

THE ROLE OF CRIMINAL LAW IN TRADE SECRET PROTECTION

Mladen M. Milošević, PhD¹

Faculty of Security Studies, University of Belgrade, Serbia

Abstract: The protection of confidential business information is one of crucial elements of corporate security policy. It is also an important tool for securing corporate reputation and market competitiveness. Trade secrets have legal protection through norms of Penal, Civil, Trade and Labor law. This paper focuses on the role of Criminal Law in prevention and reaction in cases of trade secret abuse. The author presents and analyses the provisions of Serbian Criminal Code that regulates trade secret breach. He also considers relations between different forms of liability for trade secret misuse in Serbian legal system. Special attention is given to the problem of poor court practice since criminal sanctions are very rarely imposed for trade secret breaches.

Keywords: The Role of Criminal Law, Trade Secret, EU Directive 2016/943.

INTRODUCTION

The aim of this paper is to provide theoretical analyses of the provisions of Serbian Criminal Code concerning trade secret disclosure. Although trade secrets are the subject of multiple legal protection (through Civil Law, with its sub-branches: Labour and Trade Law), Criminal Law, as ultima ratio, have a distinctive role, which should be carefully examined. The concept of trade secret in Serbian legislation was built on the ground provided by international treaties, so the analyses needs to consider their relevant provisions, and also the definitions of trade secret in other domestic legislative acts. The article is intended to achieve mentioned research goals. In the first part, we shall briefly present the establishment and main characteristics of the trade secret concept and point to two international legal documents that established the international concept of trade secret, which is now widely accepted. The central part of the article will be dedicated to relevant provisions of Serbian Criminal Code. Subjective and objective elements of criminal offense of trade secret disclosure will be thoroughly examined. In the conclusion, we shall try to provide a well based and overall assessment of these provisions and study the reasons for lack of court practise.

¹ milosevic@fb.bg.ac.rs



THE CONCEPT OF TRADE SECRET AND RELEVANT ACTS OF INTERNATIONAL LAW

The criminal offense of trade secret breach was introduced in modern Criminal Codes in order to protect the security of confidential business data, which is of great importance in the contemporary market economy. Trade secrets gained legal protection after other intellectual property rights, first in Anglo-American law. First case in which the court provided legal protection to trade secrets is considered to be *Peabody vs. Norfolk*, back in 1868 (although *Newbery v. James* in 1817 was the first case in which the trade secret was debated), while with the adoption of the American Restatements of Tort², in 1939, the protection of trade secrets acquired a legislative character. (Jameison, 1993: 521; Jovičić, 2018: 8).

The formula for making perhaps the most famous non-alcoholic beverage in the world - Coca-Cola, is not protected as a patent, but has been kept a trade secret for decades. A trade secret may remain permanently unknown to other economic entities, while the patent becomes publicly available after a certain period of time (depending on national legislation), provided that the patent holder gives permission for its use and is entitled to monetary compensation. A trade secret lasts as long as its holder can ensure secrecy. (Mandić, Putnik, Milošević, 2017; Jovičić, 2018: 12, 13).

Although a trade secret can remain hidden indefinitely, if another business entity manages to independently develop an identical formula, the holder of the trade secret does not enjoy protection as a patent owner and the entity that discovered the formula by independent research has the right to use the formula and start its own production. (Jovičić, 2018: 10, 11). This fact makes trade secret protection very important. (Mandić, Putnik, Milošević, 2017).

A trade secret provides a comparative market advantage only as long as it is hidden from competition. Trade secret breach can cause substantial economic harm to the holder (e.g. disclosure of a formula, recipe, method, market plan or strategy, results of a study or research, etc.). In addition to innovations, formulas, recipes, research, etc., examples of trade secrets include: estimated value of public procurement, the amount of income of individual employees, the content of corporate security risk assessment etc. (Milošević, Mladenović, 2017). In the information age trade secrets are obviously becoming more important. (Peterson, 1997).

Important instrument of International Law concerning trade secret was adopted by the World Trade Organization, in 1994 - The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).

(Available at: https://www.zis.gov.rs/upload/documents/pdf_sr/pdf/trips.pdf; last retrieved: 30.06.2021).

