

ЕКОНОМИЈА, КОНКУРЕНЦИЈА, ПРЕДУЗЕТНИШТВО

UDK:338.246.2:343.321:339.137.27

Biblid 1451-3188, 12 (2013)

Год XII, бр. 45–46, стр. 153–167

Изворни научни рад

Слободан НЕШКОВИЋ¹

Вук РАИЧЕВИЋ²

Раде ГЛОМАЗИЋ³

**ЕКОНОМСКА ШПИЈУНАЖА И ЗАШТИТА
КОНКУРЕНТНОСТИ – КОНТРОВЕРЗЕ ЕВРОПСКОГ
ЗАКОНОДАВСТВА**

ABSTRACT

Today's time is characterized by, among other things, the domination of the most developed countries in the sphere of economic espionage, which in the business world represents technological and developmental supremacy over competition. What represents supremacy today is information which has become the fourth obligatory factor of production, beside capital, work power and technology. The very information is the most important for acquiring advantages over competition and this is why the biggest world companies use an increasing amount of their capacities for the purpose of carefully protecting industrial, production and financial information which will enable them to gain advantage over competition

¹ Професор др, Универзитет Привредна академија, Факултет за економију и инжењерски менаџмент, 21000 Нови Сад, Цвећарска 2; тел: 021.469.513, е-маил: slobneskovic@gmail.com.

² Професор др, Универзитет Привредна академија, Факултет за економију и инжењерски менаџмент, 21000 Нови Сад, Цвећарска 2; тел: 021.469.513, е-маил: vuk.m.raicevic@gmail.com.

³ Студент докторских студија, МБА, Мр, Европски центар за мир и развој Универзитета за мир УН; glomazic@gmail.com.

and position better on the domestic and global market. Protection of confidential information from espionage or theft is critically important for the organizations that want to maintain their competitiveness and supremacy on the market. It is considered that over 70% of the value of a typical small or medium business is in its intellectual resources – knowledge, technology, employees or know-how. But how many employees actually knows and understands what trade secret is? The article before you strives to identify the main characteristics of legal framework and business practices in the protection of trade secrets. We specifically gave an overview of European legislation and the perceived shortcomings in the existing laws and practice. The article focuses on some of the controversies of European legislation in this field, especially its emphasis on civil law, and outlines the importance of the protection of trade secrets through criminal law. This law would empower European companies in their struggle against business espionage which endangers their development and by extension, their competitiveness.

Key words: economic espionage, business espionage, trade secret, competitiveness, intellectual property

1) МЕТОДОЛОГИЈА ИСТРАЖИВАЊА

Десктоп истраживањем обухваћено је и анализирано око 5000 страница различитог јавно доступног материјала и дат је преглед данашњег стања области конкуренције, пословне и економске шпијунаже и преглед релевантне легислативе у Европској унији. За потребе овог рада истакнути су само најбитнији налази правне анализе.

Чланак започињемо прегледом појма конкурентности и релевантних детерминанти, затим прегледом појма економске шпијунаже и њених релевантних елемената. Анализу економске шпијунаже завршавамо моделом сценарија да бисмо показали могуће смерове и приближили аспекте деловања, а самим тим и отворили разматрања о могућим консеквенцама ових активности. Чланак нуди базични преглед потребних података обрађених на приступачан начин, јер се често дешава да се концепти који би требало и који би чак и морали да буду јасни и недвосмислени свим грађанима, често износе ускостручним језиком, што успорава имплементацију корисних, а понекад и неопходних активности, концепата и идеја. Дакле, намера аутора није била да опишу и објасне све о економској или пословној шпијунажи, конкурентности и сродним областима, већ да прикупљајући јавне, лако доступне секундарне, али релевантне податке, да један базични критички осврт на начин који би требало да послужи као основа за будуће истраживање и деловање.

