RAFAŁ WĄDOŁOWSKI

ORCID: 0000-0003-0601-1213
DOI: 10.4467/20801335PBW.22.059.16950

Protection of classified information in Bosnia and Herzegovina and Croatia. Selected criminal and administrative regulations

Abstract

The article discusses administrative regulations relating to the organization of the system for the protection of classified information in the Republic of Croatia and Bosnia and Herzegovina, as well as presents the criminal laws on crimes against the protection of classified information in force in these countries, along with an interpretation of these laws. The article also presents selected administrative regulations governing the procedure for carrying out security clearances for the issuance of a security clearance allowing access to classified information. In addition, the rationale for classifying information and assigning it a specific classification is discussed. On the basis of an analysis of the provisions in force in Bosnia and Herzegovina (Article 164 § 9 of the Criminal Code) and a comparison with those in force in Poland, among other things, a conclusion was drawn that Polish legislation does not include a countertype that would relieve from criminal liability depositaries of secrets who transfer classified information (without obtaining the consent of the authorities specified by law) in order to prosecute the perpetrators of crimes. The above can be the basis of a legislative *de lege ferenda* request. The article does not exhaust the topic covered, but merely indicates selected issues of the system of protection of classified information. The exploration that has been initiated may be used to conduct in-depth studies of the issue at hand in the future.

Keywords

criminal code, disclosure of secrets, classified information, verification procedure, security clearance, counterintelligence.

The breakup of the Union of Soviet Socialist Republics in 1991 initiated regime changes in the former socialist bloc countries, which, like Poland, included Yugoslavia. There are few studies in the Polish literature on the legal regulations adopted in post-socialist countries, including those created after the breakup of the former Socialist Federal Republic of Yugoslavia[1]. The author covered the scope of scientific interest in two countries that currently belong to two different spheres of political influence: Croatia, a NATO and EU member, and Bosnia and Herzegovina, against which Russia is pursuing an intense policy of influence. He was also tempted to check whether the regulations adopted in the mentioned countries differ in any significant way from those in Poland. An approximation of the legislation normalizing the protection of classified information of Bosnia and Herzegovina and Croatia seems justified, especially since Croatia is a member of NATO and the lessons learned on these regulations can be used to build allied interoperability at the military level. This article does not exhaust the scientific description of information security issues in the mentioned countries due to the complexity of the issue, but it may contribute to further in-depth studies of this relevant element of RP's security in international terms.

Criminal and administrative protection of secrets in Bosnia and Herzegovina

In view of the lack of Polish literature on the legal acts stipulating the protection of classified information in Bosnia and Herzegovina (BaH), it is worth at least outlining the principles of the adopted system for the protection of secrets in this country. Due to the federal nature of the state, there are three legal orders in BaH: a nationwide one and separate ones for the Federation of Bosnia and Herzegovina and the Serbian Republic. As Przemysław Osóbka rightfully notes, the autonomy of the two constituent entities is expressed in separate administrative divisions, as well as having their own constitutions, parliaments and executive powers[2]. BaH also includes the small region of Brčko which has partial autonomy[3]. The act that

[1] The legislation of Western European countries has been described in detail in the literature. The authors also present in them issues concerning the protection of classified information, including in the study *Jawność i jej ograniczenia*, G. Szpor (scien. ed.), vol. 11: *European standards*, C. Mik (vol. ed.), Warsaw 2016. However, there is a lack of up-to-date studies on countries in the central and eastern parts of the continent.

[2] P. Osóbka, *System konstytucyjny Bośni i Hercegowiny*, Warszawa 2011, p. 63 et seq.

[3] In the article, the author focused on the legal order in the Federation of Bosnia and Herzegovina (editor's note).

establishes the integrity of the state is the BaH Constitution[4] of December 14, 1995. Among the 13 freedoms established in Article 2, none refers to the right to obtain information, only the right to freedom of speech is specified. An example of the fact that the failure to establish a constitutional right of access to public information for citizens does not prevent its enactment in other acts is the legal system in the United States, as the US Constitution[5] of September 17, 1787 also does not include a right to obtain public-law information. The First Amendment to the US Constitution of 1791 established freedom of speech[6]. On this basis, the U.S. Supreme Court has derived the right to obtain reliable information from the government in order to expand citizens' knowledge of the state of the country[7]. Thus, the lack of a separate constitutional regulation in the subject area does not exclude the right to demand information from state bodies. In view of the adopted scope of the regulation, i.e. neutrality with regard to the information obligations of the public administration towards the citizen, it should be noted that the BaH constitution also does not address the rationale for restricting access to public information.

BaH's nationwide laws are passed by a parliament consisting of the House of Representatives and the House of Nations. Parliament publishes legislation in three languages: Bosnian, Croatian and Serbian. They are announced in the Official Gazette of BaH (Bos. Službeni glasnik[8]). The essential legal acts establishing the system for the protection of Bosnia and Herzegovina's public secrets are the Act of July 28, 2005 on the Protection of Classified Information[9] (hereinafter: the BaH PCI Act), which was largely amended by a 2009 amendment, and the Criminal Code of BaH[10] (Bos. *Krivični zakon*, Cro. *Kazneni zakon*, Serb. *Кривични законик*), in effect since March 1, 2003. In the terminology of the legal acts establishing the system for the protection of secrets in Bosnia and Herzegovina, the legal definition defining classified information of the highest importance in terms of state security is "tajni

[4] *Ustav Bosne i Hercegovine*. Sarajevo, OHR – (Constitution of Bosnia and Herzegovina).

[5] *Constitution of the United States of America*, House of Representatives, doc. No. 110 – 50 (Constitution of the United States of America).

[6] For more, see: R. Wądołowski, *Ochrona informacji niejawnych w USA. Wybrane regulacje karne i administracyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, No. 25, p. 146 et seq.

[7] U.S. Supreme Court ruling in "Hustler" v. Falwell, 485 U.S. 46, 24 II 1988.

[8] The translation into Polish language of the source texts and proper names was done by Małgorzata Uryga, a sworn translator of Croatian.

[9] *Zakon o zaštiti tajnih podataka* (Službeni glasnik BiH broj 54/2005) – (Act on Protection of Classified Information of Bosnia and Herzegovina of 2005). The amendment was announced in the Official Gazette in 2009 (Službeni glasnik BiH broj 12/2009).

[10] *Krivični zakon Bosne i Hercegovine* (Službeni glasnik BiH broj 3/2003) – (Criminal Code of Bosnia and Herzegovina Act of 2003).

podatak" (Serb. *мајни податак*). The system of protection of state secrets, as in Poland, is based on two pillars – criminal law and administrative[11].

