CLASSIFIED DATA AND CRIMINAL LAW – A NEED FOR CERTAIN CHANGES?

Jovana Banović, PhD[1]
Faculty of Security Studies, University of Belgrade, Serbia

INTRODUCTION

There are many "secrets" in the "normative sea", such as state secrets, trade secrets, official secrets, or military secrets. All of these are recognized by various laws in Serbia, which prescribe not only the basic rules but also the consequences of breaching these legal norms. Given that the primary aim of this article is to analyse the legal frameworks related to data secrecy within the context of Criminal Law, the focus will be on specific provisions of the Data Secrecy Law (DSL, Official Gazette RS, 104/2009) and the Criminal Code of Serbia (CC, Official Gazette RS, 5/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, and 35/2019). Additionally, the Law on Protection of Trade Secrets (LPT, Official Gazette RS, 53/21) and the Law on Personal Data Protection (LPDP, Official Gazette RS, 87/2018) are also part of the aforementioned legal framework, although they will not be subject to further analysis. This normative basis is particularly important for determining what constitutes a secret as an object of criminal law protection (more: Bodrožić & Milošević, 2022: 95-97).

The formal and substantial similarity between Article 98 of the DSL, which addresses the disclosure of classified data, and Article 316 of the CC, which pertains to the disclosure of state secrets, contributes to the consistency of the Serbian legal system and warrants further analysis. Part of the research will include several additional offenses related to data protection, specifically their particularities, as prescribed by the CC.

There are at least two reasons for choosing this topic. The first, more general reason is to highlight the importance of protecting data, especially classified information that is vital to national security, public safety, defense, and both internal and foreign affairs of the Republic of Serbia. The second reason is to expose certain inconsistencies within the domestic legal system, which have led to the existence of two regimes for classified data protection: one before 2009, and another after the DSL came into force.

DESIGN/METHODS/APPROACH

The research paper comprises an introduction, three distinct chapters, and a conclusion. The first section of the article will provide a brief overview of the normative framework, encompassing relevant provisions of the DSL, CC, and relevant bylaws. Following this, in the second chapter, the analysis will focus on two specific offenses: Article 98 of the DSL, which deals with disclosing classified data and Article 316 of the CC, which pertains to disclosing state secrets. Particularly, attention will be paid to aggravated forms of the offense outlined in Article 316 of the CC, which deals with grave offenses against the constitutional order and security of Serbia. Additionally, a concise examination will be conducted on selected aspects of the following offenses: Disclosure of an Official Secret (Article 369 of the CC), Disclosure of a Military Secret (Article 415 of the CC), Unauthorized Disclosure of Secrets

1 jovana.banovic@fb.bg.ac.rs

(Article 141 of the CC), and Violation of Confidentiality of Proceedings (Article 337 of the CC). In the third section of the article, considerations regarding potential legal changes to existing provisions of the DSL and CC will be addressed.

The methodology employed primarily involves content analysis, complemented by the dogmatic method and a conceptual approach, aimed at achieving the primary objectives of the research. Additionally, since this article is based on legal provisions, a normative analysis has been conducted to assess the current state of classified data in primary and secondary criminal legislation, while addressing the challenges posed by contemporary issues and potential future amendments.

SUMMARY OVERVIEW OF THE NORMATIVE FRAMEWORK FOR CLASSIFIED DATA

Primarily, the field of classified data is governed by the Data Secrecy Law. There are several other legal texts that address this matter. In addition to the aforementioned law, our paper focuses on the Criminal Code of Serbia. The main reason for this approach is the criminal law perspective from which we aim to analyse classified data, particularly the sections concerning prescribed offenses in these two laws. It is important to note that the Data Secrecy Law is supplemented by 16 bylaws (Milosavljević, 2016:7). The legal nature of these bylaws is predominantly regulatory. Examples include: the Regulation on Specific Criteria for Determining the Level of Secrecy as "Top Secret" and "Secret"; the Regulation on Specific Criteria for Determining the Level of Secrecy as "Confidential" and "Restricted" within the Security Information Agency, as well as within the Office of the National Security Council and Classified Information Protection; Regulation on Special Measures for the Protection of Classified Information in Information and Telecommunication Systems, among others.

The main subject of the Data Secrecy Law (DSL) is to establish a unified system for the classification and protection of secret data that is of interest to national security, public safety, defense, internal and foreign affairs of the Republic of Serbia, and the protection of foreign classified data. It also regulates access to classified data and their declassification, the competencies of relevant authorities, the oversight of the implementation of law, accountability for non-compliance with its obligations, and other matters important for the protection of data secrecy (Article 1). From our perspective, Article 98 of the DSL is of central importance. It defines the criminal offense of unauthorized disclosure, transfer, or making accessible data or documents that have been entrusted, obtained by other means, or the acquisition of data or documents that are classified as secret, marked with the appropriate level of confidentiality. On the other hand, the Criminal Code (CC) includes Article 316, which addresses the disclosure of state secrets. Particular attention will be paid to the aggravated forms of the offense outlined in Article 316 of the CC, which pertain to serious offenses against the constitutional order and security of Serbia. As previously mentioned, an examination will also be conducted on certain aspects of the following offenses: Disclosure of an Official Secret (Article 369 of the CC), Disclosure of a Military Secret (Article 415 of the CC), Unauthorized Disclosure of Secrets (Article 141 of the CC), and Violation of Confidentiality of Proceedings (Article 337 of the CC).