Next significant act was introduced by European Union: 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. (Official Journal of the European Union, L 157/1; available at: <https://eur-lex.europa.eu/eli/dir/2016/943/oj>; last retrieved: 25. 08.2021). Those documents strengthened (practically established) the international legal concept of trade secrets. The previous development of trade secret concepts in different legislatures was not always coherent, and is even characterized by some authors as sporadic. (Hilton, 1990: 287).

² It defines trade secret as: “any formula, pattern, device or compilation of information which is used in one’s business, and which gives [one] an opportunity to obtain an advantage over competitors who do not know or use it.” (cited according to: Wingo, 1997: 196).



TRADE SECRET DISCLOSURE IN SERBIAN CRIMINAL CODE

This criminal offense, stipulated in the Article 240 of the Serbian Criminal Code (Serbian Criminal Code, 2005), has three forms - basic, aggravated (qualified) and privileged. It is classified as a crime against the economy. (Stojanović, 2018; Delić, 2021).

The basic form of disclosing a trade secret is present when the perpetrator unauthorisedly discloses, hands over or makes available (in another way) trade secret data or obtains the same data with the intention of handing them over to an unauthorized person. The Code stipulates prison sentence from six months to five years.

The subject of this crime is a trade secret. The concept of trade secret is defined in several domestic regulations: the Law on the Protection of Trade Secret (Law on the Protection of Trade Secret, 2011; Law on the Protection of Trade Secret, 2021), the Law on Companies (Law on Companies, 2011) and the Criminal Code itself.

The Criminal Code defines it in Article 240, within paragraph 4: data and documents that have been declared a trade secret by law, other regulation or decision of a competent body passed on the basis of law, the disclosure of which would cause or could cause harmful consequences for a business entity. Given that this definition refers to other laws ("... data and documents that have been declared a trade secret by law, other regulation or decision of the competent authority issued on the basis of the law"), it is important to know the legal definition of trade secret in those laws. (Mandić, Putnik, Milošević, 2017: 302). In other words, this provision is sort of a blanket norm and its true meaning cannot be determined without examination of the law on which it refers.

Bearing in mind that the definition of trade secrets exists in two other legal acts – Law on Companies and Law on Trade secret Protection, the question is which one of them is of crucial significance. However, since one of them is a special law (*lex specialis*) dedicated exclusively to the matter of trade secrets, we will focus on the Law on Protection of Trade Secret.³

Still, we also have to stress that this Law was substantially changed ten years after it came into force. The reason for legislative change lies in the need of harmonising Serbian law with the Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

The Article 4 paragraph 1 of the Law/2011 states: "For the purposes of this Law, a trade secret is considered to be any information that has commercial value because it is not generally known or available to third parties that could be of economic benefit by its use or disclosure, and which is protected by its holder by appropriate measures, in accordance with the law, business policy, contractual obligations or appropriate standards in order to preserve its secrecy, and the disclosure of which to a third party could harm the holder of a trade secret."⁴

3 The Law on Companies provides definition of trade secret in Article 72.3. This definition matches criteria established by the Law on Trade Secret Protection and the essential elements of those legal definitions are the same, so there is no need to analyze it separately.

4 However, in Article 4.2.2, there is a provision that, at first sight, questions this conclusion, because it states: "other information that has been declared a trade secret by a special law, other regulation or act of a legal entity is also considered a trade secret". But, the act of the legal entity that provision mentions also has to be harmonized with the Law, so the conclusion stands – information that does not have the characteristics described in the previous paragraph cannot be considered a trade secret.



New Law on Protection of Trade Secret was introduced in 2021 (Law on Protection of Trade Secret, 2021; further: Law/21). The definition of trade secrets is very similar to the previous version. Although the legislator uses different style and formulations, they maintained the essential characteristics of the former legislative determination. Law/21, in Article 2.2.1, also stipulates three basic requirements which data has to meet in order to deserve the designation „trade secret“: 1. it must not be generally known or easily available to those who, through their regular activities, get in touch with that sort of information; 2. the data needs to have commercial value due to its secrecy; 3. a holder of trade secrets is obliged to take reasonable measures in order to adequately protect the data. (Law on the Protection of Trade Secret, 2021).

