

**ФАКУЛТЕТ БЕЗБЕДНОСТ И
УНИВЕРЗИТЕТ У БЕОГРАДУ**

ПОСЛОВНА ТАЈНА: ПОЈАМ И ПРАВНО УРЕЂЕЊЕ

СПЕЦИЈАЛИСТИЧКИ РАД

студент: Мирјана Ђорђевић бр.индекса с42/21

ментор: Младен Милошевић

Београд 2022.године

САДРЖАЈ	2
1 УВОД	3
2 ПОЈАМ И САДРЖАЈ ПОСЛОВНЕ ТАЈНЕ	5
2.1. Пословна тајна у законодавству Републике Србије	11
2.2. Материјални губици настали одавањем пословне тајне	17
3 МЕРЕ ЗАШТИТЕ	19
4 ЗАКЉУЧАК	24
5 ЛИТЕРАТУРА	
Библиографија	26
Правни акти	28

1. УВОД

Иако се чини да је пословна тајна данас у посебном фокусу, не само теоретичара, већ и закона и практичара, овај феномен постоји готово од када и основни облици пословања. Данас пословна тајна заузима значајно место и у економским и у безбедносним разматрањима, имајући у виду да компаније, посебно критичне инфраструктуре, почивају на иновацијама, развоју, дискрецији у погледу унутрашњим радних односа, а да су истовремено изложене ризицима мита, крађе поверљивих података, индустријској шпијунажи.

Како су се пословање и односи унутар њих развијали, од меркантилизма, преко првих фабрика, до корпорација, тако су се развијале и теорије, али и нормативе која је регулисала област привреде. Једно од првих питања које се постављало, јесте постоје ли моралне норме у пословању - узимајући у обзир да је крајњи циљ бизниса остварење профита, јављају се многобројне дилеме услед којих се још увек може срести мишљење да су етика и економија две различите целине (Alavuk i Petrevska, 2014:43). из ових разматрања, али и праксе, развила се научна дисциплина пословне етике, управо кроз дискусију и препознавање заједничких интереса економије и етике. Предмет пословне етике представља пресек који подразумева укрштање моралних и економских аспеката пословања (Ристић, 2004, стр. 174). Пословна етика дефинише пожељна правила пословног понашања која представљају оквир за деловање које може бити дозвољено или недозвољено и истовремено указује на основна правила моралног деловања личности (Alavuk I Petrevska, 2014:43). Пословна етика развијала се на начелима добре праксе, али и потребе да се основни принципи пословања – економичност, профитабилност, ефикасност, остварују поштујући писане и неписане моралне норме и у области међуљудских односа, али и у области пословних и облигационих односа. У сваком организационом бизнису, нужно је обликовати и остварити корпоративну културу која ће почивати на јасно и прецизно дефинисаним правилима етике која прописују основне вредности система као и основне етичке принципе којих се организација мора придржавати и практично их примењивати (Милетић, 2009, стр. 27).

Међутим, сама пословна етика и њено поштовање, није могла одговорити на изазове које су жеља за већом конкурентношћу, монополом, социјалним инжињерингом стварали. Социјални инжињеринг постао је права опасност, с обзиром да он представља вид манипулације појединцима како би се они навели да испуне одређене захтеве нападача, који су, по правилу, у супротности са процедуралним, правним и/или етичким нормама (Милошевић и Путник, 2019). У условима и националне и глобалне трке за профитом, водећом позицијом на тржишту и профитабилнијим персоналним развојем, бројне области пословања почињале су се законски уређивати, чиме је и пословна тајна све више добијала на обухвату и значају. У привредном праву, постоје следећи извори права:

1. Прописи, које доносе државни органи: закони и подзаконски акти,
2. Аутономни извори права: пословни обичаји и општи услови пословања и
3. извори међународног привредног права.(Веселиновић, 2017:16).

Наше привредно законодавство, како наводи Веселиновић (2017), разликује три фазе:

- а) Предратну – традиционалну, која је деловала до Другог светског рата, а где су закони креирани по угледу на тадашње европске законе; Први закон из ове области звао се Трговачки законик Краљевине Србије и донет је 1860. године (Веселиновић, 2017:33).
- б) Послератну – социјалистичко самоуправна фаза, обележена је увођењем државног управљања предузећима. Закон о државним привредним предузећима из 1946., предузећа је прогласио државним органима; у овом период донети су и Основни закон о управљању привредним предузећима и вишим привредним удружењима од стране радних колектива (1950.) и Закон о предузећима (1965.)
- ц) Транзициону фазу – која се поново окреће европском законодавству. Године 1988. Доноси се нови Закон о предузећима и уводи се тржишна привреда. Овај Закон доживео је бројне ревизије и измене; Најзначајније измене десиле су се доношењем Закона о привредним друштвима 2004. године, али он још увек није био целовит оквир за привредна друштва (Веселиновић, 2017:34), те су недостаци отклањани у наредним годинама.

Напори улагани у успостављање правне регулативе у области привреде, свакако су се односили и на област пословне тајне. Ова категорија, како код нас, тако и у свету, прошла је многе ревизије, како се њен значај и садржај мењао.

2. ПОЈАМ И САДРЖАЈ ПОСЛОВНЕ ТАЈНЕ

Један део пословања захтева да буде третиран по посебним околностима, додатно правно регулисан и заштићен, без обзира на обимну легислативе у области провредног права и постојање пословне етике. Када се говори и пословној тајни, пре свега се мисли на информације, које имају посебан значај за пословање и с тога су осетљиве на бројне ризике експозиције и захтевају посебну заштиту. Пословна тајна представља један од видова заштите информације, која има посебан значај за обављање делатности једног привредног субјекта (Јовичић, 2018).

Први обриси институције пословне тајне могу се наћи још у римском праву – где је *Actio servi corrupti* била тужба коју је господар могао поднети против свог роба у случају корупције. Постојање облика пословне тајне још у време робовласништва, у својим анализама потврђује и Забел у својој монографији (Спировић-Јовановић, 1971). Ова тужба могла се покренути и против лица која су наговарала роба да почини крађу или направи непотребне трошкове. Међутим и поред ове чињенице, указује се на немогућност доказивања правног и друштвено-економског континуитета између античких, средњовековних и нововековних и савремених појавних облика пословне тајне (Забел, 1970:12). Године 1974. Донето је Пруско опште земаљско право, које је у себи укључивало и пословно тајну, а сличну регулативе, по узору на ову донела је и тадашња Француска. Свакако пословна тајна своје прве легислативне потврде добија у англо-америчком праву током XIX века. Први предмет у коме је суд дискутовао о пословним тајнама је случај *Newbery v. James* 1817. године у Енглеској, док је у Сједињеним Америчким Државама (САД) то питање нешто касније, у случају *Vickery v. Welch* из 1837 године постало предмет судског интересовања (Јовичић, 2018). Када је у САД објављен *Restatements of Tort*, 1939. године, у оквиру кога је једно поглавље било посвећено пословним тајнама, ова

проблематика почиње да привлаче већу пажњу као што расте и број судских предмета везаних за злоупотребу овог института. Мада и поред овога, пословне тајне су најкасније стекле правну заштиту у односу на друга права интелектуалне својине (Јовичић, 2018:8). Разлог томе може бити и обухват пословне тајне, који се кретао од односа послодаваца-запослени, преко патената и интелектуалне својине, до бројних других информација.