II) ЕКОНОМСКЕ ДЕТЕРМИНАНТЕ КОНКУРЕНТНОСТИ

КонкурENCIЈА је процес надметање тржишних учесника и омогућује националним економијама „да остваре одрживи раст и дугорочни просперитет“ (Schwab, 2009:3). Глобална конкурентност, која мери микроекономске и макроекономске показатеље националне конкурентности, дефинише се као „скуп институција, политика и фактора који одређују ниво просперитета земље“ (Schwab, 2009, 4). Конкурентност на тржишту резултат је најефикаснијег начина управљања ресурсима у циљу повећања продуктивности. Конкурентност подстиче развој културе, економије и менаџмента и „представља својеврстан допринос друштвеном производу, животном стандарду и запослености“ (Paraušić, 2007:598). Према Rutkauskas (2008:89) конкурентност подразумева идентификовање произвођача, фактора конкурентности и околности које ће утицати на постизање потребног нивоа конкурентности. Идентификација, односно откривање нивоа фактора конкурентности, обима средстава и трошкова, као и интеракција очекиваних резултата је озбиљан посао. Унапређење конкурентности, сматрају Aguilera-Enriquez, Gonzalez-Adame i Rodriguez-Camacho (2011: 58) могуће је модернизацијом процеса управљања и производње кроз употребу савремених технологија. Бавећи се питањем унапређења конкурентности и скраћењем животног циклуса Јовановић и сарадници (2010: 13) истичу да „пословање компанија све више зависи од интелектуалне својине (Intellectual Property, IP). Економија заснована на знању и нематеријалним добрима, као што су интелектуална својина, људски капитал и организационе способности, имају кључну улогу у вођењу послова и економском расту“.

III) ПРАВНЕ ДЕТЕРМИНАНТЕ КОНКУРЕНТНОСТИ

Право, због свога карактера, мора на специфичан начин да дефинише односе реалне привредне конкуренције и ставове економске науке о њој. То чини правна теорија изграђујући сопствени појам „конкуренције“, али и законодавни орган приликом усвајања законске материје из ове области. Закон конкуренције је основни принцип на коме се заснива слободно тржишно привређивање, које представља преовлађујући начин у данашњим привредним системима. КонкурENCIЈА није могућа без признавања тржишта, јер јој преко механизма цена припада ефикасна расподела (алокација) роба и услуга. Ограничења лојалне конкуренције која проистичу из монополских и олигополских позиција, договорним споразумима око цена, државним интервенцијама сузбија се регулативом о заштити конкуренције.

IV) ЕВРОПСКИ ЗАКОН О ЗАШТИТИ КОНКУРЕНЦИЈЕ

КонкурENCIЈА представља основни механизам тржишне економије која подстиче компаније да своје производе и услуге нуде на тржишту под најповољнијим условима. Она подстиче ефикасност и иновативност а при томе смањује тржишну цену.

Да би биле ефикасне, компаније морају да делују независно једне од других, и да та одвојеност кроз процес конкуренције ствара позитиван притисак једних на друге. Закон Европске уније о заштити конкуренције настао је из жеље да се осигура рад државе у регулацији тржишта без ометања корпорација. Управо зато настали су и европски уговори који омогућавају слободну конкуренцију, а спречавају формирање картела, монопола, поделе тржишта и намештање цена. Ово је омогућено кроз четири главне политике које спроводи Европска унија:

1. картели, контрола антиконкурентских активности које утичу на ЕУ, донесена 1994. у оквиру акта оснивања Европске економске заједнице. Ова област је покривена чланом 101. Споразума о функционисању ЕУ;
2. монополи, или спречавање формирања доминантног положаја на тржишту. Ова област је покривена чланом 102. Споразума о функционисању ЕУ;
3. спајање и аквизија, контрола спајања, аквизиција и заједничких улагања у које су укључене компаније које имају одређени, законом прописани ниво промета;
4. државна помоћ, контрола начина директног и индиректног начина давања помоћи компанијама од стране држава чланица ЕУ. Ова тачка налази се у члану 107. Споразума о функционисању ЕУ.

Задња тачка представља јединствену карактеристику Закона о заштити конкурентности ЕУ. Како је ЕУ сачињена од суверених држава чланица, тако политика заштите конкурентности и активности стварања јединственог европског тржишта не би била примењива уколико би државе чланице имале слободу да подржавају своје националне компаније по сопственом нахођењу.

Европска комисија и њен Генерални директорат за конкуренцију су надлежне инстанце за примену Закона о заштити конкуренције ЕУ иако је, на пример, државна помоћ у неким секторима, као што је транспорт под управом Генералног директората.