Criminal legislation places crimes that violate the confidentiality of classified information in the category of crimes against state security. The Criminal Code of Bosnia and Herzegovina in the special part in Chapter XVI titled *Crimes against the Integrity of Bosnia and Herzegovina* in Article 164 titled *Disclosure of Classified Information* criminalizes the behavior of disclosing classified information. A separate codification of substantive criminal law is the Criminal Code of the Federation of Bosnia and Herzegovina[12] (hereinafter: CC FBaH), which applies only to this entity, i.e. the Federation, not the whole of Bosnia and Herzegovina. The autonomous legislature uses a slightly different nomenclature and scope of regulation, as it stipulates the secrecy of the federation - "tajna Federacije", defining it in Article 2, paragraph 24[13]. The criminal act, on the other hand, is typified in Article 158, entitled *Disclosure of Federation Secrets*.

The nationwide legislature in Article 164 of the CC BaH criminalizes disclosure of classified information in the basic type of the act and several qualified types, and establishes a countertype[14]. In § 1, the subject of the crime is defined as an individual;

---

[11] Acts against classified information in the RP are criminalized in Articles 265 and 266 § 2 of *the Act of June 6, 1997 – the Criminal Code* (i.e., Journal of Laws 2022, item 1138, as amended) – (hereinafter: RP CC). The legal act with the broadest scope of regulation with regard to classified information in the Republic of Poland is the *Act of August 5, 2010 on the Protection of Classified Information* (i.e. Journal of Laws of 2019, item 742, as amended).

[12] *Krivični zakon Federacije Bosne i Hercegovine* (Službene novine FBiH broj 36/2003 ispr. – 75/2017) – (the 2003 Act of the Criminal Code of the Federation of Bosnia andHerzegovina).

[13] The secrecy of the Federation, canton, city and municipality is information or document specified by law, other regulation or general act of the competent authority issued under the law, the disclosure of which would have harmful consequences for the Federation, canton, city and municipality.

[14] Article 164 of the CC FBaH: "§ 1. An official person or person in charge in the institutions of Bosnia and Herzegovina, or a military officer, authorized to determine the secrecy of data or access to classified information, who without authorization informs another person, transmits or otherwise makes available classified information or obtains classified information for the purpose of making it known or transmitting it to an unauthorized person, shall be punished by imprisonment from six months to five years. § 2. The penalty under § 1 of this Article shall be imposed on anyone who illegally obtains classified information for unauthorized use or who informs another person, transfers or otherwise makes available classified information without authorization, as well as on anyone who informs another person, transfers or otherwise makes available to another person facts or means containing information known to be classified information, which he has illegally come into possession of. § 3. The penalty of imprisonment of one to ten years shall be imposed on anyone who commits an offense under § 1 or 2 of this Article: a) for gain; or b) with respect to information that has been marked as "confidential" or "secret" or "state secret" or "top secret" under the law; or c) for the purpose of making known, transmitting or otherwise making available classified information or its use outside of Bosnia and Herzegovina".

it is an official, soldier or person authorized to process classified information in BaH institutions. The subjective side consists of willfulness with direct or possible intent. A protected good is the confidentiality of classified information. The objective side consists of behavior that results in the disclosure of a secret to a person not entitled to know it. The penalty for committing the crime in question is imprisonment from 6 months to 5 years.

§ 2 criminalizes the act of obtaining classified information in violation of the law by any person for the unauthorized use of such information. It should be assumed, although the provision does not say so, that any use of illegally acquired information is unauthorized. Also criminalized is the disclosure of a secret to another unauthorized person without authorization. Thus, it is assumed that the person disclosing the classified information possesses it lawfully, but unlawfully disposes of it. Another sanctioned behavior in this provision is brokering the transfer of classified information to an unauthorized person, as long as the broker knows that he or she is transferring classified information. The subject of the aforementioned crimes has been identified as common. The subjective side consists of willfulness. Criminal liability was set within the penalty limits for the offense in §1.

§ 3 contains provisions for the qualified types of crimes specified in § 1 and 2. The legislator aggravates criminal liability, setting it at between 1 and 10 years, when the act is committed for the purpose of gaining profit or involves information legally marked "confidential," "secret" or "top secret" or as a state secret. A person who transfers classified information to a foreign state or uses it outside of BaH is also subject to heightened criminal liability. On the other hand, information that is a state secret is information protected under repealed civil and military acts. The BaH PCI Act in Article 86 orders their further protection according to the regime specified for "top secret" information.

In § 4, the legislator established a regime of special liability for persons professionally processing classified information[15]. If the subject of the acts stipulated

[15] Article 164 of the CC FBaH: "§ 4. If an offense under § 1 or § 3 of this Article is committed by a person who, according to the Act on the Protection of Classified Information, is statutorily authorized to determine the secrecy of information or access to classified information of that degree in respect of which the offense was committed, the offender shall be punished: a) for an offense under § 1 of this Article, by imprisonment of at least 3 years; b) for an offense under § 3 of this Article, by imprisonment of at least 5 years. § 5. If the offense under § 1-3 of this Article is committed during a state of martial law or imminent threat of war, or state of emergency, or when an order has been issued to engage and use the Armed Forces of Bosnia and Herzegovina, the perpetrator shall be punished by imprisonment of at least 5 years. § 6. If an offense under § 1 and § 4 of this Article is committed by omission, the perpetrator shall be subject to: a) for an offense under § 1 of this Article, a fine or imprisonment of at least 3 years; b) for an offense under § 4 of this Article, imprisonment of from 3 months to 3 years. § 7. If an offense under § 6 of this Article is committed in connection with

in § 1 or § 3 is a person who has access to classified information under the BaH PCI Act or who has the right to classify classified information, then for the offense under § 1 he is punishable by imprisonment for at least 3 years, and with regard to the offense under § 3 – for at least 5 years.

The increase in criminal liability for crimes under § 1-3 is due to perpetration during states of emergency, threat of war or war, as well as during military operations of the BaH army. Then the lower limit of imprisonment is 5 years (according to § 5 of the article in question). The next paragraph contains provisions for liability for the crimes specified in § 1 and § 4, which occurred as a result of omission. A guarantor of no effect who, by omission, commits an offense under § 1, may be sentenced to a fine or at least 3 years' imprisonment. A prison term of 3 months to 3 years has been established for the offense of § 4.

If, as a result of the omission (described in § 6), there was a disclosure or use of information that was legally marked as "confidential," "secret," or "top secret," or was a state secret under the previous act, the offender is subject to imprisonment from 6 months to 5 years (§ 7). An important regulation of § 8 is the stipulation that the obligation of secrecy continues even after the loss of access to classified information[16]. The editorial unit in question in § 9 is concluded with a countertype. The legislature exempts from criminal liability a person who discloses or mediates the disclosure of classified information if the content of the secret made public violates the constitutional order of Bosnia and Herzegovina or is contrary to an international agreement. The countertype applies only if the publication of the secret does not cause serious harm to the country. There is no adequate regulation in the Polish legal order, which, it seems, is detrimental to the transparency of the implementation of government functions by executive bodies.