У погледу правне природе пословне тајне Забел наилази на различите одговоре у теорији; Једно од схватања, на пример, које нам он презентира, полази од психолошког односа између послодавца и радника чија је основа поверење; друго полази од имовинског односа, па у праву на пословну тајну види заштиту имовине власника; Укратко, пословна тајна у теорији, по Забелу, нема јединствени третман - Она це негде сматра као „духовна творевина“, негде као објекат индустријске својине, а негде као објекат својине нематеријалног карактера (Спировић-Јовановић, 1971). У литератури, много је више посвећено пажње облицима тајне као што су службена, професионална или државна тајна. (Забел, 1971:636). Забел је, упоређујући тадашње национално и инострано законодавство, констатовао да је пословна тајна регулисана кривичним правом, нормама из области нелојалне конкуренције и нормама радног права. Разлог је у томе што је категорија пословне тајне више него многе друге категорије, повезана са економским односима, првенствено са тржиштем и конкуренцијом (Спировић-Јовановић, 1971:7). По Забелу (1971), предмет заштите пословне тајне представља податак из области технике, финансијског или комерцијалног пословања једног предузећа.

Поимање и дефиниција пословне тајне мењала се и еволуирала кроз време. истраживања показују да мора постојати тајна која није заштићена ни законом о патентима, ни законима о ауторским правима (Nature of Trade Secrets and Their Protection, 1928:255). У случају САД, пословну тајну и њен обухват, у највећој мери су обликовале судске одлуке и пракса, који су касније били основ законским решењима. Упркос претпоставци да постоји власнички интерес у пословној тајни, такав закључак није био од есенцијалног значаја у сваком судском случају. Најзначајнији основ у стварању судске праксе био је принцип установљен у суђењу Лумлеи против Гие (Lumley v. Gie)¹. Пракса и тумачење пословне

¹ Lumley je sa umetnicom Johanna Wagner sklopio ugovor o njenom nastupu u njegovom teatru, 3 meseca, pri čemu nema pravo da u tom period nastupa negde drugde. Gye je Wagner ponudio veći

тајне пре свега су узимали у обзир да мора постојати забрана да трећа лица сазнају или дођу у посед информација које су тајна, јер би у случају њиховог прибављања исте злоупотребили да себи стекну имовинску или неку другу корист. Анализа одлука показује несумљиву тенденцију судова да заштите пословне тајне од трећих лица које би њиховим стицањем користиле их неправедно и суд пружа заштиту од лица која сазнају тајну путем крађе или преваре (Nature of Trade Secrets and Their Protection, 1928). Судови су као поверљиве информације, пре свега третирали производне и продајне процедуре, нацрте, машине, сировине, састојке цене коштања (Protection and Use of Trade Secrets., 1951:977). При разматрању који ниво тајности треба одредити, поједини фактори имају значајну улогу:

- 1) Степен у којем су информације већ познате ван пословања,
- 2) у којој мери су те информације познате особама од поверење или које имају уговорну обавезу о чувању тајне,
- 3) које мере су предузете у циљу чувања тајне и
- 4) са којом лакоћом се те информације могу прибавити на малициозан и неприкладан начин (Protection and Use of Trade Secrets., 1951:978).

У теорији су се водиле бројне дебате и промишљања о природи и садржини пословне тајне. Довољно је тешко одредити одговарајуће врсте власништва над материјалним објектима (размотримо права на воду или минерале); још је теже одредити које врсте власништва треба да дозволимо за нетелесне, интелектуалне објекте, као што су списи, изуми и тајне пословне информације; Сложеност закона о ауторским правима, патентима и пословној тајни одражава овај проблем (Nettinger, 1989:31). Како Rand (1966) истиче, патенти су суштина права својине, једном када се они уруше, дешава се аутоматска деструкција свих власничких права (12). У пословном свету, за опстанак и развој компаније, информације и иновације су од виталног значаја, као и њихова заштита. Научници и практичари се слажу да су иновације и адаптације, у константно променљивом пословном окружењу, кључ конкуренције и опстанка компаније

novčani iznos da nastupa kod njega u teatru. Sud je smatrao da je Gye time namerno nanео materijalnu штету Lumley.

(Chowdhurya and Doukas, 2022:1). Пословне тајне подразумевају различите поверљиве и вредне пословне информације, попут оних о продаји и ценама, листи потрошача и снабдевача и производне технике (Hettinger, 1989). Поседовање вредних пословних тајни ствар је и конкуренције, њихова садржина и заштита пружа предност на тржишту. Предмет пословне тајне укључује ауторска права и патенте: све што може бити заштићено ауторским правима или патентирано може се држати као пословна тајна, иако обрнуто није тачно; Обично предузеће мора да бира између патентирања проналаска и његовог чувања као пословне тајне (Hettinger, 1989).

Разлика између дефинисања нечега као патента или пословне тајне је у томе што је ова друга заштићена, а услов за давање патента и ауторских права је јесте њихово јавно откривање (публиковање) (Hettinger, 1989). Међутим, на много начина, логика заштите пословних тајни је паралелна са логиком заштите патената и ауторских права; Људи неће развијати одређене облике информација по приватној цени ако се користи од тих информација могу одмах социјализовати једностраним акцијама других (Epstein, 2004 :57). Пословна тајна је, чини се, боља алтернатива патента, јер нуди посебни ниво заштите, као и средства за њихову успешну апликацију (know-how, листа купаца и слично). Међутим, откривањем пословне тајне, њен власник је на великом губитку, док код патената то није случај. С тога су пословне тајне важан сегмент пословања и захтевају јасну законску регулативу. Патентна заштита обезбеђује монопол носиоцу патента и накнадно долажење до истог проналаска од стране другог субјекта не утиче на положај носиоца патента (Јовичић, 2018). Патентна заштита има ограничено трајање, док пословна тајна, нема, односно одређује је онај ко дефинише ознаку тајности.

Табела 1. приказује основне карактеристике патента и пословне тајне, како су то у својој студији означили Brant and Lohse (2014).

