-их година 20-ог века. То је време када се мноштвом различитих питања која у ширем смислу улазе у оквире компјутерског права почиње озбиљно бавити и правна наука па се у литератури среће све више радова, књига и уџбеника из ове области. Већ крајем прошлога века на високим школама и универзитетима широм света се изучавају интернет право односно различити правни аспекти употребе интернета, компјутерски криминал, електронско пословање као и неки други предмети.

3. Извори компјутерског права

Када говоримо о изворима компјутерског права интересују нас само његови формални извори односно облици у којима се појављују правила која регулишу нека од питања која су предмет ове гране права.

Од формалних извора права треба на првом месту навести устав. Посебно модерни устави у овом погледу добијају на значају обзиром на непосредну везу савремених уставних одредаба о људским правима и слободама са питањима приватности односно информационе приватности. Ово се посебно односи на питање заштите података о личности. Тако рецимо Устав Републике Србије у члану 42. јемчи заштиту података о личности тако што обавезује свакога ко прикупља, држи, обрађује и користи податке о личности да то чини у складу са законом. При томе свако лице има уставно право да буде обавештено да се о њему сакупљају одређени подаци као и право на заштиту због њихове злоупотребе.

У формалне изворе компјутерског права убраја се и читав низ закона и то су уобичајено најзначајнији извори компјутерског права. Ипак, ретки су закони који су у целини посвећени неком од питања које је предмет ове гране права. Такав је рецимо код нас Закон о заштити топографија интегрисаних кола.⁴ У највећем броју случајева питања која чине предмет компјутерског права садржана су у законима који се, у већој или мањој мери, односе и на неке друге области и питања, више или мање повезана са компјутерским правом. У нашем праву то су рецимо Закон о електронском потпису, Закон о електронској трговини, Закон о ауторским и другим сродним правима, Закон о жиговима, Кривични законик... О свим овим прописима, у делу који се може довести у везу са компјутерским правом, биће речи на одговарајућем месту.

Сложеност и динамика правних односа у вези са компјутерима и компјутерским технологијама све више онемогућавају да сва отворена питања у тој области буду регулисана само законима. Отуда подзаконски акти (уредбе, одлуке, наредбе...) постају незаобилазни код уређивања питања

⁴ Службени гласник Републике Србије 104/09.

као што су рецимо техничке и организационе мере заштите, поступак подношења патентне пријаве и слично.

Обичаји, иначе веома значајан извор пословног права са којим је опет компјутерско право широко испреплетано, у области компјутерског права још увек нису у довољној мери изграђени. То је и разумљиво обзиром на „прву младост“ компјутерског права у оквиру које се још увек нису у довољној мери оформили правни односи везани за развој и коришћење компјутера и компјутерске технологије.

Коначно, судска пракса и правна наука ни у компјутерском, баш као ни у осталим правним областима, нису извор права. Уобичајено се међутим у правној литератури оне наводе у одељцима посвећеним изворима права пре свега имајући у виду њихов посредан и не ретко битан утицај на законодавну власт (ону која доноси у формалном смислу најважније изворе права – законе) али и утицај, када је реч о судској пракси, одлука виших на одлуке нижестепених судова. У англосаксонској правној традицији пак одлуке највиших судова и формално обавезују ниже судове па судска пракса у таквим правним системима има ранг значајног извора права.

Рецимо на крају да су у области компјутерског права све значајнији и све бројнији међународни правни извори. Ова околност у првом реду говори о потреби што бржег и што ширег међународно правног хармонизовања основних правила везаних за употребу компјутера и компјутерских технологија. Најважнији правни акти који се доносе на међународном нивоу су конвенције, препоруке, правилници и одлуке, а најважнији доносиоци таквих аката су важне међународне организације као што су Уједињене нације и ЕУ, затим Светска организација за заштиту права интелектуалне својине, Светска трговачка организација, Међународна привредна комора и многе друге. О једном броју најважнијих међународних правних аката који се у целини или делимично односе на област компјутерског права посебно ћемо говорити.

4. Однос компјутерског права и других грана права

Компјутерско право, као једна од грана укупног правног система, поступно заузима своје место међу осталим гранама права. То место се јасно може одредити и уочити ако се изврши анализа односа компјутерског права према другим гранама права са којима је оно у одређеним релацијама. Претходно је већ напоменуто да је компјутерско право у извесном смислу повезано са уставним и кривичним правом, такође са управним и посебно облигационим и пословним правом. На овом месту пак посебно је важно учинити разлику између компјутерског и њему сродних грана права од којих су већина такође нове и у настајању. Ово посебно имајући у виду чињеницу да се врло често, не само међу лаицима већ и међу добрим познаваоцима права, не прави разлика између права информационих технологија, информатичког права, информационог права, телекомуникационог права са једне и компјутерског права, са друге стране. Отуда ћемо о тим разлика, разуме се и сличностима надаље и говорити.

4.1. Компјутерско право и право информационе технологије

Право информационе технологије настаје као нова грана права која представља скуп правних норми, институција и принципа који се могу примењивати на чињенице, радње и активности које се односе на информациону технологију односно компјутеризацију, телекомуникације, аутоматизацију канцеларијског пословања и електронски пренос података. По свом предмету право информационих технологија је шире од компјутерског али уже од информационог права. То практично значи да је компјутерско право део права информационих технологија, а да су они заједно део информационог права.

Ова нова правна дисциплина настаје у Великој Британији крајем 80-их и почетком 90-их година прошлог века али се релативно брзо шири на друге земље Европске уније, САД као и остале државе које велику пажњу и значај посвећују развоју и конкурентности сопствене информационе индустрије.

4.2. Компјутерско право и информатичко право

Информатичко право представља скуп правних норми, института и принципа који се могу применити на чињенице, радње и активности у вези са обрадом информација и информатиком. Информатика при томе представља науку рационалног поступања са информацијама, нарочито уз помоћ аутоматских машина, а која је подлога за знање и комуникације у техничким, економским и друштвеним областима. Она дакле обухвата: а) чињенице, радње и активности у вези са обрадом података (информација), односно све оне чињенице везане за систематске операције на подацима при њиховом прикупљању, ревизији или њиховом претварању у информације; б) чињенице, радње и одговорности везане за рационално поступање са информацијама које су подлога за знање и комуникације у техничким, економским и друштвеним областима.

По свом предмету информатичко право је очигледно шире од компјутерског права обзиром да обухвата правне норме којима се уређује аутоматска обрада података која у основи има компјутерску технологију, али не само њу. Ова грана права је још увек прилично нова и недовољно оформљена. И теорија и пракса показују више интересовања за поједине делове информатичког права него за њега као целину што опет даљи развој овог права чини у неку руку проблематичним.

4.3. Компјутерско право и информационо право

Информационо право је скуп правних норми, принципа и института који се могу примењивати на чињенице, радње и активности везане за примену информационе технологије и специфичности поступања са информацијама у електронском облику. Ова грана права примарно настаје у покушају уређења правне релевантности односно пуноважности информација, података и докумената у електронском облику као и утврђивања правилног односа између права на приступ информацијама са једне односно права да се тај приступ онемогући односно ограничи, са друге стране.

И овде је реч о правној дисциплини која је тек у зачетку и која по свом садржају и природи још увек није сасвим дефинисана. Могло би се и поред

тога рећи да је информационо право по предмету свог интересовања шире од информатичког, а самим тим и од компјутерског права.

4.4. Компјутерско право и телекомуникационо право

Телекомуникације се убрајају у инфраструктурне привредне гране и улагања у телекомуникациону и информациону инфраструктуру један су од главних покретача економског напретка. За привреду информационо-комуникационе технологије су средство за модернизацију и побољшање конкурентности, а за грађане представљају средство за бољи приступ информацијама и побољшање квалитета живота.

Основне карактеристике савремених телекомуникација су:

1) телекомуникациона индустрија постала је у последњих десет година доминантна у свету. Према Форбсовој листи у 2005. години 68 телекомуникационих компанија било је заступљено на листи 2000 највећих светских компанија што је последица не само раста појединих компанија, већ и удруживања, заједничких улагања и преузимања других компанија као битних компоненти процеса глобализације;

2) глобализација телекомуникационих услуга, телекомуникационог тржишта и развојних политика и опредељења којима посебно доприносе стратешки савези између великих компанија;

3) дигитална подела и *e*-економија брзо мењају природу глобалне економије, при чему се она заснива на конкурентним телекомуникационим мрежама, интернет технологији и рачунарским ресурсима и на све мањим трошковима комуникације. Претпоставке развоја *e*-економије су изграђеност телекомуникационе инфраструктуре, распрострањеност интернета као и развој апликација за унапређење образовања, здравства, менаџмента, електронских сервиса и управе (нпр. теле-медицина, учење на даљину, *e*-управа и др.).

Интензиван развој средстава телекомуникација узроковао је и потребу правног уређења читавог низа питања која се с тим у вези постављају и на националном и на међународном нивоу. На националном нивоу највећи број држава има своје посебне прописе, најчешће законе који уређују област телекомуникација. Код нас је то Закон о телекомуникацијама из 2003. године.

У ЕУ, где се све више уместо термина телекомуникације користи термин електронске комуникације, ова област је такође широко регулисана (Опште упутство 2002/21/EZ, Упутство о одобрењу 2002/20/EZ, Упутство о приступу 2002/19/EZ, Упутство о универзалном сервису 2002/22/EZ, Упутство о приватности и заштити података 2002/58/EZ, Упутство о конкурентности 2002/77/EZ, Регулаторни оквир за електронске телекомуникационе мреже и услуге 2002/C 165/03, одредба (EZ) бр. 2887/2000 Европског парламента од 18. децембра 2000. године о отвореном приступу локалној петљи).

Околност да су компјутерске технологије нужно ослоњене на телекомуникационе технологије између ове две гране права установљава врло тесну везу. Отуда је некада веома тешко установити јасну разлику између ове две гране права.

Глава II

ПРАВНА ЗАШТИТА КОМПЈУТЕРСКИХ СИСТЕМА

У овој глави биће посебно речи о широком спектру правних мера и активности везаних за заштиту компјутерских система односно заштиту података, заштиту компјутерских програма и софтвера, заштиту база података, заштиту топографија интегрисаних кола и заштиту од компјутерског криминалитета. Видећемо у основним цртама на који начин се правна заштита компјутерских програма остварује у упоредном праву, на нивоу најважнијих међународних организација и наравно из угла домаћег права.

ЗАШТИТА ПОДАТАКА

1. Уводне напомене о заштити података

Сваки податак може представљати у одређеним околностима и под одређеним условима опасност по неко лице, физичко и/или правно, или по неку друштвену групу. Многобројни примери говоре да су у свим временима и свим друштвеним уређењима појединци и институције страховали од постојања одређених података, а још више од њиховог губљења, мењања или злоупотребе. Између 450. и 31. године п.н.е. постојале су тзв. сенаторске листе у које су се између осталог уносили и укори (ноте) који су изрицани сенаторима. Сама свест о постојању таквих података представљала је својеврсну претњу за сенаторе. Слично се данас у неким системима дешава и са пореским листима у које се уносе подаци о катастарским приходима и на основу којих се одређује стопа пореза. Незнатне грешке у подацима, учињене намерно или случајно, могу имати значајне последице за пореског обвезника, може му рецимо бити одузета имовина због неплаћања пореза.⁵ Да и не

⁵ Дракулић М, наведено дело, стр.54.

помињемо могућу злоупотребу података које имаоци кредитних карти уносе у одговарајућа поља обављајући „операције“ *on line* куповине на интернету.

Имајући претходно речено у виду, посебно у савремено доба када се подаци о одређеним лицима прикупљају на многобројне начине и за различите сврхе, разумљива је потреба изналажења и операционализације таквих метода и техника којима се ограничава и правно уређује приступ подацима од стране програма и људи. На овај начин се примарно обезбеђују приватност, сигурност, поверљивост, расположивост и интегритет података од свих опасности које им прете.

Законско уређење питања заштите података било је у прво време својствено углавном Европским и неким другим високо развијеним државама као што су Аустралија, Јапан и Канада. Данас рецимо у Европи не постоји ни једна држава која област заштите података није уредила посебним прописима, по правилу законом.

У погледу дефинисања појма заштите података једна од првих дефиниција садржана је у извештају који је влада Велике Британије поднела приликом подношења предлога Конвенције о заштити података Савету Европе. Према том одређењу под заштитом података подразумева се „законска заштита појединаца у погледу аутоматске обраде личних података који се на њих односе.“⁶

Повереник за информације ЕУ је опет заштиту података дефинисао као „поштено законодавство“ које не захтева успостављање баланса између корисника података и оних на које се подаци односе већ једноставно поштен однос према сваком појединцу.⁷

Постоје међутим и нешто шира одређења области заштите података која су углавном типична за мање развијене земље. У њима се наводи да би се таква заштита морала односити и на податке који се односе на државе. Тако се рецимо у Резолуцији усвојеној од стране Латино Америчке и Афричке

⁶ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981 (European Treaty Series No 108) (Cmnd 8341) (HMSO, 1981), Explanatory Report, p. 5.

⁷ CBI Conference, London, 4 March 1988.

конференције наводи да „информације и знања која се тичу националног суверенитета, безбедности, економских и друштвено културних интереса такође треба да буду у области заштите података.“⁸

Извесне, кад кад и значајне разлике у погледу заштите података постојале су и међу земљама Европе све до усвајања Директиве о заштити података, о којој ће касније бити више речи. Неке државе, као Данска, Аустрија и Италија, проширују заштиту и на правна лица као што су компаније и трговачка удружења. Неке опет, као Француска и Холандија, својим прописима штите не само аутоматски већ и мануелно обрађене податке. У појединим државама ван Европе, Аустралији и Јапану рецимо, прописи о заштити података су лимитирани на обраду података у јавном сектору. Додуше у Аустралији су амандманима на Закон о приватности из 2000. године његове одредбе проширене на највећи део података у приватном сектору.⁹

1.1. Објекти заштите

Да би се нешто могло штитити неопходно је претходно дефинисати шта се штити па, на основу тога, одредити начин на који ће се заштита спровести. Начелно, предмет заштите је по правилу вишеструки објекат при чему се акценат ставља на онај који одговара интересу због кога се заштита и предузима. Интерес за заштиту може бити лични и групни тј. колективни. Док се лични интерес везује за појединца (грађанина) шири се може односити на различите ентитете, почев од предузећа па до државе.¹⁰

Као објекти заштите могу се појавити четири групе података: подаци везани за личност, подаци везани за организацију, подаци у прекограничном току података и подаци у електронској размени података.

Заштита података везаних за личност везује се примарно за заштиту права приватности као једног од основних, неотуђивих и апсолутних права сваког појединца којим се обезбеђује интегритет и дигнитет људске

⁸ Intergovernmental Bureau for Informatics, TDF 270, p. 55.

⁹ Reed C – Angel J: Computer Law, Oxford University Press, New York 2003, p. 418.

¹⁰ Дракулић М, наведено дело, стр.54.

личности, а ради очувања тајности и слободе приватног живота. Право на приватност је угрожено највише прикупљањем, обрадом, меморисањем и достављањем података о одређеној личности тако да је данас све више схватања о приватности као праву појединца да контролише који, за кога и на који начин су подаци о њему доступни односно могу бити доступни другима. Овај вид приватности данас се назива и информациона приватност.

Постојање одређених података о организацији такође може бити од велике важности за њу односно људе који је чине. Они као такви могу бити изузетно значајни за њен рад, пословни успех и конкурентност.

Посебну групу података чине прекогранични подаци као и подаци у електронској размени података. Наравно, све претходно изнето не представља коначну листу објеката заштите обзиром да се нови објекти заштите непрестано формирају.

Важно је даље одредити од чега одређени предмет нужно треба заштити као и на који начин. Субјекте и податке неопходно је заштити од:

- физичких ризика (хазарда) као што су пожар, поплаве, експлозије;
- неисправности опреме;
- грешака, како људских грешака тако и софтверских (слабо тестиран оперативни систем);
- злонамерних повреда података и система (модификовање, уношење нетачних података, фалсификовање, брисање, упади, крађе...) и напада на субјекте (на приватност, поверљивост, интегритет...)¹¹.

Могли би, на основу претходно реченог и уз пажљиво прављење разлике између заштите података и заштите информационих и/или компјутерских система уопште рећи да заштита података (*data protection*) представља скуп међусобно повезаних активности, метода, техника и норми којима се обезбеђује приватност, сигурност, поверљивост, расположивост и интегритет података од свих опасности које им прете.

¹¹ Дракулић М, наведено дело, стр.56.

Анализираћемо у најкраћем најважније елементе претходно изнете дефиниције:

а) приватност се, као право појединца, појављује као субјект података и као приватност корисника. Као приватност корисника она обухвата: 1) приватност тзв. информација за укључивање одређеног терминала у систем; 2) приватност говора (онемогућавање пресретања усмених комуникација); 3) приватност података (онемогућавање пресретања података у ма којем облику они били); 4) приватност корисникове локације; 5) приватност корисникове идентификације; 6) приватност посебних начина укључивања; 7) приватност финансијских трансакција;

б) сигурност података обухвата обезбеђење података од случајног или намерног откривања неовлашћеним корисницима или заштиту од неовлашћеног мењања, брисања и коришћења од стране овлашћених корисника. Сигурност у исто време претпоставља да су корисницима доступни само они подаци који то, на основу њихових овлашћења, могу и треба да буду;

в) поверљивост података, која произилази из својинских односа и значаја података за одређене субјекте, претпоставља да се неки подаци не смеју открити од стране неауторизованих појединаца и других ентитета или се не смеју открити у неовлашћеним процесима;

г) расположивост података значи да само овлашћени корисник може благовремено доћи до података, и то одређених, а без баријера или других облика ометања и спречавања;

д) интегритет има више различитих значења, а три су основна. Интегритет података (интегритет у ужем смислу) претпоставља да се подаци неауторизовано не мењају или уништавају. Интегритет извора значи обезбеђење таквог степена поверљивости који омогућава пуно поверење „извора“ укључујући и поверење у све процесе руковања подацима. Као треће значење појма интегритета, по неким ауторима и једино, наводи се тачност која се превасходно везује за одговорност за грешке у руковању.¹²

¹² Shirey R: Security Requirements for Network Menagment Data, Computer Standards & Interfaces, No.17/95.

2. Посебно о заштити права приватности

Широка компјутеризација великог броја људских активности утицала је између осталог и на то да се све више, посебно у технолошко најразвијенијим земљама, говори о увођењу личног броја за сваког појединца, а ради идентификације у вези са питањима пореза, банкарских послова, образовања, социјалне заштите, војне обавезе као и бројних других разлога. Није тешко претпоставити какве све опасности могу настати уколико у блиској будућности дође до практичне реализације оваквих идеја. Отуда многи аутори из области информатике већ пар десетина година у назад упозоравају на непријатну истину да многи аспекти примене информатичке технологије представљају потенцијално или стварно угрожавање приватности.¹³

Од великог броја отворених питања насталих с појавом компјутерске информатичке технологије управо правна питања која произилазе из тзв. напада на приватност (*assult on privacy*) као и питања заштите и безбедности података у компјутеризованим информационим системима добијају велики значај. Посебно се развијају контраверзе у вези расправа о природи, између осталог и правној природи приватности, начинима осигурања ефикасне правне заштите од злоупотреба личних података грађана и других субјеката у таквим околностима. Тешкоће настају и у вези одређења једне прецизне и широко прихватљиве правне дефиниције приватности. Тако право приватности и заштита личних података и теоријски и практично постају предмет интересовања правника у области законодавства, управе и судства.

Мада је израз „приватност“ (*privacy*) већ стотинак година у правном оптицају, посебно у земљама англосаксонског правног подручја, претходно изнете дилеме и питања у први план избијају тек развојем и ширењем употребе информатичке технологије и компјутеризованих информационих система. Једна од најранијих дефиниција права приватности формулисана је у америчком праву крајем 19-ог века и то кроз синтагму „права да се буде остављен на миру“ (*right to be left alone*). Појава и употреба првих уређаја информатичке технологије, телефона и телеграфа најпре, рађа и нову

¹³ Mtller A.R.: The Assmdt on Privacy – Computers Data Banks and Dosiiers, The University of Michigen Press, Ann Arbour, MI, 1971, p.4.

концепцију права на приватност. У познатом раду двојице америчких судија, Семјуела Ворена (*Samual Warren*) и Луиса Брандајса (*Louis Brandais*) под насловом „Право на приватност“ (*The Right to Privacy*) изнета је тзв. негативна концепција права на приватност сходно којој је учињен покушај да се приватност изједначи са правом на неузнемиравање односно раније поменути правом да се буде остављен на миру. Овакву слободу односно овакво право правници и филозофи врло брзо почињу називати негативном слободом односно негативним правом сматрајући да је потпуно изједначавање права на заштиту приватности и права на неузнемиравање погрешно и да може изазвати суштинске заблуде. Отуда савремена правна теорија право приватности посматра са тзв. активног становишта који омогућава јасно идентификовање интереса који је у питању. Тај интерес начелно претпоставља право појединаца, група или институција да сами за себе одреде када, како и у којој мери ће се информације о њима саопштавати другим лицима.

Право на приватност се свакако може посматрати у оквиру ширег концепта заштите података али се из тог концепта и издваја како по материји коју регулише тако и у вези процедуре везане за заштиту тог права. Као шири прави концепт право заштите података треба да обезбеди оквир за проналажење баланса између интереса појединаца, корисника база података и друштвене заједнице као целине.¹⁴ У исто време право на приватност се по правилу штити на основу иницијативе појединца којем је то право повређено док се заштита података остварује најчешће ангажовањем посебних државних органа. Додуше, на нивоу ЕУ и заштита података и право на приватност, као интегрални део ширег концепта заштите података, регулисани су истим правним прописима.

3. Инструменти заштите података

Потреба савремених друштава за подацима односно за коришћењем података је огромна. Ништа мања није ни могућност њихове злоупотребе. Отуда се обезбеђење заштите података поставља као једно веома осетљиво и значајно питање за све информационе системе односно, у ширем смислу, за

¹⁴ Report of the Committee on Data Protection (Chairman: Norman Lindop) (Cmnd 7341) (1978).

сва друштва и државе. Из тог разлога се у погледу заштите података предузимају различите мере и активности од којих су најзначајније друштвене, правне, техничке и организационе.

Друштвеним мерама национални информациони системи и цело друштво се штите од злоупотребе нарочито поверљивих података. Предметне мере се реализују кроз успостављање опште политике информационе делатности, затим политике функционисања и развоја база података, посебно јавних база података, као и политике заштите података у граничним и прекограничним токовима података. На овај начин се обезбеђују суверенитет, национална сигурност, приватност као и личне слободе.

Правним мерама се кроз одговарајуће правне механизме штите подаци и процеси везани за те податке, а у неким случајевима и субјекти који се у вези са подацима и процесима појављују. Развојем рачунарске технологије ова се заштита проширује на софтвер, хардвер, трговину компјутеризованих информација, рачунарских и телекомуникационих услуга. Овај вид заштите се такође често односи и на заштиту тајности података и то кроз обавезност поштовања одређених принципа који су законом одређени.

Техничким мерама заштите штите се и обезбеђују подаци од физичких штета или уништења које им прете што се рецимо може односити на физичку заштиту објеката у којима је смештена рачунарска опрема, заштиту од пожара и елементарних непогода, обезбеђење саме опреме, програма и рачунарске мреже. У смислу заштите података у електронској форми користе се различите технологије. Рецимо: енкрипција података је технологија помоћу које се шифрирају подаци на тврдом диску, а сама енкрипција диска се може вршити у облику софтвера или хардвера; сигурносне копије (*backup*) за сврху имају осигурање података од губитака који се касније не би могли повратити; маскирање података је процес прикривања (маскирања) одређених података у табlici база података како би подаци били осигурани и како корисникове информације осетљивог садржаја не би могле процурети из ауторизоване околине; брисање података је метод којим се у потпуности уништавају сви електронски подаци на тврдом диску или неком другом дигиталном медију како би се осигурало да подаци и информације не процуре након што се уређај престане користити. У техничке мере се могу убројати и оне мере које за непосредну сврху имају заштиту аутентичности и интегритета података као што су дигитални потпис и дигитални сертификат.

Коначно, мере организационе заштите, као посебна врста мера, подразумевају организацију технологије рада у информационим системима при његовом пројектовању и оперативном раду, затим утврђивању поступака у случају ванредних околности као и обезбеђивање осталих услова за успешно функционисање информационог система (контрола људи при запошљавању, дефинисање послова и задатака, стручно усавршавање).

3.1. Правни инструменти заштите података

Право је за област заштите података на одређени начин било заинтересовано још вековима у назад. Разуме се, првобитна заштита и по обиму и по суштини била је различита од оне коју данас познајемо обзиром на битно другачије схватање предмета и субјеката заштите. Многи аутори корене правне регулативе заштите података проналазе још у енглеској Великој повељи о слободама (*Magna charta libertatum*) из 1215. године, а потом и другим сличним актима донетим у тој држави као што су Петиција о правима (*Bill of rights*) из 1628. и Корпус повеља (*Habeas Corpus Act*) из 1679. године.

Другу половину 18. века обележиле су Декларација о независности САД из 1776. и француска Декларација о правима човека и грађанина из 1789. године, акти који несумњиво значе корак у напред у односу на све дотадашње прописе који се односе на област људских права и слобода у којим се широким оквирима могу лоцирати и проблеми заштите података.

У области међународног права трендови заштите људских права и слобода кроз међународне декларације, пактове, резолуције и конвенције задржани су и у читавој првој половини 20. века. Другим речима у читавом том периоду није се могло говорити о посебним правним актима који би за предмет имали искључиво и само заштиту података. Најважнији акти у овом периоду су Универзална декларација о правима човека и грађанина УН из 1948. године, Међународни пакт о људским правима УН из 1966. године, затим Европска конвенција о правима човека из 1950. године.

Као први значајан акт који се непосредно односи на заштиту података сматра се извештај Јангерове (*Kenneth Younger*) комисије донет 1972. године у Великој Британији. Наиме у тој држави су се и нешто раније почеле водити озбиљне дебате о потреби заштите права приватности, на којем проблему су

радила разна тела и појединци. Ипак, најдаље у том послу је стигла Јангерова комисија која је у свом извештају предложила усвајање 10 принципа при заштити података који су и данас актуелни и представљали су дуго времена једину основу за многе националне законе и међународне акте. Ти принципи су следећи:

- информације се могу користити само у складу са унапред одређеном сврхом, а у случају њиховог коришћења у друге сврхе мора постојати посебна дозвола од онога на кога се информације односе;
- приступ информацијама треба ограничити само на оне који имају овлашћење да их користе за оно што су намењене;
- за задовољење одређене сврхе може се прикупљати само минималан број података који је довољан да се постављени захтев реализује;
- у компјутеризованим статистичким системима морају се на одговарајући начин, пројектовањем и програмирањем, одвојити идентификациони од осталих података;
- информације морају бити тако сређене да се проблем може изложити кроз информације које се на њега односе;
- изабрани ниво система заштите мора се претходно прилагодити потребама, захтевима и специфичностима корисника, чиме се обезбеђује злоупотреба или губитак информација;
- систем контроле треба да обезбеди откривање било које повреде сигурности;
- у пројектовању информационог система мора се навести временски период после кога се информација неће користити;
- садржај података мора бити ажуран и мора постојати механизам за корекцију неажурних података;
- мора се обратити пажња на систем вредновања одлука односно пресуда, на основу чега се у каснијој фази формирало и право на

жалбу у ситуацијама када субјект код кога се подаци у некој бази налазе одбије да их избрише, преправи, ажурира, користи у дозвољене сврхе и слично.

У даљем излагању говорићемо о једном броју значајних међународних аката у овој области. Уз напомену да је реч о оним правним актима на основу којих је временом дошло и до високог степена правне унификације националних правних система. Другим речима, основна решења и принципи садржани у тим међународним актима послужила су као елементарна грађа великом броју држава у процесу дефинисања и изградње њиховог сопственог националног законодавства у овој области.

3.1.1. Конвенција о заштити појединаца с обзиром на аутоматизовану обраду података

Конвенција о заштити појединаца с обзиром на аутоматизовану обраду података о личности, тзв. Европска конвенција, усвојена је 1980. године али је на снагу ступила тек 5 година касније, када су је ратификовале првих 5 држава. У нашој земљи она је потврђена усвајањем Закона о потврђивању Конвенције из 1992. године.¹⁵

Сврха ове Конвенције је, како је наведено у њеним општим одредбама, да осигура на територији сваке земље потписнице, сваком појединцу, било које народности и било којег места боравка, поштовање његових права и основних слобода, а посебно право на приватност с обзиром на аутоматску обраду података која се односи на њега.

Конвенција дефинише обавезе потписница, квалитет података, осигурање, додатне мере, санкције, изузетке, ограничења и проширење заштите. Њоме се такође дефинишу подаци који припадају посебној категорији и који се не смеју обрађивати аутоматски ако закон земље потписнице не обезбеђује одговарајуће мере заштите. То су подаци којима се идентификује порекло, политички ставови, религиозна и друга убеђења или здравствено стање. Сви остали подаци који се могу обрађивати морају имати одређени квалитет што значи: а) да се морају обрађивати тачно и легитимно;

¹⁵ Сл. лист СРЈ 1/92.

б) да се морају меморисати за специфичне и легитимне сврхе и не смеју бити коришћени на начин инкомпатибилан тим сврхама; в) морају бити адекватни, релевантни, непреопсежни у односу на сврху ради које се меморишу; г) тачни и када је то нужно ажурни; д) одржавани у оном облику који дозвољава идентификацију субјекта података у оној мери у којој је то потребно за сврхе ради којих се подаци меморишу.

Према Конвенцији појединац има право да: а) утврди постојање аутоматизоване датотеке података о личности, њених најважнијих сврха, као и идентитет и место боравка (седиште) контролора датотеке; б) у разумним интервалима, без превеликог закашњења или трошкова, добије потврду о томе јесу ли подаци о личности који се на њега односе меморисани у аутоматизованој датотеци података као и да му се предоче у разумљивом облику; в) захтева ратификацију или брисање таквих података ако се они обрађују супротно одредбама домаћег закона; г) има могућност предузимања одговарајуће акције (правног лека).

Конвенција је 1999. године мењана путем амандмана док је 2001. године усвојен и додатни протокол о Надзорном органу и прекограничном току података. Ипак, сматра се да је основна слабост конвенције недостатак инструмената односно мера у погледу оних држава које се евентуално не придржавају њених основних принципа. Отуда би се било каква неслагања у овом контексту морала решавати на дипломатском нивоу.

3.1.2. Смернице које се односе на компјутеризована досијеа података

На Генералној скупштини УН усвојене су 1990. године Смернице које се односе на компјутеризована досијеа података (*Guidelines concerning Computerized Data Files*). Оне представљају један од основа за хармонизацију националних законодавстава у регулисању заштите података о личности.

Највећи значај имају принципи које би свака земља чланица УН требала да угради у своје националне прописе. То су:

- принцип законитости и непристрасности, што значи да се подаци не смеју прикупљати нити обрађивати на незаконит или пристрасан начин;

- принцип тачности, што значи да подаци о личности морају бити тачни, релевантни и комплетни, а да би се то остварило нужна је њихова провера, и то редовна;
- принцип тачно утврђене сврхе, што значи да се пре него што прикупљање података почне мора утврдити намена прикупљања;
- принцип доступности, што значи да сваки појединац има право да добије информацију о подацима који се о њему воде и право увида у њих;
- принцип недискриминације, што значи да се не могу прикупљати подаци који могу изазвати незаконите или произвољне дискриминације по раси, етничком или социјалном пореклу, сексуалном животу, политичком уверењу, верским или сличним убеђењима;
- принцип посебног одобрења за изузимање, што значи да треба обезбедити да се изузеци од принципа Конвенције могу толерисати само ако су изричито и посебно предвиђени прописима;
- принцип сигурности, што значи да треба омогућити заштиту података о личности, нарочито од природних опасности, упада, неовлашћеног приступа, злоупотреба или компјутерских вируса;
- принцип уређивања прекограничног тока;
- принцип надзора, што значи да се у свакој земљи именује орган који ће бити овлашћен и надлежан за контролу и праћење свих принципа у Конвенцији садржаних.

Други део Смерница се односи на персонална досијеа података која воде владине међународне организације. У том погледу се од њих захтева успостављање посебног надзорног тела које ће надгледати приступ и коришћење ових података. Посебан значај у овом делу има тзв. хуманитарна клаузула сходно којој је могуће дерогирати основне принципе Смерница о компјутеризованим досијеима података, ако је сврха коришћења података заштита људских права и слобода или хуманитарна помоћ.

3.1.3. Директива о заштити појединаца у вези са обрадом података о личности и слободном кретању таквих података

Европска конвенција, о којој је претходно било речи, није успела да допринесе неопходном степену хармонизације у законодавству земаља чланица ЕЕЗ (ЕУ). Неке земље су своје прописе у области заштите података донеле тек десетак година након њеног усвајања, друге су опет Конвенцију прихватиле само као груби оквир за сопствена решења, а неке опет уопште и не доносе своје националне прописе. Ово је био довољан разлог да се у оквиру ЕЕЗ (ЕУ) почну озбиљне припреме на изради у усвајању акта који би допринео већој и супстанцијалнијој хармонизација прописа у овој области. На тај начин је још 1990. године израђена прва верзија Директиве о којој се у наредним годинама доста дискутовало и која је прошла кроз више радних верзија. Коначно, Директива о заштити појединаца у вези са обрадом података о личности и слободном кретању таквих података је усвојена од стране Европског парламента и Савета 1995. године.

Директива под подацима о личности подразумева сваку информацију која се односи на идентификовану или особу која може бити идентификована, директно или индиректно, а посебно на основу идентификационог броја или на основу неког другог фактора специфичног за њен физички, психички, ментални, економски или социјални идентитет.

Под обрадом података се у смислу Директиве подразумева једна или скуп операција које се обављају на подацима о личности, биле оне аутоматске или не, а које су: прикупљање, уношење, организовање, складиштење, адаптирање, претраживање, договарање, коришћење или показивање трансмитовањем, дисеминацијом или на било који други начин чињењем расположивим, или блокирање, брисање или уништавање. При томе се истичу пет основних принципа обраде података. То су:

- поштена и законита обрада;
- прикупљање за одређене, експлицитне и оправдане сврхе;
- адекватност података, релевантност и ограниченост у броју, а у складу са сврхама за које су прикупљени и/или будућим сврхама;
- тачност и уколико је потребно свакодневна ажурност;

- облик који дозвољава идентификацију субјекта података само у интервалу који је нужен за остваривање сврхе (садашње или будуће), а ако су у питању историјске, статистичке или научне сврхе тада их је могуће чувати и дуже али само уз одговарајућу заштиту.

Сваки појединац на кога се подаци односе има право да буде обавештен о томе, да има приступ подацима, право на приговор и право на јавност обраде података.

Директива забрањује обраду података о личности којима се одају расно или етничко порекло, политичка уверења, религијска или психофизичка убеђења, чланство у синдикату као и података који се односе на сексуални живот и здравље. Ови се подаци ипак могу, у строго прописаним условима, обрађивати. Рецимо, ако субјект да свој изричити пристанак за њихову обраду или је то неопходно ради заштите његових виталних интереса. Трансфер података о личности у треће земље је дозвољен али само ако таква земља осигурава адекватан степен заштите оваквих података.

Директива даље предвиђа постојање и овлашћења супервизора у свакој држави чланици ЕЕЗ (ЕУ) чији је основни посао да, као независан орган, процењује примену Директиве на одређеној територији. Он у том смислу има одговарајућа овлашћења за вршење истражних радњи, интервенција као и овлашћење да учествује у правним поступцима.

Свака држава чланица ЕЕЗ је била у обавези да у року од 3 године од дана њеног усвајања усклади своје националне прописе са Директивом. Изузетно, усклађивање одредаба које се односе на ручну обраду података одређено је на рок од 12 година.

Значај Директиве у оквирима предметне правне продукције ЕЕЗ (ЕУ) је вишеструк. Прво, Директива мења и превазилази до тада постојећи „статични“ концепт заштите података који се налазе у досијеима у корист „динамичког“ концепта обраде података о личности без обзира где се они налазе. Друго, Директива превазилази уске оквире компјутеризованих, аутоматских обрада, обухватајући и мануелне обраде којима се такође могу угрозити права појединаца на приватност и информациону приватност. Треће, Директива претендује да обухвати и приватни и јавни сектор, бришући

значај њихових разлика у односу на значај које има право приватности и заштита појединаца. Четврто, Директива даје државама чланицама извесне слободе у регулисању, посебно када је у питању трансфер података о личности унутар ЕУ и између ЕУ и трећих земаља. Пето, Директива тежи да се заштита права усклади са слободама личности, да се обезбеди еквивалентни ниво заштите у свим земљама чланицама, да се још више осигура хармонизација права, нарочито у примени нових технологија, да се омогући постојање изузетака, али само под тачно прописаним условима и критеријумима и наравно да се превазиђу оквири заједнице и одређени принципи прошире на треће земље.

Поред Директиве о којој је претходно било речи значај у погледу заштите података имају и Директива Европског парламента која се односи на обраду података о личности и заштити приватности у сектору електронских комуникација из 2002. године (2002/58/ЕС) као и Директива Европског парламента и Савета о заштити појединца у вези са обрадом података о личности и заштити приватности у области телекомуникација из 2006. године (2006/24/ЕС).

4. Посебно о заштити података у електронској размени податка

Пре више од 20 година у САД је почела експанзивна примена и развој електронске размене података (*Electronic Data Interchange/EDI*), у прво време под називом електронски трансфер података (*Electronic Data Transfer/EDF*). Мада у тесној вези са прекограничним токовима података EDI се од њега у многоме разликује јер обухвата електронски пренос података, од рачунара до рачунара, и то трговачких, административних и транспортних података, а уз коришћење договорених стандарда у које је структурирана EDI порука. То је у суштини размена структурираних комерцијалних података између рачунара посебних фирми ради пословних трансакција, извршена без мануелне интервенције, електронским путем и то посредством стандардизованих порука које замењују традиционална папирна документа. Важно је при томе напоменути да се размена EDI порука увек врши у оквиру затвореног система и да се обавља на основу унапред утврђених правила између странака које врше размену података овим путем.

Произилази да као битне елементе специфичне размене података извршене уз помоћ EDI можемо одредити:

- EDI је размена података, то је по правилу двосмерни пренос порука, при чему се под порукама подразумева низ сегмената, структурираних коришћењем договорених стандарда у компјутерски читљивом формату који су подобни да буду аутоматски и недвосмислено обрађени;
- EDI је размена структурираних података, што значи да поруке морају бити у одређеном формату и то таквом који омогућава машинску обраду;
- EDI је размена података између компјутера засебних фирми;
- у на овај начин обављеној размени података нема мануелних интервенција, што практично значи да је реч о размени између апликација, а не људи;
- EDI се најчешће спроводи у области пословних трансакција које обухватају трговину, транспорт и администрацију;
- EDI је размена порука које се појављују уместо традиционалних папирних докумената;
- EDI се реализује коришћењем договорених стандарда, најчешће EDIFACT стандарда, правила УН за ЕДИ, који представљају низ међународно договорених стандарда, именика, упутстава, нарочито везаних за размену која се односи на трговину робом и услугама између независних рачунарских информационих система;
- EDI је размена електронским путем, а не магнетним или другим медијима.

Увођење EDI био је разлог да се у литератури, а на основу његове практичне примене и ефеката те примене, говори о добрим (позитивним) и лошим (негативним) искуствима. У позитивне ефекте примене EDI најчешће се наводе:

- умањење укупних трошкова за обраду и транзицију папирних докумената;
- умањење грешака које праве људи при обради;
- умањење времена потребног за унос података;
- превазилажење језичких баријера и проблема рада у различитим временским зонама, а што се постиже недвосмисленим садржајем поруке;
- убрзање доставе података;
- менаџмент је ефикаснији на свим нивоима;
- ефикасније се управља, повећава се промет новчаних средстава, обезбеђују се ажурни токови и унапређује контрола укупних кретања готовине;
- омогућава се већа флексибилност преноса података, чији број није ограничен;
- повећава се продуктивност.

Као најзначајнији разлози примени EDI истичу се ипак економски разлози обзиром да се на овај начин елиминишу многи трошкови као што су трошкови везани за коверте, чекове, папир, трошкови штампања, куцања, обраде, поштански трошкови и слично. Са друге стране наводе се и одређени негативни елементи, другим речима неке негативне последице које произилазе из употребе EDI. У овом погледу се најчешће истичу:

- ефекти одбојног психолошког става, отворених или прикривених отпора увођењу;
- проблеми сигурности и заштите, нарочито када су у питању даваоци сервиса од којих се захтева посебна сигурност у вези веродостојности порука, контроле приступа, интегритета и поверљивости садржаја као и све веће разноврсности напада који прете;

- законска или друга правна ограничења, непотпуност или недореченост;
- тешкоће у прилагођавању постојећег апликативног софтвера;
- релативно велики иницијални трошкови увођења.

Посебно питање које се истиче у вези разматрања о укупним ефектима коришћења EDI тиче се одговорности учесника у EDI преносима и обезбеђења сигурности и заштите података односно порука. Оваква врста одговорности својствена је свим странама у EDI трансакцијама и то пошиљаоцу поруке, даваоцу комуникационе услуге (серверу) и примаоцу поруке.

Тако пошиљалац поруке има одговорност за отпремање поруке у одговарајућем формату и по одговарајућем протоколу, за безбедност од искривљавања поруке, за осигурање посебне ауторизованости порука, осигурање усклађености поруке са временом трансакције, за постизање свих неопходних права копирања, осигурање коректне адресе примаоца. Давалац комуникационе услуге (сервер) одговоран је за отпремање поруке у одређеној форми и по одређеним протоколима, за безбедност од искривљавања порука, сигурност да је порука отпремљена ка примаоцу и осигурање тајности и сигурности поруке. Прималац поруке такође је одговоран за осигурање да је порука усмерена ка њему, признање и верификовање поруке, осигурање тајности и сигурности поруке. Значи, сви учесници у EDI ланцу имају одређене одговорности и обавезе као заједнички именуатељ.

Разуме се и у било којем другом ланцу преноса података који није EDI, рецимо коришћењем класичне поште, такође постоје ове врсте одговорности свих учесника у ланцу. Опасности су међутим другачије обзиром на посебну природу EDI па се отуда, начелно говорећи, обезбеђење сигурности EDI порука остварује кроз:

- навођење минимима безбедности који треба да се гарантује, а чија основа је споразум или уговор;
- испуњење захтева „комерцијалне разумности“ приликом коришћења EDI од сваке стране;

- обезбеђење сваке стране од неауторизованог приступа или гарантовање да је у питању ауторизована трансмисија;
- примену од сваке стране одређеног система безбедности и техника које би представљале основе за тзв. комерцијално разумну безбедност.

Веома важно питање у вези заштите података у електронској форми је и питање од чега, од којих ризика и опасности такве податке треба заштитити. Навешћемо из тог разлога најнепосреднији приказ познатих претњи безбедности и интегритету података у електронској форми:

- чепркање по подацима, које подразумева неовлашћено мењање података при уносу од стране неовлашћеног лица;
- „салама“, што подразумева прикривање појединачних података од којих је сваки испод нивоа контролног процеса;
- тројански коњ, што подразумева неовлашћени софтвер који ради прикривено;
- програмске бомбе (логичке, временске), део програма који се активира неким догађајем и који уништава софтвер и податке, јавно или прикривено;
- вируси, што подразумева неовлашћени софтвер који се сам размножава и који уништава софтвер и податке, јавно или прикривено;
- хакинг, што подразумева продор неовлашћених лица у систем;
- разбијање шифара, што подразумева неовлашћено дешифровање информација или софтвера.

4.1. Европски модел EDI Споразума

Нужност дефинисања потребних услова на основу којих странке послују обављајући послове коришћењем електронског преноса порука довела је 1994. године до усвајања Препорука Европског Модела EDI споразума (*Commission Recommendation of European Model EDI Agreement*). Овај Модел споразума има само 14 чланова уз које је придодат и анекс везан за Технички додатак.

У погледу безбедности порука странке, према Моделу EDI споразума, имају обавезу да примењују поступке и мере безбедности којима ће се осигурати одговарајућа заштита порука, заштита од неовлашћеног приступа, измене, уништења или губитка. Безбедност порука обухвата примарно проверу порекла, проверу интегритета, неодбацивање порекла као и проверу пријема и поверљивости.

Поверљивост и заштита података о личности претпоставља споразумевање страна око коришћења посебних облика заштите за одређене поруке (криптографисање), ако је то њиховим правима дозвољено. Заштита података о личности обављаће се у складу са законима земаља страна у споразуму, а уколико таквих закона нема, као минимум послужиће Конвенција Савета Европе о заштити појединаца у односу на аутоматску обраду података о личности.

Модел EDI споразума поред безбедности порука и заштите података о личности и поверљивости предлаже уговорно регулисање питања доступности података као доказа и то тако што се уговорне стране обавезују да ће у случају спора суду учинити доступним податке, а да ће при томе поруке представљати доказ о чињеницама које су наведене. Посебно су регулисани и случајеви ослобађања од одговорности уколико штета настане доцњом, изостављањем или грешком, или у случају да су доцња односно пропуст настали ван контроле те странке, а за које се није могло „разумно“ очекивати да ће наступити. Уколико се пак једна страна определи да ангажује посредника за обављање услуга преноса, уписивања или обраде, па настане штета, тада ће она одговорати за штету која је настала као директна последица радње, грешке или пропуста. То ће се десити и страни која од друге стране захтева учешће посредника за трансмисију, па настане штета.

У случају настанка спора између страна потписница може се изабрати арбитража или ће се применити одредбе о клаузули надлежног суда. Странке се такође могу договорити које ће право бити меродавно у случају обраде и складиштења или поверљивости података о личности.

У погледу третмана записивања и складиштења порука предвиђа се комплетан и хронолошки запис свих порука које се налазе у размени између страна трговачке трансакције. Такве поруке дакле морају бити сачуване у неизмењеном стању и обезбеђене у законом предвиђеном периоду, не краћем од 3 године. Складиштење се врши у одређеном формату и то пошиљалац поруку складишти у формату у ком је поруку доставио, а прималац у примљеном формату. Електронски записи морају бити лако доступни и мора се обезбедити да буду репродуковани у читљивој форми што практично значи да се неће толерисати оправдања да више не постоји опрема за читање таквих порука.

Коначно, напомињемо да одредбе Модела Споразума нису намењене да се њима регулишу уговорне обавезе које произилазе из основних трансакција до којих се дошло коришћењем EDI, изузев ако странке нису уговориле другачије. Ипак, странке које се одлуче да се правно обавезу Моделом Споразума изричито се одричу права да уложи приговор у погледу ваљаности уговора закљученог коришћењем EDI само зато што је закључен коришћењем EDI.

Мада ће о том питању бити више речи касније рецимо и то да се према Моделу Споразума уговор закључен коришћењем EDI сматра закљученим у време и у месту у коме порука која представља прихват понуде стигне у рачунарску систем понудиоца.