The DSL is a fundamental law that clarifies the substantive aspects of classified data protection, as well as the basic elements of the aforementioned crimes. However, The CC provides its own definitions for similar offenses, which, whether intentionally or not, ultimately largely align with each other. The DSL is a crucial normative part of data secrecy protection because it establishes the "core" rules for determining what is lawful and, conversely, what is not. It is also an important legal act for the control and classification of data of a certain, "special" form. It is worth emphasizing that, in the realm of informa-

tion protection in cyberspace, international standards, such as the ISO/IEC 2700 series, play a significant role. The international dimension is important not only for cooperation and global security but also for alignment with European legal standards and for addressing new challenges in emerging technologies such as digital assets (Kovačević & Milošević, 2022: 95; Radisavljević, 2023; Banović, 2023a).

DSL provides definitions for certain basic terms. It categorises data into three types: Data of Interest for the Republic of Serbia, Classified Data, and Foreign Classified Data. Article 1 of the DSL establishes the legal meanings of these definitions. Firstly, Data of Interest for the Republic of Serbia refer to "any data or documents in the possession of a public authority that relate to territorial integrity and sovereignty, protection of the constitutional order, human and minority rights and freedoms, national security and public safety, defense, internal affairs, and foreign affairs". Secondly, Classified Data mean "any data of interest for the Republic of Serbia that have been classified and assigned a level of secrecy by law, other regulations, or decisions of a competent authority made under the law". Finally, Foreign Classified Data mean "any data provided to the Republic of Serbia by another country or an international organization, with the commitment that the Republic of Serbia will maintain them as classified; as well as classified data resulting from cooperation between the Republic of Serbia and other countries, international organisations, or other international entities under an international agreement concluded by the Republic of Serbia". Given the topic of the Article and the definitions provided, classified data represent a "vital" category of data that will be the focus of our analysis.

On the other hand, the CC entirely serves as a supporting source in this context, coming into force in cases of the most serious infringements of classified data. This is why we combine these two laws concerning the criminal law aspects. As previously mentioned, the offense of disclosing state secrets and its aggravated forms are a complementary part of the protection of classified data. Essentially, the main difference lies in the formal terminology: the CC addresses state secrets (or military or official secrets), while the DSL concerns classified data that have been designated with a level of secrecy, such as "top secret", "secret", "confidential", or "restricted".

It is clear that our legal system establishes two regimes for the protection of classified data: one before and one after 2009, when the DSL came into force. Unlike the Criminal Code, which defines offenses and the concept of secrets for its purposes, the Data Secrecy Law not only prescribes the offense of "misuse" of classified data but also outlines an entire system for its protection. This includes the purpose, storage, and use of collected data, data classification procedures, authorised personnel, licensing, marking, declassification, protective measures, access to different types of classified data, control and oversight, statutory norms for the Council Office, and more. This is not an unusual legal practice, as modern systems tend to replace the term "state secret" with "classified data" (Donna, 2002: 401; Gál, 2022: 587).

From an organisational perspective, a Higher Court has jurisdiction over the two crimes that form the "core" of this paper – Article 98 of the Data Secrecy Law and Article 316 of the Criminal Code (Article 25, paragraph 1, item 2 of the Law on Regulation of Courts – LRC).

CRIMINAL OFFENSES INVOLVING CLASSIFIED DATA

Article 98 of DSL

This criminal offense from the DSL is referred to descriptively in this paper, as it lacks a specific legal designation. In a sense, this is a distinctive technique characteristic of secondary legislation. The offense includes a basic form, three aggravated forms, and a privileged form.

First, the offense under Article 98 of the DSL can be committed in three alternative ways: (1) when an authorised person, meaning anyone in lawful possession of the data or the document containing the data, makes the data or document available to an unauthorised person; (2) if an unauthorised person, who has unlawfully obtained possession of the secret, transfers the secret to a third unauthorised person; or (3) when an unauthorised person unlawfully acquires data or documents containing secret information (Milošević, 2022: 202). In other words, the criminal offense can be committed by anyone who has access to confidential data or documents, whether the data have been entrusted to them or they have obtained it in another way, and then discloses or transfers that data or those documents to an unauthorised person. The basic and aggravated forms of the offense differ in terms of the classification of secret data. The basic form involves committing the crime with respect to data marked as "restricted" or "confidential", as established by the DSL. For this form, the prescribed penalty is imprisonment for a term of three months to three years. The first aggravated form pertains to data marked as "secret", (prescribed sentence is prison term of six months to five years) while the second involves data marked as "top secret" (with prescribed sentence of imprisonment for a term of one to ten years. The third aggravated form is prescribed as an alternative act of commission and applies to all three of the previous forms, with specific penalties. The qualifying circumstances for this form include: intent for personal gain, the intention to "release or use secret data abroad", or committing the offense during a state of war or emergency (Milošević, 2022: 202). The offender shall be sentenced to prison term of six months to five years for the offense from paragraph 1 of the Article 98, one to eight years for the offense from paragraph 2, and five to fifteen years for the offense from paragraph 3. The privileged form depends on a subjective element and requires negligence as the relevant degree of guilt. Prescribing negligent criminal offenses is common in the field of data protection, especially considering the importance of strengthening security culture in this area (Banović, 2022: 149). For this form, the perpetrator shall be sentenced to imprisonment up to two years for the offense from paragraph 1 of the Article 98, three months to three years for the offense from paragraph 2, and six months to five years for the offense from paragraph 3.