V) ЕКОНОМСКА И ИНДУСТРИЈСКА ШПИЈУНАЖА

Индустријска шпијунажа, економска шпијунажа или пословна шпијунажа јесу форме шпијунаже спроведене у комерцијалне сврхе, за разлику од шпијунаже које се одвија у сврхе националне безбедности. Економска шпијунажа најчешће је спроведена од стране влада и има интернационални карактер, док је индустријска или пословна шпијунажа најчешће националног карактера и одвија се између компанија или корпорација.

Анализа конкуренције и економска или пословна шпијунажа

Анализа конкуренције представља легалан начин систематског прикупљања, анализирања и управљања информацијама о пословним конкурентима. Анализа конкуренције представља активности као што су анализа новинских чланака, пословних публикација, он лајн материјала, специјализованих база података, информације на конференцијама и пословним сајмовима, а са циљем добијања јасне слике о конкурентним компанијама. Ова врста анализе потиче од маркетиншког истраживања, уз примену принципа и праксе војне и националне безбедности. Разлике између анализе конкуренције и економске или пословне шпијунаже често није јасна. Оно што је потребно јесте разумевање правних основа, односно легалних и нелегалних начина приступања информацијама, и повлачење линије између ово двоје.

Типови економске или пословне шпијунаже

Економска или пословна шпијунажа се одвија на два основна начина. Укратко, сврха шпијунаже јесте добијање информација и знања о организацији или организацијама. То може бити у форми прибављања интелектуалне својине, као што су информације о индустријским произвођачима, идејама, технологијама и процесима, формулама и рецептима. Она такође може бити и у форми прибављања оперативних информација, као што су база података клијената, продајне и куповне цене, маркетиншке информације, информације о истраживању и развоју, стратешки и пословни планови, политике или планирана учешћа на тендерима.

Индустрије у фокусу шпијунаже

Економска или пословна шпијунажа се најчешће повезује са високотехнолошким индустријама које су компјутерска, софтверска и

хардверска индустрија, аеронаутика, биотехнологија, транспортне и инжињерске технологије, телекомуникације, аутомобилска индустрија, енергетика, машинска индустрија, текстили производња одевних предмета и слично. Једна од најчешће таргетираних регија на свету је Силиконска долина у САД-у, иако се свака делатност базирана на информацијама релевантним за њену конкурентност на тржишту налази у фокусу економске шпијунаже.

Крађе и саботаже информација

Информације на тржишту најчешће могу бити разлика између успеха или пропасти компанија. Ако је релевантна информација украдена онда компанија губи тржишну предност и постаје мање конкурентна. Иако је, у пословном свету, велика већина информација прикупљена на легалан начин кроз анализу тржишта у појединим случајевима у пословним круговима, одлучују се и за нелегалне опције, то јест за крађу информације. То се најчешће дешава уколико је пословање компаније доведено у опасност од стране конкурената. Последњих година дошло је до експанзије појаве економске или пословне шпијунаже, а самим тим и до ширења дефиниције оног што сматрамо пословном шпијунажом. На пример саботирање рада компаније данас, у ширем смислу, се сматра пословном шпијунажом. То значи да се појам шпијунажа и саботажа све више поистовећују, што доказују бројне студије владиних и пословних стручњака.

Легални начини приступа информацијама

Опште је познато да се преко 95% потребних информација у економској обавештајности може добити и добија легалним путем. Постоји више начина да се до тражених информација дође без коришћења нелегалних средстава или метода.

Интернет представља најлакши и највише коришћен начин проналажења информација о економским субјектима. Према неким истраживањима, између 1990–1995. дошло је до повећања економске обавештајне активности од преко 300%, и за то је као главни кривац означен интернет и информације које он пружа. Најчешћи начин за добијање информација је путем *e-mail*, као и путем разних упита. Евидентна је ствар да је информатичка образованост запослених прилично ниска када се ради о безбедности на интернету. Приступ друштвеним мрежама типа *Facebook*, *Myspace*, *Twitter* или разним *chat*-собама, представља велику опасност за

