dialogues Security

347.775-027.21 / 342.721-027.21 Review scientific article

THE PROTECTION OF BUSINESS SECRETS AND PERSONAL DATA IN PRIVATE SAFETY

Prof. Milan Daničić, PhD

Faculty of safety and protection, Banja Luka,

E-mail: milan.danicic@fbzbl.net

Prof. Milan Milosevic, PhD

Faculty of business studies and law, Belgrade,

E-mail: milanmilos@fpsp.edu.rs

ABSTRACT: It is well known that sources which threaten data privacy of economic subjects through human interference, no matter if it is accidental or on purpose, could be divided into: inner, outer, and combined sources. As outer sources of threatening are considered persons, who are not employed in the economic subject, but whose damaging behavior could influence negatively on the subjects safety. To this group are also classified the companies that are in charge of private security, including detective agencies as well. While working on assignments in their scope of work, these safety subjects come regularly to the data, which are regarded as a business secret and should not be published. All the collected data and knowledge during their investigation work could only be used for the original purpose and in the end of investigation should be handed over to the client (except for the ones, which are not considered as significant for the job and which should be destroyed in certain period of time). When keeping the business secret, a company or an agency is obligated to abide by the regulations for personal data protection, no matter if the data analysis is done automatic, half-automatic or in some other way. If subjects of private security have a need to use personal data, this is allowed only under conditions, which are regulated by the laws in this scope of work, or with clients consent. As for determination of secret data, it is important to differentiate public from secret ones, and to respect public principles for the simultaneously protection of the society and the state. Additionally, a business secret should be differentiated from the professional one, as well as business intelligence from business espionage

Key words: private security, business secret, professional secret, personal data, protective precautions

1. Introduction

Globalization processes, quick and permanent technological changes, unexpected development of informational and communicational technologies, as well as consequences which came as a result of world economic crisis, force economic entities to adjust their strategies and to leave previous traditional working ways. That is why today it is almost impossible to implement some important business process without managing of business information, which is a kind of a support to the top management of companies, in accordance with determined business politics and the environment in which an economic entity works.

When it comes to countries with a long history in market economy, a big accent is given to the protection and security of business information. Therefore, a big amount of funding is generated to above mentioned purposes. Practice showed that the security of business subjects and related confidential information are one of the most important keys to the success on the market. The loss of confidential information can lead to serious misbalances in a company business, and sometimes even to the complete downfall.

One possible way of endangering business secrets and personal data could also be subjects in the area of a private security (companies that are ensuring private security and detective agencies), which are hired by management corporations as outsourcing companies. This is one of the reasons why more and more expressed influences of private security sector in the area, that was traditionally reserved for the state structures that are conducting force, causes a various polemics among professional and public circles, especially when it comes to the protection of generally excepted human freedom and rights, and on the other side, to need for safeness as a subject of professional and commercial service providing.

In Republic of Serbia a relatively small number of economic societies protect their business secrets in an organized way. These habits are inherited from the socialistic period, when economic societies not only did not protect their information and projects, but also gave away these information for free. That is why it is important that every employee possess a security culture, i.e. a knowledge in the area of business protection.[13]

[13] Some definitions were published in the co-authors' work. In such cases, all the authors were separately listed.

2. **Business secrets and sources of their endangering**

It is not rare that terms business secret and business information are often used without a terminological difference. The expression business information is related to all the knowledge, which is in a function of market business and realization of interests and goals of economical entities. Today, when business is not limited just to single companies and economy as a field of human action, business information can have also a political, law, social, technological or scientific character. That means that every information, if and when needed, could be used as a business one; but it also means that any information does not have to be a business one, if it is not used as the one.[14] The existence of a huge number of information leads to two aspects of business information- a relativity (some information is a business information to one business subject, and is not to the other one) and relevance (it is not looked for any business information, than for the one that is useful and worth to the company). On the other side, a term: business secret represents a number of an information and data, which are not just used in a business, but also bring economical profit and competitive advantage to the company they belong to.[15] The subject of a business secret, which is being kept by its mediator, could be different things- production processes, technologies, inventions, business methods, ingredients of a product, content of a contract and many others.