5. Национални инструменти заштите података

Данас по свој прилици не постоји ни једна земља на свету чији правни поредак на неки начин не третира питање заштите података. Када се међутим ради о врстама правних аката којима се то чини и њиховој садржини могу се уочити извесне, кад кад и значајне разлике. Многе државе (Шпанија, Португалија, Бугарска, Словачка...) већ у својим уставима регулишу начелна питања заштите података, а највећи део њих то чини законима. Некада се то

чини тако што се област заштите података нормира посебним законима који за предмет регулисања имају искључиво ову заштиту, а некада опет законима којима је основни предмет регулисања нешто друго, рецимо кривичним или трговачким законима. Постоје и примери земаља, САД рецимо, где се област заштите података детаљно регулише сетом посебних закона.

У појединим државама питање заштите података је предмет подзаконских аката (одлуке, уредбе, наредбе...) или специфичних аката донетих од стране органа управе, а не законодавне или извршне власти. Такав пример имамо у Јапану где је питање заштите података било регулисано Правилником о заштити података у компјутеризованим информационим системима из 1986. године.

Сматра се да је први посебан закон који непосредно регулише питање заштите података још 1970. године донет у Немачкој и то од савезне државе Хесе. Француска је нешто касније, 1978. године, донела Закон о информатици, евиденцијама и слободама. По основу наведеног акта основана је Национална комисија за информатику и слободе (*CNIL / Commission Nationale de Linformatique*), посебно тело снабдевано значајним регулативним, контролним и другим овлашћењима. Независност овог тела, по свом статусу правног лица, произилази и из чињенице да оно, мада у саставу државе, подлеже једино и искључиво судској контроли. У Великој Британији је такође на основу Закона о заштити података из 1984. године образован Регистар за заштиту података (*Data Protection Registrar*) као посебна врста „матичара“ за вођење евиденције о заштити података кога именује Круна и који је практично независан од Владе. Регистар је заправо орган за заштиту података с овлашћењима „повереника парламента“ односно омбудсмана. Он врши регистрацију свих корисника компјутеризованих информационих система за обраду личних података и то како у јавном тако и у приватном сектору. Након ратификовања Директиве ЕУ о заштити података у Великој Британији је у другој половини 1988. године усвојен нови Закон о заштити података (*Data Protection Act*).¹⁶

Када је реч о заштити података у EDI још увек је премало примера посебне законске регулативе у тој области. Отуда се најчешће поједина

¹⁶ Више о овом Закону види код: Reed C – Angel J: Computer Law, Oxford University Press, New York 2003, p. 428 – 453.

начела EDI пословања уграђују у неке друге посебне прописе или се њихова примена препушта слободној вољи странака које EDI форму користе у обављању својих послова.

На основу анализе постојећих упоредних прописа у овој материји, без обзира на њихов различит правни ранг, могу се извући и њихове одређене заједничке карактеристике:

прво, већином закона штите се подаци и у јавном и у приватном сектору и то, по правилу, на информационим системима који поседују аутоматску обраду података;

друго, сви закони за циљ имају заштиту одређених интереса који се могу угрозити прикупљањем, обрадом и коришћењем података. У овом погледу се у земљама евроконтиненталног права акценат ставља на заштити општих, а у земљама англоамеричког права на заштити приватних интереса;

треће, највећи број закона садржи одредбе о могућностима обраде података, начелима, поступцима и методама њиховог прикупљања и коришћења. У правима неких држава неопходно је од надлежног органа добити дозволу да би се могло бавити прикупљањем и обрадом података док у другој групи земаља важи начело регистрације, што значи да онај ко жели да се бави овим послом мора претходно да испуни одређене, законом прописане услове;

четврто, сви закони предвиђају и права субјеката на које се подаци односе, било да је реч о физичким или правним лицима. Посебно се међутим акценат ставља на права физичких лица;

пето, готово сви закони предвиђају и обавезу конституисања одређених тела која врше надзор над законитим прикупљањем, обрадом и коришћењем података;

шесто, највећи број закона предвиђа изузетке за одређене групе података који, као такви, не подлежу одредбама тих закона;

седмо, сви закони предвиђају и одређене санкције за кршење њихових одредаба. Реч је најчешће о новчаним казнама и мери забране обављања делатности у одређеном периоду. Разуме се, лица чија су права повређена имају могућност да се за накнаду штете обрате и редовним судовима.

5.1. Инструменти заштите података у праву Србије

Заштита података о личности зајемчена је у нашем праву Уставом Републике Србије. Овај акт наводи да се прикупљање, држање, обрада и коришћење података о личности уређује законом те да је забрањена и кажњива употреба података о личности изван сврхе за коју су прикупљени, изузев за потребе кривичног поступка или заштите безбедности Републике Србије и то на начин предвиђен законом. Устав такође предвиђа право сваког лица да буде обавештено о прикупљеним подацима о својој личности као и право на судску заштиту у случају њихове злоупотребе.¹⁷

На основу претходно наведене одредбе Устава Србије донет је 2008. године и Закон о заштити података о личности.¹⁸ Овим Законом се уређују услови за прикупљање и обраду података о личности, права лица и заштита права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденција, изношење података из Републике Србије и надзор над извршавањем овог закона. Сврха Закона је дакле да, у вези са обрадом података о личности, сваком физичком лицу обезбеди остваривање и заштиту права на приватност и осталих права и слобода.

Основна права у вези са заштитом података о личности су:

а) право на обавештење о обради - свако има право да захтева да га руководиоца о подацима потпуно и истинито обавести о томе да ли обрађује податке о њему, које и у коју сврху и по ком правном основу и од кога их прикупља; у којим збиркама података се налазе подаци о њему, ко су корисници и којих података и у које сврхе и по ком правном основу; као и коме и који подаци се преносе, у коју сврху и по ком правном основу;

б) право на увид - свако има право да захтева да му се ставе на увид подаци који се на њега односе;

¹⁷ Члан 42. Устава Републике Србије.

¹⁸ Службени гласник РС 97/08.

в) право на копију – свако има и право да од руковаоца захтева копију података који се на њега односе, при чему је дужан да сноси само нужне трошкове израде и предаје копије;

г) права поводом извршеног увида – свако лице има и право да од руковаоца захтева исправку, допуну, ажурирање или брисање података као и прекид и привремену обуставу обраде, под претпоставком постојања законом утврђених услова.

У вези са остваривањем горе наведених права сваком лицу које је поводом свог захтева незадовољно одлуком или поступањем руковаоца подацима зајемчено је право на жалбу Поверенику, а сходно члану 38. Закона о заштити података. Према Закону Повереник за информације од јавног значаја и заштиту података о личности је самостални државни орган, независан у вршењу својих надлежности од којих су најважније следеће: а) надзор над спровођењем заштите података; б) одлучивање по жалби у случајевима законом прописаним; в) вођење Централног регистра; г) надзор и одобрење за изношење података ван Републике Србије; д) указивање на уочене злоупотребе у поступку прикупљања података; е) састављање листе држава и међународних организација које имају одговарајуће уређену заштиту података; ж) давање мишљења у вези са успостављањем нових збирки података односно у случају увођења нове технологије у обради података.

Разуме се, циљ Закона о заштити података о личности није заштита података о личности као таква, већ заштита појединца на кога се ти подаци односе, а тиме и дела његове такозване информацијске приватности. Отуда Закон не покрива читав спектар права на приватност појединца већ само онај део права на приватност који се односи на његове податке о личности. Тако на пример, вређање неког појединца у медијима и навођење неистина у вези са њим задире у његову приватност, али то није кршење одредби о заштити података о личности. Ако би пак неко о појединцу преузео и објавио његове податке о личности, које је добио из различитих извора података (нпр. појединости о његовом здравственом стању), то би значило кршење одредби Закона.

Конечно, могли би рећи да се још један закон, додуше посредно, односи на питање заштите података о личности. Реч је о Закону о тајности

података¹⁹ који, самим тим што уређује услове и поступак проглашења неких података тајним, уређује сврху прикупљања, чување и приступ оваквим подацима, пружа гаранције да се такви подаци о личности могу прикупљати, користити и обрађивати само на начин и у поступку који је тим актом уређен.

ЗАШТИТА КОМПЈУТЕРСКИХ ПРОГРАМА И СОФТВЕРА

1. Уопште о заштити компјутерских програма и софтвера

У време појаве првих рачунара цена хардвера је била готово 2/3 цене сваке инсталације. Тек са развојем персоналних компјутера (PC) оваква ситуација се поступно и квалитативно мења.²⁰ Као предмет интересовања купаца али и као атрибут квалитета неког рачунара примарно се намећу компјутерски програми и софтвери који као такви постају основни фактор разликовања међу различитим произвођачима компјутерске опреме. А врло брзо и основни предмет пиратерије, фалсификовања и неовлашћеног коришћења. Овакви проблеми још 90-их година прошлог века добијају чак ранг озбиљних економских међудржавних спорова, рецимо између САД као водеће земље у производњи и иновацији компјутерских програма и Кине, државе у којој су се такви програми кривотворили и даље продавали. Отуда се као важно питање поставило питање правне заштите компјутерских програма али, при томе, и питање одређивања правне природе и специфичности власништва рачунарских програма. Оно што од самог почетка није било спорно је то да је компјутерски програм резултат стваралачког рада једног или више твораца, чак и онда када га у потпуности или делимично генерише машина. Из тога разлога се на ту област превасходно примењује право интелектуалне својине. Али оно што је било, делимично и остало проблем, јесте прецизно одредити објект заштите као и прецизирати врсту права интелектуалне својине којом се компјутерски програм најцелисходније може штитити.

¹⁹ Службени гласник РС 104/09.

²⁰ Дракулић М, наведено дело, стр.170.

Што се тиче објекта заштите данас се углавном сматра да је то компјутерски програм у ширем смислу у чије оквири опет улази софтвер, компјутерски програм у ужем смислу (онај којим се непосредно контролише или условљава рад рачунара), изглед корисничког интерфејса на монитору, производ реверзибилног програмирања и компјутерски генерисано дело. Но најважније питање у овом контексту је питање којим се то правим интелектуалне својине (патентом, жигом, ауторским правом...) компјутерски програм оптимално може штитити.

2. Компјутерски програм и патентноправна заштита

Упоредно право, не без одређених дилема, углавном негативно гледа на могућност заштите компјутерских програма патентним правом. Основно питање које се у овом смислу поставља је питање да ли компјутерски програми могу да задовоље услов који се за сваки проналазак тражи – да представљају новост техничког решења.²¹ Доминантно мишљење је да компјутерски програм не може бити предмет патентноправне заштите обзиром да не може да испуни услов апсолутне новости. Наиме, низ инструкција, без обзира колико њихов поредак у програму може изгледати као новост, не представља новост у смислу патентноправне заштите. Према таквим схватањима алгоритам (као метод), као саставни део програмског концепта, не би могао да ужива патентну заштиту па то онда не може ни само дело чији је он саставни елемент, односно рачунарски програм у ширем смислу.²²

Постоје међутим и мишљења према којима су рачунарски програми на самој граници која раздваја патентбилно од непатентбилног. Неки рачунарски програми остају ништа друго до инструкција о обављању интелектуалне делатности и као такви се не могу сматрати проналасцима.

²¹ Рачунарски или компјутерски програм се може одредити као низ инструкција које су, по њиховом фиксирању на машински читљиви материјални носач, у стању да на машину за обраду информација делују тако да она изрази, изведе или постигне одређену функцију или задатак или резултат. Овако: Марковић С: Патентно право, Београд 1997, стр. 70.

²² Бесаровић В: Интелектуална својина, индустријска својина и ауторско право, Београд 2005, стр.66.

Међутим програми код којих долази до конверзије операција у технички процес способан за константно понављање спадају у сферу патентног права.²³

У евроконтиненталном праву став о непатентибилности компјутерских програма уопште изражен је још у Конвенцији о европском патенту из 1973. године односно изменама наведене Конвенције из 1978. године. Према том акту рачунарски програми нису патентибилни обзиром да не испуњавају један од три обавезна и кумулативна услова патентибилности. На основу Конвенције слична односно у највећем делу истоветна решења прихваћена су у безмало свим европским државама, али и од стране судске праксе. Конвенција о европском патенту је дакле изузела из патентне заштите „компјутерски програм као такав“, што је у прво време довело до низа несугласица и неспоразума. Једна од основних несугласица се везује за оне програме којима се омогућава рад рачунара на нов или побољшан начин. Сматрало се наиме да се такви програми, дакле они који омогућавају рад рачунара на нов или побољшан начин, не могу подвести под термин „компјутерски програм као такав“ па би им, уз испуњење других услова, требало омогућити патентно правну заштиту. Оваквом решењу склон је и Водич Европског патентног завода из 1985. године у којем се препоручује патентибилност не програма као таквих већ неког другог проналаска који може бити у форми погодној програмираном рачунару, при чему се води рачуна да ли је у питању технички или нетехнички ефекат који проналазак има. Другим речима, програм којим се решава на нови начин неки технички процес или проблем може се, уз испуњење других услова, оценити као патентибилан. Уколико испуњава услове патентибилности заштита ће трајати 20 година од дана подношења пријаве.

У Европској унији је 2005. године Европски парламент одбио усвајање предлога Директиве о патентибилности проналазака везаних за компјутере (*computer related inventions*), који предлог је за сврху имао даље олакшавање признања патентне заштите за софтвер. Аргументи противника предложеног решења заснивали су се на тврдњама да би услед проширења патентно правне заштите на компјутерске програме ови поскупели, да даљи развој информационе технологије у свету није условљен постојањем оваквог облика

²³ Овако: Cornish W, Llewelyn D: Intellectual Property: Patents, Copyrights, Trade Marks and Allied Rights, Sweet&Maxwell, London, 2003, p.213.

заштите, а да је тамо где је она уведена сврха пре свега ограничење конкуренције, што је опет довело до великог повећавања броја судских спорова.²⁴

У пракси Европског завода за патенте било је случајева прихватања патентне заштите програма неких европских или ваневропских фирми у смислу претходно изложеног изузетка. Међутим, многе познате фирме (*IBM*) су и одбијане са образложењем да је реч о програмима који се користе у нетехничке сврхе.

Убрзан развој информатике и економска вредност рачунарских софтвера, како у погледу улагања у програмирање тако и у погледу могућности њиховог комерцијалног искоришћавања, створили су такву правно политичку климу да је у појединим државама постало прихватљиво извесне видове интелектуалног стваралаштва повезане са софтвером уместо ауторским правом штитити патентима.²⁵ Такву праксу заступа пре свега Завод за патенте и жигове САД који још од седамдесетих година прошлога века почиње одобравати патенте за софтвер. У том погледу је уведен тзв. Фриман-Волтеров тест за оцену математичких алгоритама на којима је софтвер базиран. Према овом тесту претходно се испитује да ли патентни захтев директно или индиректно садржи формуле или једначине. Ако би одговор био позитиван даље би се испитивало да ли је патентни захтев усмерен на математички алгоритам као такав или на процес, машину, производ или композицију, што су заправо врсте проналазака у америчком патентном праву. Почев од 1996. године у САД је у смислу поступка и услова признавања патентне заштите у примени Водич за испитивање проналазака везаних за компјутере.²⁶ Напоменимо и то да је у САД у последње време присутна тенденција ширења патентно правне заштите на пословне методе и то посебно у области интернет индустрије као што су рецимо поступци намењени анализи одлука на интернету, интернет системи за заштиту купаца,

²⁴ О овоме види више код: Davis J: Intellectual Property Law, Oxford University Press, 2008, p.267; McQueen H, Waelde C, Laurie G: Contemporary Intellectual Property – Law and Policy, Oxford University Press, 2008, p. 412.

²⁵ Идрис К: Интелектуална својина, моћно средство економског раста, Београд 2003, стр.92.

²⁶ Шарбох С: Заштита софтвера патентима у САД и земљама ЕУ, Правни живот 11/2004, стр.847.

финансијски системи на интернету. У тој држави је тако 2000. године издато 899 патената за проналаске поступака за обављање посла, а само компанија *Dell Computer* је до сада стекла 77 патената који се односе на пословне методе.²⁷ И у неким другим државама, Јапану рецимо, флексибилно се омогућава патентна заштита рачунарских програма, али само оних који проширују меморију компјутера и имају технички карактер, најчешће оперативним системима и графикама, који испуњавају технички карактер новости. Принцип индиректне заштите компјутерских програма, као дела патента машине, прихваћен је и у Великој Британији.

Наше право је у смислу патентно правне заштите уопште, па према томе и патентне заштите компјутерских програма, конципирано по угледу на Европску конвенцију о патентима. Отуда наш Закон о патентима²⁸ експлицитно искључује патентну заштиту компјутерских програма не сматрајући их проналасцима. Додуше, може се рећи да могућност индиректне патентне заштите компјутерских програма није искључена. То ће бити случај када се патентном пријавом за заштиту нових компјутера, поступака, примене производа или поступака или неког другог проналаска који може бити у форми погодној програмираном рачунару и који представља решење на нов начин неког техничког процеса или проблема, обухвати и рачунарски програм и софтвер. Тада рачунарски програм прати други проналазак, као његов део.

3. Компјутерски програми и заштита жигом

Компјутерски програми и софтвери су, без обзира на своје специфичности, роба. Појављују се на тржишту, продају и купују. Огромна експанзија фирми које се баве производњом и дистрибуцијом компјутерских програма условила је и то да међу њима постоје веће или мање сличности па се као важно поставља питање како их разликовати: по произвођачу, по називу, по амбалажи, по склопу и распореду боја, по знацима којима се обележавају или по свему овоме заједно ?

²⁷ Идрис К, наведено дело, стр. 93.

²⁸ Сл. лист СЦГ 32/04; члан 5. став 5. тачка 4. Закона о патентима.

Један од одговора на ово питање је свакако по знацима разликовања чија је основна сврха обележавање и разликовање роба и услуга које се појављују на тржишту. Да се подсетимо: знакови разликовања су право и то апсолутно право које садржи две врсте овлашћења, позитивно и негативно. Позитивно овлашћење састоји се у праву титулара да користи предмет заштите, а негативно подразумева могућност да титулар права свим трећим лицима забрани неовлашћено коришћење права.²⁹

Следеће важно питање је којим се то од знакова разликовања на оптималан начин може штитити компјутерски програм, обзиром да ових права има више: право на жиг, модел и узорак, ознака земље порекла.

Заштита компјутерских програма се изузетно ретко везује за модел и узорак па и за ознаку земље порекла. Међутим, ознака порекла производа се у ширем смислу везује не само за ознаку земље у којој је неки производ произведен већ и за специфичне вештине и знања људи са неког подручја. У овом смислу би се право на ознаку порекла производа могло у одређеним случајевима применити и на компјутерски програм и софтвер. Тако је рецимо примарно захваљујући пословном угледу *IBM* САД прихваћена као земља у којој израда компјутерских програма и софтвера претпоставља одређени квалитет па би и стављање ознаке порекла производа на такав производ имало и одређену гарантну функцију. Таква функција међутим ипак није довољна у смислу потпуне правне заштите компјутерских програма па се они у пракси најчешће штите жигом.

Имајући у виду да је жиг право којим се штити знак који је у промету намењен за разликовање робе односно услуга исте или сличне врсте једног физичког или правног лица и да се ставља на робу или њено паковање, те је везан за телесне ствари (робни жиг – *trade mark*) или служи за разликовање разних услуга (услужни жиг – *services mark*) то се њиме могу штитити и компјутерски програм и софтвер. И робни и услужни жигови могу се графички представљати као речи, слогани, слова или комбинације речи и слова, бројева или цртежа и слика. Они такође могу бити и тродимензионалне форме као и видео и аудио ознаке.

²⁹ Дракулић М, наведено дело, стр. 205-206.

Не ретко се истичу следеће функције знака заштићеног жигом: а) идентификација произвођача или пружаоца услуга; б) разликовање једне врсте програма и услуга од других истих или сличних; в) гарантовање одређеног квалитета програма или услуга; г) пропаганда, јер је моћно средство за рекламу.

Посматрајући упоредно правна законска решења као и њима одговарајућу судску праксу у области заштите компјутерских програма жигом може се констатовати следеће:

а) рачунарски програми и софтвер могу бити заштићени жигом по готово свим правима;

б) као предмет заштите жигом у вези са рачунарским програмима и софтвером појављује се њихов назив и знак под којим се појављују у промету као и знак произвођача или пружаоца услуга. Поред назива овим правом се штити и облик амбалаже, боје и њихов распоред као и низ других пратећих ствари;

в) заштита програма и софтвера жигом траје између 7 и 20 година, уз могућност неограниченог продужавања. Готово сва права предвиђају и могућност престанка права на жиг услед његовог некоришћења, углавном у периоду између 3 и 6 година;

г) у свим земљама као услов за стицање права на жиг за компјутерске програме или софтвер појављује се дистинктивност, што значи да знак програма или софтвера мора бити такав да га одваја од свих других;

д) појављују се две групе земаља у односу на основ настанка права. Једна група земаља (САД, Велика Британија, Италија) као основ овог права имају две могућности: регистрацију и право прве употребе. Друга група земаља (Немачка, Француска, Скандинавске земље...) стицање права на жиг везује само за регистрацију. Без обзира која од земаља је у питању код регистрованог жига појављује се ознака *R (registered)* у горњем десном углу знака. Постојањем овог знака или применом права прве употребе означава се да носилац права има одређена имовинско правна овлашћења, најчешће права искључиве употребе тог знака и забране трећим лицима да тај знак употребљавају;

е) углавном све земље предвиђају и додатну заштиту ауторским правом;

ж) право на заштиту жига и подношење пријаве за заштиту знака програма или софтвера може добити и међународне размере уколико се од домаћег надлежног органа тражи и међународна заштита односно међународна регистрација, углавном на основу Париске конвенције или Мадридског аранжмана.³⁰

У нашем праву, сходно Закону о жиговима³¹, такође је омогућена заштита компјутерских програма и софтвера жигом и то у поступку њихове регистрације. Основни законски услов је дистинктивност и примењивост у промету као и облик који знак може имати. Знак се може састојати од речи, слогана, слова, бројева, слика, цртежа, распореда боја, тродимензионалних облика али и од музичких фраза које се могу графички приказати. Рок заштите регистрованог компјутерског програма или софтвера је 10 година, с тим што се може неограничено продужавати. Право на заштиту међутим престаје уколико се жиг без оправданог разлога не користи непрекидно 5 година од дана уписа у регистар жигова.

4. Компјутерски програми и заштита од нелојалне конкуренције

Велико повећавање броја корисника рачунарских програма и софтвера, а с тим у вези и изузетан профит који се њиховом продајом остварује намеће оштру борбу између конкурентских фирми, борбу у којој се често не бирају средства. Тако се све чешће врши злоупотреба или имитирање жигова, оцрњивање односно давање нетачних података о програмима и софтверима својих или конкурентских фирми, што у исто време условљава и велики број судских спорова између оних који су се служили различитим делима квалификованим као дела нелојалне конкуренције и оних који су по том основу тражили правну заштиту. На основу таквих случајева у упоредном праву се поступно појављују решења која предвиђају могућност заштите компјутерских програма мерама заштите

³⁰ Дракулић М, наведено дело, стр.213-214.

³¹ Сл.гласник РС 104/09.

од нелојалне конкуренције. Њиховом анализом могу се извући и одређени закључци:

прво, компјутерски програми и софтвер могу бити угрожени делима нелојалне конкуренције и сходно томе заштићени мерама које се примењују ради предупређења или кажњавања таквих дела. При томе постоје две групе земаља: оне које примењују метод „генералне клаузуле“ и штите све оно што може бити угрожено делима нелојалне конкуренције; оне које користе метод „лимитативног набрајања“ па компјутерски програм и софтвер штите само ако су они као такви експлицитно наведени у одговарајућем закону;

друго, као појавни облици у којима се испољавају дела нелојалне конкуренције најчешћи су нелојална реклама, оцрњивање, давање нетачних података о себи или роби, прикривање мана, подмићивање, неовлашћена употреба обележја друге организације;

треће, као предмет заштите од дела нелојалне утакмице компјутерски програми и софтвер се не штите као такви већ се санкционише сама радња противна добрим пословним обичајима којом се наноси или може нанети штета другој организацији, а ради стицања предности на тржишту;

четврто, заштита се у већини правних система састоји у имовинскоправној заштити која се остварује тужбом у грађанском поступку;

пето, овај облик заштите је по правилу супсидијаран, што значи да се он појављује као додатна заштита уз друге облике заштите.³²

У нашем праву нелојална конкуренција је Законом о трговини³³ дефинисана као радња трговца противна добрим пословним обичајима и којом се наноси штета или може нанети штета другом трговцу, другом правном лицу и купцу, односно потрошачу. Актима нелојалне конкуренције сматрају се нарочито: рекламирање, оглашавање или нуђење робе навођењем података или употребом израза којима се ствара или се може створити заблуда на тржишту о тој роби, чиме се одређени трговац доводи или може

³² Дракулић М, наведено дело, стр. 231-233.

³³ Закон о трговини Републике Србије, Сл.лист СРЈ 32/93...37/02; Сл.гласник РС 85/05, 101/05; чланови 22. и 23. Закона о трговини.

довести у повољнији положај; изношење неистина или оцрњивање другог трговца који штете његовом угледу и пословању; продаја робе са ознакама или подацима који стварају или могу створити забуну у погледу порекла, начина производње, квалитета, количине или других својстава робе; прикривање мана робе или довођење купца у заблуду на други начин; неовлашћена употреба законом заштићених спољних ознака другог трговца (назив, фирма, робни жиг, услужни жиг, знак квалитета, знак порекла...) или употреба ознака које нису законом заштићене, којом се ствара или се може створити заблуда у промету робе на штету другог трговца који те ознаке употребљава у свом пословању.

Према наведеном јасно је да се нашим прописима штити све оно што може бити угрожено актима нелојалне конкуренције (генерална клаузула), па према томе и компјутерски програми.

5. Компјутерски програми и ауторскоправна заштита

Да би компјутерски програм уживао ауторскоправну заштиту он мора да представља интелектуалну творевину која је настала као резултат духовног стваралаштва одређене особе, творца дела. Обзиром да се ради о творевини људског духа поставило се питање да ли она мора бити у некој форми и ако мора у којој да би уживала ауторскоправну заштиту. У овом погледу се појављују два схватања: прво, монистичко, према којем идеја која је подобна да буде предмет ауторскоправне заштите мора бити изражена у некој форми обзиром да она сама, као део унутрашње личности неког лица и његовог интелекта не ужива ауторскоправну заштиту. При томе врста, начин и облик изражавања не представљају кључну компоненту за заштиту ауторског дела; друго, дуалистичко схватање полази од тога да се изражајна форма дела и идеја не могу одвојити па отуда ауторскоправна заштита обухвата и једну и другу компоненту ауторског дела.³⁴

Но без обзира на различите теоријске приступе, који су се као такви рефлектовали у одређеним правним системима, пракса показује да је

³⁴ Дракулић М, наведено дело, стр.247.

ауторскоправна заштита најчешће коришћени облик заштите компјутерских програма.

И овај облик заштите се примарно појављује у САД где је по први пут дошло до сврставања компјутерских програма у ауторска дела и њиховој заштити ауторским правом на идентичан начин као и за штампана ауторска дела (књиге). Од времена у којем се овакво решење по први пут појавило у САД, а реч је о 70-им годинама прошлога века, па до данас дошло је до измена прописа о ауторском праву у читавом свету. Њихов компаративни преглед омогућава да се решења постојећа у појединим државама групишу на следећи начин:

а) у прву групу земаља би могли сврстати земље које рачунарске програме подводе под литерална дела;

б) у другу групу земаља би могли сврстати земље које рачунарске програме третирају као посебна ауторска дела;

в) у трећу групу земаља спадају земље које рачунарске програме виде као преводе или друга ауторска дела;

г) четврта група земаља рачунарске програме сврстава у научно техничке приказе;

д) постоје коначно и земље у којима се компјутерским програмима признаје ауторскоправна заштита али само у судским споровима, не и у прописима.

Најзаступљенија је ипак она група земаља која рачунарске програме у погледу ауторскоправне заштите изједначава са књижевним делима. Даља анализа садржине упоредних прописа који предвиђају ауторскоправну заштиту компјутерских програма упућује на следеће закључке:

а) најчешће предвиђено решење у заштити компјутерског програма као ауторског дела је његово подвођење под књижевна дела и примена модификованих правила која се предвиђају за њихову ауторскоправну заштиту;

б) у већини земаља штите се материјализовани компјутерски програми, што је последица претходно изнетог монистичког схватања правне

природе ауторског дела. То практично значи да компјутерски програм мора бити изражен у некој форми, а да се сама идеја не штити;

в) у безмало свим националним правима ауторима се признају сва морална права док, ако је реч о врстама признатих имовинских права, постоје разлике. Тако се рецимо најчешће посебно регулишу питања заштите права аутора везана за умножавање и копирање, прераду и превођење програма.

Није неважно напоменути да ауторскоправна заштита компјутерских програма има своју снажну међународно правну димензију. Наиме, на ову форму заштите могу се применити одредбе Бернске конвенције о заштити књижевних и уметничких дела као и Универзалне или Женевске конвенције. Могло би се ипак рећи да већи непосредни значај имају они међународно правни извори који се у целини односе на ауторскоправну заштиту компјутерских програма. Такви су Модел закона за заштиту компјутерског софтвера из 1977. године донет од стране Светске организације за заштиту интелектуалне својине, Резолуција о заштити компјутерског софтвера и интегрисаних кола из 1986. године, донета од стране Међународног удружења за заштиту права индустријске својине, Директива ЕУ о правној заштити компјутерских програма из 1991. године и коначно Споразум о трговинским аспектима права интелектуалне својине (TRIPS) из 1994. године.³⁵

Директива ЕУ о правној заштити компјутерских програма полази од следећих претпоставки:

прво, компјутерски програм обухвата материјализацију у сваком облику, записа или кода низа инструкција на основу којих рачунар извршава појединачне наредбе или функције. Компјутерски програм дакле не обухвата идеје, принципе, логику, алгоритме програмског језика који су укључени у програм;

друго, програми се штите као ауторско и то као књижевно дело;

³⁵ TRIPS споразум, Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), који укључује и питање трговине кривотвореном робом, чини Анекс 1С Споразума из Маракеша којим се установљава Светска трговинска организација. Споразум је закључен 15. априла 1994. године, а на снагу је ступио 1. јануара 1995. године и од тада обавезује све чланице СТО. На основу члана 10. тачка 1. TRIPS рачунарски програми, било у изворном или извршном коду штите се као књижевна дела на основу Бернске конвенције (1971).

треће, прихватају се и други аспекти и објекти заштите компјутерских програма уколико то није део заштите предвиђене Директивом и не коси се са њом. Практично то значи да ако је рецимо софтвер по националном праву заштићен као посебно књижевно дело онда се таква могућност заштите не искључује самом чињеницом да софтвер није непосредни објект заштите који је Директивом обухваћен. Поред тога дозвољена је и могућност додатне заштите институтом пословне тајне, нелојалне утакмице или осталим правима предвиђеним у националним законима;

четврто, да би компјутерски програм могао да се штити Директивом неопходно је да буде оригиналан;

пето, заштита се гарантује 50 година од дана настанка програма.

Према нашем Закону о ауторским и сродним правима³⁶ под ауторским делом се између осталог сматра и рачунарски програм у било којем облику, укључујући и припремни материјал за његову израду.

6. Компјутерски програми и заштита *sui generis* правом

Дуго времена је могућност да се компјутерски програми и софтвери штите правом *sui generis* разматрана као најбољи оквир заштите обзиром да је и сам предмет заштите прилично специфичан. Овакав приступ је имао своје промотере и у Светској организацији за заштиту интелектуалне својине чији је Модел закона о заштити компјутерског софтвера делом био базиран на специфичним правним облицима заштите компјутерског софтвера. Мада су биле привржене овом облику заштите неке државе (Шведска, Словачка, Чешка...) нису имале довољно утицаја да своје ставове „наметну“ у нешто ширем међународноправном контексту. Видели смо претходно да је доминантни облик правне заштите компјутерских програма и софтвера како на националним тако и на међународном нивоу ауторскоправна заштита. И то без обзира на неспорне специфичности оваквих објеката заштите као ауторских дела. Из тих разлога је концепт заштите правом *sui generis* данас углавном маргинализован.

³⁶ Службени гласник РС 104/09.

7. Компјутерски програми и заштита пословне тајне

Пословном тајном се начелно говорећи штите пословне информације и документи неопходни за формирање пословног знања, дакле подаци који се користе у пословању и који се скривају и чувају од јавности. Као најчешћи подаци који се проглашавају пословном тајном појављују се производи, формуле, технолошки процеси, метод рада, документација о истраживањима и развоју, машине и њихове измене, преписка, интерна пословна документација, информације о клијентима, финансијске и књиговодствене информације, документа о плановима и стратегији, узорак, компилације и свакако рачунарски програми, софтвери као и поступак програмирања и имплементације.

Практично посматрано највише пословних тајни је везано за институт *know how* као скуп практичних знања и акумулираних искустава нематеријалног карактера за које је значајно да се материјализују у неким стварима или на неки начин како би могли бити пренети на трећа лица. Да би неко знање и искуство представљало *know how* потребно је да има следеће елементе: тајност, новост, преносивост и економски интерес за онога ко их поседује. При томе се елементи тајности и економског интереса управо обезбеђују на тај начин што се *know how* проглашава за пословну тајну.

Из претходно реченог је очигледно да компјутерски програми могу бити предмет заштите по основу правног института пословне тајне што је као такво прихваћено и у позитивном праву највећег броја земаља. При томе се могу уочити и неки различити приступи:

а) неке земље доносе посебне законе о пословној тајни, као што је случај са САД;

б) један број држава (Јапан, Немачка...) пословну тајну регулише у оквиру прописа о сузбијању нелојалне утакмице;

в) у једном броју земаља пословна тајна је предмет грађанских и кривичних законика;

г) у неким земљама се институт пословне тајне третира у читавом низу закона и других прописа, не само антимонополских, кривичних или грађанских већ и трговачких;

д) коначно, у неким земљама пословна тајна није дефинисана прописима али је зато своју пуну заштиту нашла у судској пракси.

Када су у питању компјутерски програми и софтвер готово да нема ничега у вези са њима што не може имати третман пословне тајне. Ипак, најчешћи предмет пословне тајне су: а) компјутерски програм у целини или његови делови (идеја, низ инструкција, структура, алгоритам); б) процес дизајнирања програма од спецификације проблема до тестирања програма; в) багови и процеси дебагирања; г) новост у програму заштићеном патентом; д) кориснички интерфејс и начин решавања звучне и графичке подлоге; ђ) софтвер; е) продукти реверзибилног инжењерства; ж) компилације; з) преводи; и) начин заштите од неауторизованог приступа, коришћења, модификовања, копирања; ј) методологија пројектовања и дизајнирања решења информационог система; к) документација о плановима даљег развоја софтверске фирме и њеној стратегији.

У вези претходно реченог потребно је напоменути и то да је пословна тајна уопште најчешће угрожена од садашњих и бивших запослених, хакера, аматера и професионалаца, ангажованих стручњака, конкурената, партнера, службеника пословних банака и других лица. Откривање пословне тајне врло често представља и криминалну радњу односно дело индустријске шпијунаже. Али у сваком случају починиоци односно лица која откривају пословну тајну су најчешће садашњи и бивши запослени.³⁷

На међународном плану коришћењу пословне тајне као механизма заштите компјутерских програма није посвећена већа пажња. Изузетак је Споразум о трговинским аспектима права на интелектуалну својину који садржи и дефиницију поверљивих података сматрајући их као „целину или скуп неопходних компоненти које нису познате јавности или лако доступне другим лицима у круговима који се уобичајено баве том врстом информација.“ Реч је о подацима који имају тржишну вредност између осталог и због своје поверљивости и који су предмет мера које предузимају лица обавезна да чувају поверљиве податке на основу прописа. Да би се компјутерски подаци односно програми посматрали као пословна тајна сходно наведеном Споразуму неопходно је:

³⁷ Дракулић М, наведено дело, стр. 321-322.

а) да буду поверљиви, што значи да сви програми не могу задовољити тај услов већ ће то по правилу бити одређени програми или софтвери рађени по наруџбини или они чија је природа специфична и поверљива;

б) да буду велике тржишне вредности (рецимо изворни код и програмска решења *Windows 97*);

в) да буду заштићени посебним мерама и то од стране субјеката одређеним прописима.³⁸

Наше право спада у групу оних правних система у којима је пословна тајна као правни институт третирана, непосредно или посредно, у читавом низу закона. Код нас су то рецимо Закон о привредним друштвима, Закон о заштити конкуренције, Закон о трговини, Закон о облигационим односима, Кривични законик...

Према Закону о привредним друштвима под пословном тајном се разуме информација о пословању одређена оснивачким актом, актом или уговором ортака или уговором чланова друштва, односно оснивачким актом или статутом акционарског друштва, за коју је очигледно да би проузроковала штету привредном друштву ако би дошла у посед трећег лица.³⁹

Сходно Кривичном законiku Републике Србије пак под пословном тајном се сматрају подаци и документи који су на основу закона, другог прописа или одлуке надлежног органа донетом на основу закона проглашени пословном тајном, а чије би одавање проузроковало или би могло да проузрокује штетне последице за предузеће или други субјект привредног пословања. Одавање пословне тајне је при томе предвиђено као кривично дело за које је запређена казна затвора у трајању од 3 месеца до 5 година.⁴⁰

Имајући у виду чињеницу да се пословна тајна угрожава најчешће од стране запослених, бивших или садашњих, као ефикасан облик заштите се појављују и појединачни уговори о раду. На овај начин послодавци уговарају

³⁸ Наведено према: Дракулић М, наведено дело, стр. 329-330.

³⁹ Закон о привредним друштвима РС, члан 38.

⁴⁰ Кривични законик РС, члан 240. тачка 1.

такве уговоре клаузуле конкуренције којима се запосленима забрањује да се одређено време након напуштања фирме у којој раде запосле у некој конкурентској фирми или да у истој делатности започну свој посао, као и да дуже или краће време буду обавезни, под претњом озбиљних имовинских санкција, да чувају у тајности све оно што је актима фирме одређено као пословна тајна.

Резимирајући претходно речено о употреби института пословне тајне у заштити компјутерских програма може се закључити следеће:

прво, примена пословне тајне је могућа код заштите компјутерских програма и софтвера, посебно ако је реч о производњи за познатог купца;

друго, овај облик заштите се често предвиђа у уговорима склопљеним приликом набавке „спољног“ софтвера и опреме као и у одговарајућим општим актима и уговорима уколико се програм израђује у организацији која га и користи. На тај начин се домет пословне тајне ограничава и обухвата ужи круг лица који са таквим програмом долазе у везу, што на неки начин може бити и предност у односу на остале облике заштите;

треће, пословна тајна може представљати веома ефикасан облик заштите компјутерских програма и софтвера, нарочито за оне објекте који не уживају други облик заштите;

четврто, заштита пословном тајном не искључује друге облике заштите што практично значи да се може примењивати паралелно са њима;

пето, заштита пословном тајном свој пуни смисао има када је реч о заштити од стране запослених док се њом мање ефикасно штити компјутерски програм и софтвер од екстерних починилаца, па и бивших запослених.

ЗАШТИТА БАЗА ПОДАТАКА

1. Опште напомене о заштити база података

У најопштијем смислу базе података (*data base*) се могу одредити као корисне, организоване збирке структурираних података који се налазе у различитим датотекама међусобно повезаних програмима који омогућавају приступ корисницима. То су дакле било какве збирке ускладиштених података и/или информација, без обзира како су изражене, а које су организоване и уређене сагласно неком основном принципу компилирања у дела или материјале и која омогућава кориснику проналажење (тренутно или најбрже могуће) и коришћење појединачних садржаја.

Дуго времена право није било превише заинтересовано за „бављење“ базама података обзиром да су оне служиле углавном за потребе држава и њихових органа, а ређе за појединачне, индивидуалне интересе. Експанзија савремених средстава комуницирања произвела је међутим и њихову снажну и широку економску употребљивост па се с тим у вези појављују и многобројне злоупотребе у погледу коришћења база података. Таква ситуација је налагала правним системима да се озбиљније позабаве овом проблематиком, а сам почетак је био правно одређење односно дефинисање битних елемената база података. У том смислу база података се најчешће одређује као збирка, ређе компилација, при чему се под збирком подразумева дело настало сакупљањем и складиштењем постојећих материјала или података који су одабрани, повезани или уређени на такав начин да за резултат имају оригинално дело свог аутора. Под компилацијом се пак разуме дело прераде у коме су видљиве карактеристичне особине тог, већ постојећег дела. При томе је неопходно да су:

а) подаци у бази података уређени и организовани по одређеним принципима;

б) подаци, материјал и/или дела која чине збирку тако одабрани, повезани и уређени да чине интелектуалну творевину и ново дело, при чему се под делом подразумева литерално, уметничко, музичко или неко друго ауторско дело, а под материјалима текстови, звуци, слике, бројеви, чињенице, подаци или комбинација појединих од њих;

в) такви одабрани, систематизовани и структурирани подаци материјализовани на неком носиоцу, рецимо магнетном, оптичком, електронском или неком другом.

Базе података се могу делити по различитим критеријумима. То могу бити рецимо медицинске, географске, статистичке, правничке, демографске и неке друге базе података. Ипак једна од правно најрелевантнијих подела база података је следећа:

а) библиографске базе података, су оне које садрже заглавља, наслове или друге идентификационе ознаке, уређене по неком систему или принципу, које указују кориснику где је лоцирано неко дело или информација као што су рецимо монографије, судски случајеви и слично;

б) базе абстракта или резимеа, су оне из којих корисници могу доћи до непосредних знања односно резимеа о неком делу без читања целог текста;

в) базе интегралног текста су оне које кориснику непосредно дају на увид комплетан текст неког дела;

г) остале базе могу бити адресари, именици, спискови потрошача, набављача, материјала, каталози роба и услуга.⁴¹

2. Правна заштита база података

Први прописи о заштити база података везују се за неке земље чланице ЕУ, затим САД, Аустралију и Јапан. Реч је о 80-им годинама прошлога века.

Разуме се, пре доношења било каквих правних аката нарочито дискутовано питање је било на који начин, којим правним институтима и механизмима се може постићи оптимална заштита. Разматране су разне могућности, између осталог и заштита правом *sui generis*, затим заштита на основу сродних права, ауторског права, права нелојалне конкуренције. Обзиром да је идеја о заштити правом *sui generis* релативно брзо напуштена,

⁴¹ Дракулић М, наведено дело, стр.343-345.

као уосталом идеја заштите на основу сродних права, нешто више ћемо рећи о преостала два облика правне заштите база података.

3. Базе података и ауторскоправна заштита

Ауторскоправна заштита се показала као најефикаснији односно најпотпунији облик заштите база података. У техничком смислу овакав начин заштите омогућава и једнаку заштиту у свим државама потписницама Бернске конвенције. Ипак, нека отворена питања и неке дилеме у вези са овим обликом заштите није било лако превазићи.

Једно од таквих питања је да ли базе података треба посматрати као неко већ познато или као посебно ауторско дело. Практично посматрано базе података су најчешће подвођене под омотач заштите збирки или компилација, чиме се губила разлика између папирнатих и електронских форми. Аргументи за овакво поступање су се проналазили у поређењу са писаним делима односно поистовећивању података у машински читљивој форми на било којим носиоцима са било којим записима на папирним медијима. Проблем је међутим настао када је требало уподобити термин „издавање“ односно „објављивање“ у конвенционалном смислу на аутоматизоване базе. Ово посебно услед околности да се аутоматизоване базе могу мењати континуирано, из секунда у секунд, припајањем или брисањем одређених садржаја, тако да би могао бити велики проблем шта се то заправо ауторским правом штити односно у ком моменту је заштићен садржај базе података. Расправе су такође вођене, и још увек се воде, око тога да ли нека компилација података (или материјала) каква је база поседује довољно оригиналности обзиром да подаци у рачунару често и нису посебно, креативно уређени већ се то постиже софтвером или, у неким случајевима, посебним захтевом корисника. Проблем се даље појавио око тумачења значења поступка „скидања“ (*downloading*) података (материјала) и смештања у рачунар. Питање које се поставља је да ли се „скидање“ може третирати само као просто складиштење података у машински читљивој форми или се ради о новом делу. Компилације се продужавају уколико „скинути“ подаци нису фиксно уређени на одређени начин, нов и оригиналан, тако да постоји значајна сличност између новог и раније заштићеног дела. Тешко се такође

тумачи значење термина „копирање“ и репродуковање обзиром да свако укључење базе може да се третира као својеврсно репродуковање.

Међутим, третманом базе као збирке или компилације обезбеђују се иста ауторска права у односу на кориснике као када су у питању било које збирке или антологије. Она се нарочито односе на копирање, објављивање, мењање и адаптирање као и „извођење“.

3.1. Базе података и регулисање заштите од нелојалне конкуренције

Како ауторскоправна заштита није решење за све „опасности“ које прете базама података у неким земљама се примењују и додатни механизми заштите. Један од таквих механизма је и заштита од нелојалне конкуренције посебно примењива у случајевима неовлашћеног копирања или „вађења“ садржаја из база података. Додуше, како се нелојална утакмица у основи заснива на правилима поштене тржишне утакмице односно добрих пословних обичаја то је неопходно претходно формирати у пословној пракси оно што се, када је реч о копирању односно „вађењу“ садржаја из база података, сматра добрим пословним обичајима.

У сваком случају овај облик заштите јесте, а могао би бити још заступљенији у националним законодавствима. Ово посебно имајући у виду околност да ова форма заштите не искључује примену других па може бити њихова ефикасна допуна.

4. Базе података и међународна заштита

Све већи значај и економско коришћење база података допринели су томе да за њихову заштиту постану заинтересоване и међународне струковне и друге организације. Тако је у оквиру Светске организације за заштиту права интелектуалне својине (*WIPO*) дискутована могућност заштите база података по основу Бернске конвенције за заштиту књижевних и уметничких дела. Комитет експерата који се овом проблематиком бавио донео је Меморандум у којем се, између осталог, констатује да се збирке података или других незаштићених материјала може сматрати литералним или уметничким делом

и да се могу штитити на исти начин као и збирке дела на које се примењује члан 2. Бернске конвенције. Додуше, овакав облик заштите није аутоматски, другим речима неопходно је да базе података испуњавају и одређене услове уподобљене условима који се захтевају за заштиту књижевних и уметничких дела.

Други значајан међународни напор у погледу заштите база података учињен је у оквиру *GATT* приликом Уругвајских преговора везаних за усвајање тзв. Финалног акта, чији се посебан Споразум односи на међународну трговину права интелектуалне својине. Мада је Споразум о трговинским аспектима права интелектуалне својине пропустио да дефинише посебна права која аутори база података треба да уживају његов значај је у томе што даје одређене дефиниције и услове за њихову заштиту. Њиме је дакле одређено:

а) да се базе сматрају компилацијама података или материјала, без обзира на форму у којој се налазе;

б) да се као интелектуална творевина штити избор или уређење садржаја, а не сами подаци и материјал који као такви већ уживају ауторскоправну заштиту;

в) да су у питању остварења, а не идеје, методе или математички концепти као такви;

г) да се као услов третмана базе као интелектуалне творевине појављује оригиналност;

д) да је трајање заштите онолико колико је предвиђено Бернском конвенцијом (50 година од дана настанка базе);

ж) у случају повреде права примењиваће се поступци и правила који важе за друге врсте интелектуалне својине, од грађанских, управних, кривичних и других.⁴²

⁴² Према члану 10. тачка 2. *TRIPS* збирке података или другог материјала, било да су машински читљиве или у некој другој форми, које због начина избора или груписања садржаја сачињавају интелектуалне творевине, штите се као такве. Таква заштита, која се не односи на саме податке или материјал, неће вређати ауторско право којим се штите дати подаци или сам материјал.