Табела 1. Карактеристике патената и пословних тајни. извор: Brant, and Lohse. (2014). Trade Secrets: Tools for Innovation and Collaboration. International Chamber of Commerce, str. 9

КАРАКТЕРИСТИКА	ПАТЕНТИ	ПОСЛОВНЕ ТАЈНЕ
Доступно јавности	Да	Не
Захтеви које је потребно испунити	▪ Новина ▪ Иновативни искорак	■ не може бити опште познато

	Потенцијална применљивост у индустрији	или лако утврдљиво, - има вредност јер јесте тајна - чине се разумни напори да се Тајна сачува
Регистрација	Захтева се	Не захтева се
Дужина трајања	20 година	Потенцијално неограничена
Трошкови стварања	Високи	Ниски
Парнични трошкови	Врло високи	Варијабилни
Географски обухват заштите	Национални И регионални ниво	Закони о пословним тајнама су националног карактера

Предност при одлучивању за пословну тајну, а не за заштиту патента је потенцијална лакоћа успостављања статуса тајне: пословна тајна не мора бити потпуно нова, у принципу може бити заштићена на неодређено време док је заштита патента временски ограничена; Још једна предност је што, за разлику од патената, пословне тајне не морају (заправо и не би смеле), прво бити јавно објављене, како би добиле заштиту (Directorate General for Internal Policies, 2014:6). Можда један од најпознатијих примера производа који су проглашени пословно тајном (састав и састојци), јесте Coca-Cola. Формула овог пића није патентирана, а у том случају и заштита би одавно престала (Directorate General for Internal Policies, 2014).

Пословна тајна је информација, али не било која већ само она која њеном носиоцу обезбеђује компетитивну, тј. конкурентску предност на тржишту, тако да на основу пословне тајне коју поседује остварује неку комерцијалну вредност; То може бити формула или производни метод, дизајн, компјутерски код и друго; Пословне тајне могу бити и одговарајуће комерцијалне и финансијске информације, као што су листе купаца, подаци о рабату за поједине купце, ценовне листе, маркетиншки и бизнис планови, договори о набавкама и слично (Јовичић, 2018:11). Према Uniform Trade Secrets Act (UTSA) из 1979и амандмана из 1985. пословна тајна је информација која првенствено испуњава два услова:

1) има економску вредност, стварну или потенцијалну, тиме што није опште позната људима ван организације и

2) предмет је рационалних напора да се одржи њена тајност (Ding et al, 2021).

Питање заштите пословне тајне у Европској унији (ЕУ) до скоро је било у надлежности националних законодавстава, чија су се решења међусобно разликовала, чак и у битној мери (Јовичић, 2018). Како је ЕУ јединствена наднационална организација, коју пре свега одликују слобода кретања људи, роба и јединствено тржиште, у том смислу морало је бити донето јединствено гледиште и нормативе у погледу и пословних тајни, које би националне државе поштовале и инкорпорирале у своје законодавство. Европска комисија је 2013.године усвојила Предлог Директиве о пословној тајни . Овај Предлог усвојен је од стране Европског Парламента и Савета о заштити неоткривених знања и искуства и пословних информација (пословне тајне) од незаконитог прибављања, коришћења и откривања као Директива 2016/943. У овој Директиви, пре свега је истакнуто да су глобализација, масовна употреба електронских комуникација као и све дужи ланци снабдевања узрочници повећаних ризика од незаконитог прибављања, злоупотребе и откривања пословне тајне; Таква злоупотреба наноси штету законитим носиоцима пословних тајни зато што они не могу да остваре користи од иновација до којих су први дошли (Јовичић, 2018:13). Директивом је пословна тајна одређена као информација која је тајна у смислу да није, у својој укупности или у тачној структури и склопу својих саставних делова, опште позната или лако доступна лицима из кругова који се обично баве дотичном врстом информација; Она има комерцијалну вредност због тога што је тајна и лице које ту информацију законито контролише предузело је, у датим околностима, разумне мере да сачува њихову тајност Основни услов да би информација могла бити пословна тајна јесте да она свом власнику доноси економску корист. Ова информација престаје да буде тајна када власник учини доступном другим лицима, што значи, да би задржала тај статус, претходно морају бити примењене све потребне мере за њену заштиту. Овако одређење пословне тајне у Директиви о пословној тајни усклађено је са међународним стандардом који се односи на поменуто питање, који је постављен Споразумом о трговинским аспектима права интелектуалне својине - TRIPS споразум (Јовичић, 2018:14).

Савић и Стајић (2006) пословну тајну објашњавају као податке проглашене законом, другим прописом, општим актом или одлуком надлежног органа и податке који као такви нису одређени, али чије би одавање, због њихове важности, могло очигледно да изазове теже штетне последице за привреду (стр, 244). Како Вучковић и сарадници (2016) истичу, један од начина постизања нелојалне конкуренције и неправноправних услова привређивања јесте и стицање, коришћење и откривање поверљивих послова и информација без сагласности њиховог носиоца, а ради ометања њиховог положаја на тржишту (стр. 177). Fridman и сарадници (1991) наводе да је основна тајна је податак. који има комерцијалну вредност и који фирма која поседује те информације жели да сакрије од својих конкурената како би их спречила да их дуплирају (стр.61). Позивајући се на дефиниције United States Patent and Trademark Office, Ciuriak и Ptashkina (2021), истичу да информација може бити квалификована као пословна тајна, када задовољава три критеријума:

- 1) мора имати стварну или потенцијалну независну економску вредност тиме што није опште позната,
- 2) мора имати вредност за друге који је не могу легално и легитимно добити и
- 3) мора бити предмет спровођења мера њене заштите (стр. 3).

Како EU Directorate General for Internal Policies (2014) у својој експертизи наводи, пословне тајне могу бити заштићене кривичним законом, грађанским законом, законима из области тржишта и тиме се може изгубити јединствени инструмент њиховог означавања, па се пословне тајне могу означити као производне тајне, пословне информације, know-how, техничке информације, поверљиве информације и тајне информације. (стр 4.). Као и са основним концептом и дефиницијом пословне тајне, постоји широка сагласност о томе које радње представљају проневеру, иако законска покривеност може варирати у зависности од земље (Schultz & Lippoldt, 2014)

2.1. Пословна тајна у законодавству Републике Србије

У Републици Србији, од осамостаљења, донета су два Закона о заштити пословне тајне, један 2011., а други 2021. године.

Закон о заштити пословне тајне (даље: стари Закон), донет 2011. године, у Члану 1. дефинише шта ће се сматрати пословном тајном:

“информацијама које се штите као пословна тајна у смислу овог закона сматрају се нарочито: финансијски, економски, пословни, научни, технички, технолошки, производни подаци, студије, тестови, резултати истраживања, укључујући и формулу, цртеж, план, пројекат, прототип, код, модел, компилацију, програм, метод, технику, поступак, обавештење или упутство интерног карактера и слично, без обзира на који начин су сачувани или компилирани.”