сваку компанију, јер су запослени склони да у необавезним разговорима, чак и потпуним странцима, причају врло поверљиве ствари. Популарности интернета као начину за прибављање поверљивих информација доприноси и анонимност, коју је много лакше остварити путем интернета него у неким другим ситуацијама. Могућност широкопојасног – бродбанд приступа интернету са јавних места попут библиотека или интернет кафеа пружа велике могућности за потпуно анониман економско обавештајни рад. Претрага запослених је уобичајен начин добијања информација. Најчешће се користи такозвани „фантомски интервју“. Од стране фирме А се унајми трећа особа да би интервјуисала запослене фирме Б ради наводног запослења, а у циљу извлачења података од запослених. С обзиром да не постоји намера да се интервјуисани запосли, ова метода је врло неетичка, а у неким ситуацијама се може сматрати и шпијунском делатношћу. Заједничка улагања и спајања фирми представљају још један начин како се легално долази до битних информација. Ако запослени из фирме А дуже време раде заједно са запосленим из фирме Б, очекивано је да ће се временом сматрати за партнере, попуштају безбедносни протоколи и омогућава им се приступ информацијама и технологијама. Такође још једна сигурна солуција за долазак у посед тражене технологије представља куповина или преузимање компаније, али то је прилично скупо решење. Конференције, изложбе, семинари и сајмови представљају добро место да се у директном контакту извуку важне информације. Због знања и стручности, често су учесници ангажовани од стране компанија или влада ради прибављања информација. Директне посете су дуго времена биле вредан извор информација из технолошких или производних компанија. Посетиоци су обучавани како да дођу до вредних информација намерним уласком у забрањене зоне, недозвољеним фотографисањем или постављањем питања изван дозвољених оквира. „Копање“ по смећу представља још један одличан извор разних података, као што су бачени документи, забелешке или слично. Ово је сасвим легално зато што се одбачена ствар не сматра ничијим власништвом. Наравно, уколико се канта за смеће налази у ограђеном простору без дозволе уласка, онда то представља кривично дело. Из овог извора се често могу извући веома вредне информације.

Нелегални начини приступа информацијама

Иако представљају само мали део економских обавештајних података, подаци добијени на нелегалан начин су често највреднији, пошто су толико важни да се до њих не може доћи легалним путевима. Организовани

криминал је постао врло чест начин за прибављање информација из предузећа. Глобализација бизниса омогућила је и неке нове транснационалне облике криминала. Тако се криминалци не либе да притиском и уценама на пословне људе уђу у највеће компаније, и својом снагом и моћи, која је често већа од локалних власти, представљају велику опасност за бизнис и индустрију. Независни предузетници укључују независне или слабо повезане особе у економској шпијунажи. У суштини, ради се о приватним детективима који су унајмљени од стране компанија ради прибављања информација које компанија унајмљивач сматра потенцијално корисним за себе. Ови људи, у зависности од своје похлепе за новцем, не либе се и тежих повреда закона ради прибављања тражене „робе“.

Без обзира ко је лице које прибавља информације, постоји неколико начина на које компаније или чак стране владе прибављају информације. Запослени (инсајдери) са правом приступа представљају велики безбедносни проблем за компаније. По неким истраживањима, преко 75% економске шпијунаже се обавља преко инсајдера, особа које долазе из саме фирме или имају приступ осетљивим подацима. Наравно, постоји одређен број људи који ненамерно одају тајне које не би смели. Одређен број информација се одаје приликом необавезних ћаскања уз пиће после посла, када пажња попусти и људи су склонији да кажу више него што би смели. Такође се користи измамљивање информација од стране обучених професионалаца, који на посредан и вешт начин збуњују жртву и наводе је да ода ствари које иначе не би. Ово се назива социјални инжењеринг, и иако само по себи није кривично дело може бити увод у даља кривична дела. Инфилтрација међу запослене представља добар начин за шпијунажу. Пошто се без већих тешкоћа у великом броју случајева може ући унутар субјекта шпијунаже помоћу фалсификованих – лажних докумената, овим приступом је степен успеха шпијунаже драстично повећан. Регрутација запослених је један од најефикаснијих начина шпијунаже. Једном када се инсајдер или „кртица“ регрутује помоћу мита или неког другог начина, може му се тражити посебна врста информација, а не све на шта наиђе. Сакупљач информација не треба да буде фокусиран на извршне директоре или истраживаче, већ ће се много више постићи регрутацијом нижег особља, као што су секретарице, рачунарски техничари или чак и особље одржавања. Овде постоје две предности: нижи нивои запослених су много мање сумњиви, а често имају већи приступ информацијама, и њихова цена може бити много нижа, а воља за сарадњом много већа него рецимо генералног менаџера. Овај начин шпијунаже је прилично лак, јер један број запослених и на своју руку краде информације ради даље продаје, док су други