За нас је у смислу међународно правне заштите база података посебно значајна Директива о правној заштити база података која је донета на нивоу ЕУ 1996. године.⁴³ Наведеном Директивом базе података су дефинисане као збирке независних дела, података или других материјала систематски или методично уређених и појединачно приступачних електронским путем или на други начин, при чему се правна заштита односи на све базе, без обзира у којој су форми. Предмет заштите су базе података које, на основу избора или уређења њиховог садржаја, представљају оригиналну интелектуалну творевину и оне уживају ауторскоправну заштиту која се односи на њихов садржај.

Као аутор се може појавити једно или група физичких лица која су базу створила као и правна лица, уколико су правом државе чланице признати као носиоци права. Аутор базе података при томе има следећа ексклузивна права да изврши или ауторизује:

а) повремено или стално репродуковање у било ком смислу и у било којој форми, у целини или делу;

б) превођење, адаптацију, уређивање или било коју другу промену;

в) сваки облик дистрибуције базе или њених копија;

г) сваку комуникацију, излагање или извођење базе у јавности;

д) свако репродуковање, дистрибуирање, комуницирање, приказивање или извођење резултата превођења, адаптације, уређивања или било које друге промене.

Директива такође садржи и одређена *sui generis* права која ужива произвођач база чије се инвестиције могу квалификовати и/или квантификовати у постизању, верификацији или презентацији садржаја који се жели заштитити од вађења и/или поновног коришћења комплетног или битног дела. Термин „вађење“ при томе значи стални или привремени трансфер целог или битног дела садржаја базе на други медијум у било ком смислу и било ком облику, а „поновно коришћење“ било који облик чињења доступним јавности дела или целог садржаја базе дистрибуирањем копије,

⁴³ Council Directive on the Legal Protection of Database, OJ of the EU 27/3/96.

закупом, преносом *on line* или на други начин. Право на заштиту од неовлашћеног вађења и поновног коришћења траје 15 година од дана завршетка израде базе.

Значај Директиве о чијем садржају је претходно било речи огледа се посебно у следећем: прво, она је први посебан акт којим се регулише заштита база података на целовит начин; друго, призната је специфичност база као предмета заштите и предвиђена заштита аутора али и произвођача и овлашћених корисника база; треће, правила из Директиве су правила тзв. минималне хармонизације што практично значи да су она минимум заштите коју у своје прописе морају унети све чланице ЕУ; четврто, утицај Директиве се протеже и ван граница ЕУ.

4.1. Нова *sui generis* заштита база података

Директива о правној заштити база података садржи, као што је претходно и напоменуто, и одредбе о *sui generis* заштити база података. Неки аутори ову форму заштите одређују као нову *sui generis* заштиту база података.⁴⁴

Док се ауторским правом, а сходно предметној Директиви, штити креативност аутора, његов интелектуални напор односно садржај базе података који је резултат такве креативности и напора дотле се, у исто време, правом *sui generis* штити инвестирање у базе података. Инвестирање се при томе може састојати како у улању финансијских средстава тако и у улагању времена, напора и енергије. Другим речима инвестиција се може састојати из улагања било којих ресурса: финансијских, људских и техничких односно технолошких. Али у сваком случају инвестиција мора бити суштинска, при чему њена својства морају бити мерљива квантитативно или квалитативно, или на оба начина.

У базу података у коју је неопходно инвестирати то може учинити њен аутор или било које друго физичко и/или правно лице. База података која је заштићена ауторским правом може такође бити заштићена и новим *sui generis* правом што међутим није неопходно уколико база података није резултат

⁴⁴ Chris R – John A: Computer Law, Oxford University Press, New York 2003, p. 243.

људске креативности у селекцији или аранжману њеног садржаја. Овим новим *sui generis* правом се не може штитити колекција која не одговара појму базе података из Директиве о правној заштити база података чак и ако таква колекција може бити заштићена ауторским правом сходно националним прописима. У сваком случају једна база података може се штитити и ауторским и новим *sui generis* правом али при томе: а) свака форма заштите захтева испуњење посебних критеријума; б) свака форма заштите обезбеђује различите форме и услове заштите; в) свака форма заштите може бити право различитих лица.

5. Правна заштита база података по нашем праву

Заштита база података остварује се у нашем праву углавном кроз два правна акта: Закон о ауторском и сродним правима и Кривични законик.

Закон о ауторском и сродним правима базе података, без обзира да ли су у машински читљивој или другој форми, третира као збирке и по том основу им пружа ауторскоправну заштиту као и свим другим ауторским делима. Сходно Закону базе података су збирке засебних података, ауторских дела или других материјала уређених на систематичан или методичан начин, који су појединачно доступни електронским и другим путем. Базом података се међутим не сматра рачунарски програм који се користи за њено стварање или рад.

На посебном месту Закон регулише имовинска права произвођача база података, физичког или правног лица које је сачинило базу података тако што је у квалитативном односно квантитативном смислу учинило значајно улагање у прибављање, проверу или презентацију њеног садржаја. Произвођач базе података има искључиво право да другоме забрани или дозволи:

а) повремено или стално умножавање било којим средствима базе података у целини или њених битних делова, за било коју намену и у било којој форми;

б) стављање у промет или давање у закуп примерака целе базе података или њених битних делова;

в) повезивање на рачунарску мрежу и сваки други облик јавног саопштавања базе података у целини или њених битних делова.

Кривични законик садржи између осталог и главу која је посвећена кривичним делима против интелектуалне својине. У том смислу заштита база података „покривена“ је члановима 198 (Повреда моралних права аутора и интерпретатора) и 199 (Неовлашћено искоришћавање ауторског дела или предмета сродног права).

ЗАШТИТА ТОПОГРАФИЈЕ ИНТЕГРИСАНИХ КОЛА

1. Правна заштита топографије интегрисаних кола у упоредном и међународном праву

Развој хардвера не може се замислити без „силиконског чипа“ или једноставно чипа. Овај минијатурни део компјутера постао је једна од кључних тачака компјутерске индустрије и кроз њега се у доброј мери одређује позиција једне земље у информационом окружењу. Као и за остале предмете заштите о којима је претходно било речи и овде је повећање економског значаја и улоге компјутерске индустрије непосредно утицало на појаву широког кривотворења, професионално организованог пиратства и појављивања на све захтевнијем светском тржишту чипова познатог али не и оригиналног порекла.

Када је реч о објекту заштите врло брзо се, мада не без проблема, дошло до закључка да би то морао бити тродимензионални облик слојева од којих је полупроводнички производ (чип)⁴⁵ начињен или, како смо то у наслову навели, топографија интегрисаних кола.

У погледу облика заштите међутим није све ишло тако лако. Прва топографија интегрисаних кола је регистрована и заштићена у Великој Британији још 1959. године и то као патент али се показало да овакав облик заштите као и заштита осталим правима интелектуалне својине не могу бити потпуни правни оквир у којем се интегрисана кола могу штитити. Проблем је постао посебно актуелан у САД, држави која је била и данас јесте светски лидер у производњи силиконских чипова. Као резултат ангажовања и лобирања домаће „силиконске индустрије“ у САД је 1984. године донет

⁴⁵ Појам чип означава уређај направљен превасходно од силикона који се користи за чување, извршавање или рад меморије компјутера или компјутерског програма. То је у суштини мали део полупроводничког материјала (силикона) који са слојевима сачињеним од пропусних и изолационих материјала чине микро-електронско коло укључујући бројне полупроводничке делове (транзисторе, диоде...).

Закон о заштити полупроводничког чипа⁴⁶ којим је предвиђена посебна, *sui generis* заштита интегрисаних кола. Овакав концепт заштите је касније прихваћен у безмало свим националним законодавствима али и у међународним актима. При томе *sui generis* заштита не искључује могућност заштите правима интелектуалне својине и правом нелојалне конкуренције као супсидијарним односно допунским формама заштите.

Закон САД о заштити полупроводничког чипа извршио је приметан утицај и на садржај Директиве Савета ЕЗ о правној заштити топографије полупроводничких производа⁴⁷ из 1987. године. Према Директиви под топографијом интегрисаних кола се подразумева тродимензионални облик слојева од којих је полупроводнички производ начињен. Топографија ће моћи да ужива правну заштиту ако је оригинална односно ако је резултат ауторових интелектуалних напора и ако није општепозната у компјутерској индустрији. Ексклузивна права која се Директивом гарантују су право на репродукцију, право на комерцијалну експлоатацију и право на одређену сврху коришћења. Сама заштита траје 10 година, а рок почиње да тече од дана покретања поступка заштите. Сва права припадају творцу с тим што је земљама чланицама остављено да одреде власништво послодавца ако је топографија настала на послу.

Од садржине заштите која је као таква уграђена у претходно поменути закон САД и Директиву ЕУ битно не одступају и остала два важна међународна акта у овој области: Споразум о заштити интелектуалне својине у вези са интегрисаним колима (тзв. Вашингтонски споразум) из 1986. године и Споразум о трговинским аспектима права интелектуалне својине из 1995. године.

⁴⁶ Semiconductor Chip Protection Act / Chip Act.

⁴⁷ Council Directive on the Legal Protection of Topographies of Semiconductor Products (87/54/EEC).

2. Заштита топографије интегрисаних кола у нашем праву

Доношењем Закона о заштити топографија интегрисаних кола⁴⁸ Србија је хармонизовала своје законодавство са међународним стандардима у овој области прописаним од стране Светске трговинске организације и Европске уније. Циљеви који се Законом желе остварити су подстицање развоја домаћих топографија интегрисаних кола пружањем искључивих права њиховим ствараоцима и стављањем на располагање одговарајућих правних средстава за заштиту ових права од неовлашћеног коришћења. Истовремено, адекватна и са међународним нормама усклађена заштита је предуслов за трансфер и примену страних интегрисаних кола на територији Србије. Оба ова циља су у функцији подстицања технолошког и економског напретка земље.

Закон о топографијама интегрисаних кола Србије уређује предмет, услове и субјекте заштите топографија интегрисаних кола, права субјеката и начин њиховог остваривања, права привредног друштва или другог правног лица у коме је топографија настала као и ограничења у вези заштите топографија интегрисаних кола. Према Закону топографија је на било који начин приказан тродимензионални распоред елемената, од којих је најмање један активан, и међувеза у интегрисаном колу, или такав тродимензионални распоред припремљен за производњу одређеног интегрисаног кола. При томе је интегрисано коло у смислу Закона готов производ или међупроизвод у коме се остварује одређена електронска функција и у коме су елементи, од којих је најмање један активан, и међувезе интегрално формирану у комаду материјала или на комаду материјала односно и у комаду и на комаду материјала. Законом се дакле не штити технологија која се користи у производњи топографије или интегрисаног кола, информације које се чувају у интегрисаном колу, идеје, поступци, процеси, системи, методи рада, концепти, принципи или открића, без обзира на који су начин описани или објашњени.

Може се дакле штитити само топографија која је резултат интелектуалног напора ствараоца и која у време свог настанка није била

⁴⁸ Службени гласник РС 104/09.

општепозната међу ствараоцима топографија и произвођачима интегрисаних кола. Топографије које се састоје од комбинација елемената и међувеза које су општепознате биће заштићене само ако, посматрано у целини, испуњавају услове прописане за заштиту топографија који су претходно наведени. Приметно је да је из ове дефиниције изостављена карактеристика материјала од којег се данас израђују интегрисана кола, тј. полупроводник, а то је учињено да се не би непотребно сужавао обим заштите, јер се с обзиром на брзи развој технологије може очекивати појава материјала који ће заменити полупроводнике.

Да би топографија интегрисаног кола могла бити заштићена потребно је да је комерцијално употребљена, или да није старија од 15 година уколико никада није комерцијално употребљена.

Услов комерцијалне употребе је опште прихваћен у упоредном праву. Под комерцијалном употребом топографије сматра се било каква дистрибуција топографије или интегрисаног кола у коме је топографија садржана, било независно или као део другог производа, за комерцијалне, а не приватне сврхе. Имајући у виду да топографије које нису комерцијално употребљене могу бити од значаја за нове будуће технологије, предвиђена је могућност њихове заштите под условом да није прошло више од 15 година од датума њиховог настанка. Сличну одредбу има већина закона из ове области у свету.

Глава III

ЗАШТИТА ОД КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

1. Опште напомене о заштити од компјутерског криминалитета

Компјутерски криминалитет је више мање стар колико и први компјутери. Обзиром на своју репутацију „пионира“ у области развоја и употребе компјутерске технологије не чуди да су САД земља у којој се још 1958. године бележе први судски спорови који за предмет имају злоупотребу рачунара. Међутим, тек од средине 80-их година прошлога века компјутерски криминалитет почиње да се шири геометријском прогресијом и постаје планетарна појава која забрињава све кориснике рачунара: почев од највиших представника власти најмоћнијих држава на свету па све до „обичних“, анонимних корисника ове технологије. Према неким показатељима 2006. године је укупна штета учињена кроз дела компјутерског криминала износила преко 200 милијарди еура.

Шта то уопште угрожава информационе системе ?

Могло би се начелно рећи да постоје два типа опасности, типична разуме се и за све остале објекте заштите од криминалитета: то су људи и њихово понашање са једне и опасности које настају као тзв. виша сила (*vis maior*), са друге стране. Први тип опасности везује се за човекову намеру или непажњу, а други за околности које настају независно од воље човека.

Последице које настају дејством првог типа опасности углавном се могу свести на пет врста типичних претњи за сигурност система. То су:

1. разни облици „упада“ који се манифестују као престанак рада система, бескорисност или неупотребљивост одређене компоненте или целог система на дуже или краће време. Такви се упади појављују као крађе, хакинг, пословна шпијунажа и слично;

2. „пресретања“, која значе да је неки неауторизован субјект дошао до података, софтвера или хардвера или чак до целог система са циљем да онемогући рад, проузрокује штету и прибави материјалну корист;
3. разни облици неовлашћеног мењања и модификовања неке од компоненти система или целог система од стране неауторизованих лица. Тако се рецимо као облици модификовања софтвера појављују логичке бомбе, тројански коњ и слични програми који се убацују у постојеће мењајући их при томе;
4. разни облици „фабриковања“ лажних објеката система је особито честа појава у мрежама или базама података у којима се формирају нови записи на основу лажних података или само додају такви подаци већ постојећим како би се створила лажна слика о некој појави, рецимо успешном пословању неке фирме;
5. разни облици неконтролисаног отицања и губљења података, програма или микрочипова, што се најчешће појављује као последица немарности, грешака или пропуста запослених, мада није искључено да то може бити чињено и са намером.

Други тип опасности који смо претходно поменули односи се на оне опасности које су последица више силе. Овде је реч о ризицима који се најчешће покривају осигурањем на начин како се то чини и са осталим објектима заштите. Отуда о њима и нећемо посебно говорити.⁴⁹

2. Појам и обележја компјутерског криминалитета

Несумљиво је да компјутерски криминалитет (интернет криминал, Сајбер криминал, е-криминал, мрежни криминал, криминал високих технологија...) у себи апсорбује сва општа обележја криминалитета али да је у исто време реч и о прилично специфичној области у којој важе и одређена посебна правила, нетипична за „класична“ кривична дела. Отуда је на самом почетку неопходно одредити појам компјутерског криминала. Од више

⁴⁹ Дракулић М, наведено дело, стр.406-409.

дефиниција које се могу срести у нашој и упоредно правној литератури⁵⁰ чини се да је најпримеренија она сходно којој се компјутерски криминалитет одређује као вршење кривичних дела код којих се рачунар и компјутерска технологија појављују као оруђе за чињење одређених дела или као објект заштите. Изнета дефиниција указује на одређене опште али и посебне елементе односно специфичности компјутерског криминалитета:

прво, акти компјутерског криминала су акти човека, а не машине и то акти који представљају противправно, неетичко или неауторизовано поступање које је пре свега усмерено на аутоматску обраду података и/или њихов пренос. Да би такво поступање било третирано као кривично дело оно би најпре морало бити предвиђено у закону као кривично дело, што се дуго времена у назад појављивало као велики проблем. Као и сва друга кривична дела и дела компјутерског криминала представљају друштвено опасна дела;

друго, предуслов за постојање компјутерских кривичних дела је постојање рачунара односно, у ширем смислу, знања везаних за компјутерске технологије. Компјутери при томе могу имати четвороструку улогу: 1) улогу објекта, када су криминалне активности усмерене на уништење самих компјутера, података или програма као и уређаја који им омогућавају рад; 2) улогу „субјекта“, када се компјутер појављује као одредиште или окружење криминала, извор или повод за коришћење јединствених форми и врста напада на имовину; 3) улогу инструмента, где се компјутер користи као оруђе или инструмент за вршење дела; 4) улогу симбола, где се компјутер користи за застрашивање или обмањивање;

треће, посебно значајно за компјутерски криминалитет је питање његовог откривања и вођења кривичног поступка против учioniоца тих дела. Наиме, отежано откривање је најчешће последица велике способности прерушавања, скривености трагова, невидљивости доказа, тешкоћа у дешифровању доказа, лаког брисања доказа, великог броја података, неискуства истражитеља и слично;

⁵⁰ Једна од тих дефиниција је и она коју у приручнику о компјутерском криминалу наводи Америчко министарство правде (*U.S. Department of Justice*). Према њој под компјутерским криминалом се подразумевају било које повреде кривичног закона које обухватају познавање компјутерских технологија за њихово извршење, истрагу или кривично гоњење.

четврто, компјутерски криминалитет не зна за границе и то на сасвим особен начин, квалитативно другачији од других појавних облика кривичних дела за која се такође може рећи да им границе нису препрека. Наиме, радња извршења неког компјутерског кривичног дела може бити предузета на једном, а штетне последице могу наступити на другом крају света. Отуда је и истрага ових кривичних дела веома отежана и захтева не само висок степен сарадње међу државама већ исто тако висок степен познавања свих форми односно техничких и технолошких могућности вршења оваквих дела. Посебно су у овом смислу значајне препоруке садржане у Конвенцији Савета Европе о високотехнолошком криминалитету које се односе на питања екстрадиције, међусобне помоћи, именовања посебног органа у свакој држави који ће се бавити овом проблематиком као и одређивање места за контакте, тзв. мреже 24/7, која ће у смислу неопходних међудржавних контаката и сарадње бити у функцији 24 сата 7 дана недељно.

3. Компјутерска кривична дела

Мада смо претходно одредили појам и особености компјутерског криминалитета то, само по себи, није довољно и за одређење појма компјутерских кривичних дела. У овом погледу постоје у упоредној правној литератури углавном два приступа.

Према првом од њих под компјутерским кривичним делима се подразумевају сва она дела која имају својства особена овој појави. На овој основи се о компјутерским кривичним делима говори као о делима у којима компјутери имају „активну“ улогу или се у њима појављују као периферни објекти криминала. Овакав је приступ рецимо заступљен у раније помињаном приручнику Америчког министарства правде о компјутерском криминалу сходно којем се сва компјутерска кривична дела деле у три категорије: а) дела у којима су компјутери (хардвери, софтвери, периферни објекти везани за компјутере) објекти напада и где се радња извршења састоји у незаконитом стицању тих предмета; б) дела у којима су рачунари предмет односно „жртва“ криминала и где се радња извршења састоји од напада на рачунар, рачунарски систем, његовог уништења или ометања; в) дела у којима су рачунари и сродни системи средства којима се чине „обична“ кривична дела као што су крађа идентитета, новца или дистрибуција дечије порнографије.

Други приступ полази од метода таксативног набрајања (енумерације) оних кривичних дела која се сматрају компјутерским кривичним делима. Може се рећи да је овакав приступ у највећем делу својствен међународним и националним прописима који се баве материјом компјутерског криминалитета. На овој методолошкој основи, а полазећи од последица које настају њиховим извршењем, неки аутори говоре о компјутерским кривичним делима везаним за економски криминал (превара, крађа, компјутерска шпијунажа и саботажа, неауторизован приступ системима и хакинг, пиратство софтвера...), компјутерским кривичним делима везаним за кршење права приватности (коришћење нетачних података, илегално прикупљање и чување података, илегално откривање и злоупотреба података...) и компјутерским кривичним делима којима се угрожавају остали заштићени објекти (угрожавање националне сигурности, контрола прекограничног тока података, интегритет процедура везаних за компјутере и мреже података...).

Према Конвенцији Савета Европе о високотехнолошком криминалитету из 2001. године сва кривична дела су разврстана у четири одељка. У првом одељку третирана су кривична дела против поверљивости, интегритета и доступности компјутерских података и система у која спадају недозвољен приступ, недозвољено пресретање, ометање података, ометање система и злоупотреба уређаја. (чланови 2 до 6 Конвенције). У другом одељку говори се о кривичним делима у вези са компјутерима и то фалсификовању које је у вези са компјутерима и преварама које су у вези са компјутерима (чланови 7 и 8). Одељак три за предмет има кривична дела у односу на њихов садржај и то кривична дела везана за дечију порнографију (члан 9), а одељак четири кривична дела која се односе на кршење ауторских и њима сродних права (члан 10).

Разуме се, таксативно набрајање компјутерских кривичних дела има своје добре али и лоше стране. Лоша страна је то што се, обзиром на непредвидљив развој софтверске индустрије, могу у будућности очекивати нека „нова“ компјутерска дела, она која као таква нису предвиђена позитивним кривичним законодавством. У исто време општи постулат кривичног права изражен у латинској сентенци „*Nulum crimen nula poena sine lege*“ забрањује кривично гоњење и кажњавање за дело које као кривично није утврђено законом или другим прописом. Отуда би постојао императив да се нови појавни облици компјутерских кривичних дела, они који нису експлицитно нормирани у кривичном законодавству, „подведу“ и третирају

сходно аналогiji са сличним кривичним делима, без обзира да ли су та „слична“ кривична дела из корпуса компјутерских или „класичних“ кривичних дела.

У сваком случају се као типична кривична дела компјутерског криминалитета у ужем смислу, она која су извршена помоћу и/или против рачунара појављују:

- а) прављење и убацивање компјутерских вируса;
- б) хакинг;
- в) пиратство (софтвера, микрочипова, база података);
- г) компјутерске саботаже и шпијунаже;
- д) компјутерске преваре;
- ж) крађа компјутерских услуга.

3.1. Прављење и убацивање компјутерских вируса

Према неким изворима компјутерски вируси своје прапочетке имају у компјутерској игрици названој *Core War* (језгро рата, срце рата) коју су створила три млада програмера америчке телефонске компаније AT&T Bell негде 60-их година прошлога века. Ова игра је замишљена као сет репродуктивних програма названих „организми“ где сваки играч ослобађа свој „организам“ у меморији који покушава да уништи „организам“ противника.

Сам назив „вирус“ као назив компјутерског програма употребљен је међутим први пут у литератури. Једни сматрају да је реч о делу Дејвида Герлода (*David Gerrold*) „Када је Хари био неко“ из 1972. године, а други о роману Џона Брунера (*John Brunner*) из 1975. године „*Shockwave rider*.“ Но са вирусима као стварним компјутерским програмима се почиње по први пут експериментисати почетком 80-их година прошлога века у САД. Легендаран је постао један од првих програма који се појавио на факултетском рачунару у Калифорнији, а који је у одређено време производио на екранима мале квадратиће способне да бришу текст од горе на доле, ред за редом, остављајући поруку: *Cookie, cookie, give me the cookie*. Ако се тражена реч

(cookie) не би брзо укуцала садржај текста би био неповратно изгубљен, уколико би пак реакција била брза и тачна, текст се враћао.

Јануара 1986. године у свет је кренуо и први вирус који је прешао неколико граница и произвео велике проблеме популацији *IBM PC* корисника. Он се брзо ширио од земље до земље кроз Европу и прешао у Северну Америку. Кренуо је из Пакистана и за мање од 12 месеци заразио око пола милиона компјутера. Овај је вирус назван *Pakistani Brain* и први је који је изазвао глобалну пажњу светске јавности.

Већина првих вируса настала је дакле на факултетима, писали су их професори и/или студенти и у почетку су имали само академски значај. Изузетно брзо ширење компјутерске технологије и компјутерске писмености производе могућност да компјутерски високообразовани људи широм планете вирусе праве и употребљавају не само у академске сврхе.

Након претходно реченог потребно је и одредити појам компјутерског вируса. Могли би рећи да су компјутерски вируси посебан тип рачунарских програма који могу сами себе репродуковати и/или клонирати, који се шире и то трајно, са циљем да инфицирају друге програме како би они извршавали задатке које је унапред поставио творац вируса, а да при томе у неким случајевима инфицирани програми не изгледају тако.

Дакле, компјутерски вирус је:

- а) програм који је у стању да сам себе репродукује или клонира;
- б) програм који себе копира у друге програме;
- в) програм који се шири тајно, мада су последице његовог ширења видљиве;
- г) програм чији је циљ измена других програма како је то замислио творац;
- д) програм који инфицирајући други програм чини да он, на први поглед, не изгледа другачије од нормалног, неинфицираног програма;
- е) програм који најчешће прави штету на рачунару корисника.⁵¹

⁵¹ Наведено према: Дракулић М, наведено дело, стр. 439.

3.1.1. Типови и врсте компјутерских вируса

Компјутерских програма који имају карактеристике вируса, оне о којима је претходно било речи, има више врста и могу се класификовати по различитим критеријумима. Најзначајније врсте таквих програма су:

а) бактерије су програми који се при извршавању шире ка другим корисницима и системима слањем сопствених копија, а „хране“ се једући процесор и меморијске капацитете свог домаћина;

б) логичке и временске бомбе су програми који се активирају при испуњењу раније дефинисаних услова;

в) црви су програми који су најчешће орјентисани на путовање у мрежама, шире се копирајући сами себе, најчешће не мењају програме домаћина али се могу употребити у сврху блокирања система домаћина;

г) тројански коњ је програм који се труди да преко привилегованог корисника успостави контролу над оперативним системом;

д) зец је програм дизајниран да испразни ресурсе система премештајући се по њима без икаквог ограничења;

е) *trapdoor* или *back door* је део програмског кода чијим коришћењем онај ко ради на рачунару може доћи до оперативног система. Тамо корисник може формирати нови програм или користити нове наредбе или их преправити у своју корист.

Творци вируса су данас лица, углавном мушкарци, која имају сопствену мотивацију. Неки од њих вирусе стварају и дистрибуирају забаве ради, а неки опет са злом намером и ради остварења неких циљева који опет могу бити различити: од „осветничких“ па до економских. Многе вирусе данас стварају и произвођачи софтвера не би ли се на тај начин заштитили од пиратства. Но без обзира на мотивацију твораца да би вирусни програм радио неопходно је да се „усели“ у рачунар домаћина. Он то може учинити тако што ће направити шкољку око оригиналног програма и држати га затвореног док се не уради жељена операција. Може се такође десити да се вирусни програм „залепи“ за крај оригиналног кода и да се потом пребаци на почетак мењајући податке о старту и извршавајући своје операције пре програма домаћина.

Зависно од компоненти које садрже вируси имају три фазе у свом раду. Прва фаза је активација, што практично значи да је услов њиховог ширења то да најпре буду активирани. Друга фаза је репликација, што значи да се вирус шири, мултипликује и инфицира програме домаћина. Коначно трећа фаза је фаза манипулације у којој вирус на одређени начин манипулише системом домаћина. Када ће вирус почети да функционише зависи од начина на који је смишљен његов старт. То може бити одређени датум, рецимо петак 13, постојање одређених фајлова у рачунару домаћину, појављивање одређеног садржаја на екрану, комбинација претходно изложених или других непоменутих начина иницијације.

Нема спора о томе да се број компјутерских вируса свакодневно повећава и да је све теже пронаћи ефективне и целовите мере заштите од њих. Ипак начелно се сматра да се заштита мора састојати из три дела. Она мора бити превентивна, она се мора испољавати у „лечењу“ последица до којих је дошло деловањем вируса и коначно она се мора састојати у кажњавању. Превенција и лечење су у домену техничких и организационих мера док је кажњавање твораца вируса у домену права.

3.2. Хакинг

3.2.1. Појава и историјски развој хакинга

Хакери се под тим називом појављују раних 60-их година прошлога века али не у смислу значења који углавном данас има употреба те речи. Ово је првобитно био назив за групе компјутерских заљубљеника и ентузијаста који су формирали клубове, размењивали информације, оснивали часописе, пратили све сајмове рачунара и најновија достигнућа технике у тој области па чак и имали своју сопствену Конвенцију о основним правилима понашања. Но већ крајем 60-их и почетком 70-их година 20. века двојица младих американаца, присталица анархистичког покрета, свој протест против рата у Вијетнаму су изражавали тако што су свој сопствени рат водили крађом телефонских услуга, а 1971. године чак су и покренули свој сопствени магазин. Само десетак година касније бележи се и хапшење групе младића између 12 и 22 године, познатих као Банда 414 (*414 Gang*) који су упадали у компјутерске системе више од 60 корпорацијских и владиних инсталација. Додуше, већина од тих система није имала одговарајуће обезбеђење, а за упад

су по правилу коришћени телефони и персонални рачунари који су били програмирани за аутоматско бирање бројева. Обзиром на велики публицитет који је овај догађај имао појам хакера дефинитивно добија негативне конотације и у будуће се по правилу употребљава за лица која користе компјутерске могућности за упаде у системе, крађу информација, компјутерских и телекомуникационих ресурса и ремећење рада других корисника. Хакери се почињу сматрати „електронским криминалцима“ па и „електронским вандалима“.

Тако је за хакинг 80-их карактеристично следеће:

а) провале, крађе и неовлашћени приступи бивају све разноврснији и сложенији;

б) фомирају се хакерске групе;

в) мишљење о хакерима поступно еволуира од дивљења ка забринутости и страху;

г) настаје проблем одређивања садржаја и појма хакерских активности заједно са проблемом детекције, истраге, хапшења, доказа...;

д) доносе се први прописи који регулишу ову појаву, развијају се нови системи заштите и сигурности али, са друге стране, веома брзо напредују и нови типови и дела хакинга.

Временом упади хакера постају све сензационалнији и опаснији. Многе хакерске групе постају у свету компјутера толико познате да су засениле славу свих осталих софтверских творца. Хакинг у 90-им годинама прошлога века тако карактерише и следеће:

а) упади хакера постају све више дела организованог криминала, економског и политичког тероризма;

б) хакерска субкултура бива угрожена економским и политичким притисцима, а државе се озбиљно почињу борити против њих;

в) интернационализује се и хармонизује сарадња на праћењу, откривању, гоњењу и кажњавању криваца.⁵²

3.2.2. Појам хакинга

У оригиналном односно изворном значењу термин „хакер“ се користио за означавање мајстора рачунарства, свакога онога ко је веома заинтересован да научи све о компјутерским системима и њиховом коришћењу па су многи компјутерски ентузијастички себе у том смислу и називали хакерима. Додуше, у хакерској субкултури прави се разлика између тзв. крекера (*craker*), који су истински познаваоци рачунарства и техника којима се компјутерски системи могу озбиљно угрозити и тзв. лејмера (*lamer*), „клинаца“ који користе вирусе и друге малициозне програме примарно ради забаве и „паметовања“.

Од времена уласка у употребу па до данас значење израза „хакер“ поступно еволуира. Оно што је несумњиво то је да се хакерима и данас не може оспорити да су „мајстори“ рачунарства, да поседују веома висок ниво знања и вештина у вези са рачунарима и њиховим коришћењем. Сврха употребе таквог знања и таквих вештина од стране хакера међутим у савремено доба утиче на то да се под појмом хакера и хакинга подразумева нешто сасвим друго.

Хакинг се данас може одредити као сваки неауторизовани, насилни приступ односно покушај приступа систему (компјутерском и/или комуникационом), а хакер је особа која има знање, способности и жељу да у потпуности неовлашћено користи туђе компјутерске и комуникационе системе.

Изнета дефиниција хакинга упућује на следеће његове битне карактеристике:

прво, хакинг је неауторизован и унапред припремљен приступ компјутерском и/или телекомуникационом систему;

⁵² Дракулић М, наведено дело, стр.446-447.

друго, то је насилан приступ (извршава се пробијањем заштите система) који се реализује упадом у систем, при чему се термин упад користи за означавање разних метода и техника проваљивања у систем;

треће, упади у систем базирају се на високом професионалном знању;

четврто, чињењем самог хакинга хакер по правилу у исто време чини и друга дела као што су шпијунаже, преваре, крађе, саботаже, убацивање вируса...;

пето, хакинг може чинити једна или група особа, при чему је све учесталија појава организованог хакинга од стране више извршилаца;

шесто, место провале је по правилу удаљено од места где се хакер налази;

седмо, када се једном нађе у систему хакер се понаша као ауторизовани корисник;

осмо, мотивација за чињење овог дела је различита (од наводне помоћи неправдом угроженим особама до тероризма), а многи случајеви имају широке размере и интернационализују се.⁵³

3.2.3. Типови хакинга

Критеријуми за поделу хакинга могу бити прилично разноврсни. Тако се према намери оних који се баве хакингом може говорити о добронамерном и малициозном хакингу, према циљу предузимања о хакингу чији је циљ читање, уништење, мењање, дистрибуирање, фабриковање података, остављање поруке, стартовање програма без дозволе, брисање или исправљање програма и података, према броју починилаца може се говорити о појединачном и групном хакингу, а према месту одакле је напад кренуо о екстерном и интерном хакингу. У литератури се највише пажње међутим посвећује подели хакинга на аматерски и професионални.

Аматерски хакинг је уобичајено дело младих људи који по правилу не желе да нанесу неку стварну штету, или бар то не чини намерно. Реч је о

⁵³ Дракулић М, наведено дело, стр.449-450.

компјутерским ентузијастама који сате проводе проучавајући системе обезбеђења покушавајући да их „дешифрују и разбију“. На тај начин они желе да демонстрирају своје компјутерске вештине и докажу се, сами себи али и својим истомишљеницима, пријатељима, колегама... Разуме се, и међу хакерима аматерима постоје вандала који упадима у туђе системе желе управо да некоме нанесу штету, да обришу неке податке или изврше саботажу неког система. Но начелно посматрано могло би се рећи да хакери аматери најчешће желе да испуне један од следећих циљева:

- а) да пронађу довољно изазован систем и поиграју се са њиме;
- б) да приступе систему и претраже га да би задовољили радозналост и доказали своја знања и способности;
- в) да пронађу неку нову, занимљиву игрицу у систему како би се играли;
- г) да униште или модификују податке, убаце вирусе и вирусолике програме или да оставе неку, најчешће шаловиту поруку.

Професионални хакинг врше лица којима је то стално занимање и извор прихода. Професионални хакери се не ретко удружују у политичке или субверзивне групе за оштећење и искривљавање информација, групе за индустријску шпијунажу које теже да се домогну вредних информација и да их скупо продају, тзв. спаситељске групе или групе за обављање било ког типичног криминалитета. За овај тип хакинга карактеристично је:

- а) да су напади брижљиво и дуготрајно припремани уз анализирање сопствених и искустава других хакера;
- б) да најчешће нападају исте или сличне врсте система;
- в) да хакинг обављају изузетно вешто и на најмање ризичан начин;
- г) да нападе чешће извршавају групе хакера које имају своју сопствену информативну мрежу ради међусобног обавештавања и размене искустава;
- д) да починиоци поседују високо техничко знање и добру мотивацију за то што раде обзиром да су „улози“ веома велики.

Професионални хакинг се све чешће појављује и као својеврсно упозорење на припрему различитих терористичких акција, политичких и пословних саботажа, нелојалне конкуренције, преваре... Такође, као што је претходно и речено, професионални хакинг све више поприма форму организованог криминала посебно у областима проституције, порнографије, растурања дроге и крадене робе, клађења, прања новца, зеленаштва, уцена... Тако професионални хакери оснивају и лажне фирме преко којих обављају своје недозвољене активности. Неке организоване групе професионалних хакера се чак и не прикривају већ се својом делатношћу хвале и поносе. За организовани професионални хакинг карактеристично је:

- а) да су то добро организоване и осмишљене групе;
- б) да су предвиђене да трају дуже време мада се могу појавити и као *ad hoc* групе;
- в) да имају изграђен систем сопствених норми и стандарда базиран на негацији посебних, а не ретко и општих друштвених вредности;
- г) да им је организација мање хијерархизована него код других облика организованог криминала обзиром да су знања и вештине припадника групе углавном уједначена;
- д) обављање хакинга представља само основу за вршење других криминалних активности;
- е) не ретко су повезани са овлашћеним корисницима, лицима из државне власти, политичарима.⁵⁴

На крају овог дела разматрања о типовима хакинга осврнућемо се и на гледиште америчке литературе у овом погледу. Према тзв. лексикону компјутерског подземља сва лица која врше нападе на компјутерске системе деле се у три групе. У прву улазе тзв. писмени клинци (*script kiddies*), у другу хакери (*hacker*) и у трећу крекери (*cracker*). Прва група лица чини најобимнији али у исто време и најбезазленији део напада на компјутерске системе. Они најчешће користе слабости у обезбеђењу неког система да би неовлашћено скидали одређене садржаје са интернета. Поседују ограничена

⁵⁴ Дракулић М, наведено дело, стр.451-455.

компјутерска знања, а највећи део причињених штета чине ненамерно.⁵⁵ Друга група нападача су хакери, лица са веома високим нивоом компјутерских знања и вештина који их чине способним да користе најсофистицираније компјутерске технике.⁵⁶ Крекери са друге стране такође поседује исти ниво компјутерских знања и вештина али је мотивација њихових напада на компјутерске системе другачија. За хакере је по правилу највећа награда сопствено задовољство услед „проваљивања“ неког безбедносног компјутерског система. Важна им је такође и тзв. војерска компонента која значи моћ имати приступ оним информацијама и садржајима којима приступ има само ограничен број других лица.⁵⁷ Из ових разлога деловање хакера и није, како се сматра, оно које суштински угрожава и наноси штету компанијама и институцијама као корисницима компјутерских технологија. Крекери су они који нападају компјутерске системе не из сопственог задовољства било које врсте већ искључиво и само ради стицања профита. То је њихов посао од кога живе и зарађују. У ову трећу групу компјутерских криминалаца убрајају се и сајбертерористи који, мада као и крекери мотивисани стицањем профита, у суштини остају терористи са свим оним мотивима које дела тероризма са собом носе.

3.2.4. Како хакери улазе у системе

Сваки улазак у туђи систем хакери припремају и планирају. Најпре се врши прикупљање обавештења и покушај упада. Претходна обавештавања о систему се најчешће састоје из следећих „акција“:

а) примене „опортунистичких“ техника као што су прислушкивање разговора запослених или корисника на свим могућим местима;

б) претраживања новина, публикација и библиотека;

в) претраживања поште, електронске и класичне, отпада и ђубрета;

⁵⁵ Richard Barber: Hackers Profiled – Who Are They and What Are Their Motivations ? – Computer Fraud & Sec. Feb. 2001, at. 14.

⁵⁶ Douglas Thomas: Hackers Culture, 43 – 44 (2002).

⁵⁷ Paul A Taylor: Hackers: Crime in Digital Sublime, 56 – 58 (1999).

в) лажног представљања, нпр. јављањем на конкурс, изигравањем заборавних корисника и слично;

г) заустављања односно пресретања комуникација, крађом, подмићивањем, изнуђивањем и искоришћавањем.

Када прикупе довољно информација о систему који желе да „нападну“ хакери покушавају да уђу у њега користећи се свим слабостима заштитног система. Технике које им стоје на располагању су разноврсне. Ако успеју да уђу у систем хакери покушавају да добију привилегије највишег нивоа како би могли да обаве посао због кога су у систем и ушли.

3.2.5. Откривање, истрага и превенција хакинга

Да би се хакинг могао открити неопходно је испуњење одређених претпоставки. То су пре свега постојање и коришћење софвера са програмом за добро „ухођење“, редовно надгледање системских улазака и праћење свих сигнала. Откривање је у сваком случају веома тешко и у доста случајева се своди само на констатацију о постојању „уљеза“ у систему. Из наведених разлога је и истрага изузетно отежана. Али не само то. Додатну тежину за успешну истрагу чини и то што су починиоци веома вешти, интелигентни и лукави, што постоји временска и просторна удаљеност између места и времена предузимања радње и места и времена наступања последице, што добар број жртава прикрива нападе необавештавајући о њима истражне органе и коначно што судски процеси, ако до њих дође, дуго трају.

Имајући у виду претходно речено јасно је колики значај у овој области имају мере превенције. Оне би морале бити такође техничке, организационе и правне. Ове прве тичу се добре софтверске заштите система, а ове друге се односе на организовање посебних одељења професионалаца који би се непосредно и на дневној бази бавили одржавањем сигурности компјутерских система, анализом ризика његове угрожености, контролом извора података из којих хакери могу црпити своја обавештења као и демотивацијом запослених у вези изношења информација о систему и његовим слабостима. Коначно, правне мере превенције се и овде могу односити како на генералну тако и на посебну превенцију, речју на успостављање таквог кривичног законодавства које ће својим одредбама одвраћати потенцијалне учиниоце од намере да се хакингом баве.

4. Остала типична компјутерска кривична дела

4.1. Компјутерска крађа

Компјутерска крађа заузима високо место у области компјутерског криминалитета, посебно када је реч о крађи идентитета. Ова врста крађе наине представља нарочито друштвено опасно дело обзиром да, поред осталог, доводи у питање поверење у интегритет и безбедност комерцијалних трансакција и угрожава приватност. Процене су да ће се компјутерске крађе временом увећавати имајући у виду снажан замах електронске трговине. Снабдевени персоналним информацијама неког лица крадљивци идентитета могу да отворе рачун у банкама, обављају куповину, а у одређеним земљама у којима су аутоматизоване и неке сервисне услуге за грађане могу да добију сертификат о рођењу, пасош, кредит и слично. Жртва у већини случајева и не зна да се њен идентитет користи све док рачуни не стигну на наплату. Мада један број експерата тврди да су потрошачи значајнијим ризицима изложени коришћењем кредитних картица у „реалним“ него у *on line* трговинама већина купаца има резерву према *on line* куповини управо због прикривене опасности од крађе њиховог идентитета.

4.2. Компјутерске преваре

Компјутерске преваре се врше у намери прибављања за себе или другог противправне имовинске користи, с тим што се код њих у заблуду не доводи или одржава неко лице, као у случају класичних превара, већ се та заблуда односи на компјутер у који се уносе нетачни подаци или се пропушта уношење тачних података, или се на било који други начин рачунар користи за остварење преваре. Сматра се да је ово најраширенији облик компјутерског криминалитета. Према подацима Националног центра за компјутерски криминал САД (*U.S. National Center for Computer Crime*) око 44 % свих компјутерских кривичних дела односи се на компјутерске преваре.

Број облика превара као и начин њихове реализације је практично неограничен и у пракси се сусрећу како оне врло примитивне и грубе тако и оне код којих учиниоци испољавају висок степен вештине. Али у сваком случају компјутерске преваре обзиром на природу интернета и других

средстава електронског комуницирања допиру веома далеко, одвијају се веома брзо и по правилу уз ниске трошкове извођења.

4.3. Компјутерске саботаже и тероризам

Компјутерске саботаже се у основи састоје у уништењу или оштећењу компјутера или других уређаја за обраду података у оквиру компјутерских система или брисању, мењању односно спречавању коришћења информација садржаних у меморији информатичких уређаја. Најчешћи видови компјутерске саботаже су они који делују деструктивно на оперативне информативне механизме и корисничке програме, пре свега оне који имају функцију чувања података.

Како терористи постају савременији тако и они све више као своје оружје користе компјутерске односно друге високе технологије. Када је конкретно реч о компјутерском тероризму реална је опасност да информатички ресурси, посебно глобалне мреже, све више буду коришћене од стране терориста. Још 1997. године овакав вид напада на пословне и владине компјутерске системе најавила је ИРА. И у последњој деценији много је примера где су терористи било у припреми или извршењу својих напада, од којих су неки однели и хиљаде људских жртава, користили компјутерске технологије.

4.4. Софтверска „пиратерија“

Под појмом „пиратерија“ данас се разуме читав низ недозвољених (криминалних) активности усмерених на кршење ауторских права или пак права индустријске својине. Те недозвољене активности се најчешће састоје у неовлашћеном коришћењу, репродуковању и умножавању правом заштићеног ауторског дела односно неовлашћеном коришћењу, репродуковању и умножавању неког од заштићених права индустријске својине.

Пиратерија разуме се није својствена само компјутерским програмима и софтверима. Управо супротно, тешко је пронаћи неку индустријску, уметничку или другу област у којој она није заступљена. Сматра се да се у већем обиму појављује најпре у музичкој и филмској индустрији, а потом

безмало у свим оним областима у којима је неовлашћено коришћење, кривотворење или употреба неких производа и услуга могло донети профит. У последњих неколико година међутим термин пиратерија се углавном везује за софтверску пиратерију. Разлози за то су многобројни, а чини се да су следећи посебно релевантни: прво, компјутерска индустрија данас представља високо пропульзивну и профитабилну индустрију чији су корисници стотине милиона људи широм света; друго, нека истраживања из 2008. године говоре о томе да сваки трећи рачунар на свету садржи пиратски или фалсификован софтвер те да су губици које такав облик пиратерије наноси легалним компанијама већи од 50 милијарди долара на годишњем нивоу; треће, не постоји област у којој се толико инвестира у борбу против пиратерије као што је то област компјутерских технологија и софтвера.

Поред високе профитабилности односно мањих трошкова набавке као основних мотива оних који производе и продају односно оних који купују пиратске софтвере на широко распрострањено коришћење нелегалних софтвера у свим крајевима и свим државама света утиче ван сваке сумње и мноштво појавних облика односно врста софтверске пиратерије. Најчешћи су:

а) пиратерија крајњег корисника, као неауторизовано репродуковање односно копирање софтвера од стране лица које је софтвер легално набавило. Овај облик софтверске пиратерије се испољава као коришћење једне лиценциране копије на више рачунара, као копирање дискова у сврху њиховог инсталирања и даље дистрибуције, као коришћење могућности надоградње без поседовања легалне копије верзије која се надограђује, као прибављање академског или другог софтвера који није за продају у комерцијалне сврхе, као замена дискова на радном месту и ван њега;

б) клијент – сервер преупотреба, који облик пиратерије се дешава када превише запослених на мрежи користи централну копију програма у исто време. Реч је дакле о постојању неке локалне мреже где инсталиране програме може да користи највише онолико људи колико је то лиценцом одређено па сваки корисник ван тог лиценцом дозвољеног броја корисника заправо нелегално користи инсталирани програм;

в) интернет пиратерија, као преузимање софтвера са интернета и то кроз пиратске сајтове који нуде софтвер за бесплатно преузимање, кроз

интернет аукције на којима се нуди фалсификовани софтвер или кроз тзв. *peer to peer* мреже које дозвољавају неауторизовану размену софтвера;

г) снимање на хард диск, као илегално копирање софтвера на хард диск од стране компанија које се баве продајом рачунара како би своју понуду рачунара учиниле што атрактивнијом;

д) фалсификовање софтвера, као илегално дуплирање и продаја ауторизованог материјала са намером да се директно имитира заштићени производ.