Закон о заштити пословне тајне из 2021. године (даље: нови Закон), сада пословну тајну дефинише на следећи начин:

1) пословном тајном сматрају се информације које испуњавају следеће услове:

(1) представљају тајну јер нису у целини или у погледу структуре и скупа њихових саставних делова опште познате или лако доступне лицима која у оквиру својих активности уобичајено долазе у контакт са таквом врстом информација,

(2) имају комерцијалну вредност јер представљају тајну,

(3) лице које их законито контролише је у датим околностима предузело разумне мере како би сачувало њихову тајност.²

Измена, пре свега квалитативна, у дефинисању пословне тајне у новом Закону, огледа се у чињеницама да се уводи постулат да она има комерцијалну вредност јер је тајна И да је потребно да лице законито контролише информацију И предузима све “разумне” мере за очување њене тајности. Члан 2. Новог Закона дефинише И које су то “разумне” мере за очување тајности:

² Члан 2. Закона о пословној тајни (“*Sl. glasnik RS*”, br. 53/2021)

“Разумним мерама за очување тајности информација из става 1. тачка 1) подтачка (3) овог члана сматрају се, између осталог, израда интерног акта о руковању пословном тајном и кругу лица и њиховим правима и обавезама приликом руковања пословном тајном, мере физичке или електронске заштите приступа и руковања пословном тајном, означавање докумената ознаком "пословна тајна" или сличном ознаком, ограничавање приступа просторијама и датотекама у којима се налазе информације које се сматрају пословном тајном или закључивање уговора о поверљивости, односно неоткривању поверљивих информација са лицима која потенцијално могу да дођу у посед пословне тајне, укључујући запослене, пословне партнере, спољне сараднике и консултанте, односно потписивање изјава о поверљивости или неоткривању поверљивих информација од стране наведених лица”.³

Стари Закон је део претходних дефиниција иновираних у новом Закону објашњавао у Члану 4. Наводећи да се пословном тајном, у смислу тог Закона, сматра се било која информација која има комерцијалну вредност зато што није опште позната нити је доступна трећим лицима која би њеним коришћењем или саопштавањем могла остварити економску корист, и која је од стране њеног држаоца заштићена одговарајућим мерама у складу са законом, пословном политиком, уговорним обавезама или одговарајућим стандардима у циљу очувања њене тајности, а чије би саопштавање трећем лицу могло нанети штету држаоцу пословне тајне.

Из дефиниција у оба Закона видимо да су две основне константе и одреднице пословне тајне те да она има вредност за њеног власнике (нарочито тиме што није опште позната) и да над њом морају бити примењене мере заштите, како би се сматрала тајном и могла бити предмет евентуалног судског спора, уколико до њенох нелегалног откривања дође.

Члан 8. старог Закона, бави се незаконитим прибављањем, коришћењем и откривањем информација која представљају пословну тајну и у њему се наводи да се свака радња

³ isto

предузета у оквиру индустријских или комерцијалних активности која за последицу има откривање, прибављање, односно коришћење информације која представља пословну тајну, без сагласности држаоца пословне тајне и на начин супротан закону и добрим пословним обичајима, сматра делом нелојалне конкуренције.

Под начином супротним добрим пословним обичајима, у смислу овог Закона, подразумева се свака радња предузета у циљу утакмице на тржишту којом се наноси или се може нанети штета конкуренту или другом физичком односно правном лицу, а нарочито:

- 1) повреда уговорних одредаба о чувању пословне тајне;
- 2) злоупотреба пословног поверења;
- 3) индустријска или комерцијална шпијунажа;
- 4) превара;
- 5) навођење на било коју радњу из тач. 1)-4) овог става;
- 6) прибављање информације која представља пословну тајну од стране трећих лица која знају или су била дужна да знају да та информација представља пословну тајну и да је прибављена од лица у чијем је законитом поседу.

Нови Закон је у Члану 4. На другачији начин дефинисало незаконито прибављање пословне тајне без сагласности држаоца, а ти начини су:

- 1) неовлашћеним приступом, присвајањем или умножавањем докумената, предмета, материјала, супстанци или електронских датотека који су под законитом контролом држаоца пословне тајне, а садрже пословну тајну, или се пословна тајна из њих може извести, или
- 2) другим поступањем за које се, у датим околностима, сматра да је у супротности са добрим пословним обичајима.

Коришћење или откривање пословне тајне сматра се незаконитим ако га без сагласности држаоца пословне тајне врши лице за које се установи да је:

- 1) пословну тајну прибавило незаконито;
- 2) прекршило споразум о поверљивости или другу обавезу која се односи на забрану откривања пословне тајне;
- 3) прекршило уговорну или другу обавезу којом се ограничава коришћење пословне тајне.

Специфичности нови Закон доноси И у дефинисању радњи које се сматрају прибављањем пословне тајне, а које се сматрају законитим, а то је ако је прибављена на један од следећих начина:

- 1) независним открићем или стварањем;
- 2) посматрањем, проучавањем, растављањем или тестирањем производа или предмета који је учињен доступним јавности или који је законито у државини прибавиоца информације (обрнути инжењеринг) који није везан правно важећом обавезом да ограничи прибављање пословне тајне или који није везан правно важећом обавезом забране вршења обрнутог инжењеринга;
- 3) остваривањем права запослених или представника запослених на информисање и консултовање у складу са посебним прописима;
- 4) другом радњом која је у околностима конкретног случаја у складу са добрим пословним обичајима.⁴

“ Нарочито интересантна новина садржана је у једном од примера дозвољеног располагања пословном тајном које Закон наводи, а то је ситуација вршења обрнутог инжењеринга (реверсе енгинееринг), под условом испуњења других услова које Закон предвиђа. У ИТ уговорима попут уговора о лиценцирању софтвера се овакво поступање најчешће предвиђа у оквиру забрањених радњи, те се везује за предмет лиценце на коме не долази до преноса целог права већ само појединих овлашћења у оквиру права интелектуалне својине. Било како било, уношењем у Закон једног оваквог термина који се у ИТ индустрији на глобалном нивоу врло често употребљава, док га ниједан пропис Републике Србије до сада није препознавао, назире се први корак домаћег законодавства путем модернизације домаћег правног система и приближавања развијеним светским системима са свеобухватнијим правним регулативама у области информационих технологија и интелектуалне својине.”⁵

Члан 5. Новог Закона дефинише правне могућности које пред судом има држалац пословне тајне која је незаконито откривена. Та права дефинисану сун а следећи начин:

⁴ Isto, Član 3.