незадовољни односом према њима и као створени за овакву врсту сарадње. Провале и крађе представљају традиционалан начин за прибављање обавештајних података. Иако се у већини случајева ради о физичкој крађи докумената, приликом које се они отуђују, може се десити да провалник само фотографише или умножи тражени документ, тако да жртва и не зна да је покрадена, и нормално наставља рад на пројекту, што конкуренцији омогућава праћење развоја и даље информације. Овај начин је обично повезан са осталим начинима економског обавештавања. Електронски надзор се све више користи како техника напредује, пошто је могуће издвојити један глас између хиљада на стадиону или прислушкивати мобилни телефон жртве. Док је раније ова опрема била ексклузивитет државних обавештајних служби, данас је могуће за мало новца купити најквалитетнију опрему за прислушкивање и надзор. Као што се види, широк је дијапазон средстава и техника за долажење до информација. Неке су легалне, неке не али с обзиром на жестину данашње тржишне утакмице, не треба се заваравати да свака компанија којој су потребне информације неће прибећи сваком начину да би дошла до њих, био он легалан или не. Традиционалне тржишне утакмице се претварају у праве ратове, и ту циљ оправдава свако средство, те свака компанија мора да мисли првенствено на сопствену безбедност.

Пословна шпијунажа путем информационих технологија

Компјутери, Лан мреже и интернет омогућили су да се много лакше него пре долази до пословних тајни. У данашње доба информационих технологија пословни шпијуни не морају да проваљују у канцеларију да би дошли до докумената са релевантним информацијама. Коришћењем нових технологија, копирање и преношење информација путем интернета постало је лако и анонимно. Стара изрека је да је информација моћ, а моћ је новац, а пословни свет поседује велике количине информација. Те информације налазе се у патентима, тајним формулама, шемама производње, плановима продаје и куповине, маркетиншким и извозним стратегијама и оне имају веома велику вредност у пословном свету и зато су и предмет шпијунаже. Компаније могу да очекују нападе путем разних техника, а недостатак мера безбедности и недовољна обука чланова компаније омогућава њихову успешност у мањој или већој мери. Најчешће технике које се користе за пословну шпијунажу путем информационих технологија су „хаковање” и социјални инжињеринг. Хаковање се сматра најчешћим методом шпијунског прикупљања информација и све више и више расте његова популарност.

Разлози зашто је хаковање све више популарно су двострани. Са једне стране постоји веома велики број хакерских алата, на пример тренутно постоји преко 100 000 *web* сајтова који нуде бесплатан *download* хакерских алата. Са друге стране то је метода коју је релативно лако научити зато што понуђени алати не захтевају неко веће знање компјутерских протокола и скоро су једноставна за коришћење као било који Microsoft програм. Социјални инжињеринг је друга популарна метода за прикупљање поверљивих информација, а огледа се у томе што се прати одређена особа од које се покушавају прибавити релевантне пословне информације, а најчешће кориснички налози и лозинке за приступ компанијским мрежама.

Могући сценарији пословне шпијунаже

На основу свега горе наведеног можемо да креирамо неколико ситуација које презентујемо у облику негативних сценарија пословне шпијунаже. Сценарио 1: Радник производне компаније, запослен, а уједно и хакер користећи своје компјутерско знање лако долази до информација са компанијског сервера. Он на серверу аплодује систем за праћење и прикупљање информација. Помоћу тог система он прикупља лозинке за приступ свим деловима компанијске мреже. Једном унутар система он лако долази до делова базе података у којим се налазе подаци клијената, компанијски уговори и информације о ценама. Он уступа те податке конкурентској компанији која користи те информације да их победи на тржишту. Сценарио 2: Изврсни директор компаније је на путу и са собом носи свој пословни лаптоп. У лаптопу се налазе сви пословни подаци од важности за компанију. Директор оставља лаптоп у своју хотелску собу и одлази на ручак. За то време уговараач конкурентске компаније чека испред собе док собарица не уђе да спреми собу. Тада он долази и представља се као власник собе и кад је ушао уз помоћ опреме за брзо даунлодовање „скида“ све податке са лаптопа и одлази не оставивши никакве трагове. У исто време, његов партнер прати директора за време ручка у случају да се он неочекивано врати и телефоном га обавештава о његовом кретању.