Борба против софтверске пиратерије је опсежна и одвија се на неколико нивоа почев од техничког, правног па све до политичког. Технички ниво заштите се у овом делу није показао ефикасним из разлога што управо даљи технолошки напредак олакшава широком кругу лица бављење софтверском пиратеријом. На пољу правне заштите релевантни су сви они правни акти о којима је већ било речи у излагањима о правној заштити компјутерских програма и софтвера. У овом погледу софтверске компаније којима је пиратством повређено ауторско право имају на располагању мере грађанско правне и кривично правне заштите. Додуше, код нас и у упоредном кривичном законодавству не постоји посебно кривично дело под називом пиратерија софтвера већ се најчешће говори о делу неовлашћеног искоришћавања ауторског дела или предмета сродног права. Огромни губици које компаније из технолошко најразвијенијих земаља трпе на тржиштима на којима се бележи изузетно висок ниво софтверске пиратерије мотивисали су и владе таквих држава да овај проблем подигну на политички ниво. Тако је софтверска пиратерија не ретко предмет озбиљних политичких дискусија између највиших политичких представника власти. У овом погледу опште познат је политички притисак САД на владу Кине у смислу поопштравања борбе против софтверске пиратерије.

Коначно, огромни проблеми у откривању и санкционисању софтверске пиратерије, посебно међу кућним корисницима рачунара, мотивисали су и највеће светске компаније, као што је ван сваке сумње *Microsoft*, да се укључе у акцију борбе против овог вида компјутерског криминала. Компанија *Microsoft* је не само иницијатор тзв. Светског дана борбе против пиратерије већ константно ради на програмима сарадње са владама широм света, привредним коморама и партнерским компанијама

чији су циљеви подизање свести о значају заштите права интелектуалне својине као и едукација најшире јавности и надлежних државних служби о штетним ефектима које проузрокује софтверска и други видови пиратерије.

5. Правне мере заштите од компјутерског криминалитета

Дуги низ година правне мере заштите су несумљиво биле најслабија карика у ланцу заштите компјутерских система од деловања компјутерског криминала. Данас је ситуација квалитативно другачија. Наиме данас су ретке земље које на неки начин својим прописима не регулишу сва важна питања компјутерског криминалитета. И не само то. Многе од њих имају посебна тела која се овом проблематиком баве као својом основном делатношћу. На овом месту биће нешто више речи о правним мерама заштите у упоредном законодавству, на међународном нивоу и у нашој држави.

5.1. Правне мере заштите у националним прописима

У настојању да се обезбеде адекватне правне мере заштите од вируса, хакинга као и свих других дела која у својој основи имају компјутерски криминалитет размишљало се о три могућа решења. Према првом, било би неопходно обезбедити да већ постојећи прописи, кроз њихово евентуално модификовање и доградњу, „покрију“ сва кривична дела која се третирају као дела компјутерског криминалитета. Друго решење је опет базирано на потреби доношења посебних, *sui generis* прописа док се треће заснива на комбиновању прва два методолошка приступа.

На примеру САД и Немачке видећемо какав приступ су те државе имале у свом настојању да сопствене правне системе учине ефикасним у борби против компјутерских кривичних дела односно њихових починилаца.

У САД је још 1986. године Конгрес усвојио два закона и то Закон о компјутерској превари и злоупотреби (*Computer Fraud and Abuse Act*) и Закон о приватности електронских комуникација (*Electronic Communications Privacy Act*). На основу тих аката сваки покушај неовлашћеног мењања података на компјутерима друге државе сматра се федералним прекршајем. Прислушкивање електронске поште и електронска пљачка (пресретање

електронског трансфера новца) такође је кажњиво. Прво дело је кажњиво до 5, а друго до 10 година затвора. Осим тога предвиђена је и казна затвора до 20 година за приступ информацијама чије неауторизовано откривање представља опасност по националне интересе, одбрану земље рецимо. Оба претходно наведена закона за нека дела предвиђају и новчане казне. Они су федералног карактера што практично значи да важе само ако извршено дело на неки начин „пређе“ границу макар једне од федералних држава. Ово такође значи да су федералне државе власне да у овој области доносе посебне законе. Оне то и чине било тако што, баш као и на федералном нивоу, доносе посебне законе или иновирају своје кривично законодавство тако што у њему прописују посебна кривична дела која се односе на компјутерски криминалитет.

Према Енциклопедији сајбер криминала наводи се да амерички Федерални истражни биро (*FBI*) и Национални комитет за криминал белих крагни (*National White Collar Crime Center*) откривају и прате следеће облике компјутерског криминалитета: упаде у компјутерске мреже, индустријску шпијунажу, софтверску пиратерију, дечију порнографију, „бомбардовање“ електронском поштом, „њушкање“ пасворда, „прерушавање“ једног рачунара да електронски личи на други како би се могло приступити систему који је под рестрикцијама, крађу кредитних картица. У зависности од типа почињених дела сајбер криминал може бити политички (сајбер шпијунажа, хакинг, сајбер саботажа, сајбер тероризам и сајбер ратовање), економски (преваре, хакинг, крађа интернет услуга и времена, пиратство софтвера, микрочипова и база података, индустријска шпијунажа, преварне интернет аукције), производња и дистрибуција недозвољених и штетних садржаја (дечија порнографија, педофилија, верске секте, ширење расистичких ставова, злоупотреба жена и деце, трговина дрогом, људским органима и оружјем) и повреде приватности (надгледање електронске поште, спам, прислушкивање, праћење електронских конференција...).

Немачка своју борбу са употребом нових технологија у служби вршења кривичних дела решава иновирањем свог кривичног законодавства. Још 1935. године развија се тзв. машинско кривично право у оквиру кога се препознају као кривична дело илегално телефонирање, а нешто касније (почев од 1969. године) и дело фалсификовања техничких записа. Фаза тзв. раног компјутерског права у овој држави почиње 1986. године када је усвојен посебан Кривични закон за сузбијање привредног криминалитета који

обухвата између осталог дела неовлашћеног увида у податке односно крађу података од стране хакера или штетних програма, кривотворење података који су битни као докази, измену података, компјутерску саботажу и компјутерску превару. Коначно, посебна фаза у прилагођавању кривичног права ове државе употреби савремених технологија у вршењу кривичних дела везује се за 2007. годину. Те године се наиме, поред већ постојећих, као кривично одређује и дело неовлашћеног увида у туђе податке као свршени облик кривичног дела, затим дело пресретања података и припреме неовлашћеног увида и пресретања података („хакерски параграф“), а дело компјутерске саботаже сада обухвата и приватне системе „од битног значаја“.

У већини других европских држава кривично правна заштита од дела компјутерског криминалитета обезбеђена је иновирањем одредаба постојећих кривичних закона. Ту и тамо неке државе доносе посебне законе у овој области. То је рецимо случај са Великом Британијом где је 1990. године усвојен Закон о злоупотреби компјутера. У овој држави је такође образовано посебно одељење за борбу против високотехнолошког криминала (*National High Tech Crime Unit / NHTCU*), као уосталом и у великом броју других држава.

5.2. Компјутерски криминалитет и међународноправна заштита

Почетак међународних активности у борби против компјутерског криминала везује се за 1983. годину када је у оквиру ОЕЦД основан посебан комитет са задатком да припреми студију о могућностима интернационализације и хармонизације кривичног права у вези са компјутерским криминалитетом и злоупотребама. Од тада па надаље међународне активности су биле и још увек јесу бројне и разноврсне и одвијају се у оквирима различитих међународних организација и форума.

Чини се да су најзначајнији и најбројнији међународни акти донети у оквиру ЕУ. Тако је рецимо 1998. године под вођством Урлиха Сајбера (*Ullrich Sieber*) са Универзитета у Вирзбургу (*Wurzburg*) израђена посебна студија о правним аспектима компјутерског криминала у информатичком друштву (*Legal Aspects of Computer related Crime in the information Society . COMCRIME study*) која је обухватала и основе сајбер криминала, као вишег облика. Овај акт, у комбинацији са документима усвојеним на Лисабонском

састанку Европског Савета из 2000. године, представљао је смернице за даље активности ЕУ на овом плану. 2000. године је донета и Директива о електронском пословању (*Directive on Electronic Commerce*) у којој се посебна пажња посвећује проблему злоупотреба. Исте године у оквиру ЕУ се доносе Одлука о спречавању дечије порнографије на интернету и Препоруке о стратегији за нови миленијум у заштити и контроли компјутерског криминала.

Савет Европе је крајем 1998. године објавио почетак рада на доношењу Конвенције о сајбер криминалу која је након усвајања, 2001. године, постала један од најзначајнијих међународних докумената на овом плану и као таква прихваћена не само у земљама ЕУ већ и у Јапану, САД, Канади, Јужној Африци и бројним другим државама. Предметна Конвенција је потписана али још увек не и ратификована од стране наше државе.

Бројне активности у борби против компјутерског криминала бележе се у оквиру УН, Међународне организације за заштиту права интелектуалне својине, Међународне привредне коморе, Светске трговачке организације, Азијско пацифичке организације за економску сарадњу...

Тако је 2000. године на десетом Конгресу УН посвећеном превенцији од криминала и третману починилаца у документу под називом Криминал везан за компјутерске мреже (*Crime related to computer network*) прихваћено становиште према којем се под овим криминалом подразумева криминал који се односи на било који облик кривичних дела која се могу извршити коришћењем компјутерских система и мрежа, у компјутерским системима и мрежама и против компјутерских система и мрежа. Ово наравно не значи да компјутерском криминалу и знатно раније није „признато“ својство криминала, да он као такав није третиран на различите начине у документима многих међународних организација, али свакако значи да је од појаве првих облика ових кривичних дела па до неопходне и свеобухватне међудржавне сарадње у овој области „потрошено“ безмало пуне две деценије.

Бројна међународна документа на различите начине одређује компјутерски криминал и његове врсте. Тако се у претходно поменутом документу УН (Криминал везан за компјутерске мреже) говори о компјутерском криминалу у ужем смислу, који се дефинише као свако незаконито понашање усмерено на сигурност електронских операција,

компјутерских система и података који се у њима обрађују, и компјутерском криминалу у ширем смислу под којим се подразумева свако незаконито понашање у односу на компјутерски систем и/или мрежу укључујући и такав криминал какав је незаконито поседовање, нуђење и дистрибуирање информација преко компјутерских система и мрежа.

У истом се документу наводе и конкретни облици овог криминалитета и то у складу са Препоруком Савета Европе и листом ОЕЦД (*OECD*) из 1989. односно 1985. године. То су: 1) неауторизован приступ компјутерском систему или мрежи кршењем мера сигурности (хакинг); 2) оштећење компјутерских података и/или програма; 3) компјутерске саботаже; 4) неовлашћено пресретање комуникација од и у компјутерским системима и мрежама; 5) компјутерска шпијунажа.

Сваки од наведених облика може се „укрштати“ са сваким па готово и да не постоји неки чисти облик дела. Тако хакинг у овом контексту обухвата, поред неовлашћеног уласка у компјутерске системе и мреже, и уништење података као и компјутерску шпијунажу. Измена компјутерских података и програма подразумева и „лансирање“ компјутерских црва и вируса.

Од дела компјутерског криминала у ширем смислу најчешће се појављују компјутерски фалсификати, крађе, техничке манипулације уређајима и/или електронским компонентама уређаја, злоупотребе система плаћања као што су манипулације и крађе електронских кредитних картица или коришћење лажних шифри у незаконитим финансијским активностима. Делима компјутерског криминала у ширем смислу додају се у последње време и дела подржана рачунарима која обухватају „растурање“ или само поседовање забрањених односно незаконитих садржаја при чему се мрежа користи за постизање бољих резултата и покушај избегавања казне. У ова дела се тако убрајају кршење ауторских и сродних права, продаја забрањене робе, пружање недозвољених услуга (коцка, проституција...), порнографија...

Европска конвенција о компјутерском криминалу из 2001. године предвиђа 4 групе компјутерских кривичних дела. То су дела против поверљивости, интегритета и доступности компјутерских података и система (незаконит приступ, пресретање, уплитање у податке и/или системе, коришћење уређаја, програма, пасворда...), дела везана за компјутере (фалсификовање и крађе), дела везана за садржаје (дечија порнографија) и

дела везана за кршење ауторских и сродних права (репродуковање и дистрибуција). Напомињемо да Конвенција под појмом компјутерског система подразумева и компјутерске мреже.

На пољу међународноправне заштите и борбе против компјутерског криминала појавио се међутим у већој мери него код других облика међународног криминалитета још један проблем. Он се односи на одговарајуће процедуре и поступке, укључујући и одговарајуће органе, који би требало да правосудним и истражним органима олакшају посао у вези прикупљања неопходних информација везаних за сама дела и њихове учиниоце. У том смислу ЕУ је 2000. године донела Конвенцију о међусобној помоћи у криминалној материји (*Convention on Mutual Assistance in Criminal Matters*) којом се предвиђа не само сарадња већ и усклађивање правних и правосудних система земаља чланица. У оквиру претходно поменуте *COMCRIME* студије предвиђено је такође формирање посебних јединица полиције на националним нивоима, успостављање сарадње између правосудних органа, индустрије, организација потрошача и тела за заштиту података као и „охрабривање“ производње специјализованих производа који служе за повећање сигурности компјутерских система и мрежа.

Највише се очекује од формирања специјализованих јединица за откривање, праћење и хватање компјутерских криминалаца и успостављања „врућих линија“ између великог броја земаља.

5.3. Правна заштита од компјутерског криминалитета у нашем праву

Правна заштита од компјутерског криминалитета је у Републици Србији у складу са најсавременијим светским решењима. Предмет законске регулативе су не само посебна кривична дела против безбедности рачунарских података већ и одговарајуће процедуре односно посебни државни органи који у овом погледу имају специјалне надлежности.

Кривични законик Републике Србије садржи посебну главу (Глава двадесет седам) чији је наслов „Кривична дела против безбедности рачунарских података“. У њој су као кривична посебно одређена следећа дела:

прво, оштећење рачунарских података и програма, под којим се подразумева неовлашћено брисање, измена, оштећење, прикривање или чињење неупотребљивим на други начин рачунарских података и програма. За основни облик овог кривичног дела запређена је новчана казна или казна затвора до једне године;

друго, рачунарска саботажа, под којим делом се подразумева уношење, уништење, измена, оштећење, прикривање или чињење неупотребљивим на други начин рачунарских података или програма или оштећење рачунара или других уређаја за електронску обраду података и пренос података, а са намером да се онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте. За основни облик овог кривичног дела прописана је казна затвора у трајању од шест месеци до пет година;

треће, прављење и уношење рачунарских вируса, под којим се подразумева прављење рачунарског вируса у намери његовог уношења у туђи рачунар или рачунарску мрежу, за које дело је запређена новчана казна или казна затвора до 6 месеци;

четврто, рачунарска превара, под којим делом се подразумева уношење нетачних података, пропуштање уношења тачних података или прикривање на други начин или лажно приказивање података чиме се утиче на резултат електронске обраде и преноса података, а у намери прибављања за себе или другог противправне имовинске користи и наношења другоме имовинске штете, за које дело је запређена новчана казна или казна затвора до 3 године;

пето, неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података, под којим се подразумева кршење мера заштите и неовлашћено укључивање у рачунарску мрежу или неовлашћен приступ електронској обради података, за које дело је предвиђена новчана казна или казна затвора до 6 месеци;

шесто, спречавање и организовање приступа јавној рачунарској мрежи, под којим се подразумева неовлашћено спречавање или ометање приступа јавној рачунарској мрежи, за које дело је запређена новчана казна или казна затвора до једне године;

седмо, неовлашћено коришћење рачунара или рачунарске мреже, под којим се подразумева неовлашћено коришћење рачунарске услуге или рачунарске мреже у намери прибављања себи или другом противправне имовинске користи, за које је дело запрећена новчана казна или казна затвора до 3 месеца.

Поред наведених Кривични законик познаје и нека друга кривична дела која могу бити основ за кривичноправну заштиту против компјутерског криминалитета. Тако рецимо кривично дело повреде тајности писама и других пошиљки (члан 142.) односи се и на повреду тајности електронске поште или другог средства за телекомуникацију.

Напомињемо да је код нас у сарадњи Савета за државну управу Владе Републике Србије и UNDP 2002. године израђена и радна верзија Закона о сајбер криминалу од које се касније одустало.

Посебно место у систему заштите од компјутерских кривичних дела у нашем праву има Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала. Наведеним Законом уређује се образовање, организација, надлежност као и овлашћења посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела против безбедности рачунарских података односно кривична дела против интелектуалне својине, имовине и правног саобраћаја код којих се као објект или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 500 или настала материјална штета прелази износ од 850.000 динара.

На основу овог Закона образовани су и посебни органи односно посебна одељења чији је посао непосредно везан за наведене облике кривичних дела. Тако је у оквиру Вишег тужилаштва у Београду образовано посебно одељење односно Посебно тужилаштво за борбу против високотехнолошког криминала чијим радом руководи Посебан тужилац. Даље, у оквиру министарства унутрашњих послова Србије образована је на основу предметног закона посебна служба за борбу против високотехнолошког криминала, а у оквиру Вишег суда у Београду посебно Веће за борбу против високотехнолошког криминала. Дакле, према

одредбама наведеног Закона на свим нивоима кривичног поступка, почев од откривања преко истраге и суђења образована су посебна одељења која за искључиви задатак имају борбу против наведених кривичних дела. Мада Закон то посебно не наглашава подразумева се да ће лица запослена у тим органима, почев од тужилаца и судија па до полицајаца, морати да имају висок ниво знања о функционисању и могућим злоупотребама у функционисању високих технологија. То се посебно очекује од запослених у полицији чији је посао вероватно и најсложенији и односи се на откривање ових дела и њихових починилаца.

Глава IV

ЕЛЕКТРОНСКА ЕКОНОМИЈА, ЕЛЕКТРОНСКА ТРГОВИНА И УГОВОРИ У ЕЛЕКТРОНСКОЈ ФОРМИ

1. Електронска економија

У последњих пар десетина година све више се у стручној литератури и пословној пракси користи термин „електронска економија“ или „нова економија“. Реч је о изразу односно појму који означава скуп нових економских активности које су настале као резултат развоја савремених технологија и њихове примене у економским односима, у првом реду економским трансакцијама. Тако се и у извештају који је 2001. године Европска комисија упутила Европском парламенту наводи да је електронска економија назив за модификације у понашању економских субјеката које су последица великог спектра могућности које доноси интензиван развој информационих и комуникационих технологија, посебно интернета.

Информационе и комуникационе технологије, употребљене као „алати“ нове економије, квалитативно мењају тржишта и методе људског рада. Начелно говорећи, таквих промена је у историји људског друштва било доста. Подсетимо се само какав је утицај на развој економије имао проналазак и практична употреба парне машине или бензинског мотора. Са друге стране ефекти примене савремених електронских комуникационих технологија у сфери економије су, више него код било којих „револуционарних“ промена пре њих, и шири и дубљи. Да о брзини њихове имплементације и не говоримо.

Кроз коришћење комуникационих технологија данашњице светско тржиште постаје у правом смислу „глобално село“, место у којем се сусрећу понуда и тражња роба и услуга из свих крајева света. Место у којем фабрике и трговине раде 24 часа свих 7 дана у недељи и где сваки произвођач или купац може наћи нешто за „своју душу“. Даље, поступно се губи некада јасна и оштра секторска разлика на тржишту роба и услуга. Уколико, на пример,

имате могућност да нешто платите позивом одређеног телефонског броја поставља се питање да ли је ту реч о финансијској или пак телекомуникационој услузи.

Несумљиво је да многе државе у свету свој убрзани економски развој дугују између осталог и суштинским инвестицијама у сектор информационих и телекомуникационих технологија. Не само у развој и усавршавање тих технологија самих по себи већ и њиховој практичној примени у више мање свим привредним гранама. У исто време оваква пракса захтева и непрекидно обучавање радне снаге и то не само када је у питању развој вештина повезаних са информационо комуникационим технологијама већ и свих других вештина и знања неопходних да би се на тржишту валоризовала предност таквих технологија.

Предмет нашег интересовања је у првом реду електронска трговина као важан сегмент општег појма електронске економије.

2. Електронска трговина

Електронска трговина или е-трговина односно *e-commerce*, како се још назива, састоји се примарно од дистрибуције, куповине, продаје, маркетинга и сервисирања производа и услуга путем електронских система као што је интернет и друге компјутерске мреже. Такође укључује и електронски трансфер новца, управљање ланцима снабдевања, електронску размену података и аутоматске системе за сакупљање података. У испуњавању својих задатака користи електронске комуникационе технологије као што су интернет, екстранет, електронска пошта, е-књиге, базе података, мобилни телефони...

Електронска трговина није исто што и електронско пословање, она је део ширег појма електронског пословања па у њој и када се ради о техничким нормативима и када се ради о правним стандардима важе, више мање, идентична правила.

Мада електронска трговина није сасвим нов појам, о њој се на различите начине и у различитом обиму дискутује већ последњих пар десетина година, могло би се рећи да се тек у последњој декади јављају

различите стручне интерпретације појма електронске трговине. У прво време под електронском трговином подразумевале су се само операције куповине производа и услуга које се обављају преко интернета. Али концепт електронске трговине је много шири и не ограничава се само на интернет.

Електронска трговина није ништа друго до свака форма пословне односно трговачке трансакције у којој све стране комуницирају искључиво електронским путем.⁵⁸ Слично одређење је и оно према којем је електронска трговина било која трансакција чији су предмет роба или услуге у којима дигитална електронска средства комуникације имају суштинску улогу.⁵⁹ Претходно изнетим дефиницијима електронске трговине недостаје извесна садржинска „пуноћа“. Несумњиво је да се електронска трговина може посматрати из два угла, ширег и ужег. У ужем смислу она би обухватала продају роба, услуга и информација путем мрежа, а у ширем смислу још и размену пословних информација, одржавање пословних односа и вођење пословних трансакција.

Чини се ипак да је, имајући у виду и све претходно речено, једно од најпотпунијих одређења појма електронске трговине садржано у ставу сходно којем се она дефинише као свака активност која укључује интеракцију и пословање компаније са корисницима, између две компаније или са јавним институцијама, а која се обавља електронским путем. То обухвата наручивање производа и услуга који се достављају традиционалним каналима као што је пошта или курирска служба (тзв. индиректна *e*-трговина), затим електронско наручивање, плаћање и достављање неопипљивих (нематеријалних) производа и услуга као што су софтвер, електронски часописи, услуге забаве и давање информација (директна *e*-трговина), електронски трансфер новца, електронско плаћање, размену пословних информација, електронских докумената, комерцијалне аукције, сарадњу у дизајнирању и инжењерингу, *on line* истраживање и постпродајне услуге.⁶⁰

⁵⁸ Lodder A and Kaspersen H: *eDirectives: Guide to European Union Law on E-Commerce*, 2002, The Hague: Kluwer Law International, p3.

⁵⁹ Paul Todd: *E-Commerce Law*, Great Britain 2005, p. 3.

⁶⁰ Chaffey D. “Management of e-business and e-commerce” UK 2001.

Изнета дефиниција на детаљан начин описује ниво пословних активности које су обухваћене појмом електронске трговине. При томе се електронска трговина, као што је претходно и наведено, не своди само на продају и куповину већ и на различите пред и постпродајне активности. Видели смо такође да се електронска трговина не може свести само на пословне комуникације које се обављају путем интернета већ да су то све трговачке трансакције у којима стране комуницирају искључиво електронским путем. Ипак, несумњиво је да интернет представља најснажнији покретач развоја електронске трговине, баш као и електронског пословања уопште, те да техничке могућности које ова технологија омогућава и јесу, у суштини, узрок праве мале револуције у сфери електронског пословања.

2.1. Кратак историјски развој електронске трговине

У прво време, а то је крај 60-их година прошлога века, електронска трговина је коришћена као термин за означавање пословних трансакција између тачно одређених фирми које су и раније биле у пословном односу, а углавном путем тзв. EDI технологије. Нешто касније у електронску трговину се укључују и активности првобитно означене као „мрежна трговина“, односно активности које су подразумевале куповину и продају роба и услуга путем мреже (*World Wide Web*), а преко сигурносних сервера (као HTTPS, што је специјални серверски протокол који криптује поверљиве податке ради заштите потрошача) и путем електронских сервиса плаћања, као што су кредитне картице. Када је „мрежа“ почела добијати широке светске размере, што се поступно почињене дешавати негде почев од 1994. године, електронска трговина такође добија на замаху. Требало је додуше нешто времена да сигурносни протоколи постану довољно развијени, распрострањени и наравно сигурни. Отуда највећи број компанија у почетку „мрежу“ користи за развој тзв. основних сајтова пружајући свим трећим лицима, корисницима мреже, само могућност да буду информисани о компанији о којој је реч, њеном производном програму, пословању, асортиману и другим важним пословним информацијама. Тек при крају 20-ог века највеће светске компаније почињу да преко „мреже“ непосредно тргују са свим трећим лицима.

Узроци неслућеног раста електронске трговине везују се најчешће за следеће утицаје:

- промоција производа - електронска трговина омогућава промоцију производа и услуга кроз директне и информативно богате интерактивне контакте са купцима;
- нове канале продаје - електронска трговина ствара нове канале дистрибуције за постојеће производе, захваљујући директном контакту са појединачним купцем и двосмерној природи комуникација;
- директне уштеде - трошкови испорука информација преко интернета знатно су нижи, као и сама реализација испоручених дигитализованих производа (музика, софтвер...) у односу на стварну физичу испоруку;
- смањење временског циклуса - испоруке дигитализованих производа и услуга свде се на секунде;
- услуге купцу - значајно су побољшане услед могућности купаца да проналазе детаљне информације о њима;
- имиџ марке или организације - кроз *web* активности врши се додатна афирмација идентита и марке.

Уз појам електронске трговине везује се даље више различитих начина пословања, али четири су основна. То су *business to business* (B2B), *business to consumer* (B2C), *business to administration* (B2A) и *consumer to administration* (C2A).

Даља будућност развоја електронске трговине везана је за:

- употребу интернета, чији се број корисника непрестано повећава;
- могућност куповине, број производа и услуга који се купују на интернету се рапидно повећава;

- повећана сигурност и поверење, обзиром да је то један од основних ограничавајућих фактора развоја електронске трговине;
- руковање ефикасним информацијама, које постају доступне на било ком месту у реалном времену;
- иновативне организације које ће бити реструктуриране уз помоћ информационих технологија;
- виртуелне заједнице, ојачавају *on line* комерцијалне активности и као професионална подручја интересовања олакшавају електронску трговину;
- систем плаћања, кроз *e*-кеш и микроплаћање све је ближа реалности њихова примена у широком обиму. Када интернационални стандарди постану норма електронског плаћања доћи ће до глобалног проширења електронске трговине.

У основи се сматра да је најважнија област електронске трговине везана за тзв. B2B пословање где се интернет и *web* технологија користе за куповину, продају као и јефтинију, бржу и бољу сарадњу међу пословним субјектима. Као суштинске предности овог пословног концепта истичу се смањење трошкова, повећавање транспарентности пословања, могућност приступа свим тржиштима као и нове, ефикасније и флексибилније трансакционе методе.

Различити B2B пословни механизми најчешће се разврставају на следећи начин: *e*-продаја (*e-selling*), *e*-куповина (*e-buying*), *e*-тржишта (*e-markets*) и *e*-механизми за подршку (*e-collaboration*). При томе:

E-куповина подразумева коришћење *web* базираних технологија у циљу аутоматизације процеса поручивања. Највећи део активности је фокусиран на процес индиректне куповине непроизведених добара и услуга, а водеће компаније користе интернет као подршку за све активности везане за набавку. Користи од аутоматизовања процеса набавке су повећање контроле трошења, редуковање оперативних трошкова везаних за набавку,

аутоматизација рутинских трансакција, фокусирање на стратешка питања набавке и развијање још кориснијих веза са набављачима;

E-продаја се односи на коришћење интернета као канала за продају производа и услуга. Процес продаје може да се обави директно преко веба, а може да буде интегрисан у заједници са више пословних партнера или се може обављати преко трећег учесника. Користи које се остварују овим путем односе се пре свега на ниже трошкове, приступ новим купцима, унапређење контроле залиха, задржавање и класификацију купаца. Потрошачи такође могу бити задовољни могућношћу приступа добро познатим, сигурним брендovima, добро организованом систему претраге као и каталoшке продаје;

Електронска тржишта су интернет базирани посредници који олакшавају трговину између више купаца и продаваца. Постоји их три основна типа: прво, јавно независна електронска тржишта вођена од стране неутралних компанија; друго, јавни конзорцијуми електронских тржишта које воде групе великих компанија; треће, приватна електронска тржишта или приватне трговачке мреже које опслужују једну компанију;

Спајањем огромног броја купаца и продаваца и аутоматизацијом трансакција електронска тржишта проширују дијапазон могућности које стоје на располагању купцима, омогућавају продавцима приступ новим тржиштима и смањују трошкове трансакција за све учеснике. У исто се време повећава доступност и квалитет информација.

Термин *e*-колаборација или *e*-механизми за сарадњу се односи на коришћење интернета за сарадњу са пословним партнерима у смислу ширем од куповине и продаје. Уз помоћ интернета сарадња омогућава дељење информација, прогноза и планова развоја у делићу секунде, без обзира на географску удаљеност.

3. Правне претпоставке развоја електронске трговине

Без обзира што се електронска економија односно електронска трговина не могу посматрати ван општих појмова економије и трговине чији су саставни део ипак постоји потреба правног уређења извесних специфичности које произилазе из употребе савремених електронских

средстава комуникације у њима. То је и био разлог да је у оквиру УН још 1996. године донет Модел закона о електронској трговини, а 2001. године Модел Закона о електронском потпису. Нешто касније је на истом нивоу (УН) донета и Конвенција о употреби електронске комуникације у међународним уговорима. Најзначајнији акти на нивоу ЕУ су Упутство о електронском потпису из 1999. и Упутство о електронској трговини из 2001. године.

У нашој држави је 2004. године усвојен Закон о електронском потпису, а 2009. године Закон о електронској трговини. Имајући у виду околност да прописи о електронском потпису за сврху имају углавном идентификацију потписника у правним пословима и другим правним радњама извршеним у електронском облику надаље ћемо се углавном бавити прописима о електронској трговини и у том контексту основном инструменту пословног промета: уговору у електронској форми. Ипак, пре него што кажемо нешто више о врстама и специфичностима закључења уговора у електронском облику неопходно је у најкраћем подсетити се општих правила о уговорима.

3.1. Општа правила о уговорима

Уговор је сагласна изјава воље два или више лица имовинског карактера а ради заснивања, измене или престанка облигационог односа. До сагласне изјаве воља као најважнијег састојка уговора долази у фази његовог закључења и то најчешће путем понуде за закључење уговора и њеног прихватања.

3.1.1. Понуда за закључење уговора

Понуда за закључење уговора по дефиницији представља предлог за закључење уговора учињен одређеном лицу који садржи све битне елементе уговора тако да би се његовим прихватањем могао закључити уговор. Према општем правилу понуда за закључење уговора учињена присутном лицу сматра се одбијеном ако није прихваћена без одлагања, изузев ако из околности произилази да понуђеном припада изванредан рок за размишљање. Ако је пак понуда учињена одсутном лицу онда се разликују две ситуације: прва, када је у понуди одређен рок за њено прихватање, у ком случају она

обавезује понудиоца до истека тога рока; друга, уколико у понуди није одређен рок за њено прихватање онда она обавезује понудиоца за време које је редовно потребно да понуда стигне понуђеноме, да је овај размотри, о њој одлучи и да одговор о прихватању стигне понудиоцу.⁶¹ Код уговора у привреди не ретко се рок за прихватање понуде одређује употребом израза „одмах“, „без одлагања“, „наредном поштом“ или сличним изразима. У таквим случајевима се сматра да је изјава о прихватању благовремена ако је предата непосредно понудиоцу или пошти првог наредног радног дана по пријему понуде. При томе изјаву о прихватању понуде треба послати истим или бржим средством од онога којим је послата понуда.⁶²

У трговинском праву понудом се сматра и предлог за закључење уговора учињен неодређеном броју лица, који садржи битне елементе уговора чијем је закључењу намењен, уколико другачије не произилази из околности случаја или обичаја. Овакву врсту понуде Закон о облигационим односима назива *општом понудом*.⁶³ Њене особености се састоје у томе што је она упућена унапред неодређеном и неограниченом броју лица и што свако лице може да прихвати ту понуду, која у случају прихвата постаје садржина уговора.⁶⁴ Општа понуда је стална, јер се не гаси тиме што ју је прихватило једно лице или више њих. Она заправо траје све док не протекне време везаности понудиоца овом понудом и на основу ње може бити склопљено више уговора исте садржине са истим или различитим лицима.

У пословном промету општа понуда се најчешће јавља у форми тзв. општих услова пословања, мада се општи услови и општа понуда не морају увек поистоветити. Области у којима се поклапају примарно су области јавних служби (пружање комуналних услуга, јавни превоз, ПТТ услуге) где

⁶¹ Чланови 37. и 40. ЗОО.

⁶² Члан 23. Општих узанси за промет робом.

⁶³ Члан 33. ЗОО.

⁶⁴ Прихват опште понуде се некада манифестује испуњењем обавезе из уговора који се склапа. Рецимо, убацивањем новца у *caffe* апарат. Могућа су међутим и одступања од правила да је изјављивањем прихвата на општу понуду уговор склопљен: ако је општа понуда дата под условом или је у њој наведено да понудилац има право да одлучи хоће ли прихватити учињени прихват или не. У оба ова случаја се међутим суштински и не ради о општој понуди већ о позиву на понуду.

привредни субјекти који обављају ове делатности послују управо на основу општих услова у којима су садржани и битни елементи уговора.

У већини правних система и излагање робе са назначеном ценом се такође квалификује као општа понуда. Овде је реч о понуди учињеној понашањем, прећутно, тзв. реалној понуди која је у нашем праву као правило односно правна норма прихваћена најпре Општим узансама,⁶⁵ а потом и Законом о облигационим односима.⁶⁶ Изузетно, ако је цена изложене робе назначена само ради информације, или уз назнаку “није за продају” или у рекламне сврхе, она се неће сматрати општом понудом. Практично, карактер опште има понуда оне робе са којом се свакодневно, као потрошачи, срећемо у продавницама, на киосцима, тржницама... Понуду прихватамо када плаћамо цену, а одбијамо је тако што робу не купујемо.

Може се дакле закључити да је општа понуда изузетак од правила да понуда мора бити упућена одређеном лицу и да је тај изузетак присутан углавном у пословном промету. Као и све изузетке и овај ваља тумачити рестриктивно и то тако што ће се код оцене да ли се у конкретном случају ради о општој понуди или не полазити од карактера делатности понудиоца. Ако из његове делатности произилази обавеза закључивања уговора са сваком заинтересованом особом, ограничена само “капацитетима” понудиоца, ради се о општој понуди.

У свакодневном животу смо перманентно суочени са бројним видовима “нуђења” роба и услуга као што су слање каталога, ценовника, тарифа или огласа учињених путем летака, телевизије, интернета, штампе... Одговор на питање да ли овакви акти привредних субјеката имају *de iure* значај понуде може понекад имати веома значајне практичне последице. Наш Закон о облигационим односима заузима став да се претходно поменута поступања привредних субјеката не сматрају понудом него само позивом да се учини понуда под објављеним условима.⁶⁷ Дакле, тек када потенцијални потрошач “одговори” на акт пошиљаоца каталога (ценовника, тарифе) или емитента огласа, који се назива *понуда јавности*, биће речи о понуди. Понуде

⁶⁵ Општа узанса број 12. став 2.

⁶⁶ Члан 34. ЗОО.

⁶⁷ Члан 35. тачка 1. ЗОО.

јавности се и у већини других правних система не сматрају понудом за закључење уговора већ само позивом на понуду.⁶⁸

Ово законско правило ипак није императивне природе. Наиме огласи и друге понуде јавности сматраће се понудама за закључење уговора ако то јасно произилази из њихове садржине, што је опет фактичко питање. Код нас се сматра да у том погледу није довољно само назначење цене у каталогу или огласу.⁶⁹

У сваком случају емитент понуде јавности ће одговарати за штету коју би претрпео понудилац ако без основаног разлога одбије да прихвати понуду која му је учињена на основу огласа или других инструмената.⁷⁰ Овде је реч о посебном облику тзв. предуговорне одговорности која се заснива на чињеници да је аутор огласа или других понуда јавности изразио своју начелну вољу да закључи уговор и тиме створио код понудиоца поверење у настанак уговора, тим пре што су они своје понуде поднели на основу његове иницијативе. При томе би одбијање “без основаног разлога” постојало увек, осим када није условљено чисто економским разлозима као што су исцрпљивање робе на залихама или промена услова на тржишту која би пословање на тим основама учинило нерентабилним за аутора понуде јавности.

Конечно, постоји у упоредном пословном праву и занимљиво питање квалификовања правне природе јавног позива за учешће у поступку продаје јавном аукцијом или тендером. Основна дилема је да ли се том приликом упућени јавни позив има ценити као понуда, и то општа понуда, или је то “само” позив на понуду. Код нас се сматра да је расписивање јавне аукције позив на стављање понуде те отуда и не обавезује аукционара. Тек понуде учесника аукције или јавног надметања представљају понуду за уговор, с тим

⁶⁸ Изузетак представља француско право где се и понуде јавности сматрају понудама за закључење уговора. Драшкић М: “Закључивање уговора о продаји”, Београд 1986, стр.48.

⁶⁹ Према члану 2:201 тачка 3. Начела европског уговорног права предлог да се испоруче роба или услуге по одређеној цени учињен у јавном огласу или каталогу, или излагањем робе, сматра се као понуда за продају или испоруку по тој цени, све док се залихе не испразне, односно док се не исцрпи могућност испоручиоца да пружа дате услуге.

⁷⁰ Члан 35. тачка 2. ЗОО.

што свака виша понуда искључује претходну, а одлука аукционара (“пад чекића” или други уобичајени начин) је прихват понуде и закључење уговора.⁷¹ Претходно изложено правило може бити релевантно и за тзв. интернет односно *on line* аукције па га отуда на овом месту и помињемо.

3.1.2. Прихватање понуде за закључење уговора

Прихватање понуде за закључење уговора је такође изјава воље којом се једна страна саглашава са примљеном понудом, на основу које настаје уговор. Значај прихватања понуде има само изјава понуђеног која је сагласна понуди и уколико је учињена у року одређеном за њено прихватање. Прихватање понуде производи дејство уколико је учињено слободно и озбиљно од лица способног за закључење тог уговора. Изјава о прихватању понуде је релевантна ако по садржини одговора понуди у погледу битних састојака уговора обзиром да уговорне стране споредне састојке уговора могу одредити и доцније, након његовог закључења.

Ако понуђени изјави да прихвата понуду али под условом, са резервом или слично, а уједно предложи и да се понуда измени у нечему или допуни, сматраће се да је понуду одбио и да је са своје стране учинио другу понуду свом ранијем понудиоцу.

Изјава о прихватању понуде може се учинити изричито (активним понашањем), речима написаним или изговореним или одговарајућим гестовима, конклюдентним радњама или прећутно али увек тако да по садржини одговара понуди.

Коначно, ћутање понуђеног, под којим се подразумева не само чињеница да он ништа није рекао или написао већ његов потпуно пасиван став, не значи прихват понуде. Па и у случају да понудилац у своју понуду унесе одредбу да ће се ћутање понуђеног или неко друго његово пропуштање (рецимо ако не одбије понуду у одређеном року или ако послату ствар у вези које му се нуди уговор не врати у одређеном року) сматрати као

⁷¹ Васиљевић М: “Пословно право”, Београд 1999, стр. 373-374; Голдштајн А: “Привредно уговорно право”, Загреб 1974, стр.100.

прихватање.⁷² Јер понуда је прихваћена тек кад понудилац прими изјаву понуђеног да прихвата понуду.

Пословно право пак познаје одређене, рекли би значајне изузетке од општих правила грађанског права о ћутању понуђеног. У првом реду ћутање понуђеног који са понуђачем стоји у сталној пословној вези у погледу одређене робе значи прихват понуде која се односи на такву робу, ако се понуда одмах или у остављеном року не одбије.⁷³ Претходни услов за квалификовање ћутања као прихвата понуде је дакле постојање сталне пословне везе понуђача и понуђеног у вези одређене робе али, у исто време, и одређених уговора који за предмет имају такву робу. Отуда се закључење уговора који су редовно закључивани међу пословним партнерима, али у погледу различите робе, или уговора који за предмет имају исту робу, али је њихова правна природа битно различита (рецимо уговор о продаји и уговор о превозу исте робе) не би могло квалификовати у смислу претходно изложеног правила о ћутању понуђеног.

Ћутање је као прихват понуде квалификовано и у односу на неке категорије лица која се баве вршењем туђих послова као професионалном делатношћу (адвокати, трговински заступници, комисионари, шпедитери...) или лица која се нуде другоме да извршавају његове налоге. Ако ова лица не желе да прихвате понуђени налог (понуду) дужна су да га одмах одбију, или уговор аутоматски настаје. У оваквим се случајевима наине полази од претпоставке да сагласност воља произилази из чињенице да она није изричито негирана одбијањем понуде па се сматра да је уговор закључен у тренутку када је понуда (односно налог) стигла понуђеном.⁷⁴ Разуме се, код оцене да ли ћутање у оваквим ситуацијама увек значи прихват понуде потребно је узети у обзир не само одредбе Закона о облигационим односима већ и многе друге околности, између осталог и начело савесности и поштења.

Код неких уговора у привреди могуће је и тзв. прећутно закључење уговора конклюдентним радњама понуђеног. Конклюдентно поступање међутим, за разлику од ћутања понуђеног, не представља потпуно пасиван

⁷² Члан 39. тачка 1. ЗОО, члан 42. тачка 1. ЗОО.

⁷³ Члан 42. тачка 3. ЗОО.

⁷⁴ Члан 42. тачка 5. ЗОО.

однос већ одређене активне радње из којих произилази да су се странке сагласиле на закључење уговора. Тако рецимо понуђени може платити цену назначену у понуди или предузети неку другу радњу која има значај прећутног прихвата понуде.⁷⁵

3.1.3. Време и место закључења уговора

Време закључења уговора је битна околност обзиром да од тог тренутка уговор почиње да производи правно дејство, од тог момента дакле настају права и обавезе из уговора, теку рокови за извршење обавеза. Време закључења уговора се одређује у зависности од тога да ли је уговор закључен између присутних или одсутних странака. У првом случају, ако су уговарачи непосредно присутни, уговор настаје у тренутку емитовања изјаве о прихвату понуде, када фактички и долази до сагласности воља понуђача и понуђеног.

У другом случају, ако су странке одсутне, у упоредном праву је постојало или постоји више решења:

а) сходно теорији изјаве, данас напуштеној, уговор се има сматрати закљученим у тренутку давања изјаве понуђеног о прихвату понуде;

б) сходно теорији одашиљања (САД, Велика Британија) уговор се сматра закљученим у тренутку одаслања, практично у тренутку када понуђени предаје прихват понуде у пошту;

в) према теорији пријема (наше право и право највећег броја других земаља) уговор се сматра закљученим када понудилац прими изјаву понуђеног о прихвату понуде;

г) према теорији сазнања (Италија) уговор се сматра закљученим у моменту када понудилац сазна да је понуђени прихватио његову понуду.

Што се тиче места закључења уговора важе следећа правила: ако се уговор закључује између одсутних лица, али и лица која се у погледу времена закључења сматрају присутним лицима (рецимо лица која разговарају телефоном, видео везом, телепринтером....), уговор се сматра закљученим у

⁷⁵ Примери конклюдентног поступања понуђеног са значењем прихвата понуде наведени су у члану 34. Општих узанси.

месту у коме је понудилац имао седиште (правна лица) односно пребивалиште (физичка лица) у време када је уговор закључен. Ако се уговор закључује између непосредно присутних лица јасно је да се уговор сматра закљученим у месту у којем су се странке налазиле када су уговор закључиле.

4. Специфичности уговора у електронском облику

4.1. Нека општа правила о закључењу уговора у електронском облику

Сходно нашем Закону о електронској трговини и највећем броју других компаративних прописа у свету⁷⁶ дозвољена је могућност закључивања уговора електронским путем односно у електронској форми. То практично значи да се и понуда и прихват понуде за закључење уговора могу дати електронским путем. То што је уговор закључен путем електронских порука односно то што се електронска форма користи приликом његовог закључења уговору не може оспорити пуноважност.

У нашем праву и упоредном законодавству одредбе о закључењу правних послова путем електронске размене порука односно у електронској форми не примењују се на:

а) правне послове којима се врши пренос права својине на непокретности или којима се установљавају друга стварна права на непокретностима;

б) изјаве странака и других учесника у поступку за расправљање заоставштине, форму завештања, уговоре о уступању и расподели имовине за

⁷⁶ Велики број држава у свету је своје прописе о електронској трговини донео управо на основу претходно поменутог Модела закона о електронској трговини УН. Тај акт у трећем поглављу првог дела садржи одредбе о закључењу уговора и то: одредбе које се односе на закључење и пуноважност уговора у електронској форми (члан 11), признавање пуноважности порука са подацима између уговорних страна (члан 12), утврђивање коме треба приписати слање поруке (члан 13), потврду о пријему поруке (члан 14) и место и време слања односно пријема поруке (члан 15). Напомињемо да су те одредбе диспозитивног карактера па уговорне стране могу уговорити и другачија правила.

живота, уговоре о доживотном издржавању и споразуме у вези са наслеђивањем, као и друге уговоре из области наследног права;

в) уговоре о утврђивању имовинских односа брачних другова;

г) уговоре о располагању имовином лица којима је одузета пословна способност;

д) уговоре о поклону;

е) друге правне послове или радње за које је посебним законом или на основу закона донетих прописа изричито одређена употреба својеручног потписа у документима на папиру или овера својеручног потписа.

Овде је, као што се може видети, углавном реч о уговорима који за пословни промет и немају неки велики значај. Но, ако се као претпоставка пуноважности и настанка уговора захтева потпис лица сматраће се да је тај услов задовољен уколико је електронска порука потписана квалификованим електронским потписом.

Код закључења уговора у електронском облику пружалац услуга има посебне законске обавезе. Он је најпре дужан да потенцијалном кориснику услуга пре закључења уговора обезбеди на јасан, разумљив и недвосмислен начин податке и обавештења о поступку који се примењује код закључења уговора, уговорним одредбама, општим условима пословања (ако су саставни део уговора), језицима на којима уговор може бити закључен као и о кодексима понашања у складу са којима поступају пружаоци услуга и како се ти кодекси могу прегледати електронским путем.

Пружалац услуга је даље дужан да потенцијалном кориснику услуга обезбеди техничка средства за препознавање и исправљање погрешног уноса података у поруку пре њеног слања или предаје као и да обезбеди да текст уговора и одредбе општих услова пословања које су саставни део уговора закључених у електронској форми буду доступни корисницима услуга на начин који омогућава њихово складиштење, поновно коришћење и репродуковање.

Коначно, пружалац услуга је дужан да без одлагања, електронским путем, посебном електронском поруком, потврди пријем електронске поруке која садржи понуду или прихват понуде за закључење уговора. Додуше, ако

је реч о уговорима који се закључују путем електронске поште односно других видова личне комуникације остварене електронским путем оваква обавеза на страни пружаоца услуге неће постојати.

