

Remigiusz ROSICKI

Adam Mickiewicz University in Poznań

ORCID ID:0000-0002-1187-5895

## State Security as Exemplified by the Offense of Espionage Under Polish Law

**Abstract:** The scope of the research problem encompasses selected issues concerning the content and sense of the elements characterizing the offense of espionage in Polish criminal law. In the legislation currently in force, the offense of espionage is criminalized under Art. 130 § 1–4 of the Criminal Code. The main purpose of the analysis is to perform a substantive criminal examination of the offense of espionage under Polish law, considering a practical case study and an assessment of the legal provisions regarding state security. In order to elaborate the material scope of the research problem and present the conclusions, the paper asks the following research questions: (1) To what extent are the *de lege lata* legal solutions in Poland effective in counteracting espionage offenses?, (2) What *de lege ferenda* solutions ought to be proposed to improve effective counteraction of espionage offenses? The paper includes an institutional and legal analysis aided by textual, functional, and historical interpretations, supplemented with the author's conclusions and opinions concerning *de lege lata* and *de lege ferenda* solutions. The institutional and legal analysis is supplemented with a case study of espionage activity. The case study helps consider selected legal problems and presents example legal classifications of the described acts associated with espionage activity.

**Key words:** state security, information security, espionage, offense of espionage, intelligence activity

---

### Introduction

The subject of analysis in the present text is delineated by legal solutions concerning the scope of criminalization of espionage in the context of state security. Attention is focused on the content and sense of the statutory criteria for the offense of espionage criminalized in Art. 130 § 1–4 of the Polish Criminal Code (Journal of Laws 1997, no. 88, item 553). It is noteworthy that the category of state security can be understood both in the context of political science and law. The former

case is associated with the fact that the offense of espionage *sensu lato* is treated as a political offense, especially in a situation where espionage is committed by a citizen of a given state, which is viewed as a betrayal of the mother country (for more on this see: Kuczur, 2012). In the latter case, espionage is treated as an act infringing a legal interest, i.e., a subject of substantive criminal protection – the state (i.e., the Republic of Poland) (cf. Hoc, 2002). Besides, it is worth noting that state security is reckoned among constitutional values, and so it is derived from a suprastatutory legal act.

The paper's main purpose is to perform a substantive criminal analysis of the offense of espionage under Polish law, taking into account a practical case study and an assessment of the legal provisions in force concerning the legal interest of state security. In order to elaborate the objective scope of the research problem, the following research questions have been included in the text: (1) *To what extent are the de lege lata legal solutions in Poland effective in counteracting espionage offenses?*, (2) *What de lege ferenda solutions ought to be proposed to improve effective counteraction of espionage offenses?*

The presented analysis has been performed considering an institutional and legal approach. The research problem, the doctrinal, and dogmatic debate on the offenses of espionage under Polish law have been supplemented with the author's own opinions and conclusions. Besides, regarding the analysis of the legal aspects of the offense of espionage, textual, functional, and historical interpretations have been employed (cf. Wronkowska, Ziemiński, 1997, pp. 147–179; Zieliński, 1998, pp. 1–20; Wronkowska, 2005, pp. 76–91; Nowacki, Tabor, 2016, pp. 293–312). The textual interpretation uses both the exegetical and eisegetical approaches, thereby employing both a strict textual interpretation and a broader interpretation by reading own presuppositions into the text (cf. Aichele, Phillips, 1995, pp. 7–18). The functional interpretation focuses on the function of selected legal solutions so that the presented norms are provided with proper axiological substantiation. In addition, for a better understanding of the meaning of legal regulations in force and their practical application, the text uses an abstract case study that has no factual equivalent, thereby constituting a thought experiment. As regards the historical interpretation, the text selectively juxtaposes the current statutory criteria for the offense of espionage with the statutory criteria applicable in the legislation previously in force, i.e., in the periods of 1946–1969 and 1970–1997.