It is important to note that the object of the action – classified data with a specific level of secrecy – is determined under Article 14 of the DSL[2], in conjunction with relevant bylaws issued by the Government. Legally speaking, this pertains to blanket disposition of criminal offenses. In addition to the DSL, which is part of secondary criminal legislation, bylaws can provide further interpretation of the objective elements of these crimes. While this approach to traditional criminal law is not typical, it illustrates how bylaws can function as specific sources of criminal law, although this may present challenges concerning the principle of legality (Vuković, 2021: 8). The situation becomes more complicated when considering Articles 10 and 11 of the DSL, which prescribe the procedures for data classification and the enactment of decisions on determining classification levels. Among other things, these procedures require an assessment of the potential damage to the interests of the Republic of Serbia. However, despite the DSL and relevant bylaws defining the types of classified data, there remains the possibility of a mistake of law, especially in relation to Article 105 of the DSL (for instance, a mistake of law can be applied to situations where the offender does not know that the information or document represents classified data with a relevant level of classification or believes that its disclosure is not prohibited (Donna, 2002: 405)). This article stipulates that data and documents classified under earlier regulations will retain their classification level and type. Furthermore, the heads of public authorities were required to review the classification markings of these data and documents within two years of the Law entry into

2 1) "TOP SECRET", which is designated to prevent the occurrence of non-avoidable severe damage to the interests of the Republic of Serbia; 2) "SECRET", which is designated to prevent the occurrence of serious damage to the interests of the Republic of Serbia; 3) "CONFIDENTIAL", which is designated to prevent the occurrence of damage to the interests of the Republic of Serbia; 4) "RESTRICTED", which is designated to prevent the occurrence of damage to the operations or tasks of the public authority that designated it.

force, as stipulated by the DSL. Even though this term has passed, it still seems reasonable to assert that the legislator's intention to review all previously established security classifications may have been difficult to implement in practice due to the sheer volume and number of classified data and documents (Kovačević & Milošević, 2022: 102). Additionally, this is one of the reasons for further analysing the next offense, as the factual situation creates two regimes of classified data.

The lack of statistical data on the incidence of this offense prevents us from getting a complete picture of its representation in practice, as these data are aggregated with other criminal offenses from special laws (secondary legislation). For illustration purposes, in the rare verdicts we have found, this offense is committed when "the offender unlawfully made available to a third party a document or data that were entrusted to him by his superior, specifically a list of individuals titled 'Supervision and Control of Individuals – ...,' prepared by the Police Administration…, which contains data from the information system of the Ministry of Internal Affairs of the Republic of Serbia. According to Article 6, item 47 of the Mandatory Instructions on Rules and Procedures for Using the Information System of the Ministry of Internal Affairs of the Republic of Serbia, all data contained in the mentioned information system, which fall under the jurisdiction of the state and the ministry, are classified as 'confidential'" (Judgment of the Supreme Court of Cassation of Serbia, KZZ 1120/2019, 17.12.2019).

Article 316 of CC – Disclosing a State Secret

This offense involves a specific object of action: a state secret. The group object of protection is the constitutional order and security of Serbia. The Criminal Code (CC) defines a state secret from both a formal and substantive perspective. In addition to defining what constitutes a state secret, the CC also clarifies what does not qualify as one. According to Article 316, paragraph 5 of the CC, a state secret includes information or documents that are declared as such by law, other regulations, or a decision of a competent authority pursuant to the law (formal aspect), and whose disclosure would or could harm the security, defense, or political, military, or economic interests of Serbia (substantive aspect). Conversely, a state secret does not include information or documents that involve a serious violation of fundamental human rights, undermine the constitutional order and security of Serbia, or are intended to conceal a criminal offense punishable by imprisonment of five or more years. The last one is a situation where something that cannot be classified as a secret becomes a secret. Theoretically, this can be defined as an "illegal secret" (Stojanović, 2012: 851). A similar provision is found in the DSL, specifically in Article 3: data marked as classified for the purpose of concealing a crime, exceeding authority, abusing office, or hiding any other illegal act or proceedings by a public authority shall not be considered classified. Considering the relationship between the definitions of classified data under the Data Secrecy Law and state secrets in the Criminal Code, we can conclude that, in matters of secrecy, the CC employs both formal and material criteria. In contrast, the definition of classified data in the Data Secrecy Law is primarily formal, with an indirect reference to the material element through the specification of different levels of secrecy. However, we should keep in mind that, on the one hand, the DSL came into force after the Criminal Code, and its main purpose was to unify the regulations concerning classified data. On the other hand, the content of Article 316 of the Criminal Code has not been amended since 2009 (even then, the legislator only increased the minimum penalty in Article 316, paragraph 2 of the Criminal Code[3]).

It is correctly observed that the formal process of classification is significant, especially considering historical examples where the substantive element has predominated (Gál, 2022: 593). A substantive approach simplifies the initiation of criminal proceedings but can conflict with the values of legal

3 The 2009 amendments were characterised by a trend of increasing criminal law repression (Bodrožić, 2020: 386).

certainty and predictability, which are essential components of justice. However, the fact that the definition in the Criminal Code includes both elements aligns this area with the concept of *ultima ratio*, as it restricts criminal law protection to only the most serious acts.