4.2. Специфичности коришћења интернета у процесу закључења уговора

Једно је сигурно: уговори закључени посредством интернета су „само“ уговори који са собом носе све опште карактеристике уговора уопште. Ипак, имајући у виду специфичну технику која се користи у фази закључења оваквих уговора могуће је уочити и одређена правила која важе само уколико је у питању коришћење неке од интернет техника закључења уговора. Поред тога специфичност интернет уговора се може очитовати и у погледу њиховог садржаја. Тако се према претходно изнетом критеријуму може говорити о три групе уговора склопљених преко интернета:

а) уговори за стицање материјалних добара (књиге, CD ромови, одећа, обућа, храна...), где се склапање уговора врши путем интернета док се достављање добара о којима је уговор врши на класичан начин, путем поште најчешће;

б) уговори за стицање лиценци за коришћење дигиталних производа или информација (софтвера, фотографија, музике...), где се по правилу и закључивање уговора и испорука робе врше путем интернета;

в) уговори о испуњењу неке интернет услуге као што је рецимо приступ неким садржајима на интернету, тражење или ширење информација, интернет банкарство....

Интернет технологија омогућава такође закључење уговора на различите начине, уз извесне разлике у односу на правила која важе за закључење уговора традиционалним путем односно традиционалним техникама.

Уколико се уз коришћене интернета остварује директна и интерактивна комуникација између странака, физички одсутних лица, што се постиже рецимо видеоконференцијском везом, телефонском везом оствареном преко интернета или тзв. *chat* порукама, право сматра да је реч о закључењу уговора између присутних лица у погледу времена закључења

уговора. Дакле, као и када је реч о непосредно присутним странакама, време закључења уговора ће бити време када понуђени емитује изјаву о прихватању понуде понудиоца. Што се тиче места закључења уговора у претходно наведеним случајевима као релевантно је одређено место у којем је понудилац имао своје пословно седиште односно пребивалиште у време када је уговор закључен. Када је реч о понуди, начину њеног одашиљања као и питању прихватања понуде, у претходно наведеним случајевима не постоје никакве разлике у односу на истоврсна питања код закључења класичних уговора.

Са друге стране интернет омогућава и закључење тзв. *web* уговора односно уговора разменом *e-mail* порука. И овде се у погледу одређених класичних правила појављују одређени изузеци које ћемо надаље размотрити.

5. Web уговори

У правном смислу *web* страница или *web page* се може одредити као документ (исправа) у електронском облику који је за наручиоца израдио пружалац тог типа услуга (провајдер) и који је доступан наручиоцу уз коришћење посебног програма. Тај документ може бити постављен (потхрањен) на рачунару провајдера (сервера) тако да буде доступан само наручиоцу или ограниченом броју наручилаца и корисника или сваком кориснику наведеног програма путем интернета, ако се користе тачном адресом документа и изричито затраже (кликом миша на за то одређеном месту) представљање садржаја наведеног документа на екрану свог рачунара.

Дакле, путем интернета се долази само до информације која је постављена на *www* односно до документа израђеног у складу са претходно наведеним правилима те се са таквог документа преузима (*download*) или чита. *Web* страница дакле није на интернету, како се то уобичајено каже, већ се интернетом до ње долази обзиром да се она и физички налази у облику електронског записа на рачунару интернетског послужитеља (сервера), дакле на тачно одређеном и одредивом месту. Приступ том месту електронским путем могућ је коришћењем адресе *web* странице на којој се налази уписан одређени документ.

5.1. Уопште о изјави воље на *Web* страници

Под изјавом воље подразумевају се различити облици и могућности у којима се изражава унутрашња воља неког субјекта права. Начелно, воља за закључење уговора може бити изражена на различите начине: усмено, писмено, знацима и конклюдентним радњама. Уобичајено је међутим да власник неке *web* странице своју вољу за закључење уговора са посетиоцима те странице изражава писмено. При томе би већ из садржаја саме странице морало бити видљиво да ли на тај начин изражена воља има значај понуде или позива на понуду и под којим условима.

Посетиоцима *web* странице се такође омогућава да изјавом своје воље, која се у техничком смислу састоји из додиривања одређеног места на рачунару или клика мишем на одређену икону, комуницира са програмираним садржајем *web* странице и на тај начин са њеним власником склопи одређени уговор. Дакле, један од саговорача „улази“ на одређену *web* страницу на којој постоји понуда или позив на понуду за склапање уговора унапред неодређеном броју лица. Изјава воље посетиоца странице је при томе по правилу сведена на ДА – НЕ (*I Accept – I Decline*), дакле на прихватање у потпуности понуђеног или одбијање понуђеног у потпуности. Разуме се, оваквој изјави воље уобичајено претходи преглед одређеног текста који би требао представљати текст уговора између власника и посетиоца *web* странице.

При изјави воље кликом миша (или додиривањем екрана) по правилу нема *e mail* поруке, дакле нема ни писане изјаве воље. Отуда се у правној теорији поставља питање да ли је такво поступање посетиоца *web* странице конклюдентна радња или знак којим се изражава воља. Наиме из конклюдентне радње се са сигурношћу, али посредним путем, закључује о постојању воље док би, ако би се клик или додир екрана посматрао као знак, било речи о непосредној изјави воље. У овом погледу постоје различита мишљења. Тако се рецимо према неким ауторима клик мишем или додир екрана имају посматрати као знак⁷⁷ док се у неким правним системима, канадском рецимо, они третирају као конклюдентна радња.

⁷⁷ Ведриш М-Кларић П: Грађанско право, Народне новине, Загреб 2003, стр.123.

5.2. Специфичности *Web* уговора

Web страница је у суштини електронски запис који њен власник чини доступним по правилу свим корисницима интернета и на којем запису могу бити крајње различити садржаји: текст, слика, звук, видео, анимација, база података, виртуелна стварност. Разуме се, привредни субјекти овакав вид комуникације са спољним светом користе у смислу промоције својих производа и услуга и у том погледу закључивања одговарајућих уговора. Но управо се с тим у вези поставља низ значајних питања, а једно од њих је свакако и то да ли је излагање роба и услуга на *web* страницама у правотехничком смислу понуда или само позив на понуду.

У многим случајевима на претходно постављено питање одговор даје већ сам власник *web* странице на којој се продаја неке робе односно услуге нуди. Тако се рецимо на многим *web* страницама експлицитно наводи да ће евентуални „клик“ мишем на означено поље бити сматран понудом или позивом на понуду. Рецимо: „Уговор ће се сматрати закљученим тек када потврдимо вашу поруџбину“ или „Закључење уговора зависи од тренутно расположивих залиха“. Међутим проблем постаје сложенији уколико у овом смислу на *web* страници не постоје никакви подаци. Додуше, на први поглед и у оваквим случајевима клик мишем на поље које означава прихват односно *accept* логички значи прихватање понуде, а не позив на понуду. Али правно посматрано ствари не морају бити онакве како на први поглед изгледају.

Модел закона о електронској трговини као ни Упутство ЕУ не решавају ово питање. Ипак, из одредбе Упутства која обавезује продавца да одмах потврди поруџбину могло би се закључити да је овај акт ближи томе да поруџбину интернет купца третира као понуду, потврду интернет продавца као прихват, а трговачке податке које продавац излаже на интернету само као позив на понуду. У овом смислу је опредељена и Конвенција о међународној продаји робе⁷⁸ као и закони неких европских држава, рецимо Белгије, Немачке, Велике Британије.... Све су чешћа мишљења међутим да у овом погледу треба правити разлику између интерактивних сајтова и оних који то

⁷⁸ UNCITRAL, Legal aspect of electronic commerce, UN DOC. A/CN.9/WG.IV/WP.95. На овај начин је наиме опредељен члан 14. став 2. Конвенције. Ваља међутим напоменути да се предметна Конвенција не примењује на потрошачке купопродаје које су претежан део овакве трговине.

нису. Према тим ставовима излагање робе на интерактивним сајтовима који дају могућност купцу да директно наручи робу треба сматрати понудом која важи док се не исцрпе залихе. Овакво решење је прихваћено у канадском и италијанском праву, а разлози се налазе у могућности непосредног преговарања и закључења уговора преко самог сајта. Чини се да би и у нашем праву ваљало уважити претходно изнету аргументацију. Тако би се излагање робе на интерактивним сајтовима на којима је означена и цена робе могло третирати као понуда сходно члану 34. ЗОО⁷⁹ док би се излагање робе на „обичним“ рекламним сајтовима могло третирати као позив на понуду у смислу члана 35. ЗОО.⁸⁰

Уколико је дакле реч о интерактивним сајтовима на којима продавци нуде своју робу, уз назначење њене цене, и при томе изричито не наводе да се такав њихов акт неће сматрати понудом односно да ће се сматрати „само“ позивом на понуду, онда би се у свим оваквим случајевима у правнотехничком смислу радило о понуди. И то о општој понуди, упућеној унапред неодређеном броју лица која би била ограничена само пословним капацитетима понудиоца односно стањем понуђене робе на залихама. Прихват понуде се у оваквим случајевима врши, како је то наведено у неким упоредним прописима (канадски модел закона), конклюдентним радњама у електронској форми као што су додиривање одређеног места на екрану рачунара или „кликом“ на иконицу на којој пише „прихватам“.

Следеће важно питање које се у вези закључења оваквих уговора поставља је питање да ли се овде ради о уговору закљученом између присутних или одсутних лица. Логика налаже да је реч о одсутним лицима али, имајући на уму интерактивно својство сајта, реч је о лицима која се у погледу времена закључења уговора сматрају присутним лицима. Сходно томе место закључења оваквог уговора би било место где је понуђач имао своје пословно седиште у моменту упућивања понуде. У исто време се

⁷⁹ „Изолагање робе са означањем цене сматра се као понуда, уколико другачије не произилази из околности случаја или обичаја“.

⁸⁰ (1) „Слање каталога, ценовника, тарифа и других обавештења, као и огласи учињени путем штампе, летака, радија, телевизије или на који други начин, не представљају понуду за закључење уговора него само позив да се учини понуда под објављеним условима. (2) Али ће пошиљалац таквих позива одговарати за штету коју би претрпео понудилац ако без основаног разлога није прихватио његову понуду.“

сходно посебним прописима у области електронске трговине као време закључења уговора сматра време када је понуђач примио електронску поруку која има значење изјаве понуђеног да прихвата понуду. Прихват понуде се при томе сматра примљеним када таквој „изјави“ лице коме је она упућена може приступити. Код сајтова који омогућавају интерактивну комуникацију и који су аутоматизовани тај тренутак следи у врло кратком времену након одашиљања изјаве у електронској форми о прихвату понуде. Уобичајено је сајт на тај начин софтверски уређен да онога ко је понуду прихватио аутоматски обавештава не само о томе да је његова понуда прихваћена већ и о евентуалним трошковима отпослања, датуму отпослања као и очекиваном датуму пријема. Уколико је предмет уговора нека нематеријализована ствар (софтвер, музика, филм...) рачунар понудиоца је тако програмиран да сам и извршава уговор тако што дозвољава купцу да преузме купљену робу путем свог рачунара.

Постоје са друге стране и такви сајтови који не омогућавају интерактивну комуникацију између потенцијалног купца и лица које посредством сајта „нуди“ одређен асортиман роба и/или услуга. На први поглед овакви сајтови се не разликују од оних интерактивних - и на њима се „нуди“ продаја неке робе односно услуга, уз или без назначење цене, општих услова пословања и свих других услова закључења уговора. У правнотехничком смислу пак овакво поступање власника сајта односно лица које путем сајта „нуди“ своје производе или услуге по правилу није понуда већ позив посетиоцима сајта да учине понуду под на сајту објављеним и објашњеним условима. Овде је дакле додиривање одређеног поља на екрану рачунара или клик мишем на одређену икону (без обзира шта на тој икони писало) само понуда, а не прихват понуде. Власник сајта је тај који ће на одговарајући начин прихватити понуду посетиоца сајта. Његова изјава воље о прихватању понуде може бити реализована на различите начине: електронским путем, рецимо слањем обавештења понудиоцу на његову електронску адресу или обавештавањем понудиоца путем сајта, као и конклюдентним радњама, рецимо слањем фактуре односно поруџбенице или пак испоруком саме робе. Обзиром да овакви сајтови не омогућавају интерактивну комуникацију потенцијалних уговарача овде ће свакако бити реч о уговорима који се сматрају закљученим између одсутних лица. Међутим, као што смо претходно и нагласили, опште је правило да се као место закључења уговора сматра место у којем је понудилац имао своје

пословно седиште, ако се уговор закључује између одсутних лица али и лица која се у погледу времена закључења уговора сматрају присутним. Произилази да, када је реч о месту закључења уговора, нема разлике између уговора закључених путем интерактивних и ових других сајтова. Што се времена закључења уговора тиче опште правило важеће у нашем праву засновано на теорији пријема (уговор се сматра закљученим када понудилац прими изјаву понуђеног о прихвату понуде) важиће и у овом случају. Ово посебно имајући у виду да понудилац изјаву понуђеног о прихвату понуде не мора примити у електронској форми већ, као што смо претходно и објаснили, и слањем фактуре, поруџбенице или чак испоруком саме робе неким од класичних средстава испоруке (пошта, курирска служба...).

Све у свему видимо да када је реч о институтима понуде и прихвата понуде, бар када је реч о времену и месту закључења уговора, нема суштинских разлика између уговора закључених путем интерактивних и ових других сајтова.

5.3. Web уговори као формуларни уговори

Имајући у виду начин закључења *web* уговора може се приметити да је он идентичан начину склапања формуларних уговора, по правилу адхезионих, а у мањој мери типских или оних који се вежу уз опште услове пословања. Формуларним уговорима се наине сматрају унапред писмено формулисани обрасци по којима се склапа неодређени број индивидуалних уговора. У формуларне уговоре се убрајају општи услови пословања, типски и адхезиони уговори.⁸¹ Сви претходно наведени уговори су по правилу потрошачког карактера па се при оцењивању услова њихове ваљаности увек настоји заштити слабија страна, у овом случају потрошач.

У оквиру поједностављене технике интернет трговине формуларни уговори представљају стандардизовани облик уговора било да су адхезиони (у целини подређени принципу *take it or leave it*) или типски (где модел уговора представља предлог уговора сходно којем се договарају услови уговора). У оба случаја се међутим несумњиво ради о формуларним

⁸¹ Голдштајн А: Трговачко уговорно право, међународно и компаративно, Народне новине, Загреб 1991, стр.108.

уговорима који се, када је реч о интернет техници, појављују у облику електронског записа.

5.4. Click wrap и browse wrap уговори

Два су основна типа формуларних уговора који се склапају кликом миша, а посредством *web* странице. То су *click wrap* и *browse wrap* уговори. Ови први су уговори који се склапају на *web* страници електронским путем и у електронском облику у којима купац, односно понуђени, у потпуности прихвата понуду понудиоца уз услов да је претходно прегледао (што не значи да је заиста и прочитао) целокупни текст адхезионог уговора. Код *browse wrap* уговора имплицитно се и унапред претпоставља да се лице које уговору приступа слаже са условима и одредбама тог уговора самим тим што претражује *web* страницу на којој склапа уговор (примарна страница), без обзира на то да ли прегледа или улази на *web* страницу која садржи поменуте услове и одредбе уговора којем приступа (секундарна страница). Оба претходно поменута уговора настају из претходнице, тзв. *shrink wrap* уговора односно „скраћеног“ начина склапања уговора. О овим уговорима нешто више ће бити речи.

5.4.1. Shrink wrap уговор

Овај се формуларни уговор почео примењивати у пракси нарочито када су у питању рачунарске игре и софтвери али и за остале производе који се продају и представљају купцу унутар затвореног паковања те се купац са свим условима уговора о продаји може упознати тек након што је производ купио и физички га одмотао (*unwrap*).

Реч је о формуларном уговору посебног типа код којег је купцу пре склапања уговора познат само део стандардизованих уговорних услова. Остали услови као и сам купљени производ купцу постају познати тек након куповине производа односно након склапања уговора о продаји. С тим у вези се оправдано поставило питање да ли је могуће склопити пуноважан уговор ако купац односно онај ко понуду прихвата није у могућности сазнати за све уговорне услове нити у целини перципирати предмет уговора. Мора се ипак нагласити да је овај тип уговора оправдан само у случају када је немогуће на сразмерно мали пакет или омот производа штампати потпуни садржај

уговора, што је посебно случај код продаје софтвера. У сваком другом случају могло би се радити о скривању одређених битних елемената предмета уговора од потенцијалног купца што, разуме се, не би могло уживати правну заштиту. У америчком праву правна заштита овим уговорима се пружа ако су услови куповине производа који су скривени или „неодмотани“ разумно постављени у односу на купца.⁸²

Очигледно је да се на овај начин уговор склапа под делимично непознатим условима и у погледу делимично непознатог садржаја предмета уговора али је садржај, са друге стране, потпуно стандардизован у сваком свом делу, како оном познатом тако и у оном непознатом пре склапања уговора, дакле у потпуности је адхезионе природе. Такви се уговори широм света дневно склапају у великом броју примерака. Они подсећају на уговоре који се склапају на основу општих услова пословања за које се претпоставља да су купцу познати мада му по правилу нису познати. За пружање правне заштите оваквом би уговору било неопходно да је на кутији штампан текст који потенцијалног купца упозорава да се производ купује под условима који су наведени и специфицирани на самом производу који се налази унутар кутије⁸³ јер једино тако купац може знати да постоје додатни услови куповине. Очигледно је да купац овде не може утицати на садржај било ког услова уговора, по чему је овај уговор идентичан са осталим адхезионим уговорима. Разлика од других адхезионих уговора се читава у појављивању осталих услова уговора тек када се отвори кутија и најчешће тек када се ти услови прочитају у електронском облику с медија носача података који је

⁸² Kinsella S – Simpson A: Online contract formation, Oceana Publications Inc., New York, 2004, p.327.

⁸³ Ако је реч о куповини софтвера онда натпис на кутији уобичајено садржи следећи текст: “The software inside this box is sealed inside a separate envelope. Please read this license carefully before opening that envelope or using the software. By opening that envelope, you are presumed to have used the software, and by using software, you are agreeing to be bound by the terms of this licenses. This license contains an obligation for you to arbitrate any disputes you have with... If you do not agree to the terms of this licenses, promptly return the unused and unopened software to the place where you obtained it with your receipt and your money will be refunded, if you purchased the software within the last 30 days. If you purchased the software more than 30 days ago, but you have not opened the sealed envelope, you may still return the software and receive a credit against the purchase of other software from...”

садржан у купљеном производу или се налази на посебном папиру унутар кутије.

Shrink wrap уговор се као формуларни уговор може јавити у више појавних облика односно више носача садржаја таквог уговора. Могуће је да такав уговор буде само у традиционалном писаном облику (на папиру на кутији и папиру унутар кутије) или у комбинацији традиционалног писаног облика и електронског облика: на традиционалном папирном делу који је отиснут на кутији и у електронском облику као електронски запис на медију носачу, по правилу CD-у који се може читати само као електронски запис на производу односно предмету купопродаје.

5.4.2. Click wrap уговори

Click wrap уговори садрже услове и одредбе уговора на *web* страници којима се од потенцијалног сауговорача тражи да путем типке, линка или каквог другог медија искаже сагласност са условима и одредбама уговора пре него што настави са даљим радњама. Ови су уговори у свом пуном тексту приказани у *scroll* прозору или у оквиру *web* странице.⁸⁴

Дакле, садржај *click wrap* уговора се на *web* страници у потпуности може открити и по правилу је изјаву воље могуће и дати само након прегледа целог уговора. Изјава воље односно пристанак на закључење таквог уговора

⁸⁴ *Click wrap* је електронски еквивалент *shrink wrap* метода који омогућава корисницима да прочитају услове споразума пре него што их прихвате. *Click wrap* метод је у својој практичној димензији био и предмет судског спора *ProCD vs. Zeidenberg* (6.F. 3d 1447 (7th Cir.1996)). Zeidenberg је на име од компаније ProCD купио CD ROM који је та компанија произвела, а који садржи компилацију база података из телефонског именика. Након куповине Zeidenberg је софтвер постојећи на купљеном CD ROM-у инсталирао на свом компјутеру и потом креирао сопствени вебсајт (website) посредством кога је посетиоцима нудио да купе информације које CD ROM садржи и то по повољнијој цени него што је исту „робу“ продавала компанија ProCD. Пре куповине софтвера Zeidenberg можда није био свестан било које рестрикције у погледу његовог коришћења без одобрења произвођача. Међутим, у поступку инсталирања софтвера на свом компјутеру лиценца за коришћење се појавила на екрану његовог рачунара недозвољавајући му да софтвер инсталира пре него што прихвати све предочене услове његовог коришћења, што је он и урадио кликом на дугме *accept*. Отуда је суд закључио да је Zeidenberg правно обавезан лиценцим условима коришћења софтвера и да је на њих пристао. У супротном софтвер је могао вратити.

манифестује се путем типке или линка (тзв. *hyper link*) с натписом „слажем се“ или „да“ који се најчешће налазе у близини текста уговора, а којој изјави воље претходи питање да ли се прихватају сви наведени услови уговора.

Предметни уговори, који се понекад називају и *click through* или само *click* уговорима, почели су се користити када су продавци софтвере почели продавати интернетом и то путем *downloada*. Начелно овај тип уговора није донео ништа ново осим начина упознавања странака са садржином уговора. Реч је о посебној подврсти адхезионих уговора који се склапа на *web* страници електронским путем и у електронском облику и у којем купац (приступилац) у потпуности прихвата понуду уз услов да је претходно прегледао односно прочитао текст целог адхезионог уговора. Ови су уговори прихваћени у целом свету, а за њихову пуноважност постављају се више мање стандардизовани услови који се односе на посебност електронског облика односно електронског начина склапања уговора. То су по правилу следећи услови:

- 1) текст уговора који се склапа *online* мора бити приказан кориснику односно оном ко уговору приступа;
- 2) онај ко жели да приступи уговору не може кликнути на *I accept* пре него што му је пружена прилика да прегледа односно прочита цео уговор;
- 3) величина слова уговора мора бити прихватљива;
- 4) сви битни услови уговора морају бити видљиви и без хиперлинкова да би се приступило додатним условима уговора;
- 5) оном ко приступа уговору мора бити омогућено да прочита цео уговор, да га прегледа у целини као и да прегледа и прочита све услове уговора;
- 6) језички изрази свих услова и напомена везаних уз уговор морају бити разумљиви и јасни;
- 7) *Accept/Denial* дугмад морају бити на крају уговора;
- 8) дугмад за емитовање изјаве воље морају јасно изражавати *Accept* и *Decline*;

- 9) онај ко уговору приступа мора прихватити уговор кликом на дугме *Accept* пре него што му се омогућава да приступи предмету уговора или услузи;
- 10) клик на дугме *Decline* онемогућава приступ потенцијалном предмету уговора или услузи;
- 11) онај ко уговору приступа мора примити *online* конфирмирајућу поруку или страницу потврде своје наруџбенице или прихвата и мора имати могућност да исправи евентуалне грешке у својој наруџби или прихватању пре него што кликне дугме *Accept* или *Decline*;
- 12) електронски записи које саставља провајдер који и одржава *web* страницу на којој се приступа уговору мора садржати: а) поступак у којем је приступилац изразио свој пристап; б) верзију уговора која се примењује; в) идентификационе податке приступиоца; г) његов електронски пристап; д) потпуни текст сваке верзије;
- 13) пре дугмади *Accept/Decline* мора постојати текст⁸⁵ који ће на одговарајући начин упозорити потенцијалног приступиоца на последице његовог поступка.

5.4.3. Browse wrap уговори

За разлику од *click wrap* уговора *browse wrap* или *web wrap* уговори садрже линк или типку или какав други медиј унутар *web* странице којим се потенцијални саговорач упућује да целокупни садржај уговора који ће евентуално бити склопљен пронађе на другом месту или на другој *web* адреси. Дакле садржај *browse wrap* уговора у претежном је делу приказан на другој *web* страници или на удаљеној локацији од првобитне *web* странице (нпр. при дну дугачке *web* странице) на којој је потребно извршити изјаву

⁸⁵ По правилу тај текст гласи: „Please do read the terms and conditions of this agreement carefully. By clicking on the Accept button, below, you accept the terms and conditions of this agreement when you click the Accept button. If you do not accept all these terms, click on the Decline button and the end of this agreement. If you click on the Decline button you will have no access to product of service.“

воље за склапање уговора. Уобичајени текст код тих уговора је: „Ова продаја је регулисана уговором доступним овим линком. Кликом овог дугмета пристајете на услове уговора.“. Пракса је дакле да се на уговорне услове пристаје већ самим прегледавањем *web* странице без потребе било каквог изричитог и директног изјављивања о прихватању услова, осим самог прегледа *web* странице. Дакле изјава у смислу прихватања садржаја општег дела уговора на секундарној *web* страници даје се већ самим прегледом (*browsing*) примарне *web* странице на којој се склапа уговор.

Код ових уговора међутим није неопходно прочитати уговорне услове или се са њима сложити пре него што се може изјавити воља за склапањем уговора. Овде се заправо унапред и имплицитно претпоставља да се онај ко уговору приступа слаже са условима и одредбама уговора самим тим што претражује *web* страницу на којој се склапа уговор (примарна страница), без обзира на то прегледа ли он или улази на *web* страницу која садржи те уговорне услове и одредбе (секундарна страница). Овакву технику закључења уговора у свом пословању уобичајено користи америчка компанија *Dell Inc.*⁸⁶

Browse wrap уговор је врло сличан уговорима код којих су општи услови пословања инкорпорирани у сам текст уговора. Наиме, део уговора који је „дислоциран“ од странице на којој се уговор склапа садржи опште услове као оквир за појединачни уговор који се склапа на примарној страници. Отуда се у извесној мери овакви уговори показују као проблематични. Америчка правна доктрина и пракса им пружа правну заштиту али уз услове који се захтевају и код склапања *click wrap* уговора. На овај начин се води рачуна о правној заштити друге, по правилу економски инфериорније стране, потрошача.

⁸⁶ The following are terms of a legal agreement between you and Dell Inc (Dell). By accessing, browsing and/or using this site (Site), you acknowledge that you have read, understood, and agree, to be bound by these terms and comply with all applicable laws and regulation, including U.S. export and re-export control laws and regulation. If you do not agree of these terms, do not use this Site.

5.5. Потврда склапања уговора

Раније смо већ навели да је нашим Законом о електронској трговини баш као и највећим бројем других упоредних прописа предвиђена као посебна обавеза пружаоца услуга да без одлагања, посебном електронском поруком, потврди пријем електронске поруке која садржи понуду или прихват понуде за закључење уговора. И на основу члана 11. Упутства ЕУ о електронској трговини⁸⁷ прописано је следеће: „Државе чланице морају осигурати, осим ако се странке другачије не договоре и те странке нису потрошачи, да се у случајевима када прималац услуге доставља своју наруџбеницу електронским путем примењују следећа начела: давалац услуге треба потврдити пријем наруџбенице примаоца без непотребног одлагања електронским путем; наруџбеница и потврда пријема сматрају се примљеним када им странке којима су упућене могу приступити.“ Ово се правило експлицитно примењује управо на *click wrap* и *browse wrap* уговоре, а не примењује на уговоре склопљене путем електронске поште или путем других њој изједначених облика индивидуалне комуникације.

Питање које се у смислу претходно реченог може поставити је у каквом облику мора бити та порука ? Да ли би то морала бити *e-mail* порука или електронска порука слична електронској конклюдентној поруци односно знаку који остају као траг приликом изјаве воље дате електронским путем код склапања *web* уговора ?

Наш Закон о електронској трговини као ни остали упоредни прописи у овој области, како национални тако и међународни, не дају одговор на постављено питање. Могло би се ипак сматрати да би се овакава одредба, ако су понуђени или понудилац дали своју *e-mail* адресу, могла тумачити као обавеза упућивања *e-mail* поруке на предметну адресу. Ако назначења *e-mail* адресе нема, што и није законска обавеза потенцијалних уговорача, онда би порука потврде пријема морала бити послата с рачунара понудиоца односно онога ко је упутио позив на понуду на рачунар друге уговорне стране и при томе мора бити читљива у традиционалном језичком и писаном облику на екрану рачунара друге уговорне стране и подесна за меморисање на његовом рачунару, али и за штампање у традиционалном писаном облику.

⁸⁷ Упутство 2000/31/ЕС, L.178, 17/2000.

Још једно питање на које упоредни прописи о електронској трговини не дају експлицитан одговор је питање какав је значај потврде пријема електронске поруке која садржи понуду или прихват понуде за закључење уговора ? Другим речима може ли онај ко потврду о пријему односу прихвату пријема понуде није примио сматрати да друга страна његову изјаву воље није ни примила те да отуда ни уговор није настао ?

Имајући у виду законску терминологију која у овом делу говори о „потврди пријема“ могло би се закључити да електронска порука која садржи потврду пријема понуде односно прихвата понуде има декларативни, а не конститутивни значај. Она дакле нема непосредан утицај на настанак уговора али њен изостанак несумњиво представља кршење законске обавезе пружаоца услуге. Претходно поменуто Упутство ЕУ препушта државама чланицама да утврде санкције⁸⁸ за повреду одредаба националних прописа донетих у складу са тим Упутством. Мада је наш Закон о електронској трговини у потпуности усклађен са одредбама Упутства санкција за случај непоштовање обавезе слања потврде пријема је изостала.

5.6. Место одашиљања и пријема електронске поруке

Обзиром на то да се електронска порука односно електронска пошта могу послати у име и за рачун одређеног пошиљаоца с било којег места на свету правно релевантно може бити и питање одакле је таква порука упућена. Ово у истој мери важи и у погледу одређења места на којем је нека електронска порука примљена.

Могло би се рећи да упоредни прописи у овом погледу садрже више мање истоветна решења. Према *ICC Terms*⁸⁹ електронска порука се сматра упућеном или посланом из места у којем пошиљалац има пословно седиште, а сматра се примљеном на месту у којем адресат има своје пословно седиште. Истоветно становиште заступљено је и у нацрту UNCITRAL Конвенције о електронском склапању уговора.⁹⁰

⁸⁸ Члан 20. Упутства.

⁸⁹ Члан 2. став 2.3. *ICC e Terms 2004*, UNCITRAL, Working Group IV, A/CN.9/WG.IV/WP.113.

⁹⁰ Члан 10. Став 3. Нацрта Конвенције о електронском уговору; UN GA ACN./WG.IV/WP.108.

Према *Uniform Electronic Transactions Act of 1999* одређено је да ће се, у случају да није изричито другачије наведено у електронским записима или није изричито другачије договорено између примаоца и пошиљаоца, сматрати да је електронски запис послат из пошиљачевог пословног седишта, а примљен у примаачевом пословном седишту. Ако пошиљалац или прималац имају више од једног пословног седишта, пословним седиштем у смислу предметног прописа сматраће се оно које има најближу везу или однос са предметном трансакцијом. У случају пак да прималац или пошиљалац немају пословно седиште правно релевантним местом пријема сматраће се пребивалиште примаоца.

6. *E-mail* уговори

E-mail уговори су такви уговори код којих уговорне стране сагласност воља, понуду и прихват понуду, реализују електронским путем и то слањем писаних електронских порука. Дакле за разлику од *web* уговора, код којих се сматра да будући уговарачи своју вољу изјављују знацима односно конклюдентним радњама, овде је реч о писменој форми изражавања воље за закључивање уговора. По томе се *e-mail* уговори не разликују од било којих других уговора код којих се писмена форма користи као начин емитовања понуде и прихвата понуде, рецимо уговора закључених разменом писмена путем класичне поште, телефакса или, у новије време, уговора закључених путем писаних телефонских порука, тзв. SMS уговора.

Ови се уговори по својим бројним карактеристикама разликују од *web* уговора о којима је претходно било речи. Те разлике ћемо у наредном делу навести:

прво, *e-mail* уговори нису типични потрошачки уговори, као што су то *web* уговори. Они се у сфери електронске трговине не појављују масовно и у великом броју као *web* уговори, реч је по правилу о уговорима који се закључују између већ познатих лица и то најчешће привредних субјеката између којих већ постоји неки вид пословне сарадње;

друго, претходно речено упућује и на то да понуда за закључење *e-mail* уговора која се емитује коришћењем електронске поште никада није општа понуда, дакле никада у овом смислу неће бити реч о понуди упућеној

унапред неодређеном броју лица. То разуме се не значи да таква понуда мора бити упућена само једном лицу, напротив. Међутим, она је увек упућена одређеним лицима, једном или више њих, обзиром да пошиљалац понуде то чини упућивањем електронске поруке на тачно одређену односно тачно одређене *e-mail* адресе;

треће, за разлику од *web* уговора *e-mail* уговори не спадају (по правилу) у адхезионе уговоре. Ово наравно не значи да и закључивање уговора путем слања *e-mail* порука не може бити коришћено тако што ће понудилац понуђеном послати унапред дефинисан текст уговора којем овај може приступити или не, без могућности да о предложеним уговорним условима уопште преговора. Али у сваком случају закључење адхезионих уговора није општа карактеристика уговора закључених путем електронске поште. Управо супротно, потенцијални уговарачи најчешће размењују низ електронских порука у којима се споразумевају, дакле преговарају о свим битним елементима уговора који би закључили, која могућност је код *web* уговора углавном или у потпуности искључена;

четврто, код *e-mail* уговора дилема о томе да ли се активност пошиљача електронске поруке сматра понудом или позивом на понуду, присутна код *web* уговора, углавном не постоји. Правило је наиме да онај ко шаље електронску пошту има својство понудиоца те да прималац електронске поште такву понуду у целини и безусловно може прихватити, што практично значи да се он најчешће налази у улози понуђеног. Уколико пак понуђени понудиоцу узврати електронску поруку слањем писменог предлога да се приспела понуда измени на било који начин и у било ком делу онда он, сходно општем правилу облигационог права, „преузима“ улогу понудиоца. Претходно речено свакако не значи да слање електронске поште не може бити употребљено и као техника за позивање примаоца електронске поште на стављање понуде. То ће бити случај увек када пошиљалац поруке упућене путем електронске поште адресату на његову *e-mail* адресу пошаље каталог, ценовник, тарифу и друга обавештења, као и оглас којим поступањем га заправо позива да му овај, под објашњеним односно објављеним условима, упути понуду. Мада овакав начин пословања више није редак у сфери електронске трговине, када трговачки ланци и компаније на велики број *e-mail* адреса шаљу тзв. нетражене електронске поруке које по својој правној суштини најчешће јесу позиви на понуду, не би могли рећи да је то карактеристика уговора закључених путем електронске поште;

пето, што се тиче питања места закључења уговора и код *e-mail* уговора важи опште правило да се уговор сматра закљученим у месту у којем је понудилац имао своје пословно седиште (пребивалиште) у моменту слања понуде за закључење уговора. Ово практично значи да овлашћено лице неке компаније понуду за закључење уговора слањем електронске поште може упутити са било којег рачунара у свету али да ће као место закључења уговора увек бити место пословног седишта компаније у чије име је понуда за закључење уговора упућена;

шесто, када је реч о томе да ли се уговор закључен путем електронске поште сматра уговором закљученим између одсутних или присутних лица ту ставови, ни када се ради о правној теорији а још мање позитивним прописима, нису довољно искристалисани. Према неким мишљењима на уговоре закључене путем електронске поште треба примењивати правила о закључењу уговора између одсутних лица. Овакво је становиште рецимо присутно у Немачкој и то не само када је реч о уговорима закљученим путем електронске поште већ и када је реч о *web* уговорима. Са друге стране постоје и такви ставови сходно којима се код склапања уговора путем електронске поште полази од претпоставке склапања уговора између присутних лица, која је раније примењивана на комуникацију путем телекса. Електронска пошта је заиста једнако брза као што су то телекс или телефакс али прималац електронске поште не добија обавезно сигнал о пријему поруке, као што га добија прималац телекса, телефакса или телефонске SMS поруке. Коначно, чак и да обавезан сигнал о приспећу електронске поште и постоји јавља се могућност да прималац поруке упућене електронском поштом добије поруку у време када је одсутан, рецимо ноћу, ван радног времена, па се јавља временски размак између слања и пријема поруке од стране лица којем је она упућена. Имајући у виду чињеницу да слање *e-mail* порука не омогућава интерактивну комуникацију између пошиљаоца и адресата те да је време пријема поруке од стране онога коме је она упућена тешко прецизно утврдити право је и у овом случају „принуђено“ да користи одређене претпоставке које су у крајњој линији битне за одређивање времена закључења уговора. Ако се рецимо пође од претпоставке да *mailbox* неке компаније представља заправо електронско поштанско сандуче у које поруке са ма ког краја света стижу у времену мерљивом минутима разумљиво је да ће компанија бити у обавези да своју пошту чита најмање један пут дневно, за време радног времена. Произилази да би дан електронског одашиљања

поруке био у исто време и дан када је прималац такву поруку примом к знању. Изузетно, у случају релевантне временске разлике између места отпослања и места пријема поруке, односно у случају пријема поруке ван радног времена, сматрало би се да је она примљена првог наредног радног дана. Ово би правило, разуме се, тешко било примењиво када је реч о односима између физичких лица.

У сваком случају чини се прихватљивим за све врсте електронске комуникације које омогућавају тренутно саопштавање порука односно њихово слање и пријем у врло кратком временском периоду претпоставити да се ради о уговорима закљученим између присутних лица у погледу времена њиховог закључења, изузев уколико посебне околности случаја не упућују на нешто друго.

7. Електронско плаћање – електронски пренос средстава

7.1. Уводне напомене о електронском плаћању

Нису ретка мишљења према којима је електронско плаћање најпогоднија форма за примену електронике, што се опет образлаже чињеницом да је у оквиру банкарства постигнут највећи продор у примени електронских технологија. И то не само између банака односно између банака и привредних субјеката већ у истој мери између банака и физичких лица, потрошача. Више да готово нема банке која *www* не користи као средство за маркетинг, а све се више како по врсти тако и по броју трансакција користе разни облици новчаних трансакција везаних за бројне врсте банкарских услуга. С тим у вези посебно ваља имати у виду све присутнију могућност коришћења тзв. електронског новца, електронских чекова и наравно кредитних картица. Да би банке пословале електронски потребно је да користе стандарде које им омогућавају слање порука у структурираној форми. На међународном плану то су UN/EDIFACT стандарди.

Електронско плаћање није једноставно дефинисати. У смислу Европског кодекса у области електронског плаћања из 1987. године под овим појмом се подразумевају све платне трансакције које се обављају платним картицама са магнетном траком или микрочипом на електронским платним терминалима (ЕРТ) или терминалима на месту продаје (POS - *Point Of Sale*).

Према Моделу Закона UNCITRAL о међународном преносу средстава из 1992. године, који се додуше примењује на преносе средстава када се било која банка пошиљалац и њена банка прималац налазе у различитим државама, „пренос средстава“ означава серију послова који почињу са налогом за плаћање налогодавца који је сачињен у циљу стављања средстава на располагање кориснику. Израз обухвата било који налог за плаћање који изда банка налогодавца или било која банка посредник са намером да изврши налог за плаћање налогодавца. Налог за плаћање који је издат за сврхе реализације плаћања таквог налога сматраће се као део различитог преноса средстава.

Чини нам се да је у смислу начелног одређења појма електронског плаћања сасвим одговарајућа дефиниција садржана у нашем Закону о платном промету сходно којој се електронским означава начин преноса налога за плаћање и других података у трансакцији плаћања - телекомуникацијски или физичком испоруком трака, дискета и сличних носилаца података.⁹¹

Још шире, у смислу Одлуке о електронском начину обављања платног промета електронски платни промет се обавља разменом електронских порука кроз информационе системе учесника у трансакцији плаћања. При томе се под електронском поруком разуме информација која је електронски генерисана, послата, проверена, примљена и сачувана електронски (електронски налог за плаћање или други финансијски документ).⁹² У овом контексту се, сходно предметној Одлуци, електронски пренос новчаних средстава између клијената у платном промету сматра електронском платном трансакцијом.

У сваком случају се сматра да је први електронски трансфер новца извршен још далеке 1860. године у САД, а посредством телеграфа који је за потребе свог пословања користила компанија *Western Union*. Нешто касније, 1918. године, је у истој земљи формиран и први сервис (FEDWIRE) за телеграфско слање новца, а крајем 60-их година прошлога века формирају се

⁹¹ Члан 2. Тачка 23. Закона о платном промету РС (Сл.лист СРЈ 03/02; 05/03).

⁹² Одлука о електронском начину обављања платног промета, тачке 2 и 3, Сл. гласник РС 57/04.

и одговарајуће радне групе стручњака различитих опредељења чији је посао био унапређење техника и метода размене новца без употребе папира. Но ван сваке сумње до „експлозије“ у погледу коришћења електронског плаћања односно електронског трансфера новца долази упоредо са појавом и развојем интернета односно његовим увођењем у област пословних, пре свега банкарских трансакција.

Примарни циљ увођења система електронског плаћања је био решавање проблема плаћања заснованих на папиру, а коришћењем упоредних предности које пружају савремене информационе технологије. Пракса је међутим врло брзо показала да увођење система електронског плаћања значи много више од саме замене папирних докумената и да доноси више мање потпун реинжењеринг пословних процеса.

Имајући у виду да су основни пословни субјекти преко којих се обавља процес електронских плаћања банке неопходно је у контексту општих разматрања о питањима електронског преноса средстава рећи понешто и о основним појмовима важним за функционисање тзв. електронског банкарства.

7.2. Електронско банкарство

Под електронским банкарством се у најширем смислу разуме процес вршења банкарских послова електронским путем. У зависности од врсте електронских технологија које се користе при обављању банкарских послова разликују се:

а) *телефонско банкарство*, које се појавило 70-их година прошлога века и омогућило директно коришћење банкарских услуга путем телефонске мреже и то директном телефонском везом са службеником банке или са банковним рачунаром;

б) *интранет банкарство*, које омогућава обављање банкарских трансакција директном везом клијента и банке уз помоћ специјализованог софтвера инсталираног на клијентовом рачунару;

в) од почетка 90-их година двадесетог века са развојем почиње и *интернет банкарство* где је приступ банкарским услугама могућ са сваког места на свету где постоји рачунар прикључен на интернет;

г) коначно, најновији тренд у развоју електронског банкарства је тзв. *мобилно банкарство* обзиром да нове генерације мобилних телефона омогућавају коришћење интернета. Још од 1999. године више од 90 % банака у Европи већ нуди неке од услуга мобилног банкарства.

Разуме се, за функционисање електронског плаћања и посебно у тим оквирима функционисање електронског банкарства, неопходно је било у употребу увести и основне инструменте односно средства за обављање финансијских трансакција у електронској форми. Отуда су у контексту разматрања о електронском банкарству посебно битни појмови електронског новца, платних и паметних картица и електронског чека.

Електронски или дигитални новац (*electronic money, digital cash*) се дефинише као монетарна информација која се електронским путем у реалном времену преноси између трансактора који обављају плаћања. Овај пренос, који заправо и омогућава куповину роба и услуга помоћу рачунара, врши се како у оквиру комерцијалних рачунарских мрежа (интернет) тако и у оквиру пословних банкарских односно међубанкарских мрежа (*SWIFT*). Постоје у основи два облика електронског новца. Први је облик заснован на картицама (*Mondex, Visa Cash...*) где се плаћање врши у продавницама које имају одговарајуће терминале који аутоматски скидају одређени износ са картице и тај износ одобравају продавцу. Други је облик тзв. мрежни новац (*Network Money, Cybercash...*) где се трансфер врши преко телекомуникационих мрежа, углавном интернета, а између рачунара (софтвера) који припадају различитим корисницима.

Платне картице, које могу бити кредитне и дебитне, су инструменти безготовинског плаћања и инструменти подизања новца код издаваоца картице или посредством банкомата. Поред података о кориснику и издавачу, који су утиснути у парче пластике, платне картице садрже и магнетни медиј који је у облику траке нанесен на површину картице. Тај медиј такође садржи податке о кориснику картице, његове личне податке, број рачуна и друге податке. Процес плаћања са оваквим картицама се врши тако што корисник стави своју картицу у уређај помоћу којег се врши плаћање, уноси свој PIN (*Personal Identification Number*) ако је у питању дебитна картица, а потом уређај „прочита“ број корисниковог рачуна и успоставља електронску везу са централним рачунаром који врши верификацију података о рачуну. На сличан начин, укуцавањем захтеваних података са кредитне односно дебитне

картице, омогућено је плаћање роба и услуга које се наручују преко интернета. У овом случају заправо имаоци кредитне картице у одговарајућа поља на *web* сајту продавца укуцавају број картице, њену валидност односно датум од када кредитна картица важи као и тзв. CVV2 број (*Card Verification Value 2*), што је троцифрени број који се налази на полеђини картице.⁹³

Паметне или смарт картице (*smart card, intelligent card*), које су по изгледу готово идентичне платним картицама, садрже микро чип односно интегрисано коло што је у суштини микропроцесор са меморијским капацитетом у који се могу потхранити одређене информације. Управо у зависности од врсте уграђеног чипа ове картице се могу делити на меморијске, процесорске или комбиноване. Сигурност и безбедност употребе ових картица све их више намеће као потпуну алтернативу картицама са магнетним медијима.

Електронски чек (*eCheck*) није ништа друго него чек у електронској форми. Несумњиво је да би његово шире увођење у област банкарског пословања донело бројне уштеде али и друге погодности које иначе пружа електронско пословање. Са друге стране ова форма пословања захтева и велике инвестиције у додатну инфраструктуру не само на страни банака и корисника електронског чека већ и на страни трговаца односно понуђача роба и услуга. Отуда његова употреба ни из далека није на нивоу употребе пластичних картица али се свакако може очекивати да ће и овај вид електронског плаћања у будућности бити значајно присутан у сфери банкарског пословања.

Бројне погодности које коришћење услуга електронског банкарства пружа утицале су на то да данас готово и не постоје банке које својим клијентима, како пословним субјектима тако и физичким лицима, не нуде широк спектар услуга електронског банкарства. Масовност коришћења система електронског плаћања отвара разумљиво питање сигурности и безбедности таквог вида пословања. И овде се свакако може говорити о различитим нивоима „заштите“, како оним техничким, организационим тако

⁹³ Опасност од крађе података о кредитним картицама и њиховим власницима не појављује се само као опасност крађе из базе података електронских продавница. Пракса је наиме показала да се такви подаци краду на неколико начина, а да су најраспрострањенији: слање нежељених порука (*spam*), пецање (*phishing*) и фарминг (*pharming*).

и правним. На овом месту предмет нашег интересовања су правне мере и механизми заштите у вези са електронским преносом средстава.

7.3. Правни инструменти заштите у вези са електронским преносом средстава

Као и код свих осталих преноса података односно размене информација у електронској форми и приликом електронских плаћања су могуће злоупотребе, грешке и преваре. Статистика указује да су грешке најчешће последица грешке човека који користи рачунар али је разуме се могуће да до грешака у преносу дође услед техничке неисправности опреме, како софтвера тако и хардвера. Грешке се најчешће манифестују као оне у погледу личности односно оне у погледу износа који треба трансферисати са једног рачуна на други. Ако је пак реч лажним налозима за плаћање они такође могу бити последица различитих узрока. То рецимо може бити околност да је налог за плаћање дало неовлашћено лице, или га је дало овлашћено лице али је сам налог у току преноса измењен. Због наведених али и бројних других опасности и у електронском трансферу новца посебну важност имају утврђивање веродостојности пошиљаоца, поруке и примаоца.