Article 164 of the CC BaH is a partially incomplete provision, because in order to decode the criminal prohibition norm, it is necessary to use the Code definition

information that is marked as "confidential" or classified as "secret" or as "state secret" or classified as "top secret" according to the act, the offender shall be punished by imprisonment from 6 months to 5 years."

[16] Article 164 of the CC FBaH: "§ 8. The provisions of § 1, § 3-7 of this Article shall also apply to a person who, without authority, informs another person, provides or makes available classified information after the expiration of his duties as an official or responsible person in the institutions of Bosnia and Herzegovina, or a military officer, or a person authorized to determine the secrecy of information or access to classified information. § 9. It is not a crime to disclose classified information to publish or mediate the publication of classified information, the content of which is contrary to the constitutional order of Bosnia and Herzegovina, in order to make public irregularities related to the organization, operation or management of services, or to make public facts that constitute a violation of the constitutional order or an international agreement, if the disclosure does not have seriously negative consequences for Bosnia and Herzegovina".

of classified information from Article 2 § 24 of the CC BaH[17]. Unfortunately, the cited definition does not specify the classification rationale, it merely indicates the areas (administrative, defense and economic departments) from which information may constitute a secret. The more detailed classification prerequisites referred to in the Criminal Code are set forth in the BaH PCI Act. In it, the legislature also lists areas, including public security and defense, from which information is protected as classified. At the same time, it identifies and assesses the criterion of harm to selected state interests. An important provision is the inclusion of the code term "classified information" in the secrets of other countries and international and regional organizations, so that they become covered by criminal protection, i.e., Article 164 of the CC BaH, as a good with an axiological basis. In addition, the Criminal Code refers not only to secrets classified under the BaH PCI Act, but also to secrets resulting from regulations of other laws or ordinances.

Thus, the broad statutory understanding of the term "classified information" determines the extensive criminal law protection of BaH public secrets and classified information received from other subjects of international law and regional organizations. This is relevant to the security of information also transmitted by Poland under the 2016 Agreement between the Government of the Republic of Poland and the Council of Ministers of Bosnia and Herzegovina on the Protection of Classified Information[18]. Under this agreement, the parties have committed to mutually protecting classified information exchanged in the course of cooperation. Governments have determined the mutual assignment of applicable clauses to ensure adequate protection of the information received. The following table presents the clauses used by both countries.

[17] Classified information – information on public security, defense, foreign affairs and interests, on the activities or interests of intelligence, security of BaH, communications and other systems relevant to the interests of the state, the judiciary, projects and plans important for defense and intelligence activities, scientific, research, technological, economic, financial activities, as well as matters important for the security and functioning of BaH institutions, i.e., the security structure at all levels of the BaH state organization. This is information determined to be classified by law, other regulation or general act of a competent authority issued under the law, or information determined to be classified in accordance with laws and regulations on the protection of classified information. The term also includes classified information of another country, international entities and regional organizations.

[18] A*greement between the Government of the Republic of Poland and the Council of Ministers of Bosnia and Herzegovina on the protection of classified information, signed in Sarajevo on June 7, 2016.* (Journal of Laws of 2017, item 1254).

Clause applicable in RP	Clause used in BaH	Counterpart in English
Ściśle tajne	Vrlotajno	Top secret
Tajne	Tajno	Secret
Poufne	Povjerljivo	Confidential
Zastrzeżone	Interno	Restricted

Due to the code reference, the decoding of the criminal prohibition norm and the determination of the elements of certain offenses under Article 164 of the CC BaH involving the disposition of classified secrets can only be done on the basis of the provisions of the BaH PCI Act.

In Article 1 of the BaH PCI Act, the legislator defined the scope of the regulations introduced by it. The unification of the system for processing and protection of classified information of BaH in the areas specified in this provision, i.e. public security, defense and foreign affairs, among others, was adopted as a priority legislative goal.

The entities required to comply with and apply the Act are listed in Articles 2 and 3. The legislator orders the public administration and other BaH institutions that produce or use classified information in the course of their activities arising from their statutory powers, including international and regional organizations, if this is the result of agreements concluded, to apply the provisions of this act. In the act in question, the legislator also established a general norm of prohibition of disclosure of classified information, obliging any person who legally or otherwise came into possession of it to protect it and keep it secret.

Article 4 contains many statutory definitions. From the point of view of criminal responsibility, the most relevant is the understanding of the term "threat to the integrity of Bosnia and Herzegovina." The legislator defines that it is an objective threat or attack on: constitutional order, independence, territorial indivisibility, sovereignty, security, defense capability and international subjectivity of BaH.

Determining the elements of the offenses stipulated in Article 164 CC BaH seems impossible without determining what type of information can be classified as confidential, secret or top secret. The classification of secrets on the basis of the BaH PCI Act, as in the Polish legal order, is implemented in two stages. According to Article 8 of the cited act, the preliminary stage consists of selecting such information, the disclosure of which to an unauthorized person, to the mass media or to an institution or body of another state could cause a threat to the integrity of BaH, especially in the fields of public security, defense, foreign affairs and interests, intelligence and security interests of BaH, communication systems, scientific

research, state finances, economy and judiciary. The information thus extracted acquires the status of classified and is subject to classification in accordance with the prerequisites of Article 19 of the BaH PCI Act.

The Act, in the article cited above, establishes four levels of classification of classified information. State interest was used as a criterion for the material division of secrets. Included in the following security classifications is classified information, the unauthorized disclosure of which may:

1) jeopardize the integrity of BaH or cause irreparable harm to the state – they are classified "top secret."
2) cause exceptionally negative consequences for the security, political, economic or other interests of BaH – they are classified as "secret."
3) cause negative consequences for the security or interests of BaH – they are classified as "confidential."
4) jeopardize the activities of state bodies or entities at other levels of state organization – they are classified as "restricted."

Based on the analysis of the above regulations, it should be concluded that the classification of information as classified is done on the basis of the threat to the interests of BaH that could arise as a result of the disclosure of its contents, and therefore, in principle, coincides with the Polish regulations. The fields listed in the act correspond to those indicated in the Code's definition of classified information.

In order to follow the rules of legal comparativism for this important issue, it is necessary to examine how the subject matter is regulated in the Polish legal system. The act with the broadest scope of regulation, in which the legislator has established a definition of classified information, is the Act on Protection of Classified Information of 2010[19] (hereinafter: RP PCI Act). The legislator in Article 1(1)[20] indicates the criteria to be used in the process of selecting unclassified information in order to single out only those which, in view of the constitutional[21] prerequisites for restricting the right to information, can be produced as classified or consequently be given such protection. The established verifiers are the effects that could occur as a result of the disclosure of such information. These include the occurrence of harm to the RP, causing a threat of harm to the RP, and causing an adverse state of the RP's interests. After analyzing

[19] Act on Protection of Classified Information.