The endangerment of business secrets by human action, irrelevant if it is done by accident or on purpose, could be divided, depending on the environment where the source is, into three groups: inner sources, outer sources and combined sources of endangerment.[16] When it comes to inner sources of endangerment, they are caused by employees in the company. The area of endangerment cannot be precise defined just to the working hours. That means that employees beside the working hours, caused by not implemented or not enough implemented security culture, by accident or on purpose could jeopardize a corporation business by transmitting the important business data. In outer sources of endangerment are classified all persons that are not employed in the company, but with their harmful actions could influence on a company security.[17] Finally, combined sources of endangerment are represented by common harmful actions of employees and persons that are not in a working relation to the company.

[14] Refers to: Javorović Božidar, Bilandžić Mirko, Poslovne informacije i business intelligence, Golden marketing & Tehnička knjiga, Zagreb 2007., page 115.

[15] Compare to: Katulić Tihomir, Uvod u zaštitu intelektualnog vlasništva u Republici Hrvatskoj, CARNet – Hrvatska istraživačka i akademska mreža, Zagreb 2006., page 50.

[16] Trivan Dragan, original quote, page 146.

[17] Extended in: Mandic Goran, Sistemi obezbedjenja i zastite, FCO, Belgrade 2004, page 35-37.

Negative effects on the level of endangerment of business secrets are higher when the business is led outside the home country; the information system is decentralized; the business is connected to the national security; the cooperation with competitive subjects is on a high level; „joint venture" investments are really high; dismissing of employees are in the process or are about to come in the near future; a high technology is used; there is no „business counterintelligence" programs for a protection from a business espionage; electronic business is involved; branched business partnerships exist etc.

1.1. **Subjects of Private Security and Endangerment of Business Secrets**

The main principle for the establishing and functioning of different types of private security is the individual's right to self-protection, which is transmitted by a contract to the other subjects in a private security sector. Besides that, the key impulse to the process of the privatization of the security in developed countries was a demand for improvement of efficiency of state institutions. The answer was more and more popular outsourcing of security jobs, which were confided before just to the state institutions.[18]

Considering possible illegal actions related to business in the area of private security, including revealing business secrets, the security culture of employees working in that sector demands a full professionalism, respect of legal principles, knowledge of methods and mediums, that are used by jeopardizers, knowledge of adequate mechanisms and procedures which could prevent endangerment of business subjects, admission of job applicants with a total respect of security demands, an effective inner work control and cooperation during an outer control, respect for the principles of confidentiality, growing cooperation with other subjects in the security system, avoiding influences of formal and informal centers of power, strict adherence to security procedures, taking care of personal security and document security, as well as avoiding „conflict of interest".[19]

When it comes to the Republic of Serbia, The Law of Private Security[20] determines the obligation of data protection, which is available to the subjects in the area of private security. The Clauses 30-32 of The Law determine that the data collected during the investigation of private security could only be used in that purpose, and cannot be given to other persons or publicized, unless if it is other declared or agreed. The person, to whom the data relate, has the full right to demand to see all the data, which includes overview, reading and listening, as well as noticing. On the other side, copying the material is also possible, but the person must bear the cost; as well as demanding for certain parts of data to be deleted or changed.

[18] Extenden in: Toyne Sewell Patrick, „Private Security Companies: The Reasons Why", Military Technology, Vol. 31, Issue 3, Mönch Publishing Group, Bonn 2007., pp. 60-61.
[19] Compare: Danicic Milan, stajic Ljubomir, Privatna bezbjednost, VSUP, Banja Luka, 2008., page 223.
[20] „Sluzbeni glasnik RS" 6poj 104/2013.

In the case of fulfillment or breach of contract, a legal entity, i.e. an entrepreneur for private security is obligated to hand over the data to the user or to delete them in the following 15 days from the day of the contract breach, or the agreement withdrawal; and the other data, which are not relevant or which the user refuse to take, should be destroyed in the following 8 days. The Law also established the obligation of the subjects of the private security to keep as a secret, in accordance to the law and other principles that arrange the data confidentiality, all the data collected during the work, except in the cases that are excluded by the law.