Имајући у виду околност да се читав процес електронског преноса средстава може у општем смислу посматрати као процес размене информација (података) - видели смо претходно да и електронски новац по свом одређењу није ништа друго него „монетрана информација“ - поставља се питање захтева ли овај вид електронског пословања неку посебну правну регулативу или су на област електронских плаћања примењива више мање сва она правна правила везана за пренос података и склапање уговора у електронској форми. Имајући пре свега у виду упоредно правна искуства у овом смислу се не може дати линерана одговор.

Наиме, правна и технолошка природа информација које се размењују при електронском преносу средстава несумњиво упућују на то да се и на ову област могу применити углавном сви прописи о којима смо претходно говорили када је реч о електронској трговини. Рецимо: прописи о закључењу и важности уговора односно других докумената у електронској форми, прописи о електронском потпису и многи други. И поред тога неке државе и у области електронског преноса средстава доносе посебне прописе, оне који

се односе само на ту материју. То је случај са САД где је још 1978. године усвојен Закон о електронском преносу средстава (*Electronic Funds Transfer Act / EFTA*) који се користи у домаћем банкарском саобраћају. Нешто касније, 1989. године, извршена је и допуна Једнообразног трговачког законика правилима која се односе на електронски пренос средстава. Коначно, 1999. године Национална конференција комисионара за унификацију права држава чланица (*National Conference of Commissioners on Uniform State Laws*) и Амерички правни институт (*American Law Institute*) предложили су државама чланицама за усвајање и Јединствени закон о електронским трансакцијама (*Uniform Electronic Transactions Act – UETA*). Овај Закон ипак није у целини посвећен питањима електронског трансфера средстава већ се примењује на све односе између две или више особа које су повезане са пословним, трговачким или владиним активностима.

Не може се међутим рећи да је пример САД типичан и он има своје „оправдање“ пре свега у чињеници да се у овој земљи електронски пренос средстава у пракси појавио прилично рано што је, у недостатку других одговарајућих прописа, захтевало његово правно уређење посебним законом. Другим речима највећи број држава на свету нема посебне прописе који се односе искључиво на област електронског преноса средстава. То је случај и са нашом државом. Србија дакле нема посебан пропис којим је област електронског преноса средстава уређена па се тако на све трансакције и уговоре тог типа могу примењивати Закон о електронској трговини и Закон о електронском потпису. Додуше и неки други закони могу бити и јесу релевантни у овом погледу, као што су рецимо Закон о платном промету, Закон о банкама и Закон о Народној банци Србије.

У исто време може се приметити да је на међународном плану присутан приличан број прописа који се у целини односе на питање електронског трансфера средстава односно неке од облика електронског трансфера средстава.

Тако је рецимо у оквиру Комисије УН за међународно трговинско право (UNCITRAL) још 1987. године усвојен Правни водич о електронском преносу средстава (*UNCITRAL Legal Guide on Electronic Funds Transfer – EFT*). Према овом документу електронски пренос средстава је термин који се користи да би се њиме указало да је пренос извршен електронским путем. Постоје преноси о одобрењу (*credit transfer*) и задужењу (*debit transfer*).

Водич детаљно разматра питања преноса средстава и с тим у вези посебно споразум о преносу средстава и упутстава за пренос, преваре, грешке, неправилно руковање упутствима за пренос и одговорност с тим у вези, питање „коначности“ (када се сматра да је пренос завршен), као и нека друга правна питања везана за пренос средстава.

Питање „коначности“ електронског потписа је изузетно важно код електронског преноса најпре због брзине којом се тај пренос врши односно што се за њега везују одређена права и обавезе повериоца и дужника у правном односу који настаје поводом електронског трансфера. Отуда није необично што су у Водичу посебно обрађена питања када се сматра да је пренос коначан, однос између коначности преноса између потрошача и коначност преноса између банака, последице повезане са коначности као и ризик везан за питање коначности.

Од других међународних правила која се односе на ову материју важно је поменути: Модел закон UNCITRAL о међународном преносу средстава из 1992. године; Конвенцију УН о независним гаранцијама и *stand by* акредитивима из 1995. године; Правила Међународне трговинске коморе о *stand by* акредитивима из 1998. године; Препоруке Комисије ЕУ у вези са трансакцијама које се обављају електронским инструментима плаћања и посебно у вези са односом између издаваоца и имаоца из 1997. године.

Прва три претходно поменута документа посебну пажњу посвећују питању заштите код електронског преноса. Тако се у Моделу закона UNCITRAL, који се примењује на преносе средстава када се било која банка пошиљалац и њена банка прималац налазе у различитим државама, наводи да аутентификација представља споразумом утврђен поступак којим се одређује да ли је један налог за плаћање, налог за његову измену или опозив, издало лице које је наведено као пошиљалац.⁹⁴ У Конвенцији УН о независним гаранцијама и *stand by* акредитивима је, између осталог, наведено да јемство може бити дато у било ком облику којим се обезбеђује потпуна забелешка текста јемства и аутентичност његовог извора на основу општеприхваћених начина или поступака са којима су се сложили гарант/издавалац и корисник. У Правилима МТК су обрађена питања електронског записа, провере аутентичности, електронског потписа и пријема. У вези са провером

⁹⁴ Члан 2 (i) Модела закона.

аутентичности наводи се да је то провера електронског записа општеприхваћеним поступком у комерцијалној пракси којим се утврђује идентитет пошиљаоца или извора и целовитост или грешке у преносу садржаја информације. Даље се наводи да је критеријум за процену интегритета информација то да ли је информација остала потпуна и неизмењена, осим додатака било каквог индосирања или било какве измене која настане у уобичајеном току комуникације, чувања и приказивања. Према дефиницији електронски потпис су слова, ознаке и бројеви или други симболи у електронском облику који су додати или су логички повезани са електронским записом који је потписала или усвојила једна од страна са намером да електронски запис учини аутентичним. У погледу пријема сматра се да је он учињен када електронски запис уђе у информациони систем као такав одређен у *stand by* акредитиву и то у облику који тај информациони систем може обрадити или када издавалац врати електронски запис послат у информациони систем различит од система који је издавалац одредио. О аутентичности порука говори се и на другим местима ових Правила.

Посебну важност имају и претходно поменуте Препоруке Комисије ЕУ из 1997. године. Њима се обрађују питања транспарентности услова за трансакције, обавезе и одговорност уговорних страна, обавештавање, решавање спорова и друга важна питања. Обавеза обавештавања за случај губитка или крађе електронског инструмента плаћања подразумева да издавалац (или субјект кога он одреди) по пријему обавештења мора да предузме све разумне мере које му стоје на располагању да заустави свако даље коришћење електронског инструмента плаћања.

Погодности које електронски трансфер средстава пружа постале су јако брзо прихваћене од стране физичких лица односно потрошача који, не одлазећи у банку, могу преко својих рачунара дати налог да се одређени износи уплате на одређене рачуне. Уобичајено се сматра да је истинска револуција у електронском преносу средстава и настала оног тренутка када је потрошач могао да коришћењем интернета наручује и плаћа жељене производе и услуге.

Разуме се да је и ова област банкарског пословања захтевала одређену правну регулативу. Од низа директива и других правила усвојених на нивоу ЕУ којим се штите права потрошача помињемо Директиву Европског парламента из 1997. године о заштити потрошача у вези са дистанционим

уговорима. Њоме се предвиђа право потрошача да опозове сваки дистанциони уговор у року од 7 радних дана и то без санкција и без давања било каквог образложења. Ова врста уговора је постала актуелна нарочито када су многе фирме почеле да рекламирају своју робу преко интернета, а потрошачи да је наручују „на невиђено“.

Поменимо на самом крају још један пропис релевантан за област електронског трансфера средстава који је донет у оквиру МТК. Реч је о Додатаку Једнообразним правилима и обичајима за документарне акредитиве за електронску презентацију. Овај Додатак није ревизија Једнообразних правила, он се користи уз та Правила и омогућава презентацију документарног акредитива у електронској форми. Прва верзија Додатака ступила је на снагу 2002. године, а примењивала се уз ревизију Једнообразних правила из 1993. године (МТК 500). Друга верзија Додатака ступила је на снагу 2007. године и она се примењује као додатак ревизији Једнообразних правила из 2006. године (МТК 600).

ЗАКОН О ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ

(Службени гласник РС 97/08)

I. ОСНОВНЕ ОДРЕДБЕ

Предмет закона

Члан 1.

Овим законом се уређују услови за прикупљање и обраду података о личности, права лица и заштита права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденција, изношење података из Републике Србије и надзор над извршавањем овог закона.

Заштита података о личности обезбеђује се сваком физичком лицу, без обзира на држављанство и пребивалиште, расу, године живота, пол, језик, вероисповест, политичко и друго уверење, националну припадност, социјално порекло и статус, имовинско стање, рођење, образовање, друштвени положај или друга лична својства.

Послове заштите података о личности обавља Повереник за информације од јавног значаја и заштиту података о личности (у даљем тексту: Повереник), као самосталан државни орган, независан у вршењу своје надлежности.

Циљ закона

Члан 2.

Циљ овог закона је да, у вези са обрадом података о личности, сваком физичком лицу обезбеди остваривање и заштиту права на приватност и осталих права и слобода.

Значење израза у овом закону

Члан 3.

Поједини изрази у овом закону имају следеће значење:

1) Податак о личности је свака информација која се односи на физичко лице, без обзира на облик у коме је изражена и на носач информације (папир, трака, филм, електронски медиј и сл), по чијем налогу, у чије име, односно за чији рачун је информација похрањена, датум настанка информације, место похрањивања информације, начин сазнавања информације (непосредно, путем слушања, гледања и сл, односно посредно, путем увида у документ у којем је информација садржана и сл), или без обзира на друго својство информације (у даљем тексту: податак);

2) Физичко лице је човек на кога се односи податак, чији је идентитет одређен или одредив на основу личног имена, јединственог матичног броја грађана, адресног кода или другог обележја његовог физичког, психолошког, духовног, економског, културног или друштвеног идентитета (у даљем тексту: лице);

3) Обрада података је свака радња предузета у вези са подацима као што су: прикупљање, бележење, преписивање, умножавање, копирање, преношење, претраживање, разврставање, похрањивање, раздвајање, укрштање, обједињавање, уподобљавање, мењање, обезбеђивање, коришћење, стављање на увид, откривање, објављивање, ширење, снимање, организовање, чување, прилагођавање, откривање путем преноса или на други начин чињење доступним, прикривање, измештање и на други начин чињење недоступним, као и спровођење других радњи у вези са наведеним подацима, без обзира да ли се врши аутоматски, полуаутоматски или на други начин (у даљем тексту: обрада);

4) Орган власти је државни орган, орган територијалне аутономије и јединице локалне самоуправе, односно други орган или организација којој је поверено вршење јавних овлашћења;

5) Руковалац података је физичко или правно лице, односно орган власти који обрађује податке (у даљем тексту: руковалац);

6) Збирка података је скуп података који се аутоматизовано или неаутоматизовано воде и доступни су по личном, предметном или другом основу, независно од начина на који су похрањени и места где се чувају;

7) Корисник података је физичко или правно лице, односно орган власти, који је законом или по пристанку лица овлашћен да користи податке (у даљем тексту: корисник);

8) Обрађивач података је физичко или правно лице, односно орган власти, коме руковалац на основу закона или уговора поверава одређене послове у вези са обрадом (у даљем тексту: обрађивач);

9) Писмени облик подразумева и електронски облик, под условима из закона којим се уређује електронски потпис;

10) Централни регистар збирки података (у даљем тексту: Централни регистар) је евиденција коју чини регистар збирки података и каталог збирки података коју води Повереник.

Примена закона

Члан 4.

Одредбе овог закона примењују се на сваку аутоматизовану обраду, као и на обраду садржану у збирци податка која се не води аутоматизовано.

Подаци на које се закон не примењује

Члан 5.

Осим ако очигледно претежу супротни интереси лица, поједине одредбе овог закона о условима за обраду, као и о правима и обавезама у вези са обрадом не примењују се на обраду:

- 1) података који су доступни свакоме и објављени у јавним гласилима и публикацијама или приступачни у архивама, музејима и другим сличним организацијама;
- 2) података који се обрађују за породичне и друге личне потребе и нису доступни трећим лицима;
- 3) података који се о члановима политичких странака, удружења, синдиката, као и других облика удруживања обрађују од стране тих организација, под условом да члан да писмену изјаву да одређене одредбе овог закона не важе за обраду података о њему за одређено време, али не дуже од времена трајања његовог чланства;
- 4) података које је лице, способно да се само стара о својим интересима, објавило о себи.

Обрада у историјске, статистичке или научноистраживачке сврхе

Члан 6.

Подаци прикупљени и обрађивани у друге сврхе могу да се обрађују искључиво у историјске, статистичке или научноистраживачке сврхе, ако не служе доношењу одлука или предузимању мера према одређеном лицу уз обезбеђивање одговарајућих мера заштите.

Мере заштите података који се архивирају у искључиво историјске, статистичке или научноистраживачке сврхе уређују се посебним прописом.

Руковалац одређен посебним прописом

Члан 7.

Ако посебан пропис уређује сврху и начин обраде, руковалац може да се одреди тим прописом.

II. УСЛОВИ ЗА ОБРАДУ

Недозвољеност обраде

Члан 8.

Обрада није дозвољена ако:

- 1) физичко лице није дало пристанак за обраду, односно ако се обрада врши без законског овлашћења;

- 2) се врши у сврху различиту од оне за коју је одређена, без обзира да ли се врши на основу пристанка лица или законског овлашћења за обраду без пристанка;
- 3) сврха обраде није јасно одређена, ако је измењена, недозвољена или већ остварена;
- 4) је лице на које се подаци односе одређено или одредиво и након што се оствари сврха обраде;
- 5) је начин обраде недозвољен;
- 6) је податак који се обрађује непотребан или неподесан за остварење сврхе обраде;
- 7) су број или врста података који се обрађују несразмерни сврси обраде;
- 8) је податак неистинит и непотпун, односно када није заснован на веродостојном извору или је застарео.

Одлука помоћу аутоматизоване обраде

Члан 9.

Одлука која производи правне последице за лице или погоршава његов положај, не може бити искључиво заснована на подацима који се обрађују аутоматизовано и који служе оцени неког његовог својства (радне способности, поузданости, кредитне способности и сл).

Одлука из става 1. овог члана може се донети када је то законом изричито одређено, односно када се усваја захтев лица у вези са закључењем или испуњењем уговора, уз спровођење одговарајућих мера заштите.

У случају из става 2. овог члана лице мора бити упознато са поступком аутоматизоване обраде и начином доношења одлуке.

Обрада са пристанком

Члан 10.

Пуноважан пристанак за обраду може дати лице, након што га руковалац претходно обавести у смислу одредбе члана 15. овог закона.

Пуноважан пристанак лице може дати писмено или усмено на записник.

Пристанак се може дати преко пуномоћника.

Пуномоћје мора бити оверено, изузев ако законом није прописано друкчије.

Пристанак за лице које није способно за давање пристанка даје законски заступник или старалац.

Пристанак за обраду података о лицу које је умрло могу дати супружник, деца са навршених 15 година живота, родитељи, браћа и сестре, односно законски наследник или лице које је за то одредио умрли.

Опозив пристанка

Члан 11.

Пристанак се може опозвати.

Пуноважан опозив лице може дати писмено или усмено на записник.

У случају опозива, лице које је дало пристанак дужно је да руковаоцу накнади оправдане трошкове и штету, у складу са прописима који уређују одговорност за штету.

Обрада података је недозвољена после опозива пристанка.

Обрада без пристанка

Члан 12.

Обрада без пристанка је дозвољена:

- 1) да би се остварили или заштитили животни важни интереси лица или другог лица, а посебно живот, здравље и физички интегритет;
- 2) у сврху извршења обавеза одређених законом, актом донетим у складу са законом или уговором закљученим између лица и руковаоца, као и ради припреме закључења уговора;
- 3) у другим случајевима одређеним овим законом или другим прописом донетим у складу са овим законом, ради остварења претежног оправданог интереса лица, руковаоца или корисника.

Обрада од стране органа власти

Члан 13.

Орган власти обрађује податке без пристанка лица, ако је обрада неопходна ради обављања послова из своје надлежности одређених законом или другим прописом у циљу остваривања интереса националне или јавне безбедности, одбране земље, спречавања, откривања, истраге и гоњења за кривична дела, економских, односно финансијских интереса државе, заштите здравља и морала, заштите права и слобода и другог јавног интереса, а у другим случајевима на основу писменог пристанка лица.

Прикупљање података

Члан 14.

Подаци се прикупљају од лица на које се односе и од органа управе који су законом овлашћени за њихово прикупљање.

Подаци се могу прикупљати и од другог лица ако:

- 1) је то предвиђено уговором закљученим са лицем на које се подаци односе;
- 2) је то прописано законом или другим прописом донетим у складу са законом;
- 3) је то неопходно с обзиром на природу посла;
- 4) прикупљање података од самог лица на које се односе захтева прекомерни утрошак времена и средстава;
- 5) се прикупљају подаци ради остварења или заштите животно важних интереса лица на које се односе, посебно живота, здравља и физичког интегритета.

Обавештавање о обради

Члан 15.

Руководилац који податке прикупља од лица на које се односе, односно од другог лица, пре прикупљања, упознаће лице на које се подаци односе, односно друго лице о:

- 1) свом идентитету, односно имену и адреси или фирми, односно идентитету другог лица које је одговорно за обраду података у складу са законом;
- 2) сврси прикупљања и даље обраде података;
- 3) начину коришћења података;
- 4) идентитету лица или врсти лица која користе податке;
- 5) обавезности и правном основу, односно добровољности давања података и обраде;
- 6) праву да пристанак за обраду опозове, као и правне последице у случају опозива;
- 7) правима која припадају лицу у случају недозвољене обраде;
- 8) другим околностима чије би несаопштавање лицу на које се односе подаци, односно другом лицу било супротно савесном поступању.

Обавеза из става 1. овог члана не постоји када такво упознавање, с обзиром на околности случаја, није могуће или је очигледно непотребно, односно непримерено, а нарочито ако је

лице на које се односе подаци, односно друго лице већ упознато са тиме или ако лице на које се подаци односе није доступно.

Руковалац који је податке о лицу прикупио од другог лица, упознаће са условима из става 1. овог члана, лице на које се подаци односе, без одлагања или најкасније при првој обради, осим када такво упознавање, с обзиром на околности случаја, није могуће, односно захтева прекомерни утрошак времена и средстава или је очигледно непотребно, а нарочито ако је лице на које се односе подаци већ упознато са тиме, односно ако лице на које се подаци односе није доступно или ако је прикупљање и даља обрада података од другог лица прописана законом.

У случају из става 3. овог члана, руковалац је дужан да обавести лице на које се подаци односе чим то постане могуће, односно ако лице то захтева.

Упознавање из става 1. овог члана врши се у писменом облику у случају када се за пристанак за обраду даје у писменом облику, осим ако лице на које се подаци односе, односно друго лице, пристане на усмено упознавање.

Руковалац ће обавестити лице на које се подаци односе и корисника о измени, допуни или брисању података без одлагања, а најкасније у року од 15 дана од дана измене, допуне или брисања података.

Нарочито осетљиви подаци

Члан 16.

Подаци који се односе на националну припадност, расу, пол, језик, вероисповест, припадност политичкој странци, синдикално чланство, здравствено стање, примање социјалне помоћи, жртву насиља, осуду за кривично дело и сексуални живот могу се обрађивати на основу слободно датог пристанка лица, осим када законом није дозвољена обрада ни уз пристанак.

Изузетно, подаци који се односе на припадност политичкој странци, здравствено стање и примање социјалне помоћи, могу се обрађивати без пристанка лица, само ако је то законом прописано.

У случају из ст. 1. и 2. овог члана, обрада мора бити посебно означена и заштићена мерама заштите.

У случају из ст. 1. и 2. овог члана, Повереник има право увида у податке и провере законитости обраде по службеној дужности или по захтеву лица, односно руковооца.

Начин архивирања и мере заштите података из ст. 1. и 2. овог члана, уз претходно прибављено мишљење Повереника, уређује Влада.

Пристанак за обраду нарочито осетљивих података

Члан 17.

Пристанак за обраду нарочито осетљивих података даје се у писменом облику, који садржи ознаку податка који се обрађује, сврху обраде и начин његовог коришћења.

Ако давалац пристанка није писмен или из другог разлога није у стању да пристанак својеручно потпише, пристанак је пуноважан ако два сведока својим потписима потврде да писмено садржи изјаву воље даваоца пристанка.

Опозив пристанка за обраду нарочито осетљивих података

Члан 18.

У случају опозива, лице које је дало пристанак дужно је да руковоацу накнади оправдане трошкове и штету, у складу са прописима који уређују одговорност за штету, осим ако је друкчије одређено у изјави о пристанку.

На опозив пристанка за обраду нарочито осетљивих података сходно се примењује члан 11. овог закона.

III. ПРАВА ЛИЦА И ЗАШТИТА ПРАВА ЛИЦА

1. Права

Право на обавештење о обради

Члан 19.

Лице има право да захтева да га руковалац истинито и потпуно обавести о томе:

- 1) да ли руковалац обрађује податке о њему и коју радњу обраде врши;
- 2) које податке обрађује о њему;
- 3) од кога су прикупљени подаци о њему, односно ко је извор података;
- 4) у које сврхе обрађује податке о њему;
- 5) по ком правном основу обрађује податке о њему;
- 6) у којим збиркама података се налазе подаци о њему;
- 7) ко су корисници података о њему;
- 8) које податке, односно које врсте података о њему користе;
- 9) у које сврхе се користе подаци о њему;
- 10) по ком правном основу користи податке о њему;

- 11) коме се подаци преносе;
- 12) који подаци се преносе;
- 13) у које сврхе се подаци преносе;
- 14) по ком правном основу се подаци преносе;
- 15) у ком временском периоду се подаци обрађују.

Право на увид

Члан 20.

Лице има право да од руковоаца захтева да му стави на увид податке који се на њега односе.

Право на увид у податке који се на њега односе обухвата право на преглед, читање и слушање података, као и прављење забележака.

Право на копију

Члан 21.

Лице има право да од руковоаца захтева копију податка који се на њега односи.

Руководалац издаје копију податка (фотокопију, аудио копију, видео копију, дигиталну копију и сл) у облику у којем се информација налази, односно у другом облику ако би у облику у коме се информација налази лицу била неразумљива.

Лице сноси нужне трошкове израде и предаје копије податка.

Права лица поводом извршеног увида

Члан 22.

Лице има право да од руковоаца захтева исправку, допуну, ажурирање, брисање података, као и прекид и привремену обуставу обраде.

Лице има право на брисање података ако:

- 1) сврха обраде није јасно одређена;
- 2) је сврха обраде измењена, а нису испуњени услови за обраду за ту измењену сврху;
- 3) је сврха обраде остварена, односно подаци више нису потребни за остваривање сврхе;
- 4) је начин обраде недозвољен;
- 5) податак спада у број и врсту података чија је обрада несразмерна сврси;

6) је податак нетачан, а не може се путем исправке заменити тачним;

7) се податак обрађује без пристанка или овлашћења заснованог на закону и у другим случајевима када се обрада не може вршити у складу са одредбама овог закона.

Лице има право на прекид и привремену обуставу обраде, ако је оспорило тачност, потпуност и ажурност података, као и право да се ти подаци означе као оспорени, док се не утврди њихова тачност, потпуност и ажурност.

2. Ограничења

Ограничења права

Члан 23.

Право на обавештење, увид и копију може се ограничити ако:

1) лице тражи обавештење из члана 19. тач. 2) и 7) до 10) овог закона, а руковалац је податке о њему унео у јавни регистар или их је на други начин учинио доступним јавности;

2) лице злоупотребљава своје право на обавештење, увид и копију;

3) је руковалац или друго лице, у складу с чланом 15. овог закона, већ упознао лице са оним о чему тражи да буде обавештен, односно ако је лице извршило увид или добило копију, а у међувремену није дошло до промене податка;

4) би руковалац био онемогућен у вршењу послова из свог делокруга;

5) би давање обавештења озбиљно угрозило интересе националне и јавне безбедности, одбране земље, или радње спречавања, откривања, истраге и гоњења за кривична дела;

6) би давање обавештења озбиљно угрозило важан привредни или финансијски интерес државе;

7) би се обавештењем учинио доступним податак за који је законом, другим прописима или актима заснованим на закону одређено да се чува као тајна, а због чијег би одавања могле наступити тешке последице по интерес заштићен законом;

8) би обавештење озбиљно угрозило приватност или важан интерес лица, посебно живот, здравље и физички интегритет;

9) се подаци о њему користе искључиво за научноистраживачке и статистичке сврхе, док такво коришћење траје.

Лице нема право на увид док траје обустава обраде ако је обрада обустављена на његов захтев.

3. Захтев

Захтев за остваривање права

Члан 24.

Захтев за обавештење, увид и копију подноси се руковоаоцу у писменом облику, а руковалац може прихватити и усмени захтев, из разлога ефикасности и економичности. Захтев за остваривање права поводом извршеног увида подноси се руковоаоцу у писменом облику.

Захтев из става 1. овог члана садржи: податке о идентитету подносиоца (име и презиме, име једног родитеља, датум и место рођења, јединствени матични број грађана), адресу пребивалишта, односно боравишта, као и друге податке неопходне за контакт.

Захтев који подноси законски наследник умрлог лица садржи и податке о идентитету умрлог. Уз захтев се прилаже извод из матичне књиге умрлих, као и доказ о сродству подносиоца са умрлим.

Неписмено лице, односно лице које због телесних или других недостатака није у могућности да захтев сачини у писменом облику може захтев усмено саопштити у записник.

Руковалац може прописати образац за подношење захтева, али је дужан да размотри и захтев који није сачињен на том обрасцу.

Ако је захтев неразумљив или непотпун, руковалац је дужан да поучи подносиоца како да недостатке отклони.

Ако подносилац не отклони недостатке у одређеном року, а најдуже у року од 15 дана од дана пријема поуке о допуни, а недостаци су такви да се по захтеву не може поступати, руковалац ће закључком одбацити захтев као неуредан.

4. Одлучивање

Одлучивање о захтеву за обавештење, увид и копију

Члан 25.

Руковалац је дужан да обавештење о поднетом захтеву изда без одлагања, а најкасније у року од 15 дана од дана подношења. Обавештење се даје у писменом облику, а изузетно се може дати и усмено ако на то пристане подносилац.

Руковалац је дужан да без одлагања, а најкасније у року од 30 дана од дана пријема уредног захтева за увид, односно за издавање копије, омогући подносиоцу да изврши увид, односно да му преда копију.

Руковалац ће заједно са обавештењем о томе да ће подносиоцу захтева ставити на увид податак, односно издати му копију податка, саопштити и време, место и начин на који ће му податак бити стављен на увид, износ нужних трошкова израде копије податка, а у случају да не располаже техничким средствима за израду копије, упознаће подносиоца са могућношћу да употребом своје опреме изради копију.

Подносилац захтева из става 2. овог члана може из оправданих разлога тражити да увид у податке изврши у друго време. Увид у податке врши се по правилу у службеним просторијама руковоаца.

Ако руковалац није у могућности, из оправданих разлога, да поступи по захтеву у прописаном року, обавестиће о томе подносиоца и одредити нови рок за поступање који не може бити дужи од 30 дана од истека рока из ст. 1. и 2. овог члана.

Ако прихвати захтев за обавештење, увид и копију, руковалац о томе сачињава забелешку.

Ако руковалац одбије захтев, о томе доноси решење са поуком о правном средству.

Ако руковалац не одговори на захтев у роковима из ст. 1. и 2. овог члана, као и ако одбије захтев, подносилац захтева може изјавити жалбу Поверенику.

Одлучивање о захтеву поводом извршеног увида

Члан 26.

Руковалац је дужан да одлучи о захтеву поводом извршеног увида из члана 24. овог закона, без одлагања, а најкасније у року од 15 дана од дана подношења захтева и да о одлуци обавести подносиоца захтева.

Када руковалац одбије захтев из става 1. овог члана, у образложењу решења наводи разлоге за одбијање захтева, као и разлоге за дозвољеност обраде.

Подносилац захтева може изјавити жалбу Поверенику против решења о одбијању захтева из става 1. овог члана, у року од 15 дана од дана достављања решења.

Ако је руковалац утврдио да је захтев поводом извршеног увида основан, а не постоји техничка могућност да се без одлагања поступи по захтеву, или ако би неодложно поступање по захтеву изискивало прекомерни утрошак времена и средстава, руковалац ће по службеној дужности означити податке као оспорене и привремено обуставити њихову обраду.

Руковалац који је орган власти, а који је утврдио да је захтев поводом извршеног увида основан, означити податак као оспорен и привремено обуставити његову обраду. Руковалац неће исправити, допунити, ажурирати и брисати податак, односно прекинути обраду ако:

- 1) није истекао рок за обавезно чување података;
- 2) је очигледно да би поступање по захтеву нанело озбиљну штету интересима других лица;
- 3) је због посебног начина чувања података поступање по захтеву немогуће или изискује прекомерни утрошак времена или средстава.

Ознака оспорености из члана 22. став 3. овог закона, брисаће се на основу одлуке надлежног органа или по пристанку лица на које се податак односи.

5. Начин остваривања права

Начин остваривање права на увид

Члан 27.

Руковалац је дужан да подносиоцу учини доступним податак који се на њега односи, у разумљивом облику.

Руковалац је дужан да подносиоцу учини доступним све податке у стању у каквом се налазе.

Ако се податак чува у разним облицима (папир, аудио, видео или електронски запис и др), подносилац има право да изврши увид у облику који сам изабере, осим када је то неизводљиво.

Лице које није у стању да без пратиоца изврши увид у податке, може да то учини уз помоћ пратиоца.

Руковалац ће, на захтев лица којем је потребна стручна помоћ ради разумевања садржине података који се на њега односе, пружити такву помоћ.

Вршење права на увид у податке руковалац не сме условити плаћањем накнаде.

Ако руковалац располаже податком на језику на коме је поднет захтев, дужан је да подносиоцу стави на увид податак и изради копију на том језику, осим ако подносилац не одреди друкчије, а руковалац има могућности да удовољи захтеву.

Начин остваривања права на копију

Члан 28.

Руковалац издаје копију податка (фотокопију, аудио копију, видео копију, дигиталну копију и сл) у облику у којем се информација налази, односно у другом облику, ако би у облику у коме се информација налази лицу била неразумљива.

Нужне трошкове израде и предаје копије податка сноси подносилац.

6. Обрада за делатност јавних гласила

Члан 29.

За обраду од стране новинара и других медијских посленика која искључиво служи публицистичкој делатности јавног гласила, изузимајући обраду која служи оглашавању, важе одредбе чл. 3, 5. и 8. тач. 1) до 5) и чл. 46. и 47. овог закона.

За потребе обраде из става 1. овог члана могу се користити и подаци који се односе на припадност политичкој странци лица, ако су важни с обзиром на јавну функцију коју лице врши.

Прикључивање одговора и других информација

Члан 30.

Одговор, исправку, опозив или коју другу информацију која се објави на захтев лица на кога се односи податак из члана 29. овог закона, руковалац прикључује обрађиваном податку и чува у року за чување тог податка.

Заштита личности

Члан 31.

Ако се објављивањем податка у јавном гласилу и публикацији повреди право или правно заштићен интерес лица, повређено лице може захтевати од одговорног уредника и издавача јавног гласила обавештење о подацима који се о њему обрађују, увид у податке и копију, изузев ако:

- 1) би се тиме открили подаци у вези са извором информације које новинар и други медијски посленик нису дужни или нису спремни да открију;
- 2) би се тиме открили подаци у вези са лицем које је учествовало у припреми и објављивању информације, а одговорни уредник није спреман да их открије;
- 3) постоје околности у којима би обавештавање, увид или израда копије битно омели обавештавање јавности о информацијама од јавног значаја.

7. Посебне одредбе

Прослеђивање захтева Поверенику

Члан 32.

Када руковалац не обрађује податак, проследиће захтев Поверенику, осим ако се подносилац захтева томе противи.

Поступање Повереника

Члан 33.

По пријему захтева Повереник проверава да ли руковалац обрађује тражени податак.

Ако утврди да руковалац не обрађује податак, Повереник ће доставити захтев руковоацу који обрађује податак и о томе ће обавестити подносиоца захтева или ће га упутити на руковоаца који обрађује податак, у зависности од тога на који ће се начин ефикасније остварити захтев.

Ако утврди да руковалац обрађује податак, Повереник ће решењем наложити руковоацу да одлучи о захтеву.

Руковалац одлучује о достављеном захтеву из става 2. овог члана у роковима из члана 25. став 1. и члана 26. став 1. овог закона од дана достављања, а у случају из става 3. овог члана у року од седам дана од дана достављања решења Повереника.

Пуномоћник

Члан 34.

Права прописана овим законом могу се остварити лично или преко пуномоћника.

Пуномоћје мора бити оверено.

Чување и коришћење у случају смрти

Члан 35.

У случају смрти и проглашења несталога лица за умрло, подаци који су прикупљени на основу уговора, односно сагласности у писменом облику, чувају се у складу са условима утврђеним у уговору, односно пристанку, а подаци који су прикупљени на основу закона чувају се најмање годину дана од дана смрти, односно проглашења несталога лица за умрло, а након тога се уништавају. О уништавању података сачињава се забелешка.

Пристанак за коришћење података о умрлом лицу дају лица из члана 10. став 6. овог закона.

Обавеза руковоаца

Члан 36.

Ако је збирка података успостављена уговором, односно на основу пристанка у писменом облику, у случају раскида уговора, односно повлачења пристанка у писменом облику, руковалац је обавезан да податке брише у року од 15 дана од дана раскида уговора, односно повлачења пристанка, осим ако је другачије прописано или уговорено.

Сходна примена одредаба закона о управном поступку

Члан 37.

На поступак одлучивања о захтевима примењују се одредбе закона којим се уређује општи управни поступак, осим ако овим законом није друкчије одређено.

IV. ПОСТУПАК ПО ЖАЛБИ

Право на жалбу

Члан 38.

Подносилац захтева за остваривање права у вези са обрадом може изјавити жалбу Поверенику:

- 1) против одлуке руковоаца којом је одбијен или одбачен захтев;
- 2) када руковалац не одлучи о захтеву у прописаном року;
- 3) ако руковалац не стави на увид податак, односно не изда копију податка или то не учини у року и на начин прописан овим законом;
- 4) ако руковалац услови издавање копије података уплатом накнаде која превазилази износ нужних трошкова израде копије;
- 5) ако руковалац, супротно закону, отежава или онемогућава остваривање права.

Жалба се може изјавити у року од 15 дана од дана достављања одлуке којом је захтев одбијен или одбачен, односно по истеку прописаног рока за одлучивање и поступање.

Уз жалбу се прилаже захтев са доказом о предаји руковоацу и одлука која се оспорава.

Решавање Повереника по жалби

Члан 39.

Повереник доноси одлуку по жалби најкасније у року од 30 дана од дана подношења жалбе. Жалба се доставља руковоацу ради одговора на жалбу. О наводима из одговора на жалбу може се изјаснити подносилац.

Повереник одбацује решењем неблаговремену или непотпуну жалбу, односно жалбу која је изјављена од неовлашћеног лица.

Када Повереник, поводом жалбе изјављене због недоношења одлуке по захтеву, утврди да је жалба основана, решењем ће наложити руковоацу да у одређеном року поступи по захтеву.

Ако руковалац након изјављене жалбе због непоступања по захтеву, а пре доношења одлуке по жалби, омогући остваривање права на увид, односно копију или по захтеву одлучи, Повереник ће закључком обуставити поступак по жалби.

Поступак по жалби се обуставља и када подносилац одустане од жалбе.

Утврђивање чињеничног стања у поступку по жалби

Члан 40.

Повереник предузима радње за утврђивање чињеничног стања које су неопходне ради одлучивања по жалби.

Поверенику, односно лицу кога он посебно овласти, ради утврђивања чињеничног стања, омогућиће се увид у податак, односно збирку података, изузев у случају из члана 45. став 2. овог закона.

Обавезност и извршење решења

Члан 41.

Решење Повереника по жалби је обавезујуће, коначно и извршно.

Влада у случају потребе обезбеђује извршење решења Повереника и може ближе да одреди начин извршења решења.

Правни лек против одлуке

Члан 42.

Против одлуке Повереника може се покренути управни спор.

Остале одредбе поступка

Члан 43.

На поступак одлучивања по жалби примењују се одредбе закона којим се уређује општи управни поступак, осим ако овим законом није друкчије одређено.

V. ПОВЕРЕНИК

Надлежност

Члан 44.

Повереник:

- 1) надзире спровођење заштите података;
- 2) одлучује по жалби у случају прописаним овим законом;
- 3) води Централни регистар;
- 4) надзире и дозвољава изношење података из Републике Србије;
- 5) указује на уочене злоупотребе приликом прикупљања података;

- 6) саставља листу држава и међународних организација које имају одговарајуће уређену заштиту података;
- 7) даје мишљење у вези са успостављањем нових збирки података, односно у случају увођења нове информационе технологије у обради података;
- 8) даје мишљење, у случају када постоји сумња да ли се неки скуп података сматра збирком података у смислу овог закона;
- 9) даје мишљење Влади у поступку доношења акта о начину архивирања и о мерама заштите нарочито осетљивих података;
- 10) прати примену мера за заштиту података и предлаже побољшање тих мера;
- 11) даје предлоге и препоруке за унапређење заштите података;
- 12) даје претходно мишљење да ли одређени начин обраде представља специфичан ризик за права и слободе грађанина;
- 13) прати уређење заштите података у другим земљама;
- 14) сарађује са органима надлежним за надзор над заштитом података у другим земљама;
- 15) одређује начин даљег поступања са подацима када је руковалац престао да постоји, осим ако је прописано друкчије;
- 16) обавља и друге послове из своје надлежности.

Повереник може имати заменика за заштиту података о личности.

Извештај који подноси Народној скупштини, Повереник доставља председнику Републике, Влади и Заштитнику грађана и на одговарајући начин ставља на увид јавности.

Право приступа и увида

Члан 45.

Повереник има право приступа и увида у:

- 1) податак и збирку података;
- 2) комплетну документацију која се односи на прикупљање података и друге радње обраде, као и на остваривање права лица из овог закона;
- 3) опште акте руковоаоца;
- 4) просторије и опрему коју користи руковалац.

Приступ и увид из става 1. тач. 1), 2) и 4) овог члана може се ограничити ако би се тиме озбиљно угрозио интерес националне или јавне безбедности, одбране земље или радње спречавања, откривања, истраге и гоњења за кривична дела, док трају разлози за ограничење, у складу са законом.

У случају да руковалац сматра да постоје разлози за ограничење из става 2. овог члана дужан је да, у року од осам дана од дана достављања захтева

Повереника, затражи мишљење председника Врховног касационог суда о постојању разлога за ограничење права приступа и увида Повереника.

Председник Врховног касационог суда дужан је да, у року од осам дана од дана достављања захтева руковаоца из става 3. овог члана, достави мишљење руковаоцу. Руковалац је дужан да о мишљењу председника Врховног касационог суда обавести Повереника.

VI. ОБЕЗБЕЂЕЊЕ ПОДАТАКА

Обавеза чувања тајне

Члан 46.

Повереник, заменик Повереника и запослени у стручној служби, дужни су да као тајну, у складу са законом и другим прописима којима се уређује тајност података, чувају све податке које сазнају у обављању својих дужности, осим ако је друкчије прописано.

Обавеза из става 1. овог члана траје и по престанку обављања дужности Повереника и заменика Повереника, односно по престанку радног односа у стручној служби.

Руковалац је дужан да упозна обрађивача и лице које има увид у податке са мерама за заштиту тајности података.

Организационе и техничке мере

Члан 47.

Подаци морају бити одговарајуће заштићени од злоупотреба, уништења, губитка, неовлашћених промена или приступа.

Руковалац и обрађивач дужни су да предузму техничке, кадровске и организационе мере заштите података, у складу са утврђеним стандардима и поступцима, а које су потребне да би се подаци заштитили од губитка, уништења, недопуштеног приступа, промене, објављивања и сваке друге злоупотребе, као и да утврде обавезу лица која су запослена на обради, да чувају тајност података.

VII. ЕВИДЕНЦИЈА

Евиденција о обради

Члан 48.

Руковалац образује и води евиденцију која садржи:

- 1) врсту података и назив збирке података;
- 2) врсту радње обраде;
- 3) назив, име, седиште и адресу руковоаца;
- 4) датум започињања обраде, односно успостављања збирке података;
- 5) сврху обраде;
- 6) правни основ обраде, односно успостављања збирке података;
- 7) категорију лица на које се подаци односе;
- 8) врсту и степен тајности података;
- 9) начин прикупљања и чувања података;
- 10) рок чувања и употребе података;
- 11) назив, име, седиште и адресу корисника;
- 12) ознаку уношења, односно изношења података из Републике Србије са називом државе, односно међународне организације и страног корисника, правни основ и сврху уношења, односно изношења података;
- 13) предузете мере заштите података;
- 14) захтев поводом обраде.

Руковалац није дужан да образује и води евиденцију обраде: података који се обрађују искључиво у породичне и друге личне потребе у смислу одредбе члана 5. тачка 2) овог закона, података који се обрађују ради вођења регистара чије је вођење законом прописано, података за збирку података коју чине само јавно објављени подаци, као ни података који се односе на лице чији идентитет није одређен а руковалац, обрађивач, односно корисник није овлашћен да идентитет одреди.

Руковалац ажурира евиденцију када дође до промене у вези са основним подацима из става 1. овог члана у року од 15 дана од дана настанка промене.

Образац за вођење евиденције и начин вођења евиденције из става 1. овог члана прописује Влада.

Обавештавање Повереника

Члан 49.

Руковалац је дужан да пре започињања обраде, односно успостављања збирке података достави Поверенику обавештење о намери успостављања збирке података заједно са подацима из члана 48. овог закона, као и о свакој даљој намераваној обради, пре предузимања обраде и то најкасније 15 дана пре успостављања збирке података, односно обраде.

Обавеза достављања обавештења из става 1. овог члана не односи се на започињање обраде, односно успостављање збирке података у случају када је посебним прописом одређена сврха обраде, врста података који се обрађују, врсте корисника којима ће подаци бити доступни, као и време за које ће подаци бити архивирани.

Претходна провера

Члан 50.

Након пријема обавештења из члана 49. овог закона, пре успостављања збирке података, Повереник проверава радње обраде које би у значајној мери могле да доведу до повреде права лица.

Начин провере из става 1. овог члана уређује се актом Повереника.

Обавеза достављања

Члан 51.

Руковалац доставља Поверенику евиденцију о збирци података, односно промене у евиденцији података најкасније у року од 15 дана од дана успостављања, односно промене.

Обавештења из члана 49. став 1. овог закона и евиденције из става 1. Овог члана уписују се у Централни регистар.

Централни регистар

Члан 52.

Повереник успоставља и води Централни регистар.

Централни регистар се састоји од регистра збирки података и каталога збирки података.

Регистар збирки података садржи податке из члана 51. став 2. Овог закона.

Каталог збирки података садржи опис евидентираних збирки података.

Централни регистар је јаван и обавезно се објављује путем интернета.

Повереник једном годишње објављује попис збирки података у „Службеном гласнику Републике Србије”.

Повереник ће ускратити право на увид у евиденцију о збирци података ако то захтева руковалац, под условом да је то неопходно за остваривање претежног интереса очувања националне или јавне безбедности, одбране земље, рада органа власти, финансијског интереса државе или ако је законом, другим прописом или актом заснованим на закону одређено да се евиденција о збирци података чува као тајна.

VIII. ИЗНОШЕЊЕ ПОДАТАКА ИЗ РЕПУБЛИКЕ СРБИЈЕ

Члан 53.

Подаци се могу износити из Републике Србије у државу чланицу Конвенције о заштити лица у односу на аутоматску обраду личних података Савета Европе.

Подаци се могу износити из Републике Србије у државу која није чланица конвенције из става 1. овог члана, односно међународну организацију, ако је у тој држави, односно међународној организацији, прописом, односно уговором о преносу података, обезбеђен степен заштите података у складу са конвенцијом.

Приликом изношења података из става 2. овог члана, Повереник утврђује да ли су испуњени услови и спроведене мере заштите података приликом њиховог изношења из Републике Србије и даје дозволу за изношење.

IX. НАДЗОР

Надлежност

Члан 54.

Надзор над спровођењем и извршавањем овог закона врши Повереник.

Послове из става 1. овог члана Повереник врши преко овлашћених лица.

Овлашћено лице је дужно да надзор врши стручно и благовремено и да о извршеном надзору сачини записник.

У вршењу надзора овлашћено лице поступа на основу сазнања до којих је дошао по службеној дужности, од стране подносиоца жалбе или трећег лица.

У вршењу надзора овлашћено лице је дужно да покаже легитимацију.

Образац легитимације прописује Повереник.

Омогућавање вршења надзора

Члан 55.

Лица којима су овим законом утврђене обавезе у вези са заштитом података, дужна су да овлашћеном лицу омогуће несметано вршење надзора и ставе му на увид и располагање потребну документацију.

Овлашћења Повереника у надзору

Члан 56.

Ако се приликом обављања надзора утврди да су повређене одредбе закона којима се уређује обрада, Повереник ће упозорити руковођа на неправилности у обради.

На основу налаза овлашћеног лица, Повереник може:

- 1) наредити да се неправилности отклоне у одређеном року;
- 2) привремено забранити обраду која се обавља супротно одредбама овог закона;
- 3) наредити брисање података прикупљених без правног основа.

Против акта из става 2. овог члана жалба није дозвољена, али се може покренути управни спор.

Спровођење мера из става 2. овог члана уређује се актом Повереника.

Повереник је дужан да поднесе прекршајну пријаву због повреда одредаба овог закона.

Х. КАЗНЕНЕ ОДРЕДБЕ

Члан 57.

Новчаном казном од 50.000 до 1.000.000 динара казниће се за прекршај руковођац, обрађивач или корисник који има својство правног лица ако:

- 1) обрађује податке без пристанка супротно условима из члана 12. овог закона;
- 2) обрађује податке супротно условима из члана 13. овог закона;
- 3) прикупља податке од другог лица супротно условима из члана 14. став 2. овог закона;
- 4) пре прикупљања података не упозна лице на које се подаци односе, односно друго лице о условима из члана 15. став 1. овог закона;
- 5) обрађује нарочито осетљиве податке супротно чл. 16. до 18. овог закона;

- 6) не учини доступним све податке у стању у каквом се налазе супротно члану 27. став 2. овог закона;
- 7) не изда копију податка у облику у којем се информација налази супротно члану 28. став 1. овог закона;
- 8) не обрише податке из збирке података супротно члану 36. овог закона;
- 9) не изврши решење Повереника по жалби (члан 41. став 1. овог закона);
- 10) поступи супротно обавези чувања тајне из члана 46. ст. 1. и 2. овог закона;
- 11) поступи супротно обавези предузимања мера из члана 47. став 2. овог закона;
- 12) не образује евиденцију, односно не ажурира евиденцију супротно члану 48. ст. 1. и 3. овог закона;
- 13) не обавести Повереника о намери успостављања збирке података у прописаном року супротно члану 49. став 1. овог закона;
- 14) не достави Поверенику евиденцију, односно промене у збирци података у прописаном року (члан 51. став 1. овог закона);
- 15) износи податке из Републике Србије супротно члану 53. овог закона;
- 16) не омогући овлашћеном лицу несметано вршење надзора и не стави му на увид и располагање потребну документацију (члан 55. овог закона);
- 17) не поступи по налозима Повереника (члан 56. став 2. овог закона).