⁵ Advokatska kancelarija Žunić - <https://zuniclaw.com/>

“У случају повреде пословне тајне држалац пословне тајне може тужбом захтевати:

- 1) утврђивање повреде;
- 2) престанак повреде, или у зависности од случаја, забрану коришћења или откривања пословне тајне;
- 3) забрану производње, нуђења, стављања у промет или коришћења робе којом је извршена повреда, односно забрану увоза, извоза или складиштења робе којом је извршена повреда у сврхе производње, нуђења, стављања у промет или коришћења робе;
- 4) одређивање одговарајућих мера које се односе на робу којом је извршена повреда, које обухватају повлачење такве робе с тржишта, уклањање с робе својстава која је чине робом којом је извршена повреда пословне тајне или уништење робе којом је извршена повреда, односно ако је то оправдано, њено повлачење с тржишта, под условом да се повлачењем робе не угрожава заштита пословне тајне на коју се тужба односи;
- 5) уништење у целини или делимично докумената, предмета, материјала, супстанци или електронских докумената који садрже пословну тајну или који сами представљају пословну тајну или ако је примерено, предају тих докумената, предмета, материјала, супстанци или електронских докумената у целини или делимично тужиоцу.

Против лица чије неовлашћено предузимање одређене радње представља непосредну претњу да ће незаконито прибавити, користити или открити пословну тајну, држалац пословне тајне може тужбом захтевати престанак предузимања те радње и забрану незаконитог прибављања, коришћења или откривања пословне тајне.”⁶⁶

У односу на стари Закон новине су се сви тужбени захтеви могу поднети не само против лица које је извршило повреду, већ и против посредника који пружа услуге лицу које је извршило повреду чиме индиректно омогућава, односно олакшава повреду, као и да, поред држаоца пословне тајне, тужбу сада може поднети и стизалац лиценце за коришћење пословне тајне, уколико за то има одговарајући основ.

Глава VI старог Закона дефинише казнене одредбе и у Члану 19. Став 1. наводи се да ће се за привредни преступ новчаном казном у износу од 100.000 до 3.000.000 динара привредно друштво, или друго правно лице које на начин из Члана 8. Став 1. и Члана 9. Став 1. Закона повреди пословну тајну. У Ставу 2. Члана 19. наводи се да се за радње из става 1. овог Члана у случају привредног преступа, изричу новчане казне у износу од

⁶⁶ Isto, Član 5.

50.000 до 200.000 динара према одговорном лицу у привредном друштву или другом правном лицу.

У новом Закону, казнене одредбе дефинисане су у Глави ИВ, Члан 21, где се наводи следеће:

“Казниће се за привредни преступ новчаном казном у износу од 100.000 до 3.000.000 динара правно лице које у складу са чланом 4. овог закона незаконито прибави, користи или открије пословну тајну.

За радње из става 1. овог члана казниће се за привредни преступ одговорно лице у правном лицу новчаном казном у износу од 50.000 до 200.000 динара.

За радње из става 1. овог члана казниће се за прекршај предузетник новчаном казном у износу од 50.000 до 500.000 динара.

За радње из става 1. овог члана казниће се за прекршај физичко лице новчаном казном у износу од 20.000 до 150.000 динара.”⁷

Пословна тајна, тј. њено откривање дефинисано је и Кривичним закоником Републике Србије, у делу Кривична дела против привреде. Члан 240. Кривичног законика дефинише да се одавањем пословне тајне сматра ко неовлашћено другом саопшти, преда или на други начин учини доступним податке који представљају пословну тајну или ко прибавља такве податке у намери да их преда непозваном лицу.

Према истом Члану. према овом лицу може се изрећи казна затвора од шест месеци до пет година.

У овом Члану. наводи се и следеће:

- Ако је дело из става 1. овог Члана учињено из користољубља или у погледу нарочито поверљивих података, учинилац ће се казнити затвором од две до десет година и новчаном казном.

- Ко дело из става 1. овог Члана учини из нехата, казниће се затвором до три године.

2.2. Материјални губици настали одавањем пословне тајне

⁷ Isto, Član 21.

Константе које се у свим теоријским расправама и законским решењима подвлаче јесу да откривање пословне тајне наноси економску штету и да информације таквог значаја захтевају спровођење потребних мера заштите, како би уживале и заштиту у легислативи.

Систематизовани докази на основу досуђене штете у складу са правним тужбама, указују на све већи број случајева - Stout, глобална инвестициона банка и саветничка компанија специјализована за корпоративне финансије и истраге, сакупила је податке о резултатима парница због кршења пословне тајне (крађе, одавања) у САД, а које покривају период од 1990. до 2019. Показују да је “повољних одлука” (пресуде у корист власника пословне тајне), било у 68% случајева (Mordaunt, Eisgruber and Swedlow, 2020: 9). У тим предметима, досуђене су новчане одштете у 52% случајева и износиле су око 3 милијарде долара (Mordaunt, Eisgruber and Swedlow, 2020: 9).

Подаци до којих је компанија Стоут дошла и приказала их у свом извештају из 2020.године, показују следеће:

- Више од 22% случајева компромитовања пословне тајне десио се у сектору индустрије,
- 46% случајева нарушавања тајности информација догодио се у сектору трговине,
- Области информационих технологија, заштите података о потрошачима и сервиси здравствене неге бележе пораст броја компромитовања пословних тајни.

Један од најзначајнијих фактора који утичу на покретање судских спорова у вези са пословном тајном је разноврсност и брзина уласка на тржиште нових технологија, што олакшава нелегално присвајање информација о пословној тајни; Како се компаније све више ослањају на дигиталне медије за складиштење и креирање информација, удаљавајући се од физичких облика архивирања и заштите, померају се и баријере за крађу ових заштићених информација (Stout, 2020).