Unlike espionage, this offense is "situated" in a "domestic environment", meaning it does not involve any foreign elements (Delić, 2021: 334-340; Milošević, 2022: 203). In some legal systems, there was a distinction between a breach of confidentiality and the disclosure of a secret, which led to a lack of clear differentiation between disclosing a state secret and committing espionage. Both criminal offenses were part of a single one. Later, this ambiguity led to certain reforms in this field (Creus, 1998a: 163-165; Donna, 2002: 405).[4]

Article 316 of the Criminal Code includes a basic form, two privileged forms, and an aggravated form. Article 321 of the Criminal Code – Grave Offenses against the Constitutional Order and Security of Serbia – also references the criminal offense of disclosing a state secret by introducing an additional aggravated form in paragraph 3. We will explore why this presents an issue in the continuation of the paper.

According to Article 316, paragraph 1 of the Criminal Code, this offense can be committed by anyone who, without authorisation, discloses, hands over, or makes available to another person information or documents that are entrusted to them or that they have otherwise acquired and that constitute a state secret. The prescribed sentence is imprisonment for one to ten years. Unlike the basic form, where the perpetrator has authorisation to possess classified data but unlawfully makes it available to a third person, the first privileged form can be committed by anyone who discloses to another person information or documents they know to be a state secret and which they have unlawfully acquired[5]. In this case, the offender shall be punished by imprisonment extending from six months to five years. The

4 This issue may also be relevant under Serbian law, particularly regarding the distinction between aggravated forms of criminal offenses involving the disclosure of classified data or secrets, as defined in the perpetration acts prescribed by Article 98, paragraph 4 of the DSL, Article 369, paragraph 2 of the CC (disclosure of official secrets), and Article 415, paragraph 2 of the CC (disclosure of military secrets). Considering that these criminal offenses are committed "for the purpose of publishing or using abroad", which serves as a qualifying circumstance, a question may arise regarding the distinction between these offenses and the criminal offense of espionage under Article 315, Paragraph 1 of the CC (where the offense is completed by disclosing, handing over, or making available military secrets, economic or official information, or documents to a foreign state, foreign organisation, or person in their service), and particularly the specific form under Article 315, paragraph 4 of the CC (which is committed by anyone who obtains secret information or documents with the intent to disclose or hand them over to a foreign country, foreign organisation, or person serving them), and these forms, given that the type of information (the object of the action) may coincide. This is notably relevant because, in aggravated forms of the aforementioned criminal offenses, the essence lies in preparatory acts raised to the level of perpetration acts. In contrast, in the case of espionage, such actions are otherwise punishable under Article 320, paragraph 1 of the CC (Preparation for Offenses Against the Constitutional Order and Security of Serbia), while in the specific form of espionage under Article 315, paragraph 4, a preparation act is inherently involved (Milošević, 2022: 206-207). However, the main difference is that espionage implies a more direct connection with a foreign country and a stronger foreign element, while the aggravated forms of the mentioned criminal offenses are committed "within the country" and involve a more indirect level of connection with foreign entities. This is reflected both through the use of the broader term "abroad" instead of "foreign country" and the specific aim of disclosure that does not need to be achieved for the offense to exist (although this argument does not apply to the specific form of espionage). The group protective object in the context of teleological interpretation should also not be overlooked. Additionally, in these aggravated forms, the legislator uses the preposition "for (the purpose of)", which is not always unambiguous, as it sometimes equates to intent and sometimes to motive (Delić, 2016: 107). However, this is certainly a subjective element. Due to the difficulties that generally accompany proving subjective elements, and to overcome potential problems that could lead to impunity for certain borderline behaviours that could also seriously endanger the security of the country, such a normative solution – despite certain overlaps and the need for a more detailed analysis – is more comprehensive. This is particularly due to the "dual secrecy regime" established after the adoption of the Data Secrecy Law. Finally, the legal qualification of such behaviours based on this "foreign" element would depend on the circumstances of the specific case, which would enable a more nuanced response to these theoretical dilemma.

5 For example, unlike this provision, with regard to the elements of the crime, the offense of Disclosing a Trade Secret under Article 240 of the Criminal Code does not clearly distinguish between an authorised and an unauthorised person who discloses information (see: Milošević, 2022: 130-132; Banović, 2023b: 266).

primary reason for the difference in the prescribed sentences is that the perpetrator of the basic form has an obligation to maintain a state secret and violates this duty by committing the crime, whereas the offender in the privileged form unlawfully obtained the information or documents (Stojanović, 2012: 850). The secondary difference is noteworthy. Specifically, in terms of the perpetrating act, the basic form of the crime can be committed in various ways: by disclosing, handing over, or making information or documents that constitute a state secret available to another person (paragraph 1), while the first privileged form (paragraph 2) can be committed only by disclosing a state secret (for example: whether orally, in writing, or electronically…). This form of incrimination is more narrowly defined. The consequence is a concrete danger (similar: Donna, 2002: 405). It is interesting to mention that, in some legal systems, a criminal offense exists even when a secret is merely obtained unlawfully, without the requirement that it be disclosed (Donna, 2002: 401). This topic could arise in future discussions about potential amendments (Milošević, 2022: 204).

The second privileged form applies if the basic form of the offense is committed negligently. The prescribed sentence for this form is imprisonment extending from six months to five years. In the context of negligent crimes, it is important to emphasise that the duty of care or confidentiality imposed on the offender, along with the knowledge of the information by an unauthorised person, should be related to causality (Donna, 2002: 410-411).