За прекршај из става 1. овог члана казниће се предузетник новчаном казном од 20.000 до 500.000 динара.

За прекршај из става 1. овог члана казниће се физичко лице, односно одговорно лице у правном лицу, државном органу, односно органу територијалне аутономије и јединице локалне самоуправе новчаном казном од 5.000 до 50.000 динара.

XI. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 58.

На седиште, избор, престанак мандата, поступак разрешења, положај Повереника, заменика Повереника, стручну службу, финансирање и подношење извештаја примењују се одредбе Закона о слободном приступу информацијама од јавног значаја („Службени гласник РС”, бр. 120/04 и 54/07).

Члан 59.

Повереник за информације од јавног значаја, установљен Законом о слободном приступу информацијама од јавног значаја („Службени гласник РС”, бр. 120/04 и 54/07) наставља са радом под називом Повереник за информације од јавног значаја и заштиту података о личности.

Члан 60.

Подзаконски акти на основу овог закона биће донети у року од шест месеци од дана ступања на снагу овог закона.

Члан 61.

Збирке података и евиденције успостављене до ступања на снагу овог закона ускладиће се са његовим одредбама у року од 12 месеци од дана ступања на снагу овог закона.

Руковаоци података дужни су да евиденције из члана 48. овог закона доставе Поверенику, у року од 12 месеци од дана ступања на снагу овог закона.

Члан 62.

Даном почетка примене овог закона престаје да важи Закон о заштити података о личности („Службени лист СРЈ”, бр. 24/98 и 26/98-исправка).

Члан 63.

Овај закон ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”, а примењиваће се од 1. јануара 2009. године.

ДИРЕКТИВА САВЕТА ЕВРОПСКЕ ЗАЈЕДНИЦЕ О ПРАВНОЈ ЗАШТИТИ КОМПЈУТЕРСКИХ ПРОГРАМА

САВЕТ ЕВРОПСКИХ ЗАЈЕДНИЦА,

на основу споразума о оснивању Европске економске заједнице, а нарочито његовог члана 100 А,

на основу предлога Комисије (1),

у сарадњи са Европским парламентом (2),

на основу мишљења Економског и социјалног комитета (3),

имајући у виду да компјутерски програми данас нису јасно заштићени у свим земљама чланицама важећим законима; да једна таква заштита, када постоји, поприма различите особености;

сматрајући да стварање компјутерских програма захтева коришћење знатних људских, техничких и финансијских потенцијала, а могуће их је прекопирати уз знатно ниже трошкове од оних које захтева самостална израда;

с обзиром да компјутерски програми играју све значајнију улогу у бројним индустријским секторима и да се технологија која се на њих односи може стога сматрати као основа за индустријски развој Заједнице;

сматрајући да извесне разлике које карактеришу правну заштиту компјутерских програма које обезбеђује законодавство држава чланица имају негативне утицаје на функционисање заједничког тржишта у погледу компјутерских програма и да би се ове разлике могле све више повећавати уколико би државе чланице усвојиле нове законодавне одредбе у овој области;

сматрајући да би требало укинути постојеће разлике које имају за последицу спречавање појављивања новина док не би требало укидати или спречавати појављивање оних разлика које не би осетно оштећивале функционисање заједничког тржишта;

сматрајући да правни оквир Заједнице који се односи на заштиту компјутерских програма може дакле да се, у прво време, ограничи на прописивање да државе чланице морају дозволити заштиту ауторских права на компјутерске програме као књижевних дела и да се одреди корисник и објект заштите, на ексклузивна права на која би се заштићена лица могла позивати како би дозволила или забранила одређена чињења, као и на трајање заштите;

узимајући у обзир да, за потребе ове директиве, термин "компјутерски програм" означава програме без обзира на њихов облик, рачунајући и оне који су уграђени у хардвер; да овај термин такође обухвата припремне радове конципирања који на крају доводе до развијања

неког програма, под условом да су такве природе да омогућавају израду компјутерског програма у каснијем стадијуму;

сматрајући да критеријуми који се примењују да би се одредило да ли један компјутерски програм представља или не представља оригинално дело не би требало да садрже никакву процену квалитета или естетске вредности програма;

с обзиром да се Заједница труди да промовише увођење међународних стандарда;

с обзиром да је компјутерски програм позван да комуницира и да оперише са другим елементима неког информатичког система као и са корисницима; да је, у том циљу, неопходна логичка, према случају, и физичка веза за међусобно повезивање и интеракцију у циљу омогућавања потпуног функционисања свих елемената софтвера и хардвера са другим софтверима и хардверима као и са корисницима;

с обзиром да се делови програма који обезбеђују ово међусобно повезивање и ову интеракцију између елемената софтвера и хардвера уобичајено називају "интерфејс" (интерфејс);

с обзиром да се ово међусобно повезивање и ова функционална интеракција уобичајено називају "интероперативност"; да ова интероперативност може да се дефинише као способност да се размењују информације и да се узајамно користе размењене информације;

сматрајући да, да би се избегла свака двосмисленост, треба прецизирати да је заштићена само формулација одређеног компјутерског програма, а да принципи и идеје које се налазе у основи различитих елемената неког програма, рачунајући и принципе и идеје које се налазе у основи његових интерфејса, нису заштићени на основу ове директиве;

с обзиром да, у складу са овим принципом ауторског права, идеје и принципи које се налазе у основи логике, алгоритама и програмског језика нису заштићени на основу ове директиве;

с обзиром да у складу са законодавством и судском праксом држава чланица као и са међународним конвенцијама о ауторском праву, формулација ових идеја и принципа треба да је заштићен ауторским правом;

сматрајући да се, за потребе ове директиве, под појмом "изнајмљивање" сматра стављање на располагање једног компјутерског програма или његове копије ради његовог коришћења у ограниченом периоду и у привредне сврхе; да овај појам не подразумева позајмљивање физичким лицима која дакле не спадају у поље примене ове директиве;

сматрајући да ексклузивно ауторово право да спречи недозвољено умножавање свог дела треба да подлеже ограниченом изузетку у случају компјутерског програма, како би се омогућило умножавање које је технички неопходно за коришћење ономе који га је легално стекао; да то значи да се операција учитавања и пуштања у рад неопходне за коришћење једне копије легитимно стеченог програма, као и исправке њених грешака, не могу забранити уговором, да се, у одсуству специфичних одредаба у уговору, нарочито у случају продаје једне копије програма, и свака друга операција неопходна за коришћење програма може

извршавати, у складу са својим предвиђеним циљем, од стране лица које је легитимно стекло копију;

сматрајући да уживалац права на коришћење компјутерског програма не сме бити спречен да извршава потребне поступке за посматрање, проучавање или испробавање функционисања овог програма, под условом да ови поступци не повређују права аутора програма;

сматрајући да умножавање, превођење, адаптација или недозвољено преуређивање облика кодирања под којим је достављена копија програма представљају повређивање искључивих права аутора;

сматрајући, ипак, да се у извесним околностима умножавање кода неког компјутерског програма, или превођење његовог облика у смислу члана 4 тачке а) и б) може показати неопходним за добијање информација потребних за интероперативност неког програма креираног на независан начин са другим програмима;

сматрајући да је дакле потребно да се предвиди да је, једино у овим прецизно одређеним околностима, превођење од стране или у име лица које поседује право да користи копију програма легитимно и у складу са добрим пословним обичајима, и да за њега није потребно добијање одобрење од носиоца ауторског права;

сматрајући једном од сврха овог изузећа, омогућавање међусобног повезивања свих елемената једног информатичког система, укључујући и системе различитих произвођача, како би могли функционисати заједно;

сматрајући да једно овакво изузеће од искључивих ауторских права не сме да се примењује на начин који би проузроковао повређивање легитимних интереса носиоца права или који би угрожавао нормално коришћење програма;

сматрајући да, како би остали у складу са одредбама Бернске конвенције о заштити књижевних и уметничких дела, трајање заштите мора бити једнако дужини живота аутора плус педесет година почевши од 1. јануара следеће године у односу на годину у којој је аутор преминуо, или у случају анонимног дела или дела објављеног под псеудонимом, педесет година почевши од 1. јануара следеће године у односу на годину у којој је дело по први пут објављено;

сматрајући да заштита компјутерских програма законодавством из области ауторског права не треба да представља препреку, ако је такав случај, коришћењу других облика заштите, да свака уговорна одредба противна члану 6. или изузецима предвиђеним чланом 5. параграфи 2 и 3 треба међутим да буде ништава и да се сматра непостојећом;

сматрајући да одредбе ове директиве не дирају у примену прописа о заштити конкуренције из члана 85. и 86. Споразума о оснивању ЕЕЗ уколико добављач који заузима доминантан положај на тржишту одбије да стави на располагање информације потребне за постизање интероперативности каква је дефинисана у овој директиви;

сматрајући да одредбе ове директиве не би требало да прејудуцирају посебне одредбе већ донетог права Заједнице у области објављивања карактеристика интерфејса у сектору телекомуникација, као ни одлуке Савета у вези са стандардизацијом у области технологије информација и телекомуникација;

сматрајући да ова директива не утиче на изузећа предвиђена националним законодавствима, утврђена применом Бернске конвенције, у тачкама које ова директива не покрива,

ДОНЕО ЈЕ СЛЕДЕЋУ ДИРЕКТИВУ:

Члан 1.

Објекат заштите

1. У складу са одредбама ове директиве, државе чланице заштићују компјутерске програме ауторским правом као књижевна дела у смислу Бернске конвенције за заштиту књижевних и уметничких дела. Појам "компјутерских програм", за потребе ове директиве, обухвата и припремни материјал за конципирање програма.
2. Заштита предвиђена овом директивом примењује се на сваки облик формулисања неког компјутерског програма. Идеје и принципи који се налазе у основи било ког елемента компјутерског програма, укључујући и идеје и принципе који се налазе у основи његових интерфејса, нису заштићени ауторским правом у складу са овом директивом.
3. Компјутерски програм је заштићен када је оригиналан, у том смислу да је лична интелектуална творевина свог аутора. Никакав други критеријум се не примењује за утврђивање да ли он може потпадати под ову заштиту.

Члан 2.

Ауторство компјутерског програма

1. Аутор неког компјутерског програма је физичко лице које је створило програм, или група физичких лица која су створила програм, или уколико то дозвољава закон одговарајуће државе чланице, правно лице које се сматра тим законодавством као носилац права. Када се колективна дела признају законодавством неке државе чланице, лице које законодавство одговарајуће државе чланице сматра ствараоцем дела сматра се аутором.
2. Када је компјутерски програм стварало заједнички више физичких лица, искључива права заједнички задржавају та иста лица.

3. Када је компјутерски програм стварао један службеник у обављању своје службе или према налозима свог послодавца, једино је послодавац правно овлашћен да врши сва имовинска права која се односе на овакво створен компјутерски програм, осим ако је одредбама уговора утврђено супротно.

Члан 3.

Корисник заштите

Заштита се пружа сваком физичком или правном лицу за које је прихваћено да потпада под одредбе националних законодавстава у области ауторског права применљивог на књижевна дела.

Члан 4.

Ограничавајући акти

Уз ограничења у члановима 5. и 6, ексклузивна права носиоца у смислу члана 2. садрже право да се врши и да се даје дозвола да се врши:

а) трајно или привремено умножавање неког компјутерског програма, у целости или делимично, било којим средством и на било који начин. Када учитавање, истицање на монитору, прелажење, преношење или похрањивање неког компјутерског програма захтевају неко такво умножавање програма, такво умножавање ће бити подвргнуто добијању одобрења од носиоца права;

б) превођење, прилагођавање, приређивање и свако друго мењање компјутерског програма и умножавање програма који из тога произлазе, не прејудуцирајући права лица које мења компјутерски програм;

ц) сваки облик јавне дистрибуције, укључујући и изнајмљивање, оригинала или копија компјутерског програма. Прва продаја копије компјутерског програма у Заједници од стране носиоца права или уз његов пристанак исцрпљује право на дистрибуцију ове копије у Заједници, изузев права на контролу накнадних изнајмљивања компјутерског програма или његове копије.

Члан 5.

Изузеци од ограничења

1. Изузев специфичних уговорних одредби, не подлежу одобрењу носиоца права, чињења предвиђена чланом 4. тачке а) и б) када су ова чињења неопходна да се омогући лицу које је

легитимни стицатељ коришћење компјутерског програма на начин који одговара његовој намени, као и ради исправљања грешака.

2. Лице које има право да користи компјутерски програм не може се спречити уговором да направи једну његову резервну копију (ради заштите од случајног уништења) када је то потребно за такву употребу.

3. Лице овлашћено за коришћење једне копије компјутерског програма може, без одобрења носиоца права, посматрати, проучавати или испитивати функционисање тог програма ради утврђивања идеја и принципа који се налазе у основи било ког елемента програма, приликом вршења било које операције учитавања, истицања на монитору, прелажења, преношења или похрањивања компјутерског програма за које има права да их чини.

Члан 6.

Декомпилација

1. Одобрење носиоца права не захтева се када је умножавање кода или превођење облика тог кода у смислу члана 4. тачке а) и б) неопходно за добијање информација потребних за интероперативност неког компјутерског програма створеног независно од других програма, под резервом да се стекну следећи услови:

а) ова чињења су извршена од носиоца лиценце или другог лица које ужива право да користи копије програма или за рачун тих лица од стране лица које је за то овлашћено;

б) информације потребне за интероперативност нису дотад биле лако и брзо доступне лицима из тачке а)

и

ц) ова чињења су ограничена на делове оригиналних компјутерских програма потребних за ту интероперативност.

2. Одредбе из параграфа 1 не могу бити оправдање да се информације добијене његовом применом:

а) употребљавају за друге циљеве осим постизања интероперативности компјутерског програма створеног на независан начин;

б) саопштавају трећим лицима, изузев уколико се то не покаже неопходним за интероперативност компјутерског програма створеног на независан начин,

или

ц) користе за усавршавање, израду или комерцијализацију неког компјутерског програма чија формулација је битно слична или за било које друго чињење којим се повређују ауторска права.

У складу са одредбама Бернске конвенције за заштиту књижевних и уметничких дела, овај члан не може да се тумачи тако да то омогућава да се он примењује на начин који би неправедно повредио легитимне интересе носиоца права или штетно нормалном коришћењу компјутерског програма.

Члан 7.

Специјалне мере заштите

1. Не дирајући у одредбе чланова 4, 5. и 6, Државе чланице, у складу са својим националним законодавствима, предузимају одговарајуће мере против особа које изврше неко од чињења поменутих у тачкама а), б) и ц) из текста који следи:

а) стављање у промет копије компјутерског програма, знајући да је копија недозвољена или имајући разлога за основану сумњу у њену недозвољеност;

б) држање из комерцијалних разлога копије компјутерског програма, знајући да је копија недозвољена или имајући разлога за основану сумњу у њену недозвољеност;

ц) стављање у промет или држање у комерцијалне сврхе сваког средства чија је једина сврха да олакша недозвољено уклањање или неутрализацију сваког техничког механизма евентуално направљеног у циљу заштите компјутерског програма.

2. Свака недозвољена копија компјутерског програма подлеже заплени у складу са законом заинтересоване државе чланице.

3. Државе чланице могу предвидети запленту средстава наведених у члану 1. тачка ц).

Члан 8.

Трајање заштите

1. Заштита је обезбеђена у трајању ауторовог живота и током педесет година од његове смрти или смрти последњег живог аутора; уколико је компјутерски програм анонимно дело или дело објављено под псеудонимом или се националним законима аутором сматра неко правно лице у складу са чланом 2. параграф 1, трајање заштите је педесет година почев од дана када је компјутерски програм законито учињен јавно доступан по први пут. Трајање заштите се рачуна почев од 1. јануара године која следи претходно наведеним догађајима.

2. Државама чланицама које већ примењују заштиту у дужем трајању него што је предвиђено у параграфу 1 дозвољено је да задрже своје садашње трајање заштите до тренутка када ће се трајање заштите за заштићена дела уједначити правом Заједнице на један општији начин.

Члан 9.

Очување других правних одредби

1. Одредбе ове директиве не утичу на друге одредбе из законодавства која се нарочито односе на патенте, жигове, нелојалну конкуренцију, пословну тајну, заштиту полупроводника или уговорних права. Свака одредба уговора супротна члану 6. или изузецима предвиђеним у члану 5, параграфи 2 и 3 сматраће се ништавом и непостојећом.

2. Одредбе ове директиве су такође применљиве на компјутерске програме створене пре 1. јануара 1993. године, не дирајући у закључене акте и права стечена пре тог дана.

Члан 10.

Завршне одредбе

1. Државе чланице стављају на снагу законске одредбе, одредбе прописа и административне одредбе потребне ради усклађивања са овом директивом пре 1. јануара 1993.

Када државе чланице усвоје ове одредбе, оне ће садржати позивање на ову директиву или ће њихово званично објављивање бити пропраћено позивањем на ову директиву. О начинима позивања на ову директиву одлучују државе чланице.

2. Државе чланице достављају Комисији текстове одредби унутрашњег права које оне усвајају у областима које су уређене овом директивом.

Члан 11.

Ова директива је намењена државама чланицама.

ЗАКОН О АУТОРСКИМ И СРОДНИМ ПРАВИМА

(извод из Закона који се односи на ауторско правну заштиту компјутерских програма и база података)

І ПРЕДМЕТ ЗАКОНА

Члан 1.

Овим законом уређују се права аутора књижевних, научних, стручних и уметничких дела (у даљем тексту: ауторско право), право интерпретатора, право првог издавача слободног дела, права произвођача фонограма, видеограма, емисија и база података као права сродна ауторском праву (у даљем тексту сродна права), начин остваривања ауторског и сродних права и судска заштита тих права.

ІІ АУТОРСКО ПРАВО

1. АУТОРСКО ДЕЛО

Члан 2.

- (1) Ауторско дело је оригинална духовна творевина аутора, изражена у одређеној форми без обзира без обзира на његову уметничку, научну или другу вредност, његову намену, величину, садржину и начин испољавања, као и допуштеност јавног саопштавања његове садржине.
- (2) Ауторским делом сматрају се нарочито:
 - 1) писана дела (књиге, брошуре, чланци, преводи, **рачунарски програми у било којем облику њиховог изражавања, укључујући и припремни материјал за њихову израду и друго**);
 - 2) говорна дела (предавања, говори, беседе и друго);
 - 3) драмска, драмско музичка, кореографска и пантомимска дела, као и дела која потичу из фолклора;
 - 4) музичка дела, са речима или без речи;
 - 5) филмска дела (кинематографска и телевизијска дела);
 - 6) дела ликовне уметности (слике, цртежи, скице, графике, скулптуре и друго);
 - 7) дела архитектуре, примењене уметности и индустријског обликовања;
 - 8) картографска дела (географске и топографске карте);
 - 9) планови, скице, макете и фотографије;
 - 10) позоришна режија.

Члан 5.

- (1) Ауторским делом сматра се и збирка која, с обзиром на избор и распоред саставних делова, испуњава услове из члана 2. став 1. овог закона

- (енциклопедија, зборник, антологија, изабрана дела, музичка збирка, збирка фотографија, графичка мапа, изложба и слично);
- (2) Ауторским делом сматра се и збирка народних, књижевних и уметничких творевина, као и збирка докумената, судских одлука и сличне грађе која, с обзиром на избор и распоред саставних делова испуњава услове из члана 2. став 1. овог закона;
 - (3) **Збирком се сматра и база података, без обзира да ли је у машински читљивој или другој форми која, с обзиром на избор и распоред саставних делова, испуњава услове из члана 2. став 1. овог закона;**
 - (4) Заштита збирке ни на који начин не ограничава права аутора дела која се саставни део збирке.

Члан 24.

Аутор рачунарског програма има искључиво право да другоме забрани или дозволи давање на послугу примерака свог дела. Давање на послугу, у смислу овог закона, је давање примерака дела другоме од стране институција доступних јавности, без непосредне или посредне имовинске користи.

КОНВЕНЦИЈА О ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ

Будимпешта, 23. новембар 2001

Увод

Државе Чланице Савета Европе и друге државе потписнице,

Сматрајући да је циљ Савета Европе да постигне веће јединство својих чланова;

Признавајући важност промовисања сарадње са другим државама чланицама ове Конвенције;

Убеђене у потребу да се као приоритетна спроводи заједничка казнена политика у сврху заштите друштва од сајберкриминала, интер алиа усвајањем одговарајуће легислативе и унапређивањем међународне сарадње;

Свесне дубоких промена које је донела дигитализација, конвергенција и стални тренд ка глобализацији компјутерских мрежа;

Свесне ризика да се компјутерске мреже и електронске информације могу такође користити за извршење кривичних дела и да доказни материјали који се односе на такве преступе могу бити ускладиштени у тим мрежана или **преносени** преко њих;

Признавајући потребу сарадње између држава и приватних предузећа у борби против сајберкриминала и потребу заштите легитимних интереса у коришћењу и развоју информатичке технологије;

Са уверењем да ефикасна борба против сајберкриминала захтева повећану, брзу и веома функционалну међународну сарадњу у кривичним стварима;

Убеђене у неопходност ове конвенције у циљу спречавања дела усмерених против поверљивости, интегритета и доступности компјутерских система, мрежа и компјутерских података, као и спречавања злоупотребе тих система, мрежа и података на тај начин што ће се предвидети казнене мере за таква чињења као што је описано у овој конвенцији и што ће се усвојити мере довољне за ефикасну борбу против таквих кривичних дела, на тај начин што ће се на унутрашњем и међународном нивоу олакшати откривање, истрага и гоњење таквих кривичних дела и што ће се обезбедити услови за брзу и поуздану међународну сарадњу;

Свесне потребе да се обезбеди одговарајући баланс између потребе за спровођењем закона и поштовања основних људских права садржаних у Конвенцији Савета Европе о заштити људских права и основних слобода из 1950 године, Међународној конвенцији о грађанским и политичким правима Уједињених Нација из 1966 године, као и другим важећим међународним уговорима о људским правима који реafirмишу право сваког појединца да има сопствено мишљење без икаквог ометања, као и право на слободу изражавања, које обухвата слободу да, без обзира на границе, тражи, прима и да са другима дели информације и идеје свих врста, и права која се тичу приватности сваког појединца.

Свесне такође потребе заштите личних података, као што је предвиђено на пример у Конвенцији Савета Европе о заштити лица у односу на аутоматску обраду личних података из 1981 године;

Узимајући у обзир Конвенцију Уједињених Нација о правима детета из 1989 године и Конвенцију о најгорим облицима дечијег рада међународне организације рада из 1999 године;

Узимајући у обзир постојеће конвенције Савета Европе о сарадњи у области казнене политике као и сличне уговоре који постоје између држава чланица Савета Европе и осталих држава, и наглашавајући да је сврха ове конвенције да допуни те конвенције како би кривичну истрагу и процедуре које се тичу кривичних дела у вези компјутерских система и података учинила ефикаснијом и да би омогућила прикупљање доказа за та кривична дела у електронском облику;

Поздрављајући најновији развој догађаја који даље унапредјује међународно разумевање и сарадњу у сузбијању сајберкриминала, укључујући ту акције Уједињених Нација, ОЕЦД-а, Европске Уније и групе Г 8;

Подсећајући на препоруку број Р (85) 10 која се тиче практичне примене Европске Конвенције о узајамној помоћи у кривичним стварима у случајевима "леттерс рогатору" за пресретање комуникација, препоруку број Р (88) 2 о пиратерији у области ауторских и њима сличних права, препоруку број Р (87) 15 која регулише коришћење личних података у полицијске сврхе, препоруку број Р (95) 4 о заштити личних података у области телекомуникационих услуга са посебним освртом на телефонске услуге, као и препоруку број Р (89) 9 о преступима који су у вези са компјутерима, која даје смернице националним законодавствима у погледу дефинисања одређених преступа који су у вези са компјутерима, и препоруку број Р (95) 13 која се тиче проблема процедуралног кривичног права у вези са информатичком технологијом;

Узимајући у обзир Резолуцију број 1 коју је усвојило Европско министарство правде на свом 21-ом заседању (Праг, јуна 1997) и која препоручује Комитету министара да подржи напоре које је Европски комитет за питања кривичног права (ЦДПЦ) уложио како би међусобно приближио одредбе националних кривичних законика на пољу сајберкриминала и омогућио коришћење ефикасних начина спровођења истраге у вези таквих кривичних дела, као и Резолуцију број 3 усвојену на 23-ћем заседању Конференције Европских министара правде (Лондон, јун 2000) која подстиче учеснике договарања у њиховим напорима да пронађу одговарајућа решења која ће омогућити што већем броју држава да постану чланице ове Конвенције, и која признаје потребу за бржим и ефикасним системом међународне сарадње који узима у обзир специфичне захтеве борбе за сузбијање сајберкриминала;

Узимајући такође у обзир акциони план који су усвојили шефови држава и влада Савета Европе приликом њиховог другог састанка (Стразбур, 10 – 11 октобар 1997), чији је циљ тражење заједничког одговора на развој нових информатичких технологија, базираног на стандардима и принципима Савета Европе;

договориле су се о следећем:

Поглавље 1 - Употреба термина

Члан 1 Дефиниције

У сврху ове Конвенције:

а. Израз "компјутерски систем" означава сваки уређај или групу међусобно повезаних или условљених уређаја, од којих један или више њих, у зависности од програма, врши аутоматску обраду података;

б. Израз "компјутерски подаци" означава свако излагање чињеница, података или концепата у облику који је погодан за њихову обраду у компјутерском систему, укључујући ту и одговарајући програм на основу којег компјутерски систем врши своју функцију;

ц. Израз "давалац услуга" означава:

и. Свако јавно или приватно лице које корисницима пружа своје услуге на пољу комуницирања путем компјутерских система, и

ии. Свако друго лице које обрађује или складишти компјутерске податке за рачун таквих комуникацијских услуга или за рачун корисника таквог сервиса.

д. Израз "промет података" означава све компјутерске податке који су у вези са комуницирањем путем компјутерских система, а које генерише компјутерски систем и који чине део ланца комуницирања, у којима се садрже подаци о пореклу, одредишту, путањи, времену, датуму, величини, трајању и врсти предметне услуге.

Поглавље 2 - Мере које ће се предузимати на националном нивоу

Део 1 - Материјално кривично право

Одељак 1 – Кривична дела против поверљивости, интегритета и доступности компјутерских података и система

Члан 2 Недозвољени приступ

Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се бесправно приступање компјутерском систему као целини или неком његовом делу, када се учини намерно, оквалификовало у њеном националном праву као кривично дело. Чланица може да услови да дело мора бити учињено кршењем безбедносних мера са намером прибављања компјутерских података или са неком другом нечасном намером, или учињено у вези са компјутерским системом који је повезан са другим компјутерским системом.

Члан 3

Недозвољено пресретање

Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се у њеном националном праву као кривично дело оквалификовало бесправно пресретање преноса компјутерских података који нису јавне природе, ка компјутерском систему, од њега или унутар самог система, у шта спада и електромагнетска емисија из компјутерских система којом се преносе такви подаци, а кад је учињено са намером и уз помоћ техничких уређаја. Чланица може условити да дело мора бити учињено са нечасним намерама, или учињено у вези са компјутерским системом који је повезан са другим компјутерским системом.

Члан 4

Ометање података

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се бесправно оштећење, брисање, кварење, мењање или прикривање компјутерских података оквалификовало у њеном националном праву као кривично дело, уколико се учини са намером.

2. Чланица може резервисати право да услови да дела из става 1 морају да резултирају великом штетом.

Члан 5

Ометање система

Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се у њеном националном праву као кривично дело оквалификовало бесправно и у већем степену ометање функционисања компјутерских система путем уношења, преношења, оштећења, брисања, кварења, мењања или прикривања компјутерских података, уколико је учињено са намером.

Члан 6

Злоупотреба уређаја

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се у њеном националном праву као кривично дело, уколико је учињено са намером и бесправно, оквалификовало следеће:

а. Производња, продаја, набављање ради употребе, увоз, дистрибуција и други видови стављања на располагање:

и. Средства, што подразумева и компјутерске програме, пројектоване или преуређење првенствено у сврху извршења неког од дела наведених у цлановима 2 – 5.

ии. Компјутерских лозинки, шифри за приступ, или сличних података путем којих се може приступити компјутерском систему као целини или неком његовом делу са намером да буде употребљен у сврху извршења неког од дела наведених у цлановима 2 – 5, и

б. Поседовање неке од ствари наведених у горњим ставовима (а)(1) или (2), са намером да се употреби у сврху извршења неког од дела наведених у члановима 2 – 5. Чланица може кроз закон условити да се мора поседовати одређени број поменутих ствари да би постојала кривична одговорност.

2. Не сме се тумачити да овај члан успоставља кривичну одговорност у случају када производња, продаја, набављање ради употребе, увоз, дистрибуција и други видови стављања на располагање, или поседовање, о којима је реч у ставу 1 овог члана, не служе у сврху извршења дела наведених у члановима 2 до 5 ове конвенције, на пример када служе за овлашћено тестирање или заштиту компјутерских система.

3. Свака чланица може резервисати право да не примени став 1 овог члана, под условом да се та резервација не односи на продају, дистрибуцију и друге видове стављања на располагање ствари наведених у ставу 1 (а) (2).

Одељак 2 – Кривична дела у вези са компјутерима

Члан 7

Фалсификовање које је у вези са компјутерима

Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се у њеном националном праву као кривично дело оквалификовало уношење, мењање, брисање или прикривање компјутерских података које резултира у подацима који нису аутентични, са намером да се учини да они буду сматрани за аутентичне и да се са њима у редовне сврхе поступа као да су аутентични, без обзира на то да ли су ти подаци директно читљиви и разумљиви. Чланица може условити да постоји намера преваре, или слична нечасна намера, да би се установила кривична одговорност.

Члан 8

Преваре које су у вези са компјутерима

Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се у њеном националном праву као кривично дело оквалификовало уношење имовинске штете другим лицима када се то учини бесправно и са намером, на следеће начине:

- а. Било каквим уношењем, мењањем, брисањем или прикривањем компјутерских података,
- б. Било каквим ометањем функционисања компјутерских система,

Са намером преваре или другом нечасном намером да се бесправно прибави економска добит за себе или за друга лица.

Одељак 3 – Кривична дела у односу на садржај

Члан 9

Кривична дела везана за дечију порнографију

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се у њеном националном праву као кривично дело оквалификовале следеће радње, ако се учине намерно и бесправно:

- а. Производња дечије порнографије у циљу њене дистрибуције преко компјутерских система;
- б. Нуђење или стављање на располагање дечије порнографије преко компјутерских система;
- ц. Дистрибуција или преношење дечије порнографије преко компјутерских система;
- д. Добављање дечије порнографије преко компјутерских система за себе или за друга лица;
- е. Поседовање дечије порнографије у компјутерском систему или на медијима за смештање компјутерских података.

2. У сврху горњег става 1 израз "дечија порнографија" обухвата порнографски материјал који визуелно приказује:

- а. Малолетника који учествује у експлицитно сексуалном чину;
- б. Лице по чијем се изгледу може закључити да је малолетник, које учествује у експлицитно сексуалном чину;
- ц. Реалистичке слике које представљају малолетника који учествује у експлицитно сексуалном чину;

3. У сврху горњег става 2 израз "малолетник" обухвата сва лица млађа од 18 година. Чланица може, међутим, да постави нижу старосну границу, која не сме бити мања од напуњених 16 година.

4. Свака чланица може себи резервисати право да не примењује, у целини или делимично, ставове 1 (д), 1 (ц), 2 (б) и 2 (ц).

Одељак 4 - Кривична дела који се односе на кршење ауторских и њима сличних права

Члан 10

Дела која се односе на кршење ауторских и њима сличних права

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се у њеном националном праву као кривично дело оквалификовало кршење ауторских права, дефинисаних у законима те чланице који се односе на обавезе које је она преузела по Париском акту од 24 јула 1971 о Конвенцији из Берна о заштити литерарних и уметничких дела, затим по Уговору о комерцијалним аспектима права на интелектуалну својину и WIPO уговору о ауторским правима, изузимајући морална права садржана у тим Конвенцијама, када су та дела учињена намерно, у обиму који их квалификује да имају комерцијални карактер, а учињена су помоћу компјутерских система.

2. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се у њеном националном праву као кривично дело оквалификовало кршење сличних права дефинисаних у законима те чланице који се односе на обавезе које је она преузела по Медјународној конвенцији из Рима о заштити извођача, произвођача фонограма и емисионих организација, (Римска конвенција), затим по Уговору о комерцијалним аспектима права на интелектуалну својину и WIPO уговору о ауторским правима, изузимајући морална права садржана у тим Конвенцијама, када су та дела учињена намерно, у обиму који их квалификује да имају комерцијални карактер, а учињена су помоћу компјутерских система.

3. Свака чланица може себи резервисати право да у ограниченом броју случајева не примењује кривичну одговорност по ставовима 1 и 2 овог члана, под условом да на располагању стоје друге врсте ефикасних правних средстава и да та резерва не негира међународне обавезе те чланице дефинисане у међународним инструментима наведеним у ставу 1 и 2 овог члана.

Одељак 5 – Споредна одговорност и санкције

Члан 11

Покушај и помагање или подстрекивање

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се у њеном националном праву као кривично дело оквалификовало намерно помагање или подстрекивање на извршење неког од преступа дефинисаних у члановима 2 – 10 ове конвенције, са намером да се такав преступ учини.

2. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се у њеном националном праву као кривично дело оквалификовао намерно учињен покушај извршења неког од дела дефинисаних у члановима 3 до 5, 7, 8, 9 (1) а. и 9 (1) ц. ове конвенције.

3. Свака чланица може себи резервисати право да не примењује, у целини или делимично, став 2 овог члана.

Члан 12

Одговорност правних лица

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се правна лица могла позвати на одговорност за кривично дело установљено на основу ове конвенције, који је извршило физичко лице које има руководећу улогу у том правном лицу делујући као појединац или као део неког органа правног лица, а на основу:

- а. Овлашћења да заступа правно лице;
- б. Овлашћења да доноси одлуке за рачун правног лица;
- ц. Овлашћења да врши контролу унутар тог правног лица.

2. Осим случајева који су предвиђени у ставу 1, свака чланица треба да предузме мере неопходне да би се правно лице могло сматрати одговорним и у случајевима када је непостојање надзора или контроле од стране физичких лица наведених у ставу 1 омогућило извршење кривичних преступа дефинисаних у складу са овом конвенцијом, које је извршило физичко лице за рачун тог правног лица и у његово име.

3. У зависности од правних принципа појединих чланица, одговорност правног лица може бити кривичне, грађанске или административне природе.

4. Та одговорност неће искључивати кривичну одговорност физичког лица које је преступ извршило.

Члан 13

Санкције и мере

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се омогућило да кривична дела установљена у складу са ставовима 2 – 11 подлежу ефикасним, пропорционалним и одвраћајућим санкцијама које обухватају и лишење слободе.

2. Свака чланица треба да омогући да правно лице које је одговорно на основу члана 12, подлеже ефикасним, пропорционалним и одвраћајућим кривичним санкцијама, или санкцијама које нису кривичне природе, а које обухватају и новчане казне.

Део 2 – Процедурално право

Одељак 1 – Заједничке одредбе

Члан 14

Област примене процедуралних одредби

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би успоставила она овлашћења и процедуре, који су предвиђени у овом одељку, у сврху одређених кривичних истрага и поступака.

2. Изузев ако чланом 21 није другачије предвиђено, свака чланица ће овлашћења и процедуре наведене у ставу 1 примењивати на:

- а. Кривична дела установљена у складу са члановима 2 – 11 ове конвенције;
- б. Остале кажњиве преступе извршене помоћу компјутерских система; и
- ц. Прикупљање доказа за кажњиве преступе у електронској форми.

3. а. Свака чланица може резервисати право да мере наведене у члану 20 примени само на оне преступе или категорије преступа које специфицира у својој резерви, под условом да опсег тих преступа или категорија преступа није ограничен више од опсега преступа на које се примењују мере наведене у члану 21. Свака чланица треба да настоји да своју резерву сведе на што мањи обим како би се мере наведене у члану 20 могле примењивати што шире.

б. У случају да чланица, услед ограничења своје легислативе која је била на снази у време усвајања садашње конвенције, није у стању да мере наведене у члановима 20 и 21 примени на комуницирање које се одвија унутар компјутерских система даваоца услуга у случају када ти системи:

и. функционишу за рачун затворене групе корисника, и

и. не користе јавне комуникационе мреже и нису повезани са другим компјутерским системом, било јавним било приватним,

онда та чланица може резервисати право да не примењује те мере на такав тип комуницирања. Свака чланица треба да настоји да своју резерву сведе на што мањи обим како би се мере наведене у члановима 20 и 21 могле примењивати што шире.

Члан 15

Услови и ограничења

1. Свака чланица треба да обезбеди да успостављање, имплементирање и примена овлашћења и поступака наведених у овом одељку, подлеже условима и ограничењима предвиђеним националним правом, које мора омогућити адекватну заштиту људских права и слобода, укључујући и права која произилазе из обавеза које је чланица преузела по основу конвенције Савета Европе о заштити људских права и основних слобода из 1950 године, Медјународног пакта Уједињених Нација о грађанским и политичким правима из 1966 године и осталих важећих међународних докумената о људским правима, и које ће поштовати принцип пропорционалности.

2. Ти услови и ограничења могу, у зависности од карактера овлашћења или процедура о којима се ради, измедју осталог, обухватати судску контролу или другу врсту независног надзора, основе које оправдавају примену тих овлашћења или процедура, и ограничење подручја примене и трајања овлашћења или процедура.

3. У степену који је сагласан са јавним интересима, а нарочито са правилном применом права, чланица треба да размотри утицај који овлашћења и процедуре из ове секције имају на права, одговорности и легитимне интересе трећих страна.

Одељак 2 – Експедитивно конзервисање и заштита ускладиштених компјутерских података

Члан 16

Експедитивно конзервирање ускладиштених компјутерских података

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би своје надлежне органе овластила да могу да нареду или на други сличан начин постигну експедитивно конзервисање и заштиту одређених компјутерских података, укључујући ту и податке везане за пренос података, који су ускладиштени коришћењем компјутерских система, а посебно у случају када постоји основана сумња да су компјутерски подаци нарочито изложени губљењу или изменама.

2. Када чланица спроведе у дело горњи став 1 тако што нареди лицу да сачува и заштити одређене ускладиштене компјутерске податке који су у поседу тог лица или су под његовом контролом, чланица треба да донесе такве легислативне и остале неопходне мере да би могла то лице да обавезе да интегритет тих компјутерских података штити и сачува на онај временски период колико је потребно, а највише до 90 дана, како би се надлежним органима омогућило да податке прегледају. Чланица може да предвиди да се наведена наредба може узастопно обнављати.

3. Свака чланица треба да усвоји такве легислативне и остале неопходне мере којима може да обавезе лице које чува или лице које штити компјутерске податке да покретање такве процедуре држи у тајности на период који је за то предвиђен у националном законодавству.

4. На овлашћења и процедуре о којима је реч у овом члану примењиваће се одредбе чланова 14 и 15.

Члан 17

Експедитивно конзервирање и заштита и делимично откривање података о преносу

1. Свака чланица треба да усвоји, у вези са подацима о преносу које треба сачувати на основу члана 16, такве легислативне и остале неопходне мере да би:

а. Обезбедила да експедитивна конзервација података о преносу буде могућа без обзира да ли је у преносу тог комуницирања учествовао један давалац услуга или више њих, и

б. Обезбедила да се надлежним органима те чланице или лицу које ти органи именују, може експедитивно открити она количина података о преносу која ће бити довољна за идентификацију даваоца услуга и путање којом је пренос извршен.

2. На овлашћења и процедуре наведене у овом члану примењују се одредбе чланова 14 и 15.

Одељак 3 – Издавање наредбе

Члан 18

Издавање наредбе

1. Свака чланица треба да усвоји такве легислативне и остале мере које су потребне да би своје надлежне органе овластила да могу наредити:

а. Сваком лицу на територији чланице да мора предати одређене компјутерске податке које поседује односно који су под његовом контролом, а који су смештени на компјутерском систему или на медијуму за смештај компјутерских података; и

б. Сваком даваоцу услуга који своје услуге врши на територији те чланице да мора предати податке о претплатнику на те услуге које тај даваоц услуга поседује или над којима има контролу;

2. На овлашћења и процедуре које се наводе у овом члану односице се одредбе чланова 14 и 15.

3. У сврху овог члана, израз "подаци о претплатнику" означава сваки податак који постоји у облику компјутерских података или у било ком другом облику, које поседује давалац услуга и који се односе на претплатника на његове услуге, при чему се изузимају подаци о преносу или подаци из садржаја који се преноси, на основу којих се може установити:

- а. Врста комуникацијских услуга које је користио, техничке услуге и временски период коришћења услуга;
- б. Идентитет претплатника, његова поштанска адреса или географска локација, број телефона и остали бројеви преко којих се може контактирати, листинг плаћања и подаци о плаћању, који су доступни кроз уговор или другу врсту споразума о коришћењу услуга;
- ц. Свака информација о локацији на којој је комуникациона опрема постављена, до које се може доћи преко уговора или споразума друге врсте о коришћењу услуга.

Одељак 4 – Претраживање и заплена компјутерских података

Члан 19

Претраживање и заплена ускладиштених компјутерских података

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би овластила своје надлежне органе да на њеној територији могу претражити или на сличан начин приступити:

- а. Компјутерском систему или неком његовом делу и компјутерским подацима који су тамо смештени; и
- б. Медијумима за смештај компјутерских података на којима би одређени компјутерски подаци могли бити смештени.

2. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би у случају када њени надлежни органи претражују или на сличан начин приступе компјутерском систему или неком његовом делу у складу са ставом 1 (а) и основано посумњају да су подаци које траже смештени на другом компјутерском систему или делу система на територији те чланице, при чему су подаци редовно доступни са првог система, ти надлежни органи могли да одмах прошире своју претрагу или сличан начин приступа и на тај други компјутерски систем.

3. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би своје надлежне органе могла овластити да заплене или на сличан начин обезбеде компјутерске податке до којих су дошли у складу са ставом 1 или 2. Те мере треба да обухвате средства и овлашћења:

- а. Да се заплени или на сличан начин обезбеди компјутерски систем или његов део, или медијум за смештај компјутерских података;
- б. Да се направи и задржи копија тих компјутерских података
- ц. Да се одржи интегритет важних ускладиштених компјутерских података; и

д. Да се ти компјутерски подаци учине неприступачним или да се уклоне из компјутерског система коме се приступило.

4. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би своје надлежне органе могла овластити да нареду сваком лицу које познаје функционисање компјутерског система или познаје мере заштите компјутерских података на том систему, да пружи све потребне податке како би се омогућило предузимање мера наведених у ставовима 1 и 2.

5. На овлашћења и процедуре наведене у овом члану примењују се одредбе чланова 14 и 15.

Одељак 5 – Прикупљање компјутерских података у реалном времену

Члан 20

Прикупљање информација о промету података у моменту њиховог настајања (у реалном времену)

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би своје надлежне органе могла овластити да:

а. На територији те чланице прикупљају или снимају примењујући техничка средства, и
б. Приморају даваоца услуга да у оквиру његових техничких могућности

и. на територији те чланице прикупља или снима примењујући техничка средства, или
ии. сарађује са надлежним органима и помаже им у прикупљању или снимању у реалном времену података који се односе на пренос одређеног комуницирања на њеној територији које се преноси преко компјутерских система.

2. У случајевима када чланица, због принципа који постоје у њеном националном правном систему, не може да усвоји мере које се наводе у ставу 1 (а), може уместо тога да усвоји законодавне и друге мере које су потребне да би омогућила прикупљање или снимање у реалном времену података који се односе на пренос одређеног комуницирања које се обавља на њеној територији а преко техничких средстава која се налазе на тој територији.

3. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би даваоца услуга могла обавезати да чува тајност свих информација о спровођењу и у вези спровођења мера предвиђених у овом члану.

4. На овлашћења и процедуре наведене у овом члану примењују се одредбе чланова 14 и 15.

Члан 21

Пресретање података који се налазе у садржају електронских комуникација

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере, у вези са низом тешких прекршаја који ће бити специфицирани кроз национално право, да би омогућила својим надлежним органима да:

а. На територији те чланице прикупљају или снимају применом техничких уређаја, и да
б. Приморају даваоца услуга да у оквиру својих техничких могућности:

и. на територији те чланице прикупља или снима применом техничких уређаја, или
ии. сарађује и помаже надлежним органима у прикупљању или снимању
у реалном времену података који се налазе у садржају одређеног комуницирања на њеној
територији, који се преносе преко компјутерских система.

2. У случајевима када чланица, због принципа који постоје у њеном националном правном
систему, не може да усвоји мере које се наводе у ставу 1 (а), може уместо тога да усвоји
законодавне и друге мере које су потребне да би омогућила прикупљање или снимање у
реалном времену података који потичу из садржаја одређених комуницирања на њеној
територији кроз примену техничких уређаја који се налазе на тој територији.

3. Свака чланица треба да усвоји законодавне и друге мере које су потребне да би обавезала
даваоца услуга да као поверљиву чува чињеницу о примени свих мера предвиђених у овом
члану, као и тајност свих података.

4. На овлашћења и процедуре наведене у овом члану примењују се одредбе чланова 14 и 15.

Део 3 – Јурисдикција

Члан 22 Јурисдикција

1. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би
успоставила своју јурисдикцију над свим преступима установљеним у складу са члановима 2
– 11 ове конвенције, у случају када је преступ извршен:

- а. На територији те чланице; или
- б. На броду под заставом те чланице; или
- ц. У ваздухоплову који је регистрован на основу закона те чланице; или
- д. Од стране њеног држављана, уколико је преступ кажњив по кривичним законима оне
територије на којој је извршен, или уколико је преступ извршен изван територијалне
јурисдикције било које државе.

2. Свака чланица може резервисати право да не примењује, или да само у одређеним
случајевима или под одређеним околностима примењује правила о надлежности дефинисана
у ставовима (1) б – (1) д овог члана или у неком другом делу тога текста.

3. Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би након
захтева за екстрадицију успоставила своју јурисдикцију над преступима наведеним у члану
24, став (1) ове конвенције, у случајевима када се осумњичени починилац налази на њеној
територији а чланица га, само на основу његовог или њеног држављанства, не изручи другој
чланици.

4. Ова конвенција не искључује кривичну јурисдикцију која се врси у складу са националним правом.

5. У случају када више чланица захтева јурисдикцију над преступом установљену у складу са овом конвенцијом, умешане чланице ће се међусобно консултовати да би одредиле чија јурисдикција је за поступак најпогоднија.