## 1. Characterization of the Offense of Espionage *de lege lata*

### 1.1. General Assumptions Underlying Criminalization of Espionage

As the legislator passed a new criminal code in 1997, he used some of the statutory criteria for the espionage offense known in other legislation, particularly in the criminal code passed in 1969. Also, it is noteworthy that in the legislation in force between 1970 and 1997, there were two prohibited acts related to a broader category that might be termed espionage activity. In the former case, criminalization applied to various types of offense doctrinally referred to as espionage, while in the latter case, to the offense consisting in betrayal of the mother country whose statutory criteria only partially covered espionage activity (cf. Art. 124 and 122, Journal of Laws 1969, no. 13, item 94).

The 1969 Criminal Code, in Art. 124, criminalized the offense of espionage in three types. However, in each of these cases, the activities undertaken by the offender consisted of various forms of behavior. The basic type criminalized partaking in foreign intelligence activity and providing messages to a foreign intelligence service, thereby acting on its behalf. The aggravated type criminalized organization or management of foreign intelligence activity. The mitigated type was concerned with collecting or storing messages to supply them to a foreign intelligence service, as well as engaging in activity for the benefit of a foreign intelligence service (Journal of Laws 1969, no. 13, item 94; Bafia, Mioduski, Siewierski, 1977, pp. 315–318; Andrejew, 1978, pp. 98–99).

Regarding the Art of legislation, the distinctive feature was that the basic and aggravated types of the offense of espionage were criminalized in one clause – the first clause of Art. 124. The mitigated type of this offense was criminalized in the subsequent clause – the second clause of Art. 124. Of the greatest significance were the criteria for the *ratione materiae* scope, especially providing a foreign intelligence service with messages, thereby acting on its behalf. Unlike the legislation in force before 1970 and nowadays, the kind of messages typifying a prohibited act was of no import. Therefore, next to participating in foreign intelligence activity, penalization encompassed providing any information that might be useful to a foreign intelligence service. The mitigated type criminalized collecting or storing messages to provide them to a foreign intelligence service, but in this case, the legislator did not provide any specifics,

e.g., about the import of this kind of information. Apart from these mitigated types, the legislator criminalized undertaking activity for the sake of a foreign intelligence service. In the legislation in force between 1970 and 1997, undertaking activity for a foreign intelligence service meant expressing willingness to act for the sake of a foreign intelligence service, e.g., declaring oneself willing to work for the benefit thereof. Thus, we are dealing with an offense by an offeror in a situation when his offer has reached a specific entity and has been accepted. However, if there is no acceptance of the offer of willingness to act, the act is treated as a prohibited act of attempt in its inchoate form. It is noteworthy that the statutory criteria for the aggravated type of the offense of espionage consisting in organization and management of a foreign intelligence service's activity are again used in the current legislation (Bafia, Mioduski, Siewierski, 1977, pp. 315–318; Andrejew, 1978, pp. 98–99).

As indicated previously, next to the offense of espionage, the legislation in force between 1970 and 1997 featured an offense of the betrayal of the mother country (Art. 124), which was the most serious crime against the external security of the Republic of Poland. The criminal weight of this act was also amplified by Art. 93 of the 1952 Constitution. The provision of the then Constitution indicated that the betrayal of the homeland, e.g., espionage, enfeebling of the armed forces and defecting to the enemy's side were to be punished most severely, as the gravest crimes should (Journal of Laws 1952, no. 33, item 232, as amended; Journal of Laws 1976, no. 7, item 36, consolidated text). The Criminal Code specified two types of betrayal of the homeland, of which the latter one is of the greatest relevance for the subject matter under analysis in the present text. That is because it directly pertains to the prohibited activity for the benefit of a foreign intelligence service and against the essential interests related to the national security or defense of the Republic of Poland. Therefore, the activity characterized by the statutory criteria presents damage to national security and defense, i.e., concerns a particularly dangerous kind of espionage (Bafia, Mioduski, Siewierski, 1977, pp. 311–314; Popławski, 1983, pp. 28–33). For instance, one of the individuals sentenced under this provision to death *in absentia* was R. J. Kukliński, the deputy head of the Operations Administration of the General Staff of the Polish People's Army, and a US intelligence agent (Nurowska, 2004; Puchała, 2012, pp. 164–184; Krajewski, 2014, pp. 134–136).