[20] Ibid., Art. 1. para. 1: "The Act establishes rules for the protection of information, the unauthorized disclosure of which would or could cause damage to the Republic of Poland or would be detrimental from the point of view of its interests, including during its development and regardless of the form and manner of its expression, hereinafter referred to as "classified information".

[21] See especially Articles 61(3), 54, and 31(3) *of the Constitution of the Republic of Poland of April 2, 1997* (Journal of Laws of 1997, No. 78, item 483, as amended).

the cited premises, it can be seen that they form a material definition of classified information, as they indicate the content of the information, not its form.

If it is determined that the disclosure of the information in question would lead to at least one of the listed consequences, the information should be classified and given the appropriate protection clause, thus taking into account the order established by Article 5 of RP PCI Act. As the Constitutional Tribunal points out in its 2009 judgment: *The obligation to grant proper classification exists and is based on the substantive legal criteria for classifying information and Article 7 of the Constitution*[22]. Classifying information solely using the aforementioned vague criteria would consequently affect an overly extensive amount of information. In real-world operations of those authorized to assign clauses, this would result in a high degree of discretion in assessing which information should be protected from disclosure. For this reason, the legislator, after constructing the general definition of classified information contained in Article 1, specifies in Article 5 the areas from which classified information may constitute a secret. Between the general (abstract) definition of classified information and the subject definition of the areas of state activity that must be protected by limiting information, there is a relationship of overriding and underriding. The areas enumerated in Article 5 of the PCI Act prevent broad restrictions on the right to information as a result of the autonomous application of Article 1(1) of the act.

Reasonable are interpretive doubts arising in the context of the vague terms that the legislator used to construct the formal and legal prerequisites for granting the required level of protection to classified information. This implies the question of whether any statutory classifier has sufficient knowledge to consider that the disclosure of a particular classified information will cause or could cause, for example, the occurrence of exceptionally serious or "only" serious damage to the RP. The legislator, in Article 5(1)-(4), lists the areas in which damage[23] supposedly may occur, but does not define how it is to be understood and what the criteria for valuing it are. The statutory specification in this article of damage with the terms: will endanger, worsen, disrupt, hinder, impair or have a detrimental effect does not set a clear interpretive framework.

It seems that the legislator, in pointing out the interests of the RP in Article 1, was referring to those areas of state activity that are listed in Article 5, paragraphs 1-4. Therefore, the cited provisions should be applied together, as their separate application leads to an interpretation *ad absurdum*.

---

[22] Judgment of the Constitutional Court of October 15, 2009, ref. K 26/08, justification in paragraph 183.

[23] Following the principle of the prohibition of homonymity of terms, it should be assumed that the damage indicated in Article 1 is the same as the damage in Article 5.

In part, such a situation is confirmed by the position of the Supreme Administrative Court, which stated that (...) *information is classified information not as a consequence of its classification, but because of the threat posed by its content or the manner in which it was obtained. It is therefore protected as classified information regardless of whether the authorized person has seen fit to mark it with the appropriate classification*. The Supreme Administrative Court rightly recognized that the content of the information is a priority premise for its inclusion in the protection of the state, and at the same time ignored the formal classification (classification marking) as an element that prejudices this protection[24]. The above analysis forms the basis for what appears to be a legitimate conclusion that the only lawful course of action for those making the extraction from a broad set of information of those that should be given classified status is the combined application of Article 1 and Article 5 of RP PCI Act.

When examining regulations on information classification, one cannot overlook the flaws in legal institutions that hinder their establishment. The criteria listed in Article 5 of RP PCI Act, given the vagueness of the terms used in their construction and the general prerequisites for classifying information as classified (Article 1), make it difficult to accurately classify specific information. Additionally, and perhaps most importantly, they create conditions that encourage unwarranted discretion in determining the level of protection of classified information. Official discretion in assigning classification creates a state of uncertainty, which consists of creating doubts about the actual relevance of the information in question for the state's interest. Misinterpretation of the material and formal definition of classified information can result in irrelevant information being protected or important information being deprived of such protection.

An interesting legislative solution used in the BaH PCI Act is the power of the secret depositary to deny the existence of classified information, which is established in Article 26. If the existence of secrecy may adversely affect the interests of BaH, then the authorities are not obliged to confirm or deny its existence despite the demands of the interested parties. Thus, they are not obliged to justify their refusal to provide information, since they can claim that they do not have it. Another important legal institution introduced into the system for the protection of BaH secrets is the establishment, as a separate authorization, of the right to classify classified materials. This authorization is independent of the right to access classified information, as a specific person can only have access to secrets without the right to classify. The legislator, in Article 13, lists those who, in connection with their positions, are authorized to assign the classification "restricted", "confidential" and

[24] Judgment of the Supreme Administrative Court of July 6, 2017, ref. I OSK 932/16.

"secret." Article 14, on the other hand, identifies senior government officials who have the right to classify classified information as "top secret", as well as assign other degrees of protection to the information.

In accordance with the procedure for classifying information adopted in Article 17, the person classifying it shall prepare a written justification specifying the potential harm to BaH if it is disclosed. At the same time, Article 9 prohibits covering information with secrecy if the purpose is to conceal a crime committed, an overstepping of authority, or any violation of administrative law. Declassifying information (reclassifying it to a lower classification or removing classification) also requires written justification (Article 22). The above provisions arguably avoid accidentally over- or under-classifying or classifying such information as secrets.

Persons mentioned in Article 2 of the BaH PCI Act may gain access to classified information after a security clearance is conducted against them. Proceedings may be initiated after obtaining the consent of the person who is to be the subject of the proceedings. The obligation to investigate does not apply to "restricted" information, which is made available to employees (as in the RP) in connection with their position and the decision of their superior. The body that conducts security investigations (Bosn. *sigurnosnih provjera*) in BaH is the Intelligence and Security Agency (Bosn. Obavještajno-sigurnosna Agencija). Persons occupying positions related to access to information with a certain classification submit a personal security questionnaire (the substantive scope is similar to the Polish model), which, together with the application of the head of the organizational unit, is forwarded to the said Agency through the Ministry of Security (Bosn. Ministarstvo sigurnosti). The legislature has established three types of security clearances, which are applied depending on the classification of the information to which the person is to be granted access. The procedure with a basic scope of checks is applied to the "confidential" classification, and with an expanded one – to secret information. In contrast, access to top-secret material is contingent on submitting an expanded security questionnaire and completing a special range of checks. The organizational units of the Ministry of Defense and the police authorities and special services, based on Article 33 of the BaH PCI Act, carry out basic vetting of employees on their own.