Поглавље 3 – Међународна сарадња

Део 1 – Општи принципи

Одељак 1 – Општи принципи који се односе на међународну сарадњу

Члан 23

Општи принципи који се односе на међународну сарадњу

Чланице ће сарађивати међусобно у највећем могућем степену, у складу са одредбама ове конвенције, кроз примену релевантних међународних докумената о међународној сарадњи у кривичним стварима, кроз договоре склопљене на бази једнаке или реципрочне легислативе и у складу са националним правима, у сврху истраге или процедура које се односе на кривичне преступе у вези компјутерских система и података, или у сврху прикупљања доказа у електронском облику.

Одељак 2 – Принципи који се односе на екстрадицију

Члан 24

Екстрадиција

1. а. Овај члан односи се на екстрадицију која се врши измедју чланица за кривична дела установљена у складу са члановима 2 – 11 ове конвенције, под условом да су она по законима обе чланице кажњива затворском казном од најмање годину дана или строжијом казном.
б. У случају када се може применити различита минимална казна на основу договора склопљеног на бази једнаке или реципрочне легислативе, или на основу уговора о екстрадицију, укључујући ту и Европску конвенцију о екстрадицији (ЕТС Но. 24), који се примењују на две или више чланица, примениће се минимална казна предвиђена тим договорима или уговорима.

2. За кривична дела описана у ставу 1 овог члана сматраће се да спадају у групу преступа који подлежу екстрадицији у сваком уговору о екстрадицији који постоји између две или више чланица. Чланице се обавезују да у сваки уговор о екстрадицији, који ће бити закључен између две чланице или више њих, те преступе укључе у групу преступа који подлежу екстрадицији.

3. Кад чланица која екстрадицију условљава постојањем одговарајућег уговора прими захтев за изручење од друге чланице са којом нема уговор о екстрадицији, она може ову конвенцију сматрати као правни основ за изручење за свако кривично дело наведено у ставу 1 овог члана.

4. Чланице које изручење не условљавају постојањем одговарајућег уговора ће кривична дела наведена у ставу 1 овог члана сматрати за преступе који подлежу међусобној екстрадицији.

5. Екстрадиција ће бити подложна условима који су предвиђени законима замољене чланице или важећим уговорима о екстрадицији, укључујући ту и разлоге на основу којих замољена чланица може да одбије екстрадицију.

6. Уколико се екстрадиција за кривично дело наведено у ставу 1 овог члана одбије само на основу држављанства лица чије се изручење тражи, или зато што замољена чланица сматра да има јурисдикцију над тим преступом, замољена чланица ће на захтев чланице која подноси захтев поднети случај својим надлежним органима у сврху кривичног гоњења и благовремено ће чланица која тражи саопштити крајњи исход. Наведени надлежни органи ће донети своју одлуку, спровешће истрагу и друге процедуре на исти начин по законима те чланице као у случају било ког другог преступа сличне природе.

7. а. Свака чланица ће, приликом потписивања или приликом депоновања њених инструмената ратификације, прихватања, одобравања или приступања, доставити Генералном секретару Савета Европе име и адресе свих установа које су у случају непостојања уговора одговорне за подношење или слање захтева за екстрадицију или притвор.

б. Генерални секретар Савета Европе ће формирати и одржавати ажурност регистра тих установа које чланице именују. Свака чланица ће се старати да детаљи у регистру буду увек тачни.

Одељак 3 – Општи принципи у вези међусобне помоћи

Члан 25

Општи принципи у вези међусобне помоћи

1. Чланице треба да једна другој пружају помоћ у највећем могућем степену у циљу истраге или процедура које се тичу кажњивих дела у вези компјутерских система и података, или у прикупљању, у електронском облику, доказа за кривично гоњење.

2. Свака чланица треба такође да усвоји такве легислативне и остале мере које су потребне да би могла извршавати своје обавезе одређене у члановима 27 – 35.

3. Свака чланица може, у хитним случајевима, да захтева међусобну помоћ или комуницирање у вези тога користећи се експедитивним начинима комуницирања у које спада факс и електронска пошта, до оног степена који обезбеђује одговарајући безбедносни ниво и

аутентичност (укључујући коришћење шифровања када је потребно), с тим што ће на захтев замољене чланице морати да следи и званична потврда таквог комуницирања. Замољена чланица треба да прихвати такав захтев и да на њега одговори исто тако експедитивним начином комуницирања.

4. Изузев уколико није другачије одређено у члановима овог поглавља, узајамна помоћ ће бити подложна условима који су предвиђени законима замољене чланице, или важећим уговорима о међусобној помоћи, у шта спадају и услови на основу којих замољена чланица може да одбије сарадњу.

5. У случајевима када је, у складу са одредбама из овог поглавља, замољеној чланици дозвољено да међусобну сарадњу услови постојањем обостране кажњивости, сматраће се да је тај услов испуњен, без обзира да ли закони замољене чланице стављају тај преступ у исту категорију преступления или га означавају истим терминима као у чланици која захтева сарадњу, уколико чињење које је основа преступления у вези којег се сарадња захтева, представља кривично дело и по њеним законима.

Члан 26

Спонтане информације

1. Чланица може, у границама свог националног права, без претходног захтева, да другој чланици проследи информације до којих је дошла у оквиру сопствених истрага уколико сматра да би откривање таквих информација могло помоћи чланици која их прима у покретању или вођењу истраге или других процедура које се тичу кажњивих дела установљених у складу са овом конвенцијом, или би могло водити томе да та чланица упути, на основу овог поглавља, захтев за међусобну сарадњу.

2. Пре него што достави такве информације, чланица која их доставља може захтевати да оне буду чуване у тајности или да се могу користити само под одређеним условима. Уколико чланица која информације прима не може да прихвати такав захтев, она мора о томе да обавести чланицу која доставља информације, која ће након тога одлучити да ли ће ипак да проследи информације. Уколико чланица прихвати информације под одређеним условима, ти услови ће за њу бити обавезујући.

Одељак 4 – Процедуре које се односе на захтеве за међусобну сарадњу у случају непостојања важећих међународних уговора

Члан 27

Процедуре које се односе на захтеве за међусобну сарадњу у случају непостојања важећих међународних уговора

1. Уколико не постоји уговор или споразум о узајамној помоћи на основу униформног или реципрочног права, који је на снази између чланице која упућује захтев и чланице којој је захтев упућен, примењиваће се одредбе ставова 2 до 9 овог члана. Одредбе овог члана неће се примењивати уколико постоји такав уговор, договор или легислатива, изузев ако се те чланице сагласе да уместо тога примењују овај члан или његов део.

2. а. Свака чланица ће именовати централни овлашћени орган или органе који ће бити одговорни за слање захтева за узајамну помоћ, одговарање на њих, њихово извршавање или

прослеђивање органима надлежним за њихово извршење.

б. Централни органи ће међусобно комуницирати директно.

ц. Свака чланица ће приликом потписивања или депоновања њених инструмената ратификације, прихватања или приступања, доставити генералном секретару Савета Европе имена и адресе овлашћених органа именованих у складу са овим ставом.

д. Генерални секретар Савета Европе ће оформити регистар централних овлашћених органа које именују чланице и одржаваће га ажурним. Свака чланица има обавезу да регистру доставља тачне податке.

3. Захтеви за узајамну помоћ на основу овог члана извршаваће се у складу са процедурама које одреди чланица која упућује захтев, изузев уколико оне нису компатибилне са законима замољене чланице.

4. Замољена чланица може, поред основа за одбијање наведених у члану 25 став (4), одбити помоћ у следећим случајевима:

а. Уколико се захтев односи на преступ који замољена чланица сматра за политички или за преступ који је повезан са политичким преступом; или

б. Уколико сматра да извршење захтева може угрозити њен суверенитет, безбедност, јавни поредак или друге битне интересе.

5. Замољена чланица може да одложи извршење захтева уколико би оно угрозило кривичну истрагу или процедуре које спроводе њени органи.

6. Пре одбијања или одлагања извршења захтева, замољена чланица ће, након евентуалне консултације са чланицом која упућује захтев, размотрити да ли се захтеву може удовољити делимично или ће извршење захтева везати за испуњење одређених услова.

7. Замољена чланица ће хитно обавестити чланицу која упућује захтев о исходу извршења захтева за помоћ. Уколико се захтев одбија или одлаже, морају се навести разлози одбијања или одлагања. Замољена чланица ће такође чланицу која упућује захтев обавестити о сваком разлогу који онемогућава извршење захтева или ће вероватно у значајној мери одложити извршење.

8. Чланица која упућује захтев може тражити да замољена чланица чува тајност како самог захтева тако и садржаја захтева, који је поднет у складу са овим поглављем, до степена који је неопходан да би се захтев могао извршити. Уколико замољена чланица не може да испуни критеријум тајности, она треба одмах о томе да обавести чланицу која упућује захтев, која ће затим одлучити да ли ће захтев упркос томе проследити на извршење.

9. а. У хитним случајевима, захтев за узајамну помоћ или комуницирање у вези ће могу упутити судске власти чланице која упућује захтев директно одговарајућим властима замољене чланице. У таквим случајевима истовремено треба преко централног органа чланице која упућује захтев послати копију захтева централном органу замољене чланице,

б. Сваки захтев или комуницирање по овом ставу мора се спровести кроз Међународну организацију криминалистичке полиције (Интерпол).

ц. Ако је захтев поднет у складу са подставом (а) али овлашћени орган није компетентан да реши захтев, он ће захтев проследити националним установама које су за то компетентне и о томе директно обавестити чланицу која упућује захтев.

- д. Захтеви или комуницирање на основу овог става који за собом не повлаче мере присиле могу надлежни органи чланице која упућује захтев проследити директно надлежним органима замољене чланице.
- е. Свака чланица може, приликом потписивања или приликом депоновања њених инструмената ратификације, прихватања, одобравања или приступања, обавестити Генералног секретара Савета Европе да, због ефикасности, захтеви учињени на основу овог става морају бити упућени њеном централном овлашћеном органу.

Члан 28

Тајност и ограничења коришћења

1. Када између чланице која упућује захтев и замољене чланице не постоји важећи уговор или споразум о узајамном помагању на бази униформног или реципрочног права, примењиваће се одредбе овог члана. Одредбе овог члана се неће примењивати уколико такав уговор или споразум или одговарајућа легислатива постоји, изузев ако се чланице сагласе да уместо њих примењују овај члан у целини или делимично.
2. Замољена чланица може захтевано снабдевање информацијама или материјалима условити испуњењем следесих услова:
 - а. Да се сачува тајност уколико се захтеву за помоћ не може изаћи у сусрет
 - б. Да се оно не користи за друге истраге или процедуре осим оних које су наведене у захтеву
3. Уколико чланица која захтева помоћ не може да испуни услов из става 2, она треба одмах о томе да обавести другу чланицу, која ће затим да одлучи да ли ће и поред тога да достави информације. Ако чланица која захтева помоћ прихвати услов, она је обавезна да га испуни.
4. Свака чланица која доставља информације или материјале под условом наведеним у ставу 2, може захтевати од друге чланице да објасни, у вези тог услова, у коју ће сврху те информације или материјале да употреби.

Део 2 – Специфичне одредбе

Одељак 1 – Узајамна помоћ у односу на привремене мере

Члан 29

Експедитивно конзервирање компјутерских података

1. Свака чланица може од друге чланице захтевати да нареди или на неки други начин обезбеди експедитивно конзервирање података који су ускладиштени коришћењем компјутерског система који се налази на територији те друге чланице и у вези којих чланица која захтева има намеру да затражи узајамну помоћ у циљу претраге или сличне форме приступа тим подацима, њиховог одузимања, обезбеђивања или откривања.
2. У захтеву за конзервирање података поднетом на основу става 1 треба да буде специфицирано следеће:
 - а. Орган који захтева конзервирање података;

б. Преступ који је предмет кривичне истраге или поступка и сажет резиме чињеница у вези тога;

ц. Опис ускладиштених компјутерских података које треба конзервирати и њихове повезаности са преступом;

д. Сви расположиви подаци у циљу идентификације лица које поседује односно чува ускладиштене компјутерске податке, као и податке о локацији компјутерског система;

е. Разлог због којег је неопходно да се подаци конзервишу; и

ф. Изјава намере чланице да поднесе захтев за узајамну помоћ у циљу претраживања или сличну форму приступа компјутерским подацима, њиховог одузимања, обезбеђивања или откривања.

3. Након пријема захтева друге чланице, замољена чланица треба да предузме све мере које су неопходне да би експедитивно, у складу са националним правом, конзервирала тражене податке. У одговору на захтев не сме се као услов за спровођење конзервирања података захтевати постојање обостране кажњивости.

4. Чланица која, у вези других преступа осим оних установљених у члановима 2 – 11 ове конвенције, свој одговор на захтев за узајамну помоћ у циљу претраживања или сличног облика приступа компјутерским подацима, њиховог одузимања или сличног обезбеђивања или откривања, условљава постојањем обостране кажњивости, резервише право да одбије захтев за конзервирањем података у случајевима када има основа да сматра да у време откривања података захтев за постојањем обостране кажњивости неће бити испуњен.

5. осим тога, захтев за конзервирање података може бити одбијен само у следећим случајевима:

а. Када се захтев односи на преступ који замољена чланица сматра политичким преступом или сматра да је у вези са политичким преступом, или

б. Када замољена чланица сматра да извршење захтева може угрозити њен суверенитет, безбедност, јавни ред или друге битне интересе.

6. У случају када замољена чланица сматра да би конзервирањем онемогућила будућу доступност података или сматра да би тиме угрозила тајност или друге аспекте истраге коју води чланица која захтев упућује, она мора о томе одмах обавестити чланицу која захтев упућује, која ће затим да одлучи да ли ће и поред тога тражити испуњење свог захтева.

7. Свако конзервирање обављено на захтев наведен у ставу 1 биће извршено у трајању не мањем од 60 дана да би се чланица која захтев упућује омогућило да поднесе захтев за претраживање или слични облик приступа компјутерским подацима, њихово одузимања или слично обезбеђивање или откривање. Након пријема тог захтева, подаци ће наставити да буду конзервирани до исхода тог захтева.

Члан 30

Експедитивно откривање конзервираних података који се односе на пренос

1. Уколико замољена чланица, приликом извршавања захтева за конзервирањем података који се односе на пренос одређеног комуницирања, учињеног на основу члана 29, открије да је давалац услуга из друге државе умешан у пренос тог комуницирања, замољена чланица ће одмах чланица која је захтев упутила открити довољно података о том преносу и путању којом је комуницирање обављено да би се тај давалац услуга могао идентификовати.

2. Откривање података који се односе на пренос у складу са ставом 1 може се одбити само у следећим случајевима:

- а. Уколико се захтев односи на преступ који замољена чланица сматра за политички или за преступ који је повезан са политичким преступом; или
- б. Уколико замољена чланица сматра да извршење захтева може угрозити њен суверенитет, безбедност, јавни поредак или друге битне интересе

Одељак 2 – Узајамна помоћ у вези истраге

Члан 31

Узајамна помоћ у вези приступања ускладиштеним компјутерским подацима

1. Свака чланица може захтевати од друге чланице да претражи или на сличан начин приступи, одузме их или на сличан начин обезбеди и открије податке ускладиштене коришћењем компјутерских система који се налазе на територији замољене чланице, укључујући ту и податке који су конзервирани у складу са чланом 29.

2. Замољена чланица треба да одговори на захтев примењујући међународне инструменте, споразуме и законе наведене у члану 23, и у складу са осталим релевантним одредбама овог поглавља.

3. На захтев треба експедитивно одговорити уколико:

- а. Постоји основана сумња да су релевантни подаци веома подложни губитку или модификовању; или
- б. Инструменти, споразуми и закони наведени у ставу 2 и иначе налазу експедитивну сарадњу.

Члан 32

Прекогранични приступ ускладиштеним компјутерским подацима уз пристанак или у случају када су они јавни Чланица може, без тражења овлашћења од друге чланице:

- а. да приступи јавним (отвореним) ускладиштеним компјутерским подацима, без обзира где се подаци географски налазе; или
- б. Да приступи компјутерским подацима или да преко компјутерског система који се налази на њеној територији прими ускладиштене компјутерске податке који се налазе на територији друге чланице, уколико добије легалан и добровољни пристанак од лица које је овлашћено да открије податке тој чланици преко компјутерског система.

Члан 33

Узајамна помоћ у прикупљању у реалном времену података који се односе на пренос

1. Чланице треба да обезбеде узајамну помоћ у циљу прикупљања у реалном времену података о преносу који се односе на одређена комуницирања на територији једне од њих која су обављена преко компјутерских система. На основу одредби става 2, помоћ ће се вршити у складу са условима и процедурама предвиђеним у националном праву.

2. Свака чланица треба да пружи такву помоћ барем у случају оних кривичних дела за које би прикупљање у реалном времену података о преносу било могуће у сличном домаћем случају.

Члан 34

Узајамна помоћ у пресретању података из садржаја који се преноси

Чланице треба да обезбеде узајамну помоћ у циљу прикупљања или снимања у реалном времену података из садржаја одређених комуницирања која се преносе преко компјутерских система, до степена који дозвољавају важећи уговори и национално право.

Одељак 3 – Мреза типа "24/7"

Члан 35

Мрежа типа "24/7"

1. Свака чланица треба да одреди место за контакте које ће бити доступно 24 сата, свих 7 дана у недељи, да би омогућила моменталну помоћ у истражне сврхе или за процедуре у вези кривичних дела која се односе на компјутерске системе и компјутерске податке, или ради прикупљања доказа за кривична дела у електронском облику. Та помоћ треба да обухвати, или, уколико то национално право и правна пракса дозвољавају, да непосредно омогући:

а. Давање техничких савета

б. Конзервирање података у складу са члановима 29 и 30, и

ц. Прикупљање доказа, давање информација правног карактера и лоцирање осумњичених.

2. а. Место за контакте сваке чланице мора располагати могућностима довољним да може експедитивно преносити комуницирање са местом контакта друге чланице.

б. Уколико место за контакте које је одредила једна чланица није део овлашћених органа који су задужени за међународну узајамну помоћ или екстрадицију, то место за контакте мора да гарантује да са тим органима може експедитивно да сарађује.

3. Свака чланица треба да обезбеди увежбано и обучено особље да би мрежа могла да функционише.

Поглавље 4 – Финалне одредбе

Члан 36

Потписивање и ступање на снагу

1. Ова Конвенција отворена је за потпис за државе чланице Савета Европе и за државе које нису чланице, а које су учествовале у њеној изради.

2. Ова конвенција подлеже ратификацији, прихватању или одобрењу. Инструменти ратификовања, прихватања или одобравања треба да буду депоновани код Генералног секретара Савета Европе.

3. Ова конвенција ће ступити на снагу првог дана у месецу који следи након истека рока од три месеца од датума када пет држава, од којих су најмање три чланице Савета Европе, буде изразило свој пристанак да се обавезу овом Конвенцијом у складу са одредбама ставова 1 и 2.

4. За сваку државу потписницу која накнадно изрази свој пристанак да се обавезе Конвенцијом, она ће ступити на снагу првог дана у месецу који следи након истека рока од три месеца од датума када је она изразила свој пристанак да се обавезе овом Конвенцијом у складу са одредбама ставова 1 и 2.

Члан 37

Приступање конвенцији

1. Након ступања на снагу ове конвенције, Комитет министара Савета Европе, након консултовања са државама потписницама ове конвенције и добијања њиховог једногласног пристанка, може да позове сваку државу која није чланица Савета и која није учествовала у изради, да приступи овој конвенцији. Одлука о томе доноси се већином предвиђеном чланом 20 (д) Статута Савета Европе и једногласним изгласавањем од стране представника држава чланица које су овлашћене да присуствују Комитету министара.

2. За сваку државу која овој конвенцији приступа у складу са горњим ставом 1, она ће ступити на снагу првог дана у месецу који следи након истека рока од три месеца од датума депоновања инструмента приступања код Генералног секретара Савета Европе.

Члан 38

Примена у односу на територију

1. Свака држава може, у тренутку потписивања или приликом депоновања својих инструмената ратификације, прихватања, одобравања или приступања, да дефинише територију или територије на којима ће се ова конвенција примењивати.

2. Свака држава може, касније, изјавом упућеном Генералном секретару Савета Европе да примењивање ове конвенције прошири на било коју другу територију наведену у изјави. У односу на ту територију, ова конвенција ће ступити на снагу првог дана у месецу који следи након истека рока од три месеца од датума када је Генерални секретар изјаву примио.

3. Свака изјава која је дата на основу два претходна става може бити, у односу на сваку територију наведену у таквој изјави, повучена на основу обавештења упућеног Генералном секретару Савета Европе. Повлачење изјаве ступиће на снагу првог дана у месецу који следи након истека рока од три месеца од датума када је Генерални секретар примио такво обавештење.

Члан 39

Дејство конвенције

1. Сврха ове конвенције је да допуни мултилатералне или билатералне уговоре или споразуме између чланица, укључујући следеће одредбе:

- Европска конвенција о екстрадицији, која је била отворена за потписивање 13 децембра 1957 у Паризу (ЕТС Но. 24);
- Европска конвенција о узајамној помоћи у кривичним стварима, која је била отворена за потписивање 20 априла 1959 у Стразбуру (ЕТС Но. 30);
- Додатни протокол Европске конвенције о узајамној помоћи у кривичним стварима, која је била отворена за потписивање 17 марта 1978 у Стразбуру (ЕТС Но. 99).

2. Уколико су две или више чланица већ закључиле споразум или уговор о стварима на које се односи ова конвенција, или су на други начин уредиле своје односе у вези тих ствари, или уколико то у будућности ураде, оне ће моћи такође да примењују тај споразум или уговор. Медјутим, уколико чланице уреде своје односе у вези ствари на које се односи ова конвенција другачије него што је њоме предвиђено, оне то могу спроводити на начин који није у супротности са циљевима и принципима ове конвенције.

3. Ништа у овој конвенцији не сме утицати на друга права, ограничења, обавезе и одговорности чланица.

Члан 40 Изјаве

Свака чланица ове конвенције може, писменом изјавом упућеном Генералном секретару Савета Европе приликом потписивања или приликом депоновања својих инструмената ратификације, прихватања, одобравања или приступања, да изјави да ће искористити могућност захтевања додатних елемената предвиђених у члану 2, члану 3, члану 6, став 1 (б), члану 7, члану 9, став 3 и члану 27, став 9 (е).

Члан 41 Федерална клаузула

1. Федерална држава може да резервише право да преузме оне обавезе по поглављу ИИ ове конвенције које су у складу са основним принципима на којима се заснива веза њене централне владе и конститутивних држава или других сличних територијалних јединица, под условом да и поред тога има могућност да сарађује у складу са одредбама поглавља ИИИ.

2. Када у складу са ставом 1 резервише право, федерална држава не сме да примени услове такве резерве да би искључила или битно умањила своје обавезе да спроведе мере предвиђене у поглављу ИИ. Укупно гледајући, она мора да обезбеди широко и ефикасно спровођење закона у погледу тих мера.

3. У погледу одредби ове конвенције, чија примена потпада под јурисдикцију конститутивних држава или других сличних територијалних јединица које уставни систем федерације не обавезује да предузму легислативне мере, федерална влада ће информисати надлежне органе тих држава о наведеним одредбама прилазући своје повољно мишљење о њима, подстичући их да предузму потребне мере да би те одредбе спровели.

Члан 42 Резерве

Свака држава може, писменом изјавом упућеном Генералном секретару Савета Европе, приликом потписивања или приликом депоновања својих инструмената ратификације, прихватања, одобравања или приступања, да изјави да ће користити резерву, односно резерве предвиђене у члану 4, став 2, члану 6, став 3, члану 9, став 4, члану 10, став 3, члану 11, став 3, члану 14, став 3, члану 22, став 2, члану 29. став 4 и члану 41, став 1. Никакве друге резерве се не могу ставити.

Члан 43

Статус и повлачење резерве

1. Чланица која стави резерву у складу са чланом 42, може у целини или делимично да је повуче на основу писменог обавештења упућеног Генералном секретару. Такво повлачење ступа на снагу на дан када је Генерални секретар примио обавештење. Уколико је у обавештењу наведено да ће повлачење резерве ступити на снагу на дан одређен у обавештењу, а тај датум долази након дана када је Генерални секретар примио обавештење, повлачење ће ступити на снагу тог каснијег датума.

2. Чланица која је ставила резерву као што је наведено у члану 42, може да повуче такву резерву, делимично или у целости, чим околж периодично да чланице које су ставиле једну или више резерва наведених у члану 42, консултује у вези могућности повлачења тих резерва.

Члан 44

Амандмани

1. Свака чланица може предложити амандмане на ову конвенцију, које ће Генерални секретар Савета Европе проследити државама чланицама Савета Европе, државама које нису чланице а које су учествовале у изради ове конвенције, као и свакој држави која је приступила или је позвана да приступи овој конвенцији у складу са одредбама члана 37.

2. Сваки амандман који чланица предложи биће достављен Европском комитету за питања криминала (ЦДПЦ), који ће своје мишљење о предложеном амандману поднети Комитету министара.

3. Комитет министара ће размотрити предложени амандман и мишљење које је поднео Европски комитет за питања криминала (ЦДПЦ), и након консултација са државама које нису чланице ове конвенције, може да усвоји амандман.

4. Текст сваког амандмана којег усвоји Комитет министара у складу са ставом 3 овог члана, биће достављен свим чланицама на усвајање.

5. Сваки амандман који је усвојен у складу са ставом 3 овог члана ступиће на снагу тридесетог дана од датума када све чланице буду обавестиле Генералног секретара о његовом прихватању.

Члан 45

Решавање спорова

1. Европски комитет за питања криминала (ЦДПЦ) мора бити информисан у вези тумачења и примене ове конвенције.

2. У случају настанка спора између чланица у погледу тумачења и примене ове конвенције, чланице ће покушати да кроз преговоре или на други миран начин спор реше, у шта спада и подношење спора Европском комитету за питања криминала (ЦДПЦ),

ОВДЕ ФАЛИ ТЕКСТ арбитражном суду чије ће одлуке бити обавезујуће за те чланице, или Међународном суду правде, што зависи од међусобног договора чланица које су у спору.

Члан 46 Консултације чланица

1. чланице ће се међусобно повремено консултовати са циљем да олакшају:
а. Ефикасну употребу и примену ове конвенције, укључујући идентификацију свих проблема у вези тога, као и ефекте сваке изјаве или резерве учињене по овој конвенцији;
б. Размену информација о важним правним, политичким или технолошким унапређењима који су вазни за сајберкриминал и прикупљање доказа у електронском облику;
ц. Разматрање евентуалних допуна или побољшања ове конвенције.

2. Европски комитет за питања криминала (ЦДПЦ) треба да буде повремено обавештаван о резултатима консултација наведених у ставу 1.

3. Европски комитет за питања криминала (ЦДПЦ) ће, по потреби, пружити помоћ консултацијама из става 1 и предузети неопходне мере да би помогао чланицама у њиховим напорима да допуне и побољшају ову конвенцију. Најкасније три године након ступања на снагу ове конвенције, Европски комитет за питања криминала (ЦДПЦ) ће, у сарадњи са чланицама, обавити разматрање свих одредби ове конвенције и уколико буде потребно, препоручиће одговарајуће амандмане.

4. Изузев када их на себе преузме Савет Европе, трошкове спровођења одредби става 1 сносиће чланице на начин на који саме одреде.

5. У извршавању својих функција по овом члану, чланицама ће помагати секретаријат Савета Европе.

Члан 47 Отказивање

1. Свака чланица може у било које време да откаже ову конвенцију на основу писменог обавештења упућеног Генералном секретару Савета Европе.

2. Такво отказивање постаће пуноважно првог дана у месецу који следи након истека рока од три месеца од датума када је Генерални секретар примио обавештење.

Члан 48
Обавештавање

Генерални секретар Савета Европе обавештаваће државе чланице Савета Европе, државе које нису чланице Савета Европе а које су учествовале у изради ове конвенције, као и сваку државу која је приступила овој конвенцији или је позвана да јој приступи, о следећем:

- а. Сваком потписивању;
- б. Депоновању свих инструмената ратификације, прихватања, одобравања или приступања;
- ц. Сваком датуму ступања на снагу ове конвенције у складу са Члановима 36 и 37;
- д. Свакој изјави датој у складу са Чланом 40 или резерви учињеној у складу са чланом 42;
- е. Сваком другом поступку, обавештењу или комуницирању који се односе на ову конвенцију;

Потврђујући наведено, долепотписани, прописно за то овлашћени, потписали су ову конвенцију.

Сачињено у Будимпешти, данас, 23 новембра 2001, на енглеском и француском језику, при чему су оба текста подједнако аутентична, у једној копији која ће бити депонована у архиву Савета Европе. Оверену копију ће генерални секретар Савета Европе проследити свакој држави чланици Савета Европе, државама које нису чланице Савета Европе а које су учествовале у изради ове конвенције, као и свакој држави која је позвана да јој приступи.

КРИВИЧНИ ЗАКОНИК РЕПУБЛИКЕ СРБИЈЕ

(извод из Закона који се односи на кривична дела против безбедности рачунарских података)

ГЛАВА ДВАДЕСЕТ СЕДМА

КРИВИЧНА ДЕЛА ПРОТИВ БЕЗБЕДНОСТИ РАЧУНАРСКИХ ПОДАТАКА

Оштећење рачунарских података и програма

Члан 298.

- (1) Ко неовлашћено избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм, казниће се новчаном казном или затвором до једне године.
- (2) Ако је делом из става 1. овог члана проузрокована штета у износу који прелази четиристопедесет хиљада динара, учинилац ће се казнити затвором од три месеца до три године.
- (3) Ако је делом из става 1. овог члана проузрокована штета у износу који прелази милион и петсто хиљада динара, учинилац ће се казнити затвором од три месеца до пет година.
- (4) Уређаји и средства којима је учињено кривично дело из става 1. и 2. овог члана, ако су у својини учиниоца, одузеће се.

Рачунарска саботажа

Члан 299.

Ко унесе, уништи, избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм или уништи или оштети рачунар или други уређај за електронску обраду и пренос података са намером да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте, казниће се затвором од шест месеци до пет година.

Прављење и уношење рачунарских вируса

Члан 300.

- (1) Ко направи рачунарски вирус у намери његовог уношења у туђи рачунар или рачунарску мрежу, казниће се новчаном казном или затвором до шест месеци.
- (2) Ко унесе рачунарски вирус у туђи рачунар или рачунарску мрежу и тиме проузрокује штету, казниће се новчаном казном или затвором до две године.
- (3) Уређај и средства којима је учињено кривично дело из става 1. и 2. овог члана одузеће се.

Рачунарска превара

Члан 301.

- (1) Ко унесе нетачан податак, пропусти уношење тачног податка или на други начин прикрије или лажно прикаже податак и тиме утиче на резултат електронске обраде и преноса података у намери да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету, казниће се новчаном казном или затвором до три године.
- (2) Ако је делом из става 1. овог члана прибављена имовинска корист која прелази износ од четиристопедесет хиљада динара, учинилац ће се казнити затвором од једне до осам година.
- (3) Ако је делом из става 1. овог члана прибављена имовинска корист која прелази износ од милион и петсто хиљада динара, учинилац ће се казнити затвором од две до десет година.
- (4) Ко дело из става 1. овог члана учини само у намери да другог оштети, казниће се новчаном казном или затвором до шест месеци.

Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података

Члан 302.

- (1) Ко се, кршећи мере заштите, неовлашћено укључи у рачунар или рачунарску мрежу, или неовлашћено приступи електронској обради података, казниће се новчаном казном или затвором до шест месеци.
- (2) Ко употреби податак добијен на начин предвиђен у члану 1. овог члана, казниће се новчаном казном или затвором до две године.
- (3) Ако је услед дела из става 1. овог члана дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже или су наступиле друге тешке последице, учинилац ће се казнити затвором до три године.

Спречавање и ограничавање приступа јавној рачунарској мрежи

Члан 303.

- (1) Ко неовлашћено спречава или омета приступ јавној рачунарској мрежи, казниће се новчаном казном или затвором до једне године.
- (2) Ако дело из става 1. овог члана учини службено лице у вршењу службе, казниће се затвором до три године.

Неовлашћено коришћење рачунара или рачунарске мреже

Члан 304.

- (1) Ко неовлашћено користи рачунарске услуге или рачунарску мрежу у намери да себи или другом прибави противправну имовинску корист, казниће се новчаном казном или затвором до три месеца.
- (2) Гоњење за дело из става 1. овог члана предузима се по приватној тужби.

ЗАКОН О ЕЛЕКТРОНСКОЈ ТРГОВИНИ

І. ОСНОВНЕ ОДРЕДБЕ

Предмет

Члан 1.

Овим законом уређују се услови и начин пружања услуга информационог друштва, обавезе информисања корисника услуга, комерцијална порука, правила у вези сазакључењем уговора у електронском облику, одговорност пружаоца услуга информационог друштва, надзор и прекршаји.

Области на које се закон не примењује

Члан 2.

Одредбе овог закона не примењују се на: заштиту података, опорезивање, заступање странака и заштиту њихових интереса пред судовима, као ни на игре на срећу са новчаним улозима, укључујући лутријске игре, игре у казинима, кладионичке игре и игре на срећу на аутоматима, ако посебним законом није друкчије одређено.

Значење појединих израза

Члан 3.

Поједини изрази у смислу овог закона имају следеће значење:

- 1) **податак** је информација, порука и документ сачињен, послат, примљен, забележен, складиштен или приказан електронским путем, укључујући пренос Интернетом и електронску пошту;
- 2) **недопуштени податак** је информација, порука и документ који је у супротности са прописима и моралом или који је законом одређен као поверљив;
- 3) **услуга информационог друштва** је услуга која се пружа на даљину уз накнаду путем електронске опреме за обраду и складиштење података, на лични захтев корисника услуга, а посебно продаја робе и услуга путем Интернета, нуђење података и рекламирање путем Интернета, електронски претраживачи, као и омогућавање тражења података и услуга које се преносе електронском мрежом, обезбеђивање приступа мрежи или складиштење података корисника услуга;
- 4) **пружалац услуга информационог друштва** је правно лице или предузетник који пружа услуге информационог друштва (у даљем тексту: пружалац услуга);
- 5) **корисник услуга** је свако физичко или правно лице које због професионалних или других циљева користи услуге информационог друштва;
- 6) **потрошач** је свако физичко лице које закључује правни посао на тржишту у сврхе које нису намењене обављању његовог занимања, пословне активности или предузетничке делатности;
- 7) **уговор у електронској форми** је уговор који правна и физичка лица закључују, шаљу, примају, раскидају, отказују, коме приступају и који приказују електронским путем уз коришћење електронских средстава;
- 8) **комерцијална порука** је порука у било којем облику, сачињена да промовише, непосредно или посредно, робу, услуге или углед правног или физичког лица које обавља регистровану делатност.

Примена

Члан 4.

Пружалац услуга са седиштем у Републици Србији дужан је да поступа и пружа услуге у складу са законима и прописима донетим на основу закона Републике Србије.

Електронска трговина робом и услугама јесте даљинска трговина у смислу закона којим се уређује трговина.

Одредбе овог закона примењују се и на питања заштите потрошача, ако су повољније за потрошача.

Овлашћена струковна удружења и организације пружалаца услуга, могу да уређују пословање својих чланова својим унутрашњим правилима – кодексима.

Ако овим законом није друкчије одређено, на правне односе настале из или у вези са уговорима закљученим електронским путем или у електронској форми, примењују се прописи којима се уређују облигациони односи.

Слобода пружања услуга

Члан 5.

Пружање услуга информационог друштва слободно је.

За пружање услуга информационог друштва није потребна посебна дозвола или одобрење.

Пружалац услуга мора, пре него што отпочне да обавља делатност пружања тих услуга, да буде регистрован у Регистар привредних субјеката у складу са законом којим се уређује регистрација привредних субјеката.

Одредба става 3. овог члана не односи се на пружаоца услуга који има својство страног лица у смислу закона којим се уређује спољнотрговинско пословање.

II. ОБАВЕЗА ИНФОРМИСАЊА И КОМЕРЦИЈАЛНА ПОРУКА

Обавезне информације

Члан 6.

Пружалац услуга дужан је да, у облику и на начин који је непосредно и стално доступан, корисницима услуга и надлежним органима државне управе пружи следеће информације:

- 1) име и презиме или назив пружаоца услуга;
 - 2) седиште пружаоца услуга;
 - 3) остале податке о пружаоцу услуга на основу којих корисник услуга може са њим брзо и несметано да оствари комуникацију, укључујући и електронску адресу;
 - 4) податке о упису у Регистар привредних субјеката;
 - 5) појединости о надлежном органу, ако делатност пружаоца услуга подлеже службеном надзору;
 - 6) у погледу посебно регулисаних делатности, односно професија:
 - професионално или слично струковно удружење код кога је пружалац услуга регистрован;
 - професионални назив и држава која га је одобрила;
 - упутства о професионалним правилима у држави у којој се обавља делатност и месту њихове доступности;
 - 7) порески идентификациони број (ПИБ), као и број обвезника пореза на додату вредност, из потврде о извршеном евидентирању за порез на додату вредност издате од стране надлежног пореског органа, ако је пружалац услуга обвезник пореза на додату вредност.
- Ако пружалац услуга наводи цене, оне морају бити јасно и недвосмислено назначене, а посебно мора назначити да ли су у те цене укључени трошкови доставе, остали манипулативни трошкови, порез и други

трошкови који на њих утичу.

Комерцијална порука

Члан 7.

Пружалац услуга дужан је да обезбеди да сваки податак из комерцијалне поруке који је делимично или у целини услуга информационог друштва задовољи следеће услове:

- 1) да је комерцијалну поруку могуће као такву јасно идентификовати у тренутку када је корисник услуга прими;
- 2) да је лице у чије име је комерцијална порука сачињена могуће јасно идентификовати;
- 3) да сваки промотивни позив за стављање понуде из комерцијалне поруке (укључујући попусте и поклоне) мора као такав бити јасно идентификован;
- 4) да услови који морају бити испуњени за стављање понуде из комерцијалне поруке морају бити лако доступни, као и да су предочени на јасан и недвосмислен начин.

Нетражена комерцијална порука

Члан 8.

Коришћење електронске поште у сврху слања нетражене комерцијалне поруке, дозвољено је само уз претходни пристанак лица коме је таква врста поруке намењена, у складу са законом.

III. УГОВОРИ У ЕЛЕКТРОНСКОМ ОБЛИКУ

Форма и пуноважност уговора

Члан 9.

Уговор може бити закључен електронским путем, односно у електронској форми. Понуда и прихват понуде могу се дати електронским путем, односно у електронској форми. Када се електронска порука, односно електронска форма користи приликом закључења уговора, таквом уговору се не може оспорити пуноважност само због тога што је сачињен у електронској форми.

Уговори на које се закон не примењује

Члан 10.

Одредба члана 9. став 3. овог закона не примењује се на:

- 1) правне послове којима се врши пренос права својине на непокретности или којима се установљавају друга стварна права на непокретностима;
- 2) изјаве странака и других учесника у поступку за расправљање заоставштине, форму завештања, уговоре о уступању и расподелу имовине за живота, уговоре о доживотном издржавању и споразуме у вези са наслеђивањем, као и друге уговоре из области наследног права;
- 3) уговоре о утврђивању имовинских односа између брачних другова;
- 4) уговоре о располагању имовином лица којима је одузета пословна способност;
- 5) уговоре о поклону;
- 6) друге правне послове или радње, за које је посебним законом или на основу закона донетих прописа, изричито одређена употреба својеручног потписа у документима на папиру или овера својеручног потписа.

Електронски потпис

Члан 11.

Када се као претпоставка пуноважности и настанка уговора захтева потпис лица, сматра се да тај услов задовољава електронска порука потписана квалификованим електронским потписом, у складу са законом којим се уређује електронски потпис.

Обавезни подаци и обавештења пре закључења уговора

Члан 12.

Пружалац услуга дужан је да потенцијалном кориснику услуга, пре закључења уговора о пружању услуга, обезбеди на јасан, разумљив и недвосмислен начин податке и обавештења о:

- 1) поступку који се примењује код закључивања уговора;
- 2) уговорним одредбама;
- 3) општим условима пословања, ако су саставни део уговора;
- 4) језицима на којима уговор може бити закључен;
- 5) кодексима понашања у складу са којима поступају пружаоци услуга и како се ти кодекси могу прегледати електронским путем.

Пружалац услуга дужан је да потенцијалном кориснику услуга, пре закључења уговора, обезбеди техничка средства за препознавање и исправљање погрешног уноса података у поруку пре њене предаје или слања.

Уговорне стране које нису потрошачи у међусобним уговорним односима могу изричито уговорити одступање од одредаба ст. 1. и 2. овог члана.

Одредбе ст. 1, 2. и 3. овог члана не примењују се на уговоре закључене путем електронске поште, односно другим видом личне комуникације остварене електронским путем.

Доступност уговора

Члан 13.

Пружалац услуга дужан је да обезбеди да текст уговора и одредбе општих услова пословања које су саставни део уговора закључених у електронској форми буду доступни корисницима услуга на начин који омогућава њихово складиштење, поновно коришћење и репродуковање.

Потврда пријема

Члан 14.

Пружалац услуга дужан је да, без одлагања, електронским путем, посебном електронском поруком, потврди пријем електронске поруке која садржи понуду или прихват понуде за закључење уговора.

Уговорне стране, које нису потрошачи, у међусобним уговорним односима могу изричито уговорити одступање од одредбе става 1. овог члана.

Одредбе ст. 1. и 2. овог члана не примењују се на уговоре закључене путем електронске поште, односно другим видом личне комуникације остварене електронским путем.

Време закључења уговора

Члан 15.

Уговор у електронској форми сматра се закљученим оног часа када понуђач прими електронску поруку која садржи изјаву понуђеног да прихвата понуду.

Понуда и прихват понуде, као и друге изјаве воље учињене електронским путем, сматрају се примљеним када им лице коме су упућене може приступити.

IV. ОДГОВОРНОСТ ПРУЖАОЦА УСЛУГА

Искључење одговорности

Члан 16.

Пружалац услуга који преноси електронске поруке које му је предао корисник услуга, није одговоран за садржај послате поруке и њено упућивање, ако није:

- 1) иницирао пренос;
- 2) извршио одабир података или докумената који се преносе;
- 3) изузео или изменио податке у садржају поруке или докумената;
- 4) одабрао примаоца преноса.

Пренос порука и пружање приступа порукама из става 1. овог члана морају бити обављени на начин који омогућава аутоматско, посредничко и привремено складиштење пренетих порука и у њима садржаних података и морају бити привремено складиштене само у временском периоду који је неопходан за пренос порука.

Привремено складиштење података

Члан 17.

Пружалац услуга који податке унете од стране корисника услуга преноси посредством комуникационе мреже, није одговоран за аутоматско, посредничко и привремено складиштење које служи само за ефикасније формирање преноса података тражених од стране других корисника услуга, ако:

- 1) не мења податке;
- 2) уважава услове за приступ подацима;
- 3) поступа у складу са правилима за ажурирање података;
- 4) делује у складу са дозвољеном применом технологија за прикупљање података;
- 5) уклони или онемогући приступ подацима које је чувао одмах након сазнања да су подаци уклоњени из преноса посредством мреже или је онемогућен приступ до њих, као и када је суд, односно други надлежни орган, наредио њихово уклањање или онемогућавање приступа.

Трајно складиштење података

Члан 18.

Пружалац услуга који складишти податке пружене од стране корисника услуга, на захтев корисника услуга, није одговоран за садржај складиштеног податка, ако:

- 1) није знао нити је могао знати за недопуштено деловање корисника услуга или за садржај податка;
- 2) одмах након сазнања да се ради о недопуштеном деловању или податку уклони или онемогући приступ том податку.

Одредба става 1. овог члана не примењује се у случајевима када је корисник услуга лице зависно на било који начин од пружаоца услуга (повезана привредна друштва у смислу закона којим се уређује положај привредних друштава).

Линкови

Члан 19.

Пружалац услуга који посредством електронског упућивања омогући приступ подацима другог пружаоца услуга, није одговоран за те информације, ако:

- 1) није знао нити је могао знати за недопуштено деловање корисника услуга или за садржај података у тим информацијама;
- 2) одмах након сазнања да се ради о недопуштеном деловању или податку уклони или онемогући приступ подацима.

Обавезна обавештења

Члан 20.

Приликом пружања услуга информационог друштва, пружалац услуга није дужан да прегледа податке које је складиштио, пренео или учинио доступним, односно да испитује околности које би упућивале на недопуштено деловање корисника услуга.

Пружалац услуга мора да обавести надлежни државни орган ако основано сумња да:

- 1) коришћењем његове услуге корисник услуга предузима недопуштене активности;
- 2) је корисник његове услуге пружио недопуштени податак.

Пружалац услуга дужан је да на основу одговарајућег судског, односно управног акта, предочи све податке на основу којих се може предузети откривање или гоњење починилаца кривичних дела, односно заштита права трећих лица.

V. НАДЗОР

Надзор над применом закона

Члан 21.

Надзор над применом овог закона врши министарство надлежно за послове трговине и услуга, односно министарство надлежно за послове телекомуникација и информационог друштва.

Инспекцијски надзор над применом овог закона министарство надлежно за послове трговине и услуга врши преко тржишних инспектора, а министарство надлежно за послове телекомуникација и информационог друштва преко инспектора за поштанске услуге и инспектора за телекомуникације и информатику.

Ради вршења надзора, пружаоци услуга дужни су да овлашћеним лицима органа из става 2. овог члана омогуће приступ рачунарској опреми и уређајима, као и да без одлагања покажу или доставе потребне податке и документацију у вези са предметом надзора.

VI. КАЗНЕНЕ ОДРЕДБЕ

Прекршаји

Члан 22.

Новчаном казном од 100.000 до 1.000.000 динара казниће се за прекршај правно лице - пружалац услуга, ако:

- 1) корисницима услуга и надлежним органима државне управе не пружи прописане информације у облику и на начин који је непосредно и стално доступан (члан 6);
- 2) пошаље нетражену комерцијалну поруку без претходног пристанка лица којем је таква порука намењена (члан 8);
- 3) потенцијалном кориснику услуга, пре закључења уговора, не обезбеди на разумљив и недвосмислен начин прописане податке и обавештења (члан 12. став 1);
- 4) не омогући приступ тексту уговора и општих услова пословања на начин који омогућава да их корисник услуга може складиштити, поново користити и репродуковати (члан 13);

5) не обавести надлежни државни орган о недопуштеним активностима или подацима корисника његове услуге или не предочи све податке, сагласно одговарајућем судском, односно управном акту (члан 20. ст. 2. и 3);

6) не омогући приступ рачунарској опреми и уређајима, као и ако без одлагања не покаже или не достави потребне податке или документацију ради вршења надзора (члан 21. став 3).

За прекршај из става 1. овог члана казниће се новчаном казном од 10.000 до 50.000 динара одговорно лице у правном лицу.

Ако прекршај из става 1. овог члана учини предузетник – пружалац услуга, казниће се новчаном казном од 10.000 до 100.000 динара.

У случају посебно тешких повреда или понављања повреда из става 1. овог члана може се изрећи забрана вршења делатности правном лицу у трајању од три до шест месеци.

VII. ЗАВРШНА ОДРЕДБА

Члан 23.

Овај закон ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.