Both definitions reveal essential elements of a trade secret: it is information that has a commercial (market, economic value) precisely because it is hidden, i.e. inaccessible to a wider circle of persons; the knowledge about it by unauthorized person potentially brings economic benefits to the perpetrator and the holder of a trade secret has taken protective measures - which means that it can enjoy criminal protection only if the holder has taken reasonable measures to remain its secrecy. (Jovicic, 2018: 11). It is of crucial importance, therefore, that the holder takes appropriate measures (physical-technical, personnel, organizational, personal) to protect data (Mandić, Putnik, Milošević, 2017). U.S. case law confirms that simple business precautions are not sufficient. It is necessary for the holder to take more serious measures, to show that this kind of data is kept separately and more securely in relation to other business data. (Jovicic, 2018: 12). Therefore, the subject of the criminal offense can only be the information that meets the requirements of the Law. (Mandić, Putnik, Milošević, 2017: 302).⁵

ACTUS REUS OF OFFENSE

The actus reus of this crime is alternatively determined. The first form of action (actus reus) of the offense is to reveal a trade secret to an unauthorised person. Since the essential feature of a trade secret is exclusivity, it is only available to a narrow, limited circle of people. Any disclosure of information to a person outside that circle constitutes a breach of professional secrecy. For example, if a technologist from food company A, transfers to the director of food company B a recipe for making a special cured meat product, characteristic exclusively for company A. It is clear that a representative of a competing firm can have an important economic benefit from the knowledge gained, just as firm A has obvious harm. However, it is not necessary for the damage to occur and for the unauthorised person to benefit. Only revealing a secret to an unauthorised person is a completed criminal offense, and possible damage can only be an aggravating circumstance. Revealing (disclosure) of trade secrets can be done in a variety of ways. The legislator lists communication (orally, in writing, electronically, etc.), submis-

⁵ It is important to notice that previous Law on Trade Secret Protection introduced the so-called illegal trade secret, thus determining which data cannot be labeled as secret. Article 3 of the Law/2011 did not allow information to be classified as secret if it was made secret for the purpose of concealing a criminal offense, abuse of official position, exceeding of authority or other illegal conduct. Also, information that has to be made public by provisions of special laws cannot be proclaimed a trade secret (e.g. annual financial reports of legal entities must be publicly available on the website of the Business Registers Agency, and cannot maintain secrecy). However, the Law/21 failed to explicitly determine the concept of illegal trade secret, although it provided the indirect definition through provisions of Article 17.1, which explains the exceptions of the implementation of the Law. The approach is different in comparison with Law/11 – the legislator does not forbid some sort of data to be labeled as trade secret but stipulates that the person who reveals it will not be subject of sanctions or other legal measures and actions provided by the Law.



sion (by physically submitting a document containing data, e.g. a register with all research data and its results, or a prototype, sample, etc.) and making it available otherwise (a general clause introduced in order not to miss some form of revealing a trade secret that cannot be classified as disclosure or surrender, e.g. giving the key to a metal locker containing trade secret documents or giving a password for electronic access to a protected data).

The second (alternative) form of the offense exists when the perpetrator collects the trade secret data with the purpose of handing it over to unauthorised person. For example, person A asks his relative, person B, employed by CC, to collect market research data, which the company keeps as a trade secret. Person B did it unnoticed. The act could also be committed by a computer hacker, who would decipher electronic protection and get someone's trade secret, if they intends to hand over such data to an unauthorised person, i.e. if he does so with mentioned intention. (Almeling, 2012). This sort of breaching a trade secret is (in literature) sometimes also called betrayal of a trade secret. It is interesting that the name of this criminal act in the former Criminal Code of SR Serbia was “betrayal and obtaining a trade secret”, on which this interpretation is based. (Sržentić et al., 1986: 459). It should be borne in mind that the second alternative action is, by its legal nature, a preparatory action, which is elevated to the level of the act of execution by the will of the legislator. It is not necessary for the perpetrator to actually hand over trade secret data to an uninvited person. The offense is completed when he collected the data with the appropriate intention. The fact that data was actually handed over is considered aggravating circumstances.