The literal interpretation of the content of the prohibited act of espionage criminalized in Art. 130 of the Criminal Code of 1997 makes it

possible to divide it into different types – basic (§ 1), mitigated (§ 3), and aggravated (§ 2 and 4). The basic type criminalizes partaking in activity undertaken by a foreign intelligence service against the state of Poland. The aggravated type, as specified in § 2, criminalizes providing a foreign intelligence service with messages, the passing of which might harm the state of Poland, and where providing the said messages is related to playing a part in a foreign intelligence service or acting for the benefit thereof. The aggravated type, as specified in § 4, criminalizes the organization or management of a foreign intelligence service. In the mitigated type, the legislator criminalizes collecting or storing messages, the passing of which onto a foreign intelligence service might harm the state of Poland. Later on, the criminalization scope of the mitigated type was extended to include accessing the IT system to obtain messages, the passing of which onto a foreign intelligence service might harm the state of Poland. Next to collecting or storing specific messages or accessing the IT system, the mitigated type encompasses declaring oneself ready to act for the benefit of a foreign intelligence service (Art. 130, Journal of Laws 1997, no. 88, item 553; Gardocki, 2013, pp. 80–100). Hence, it can be seen that in reality, individual actions of the mitigated type of the offense of espionage constitute criminalized preparatory actions as *delictum sui generis*, or preparation specified regarding the code-regulated model (cf. Kunze, 1983, pp. 77–85; Kunze, 1990, pp. 89–97; Giezek, 2013, pp. 41–56; Małeck, 2016, pp. 262–266, 296–308).

## 1.2. Types of the Offense of Espionage and Their Statutory Criteria

In the basic type of the offense of espionage, the legislator criminalizes partaking in activity undertaken by a foreign intelligence service against the state of Poland. The crucial elements in the *ratione materiae* of this type of offense include “partaking in activity,” “foreign intelligence,” and “against the Republic of Poland.”

As for blaming the perpetrator for the offense, it is essential to properly assign the factual circumstances to the statutory criteria for a prohibited act. Undoubtedly, such a criterion as partaking may sometimes raise doubts about what factual circumstances may be connected with it (i.e., what *designata* may be regarded as belonging in the semantic scope of “partaking”). It is also worth indicating that with regard to the doctrinal remarks on the legislation in force in the context of the 1969 Code, the

legislator supplemented the criteria with partaking in activity by a foreign intelligence service – formerly, the legislator did not use the phrase “in activity.” The lack of this specific wording raised doubts about the understanding of partaking in a foreign intelligence service, e.g., whether it was about formal accession or any form of cooperation with a foreign intelligence service. The synonym of the term “partaking” is the word “participation,” so “partaking” denotes “participation” in some event. From the practical viewpoint, participation in foreign intelligence consists of performing tasks assigned based on the earlier agreement regarding the scope of intelligence activities. If there is no agreement in this scope, then the case is of a foreign intelligence representative instigating intelligence activity against the state of Poland (cf. Taras, 1970, pp. 10; Pikulski, 1987, pp. 65–134; Dukiet-Nagórska, 2018, pp. 368–371). Suppose the offer extended to a foreign intelligence service has been declined. In that case, we are dealing with the fulfillment of the statutory criteria for one of the mitigated types of espionage – declaring oneself ready to act for the benefit of foreign intelligence and against the state of Poland.

For the statutory criterion of partaking in, or participating, in foreign intelligence to be fulfilled, it is enough to perform one task set by a foreign intelligence service and targeted at the state of Poland. Noteworthy, the textual and doctrinal interpretations do not indicate the weight of this task, but only its being targeted at the state of Poland. Hence, fulfilling the statutory criteria for the basic type of espionage offense will consist of, e.g., carrying out an order to pick up a letter or parcel, passing information, operating contact points, and spreading disinformation in cyberspace. Undoubtedly, of relevance are theses by S. Pikulski, who in the legislation of the 1969 Code indicated that the fulfillment of the statutory criteria for partaking in the activity of a foreign intelligence service requires the following conditions: (1) the fact of establishing an agreement with a foreign intelligence service, (2) the fact of carrying out at least one task at the behest of a foreign intelligence service. Besides, partaking in foreign intelligence activity is also to be understood as formal affiliation, e.g., being an intelligence resident in the territory of Poland, or carrying out intelligence activities by foreign intelligence staffers (Pikulski, 1987, pp. 65–134; Mozgawa, 2017, pp. 431–433).