The Clause 68. of The Law of Detective Investigation[21]
determines that the data collected during the investigation can be used just for that purpose, and cannot be given to other persons or publicized, unless if it is other declared or agreed. In the case of fulfillment or breach of contract, i.e. written agreement withdrawal, a legal entity and entrepreneur for detective investigation are obligated to hand over the data to the user or to delete them in the following 15 days from the day of the contract breach, or the agreement withdrawal; and the other data should be destroyed in the following 8 days.

Besides that, a legal entity, i.e. entrepreneur for detective investigation, as well as employed detective are obligated to follow the law and other principles that arrange the data confidentiality, and to keep as a secret all the data collected during the work, unless if it is other declared or agreed. That obligation stays even after the investigation, i.e. after the employment of a detective. Otherwise, a legal entity/entrepreneur is obligated to keep all the contracts for years.

Adequate and effective regulations of private security sector, which means that democratic state institutions control and observe that sector, and the subjects in a private security on a professional and responsible way provide services to clients, is the main assumption that the sector contributes to the safety insurance in general. On the other side, private security without supervision and control, as well as weak regulated activities of the sector in developed countries can represent a serious problem that meanwhile in transitional and post-conflict countries can represent an obstacle to the establishment of peace, strengthening of the democracy and long-term development.[22]

[21] „Sluzbeni glasnik RS" 6poj 104/2013.
[22] Following: Pavlovic Gojko, Pravo privatne bezbjednosti – uporeda studij, Defendologija centar, Banja Luka, page 12.

1. The Protection of Business Secrets

Beside the standards of business ethics, business secrets exist because they are after all the protection from disloyal competition, support to the investigation activities and fomentation of innovation. In companies that are involved to development of new technologies, a business secret is used to keep safe the innovations during the patent admission process, and all the other data that are not covered with the patent (business strategies, data about business partners, deliverers, clients etc.)

The meaning of the protection of the business secret from disloyal competition is to legally sanction every act of illegal disclosure or acquisition of confidential information, which are legally controlled by an individual or a legal entity, i.e. the data usage by other persons in a way that is opposite to the law and good business practice. The main preconditions for enabling this kind of a protection are: that it is about the information, whose disclosure to other persons could harm the person, in whose possession the information is; that the information represents a secret, which as a whole or in a precise shape and as a part of an information collection, is not publicized or easy accessible to persons that are usually related to that kind of information; that the information has a commercial value and that is protected by its carrier in a certain way to keep its confidentiality.

It is considered that a program for a protection of business information, i.e. business secrets, has 3 functions: controlling over the information; enabling the individual access to the protected data, with previous identification of every individual, who is about to access; the existence of a technical possibility that in every moment it can be determined who, when, how, in which way and why had the access to the confidential data of the company, with an adequate record about that.[23]

[23] Refers to: Kovacich L.Gerald, *Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program,* Butterworth Heinemann Boston/Oxford 1999., p. 50

1.1. General and Special Ways of Protection of Confidentiality of Business Secrets

The protection of business information, compared to inner sources of endangerment of business subjects, is possible to perceive through its organizational, personal and normative aspects. The establishment of every organizational structure demands a work distribution, grouping and connection of certain types of jobs, as well as the process of transmission of authorization and responsibilities in doing jobs. The choice of an inner structure model depends on a certain number of conditions and environment, such as a number and structure of executants, available technical-technological possibilities, a type and a character of data that should be protected, a number of data users and other factors, which opens space for different solutions.[24]

Special protective measures in companies are: taking a special evidence about confidential data and about persons, who can access them; taking a written statements from the persons who have access to data, that they will not violate the confidentiality; giving secret names to the business documents; determining the number of copies and persons, who will access the data; copying or excerpting; keeping the secret documents in locked cases in the rooms with certain protective measures; organizing the transmission of documents using a courier, with a mandatory armed escort and all the possible technical protection measures; required written handover of duties between the persons, who use the secret documents, and the persons, who are keeping the documents safe; commission destruction of sketches, concepts, matrix and other material, that was used while working with the secret documents.[25]

An important role also plays a business counterintelligence, which is directed to safety of a business subject, arranging mechanism for its protection from competitive intelligence operations, as well as for protection from industrial espionage and similar illegal acts. The goals of Business Counterintelligence are: maintaining the position in the business environment, estimation of possible risks, threats and challenges to business subject, and effective protection of business subject from competitive illegal and unethical actions. That can only be achieved if the protection and safety measures are applied to all business segments. As confidential information are being located in various data bases, certain measures are needed to get the ultimate protection, confidentiality and integrity of informatics and other communication systems in a company.