The perpetrator of the offense is one who is authorised to keep the data or the document in control. He is considered to be in control of the document/data even if he doesn't have the mandate to be acquainted with the content of the document. It is enough for him to be authorised to control the access to documents. These are persons to whom a trade secret has been entrusted in some way, but without the authority to disclose it to other, uninvited persons. First, these are people who know the content of a trade secret (e.g. one of the technologists or engineers in the company, who participates in the preparation of the recipe or conducting the study). Then, persons who do not know the content of the trade secret, but are entrusted with a document containing the data.

A document is a data carrier (e.g. paper, electronic file, external memory, disk, etc.). (Mandić, Putnik, Milošević, 2017: 303). For example, the document is entrusted to a courier or archivist. Finally, the perpetrators may also be persons authorized to indirectly keep documents that contain trade secrets - e.g. those who secure the room or other enclosed space in which it is located. So, the perpetrator is the person who is in legal control of the information/document or in the legal control of access to it. This conclusion stands without dispute for the first form of actus reus (disclosure of trade secret). But in the case of the alternative form of offense action (acquiring data with the purpose of handing it over to an uninvited person) one can argue that even an unauthorised person, who accidentally has the opportunity to access the data/document, can be the perpetrator of the offense. Following that reasoning, we can conclude the perpetrator is the person who controls (or can achieve control of) the data/document in fact, legally or illegally. In other words, this form of offense can be performed by person that abuses the factual circumstances in order to illegally obtain data and then hands it over to another uninvited person; and also by the authorised person who exceeds or misuse their authority with intent to collect and hand over data to unauthorised person. This could be performed in the manner of social engineering. (Mandić, Putnik, Milošević, 2017a). The circle of potential perpetrators, if we accept this interpretation, would be significantly wider than in the case of the first alternative action.

However, this conclusion is not on solid ground, due to the fact that the legislator did not explicitly state the first alternative action is performed exclusively by an authorized person who reveals data in



excess of the authorization, while the second action is performed by authorised or uninvited person. Moreover, the legal title of the offense (disclosure of trade secret) and the formulation of the provision implied that the perpetrator is exclusively the person in legal control of access to data. Court practice (which is poor) supports this view. In the case of banking secret breach, the court states: „the defendant unauthorizedly submitted data representing the banking secret to R.Đ. and an excerpt on the balance on four accounts kept in the name of V.J. - number ..., whose owner is appointed VJ, account number ..., technical account for functional operations of Branch P, account number ..., technical account for functional operations of Branch K. and account number ..., technical account for the functional business of Branch V, which R.Đ. announced in the television show “T.” on Television B. A.“ The defendant was a bank clerk, while the person that published the secret data in the TV show had no criminal charges. (Presuda Osnovnog suda u Nišu K 65/14, 2015).

However, this leads us to the next conclusion – only illegal disclosure of trade secrets is a criminal offense in our law, while unlawful acquisition of data by unauthorised person is not under the scope of Article 240 of Criminal Code. If someone, for example, uses instruments of social engineering to acquire trade secret data, his conduct could not be qualified as a criminal offense under this Article. Only breach of trust and duty by a person who has legal control of access to data was in the focus of our legislator. Unlawful acquisition of trade secret data was not characterised as socially dangerous behaviour, although, actually, it is clearly not less harmful than disclosure of data. The same conclusion stands for illegal use of trade secret data, since the unauthorised person cannot be the perpetrator of this offense.

According to that, if someone accidentally comes into possession of a trade secret data and then uses it without authorisation (e.g. found a folder with papers containing test results), his conduct is not under the scope of Criminal Law. Of course, the described act could be a violation of law (depending on the circumstances, civil, commercial or labour law sanctions could be imposed). One should also keep in mind the Article 3 of the Law/21, that allows third parties to acquire, use and reveal trade secrets in a legal way (id by independent discovery or creation). In this case, the conduct would be lawful. (Bone, 1998).

As for the liability of the unauthorised person who persuaded the perpetrator to perform an offense or aided him in it, according to the provisions of the general part of the Criminal Law, the same will be considered an accomplice. (Stojanović, 2018; Delić, 2021). On the other hand, if that person did not previously persuade the perpetrator to collect data or helped him, but only used the data that were disclosed, the issue of liability would be very complex, and there would probably be no place for imposing criminal, but possibly other legal sanctions.