S. Pikulski pointed out, inter alia, the problem of the overlapping *ratione materiae* scopes of the criteria for partaking in foreign intelligence activity and organizing or managing foreign intelligence activity. From the logical perspective, there is no doubt that organizing and managing

are, after all, connected with partaking in foreign intelligence. However, what should distinguish the aggravated type, like organizing and managing, is the perpetrator's special manner of operating. While organizing is a (formal) offense with no criminal consequences, managing is a (material) offense with criminal consequences. It results from the fact that, for an offense to be committed, the organization of intelligence activity does not require a consequence in the form of constructing a functional structure to perform intelligence tasks. S. Hoc indicates that a person who creates and develops a spy ring and recruits new members can be recognized as an organizer. At this point, a problem arises concerning distinguishing organization from management because, among the statutory criteria, S. Hoc reckons assigning roles, issuing instructions, setting contact points, hiding spots, or transferring posts. The bulk of these activities can be directly associated with the criterion for management. Hence, it should be indicated that separating roles and functions, collecting information from other members, and further processing information to pass it on to the intelligence agency should be associated with the criterion for management and not organization. S. Hoc stresses that these criteria can be most often fulfilled by foreign intelligence residents, and currently most frequently by intelligence staffers at diplomatic posts (Pikulski, 1987, pp. 65–134; Hoc, 2002, pp. 74–77; Mozgawa, 2017, pp. 431–433; Dukiet-Nagórska, 2018, pp. 368–371). However, the case of Anna Chapman (aka Anna Vasilyevna Kushchenko) and other Russian illegals apprehended in the US in 2010 shows that the methods for operating residencies by civilians are not only characteristic of the early cold-war period in the 20th century. Nevertheless, in the mentioned case, the special services did not find evidence that all the apprehended Russian illegals knew one another, except for married ones. Besides, it is worth pointing out various assessments found in analyses of the activity of this spy group and the relationships between its members (*Suspected Russian...*, 2010; Lucas, 2012).

In assessing and understanding the criteria for participation, organization, and management of intelligence activity, attention should be focused on the development of ICT technologies that may affect the extension of their perception concerning new forms of transmission, aggregation, processing of data, and communication.

Commentators indicate that in the aggravated type criminalized in Art. 130 § 4, next to the criteria for organization and management, the legislator omitted activity targeted at the state of Poland. A literal interpretation only would result in an inconsistency between the content of

this type of offense and the contents in other clauses. The inconsistency would be that the types of espionage offenses with lower criminal sanctions would require activity against the state of Poland, while the type of espionage offense with the highest criminal sanction would not require such activity. Hence, as per the functional interpretation, it should be assumed that the legislator chose to criminalize the organization and management only of such activity targeted at the state of Poland (Hoc, 2002, pp. 74–77; Gardocki, 2013, pp. 96–99).

Another problematic criterion is partaking in foreign intelligence activity against the state of Poland. It means that it is not enough to participate in a foreign intelligence service or carry out tasks ordered by it, but this type of activity must be targeted at the state of Poland. It also means that participation in foreign intelligence that is not related to activity against Poland is beyond the bounds of criminalization under Art. 130 of the Criminal Code. Therefore, participation in, say, intelligence activity undertaken by Egypt against Israel does not meet the criteria set in the basic type of espionage offense (Gardocki, 2002, pp. 209–211; Hoc, 2002, pp. 64–65). It might raise doubts when the participant in the intelligence activity is a Polish citizen performing intelligence tasks in the territory of Poland. The doubt does not concern the ambiguous understanding of the provision but the citizen's attitude to the state of Poland. It is, therefore, worth considering whether the legislator should criminalize every kind of Polish citizen's cooperation with any foreign intelligence service, which might constitute a security mechanism protecting against possible exploitation of a Polish citizen in espionage activities. The axiological rationale in this respect is concerned with the citizen's obligations towards his or her homeland and internal and external state security considerations.