[24] Trivan Dragan, original quoet page 146.

[25] Compare to: Stajic Ljubomir, *Osnovi sistema bezbjednosti,* Pravni fakultet, Novi Sad 2008., page 325.

[26] Extended in: Bilandžić Mirko, *Poslovno-obavještajno djelovanje: Business intelligence u praksi,* AGM, Zagreb 2008., str. 78

As employees also have access to the confidential data, certain protection mechanisms, procedures and norms of behavior need to be implemented. That is why it should be defined with certain acts which information are considered as a business secret, as well as which measures, actions and other procedures are required in order to preserve the confidentiality.[27] Likewise, certain safety mechanisms are required when new job applicants are being tested, so that the risk of a possible abuse of confidential data is minimized.

1. Normative Aspects of Protection Of Business Secrets in the Republic of Serbia

The Law of Protection of Business Secret[28] from 2011. represents a try to fill an emptiness and to generally solve problems related to the protection of business data and information, which were before protected just on the level of individual business subjects. As a consequence, as business secrets were declared various processes and procedures in companies, while in practice there was no sanctioning of real and harmful disclosures of business secrets. Even though the mentioned Law is still valid, court and business practice until now did not meet the acquirements, which were promised by the Law.

The main subject of the Law is a normative ordering of legal protection of business secrets, which belong either to national or foreign individuals and legal entities, from a various actions of disloyal competition. The legal definition of business secret covers every information that has a commercial value, with a condition that the mentioned one is not publicized or that its content is accessible to unauthorized persons, who could have some financial benefit while using or transmitting it. The business secret can exist only if its carrier is protecting it in an adequate way according to the law, business politics, contract obligations of business subject or valid national or international standards, with a goal to keep the confidentiality of information, assuming that the disclosure to other persons could have harmful effects to the carrier of business secret. That is why, the Clause 8. of the Law determines that any action taken within business activities, that as a consequence has a disclosure, collection, transmission or usage of data and information, that represent a business secret, with a condition that all the actions are done without an approval from a carrier, in illegal way and opposite to good business practice, represents an act of disloyal competition.

In this way defined a term of business secret direct us to the fact that not every information represents a business secret, neither can any arbitrarily be declared in that way. To have the status and to be accepted as the business secret by the law, the information has to meet the acquirements of confidentiality, market values compared to the competition and previous reasonable taken measures for keeping it confidential.

[27] Following: Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, *Korporativna sigurnost,* Udruga hrvatskih menadžera sigurnosti – UHMS, Zagreb 2011., str. 239.

[28] „Sluzbeni Glasnik RS", number 72/2011

When it is said „in the way opposite to good business practice", the Law implies on every action, which is taken in the market game, and which is harming or could harm competitive business subject or other individual or legal entity. That especially is applied to: violation of contract regulations, related to protection of business secret; a various number of cheats; abuse of business trust; business espionage; inducement to any of the mentioned actions; collection of the data and information, which represent a business secret, by persons who knew or had to know that such an information is a business secret, and that it is obtained from a person, in whose possession it is.

The Clauses of the Law of Protection of a Business Secret determine civil-law protection of subjects in this area, so that in cases of violation of the protection of business secret, the carrier has a right to sue, i.e. to activate the process in front of the judicial instance against all the persons, who took a part in the violation of the protection of the business secret. That applies to illegal collection, obtaining, disclosure, use or any other way of abusing of a business secret.

In the Clause 11, Paragraph 3 of the Law of Protection of Business Secret, a procedure for compensation of damage is determined (the real damage and the lost gain). If the violation is done on purpose, it could be legally demanded that instead of the compensation for the damage, the triple bigger compensation than a usual one is asked for. The Law also determines other sanctions, such as exclusion from the economic society, cessation of employment, and publishing the verdict at the expense of the defendant. Finally in these cases, the court can pronounce a temporary measure, that refers to exclusion and withdrawal of the subject and products, which came as a result of the violation of the business secret, from the market.