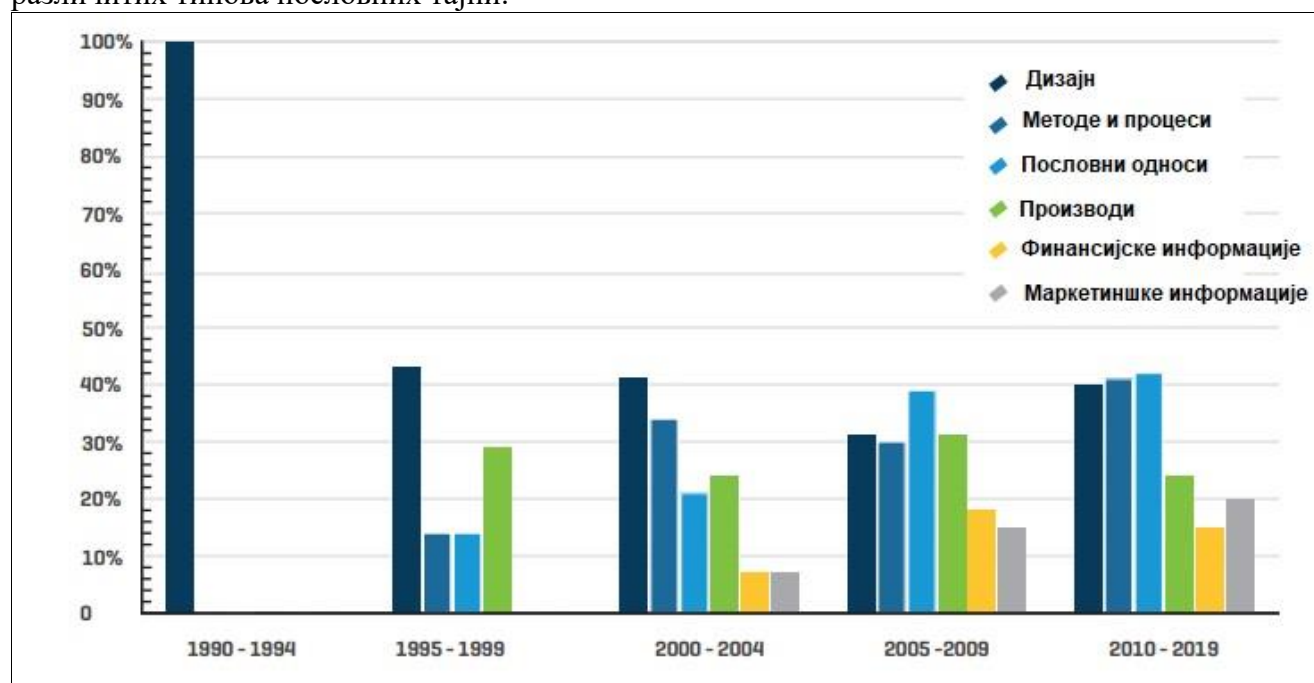
За потребе истраживања, компанија Стоут је садржаје пословних тајни категорисала на следећи начин:

ВРСТА ПОСЛОВНЕ ТАЈНЕ	ПОДВРСТА
<i>Пословни односи</i>	Информације о потрошачима, информације о запосленима, информације о продавцима,

	информација о снабдевачима
<i>Дизајн</i>	Производи у развоју, нацрти, формуле, рецепти, планови, инжењерска решења, инструкције
<i>Методе И Процеси</i>	Обрада података, обуке, интерне одлуке, пословна пракса, упутства за употребу, пословни модели, карактеристике објекта
<i>Производи</i>	Софтвер, хардвер, опрема, компјутерска фајлови, технологија, набавка залиха
<i>Финансијске информације</i>	Листа цена, продаја, пословне прогнозе, цена репроматеријала, цена готовог производа, планови за компензације
<i>Маркетиншке информације</i>	Стратегије, трендови

На основу спроводених истраживања, резултати показују да је нарушавања пословне тајне највише било у случајевима Пословних односа (37%) и Дизајна (35%), а најмање код Финансијских и Маркетиншких информација (по 15%) (Stout, 2020).

На Графикону 1. Процентуално су приказани судски случајеви везани за нарушавање различитих типова пословних тајни.



Графикон 1. Процентуални однос судских случајева везаних за нарушавање различитих типова пословних тајни, у САД, за период 1990-2019. извор. Stout.com

Захтеви за заштитом података отежавају процену економске вредности пословних тајни, иако се у литературе могу наћи одређени индикатори, постоје препреке попут недостатка међународно стандардизоване методологије вредновања неоткривених информација, а са друге стране и невољности многих фирми да прикажу вредност њихових поверљивих информација (OECD, 2014:136).

Almeling и сарадници (2010), су проценили да је годишњи износ трошкова због крађе пословних тајни у САД износио 300 милијарди долара. Студија коју је Европска комисија спровела 2013.године, а која је укључила 537 компанија у Европи, показала је да је њих 75% своје пословне тајне окарактерисало као стратешки важне за развој компаније, конкуритивност и иновативност. Њих 52% су навели да је основни разлог што су одређене иновације дефинисали као пословну тајну, а не као патент, тај да избегну објављивање у јавности. Недавна истраживања су показала да, у просеку, интелектуална својина чини око 70% маркетиншке вредности компаније (Degnan and Jaros, 2004:5).

3. МЕРЕ ЗАШТИТЕ ПОСЛОВНЕ ТАЈНЕ

Иако се у готово свим дефиницијама као пословне тајне означавају информације, оне заправо имају различите типове података – од интерних уговора, преко инжењерских решења, нацрта, до софтвера. Самим тим, ове информације и тајне могу бити у физичком, али и виртуелном облику, што значи и да мере заштите морају бити разноврсне, као што су и начини на које се исте могу компромитовати. Пословне тајне могу бити иодате усменим путем, физичком крађом са места где се чувају, предајом копија или оригинала заштићених података, па све до хакерских напада на компјутерске системе. имајући у виду, са једне стране какав пословни значај ове тајне имају за њихове држаоце и са друге стране разноврсност извора и начина њиховог компромитовања, који се развијају, заједно са техничко-технолошким развојем, заштита пословних тајни мора бити вишеслојна и обухватна. Како Директива ЕУ 2016/943 наводи, систем заштите, у смислу мера, поступака и правних средстава мора бити пажљиво осмишљен у складу са потребом да буде поштен и правичан, а прописане мере, поступци и правна средства доступни и ефикасни; То су квалитети који систем заштите пословне тајне чине делотворним³¹, што

је веома важно, јер само када је делотворан, одвраћа потенцијалне починиоце да чине злоупотребе (Јовичић, 2018:15).

Најважније начело којим се доносиоци одлука и пословни менаџмент требају водити у разматрању заштите не само пословних тајни, већ и свих других елемената и ресурса компаније јесте – проактивност и да улагање у мере заштите није трошак, већ инвестиција у сигурност и стабилност рада и пословања. Најсофистицираније компаније на свету се боре да сачувају своје пословне тајне, а та борба постаје све тежа и важнија; Технологија је већ учинила да се чин крађе многих врста пословних тајни може извршити врло брзо након успостављања таквог њиховог статуса (Degnan and Jaros, 2004:1). Мандић (2020), наводи да имовину правног лица представља све оно што је правно лице досадашњим радом и наступом на тржишту остварило, то су су, између осталих и заштитни знак, основна средства за рад, процес производње, интелектуална својина, проналасци и иновације. Заштитом имовине, запослених и пословне тајне, компанија не штити само своју стабилност и профитабилност, већ и репутацију на тржишту и у јавности. Заштита корпоративних ресурса и интереса је зависна од ефективности процеса управљања ризицима, посебно у сфери заштите кадрова и других субјеката, имовине, инфраструктуре и пословања (Милошевић и Младеновић, 2017:290). Самозадовољство може бити највећа претња пословној тајни; иако већина компанија има писане политике у вези са заштитом информација о пословној тајни, примена, спровођење и поновна процена ових политика се не могу сматрати главним приоритетом све до тренутка када је тајна је изгубљена (Дегнан анд Јарос, 2004:2).