The procedure for obtaining a security clearance, as in the Polish legal system, is an autonomous administrative procedure. A vetted person may appeal against the decision to refuse to issue a certificate to the Parliamentary Commission overseeing the Intelligence and Security Agency. If the appellate body upholds a negative decision, the party has the right to appeal to the administrative court. The certificate allowing access to confidential information is valid for 10 years, and for higher clauses – 5 years.

An important regulation that protects the interests of the vetted person is the guarantee of employment in a given organizational unit in the event of refusal to issue or revocation of a security clearance, as mentioned in Article 61 of the BaH PCI Act. The employer is obliged to offer a person against whom security vetting has been initiated, if required by security considerations, or whose authorizations have been revoked, another job position not related to access to classified information. In the absence of other positions, the employee is dismissed with consideration of termination compensation. The means of enforcing compliance with the regulations introduced by the act is not only criminal liability, but also the fines established by the act (Articles 78 and 79 of the BaH PCI Act). Persons holding managerial positions in entities required to comply with the Act who fail to perform the duties imposed on them may be fined between 1,000 and 5,000 convertible marks[25]. The legislator has sanctioned for violations employees who perform duties related to information protection, such as maintaining records, issuing security certificates, classifying information, or are responsible for applying physical and other safeguards.

The regulation of the system of protection of public secrets by administrative law, as well as the partially blanket nature of the criminal provisions in force in BaH, allow to identify analogous elements in the Polish system of protection of classified information. It is worth considering the introduction into Polish legislation of the institution of the countertype of the crime of disclosure of classified information committed for the purpose of reporting a criminal act or irregularities in the functioning of public administration. Given the numerous criteria for obtaining the right to access secrets and exercising it, also the guarantee of employment in the event of loss of warranty – at least in some cases – seems an apt solution.

Criminal and administrative protection of secrets in the Republic of Croatia

The 1990 Constitution of the Republic of Croatia (RCr)[26] until its amendment in 2010, like the Constitution of Bosnia and Herzegovina, did not explicitly include

[25] Convertible mark – the official currency of Bosnia and Herzegovina. One convertible mark is divided into 100 convertible pfennigs (editor's note).

[26] *Ustav Republike Hrvatske* (Narodne Novine broj 56/1990) – (Constitution of the Republic of Croatia of December 22, 1990). This legal act has been amended five times: by the Act of 12 December 1997, by the Act of 9 XI 2000, by the Act of 28 III 2001, by the Act of 16 VI 2010 and by the Constitutional Court's judgment of 15 I 2014. All the amendments are available on the website of the official

provisions on the right of access to information. Croatian Parliament (Croatian: Hrvatski sabor[27]) on June 16, 2010, passed an amendment to the Constitution of the RCr, including, among other things, Article 38, to which another paragraph was added[28]. With the extension introduced, the right of access to information available to any public body was established, with the proviso that the limitation of this right may be made within the limits set by the common law in proportion to need, taking into account the values of a free and democratic society. Arsen Bačič and Petar Bačič assess that the regulation, which reflects basic human rights, maintains the normative level of similar legal solutions in force in other democratic countries of the world. They note that effective control of power by the public is accomplished through the introduction and observance of human rights and fundamental freedoms. The right of access to information regarding the exercise of power limits that power and allows the people as sovereign to effectively oversee the actions of the government[29]. Regulations coinciding in essence are contained in the constitutions of the Republic of Poland and the Russian Federation[30].

The principal legal act establishing the system for protecting Croatian public secrets is the Act of July 13, 2007[31] on the Protection of Classified Information (hereinafter: the RCr PCI Act). The aforementioned act was amended by the Act of July 3, 2012[32] with regard to the exemption of certain government officials from the requirement to have security clearance. The second act shaping the protection system is the Criminal Code, enacted by the Croatian Parliament on October 21, 2011[33] (hereinafter: RCr CC). Alen Rajko, on the basis of the Croatian law shaping the system of information protection, rightly notes that the study of the essence

publication body of the Republic of Croatia Narodne Novine (hereinafter: N.N.), https://narodne novine.nn.hr/clanci/sluzbeni/1990_12_56_1092.html.

27 Unicameral parliament. For more, see: K. Składowski, *System rządów w Republice Chorwacji*, Łódź 2013, p. 98 et seq.

28 *Odluku o proglašenju promjene Ustava Republike Hrvatske* (N.N. broj 76/2010).

29 A. Bačič, P. Bačič, *Sloboda informiranja u sistemu ustavne podjele vlasti*, in: *Pravo na pristup informacjiam i zaštita osobnih podataka*, B.B. Vetma, M. Boban (ed.), Split 2015, p. 62 et seq. (materials of the international scientific and professional conference "The right of access to information and protection of personal data").

30 For more, see: R. Wądołowski, *Ochrona tajemnicy państwowej w Federacji Rosyjskiej. Wybrane regulacje karne i administracyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, No. 24, p. 64 et seq.

31 *Zakon o tajnosti podataka* (N.N. broj 79/2007) – (Act on Protection of Classified Information, passed by the Croatian Parliament on July 13, 2007).

32 *Zakon o izmjeni Zakona o tajnosti podataka* (N.N. broj 86/ 2012) – (Act on amending the Act on Protection of Classified Information, passed by the Croatian Parliament on July 3, 2012).

33 *Kazneni zakon* (N.N. broj 125/2011) – (Criminal Code Act, enacted on October 21, 2011).

of secrecy is to determine the boundary between the citizen's right to know and the public interest in keeping certain information secret, i.e. between legitimate and illegitimate secrets[34].

The legislature's response to the amendment of the RCr Constitution and the introduction of the right to information was the enactment in 2013 of a new Act on the Right To Access Information[35]. The act in question was largely amended in 2015.[36] The legislature, in Article 1, paragraphs 4 and 5, limited the scope of the amendment, indicating that the regulation does not cover classified information – both domestic and from international exchanges. An important institution of the amended act is the "proportionality and public interest test" defined in Article 5, paragraph 7, the procedure for applying which is specified in Article 16. According to the cited test, in case of doubts when resolving a request for information, the institution either releasing the information or protecting it is first of all obliged to examine whether its release may result in the violation of one of the interests specified in Article 15(2)-(4)[37] and to what extent. It considers both the individual interest of the party and the public interest in terms of the good that will occur if the information is released.

In the texts of the laws establishing the Croatian system for the protection of secrets, the legal definition defining classified information of the highest importance in terms of state security is "tajni podatak". The protection system, as in Poland and BaH, is based on two pillars – criminal and administrative.