Next to the analyzed criteria concerned with "participation" and "acting for the benefit of foreign intelligence," attention should be drawn to the very category of "foreign intelligence." Not every legislator penalizes espionage activity so narrowly, narrowing the prohibited act down to activity undertaken for the benefit of a foreign intelligence service. A frequent practice is to cite not so much the category of intelligence but, for instance, the category of a foreign state or foreign authority (cf. Rosicki, 2018, pp. 180–201).

Understanding the very term 'intelligence' may, in some cases, raise doubts because we can speak about foreign (external) intelligence, internal one (counterintelligence), and criminal intelligence. Depending on



the state, special services may fall within any one of the three models, regarding the civilian and military specificity, or constitute mixed models. The Polish civilian counterintelligence furnishes a good example, i.e., the Internal Security Agency (abbreviated in Polish as ABW), which has the scope of activity encompassing both the issues typifying internal intelligence and criminal intelligence (cf. Minkina, 2014, pp. 27–208; Rosicki, 2016, pp. 165–176). One might, then, pose a question of whether cooperation with a typical criminal service of another state targeted at Poland meets the statutory criteria for the offense of espionage in the context of Art. 130 of the Criminal Code.

Another problem concerning the meaning of the term ‘intelligence’ might arise in a situation requiring consideration of its organizational and procedural character. In the former case, intelligence will be treated as a specific institution with a special type of organization, structure, and function. In the latter, it will present a special type of activity, independently of the institutional determinants. Both of these approaches have their drawbacks, as neither eliminate the ambiguity of the term ‘intelligence.’ As regards the organizational approach, the issues that will remain open to interpretation will include the degree to which intelligence must be institutionally related to a foreign state or the boundary between foreign intelligence or counterintelligence and criminal intelligence. In the procedural approach, the issues that will remain open to interpretation will include the kind of activities falling within the compass of intelligence activity and the kind of surveillance that needs to be recognized as intelligence activity. To sum up, as S. Hoc points out, the category of intelligence can be considered both narrowly, i.e., in the organizational aspect, and broadly, i.e., in the procedural aspect, as an element in the intelligence cycle. Besides, it needs to be emphasized that the intelligence cycle alone often constitutes the *definiens* of the terms ‘intelligence’ or ‘intelligence activity’. Still, there is no doubt that the question of what intelligence should be about has always given rise to heated debate among intelligence representatives and researchers. The problem is further compounded by the lack of an established theory, which is aptly illustrated by the words of K. Knorr, one of the researchers who in the 1960s wrote that there is no fully-developed theory of intelligence. Interestingly, there is still no well-established theory of intelligence nowadays, even though several decades have passed since the theses put forward by K. Knorr (cf. Knorr, 1964, pp. 46–47; Kent, 1965; Świda, 1977, p. 81; Hoc, 1979, p. 4; Pikulski, 1980, p. 80; Hoc, 1985, pp. 34–40, 67–91; Pikulski, 1987,

pp. 49–57; Johnson, 2003, pp. 1–28; Johnson, 2009, pp. 33–52; Minkina, 2014, pp. 27–208).

Like S. Pikulski, one should cite various approaches to intelligence, indicating that they were developed in the context of the previous legislation and political system. According to this author, the typology of intelligence makes it possible to distinguish the following meanings of it: (1) a state organ or an organ of an international institution (e.g., NATO), (2) all the activities concerned with providing information to state organs or organs of international institutions to increase security, but also to conduct such offensive activities as misinformation, subversion or any other forms of interference in the state's internal affairs, (3) activities most frequently classified and undertaken in the territory of foreign states, (4) activities involving special forms of communication (e.g., in older forms of espionage via hiding spots, safe houses, secret messages, codegrams, and radiograms), (5) activities carried out through special forms of collaboration with personal sources of information (e.g., via a spy network or infiltration of environments and institutions) (Pikulski, 1987, pp. 49–57).