Заштита од економске шпијунаже

Заштита поверљивих података од шпијунаже или крађе је критично важна за организације које желе да задрже своју конкурентност и надмоћ на тржишту. Рачуна се да преко 70% вредности типичног малог или средњег предузећа представљају његови интелектуални ресурси – знање,

технологије, запослени или *know-how*, али колико запослених заиста зна и разуме шта је то пословна тајна? Свака компанија која размишља „корак унапред“ требало би да оформи посебан тим који ће се бавити интеграцијом и управљањем трима стубовима традиционалне безбедности: физичком безбедношћу, ИТ безбедношћу и управљањем ризицима. Наравно, да би компанија избегла да буде жртва економске шпијунаже, морају се предузети три обавезна корака. Идентификовање пословне тајне представља први важан корак у заштити од економске шпијунаже. Јер да би се пословна тајна могла штитити, мора се прво препознати и документовати. Тек када се процени њена тржишна вредност, могуће је предузети кораке ради креирања програма њене заштите, што није увек лако. Велики део проблема је то што већина запослених не уме да препозна шта би могло представљати пословну тајну. Осетљиви делови, као што су *know-how* и нове технологије су веома рањиве према крађи. Пословна тајна која није документована је још увек овде, али је незаштићена. Зато је задатак тима за заштиту да развије и примени технике и поступке који омогућавају запосленима да препознају пословну тајну и активније учествују у њеном управљању и чувању. Управљање ризицима или предузимање разумних мера да би се избегло шпијунирање. С обзиром да се много пословних тајни предузећа може наћи у личним рачунарима запослених, електронским порукама или разним интерним документима, тим задужен за безбедност мора да разуме како се пословне тајне употребљавају, како им се приступа, како се уносе и износе из компаније. Када потпуно овладају путањама пословних тајни, могу креирати систем који ће класификовати, архивирати или уништавати искоришћене пословне тајне без бојазни да ће оне да падну у погрешне руке. Наравно, да би се ово постигло, тим мора имати неограничен приступ тајнама и систему, што значи да у њему морају бити људи од врхунског поверења. Чување пословне тајне је од виталног значаја за економску стабилност предузећа. Без јасног и квалитетног плана о чувању пословних тајни постоји ризик да запослени, који напуштају компанију, свесно или несвесно са собом понесу веома важне пословне тајне. Накнадно доказивање одговорности је тешко, а последице по компанију могу бити понекад катастрофалне, а по правилу веома скупе. Зато је много једноставније и ефикасније да се пословна тајна јасно идентификује, а запосленима јасно предочи њена важност и вредност. Једном када су правилно информисани, запослени поклањају много већу пажњу чувању пословне тајне. Наравно, не треба запоставити ни остале компоненте, као што је физичка безбедност података предузећа, као и ИТ заштита, јер су ту ризици много апстрактнији за већину запослених који не разумеју функционисање информационих система, а један квалитетан професио-

налац може направити већу штету него група лопова која физички упадне у компанију. Безбедносни тим јесте одговоран за прављење квалитетних и примамљивих програма заштите, али је одговорност свих запослених да те програме примењују, да би се осигурала њихова успешна примена. Тако се на радним местима развија једна општа култура безбедности, где је свако упознат са тиме која је то пословна тајна којом располаже и каква је његова одговорност у односу на њу. Наравно, једном направљен и имплементиран програм није гарант сигурности, већ се он мора стално прилагођавати, а запослени непрестано учити и тренирати безбедносној култури.

За разлику од економски развијених држава, код земаља у развоју, посебно у земљама у транзицији, као што је и наша, економска шпијунажа је, с једне стране, међу предузећима и предузетницима веома мало позната, док је са друге стране омражена, јер код многих још увек подстиче негативне конотације повезане са радом државних/владиних класичних обавештајно-безбедносних служби из прошлости, као и данас. Земље у транзицији су мање или више технолошки заосталије у односу на развијене земље, што условљава посебан приступ њиховој шпијунажи. Сваки вид шпијунаже се врши ради стицања одређене предности над конкуренцијом, док код земаља у развоју и транзиционих земаља она има и улогу вршења притиска ради остваривања циљева држава или њихових компанија.