Генерално, ризици по компромитовање пословне тајне могу се поделити у две категорије:

- 1) индустријска шпијунажа, која укључује:
 - Корпоративну шпијунажу,
 - Хакерске нападе
 - Уцену или подмићивање запослених
- 2) интерна крађа

- Лични или финансијски мотиви да се компанији нанесе штета
- Прелазак на рад у другу компанију

Облици су одавања и крађе су врло разноврсни: физичко отуђење документације, фотокопирање, сликање документације, копирање на преносиве меморијске уређаје, преузимање хакерским упадом у систем и други.

имајући у виду ове и друге опасности, Светска организација за интелектуалну својину (World Intellectual Property Organization – WIPO), креирала је приручник за управљање заштитом пословних тајни, а који користи и у својим обукама. Основне препоруке за успостављање управљања заштитом пословних тајни, према WIPO, јесу неке од следећих:

1. Успостављање система за идентификацију пословних тајни - идентификација и категоризација пословних тајни је предуслов за покретање програма заштите пословне тајне, а кораке за заштиту треба да диктира природа самих тајни.

Питања која требају бити постављена јесу: Које информације (њихово откривање) би угрозило пословање?, Колику штету откривање тих информација може нанети?, Да ли постоје запослени посебно задужени за чување пословне тајне?.

Потребно је направити писану листу информација које треба заштитити и организовати их у различите врсте досије, у зависности од њихове вредности за пословање и врсту заштитних мера које би биле потребне за његову заштиту (WIPO, 2019).

2. Креирање политике информационе безбедности, која укључује и информациону заштиту пословних тајни

Политика безбедности информација обухвата системе и процедуре дизајниране да заштите информациона средства од откривања било ком лицу или субјекту који није овлашћен да има приступ тим информацијама, са посебним освртом на информације које се сматрају осетљивим, заштићеним, поверљивим. WIPO чак наглашава да је информациона заштита која се конструише за заштиту пословних података и пословних тајни, врло слична онима које национални одбрамбени системи имају, што говори о

важности обезбеђења ових података, како за саму компанију, тако и за националну економију.

Важно је имати писмену политику заштите информација или пословне тајне. Писана политика даје јасноћу о свим аспектима које треба оперативно спровести; она објасни зашто и како се заштита спроводи; прописује које информације се могу интерно и екстерно делити, а које не; постојање оваквог документа има важну улогу у евентуалним судским парницама (WIPO, 2019).

информациона заштита, уједно укључује и физичку контролу (дефинисање права приступа, личне идентификације, података о корисничким налозима) и техничку контролу.

3. Едукација запослених о питањима битним за спровођење и поштовање информационе заштите

4. Провера при запошљавању лица која супретходно радила у конкурентским компанијама

- упознавање са политиком безбедности и информационе безбедности

- обавезивање запослених на стварање безбедног радног окружења. Овде је корисно навести мишљење које је дао Mearns (2003), а које су у свом раду изнели Кековић и Милошевић (2011), да безбедносна култура формира контекст у оквиру кога се развијају и одржавају безбедносни ставови појединца и промовишу се разна безбедносна понашања (стр. - периодична провера запослених (у складу са законом), ради откривања промена у понашању, сумњивог понашања

5. Ограничен приступ пословним тајнама у папирној форми

- дефинисање запослених који имају право приступа пословним тајнама и местима на којима се оне чувају

6. Ограничавање употребе мобилних телефона и таблета у просторијама где се чувају пословне тајне, као и контрола приликом коришћења фотокопир машина и факс апарата

7. Одржавање компјутерског система безбедним

- обавезна употреба података за приступ (логовање) компјутерским системима на којима се налазе пословне тајне

- периодична измена лог-ин података

- контрола обавезне одјаве (лог-оут) након коришћења компјутерског система

Људски фактор, као централни елемент у архитектури информационе безбедности (не постоје рачунари или мреже који се не заснивају на учешћу човека), уједно представља и њену најслабију компоненту (Милошевић и Путник, 2019:71).

- периодична тестирања софтвера на “слабости” и усавршавање информационе заштите

8. Успостављање видео надзора и сензора покрета испред и унутар просторија где се налазе и чувају пословне тајне

Компанија IBM потрошила је 3 милиона долара на додатне ТВ камере, сензоре, сигурносне браве, сфове и компјутерски контролисане системе уласка/изласка, како би спречила откривање пословне тајне, за коју је добила упозорење да се може догодити (Degnan and Jaros, 2004).

4. ЗАКЉУЧАК

Неспорно је да данас живимо у корпоративним и информационим друштвима. Правовремена и тачна информација од значаја је за готово све гране пословања. Дobar менаџмент, планови и информације основ су успешном пословању и даљем развоју компанија. Оне највредније информације, од значаја за конкурентност на тржишту и даљи развој компаније, проглашавају се пословним тајнама. информације које су суштинске за делатност једног предузећа, његов даљи развој и профитабилност јесу оне које се тичу иновација, различитих техничких, архитектонских, графичких и других решења и дизајна, листе добављача и купаца и слично. С обзиром на своју важност, пословне тајне нису предмет заштите само њихових држаоца, већ уживају и законску заштиту. Основне

карактеристике које свака теоријска и законска дефиниција пословне тајне садржи, јесте да оне имају вредност за свог држаоца и чињеницом да не смеју бити доступне јавности, као и да су предузете све разумне мере за њену заштиту. Нарочито спуњавајући други услов, држаоц пословне тајне коме је она украдена или компромитована, има право на тужбу и спор пред надлежним судом, пре свега за надокнаду штете која је насталаа овом нелегалном активношћу. У ери мултинационалних корпорација, али и бројних националних компанија, све чешћих рецесија и економских криза, опасност по откривање пословне тајне и нелојална конкурентност све су веће, а штете настале њиховим откривањем, мере се и милијардама долара.

Мере заштите пословне тајне су разнооверсне:

- Нормативне: закони, инерна документа компанија, досије запослених
- Физичке: посебне просторије, видео надзори, сензори, физичко обезбеђење, легитимације
- Технолошке и информационе: приступне шифре, кодови, софтверска заштита и друго.
- Едукативне: креирање безбедносне културе међу запосленима

Ипак, све ове и многе друге мере и иновације у области заштите, чини се да нису довољне и да у ери константних иновација, личних усавршавања, али и социо-економским изазова, воде сталну битку са изворима и начинима угрожавања. Технологија је смањила трошкове крађе, повећала трошкове заштите и отежала откривање губитака; Повећање мобилности запослених додатно отежава проблем заштите информација и пословних тајни (Degnan and Jaros, 2004). Глобализација је поред отворености и ширења тржишта, донела и брзу размену података, који не морају увек бити у корист компанија и заштите пословања. У циљу смањења трошкова рада и производње, водеће компаније САД и Западне Европе, делове своје производње и других технолошких послова (програмирање, инжењерство), “селе” у земље са мањим трошковима рада и радне снаге, попут индије и Пакистана. Дивергентност пословања, трансфер технологија и расподела ризика, могу водити

слабљењу управљања мерама заштите пословне тајне и бројним могућностима за социјални инжињеринг.