In criminal legislation, crimes that violate the confidentiality of classified information fall into the category of crimes against the Republic of Croatia. The Criminal Code of the RCr, in the special part in Chapter XXXII, Article 347 titled *Disclosure of classified information*, criminalizes in § 1 the behavior of providing classified information to an unauthorized person. § 2 stipulates a separate criminal act of obtaining classified information for unauthorized use by either the acquirer or another person. In the subsequent provisions, i.e. § 3 and § 4, the legislator typified

[34] A. Rajko, *Tajni podaci: nužnost i (ili) informativna diskriminacija?*, "Politička misao" 1997, vol. 34, No. 3, p. 179 et seq.

[35] *Zakon o prawu na pristup informacijama* (N.N. broj 25/2013) – (Act on the Right of Access to Information).

[36] *Zakon o izmjenama i dopunama Zakona o pravu na pristup informacijama* (N.N. broj 85/2015) - (Act on Amendments to the Act on the Right of Access to Information).

[37] Among others: classified information, trade and professional secrets, the area of personal data and other cases, such as the existence of suspicions that the disclosure of information will impede the conduct of administrative or judicial proceedings or the exercise of inspection supervision.

the qualified forms of the acts described in § 1 and § 2, while in § 5 it sanctioned an omission resulting in the fulfillment of the elements of the offense of § 1[38].

The commentary to Article 347 of the CC RCr by the Codification Team of the Ministry of Justice shows that the perpetrator of the principal form of the criminal act specified in § 1 can only be a person who has been lawfully entrusted with classified information, i.e. an individual entity[39]. The verb form "shall make available" used in the construction of the provision is reflected in the Polish term "shall disclose," as used in Article 265 § 1 of the RP CC. The subjective side consists of intentional behavior with direct or possible intent. The crime committed as a result of the action is punishable by imprisonment from 6 months to 5 years. Perpetration by omission, on the other hand, is sanctioned by imprisonment for up to 3 years, as provided in § 5 of the article in question.

The crime stipulated in § 2 may be committed by a person who obtains classified information for the purpose of its unauthorized use or use by another person. A person who discloses classified information to another unauthorized person will also fulfill the elements of this crime, including when he or she learns the information involuntarily. The subject of this crime is widespread, as potentially anyone can accidentally, or even against their will, become acquainted with classified information. This is because it is difficult to protect oneself from receiving (hearing, reading) the information provided by the other person, who informs about its protection only after it has been transmitted. The subjective side of the aforementioned crimes consists in the willfulness of behavior with direct or possible intent. The good protected in § 1 and § 2, as in the relevant RP regulations, is the confidentiality of information and the interest of the state. The verb phrase "shall acquire" as used in § 2, is indefinite, so it includes both lawful and unlawful actions; what is important is the purpose of acquisition, i.e. using the acquired information, disposing of it without having a legal basis for doing so. This provision stipulates "unauthorized use", i.e. any use that is contrary to the law, regardless of whether it will result in financial or personal gain. An important premise

[38] Article 347 of the CC RCr: "§ 1. Whoever provides classified information entrusted to him to an unauthorized person shall be subject to a penalty of imprisonment from 6 months to 5 years. § 2. Whoever obtains classified information for the purpose of unauthorized use by himself or another person, or whoever makes available to another person such information, the possession of which he came into accidentally, shall be subject to the penalty of imprisonment for up to 3 years. § 3. Whoever does an act under § 1 and 2 of this Article for profit, shall be punished with imprisonment from one to ten years. § 4. Whoever commits an offense under § 1 and 2 of this article during martial law or imminent threat of war, shall be punished by imprisonment from 3 to 12 years. § 5. Whoever commits the offense of § 1 of this article by omission shall be punished by imprisonment for up to 3 years."

[39] K. Turkovič, *Komentar kazanenog zakona*, Zagreb 2013, p. 417.

that fulfills the hallmark of a criminal act is to take an activity (action) against the "acquired" information, in the absence of legal legitimacy to do so. The mere accidental acquaintance with a secret is not criminalized, but it becomes a criminal act when it is used unauthorized or transferred to another unauthorized person.

In § 3 of Article 347 of the CC RCr, the Croatian legislature has established an aggravated type of the crimes specified in §1 and §2. The rationale for aggravating criminal liability is the commission of the said criminal acts for low motives, i.e. for profit. Both the upper and lower limits of imprisonment have been raised – from 1 year to 10 years, respectively. The commission of offenses under § 1 or § 2 when Croatia is in a state of war or wartime danger results in increased criminal liability. The threat to state security caused by the disclosure of a secret or its unauthorized use in the face of waging or preparing for war is more likely and more severe for the interests of Croatia[40]. According to the retributive model of responsibility, the dimension of punishment should be adequate to the act, which is probably why the length of imprisonment was increased and set at 3 to 12 years.

Although Article 87 § 12 of the CC RCr[41] defines the term "classified information," the drafting of the criminal regulations in question (Article 347 § 1 and § 2) should be considered incomplete. The legislator, through the aforementioned definition, introduces two relevant regulations. The first is a reference to another act (without specifying further which one) on the basis of which a given information was granted protection due to its inclusion in the collection of classified information. So, the classification criteria are not established by the Criminal Code, but by another act. The second regulation is a universal prohibition standard. The legislator constructs it by using a statement in the body of the definition under discussion: *Classified information does not include information whose content is contrary to the constitutional order*, and therefore formulates the imperative of prohibiting the secrecy of unclassified information. The addressee of the prohibition is everyone, so also those who are entitled to consider the information in question as classified due to its importance. The legislature prohibits restricting access to such information if it constitutes evidence of crime or other violations of the act in state bodies. Thus, by prohibiting the secrecy of information regarding irregularities in the functioning of the government, it allows the sovereign to exercise oversight

[40] Ibid.

[41] Classified information – information that has been designated as classified information according to a separate act. Information, the content of which is contrary to the constitutional order of the Republic of Croatia, or information that has been marked as classified in order to conceal a crime, overstepping or abuse of authority, and other forms of illegal conduct in state bodies, shall not be treated as classified information.

over the government, which ensures the maintenance of the model of a democratic state system.