Европски закони о заштити пословне тајне и интелектуалне својине

Заштита пословне тајне у оквиру ЕУ се разликује од земље до земље чланице и огледа се у различитим законским решењима и процедурама која су у неким земљама чланицама и веома нејасна. Земље чланице Европске уније не третирају пословне тајне као интелектуалну својину, стога оне и немају адекватну правну заштиту. Само поједине земље чланице третирају пословне тајне законом сличним традиционалној заштити интелектуалне својине као патент, жиг или ауторска права. Шведска је на пример донела Акт о заштити пословних тајни. Немачка је увела одређене клаузуле о заштити пословних тајни у законима о заштити против нелојалне конкуренције, закона о раду и кривичног закона. Велика Британија и Република Ирска су на пример уставним и законским решењима заштитиле право на пословне тајне. Уговорна одговорност се користи као заштита пословних тајни у односима са радницима у скоро свим чланицама Европске уније.

Контроверзе европског законодавства

Крађе пословних информација и интелектуалне својине једне компаније од стране конкурентске компаније или радника јесу најнегативнији сценарији које фирма може да доживи. За разлику од САД где се радикално покушавају зауставити овакве и сличне криминалне активности које угрожавају рад компанија, у Европи је знатно мање учињено на том плану. У овој области Европа заостаје за САД-ом како у дефинисању адекватне правне легослативе тако и техникама истраге које не могу бити спроведене због европских стандарда заштите људских права. Све ово је, у Европи, креирало амбијент у коме се крађа пословних тајни и економска шпијунажа врло ретко открива, а још ређе кажњава. За европске компаније од виталног је значаја да се оваква ситуација што пре промени. Пословне тајне које садрже информације од виталног значаја за рад компаније и чија економска вредност произилази из тога што су недоступне јавности заштићене су грађанским и кривичним правом у САД-у. Са друге стране, у Европи, где постоји корпус регулативе постоји и неискуство истражитеља и недостатак финансијских средстава за куповину технологија за надгледање и истраживање. Поред ових очигледних недостатака постоји и прекогранични елеменат ових кривичних дела, што додатно отежава њихово праћење и откривање. Једна од главних мањкавости европског законодавства у борби против пословне шпијунаже јесте недостатак сета стандардизованих закона који би регулисали ову материју међу државама Европске уније и координисали рад њихових служби за сузбијање ове врсте криминала. Међутим, Закон о приватности у Европи умногоме отежава овај посао, посебно у делу активности, праћења и прикупљања доказа против радника који се сумњиче за овакву врсту криминалних активности од стране компаније. Тако на пример, коришћење видео надзора у неким случајевима пословне шпијунаже користило се као доказни материјал, али у неким деловима Европе видео надзор радника је лимитиран, па чак и недозвољен. Компаније све више и више раде вишеструке провере приликом запошљавања. Оне такође, и из године у годину смањују број радника који имају приступ виталним подацима. У појединим деловима Европе, где то законодавство дозвољава, постоје системи за праћење рада рачунара запослених и приступа и трансфера података, али оно што недостаје европским компанијама јесте сет строжих закон против пословне шпијунаже који ће им омогућити да се радикалније боре са овом врстом активности која угрожава њихову конкурентност. У Европском систему пословне тајне су заштићене правним режимом који није део Кривичног закона. Тако на пример, Директива 2009/24/ЕЦ дефинише заштиту ауторских права за

компјутерске програме и даје ексклузивна права њиховом власнику, али у данашње доба интернета и пиратерије то није и не може бити довољно за заштиту ових права. Компаније које своје пословање заснивају на истраживању и развоју и проналазе иновативна решења кроз дугорочни рад и велике инвестиције. Оне самим тим долазе до конкурентске позиције на тржишту па самим тим морају бити заштићене и мора им се омогућити пословање у позитивним правним оквирима које штите и подстичу њихов рад и допринос у заједници.