The qualifying circumstances are prescribed under Article 316 paragraph 3 of CC. It represents either the timing – if the offense is committed during state of war or state of emergency, or the consequence – if it endangers the security, economic, or military power of Serbia. The prescribed penalty is imprisonment for a term of three to fifteen years. This provision would not be disputable by itself if it were not for Article 321, paragraph 3 of the Criminal Code (Grave Offenses against the Constitutional Order and Security of Serbia). Specifically, it prescribes that the penalty specified in paragraph 2 of this Article – which is imprisonment for a minimum of ten years or life imprisonment – shall be imposed on anyone who commits a criminal offense specified in Articles 307, 309 through 311, Articles 314 through 319, and Article 320, paragraph 2 during a state of war, armed conflict, or state of emergency. Since the offense of Disclosing a State Secret is included in this incrimination, it leads to the conclusion that there are two penalty ranges if this offense is committed during a state of war or state of emergency: imprisonment extending from three to fifteen years under Article 316, paragraph 3, and imprisonment for a minimum of ten years or life imprisonment under Article 321, paragraph 3. Additionally, considering the incrimination under Article 98, paragraph 4 of the DSL, which relates to classified data with the level "top secret" (equivalent to state secret under the Criminal Code), there is an additional penalty range: imprisonment extending from five to fifteen years related to the same qualifying circumstances. For example, the Criminal Code does not employ the same approach when prescribing penalties for criminal offenses committed during a state of war, armed conflict, or state of emergency (Article 417) concerning the offense of disclosing a military secret. It is clear that these inconsistencies regarding essentially the same offenses should be amended in the future (same: Milošević, 2022: 204; Bodrožić & Milošević, 2022: 109). Legal uncertainty is undesirable, although it is noteworthy that, according to data from the Statistical Office of the Republic of Serbia, this criminal offense is statistically infrequent.

Other 'Secrets' under the Criminal Code: Official and Military Secrets

Criminal law protection in Serbia, in addition to state secrets, also includes official secrets, military secrets, and trade secrets (Bodrožić & Milošević, 2022: 100-102). Unlike certain legal frameworks, the Serbian legislator clearly defines the group object that is protected by these types of secrets. For

example, in some legal systems, the disclosure of an official secret is categorised under criminal offenses against the freedoms and rights of individuals, with a broad explanation that personal data can constitute an official secret as well. While this may be accurate, it is not sufficiently precise. It is also important to distinguish between these types of secrets for the purpose of the joinder of offenses, as they represent distinct crimes (Creus, 1998b: 370-371).

Each of the aforementioned types of secrets protects different objects: an official secret protects official duties; a military secret protects the interests of the Serbian Army; and a trade secret safeguards economic interests. Our focus will not be on trade secrets, as they pertain to corporate security, whereas this paper emphasises national security.

Disclosing an official secret, as well as disclosing a military secret, follows the same concept as the previous offenses. These offenses provide definitions of these secrets in both positive and negative terms.

According to Article 369, paragraphs 4 and 5 of the Criminal Code, an official secret is defined as information or documents declared by law, another regulation, or a decision of the competent authority issued pursuant to law, and whose disclosure would or could cause damage to the service. Furthermore, data or documents that aim at a serious violation of fundamental human rights, endangering the constitutional order and security of Serbia, or concealing a criminal offense punishable by imprisonment of five years or more, shall not be deemed an official secret under this definition. This offense has a basic form with prescribed sanction extending from six months to five years of imprisonment (an official who, without authorisation, communicates, conveys, or otherwise makes available information constituting an official secret or obtains such information with the intent to convey it to an unauthorised person), an aggravated form, with prescribed imprisonment extending from one to eight years (if it is committed for gain, involves particularly confidential information, or is intended for publication or use abroad), and a privileged form, that shall be punished by imprisonment up to three years (if the basic form is committed negligently).

Furthermore, Article 415, paragraphs 4 and 5 of the Criminal Code define what constitutes a ”legal” and “illegal” military secret. A military secret is information declared as such by law, other regulations, or a decision of a competent authority made in accordance with the law, whose disclosure would or could cause harm to the Army of Serbia or to the defense and security of the country. Additionally, information or documents aimed at the serious violation of fundamental human rights or compromising the constitutional order and security of Serbia, as well as information and documents intended to conceal a committed criminal offense punishable by imprisonment of five years or more, shall not be deemed a military secret. The offense under Article 415 is divided into basic, aggravated, and privileged forms. Similar to the offense of disclosing a state secret, an additional aggravated form exists if the crime is committed during a state of war, armed conflict, or state of emergency. The basic form is committed when anyone, without authorisation, communicates, hands over, or otherwise makes available information that constitutes a military secret, or when someone obtains such information with the intent to hand it over to an unauthorised person. An imprisonment term extending from six months to five years may be imposed for this form. The aggravated form occurs when the offense is committed for any of the three alternatively prescribed qualifying circumstances: for gain, involving particularly confidential information, or for publishing or using such information abroad. The prescribed sentence for the aggravated form is imprisonment extending from one to eight years. A privileged form exists when the basic offense is committed negligently, and a negligent offender may be punished by imprisonment of up to three years. If the basic or privileged forms are committed during specific times (such as a state of war, armed conflict, or state of emergency), a prison sentence extending from two to ten years may be imposed (Article 417 paragraph 1 of the CC). For the aggravated form, the sentence may range from three to fifteen years (Article 417 paragraph 2 of the CC).