The above considerations give rise to the conclusion that if the content of classified information is contrary to the constitutional order of the RCr or has been placed under the protection of the state in order to cover up a crime or other violations in its organs, especially the exceeding or abuse of authority, then the disclosure of such classified information is not subject to the criminalization established by Article 347 of the CC RCr. This kind of formally classified information does not enjoy the protection of the law inherent in information that has been declared classified in accordance with the substantive grounds. Paralleling the above regulation are the provisions of the President's Executive Order 13526 of 2009.[42] Under it, the U.S. President prohibits keeping information secret or covering it with a clause to hide a violation of the law by the administration, limit competition, or conceal information troublesome to an individual or legal entity[43]. Due to the reference in Article 87 § 12 of the CC RCr to another act, the decoding of the norm of the criminal prohibition and the determination of the elements of the offenses under Article 347 of the CC RCr, the disposition of which includes classified information, can only be done on the basis of the provisions of the Act on the Protection of Classified Information of 2007. As Branko Peran aptly notes, in Article 1 of the RCr PCI Act, the legislator defines the material scope of the areas regulated by it, which are: the concept of classified information without a specific degree of secrecy and access to and protection of such information, as well as the degrees of secrecy and the procedure for classification and declassification of classified information[44]. In addition, the Croatian legislator, by indicating specific institutions and positions (civil servant posts), specifies which entities are obliged to apply it. These are: state bodies, local government units, legal entities authorized to exercise public authority, legal entities and individuals who, in accordance with the Act on Protection of Classified Information, gain access to classified information or information without specifying the degree of secrecy use classified information (this type of information is considered service or so-called sensitive) or handle such information.

In Article 2, the legislator formulated several legal definitions. From the point of view of criminal liability, the most relevant is the understanding of the term

[42] *The President Executive Order 13526* of 2009, *Classified National Security Information*, https://www.federalregister.gov/documents/2014/07/30/2014-17836/classified-national-security-information [accessed: 18 May 2022].

[43] R. Wądołowski, *Ochrona informacji niejawnych w USA*…, p. 155.

[44] B. Peran, M. Goreta, K. Vukošić, *Pojam i vrste tajni*, „Zbornikradova. Veleučilišta u Šibeniku" 2015, No. 3–4, p. 127.

"classified information". According to the Act, it is information that has been marked as classified by an authorized body using a procedure prescribed by law and for which a classification has been determined, with the proviso that classified information is also classified information received from another country.

The subsumption of an act as fulfilling Article 347 of the CC RCr depends first and foremost on resolving whether the disclosed or unlawfully used information was indeed classified information. The Croatian legislator does not make criminal liability dependent on the classification of the classified information in question, as the criminal provision applies to all grades of classified information. It should be assumed that the dimension of the penalty is likely to depend on the damage that the offender's criminal action has caused or could have caused, which is mainly determined by the classification of the disclosed classified information. In connection with the aforementioned definition, it is therefore expedient to determine what entities are authorized to classify information and what criteria determine its secrecy.

According to Article 13 of the RCr PCI Act, classification of information as top secret, secret, confidential and restricted may be made by the President, the Speaker of Parliament[45], the Prime Minister of the Government, ministers, the Attorney General, the head of the General Staff of the Armed Forces, the heads of the intelligence and security organs of the RCr, and persons authorized by the aforementioned officials – within the scope of their authority. The classification "confidential" and "restricted" may be granted by the heads of other state bodies. It is the duty of those authorized to classify information to cover the protection of information that is produced by scientific institutions and enterprises in the implementation of projects relevant to the security of the RCr.

The legislature, in Article 3 of the Act in question, prohibits the classification of information for the purpose of concealing a crime, exceeding or abusing powers, and other forms of illegal conduct in state bodies. The regulation in question corresponds to the imperative of Article 87 of the CC RCr, mentioned above.

In Article 6, the legislature requires authorized persons to classify information. He points to the state interest as a criterion for the substantive division of secrets. Peran's observation that the procedure for classifying information means assigning one of the degrees of secrecy of information adequate to the threat and values protected by the law[46] should also be considered correct. The legislature stipulates that top secret is information the unauthorized disclosure of which would cause

[45] For more, see: K. Krysieniel, *Ewolucja systemu politycznego w Chorwacji 1990–2010. Próba bilansu*, „Przegląd Prawa Konstytucyjnego" 2010, No, 2–3, p. 241–260.

[46] B. Peran, M. Goreta, K. Vukošić, *Pojam i vrste tajni*…, p. 133.

irreparable harm to the national security and vital interests of the RCr, particularly: the foundations of its constitutional order, independence, integrity and security, international relations, defense capability and intelligence system, security of citizens, the foundations of the economic and financial system, scientific discoveries, inventions and technologies important to national security.

Defining the lower classification levels involves valuing the harm to the state interest for assets that should be given the highest level of protection, i.e. "top secret." The legislator specifies in Article 7 that information whose unauthorized disclosure would seriously harm the values listed in Article 6 of the Act should be classified as "secret." If, on the other hand, unauthorized disclosure would harm the aforementioned values without indicating the intensity (dimension) of the harm, then the "confidential" classification should be used.

The "restricted" clause classifies information, the unauthorized disclosure of which would harm the activities and performance of the tasks of state bodies in carrying out the activities listed in Article 5 of the said act[47].

It is worth mentioning that under the 2016 Agreement between the Government of the Republic of Poland and the Government of the Republic of Croatia on the Mutual Protection of Classified Information, the parties undertook to mutually protect classified information exchanged in the course of cooperation[48]. Governments have determined the mutual assignment of applicable clauses to ensure adequate protection of the information received. The following table presents the clauses used by both countries.

Clause applicable in RP	Clause used in RCr	Counterpart in English
Ściśle tajne	Vrlotajno	Top secret
Tajne	Tajno	Secret
Poufne	Povjerljivo	Confidential
Zastrzeżone	Ograničeno	Restricted

[47] Article 5 of the CC RCr: Due to the degree of threat to the protected values, the degrees of secrecy (top secret, secret, confidential, restricted – author's note) of Article 4 of this Act may be used to classify information from the area of state bodies in the field of defense, intelligence and security system, foreign affairs, public security, criminal proceedings, and science, technology, public finance and economy, if this information is relevant to the security interests of the Republic of Croatia.

[48] *Agreement between the Government of the Republic of Poland and the Government of the Republic of Croatia on the mutual protection of classified information, signed in Warsaw on October 6, 2016.* (Journal of Laws of 2017, item 2071).

The Croatian legislator specifies in the Act on Protection of Classified Information the scope of the security clearance procedure and the criteria for obtaining a security clearance (Croatian: *certifikat*), which are similar to the corresponding Polish regulations. Persons who occupy positions involving classified information can gain access to such information after completing a special questionnaire and agreeing to apply to them the (Croatian: *sigurnosna provjera*) security screening procedure. The head of the organizational unit in which the person concerned is employed applies to the Office of the National Security Council (Croatian. Ured Vijeća za nacionalnu sigurnost)[49]. The Council, in order to make the necessary checks, forwards the candidate's questionnaire to the Intelligence and Security Agency (Croatian Sigurnosno–obavještajna agencija)[50]. The Council, within the framework of the security control procedure of the person in question, verifies the information contained in the questionnaire and examines whether there are the so-called security obstacles listed in Article 18 (6) of the RCr PCI Act, i.e.: the provision of false information in the questionnaire, circumstances specified in separate laws that prevent the admission of a person to state service, adjudicated disciplinary sanctions, and other facts that provide grounds for suspicion of the confidentiality and reliability of the handling of classified information. The Office of the National Security Council, on the basis of the security assessment performed by the Intelligence and Security Agency, issues a certificate or a denial decision. A party does not have the right to appeal against a negative decision to a higher authority, but it is entitled to file a complaint with the court and litigate before the administrative courts.