SUBJECTIVE ELEMENTS OF THE OFFENSE (MENS REA)

Disclosure of a trade secret is always performed with intent. The intention is to acquaint the unauthorised person with the content of the trade secret. The fact that the legislator requires the determination of particular intention unequivocally means that the act can be committed only with direct intent. Although this intention has to be determined only in the case of second alternative offense action, the nature of this crime clearly leads to the conclusion that the perpetrator acts with direct intent in both cases. Qualified form of disclosing a trade secret exists if the perpetrator commits the act out of greed or if the disclosed data was particularly confidential. The legislature prescribed a sentence of two to ten years in prison and also a fine (cumulatively). Greed is an incentive to acquire illegal material gain.



It is not necessary that the gain was actually achieved. It is sufficient that the perpetrator disclosed the trade secret with the incentive to gain benefits (e.g. he was promised money or employment).

Particularly confidential data are those from which disclosure the holder of a trade secret could have significant damage. However, in order to conclude that some trade secret information was particularly confidential in relation to others, it is necessary for the holder to treat it with a higher degree of protection and to take stricter measures compared to one applied to protect other trade secret information. (Mandić, Putnik, Milošević, 2017: 303). In the previous Criminal Code of SR Serbia (Criminal Code of SR Serbia, 1977) one of the qualifying circumstances was the disclosure of a trade secret for the purpose of its use abroad. Judgments from earlier court practice are also cited in the literature: „the perpetrator systematically provided foreign companies with data on the needs of construction, expansion or reconstruction of some of our companies“, as well as: „the perpetrator informed a foreign company that one of our companies does not intend to procure a certain type of machine“. (Sržentić et al., 1986: 459, 460).

Although these verdicts are a consequence of a somewhat broader definition of trade secrets in the previous legislation, we consider it more adequate in comparison with the present solution. Today, Serbian legislator no longer incriminates disclosing a trade secret with an element of foreignness, but practically equates it with disclosing a secret in the domestic environment.

Industrial espionage can be an important factor of endangering the stability of economic systems. However, Serbian legislation lacks adequate criminal law protection from this phenomenon.

PRIVILEGED FORM OF OFFENSE

Disclosure of a trade secret is also criminalized when it was done out of negligence. The existence of a privileged form is of great importance, because it influences the prevention of crime through the strengthening of security culture. A negligent form will exist when, for example, one of the employees does not adhere to the prescribed company procedures and protection standards, lightly holding that the data will not fall into the hands of an uninvited person or that he will be able to prevent it, and because of this misconduct, trade secret data is disclosed by unauthorized person. The same will be the case when the perpetrator did not want or was not aware that their actions could lead to a violation of trade secrets, but they were obliged and could have foreseen that, based on his personal characteristics and circumstances. For example, when he leaves written down parameters for electronic access to data on his office desk (unprotected from “other people’s views”), not thinking that someone could notice and use them. A prison sentence for negligence form of offense is of up to three years of prison. It is not clear why legislator did not prescribe fines as an alternative sanction, considering the nature of this crime. Although the existence of a negligent form of disclosing a trade secret is a sign of the importance that the legislator attaches to its protection, the problem of delimiting the perpetrator’s liability under the Criminal Code and the Law on the Protection of Trade Secret arises here as well.



TRADE SECRET DISCLOSURE IN OTHER BRANCHES OF PENAL LAW

The breach of trade secret is sanctioned by provisions of Criminal, Commercial and Labour law. This paper aims to analyze criminal liability. However, the relation between criminal and liabilities stipulated in other laws is sometimes complex and challenging.

The relationship between civil and criminal liability is relatively less complex, as criminal and civil sanctions can be imposed in parallel. The Law on Trade Secret Protection introduces civil liability for the acts of trade secret illegal acquisition, use and disclosure, but also proclaims those acts to be misdemeanors and commercial offenses (the category of illegal conduct that was exclusively established in former Yugoslavia and still exists in Serbia). (Đorđević, 2013). The potential problem lies in the relation between criminal and other penal liability (misdemeanor and commercial offense).