Unlike the offenses of disclosing a state secret, disclosing a military secret, and the offense under Article 98 of the DSL, the perpetrator of criminal offense disclosing an official secret cannot be just anyone; it must be an official person or additionally, according to Article 369, paragraph 6 of the Criminal Code, a "specific" official – one who has disclosed an official secret after their official position has ceased.

As we can see, the prescribed penalties are consistent and become more severe in cases involving the most serious threats to protected interests. It is noteworthy that the penalty ranges are quite broad, giving judges considerable discretion in determining sentences. This means that the "human factor", both from professionals and laypersons, is also important in the application of these provisions and in strengthening the culture of data protection in the area of national security.

(Additional) Secrets and Confidentiality under the Criminal Code

There are two specific crimes involving certain types of secrets that are noteworthy for a brief mention: Unauthorised Disclosure of Secrets (Article 141 of the CC), which protects rights and freedoms of man and citizen, and Violation of Confidentiality of Proceedings (Article 337 of the CC) which protects the judiciary.

The criminal offense under Article 141 of the CC can be committed by a lawyer, physician, or any other person who, without authorization, discloses a secret that came to their knowledge during the performance of their professional duties. This offense may be punishable by a fine or imprisonment of up to one year. Paragraph 2 of the same article provides a special ground for excluding criminal liability: anyone who discloses a secret in the public interest or in the interest of another person, where such interest outweighs the interest in maintaining the confidentiality of the secret, shall not be punished for the offense. Since the rights and freedoms of individuals represent a group protective object, the purpose of this incrimination is to protect the "owner of the secret" from unauthorised disclosure (Creus, 1998b: 364). This type of secret is specific to certain professions, which is why it is referred to as a professional secret. Perpetrators may include individuals who, due to the nature of their work, have the opportunity to learn personal secrets of others and then disclose them. These professions include clerics, pharmacists, midwives, nurses, and trainee lawyers, as they may come into possession of personal secrets of the people they interact with during the performance of their duties (Bodrožić & Milošević, 2022: 99). With regard to this offense, in addition to the Criminal Code, bylaws serve as a legal source for better understanding and clarifying the elements of the crime, especially since unlawfulness is a mandatory element. For example, relevant codes include the Code of Medical Ethics of the Medical Chamber of Serbia (Official Gazette of the Republic of Serbia, 104/2016) and the Code of Professional Ethics of Lawyers (Official Gazette of the Republic of Serbia, 27/2012 and 159/2020 – decision by the Constitutional Court). Prosecution for this offense is initiated by a motion from the injured party, which must be submitted to the competent public prosecutor. The provisions, including lower penalties, special grounds for exclusion of liability, and specific rules for criminal prosecution, suggest a lower level of social danger associated with this crime and a preference for addressing such infringements primarily through less severe mechanisms of law.

The offense of Violation of Confidentiality of Proceedings under Article 337 of the Criminal Code protects the unimpeded functioning of the judiciary. This offense includes a basic form and three aggravated forms. The basic form can be committed by anyone who, without authorisation, discloses information learned in a court, misdemeanour, administrative, or other procedure established by law, where the law stipulates that such information must not be publicised or has been declared secret by a decision of the court or another relevant body. The offender may be punished by a fine or impris-

onment of up to one year. The first aggravated form can be committed in four alternative ways: by anyone who without a court decision discloses the course of a criminal proceeding in which the public has been excluded, reveals a decision made in a criminal proceeding against a minor, discloses the name of the minor involved in the proceeding, or shares information that could reveal the identity of the minor. The prescribed sentence is imprisonment of up to two years. The second aggravated form occurs when the perpetrator, without authorisation, discloses information regarding the identity or personal data of a person protected in criminal proceedings or data concerning a special protection program. The punishment for this is imprisonment extending from six months to five years. The third aggravated form is related to the previous one. If this offense results in serious consequences for the protected person or significantly prevents or hinders the criminal proceedings, the offender shall be punished by imprisonment extending from one to eight years.

In 2009, certain changes were made to this incrimination. The sentences for the aggravated forms were increased, and paragraph 2 of Article 337 was slightly redefined. Before these amendments, it constituted a specific form with the same prescribed penalty as the basic form. Additionally, a new act was incriminated, referring to the disclosure of the course of a criminal proceeding from which the public has been excluded.

This criminal offense applies when information obtained during a procedure is disclosed, despite being declared secret based on relevant laws (such as Data Secrecy Law or Criminal Procedure Code – CPC, Official Gazette RS, 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - decision by the Constitutional Court and 62/2021 - decision by the Constitutional Court). Given that information from criminal proceedings represents one of the most "sensitive" types of data and encompasses the most important values protected by criminal law, it is important to consider some theoretical and practical implications of classified data in criminal procedure. Especially, in the context of "state secret doctrine" that deals with considering the justification for classifying certain information as secret, with the explanation of protecting a prevailing interest. In other words, it represents the relationship between constitutionally guaranteed rights and security interests. An illustrative example of "overprotection of data" is the frequent declaration of secrets under the pretext of protection against terrorism following the September 11, 2001 terrorist attacks in the United States (Cassman, 2015: 1215-1217). Furthermore, "the state secrets privilege" is a judicial doctrine where the court assesses various interests in determining whether the information should or should not be disclosed (Raguan, 2014: 122). Under this doctrine, invoking a state secret is used to prevent judicial oversight. A well-known case is American Civil Liberties vs. NSA regarding the violation of the Fourth Amendment of the U.S. Constitution, which protects citizens from unreasonable searches and seizures. After the first instance court found a violation of this amendment and determined the surveillance to be unjustified, the appellate court ruled that the plaintiffs had not provided evidence that their communications were being monitored. The problem arose because, in response to their request, the NSA refused to provide this information, citing the state secrets doctrine (Cassman, 2015: 1213-1214). Considering that significant intrusions into citizens' privacy require judicial oversight, a similar "legal situation" occurred in Serbia before the amendments to the Law on the Security Information Agency – LSIA (particularly in Articles 13, 14, 15a-15g). In response to a request by a non-governmental organisation for the number of citizens wiretapped during 2005, the Security Information Agency essentially invoked what we have defined as the state secrets doctrine, stating that the disclosure could seriously harm an interest that outweighs the public's right to know (Application no. 48135/06, ECHR Strasbourg, Youth Initiative for Human Rights v. Serbia, 25/09/2013; Milosavljević, 2023: 362-365). After the amendments, the current legal solution is satisfactory. Nevertheless, this remains an important issue that requires special attention from both the legislator and those who apply these provisions, bearing in mind that there are many "hidden secrets" that do not surface in practice. We identified this issue based on com-