5. LITERATURA

Bibliografija:

1. Alavuk, Đ., Petrevska, M. (2014). OSNOVNI POSTULATI POSLOVNE ETIKE I IMPLEMENTACIJA ISTIH U TURISTIČKOM POSLOVANJU. *EKONOMIJA TEORIJA I PRAKSA* Godina VII, broj 3 str. 40–53
2. Almeling, D.S. et al. (2010). A Statistical Analysis of Trade Secret Litigation in State Courts. *Gonzaga Law Review* 57.
3. Arsić, Z. (1994). Poslovna tajna i predlog novog Zakona o preduzećima . *Časopis za privredu I pravo*, BROJ 9-12/1994,/G odina XXXII, str. 1-9
4. Brant, J., and Lohse, S. (2014). Trade Secrets: Tools for Innovation and Collaboration. *International Chamber of Commerce*
5. Chowdhury, R., , Doukas, J.A. (2022). Protection of trade secrets and value of cash holdings: Evidence from a natural experiment. *Journal of Banking and Finance* 143, str.1-23

6. Ding, R., Sainani, S., Zhang, Z. (2021). Protection of trade secrets and corporate tax avoidance: Evidence from the inevitable disclosure doctrine. *Journal of Business Research* 132, str. 221-232
7. Donald A. Degnan Joseph T. Jaros (2004). The Present Value of Trade Secret Protection: Do the costs outweigh the benefits?. *Holland & Hart LLP*. Str. 1-31
8. Epstein, R. (2004). The Constitutional Protection of Trade Secrets under the Takings Clause. *The University of Chicago Law Review*, Vol. 71, No. 1, pp. 57-73
9. Friedman, D.D., Landes, W.M. and Posner, R.A. (1991). Some Economics of Trade Secret Law. *Journal of Economic Perspectives*, pp. 61-67
10. *Harvard Law Review* (1888.) The Principle of Lumley v. Gye, and Its Application . Vol. 2, No. 1 (Apr. 15, 1888), pp. 19-27
11. Hettinger, E.C. (1989). Justifying Intellectual Property. *Philosophy & Public Affairs* ,Vol. 18, No. 1, pp. 31-52
12. Jovičić, K. (2018). Poslovne tajne - određenje i osnovi zaštite. *Strani pravni život* , br. 1, str. 7-19
13. Mandić, G.(2020). Korporativna bezbednost – poslovnaa funkcija pravnog lica. **005.934:334.72** https://doi.org/10.18485/fb_nauke_vio.2020.ch5.
14. Miletić, D. (2009). Korporativna društvena odgovornost - traganje za novom dimenzijom. *Anali Ekonomskog fakulteta u Subotici*, 45 (21), 23-30
15. Milošević, M., Putnik, N. (2019). Специфичности извршења кривичног дела преваре уз коришћење информационо-комуникационих технологија. *Bezbednost* 2/2019, str. 68-88
16. Mordaunt, J., Eisgruber, N., and Swedlow, J. (2020). Trends in Trade Secret Litigation. *Report 2020*. Chicago, IL: Stout.
17. Nature of Trade Secrets and Their Protection. (1928). *Harvard Law Review*, 42(2), 254–258. <https://doi.org/10.2307/1329864>
18. Protection and Use of Trade Secrets. (1951). *Harvard Law Review*, 64(6), 976–986. <https://doi.org/10.2307/1336630>
19. Ristić, D. (2004). *Osnovi menadžmenta*, Novi Sad, Fakultet za menadžment.
20. Schultz M.F., Lippoldt D.C.(2014) Approaches to Protection of Undisclosed Information (Trade Secrets). *Trade Policy Paper* 162. OECD, Paris.

21. Stajić, A., Savić, Lj. (2006) . *Osnovi civilne bezbednosti*. Fakultet za pravne I poslovne studije
22. Stout (2020). Trends in Trade Secret Litigation Report 2020.
23. Veselinović, J. (2017). *Privredno pravo*. Poljoprivredni fakultet, Novi sad
24. Vučković, V., Vučković, S., Stefanović, M. (2016). LAWS AND INSTITUTIONS FOR FAIR COMPETITION AND FAIR BUSINESS PRACTICES. *Ekonomika preduzeća*. UDK: 346.545/.546(497.11), str.175-185
25. Забел, Б. (1970). *Пословна тајна*, Београд, 1970
26. Кековић, З., Милошевић, М. (2011). КРИМИНАЛИТЕТ КОРПОРАЦИЈА – КРИМИНОЛОШКИ И КУЛТУРОЛОШКИ АСПЕКТИ . *Социолошки преглед*, vol. XLV (2011), no. 1, стр. 19–44
27. Спировић-Јовановић, Л. (1971). Prikaz: Др Бојан Забел, Пословна тајна, Београд, 1970, стр. 111, (ПР), 5–6/71, стр. 634–638.
28. Milošević, M., & Mladenović, M.. (2017). Upravljanje pravnim rizicima kao element korporativne bezbednosne politike. *Srpska politička misao*, 24(3), 289-230.

Pravni akti:

1. Directorate General for Internal Policies (2014). Trade Secrets. European Parliament
2. Direktiva 2016/943 Evropskog parlamenta i Saveta od 2016. godine, o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija (poslovne tajne) od nezakonitog pribavljanja, upotrebe i otkrivanja, Službeni list EU L br. 157/1
3. Krivični zakonik ("*Sl. glasnik RS*", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019)
4. OECD (2015). APPROACHES TO THE PROTECTION OF TRADE SECRETS. In: ENQUIRIES INTO INTELLECTUAL PROPERTY'S ECONOMIC IMPACT. Str. 127-173
5. Proposal for a Directive of the European Parliament and of the Council on the protection on undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure od 28. novembra 2013, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0813:FIN:EN:PDF>

6. World Intellectual Property Organization – WIPO (2019). Module 4: trade Secrets.
7. ZAKON O ZAŠTITI POSLOVNE TAJNE ("Službeni glasnik RS", br. 72/2011)
8. Zakon o zaštiti poslovne tajne (*"Sl. glasnik RS", br. 53/2021*)
9. Web stranica Advokatske kancelarije Žunjić - <https://zuniclaw.com>