The Article 21.1 of the Law on Trade Secret Protection (Law/21) introduced the commercial offense of unlawful acquisition, use or disclosure of trade secret data. The prescribed fine for a legal person is from 100.000 up to 3.000.000 Serbian dinars. The fine for the responsible person in the legal entity is envisaged in the amount of 50,000 to 200,000 Serbian dinars. If a natural person illegally obtains, uses or discovers a trade secret, the Article 21.4 qualifies that conduct as a misdemeanor and proscribes a fine from 20.000 up to 150.000 Serbian dinars. For the same misdemeanor, the entrepreneur can be convicted to fine from 50.000 up to 500.000 Serbian dinars. The previous Law also envisaged fines for breach of trade secrets.

The unlawful acquisition, use or disclosure of trade secret data is defined in Article 4 of the Law/21. The Article 4.1 defines unlawful acquisition: „unauthorized access, misappropriation or copying of documents, objects, materials, substances or electronic files that are under the legal control of the holder of a trade secret, and contain a trade secret, or a trade secret can be derived from them, or other conduct which, in the given circumstances, is considered to be contrary to good business practice“.

According to Article 4.2 of Law/21, use and disclosure is unlawful if: „the person (previously) obtained a trade secret illegally; violated the confidentiality agreement or other obligation related to the prohibition of disclosure of trade secrets; or violated a contractual or other obligation limiting the use of trade secrets“. Even negligence is legal ground for liability, because Article 4.3 of the Law/21, clearly states that acquisition, use and disclosure are illegal „if the person at the time of acquisition, use or disclosure knew or had to know in the given circumstances that the trade secret was obtained directly or indirectly from another person who illegally used or disclosed the trade secret“.

The same conclusion stands for „production, offering or placing on the market of infringing goods..“, as a form of illegal use of trade secrets. Those acts are also considered unlawful if „the person who performed the stated activities knew or in the given circumstances had to know that the trade secret was used illegally“ (Article 4.4).

CONCLUSION

The Role of Criminal Law in Trade Secret Protection is significant in contemporary market economy. Although Serbian Criminal Code envisaged the criminal offense of trade secret disclosure, long before Law on Trade Secret Protection was even adopted, there are certain shortcomings of the provision of Article 240. First of all, the act of acquiring a trade secret is not criminalized, although the level of its



social danger is relatively high. Second, trade secret disclosure with an element of foreignness is not envisaged as a separate offense (industrial espionage) or aggravated form of this offense.

Other downsides of Criminal Law protection of trade secrets in Serbia are the consequence of the systemic inconsistency of the relevant laws.

The Law on Trade Secret Protection qualifies trade secret disclosure (and also unlawful acquisition and use) as a misdemeanor or commercial offense (depending on the category of perpetrator – individual, entrepreneur or legal person). Thus, the same conduct can be qualified differently by those two laws - as a crime, misdemeanor or commercial offense. The constitutional right not to be tried or punished twice (the non bis in idem principle) is guaranteed and it prohibits double jeopardy. In accordance with that principle, a person cannot be trialed for the same conduct as a misdemeanor, commercial offense and criminal offense. Having in mind that three different type of courts (misdemeanor, commercial and courts of general jurisdiction - criminal departments) could have jurisdiction for misuse of trade secret (depending on which of the laws is reported to be breached), practical problems with implementation of legal norms are obvious and naturally arise from mentioned inconsistency of laws. Also, the fact that unlawful acquisition and use of trade secret data is a misdemeanor and not a criminal offense, while disclosure can be qualified as both, clearly demonstrates lack of consistent and rational legislative approach. This fact is particularly striking if one compares proscribed sanctions for misdemeanor and criminal offense.

The natural consequence of systemic inconsistency of the relevant laws is poor court practise. Legal framework is not solid and coherent enough. Apart from that, the criminal court cases in this matter are rare because Civil Law protection seems like a preferable option (although court practise is not developed here, either).

However, the responsibility is also on the holders of trade secrets, who do not take protective measures, and later cannot prove that the revealed information was a trade secret. (Mandić, Putnik, Milošević, 2017). Corporate security culture is underdeveloped, and legal entities usually fail to create and implement adequate internal regulation and provide legal, organisational, personal, technical and other reasonable measures to prevent trade secret breach and demonstrate, in an eventual court case, that they have performed all necessary steps for data protection.