As regards the aggravated type of the offense of espionage in the context of Art. 130 § 2, the legislator has criminalized providing an intelligence service with messages the passing of which may harm the state of Poland. It is noteworthy that in the legislation in force in 1970–1997, the legislator did not specify any characteristics of the message, which means that providing any information that a foreign intelligence service might need was criminalized. Therefore, the solution reduces the scope of criminalization of espionage activity, thereby referring to some extent to the criminalization of the offense of espionage in the legislation in force in 1946–1969. Back in that period, the criminalization applied to activity to the detriment of the state, i.e., collecting or passing messages and documents or other objects bound by state or military secrecy (Bafia, Mioduski, Siewierski, 1977, pp. 315–318). As regards the current legislation, potential harm to the state constitutes the relevant characteristic of the message. And so there is no necessity of passing information bound by special clauses, e.g., top-secret, secret, classified, or confidential. Still, the characteristic related to possible harm poses no mean challenge to the Polish counterintelligence combating espionage because it is ambiguous and open to doubt as to the extent in which it is to be measured objectively or subjectively. So the question is about the extent to which we are dealing with specific exposure to harm and to what extent the exposure is abstract. At the same time, it should be noted that it is not necessary to

demonstrate the factual occurrence of the harm specified in the provision because it is enough for such harm to be deemed possible (Gardocki, 2013, pp. 92–93; Dukiet-Nagórska, 2018, pp. 368–371). In a situation where messages passed do not bear such a characteristic, and the perpetrator was a part of foreign intelligence or acted for the benefit thereof, then the legal category of the perpetrator's act would be determined with Art. 130 of the Criminal Code.

The mitigated type of the offense of espionage with different types of acts refers to the solutions from the periods of 1946–1969 and 1970–1997. As regards the Decree of 1946, the legislator criminalized the establishment of an agreement by a Polish citizen with a person acting in the interests of a foreign government or a foreign organization acting to the detriment of the state of Poland, which was referred to as the offense of defecting to the enemy's side through establishing an agreement. Collecting messages, documents, or other objects that constitute a state or military secret was one of the forms of the offense of espionage. As regards the 1969 Criminal Code, the statutory criteria concerned with the mitigated type of espionage were similar to the ones used in the current legislation – with the proviso that the previous legislation featured verbal criteria of collecting instead of storing, as well as undertaking activity for the benefit of a foreign intelligence service instead of declaring oneself ready to act for the benefit thereof (see Art. 5 and 7, Journal of Laws 1946, no. 30, item 192; Art. 122, Journal of Laws 1969, no. 13, item 94).

Under the current legislation, the mitigated type formulates preparatory action into an autonomous type of the offense of espionage in four forms (*sui generis*). These include: (1) collecting specific messages, (2) storing specific messages, (3) accessing the IT system in order to obtain specific messages, (4) declaring oneself ready to act for the benefit of a foreign intelligence service and against Poland (see Art. 130 § 3, Journal of Laws 1997, no. 88 item 553). In each one of these four cases, the perpetrator needs to undertake activities with a view to a specific goal (i.e., with a directional intention – *dolus directus coloratus*), which is providing a foreign intelligence service with information the passing of which might be to the detriment of the Republic of Poland (cf. Sroka, 2014).

The messages that are collected, stored, or the perpetrator accesses the IT system to obtain them, are further specified as potentially detrimental to the state of Poland. Collecting messages is understood as obtaining (acquiring) them by all manner of means, both legal and illegal ones, regardless of whether they bear special clauses or not. The

legislator agreed to include the criterion concerned with storing messages because this action does not need to co-occur with collecting, e.g., when the person storing (holding) is not the same person as one acquiring espionage messages (a similar situation is one concerned with the statutory criteria for the offense of money laundering). Still, as S. Hoc points out, in the court practice both *sui generis* forms of the perpetrator's preparation are combined, i.e., the perpetrator collects specific messages and then stores them (Hoc, 2002, pp. 70–74; Gardocki, 2013, pp. 93–96; Mozgawa, 2017, pp. 431–433; Grześkowiak, Wiak, 2019, pp. 840–843). Later on, next to these preparatory forms, the legislator included a form based on accessing the IT system to obtain specific messages. In essence, the legislator criminalized any accessing the IT system, both legal and those that need to be reckoned among offenses against information security, e.g., hacking. At the same time, it needs to be stressed that this act is criminalized the moment the IT system is accessed and not at the stage of obtaining or becoming acquainted with the information the perpetrator is looking for.