parative experiences documented in relevant sources, as well as from national context, particularly in relation to Article 105 of the DSL, which stipulates the need for reconsideration of existing classification markings (Kovačević & Milošević, 2022: 101-102; Donohue, 2010: 215-216).

FINDINGS/ORGINALITY/VALUE

Conclusion

The offense prescribed under Article 98 of the Data Secrecy Law, which addresses the disclosure of classified data, the criminal offense of Disclosing a State Secret under Article 316 of the Criminal Code, and the offenses under Articles 369 and 415 of the Criminal Code that protect official and military secrets respectively, along with the aggravated forms prescribed under Articles 321 and 417 of the Criminal Code, constitute a significant normative framework for safeguarding secrecy against the most severe breaches. However, these analyses reveal inconsistencies within the domestic legal system. This discrepancy is the most evident in the realm of prescribed sanctions, where different penalty ranges exist for substantially similar criminal offenses. Additionally, there are shortcomings in certain manners of perpetration. Broadly speaking, our legal system delineates two regimes of classified data protection: before and after 2009, when the Data Secrecy Law came into force.

The most significant legal inconsistency concerns the offense of Disclosing a State Secret, given that there are two penalty ranges if this offense is committed during the state of war or emergency: imprisonment extending from three to fifteen years under Article 316, paragraph 3, and imprisonment for a minimum of ten years or life imprisonment under Article 321, paragraph 3. Furthermore, under Article 98, paragraph 4 of the Data Secrecy Law (DSL), which pertains to classified data marked as "top secret" (equivalent to a state secret under the Criminal Code), there is yet another penalty range: imprisonment extending from five to fifteen years for the same qualifying circumstances. This discrepancy should be addressed in future amendments to the Criminal Code, as recognized in relevant legal doctrine. One possible solution could be to delete the aggravated form prescribed under Article 321, paragraph 3, aligning it with the structure of other offenses involving the disclosure of specific secrets (such as military or official secrets). For now, both provisions – Article 316 of the Criminal Code and Article 98 of the DSL – remain in force. Despite certain differences between the definitions of classified data under the Data Secrecy Law and state secrets under the Criminal Code, both of which are important for considering the object of the crime (with the former being predominantly formal, with an indirect reference to the material element through the specification of different levels of secrecy, and the latter employing both formal and material criteria), the primary reason for the parallel existence of substantively similar incriminations can be found in Article 105 of the DSL, as the process of reconsidering existing classification markings has not yet been completed.

Besides the aforementioned offenses, Unauthorised Disclosure of Secrets under Article 141 of the Criminal Code and Violation of Confidentiality of Proceedings under Article 337 of the same law further strengthen the realm of confidentiality. These offenses protect different categories of group objects, such as the rights and freedoms of man and citizen or the judiciary. The offense under Article 141 of the CC falls into the category of minor offenses and, considering the prescribed penalty, allows for the application of lighter criminal sanctions, such as community service or warning measures like a suspended sentence or judicial admonition. It also permits the use of certain legal institutes, such as the Offense of Minor Significance under Article 18 of the CC or Deferring Criminal Prosecution under Article 283 of the Criminal Procedure Code. The second offense differs slightly from the others,

as it pertains to protecting the confidentiality of proceedings, which can be relevant in the context of potential abuse of privileged information, especially in criminal proceedings.

Moreover, we have observed that this area is regulated by a significant number of bylaws, which is exceptional in the field of criminal law as it sometimes challenges the principle of legality. Nevertheless, such regulation is necessary in this context, although it requires greater awareness among all participants – both those applying the law and potential offenders.

The issue of data secrecy is one of the most significant aspects of the national security system, both in its preventive and repressive functions. In light of the identified inconsistencies, this article aimed to propose solutions for future amendments and the application of the law. The importance of the classified data protected under the provisions of the Data Secrecy Law and the Criminal Code highlights the sensitivity of this topic, necessitating further development. While an adequate normative framework is essential, effective law enforcement is urgently required to ensure comprehensive protection. Additionally, enhancing the culture of security in the handling and management of classified data is a crucial element of data secrecy protection. As noted in domestic classic literature, Jovan Dučić remarked that "Silent people pour their trust into those they work with, as many see their own security in the silence of others".

REFERENCES

Banović, J. (2022). *Dvojna priroda nehata u krivičnom pravu*. Doktorska disertacija. Univerzitet u Beogradu: Pravni fakultet.