Генерални закључак

Број случајева под истрагом везаних за незаконито откривање пословних тајни у Европи је у порасту. То је не само због пораста свести о овом проблему него и због повећаног значаја чувања пословних тајни у раду компанија. Ово је од посебног значаја за поједине индустрије као фармацеутска и биотехнолошка индустрија које се умногоме ослањају на права заштите „*know-how*“. Такође и прехранбена индустрија користи пословне тајне, један од највише цитираних примера је тајна формула Кока-Коле. Од посебног значаја је заштита пословних тајни у софтверској индустрији. Као што смо видели у Европи не постоји хармонизован систем заштите пословних тајни. Закон о заштити пословних тајни значи онемогућити трећу страну да на нелегалан начин дође до вредних информација које би злоупотребила на тржишту и тиме прибавила себи пословну корист од иновација. Тиме компанија која је предмет крађе трпи огромну материјалну штету, јер је улагала новац и труд у развој, а економски систем доживљава поремећај јер не постоји здрав развој конкуренције и подстицај иновација и инвестиција у истраживање и развој. Креирајући одговарајући правни оквир за заштиту информација од значаја за рад компаније, држава креира повољан амбијент за подстицај инвестиција у области технолошког развоја и ствара економију базирану на иновацијама, што је од виталног значаја за Европске фирме и њихову конкурентност на глобалном тржишту. Због свега тога мора се уложити додатни напор да се створи позитиван правни оквир који ће подржати даљи развој и одрживост иновативних компанија у Европи или ће Европа ризиковати да изгуби такве компаније.

ЛИТЕРАТУРА

- Arquilla, J. (1995). Ronfeldt D., „Mrežni rat i kiber rat RAND korporacija“, izvod iz studije objavljene u *Comparative Strategy*, Volume 12.

- Davenport, Thomas H.; Jeanne G. Harris (2007). *Competing on Analytics: The New Science of Winning*. Harvard Business School Press.
- European Commission – Competition -http://ec.europa.eu/competition/index_en.html
- Filipović, A., Bejatović, M., i Raičević, V. (2008), „Konkurencija – pojam, vrste i pravna zaštita“, *Pravo – teorija i praksa*, 25(7–8), 51–61.
- Jovanović, S., Dragutinović, S., Petrović, S.D. (2010), „Značaj, vrednovanje i eksploatacije intelektualne svojine“, *Industrija*, br. 4, str. 13–14.
- Kuehl, D., Libicki M. (1997). „Information Dominance“, National Defence University, Strategic Forum, Washington, Institute for National Strategic Studies, Number 132.
- Nešković, S. (2010), *Međunarodna ekonomska špijunaža i zaštita tranzicionih država*, Beograd, CESNA B.
- Nešković, S. (2011), „Doprinos ekonomske diplomatije privrednom razvoju zemlje“, Novi Sad, FIMEK, *Ekonomija – teorija i praksa*, 4, (2).
- Nešković, S. (2011), „Ekonomska špijunaža u savremenoj međunarodnoj konstelaciji“, Novi Sad, FIMEK, *Ekonomija – teorija i praksa*, 4, (1).
- Nešković, S. (2012), „Ekonomske implikacije informacionog ratovanja u savremenim međunarodnim odnosima“, Novi Sad, FIMEK, *Ekonomija – teorija i praksa*, 4, (2).
- Paraušić, V. (2007), „Institucionalne i infrastrukturne prepreke konkurentnosti Republike Srbije“, *Međunarodni problemi*, br. 4, str. 597–626.
- Paraušić, V., Cvijanović, D. (2007), „Konkurentnost privrede Srbije merena indeksima konkurentnosti Svetskog ekonomskog foruma 2007-2008“, *Zbornik Matice srpske za društvene nauke*, br. 123, 155–172.
- Raičević, V. (2010), *Pravo industrijske svojine*, Pravni fakultet za privredu i pravosuđe, Novi Sad.
- Raičević, V., Ignjatijević, S. (2011), „Određeni ekonomski i pravni aspekti spoljnotrgovinske razmene Srbije u Evropske unije“, *Računovodstvo*, br. 11–12, str. 101–108.
- Rud, Olivia (2009), *Business Intelligence Success Factors: Tools for Aligning Your Business in the Global Economy*. Hoboken, N.J: Wiley & Sons.
- Schwab, K. (2009), *The Competitiveness Report, 2009–2010*. World Economic Forum, Geneva.
- Stallings, W. (1995), *Network and Internetwork Security Principles and Practice*, Prentice Hall, Englewood Cliffs.
- Szafranski, R. (2001), „Teorija informacionog ratovanja – priprema za 2020. godinu“, prikaz članka, prevod pukovnik Bajić B.
- Tofler, A. (1998), *Rat i antirat*, Beograd, Paideia.
- Arquilla, J. (1995). Ronfeldt D., „Mrežni rat i kiber rat RAND korporacija“, izvod iz studije objavljene u *Comparative Strategy*, Volume 12.