In summary, the basis of the Croatian system for protecting public secrets is the Act on Protection of Classified Information and partially blanket criminal laws, as in Bosnia and Herzegovina and Poland. The act that details Croatia's Act on the Protection of Classified Information is the 2007 Act on Information Security, which establishes standards for the protection of classified information[51]. The Act is targeted at public administration entities and legal and natural persons who have access to classified information. The referenced act sets out measures and rules for protecting information in five areas of security, namely: control, physical protection, data security, information systems security and commercial cooperation.

The statutory separation of the right to classify classified information from the right of access to such information, which has been applied in the legislation

[49] For more, see: Ured Vijeća za nacionalnu sigurnost, https://www.uvns.hr/ [accessed: 1 X 2021].

[50] For more, see: Sigurnosno–obavještajna agencija, https://www.soa.hr/hr [accessed: 1 X 2021].

[51] *Zakon o informacijskoj sigurnosti* (N.N. broj 79/2007, 2484) – (Information Security Act, enacted July 13, 2007).

of Bosnia and Herzegovina and Croatia, increases the certainty of correct classification of information and thus minimizes the danger of unjustified classification of unclassified information. However, it seems that the solution adopted limits the dynamics of covering information vital to state security. The Polish legislator has not introduced this type of regulation, so any person authorized to process classified information can classify it in terms of the clauses covered by his security clearance, as long as he is authorized to sign a particular document or mark the material.

As mentioned in the introduction, this article does not exhaust the subject of consideration, but it can be a contribution to the formulation of research problems, and, as a result, provide a stimulus for further scientific research. Based on the material presented, it should be concluded that the systems of protection of classified information of the Republic of Croatia and Bosnia and Herzegovina are not different, and do not differ from Polish regulations. They show great similarities with the system adopted in the Polish legal system. Some legal institutions that do not exist in the RP are of a guarantee nature with regard to a person's subjective rights, such as ensuring continued employment if security clearance is denied. They can also strengthen executive oversight, such as by not sanctioning the disclosure of classified information that has been protected to cover up a crime.

References

Bačič A., Bačič P., *Sloboda informiranja u systemu ustavne podjele vlasti*, in: P*ravo na pristup informacjiam i zaštita osobnih podataka*, B. B.Vetma, M. Boban (ed.), Split 2015, p. 25–66.

Jawność i jej ograniczenia, G. Szpor (sci. ed.), vol. 11: *Standardy europejskie*, C. Mik (ed.), Warszawa 2016.

Krysieniel K., *Ewolucja systemu politycznego w Chorwacji 1990–2010. Próba bilansu*, „Przegląd Prawa Konstytucyjnego" 2010, No. 23, p. 241–260.

Osóbka P., *System konstytucyjny Bośni i Hercegowiny*, Warszawa 2011.

Peran B., Goreta M., Vukošić K., *Pojam i vrste tajni*, „Zbornikradova. Veleučilišta u Šibeniku" 2015, No. 3–4.

Rajko A., *Tajni podaci: nužnost i (ili) informativna diskriminacija?*, „Politička misao" 1997, vol. 34, No. 3.

Składowski K., *System rządów w Republice Chorwacji*, Łódź 2013.

Turkovič K. i in., *Komentar kazanenog zakona*, Zagreb 2013.

Wądołowski R., *Ochrona informacji niejawnych w USA. Wybrane regulacje karne i administracyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, No. 25, p. 146–182.

Wądołowski R., *Ochrona tajemnicy państwowej w Federacji Rosyjskiej. Wybrane regulacje karne i administracyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, No. 24, p. 63–90.

Internet sources

Sigurnosno–obavještajna agencija, https://www.soa.hr/hr [accessed: 1 X 2021].

Ured Vijeća za nacionalnu sigurnost, https://www.uvns.hr/ [accessed: 1 X 2021].

Legal acts

Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997, No. 78, item 483, as amended).

Act of August 5, 2010 on the protection of classified information (i.e. Journal of Laws of 2019, item 742, as amended).

*Act of June 6, 1997 – Criminal Code (*i.e.: Journal of Laws of 2022, item 1138, as amended).

Agreement between the Government of the Republic of Poland and the Government of the Republic of Croatia on the mutual protection of classified information, signed in Warsaw on October 6, 2016. (Journal of Laws of 2017, item 2071).

Agreement between the Government of the Republic of Poland and the Council of Ministers of Bosnia and Herzegovina on the protection of classified information, signed in Sarajevo on June 7, 2016. (Journal of Laws of 2017, item 1254).

Acts of the Republic of Croatia

Ustav Republike Hrvatske (Narodne Novine broj 56/1990).

Zakon o izmjenama i dopunama Zakona o pravu na pristup informacijama (Narodne Novine broj 85/2015).

Zakon o prawu na pristup informacijama (Narodne Novine broj 25/2013).

Zakon o izmjeni Zakona o tajnosti podataka (Narodne Novine broj 86/2012).

Kazneni zakon (Narodne Novine broj 125/2011).

Zakon o informacijskoj sigurnosti (Narodne Novine broj 79/2007, 2484).

Zakon o tajnosti podataka (Narodne Novine broj 79/2007, 2483).

Odluku o proglašenju promjene Ustava Republike Hrvatske (Narodne Novine broj 76/2010).

Acts of Bosnia and Herzegovina

Ustav Bosne i Hercegovine. Sarajevo, Office of the High Representative, https://biblioteka.sejm.gov.pl/wp-content/uploads/2016/09/Bo%C5%9Bnia-i-Hercegowina_bos_010716.pdf.

Zakon o zaštiti tajnih podataka (Službeni glasnik BiH broj 54/2005).

Krivični zakon Bosne i Hercegovine (Službeni glasnik BiH broj 3/2003).

Krivični zakon Federacije Bosne i Hercegovine (Službene novine FBiH broj 36/2003 ispr. – 75/2017).

U.S. legislation

Constitution of the United States of America, House of Representatives, doc. No. 110 – 50.

U.S. President's Executive Order

The President Executive Order 13526 of 2009, *Classified National Security Information*, https://www.federalregister.gov/documents/2014/07/30/2014-17836/classified-national-security-information [accessed: 18 V 2022].

Case law

Judgment of the Constitutional Tribunal of October 15, 2009, ref. K 26/08.

Judgment of the Supreme Administrative Court of July 6, 2017, ref. I OSK 932/16.

U.S. Supreme Court ruling in "Hustler" v. Falwell, 485 U.S. 46, 24 II 1988.