Criminal Law Code of Republic of Serbia[29]
determines a criminal act, called Disclosure of Business Secret. This act exist in two shapes- disclosure of business secret and obtaining the business secret. Disclosure of the business secret is done by a person, who unauthorized transmits, hand over or in any other way make the confidential business data accessible, while the person, who collects these kind of information with the intention to hand it over to unauthorized person, does the criminal act of obtaining the business secret. The confidential data can represent a business secret for the whole state, a certain economic area or just for the one business subject. The Law determines data as the confidential ones because of their nature and the importance to keep them as a secret.

The criminal act Disclosure of Business Secret is alternative determined, i.e. it could be consisted out of transmission, handover or any way which makes the information available and a potential sales product. Transmission of the secret can be done in an oral or written way, direct or indirect, as well as using other communication mediums.

[29] "Sluzbeni Glasnik RS", number. 85/2005, 88/2005 - correcture, 107/2005 - correcture, 72/2009, 111/2009 and 121/2012, the Clause 240.

The condition that affirms the criminal act is that the business secret is transmitted, handed over or in any other way made available to other, uninvited person, i.e. every person, who is unauthorized to know the data or documents that represent data. Here the law makes no difference between the person who is transmitting and getting the business secret. Executor can be any person, and the act can be done direct or with eventual forethought, or from carelessness.

A severer form of criminal act Disclosure of Business Secret, which can lead to 2-10 years of imprisonment including a fine, is when the disclosure is done out of greed, or when some extreme confidential data are being revealed. The mentioned criminal act is done out of greed, when the executor did that to get some material benefit for himself or somebody else. Here is important to mention, that material benefit does not necessarily need to be obtained. The attention to disclose the confidential data is enough to determine a criminal act.

The Law of Economic Societies[30]

from 2012. determines obligations of entities, who have special duties to the economic society, and which are referred to the matter of business secret. The Clause 72. of this Law defines the term of business secret as "an information, whose transmission to other entities could harm the society, as well as an information, which has or could have economic value because it is not published, or easy accessible to others, who could get some financial benefits by transmitting or using it; and an information, which is being protected by the society with certain protection measures." Compared to earlier law solutions, a term business secret is expanded, so that it cover economic (business) significance of a certain information, harder availability of the information, as well as the protection with certain measures.

The Clause 74. of the Law of Economic Societies detailed determines consequences of violation of business secrets, which are made by entities who had a duty to keep the secret safe, and against who a sue can be conducted, as well as a demand to decompensate the damage, to exclude certain persons out of the economic society or to dismiss employees.

[30] „Sluzbeni Glasnik RS", number 36/2011, 99/2011 and 83/2014.

1. Personal Data Protection

The right to privacy in general is consisted of rights to respect an individual's private and family life, home and correspondence, as well as honor and reputation. A private life refers to a various number of rights, e.g.: personal data protection, a right to name and reputation, a right to moral and physical integrity, a right to respect of all forms of confidentiality etc.

To the privacy right appertain a personal data protection, which is guaranteed in the Republic of Serbia with the Constitution of Republic of Serbia.[31] That is why any the use of personal data outside the original purpose is forbidden and punishable, except when it comes to conduct of criminal proceedings or when the safety of Republic of Serbia is in question. Any individual, except if the data are collected in accordance with clauses of Law of Personal Data Protection[32] (collection of the data by state authorities, without a confirmation of the individual) has a right to be informed about his obtained personal data, as well to the court protection against its abuse.

The Clause 3. of the Law of Personal Data Protection defines a personal information as any information, which refers to the individual, regardless the form and the carrier of information; on whose order, on which name or for whom the information is obtained; the date of obtaining information; the place of obtaining information; the way of obtaining information (directly, by listening-in, by watching, or by obtaining the documents, which contain the information etc.); or any other information or data characteristics.

2. Conclusion

Privatization of safety business is closely connected to two processes: a process of real safety needs, respect for human rights and freedoms, and the needs to keep them safe, as well as freedom of choice of every individual, how and in which way he will secure himself from unethical behavior; and the process of adjustment, related to safety, historical, cultural and other terms, which exist in every country.