REFERENCES

1. Almeling, D. (2012). „Seven reasons why trade secrets are increasingly important“.
2. *Berkeley Technology Law Journal*, Vol. 27, pp. 1091-1117.
3. Bone, R. (1998). „A New Look at Trade Secrets Law: Doctrine in Search of Justification“. *California Law Review*, Vol. 86, 2/1998, pp. 243-270.
4. Criminal Code of the Republic of Serbia, 2005 (Krivični zakonik Republike Srbije, „Sl. Glasnik RS“, br. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19)
5. Criminal Code of the SR Serbia, (Krivični zakon Republike Srbije, „Službeni glasnik SRS“, br. 26/77, 28/77, 43/77, 20/79, 24/84, 39/86, 51/87, 6/89 i 42/89, „Službenik glasnik RS“, br. 21/90, 16/90, 26/91, 75/91, 9/92, 49/92, 51/92, 23/93, 67/93, 47/94, 17/95, 44/98, 10/02, 11/02, 80/02, 39/03 i 67/03)
6. Deliće, N. (2021). *Krivično pravo – posebni deo*. Beograd: Pravni fakultet Univerziteta u Beogradu.



7. Đorđević, Đ. (2013). *Prekršajno pravo sa osnovama privrednoprestupnog prava*. Beograd: Kriminalističko-policijska akademija.
8. Hilton, E. (1990). What Sort of Improper Conduct Constitutes Misappropriation of a Trade Secret. *30 IDEA Journal of Law and Technology*.
9. Jamieson, K. „Just Deserts: A Model to Harmonize Trade Secret Injunctions“;
10. *Nebraska Law Review*, Vol. 72, 2/1993.
11. Jovičić, K. (2018). Poslovne tajne: određenje i osnovi zaštite. *Strani pravni život*, 62 (1), pp. 7 – 19.
12. Law on Protection of Trade Secret of the Republic of Serbia, 2011 (Zakon o zaštiti poslovne tajne, „Sl.glasnik RS“, broj 72/11)
13. Law on Protection of Trade Secret of the Republic of Serbia, 2021 (Zakon o zaštiti poslovne tajne, „Sl.glasnik RS“, broj 53/21)
14. Law on Companies of the Republic of Serbia, 2011 (Zakon o privrednim društvima, „Sl. Glasnik RS“, br. 36/11, 99/11, 83/14 - dr. zakon, 5/15, 44/18, 95/18, 91/19)
15. Mandić, G., Putnik, N., Milošević, M. (2017). *Zaštita podataka i socijalni inženjering – pravni, organizacioni i bezbednosni aspekti*. Beograd: Univerzitet u Beogradu-Fakultet bezbednosti.
16. Mandić, G., Putnik, N., Milošević, M. (2017a). Contemporary Deception Techniques: Social Engineering – Semantic, Phenomenological and Security Aspects. In: Bošković, M. (Ed.), *Security Risks: Assessment, Management and Current Challenges* (pp.111-127). New York: Nova Science Publisher, Inc.
17. Milošević, M., Mladenović, M. (2017). Upravljanje pravnim rizicima kao element korporativne bezbednosne politike. *Srpska politička misao*, broj 3/2017, god. 24., vol. 57., pp. 289-304.
18. Peterson, G. (1998). *Trade Secrets Protection in an Information Age*. Glasser Legal Works.
19. Presuda Osnovnog suda u Nišu K 65/14, od 23.04.2014. godine.
20. Srzentić, N., Stajić, A., Kraus, B., Lazarević, Lj., Đorđević, M. (1986). *Komentar krivičnih zakona SR Srbije, SAP Kosova i SAP Vojvodine*. Beograd: Savremena administracija.
21. Stojanović, Z. (2018). *Komentar Krivičnog zakonika*. Beograd: Službeni glasnik.
22. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), World Trade Organisation, 1994.
23. Available at: https://www.zis.gov.rs/upload/documents/pdf_sr/pdf/trips.pdf (last retrieved: 30.06.2021).
24. The 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. (Official Journal of the European Union, L 157/1; available at: <https://eur-lex.europa.eu/eli/dir/2016/943/oj>; last retrieved: 25. 08. 2021).
25. Wingo, H. (1997). Dumpster Diving and the Ethical Blindspot of Trade Secret Law. *Yale Law & Policy Review*, Vol. 16 (195), pp. 195-219.