Banović, J. (2023a). Criminal law aspects of digital assets – Contemporary challenges. *Conference Proceedings of International Significance - Archibald Reiss Days,* 13, 89–99.

Banović, J. (2023b). Kaznenopravna dimenzija poslovne tajne u svetlu novog Zakona o zaštiti poslovne tajne. In: M. Živković, M. Lukić Radović (Eds.), *Savremeni problemi pravnog sistema Srbije – Prilozi projektu 2022*. (pp. 259–276), Beograd: Univerzitet u Beogradu – Pravni fakultet.

Bodrožić, I. (2020). Kontinuirani krivičnopravni intervencionizam – na raskršću politike i prava. *Srpska politička misao*, 68(2), 381–396. DOI: https://doi.org/10.22182/spm.6822020.17

Bodrožić, I. & Milošević, M. (2022). Secret as an object of Criminal law protection in the Republic of Serbia. *Thematic Conference Proceedings of International Significance / Ethology, Phenomenology and Trends of Contemporary Crime - Archibald Reiss Days*, 12, 93–111.

Cassman, D. R. (2015). Keep It Secret, Keep It Safe: An Empirical Analysis of the State Secrets Doctrine. *Stanford Law Review*, 67(5), 1173–1217.

Code of Medical Ethics of the Medical Chamber of Serbia, Official Gazette of the Republic of Serbia, No. 104/2016.

Code of Professional Ethics of Lawyers, Official Gazette of the Republic of Serbia, No. 27/2012 and 159/2020 – decision by the Constitutional Court.

Creus, C. (1998a). *Derecho penal – Parte especial* (Tomo 2). Ciudad de Buenos Aires: Editorial Astrea De Alfredo y Ricardo Depalma Srl.

Creus, C. (1998b). *Derecho penal – Parte especial* (Tomo 1). Ciudad de Buenos Aires: Editorial Astrea De Alfredo y Ricardo Depalma Srl.

Criminal Code of Serbia (CC), Official Gazette RS, No. 5/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, and 35/2019.

Criminal Procedure Code (CPC), Official Gazette RS, No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - decision by the Constitutional Court and 62/2021 - decision by the Constitutional Court.

Data Secrecy Law (DSL), Official Gazette RS, No. 104/2009.

Delić, N. (2016). Volja i namera u srpskom krivičnom pravu. In: Đ. Ignjatović (Ed.), *Kaznena reakcija u Srbiji* (deo VI, pp. 92–116), Beograd, Srbija: Univerzitet u Beogradu – Pravni fakultet.

Delić, N. (2021). *Krivično pravo – posebni deo.* Beograd: Univerzitet u Beogradu – Pravni fakultet.

Donna, E. A. (2002). *Derecho Penal Parte Especial* (Tomo II-C). Buenos Aires/Santa Fe: Rubinzal - Culzoni Editores.

Donohue, L. K. (2010). The Shadow of State Secrets. *University of Pennsylvania Law Review,* 159(1), 77–216.

Gál, I. I. L. (2022). The Protection of the State Secret in the Legal History of Europe. *Zbornik radova Pravnog fakulteta u Novom Sadu,* 2, 583–598. DOI: https://doi.org/10.5937/zrpfns56-38185

Application no. 48135/06, ECHR Strasbourg, Youth Initiative for Human Rights v. Serbia, 25/09/2013.

Judgment of the Supreme Court of Cassation of Serbia, KZZ 1120/2019, 17.12.2019.

Kovačević, N. & Milošević, M. (2022). Zaštita tajnih podataka u digitalnoj formi – bezbednosni i krivičnopravni aspekti. *Bezbednost,* 1, 93–107. DOI: https://doi.org/10.5937/bezbednost2201093K

Law on Personal Data Protection (LPDP), Official Gazette RS, No. 87/2018.

Law on Protection of Trade Secrets (LPT), Official Gazette RS, No. 53/21.

Law on Regulation of Courts (LRC), Official Gazette of the RS, No. 10/23.

Law on Security Information Agency (LSIA), Official Gazette RS, No. 42/2002, 111/2009, 65/2014 – decision by the Constitutional Court, 66/2014 i 36/2018.

Milosavljević, B. (2016). *Analiza pravnog uređenja obaveštajno-bezbednosnog sistema Republike Srbije*. Beograd: Beogradski centar za bezbednosnu politiku.

Milosavljević, B. (2023). *Osnovi bezbednosnog prava.* Beograd: Službeni glasnik.

Milošević, M. (2022). *Krivično pravo – posebni deo: izabrane inkriminacije za studije nauka bezbednosti*. Beograd: Univerzitet u Beogradu – Fakultet bezbednosti.

Radisavljević, I. (2023). Krivičnopravna zaštita digitalne imovine. In: Đ. Ignjatović (Ed.), *Kaznena reakcija u Srbiji: tematska monografija* (deo 13, pp. 302–314), Beograd, Srbija: Univerzitet u Beogradu – Pravni fakultet.

Raguan, G. (2014). The State Secrets Privilege: From Evidentiary Privilege to Executive Immunity in the United States. *Institute for National Security Studies,* 121–134.

Stojanović, Z. (2013). *Komentar Krivičnog zakonika.* Beograd: Službeni glasnik.

Vuković, I. (2021). *Krivično pravo – opšti deo.* Beograd: Univerzitet u Beogradu – Pravni fakultet.