The principle of securing a business secret obligates a company/agency that provides private safety services, to secure the obtained data and information. This kind of information are considered as a business secret, but the agency/company can use the obtained data just for the original purpose. After the work is done, agency/company has to hand over all the data to the client, except for the ones that are not relevant and have to be destroyed maximum 8 days afterwards. These agencies/companies are not allowed to publish or to hand over the obtained data to any other entity.

[31] „Sluzbeni Glasnik RS" number 98/2006, The Clause 42.
[32] „Sluzbeni Glasnik RS", number 97/2008, 104/2009, 68/2012 – the Decision of US and 107/2012, The Clause 13.

As a part of keeping a business secret a company, i.e. agency, that provides private safety services, is obliged to follow the principles related to the personal data protection. Every individual has a secured right to keep his privacy and other freedoms safe, especially when it comes to personal data privacy, regardless if the processing of the data is done automatic, half-automatic or on any other way. If an agency or a company has a need to use certain personal data, then it could be done just following the rules, which regulate this area, or with a client's agreement. When defining which data is confidential, a certain extent should be determined between public and confidentiality, i.e. about respect for public principles and at the same time for protection of society and state values.

Otherwise, until the end of 2013. The Republic of Serbia was characterized by a normative chaos of private sector in the area of safety, which was a consequence of old regulations, consisted of ten laws, which did not recognize the specifications of this sector. The mentioned regulation was a part of the law system in the Republic of Serbia, but did not in an adequate way determine a specific state of private safety sector, starting from the fact that for grounding of a company, that will provide a safety services, was treated as any other economic subject.

Literature

1. Bilandžić, M. (2008). *Poslovno-obavještajno djelovanje: Business intelligence u praksi*. Zagreb: AGM.
2. Boni, W., & Kovacich, L.G. (2000). *Netspionage: Netspionage: The Global Threat to Information*. Boston/Oxford: Butterworth Heinemann.
3. Ivandić Vidović, D., Karlović, L., & Ostojić A. (2011). *Korporativna sigurnost*. Zagreb: Udruga hrvatskih menadžera sigurnosti – UHMS.
4. Javorović, B., & Bilandžić, M. (2007). *Poslovne informacije i business intelligence*. Zagreb: Golden marketing & Tehnička knjiga.
5. Katulić, T. (2006). *Uvod u zaštitu intelektualnog vlasništva u Republici Hrvatskoj*. Zagreb: CARNet – Hrvatska istraživačka i akademska mreža.
6. Kovacich, L.G. (1999). *Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program*. Boston/Oxford: Butterworth Heinemann.
7. Mandic, G. (2004). *Sistemi obebedjenja i zastite.* Beograd: Fakultet civilne odbrane.
8. Pavlovic, G. (2011). *Pravo privatne bezbjednosti- uporeda studija*. Banja Luka: defendologija centar.
9. Stajic, Lj. (2008). *Osnovi sistema bezbjednosti.* Novi Sad: Pravni fakultet.
10. Toyne-Sewell, P. (2007). Private Security Companies: The Reasons Why. *Military Technology*, 31 (3), 60-62.
11. Trivan, D. (2000). *Korporativna bezbednost.* Beograd: Dosije studio.
12. *Ustav Republike Srbije,* „Sluzbeni glasnik RS" number 98/2006.
13. *Zakon o detektivskoj delatnosti* , „Sluzbeni glasnik RS" number 104/2013.
14. *Zakon o zastiti podataka o licnosti* , „Sluzbeni glasnik RS", number 97/2008, 104/2009, 68/2012 – the decision US and 107/2012
15. *Zakon o zastiti poslovne tajne*, „Sluzbeni glasnik RS", number 72/2011.
16. *Zakon o privatnom obezbedjenju,* „Sluzbeni glasnik RS" number 104/2013.
17. *Zakon o privrednim drustvima,* „Sluzbeni glasnik RS", number 36/2011, 99/2011 and 83/2014.
18. *Krivicni zakonik Republike Srbije,*"Sluzbeni glasnik RS", number 85/2005, 88/2005 – the correction, 107/2005 – the correction, 72/2009, 111/2009 и 121/2012.