The last form of the mitigated type of offense of espionage is declaring a readiness to act for the benefit of a foreign intelligence service. The actions in this offense consist in declaring, in any form and to foreign intelligence representatives, one's readiness to engage in cooperation against Poland. As regards classing this form of offense in the mitigated type as preparation *sui generis*, the doctrine is witnessing debate as to the manner of categorizing individual factual circumstances. One of the interpretations assumes that if declaring oneself ready is classed as preparation *sui generis*, then it should refer to one of the singled-out forms of preparation, i.e., establishing an agreement. For instance, if a perpetrator informed a Russian embassy about their willingness to cooperate with the Russian intelligence, but did not receive any reply, then according to this interpretation, there would be no establishment of agreement on account of non-acceptance, i.e., a lack of "agreement" between the two parties. Therefore, it would be impossible to assume that by sending his or her declaration of readiness, the perpetrator fulfilled the criteria for a prohibited act (cf. Judgement of the Appellate Court in Warsaw of 24.01.2008, II AKa 404/07; Pawela, 2003, pp. 105–106). However, in a different interpretation, it is assumed that the criteria for a prohibited act are met already at the stage of declaring oneself ready to act to a proper offer recipient, and so acceptance of the declaration on the part of a foreign intelligence service or its representative is not necessary (cf. Hoc, 2002,

pp. 70–74; Marek, 2010, pp. 347; Giezek, 2014, pp. 80–84; Wróbel, Zoll, 2017, pp. 138–155).

Regardless of the two directions of interpretation concerning the fulfillment of the criterion for declaring readiness, it needs to be noted that in the event of an ineffectual attempt at declaring oneself ready on account of a lack of the object of a prohibited act or on account of employing a measure unsuitable for the performance of a prohibited act – there are no grounds for invoking the legal category in Art. 130 § 3 of the Criminal Code. This assumption follows from the fact that there is no construct of ineffectual preparation, but only of an ineffectual attempt in the Polish criminal law – and as pointed out, the doctrine and jurisprudence treat Art. 130 § 3 as preparation *sui generis* (Małecki, 2016). It can be brought up for discussion whether if, despite declaring one's readiness, there is no response from a foreign intelligence service, we can speak about ineffectual preparation, on account of a lack of a proper measure to commit the act – that is the interpretation adopted by, inter alia, S. Paweła (2003, pp. 105–106). In this case, irrespective of the first and second interpretative direction concerning the fulfillment of the criterion for declaring readiness, it would not be possible to apply Art. 130 § 3 on account of the lack of the construct of ineffectual preparation under Polish law. This line of thinking should be termed a third interpretative direction related to the criterion for declaring readiness.

## **2. Characterization of the Offense of Espionage Illustrated with an Abstract Case Study**

### **2.1. General Assumptions Underlying the Case Study**

In order to perform an in-depth analysis, use is made of an abstract case study with no factual equivalent, i.e., no case subject to any court proceedings in Poland. Hence, the case study under analysis is a thought experiment intended to present selected problems concerned with applying the provision criminalizing the offense of espionage and with the legal classification of actual states. The content of the case under analysis is as follows:

“In 2019 the Department of Political Science at the University of Poznań (abbreviated as WNP UP) played host to a few days' academic conference organized by several research and science

institutes from Germany, Poland, and Russia. The conference brought together a group of people specializing in international and internal security. The issue that sparked the most intense debate was energy security in the relations between Poland, Germany, and Russia. The conference was attended by, inter alia, prof. Koch, prof. Starak and prof. Walewicz, all employees of WNP UP. There were also guests from Germany and Russia, inter alia, dr Mikhail Varshavsky, a colleague of prof. Koch – they both studied in Moscow, where they took their doctor's degrees at the Lomonosov State University (МГУ – MGU). Prof. Koch knew about the personal animosity between prof. Starak and prof. Walewicz. The two colleagues of prof. Koch were vying for the Chair of Transatlantic Relations. Prof. Koch also knew about prof. Walewicz's financial problems, so he decided to use a ploy to get rid of the disliked prof. Walewicz who wrote a negative review of his Ph.D. student's doctoral dissertation. He concluded that the best method would be to disgrace his colleague, preferably in the context of some offense. Prof. Koch knew that dr M. Varshavsky was working for the Foreign Intelligence Service of the Russian Federation (Russian: Служба Внешней Разведки Российской Федерации), and that earlier he had acted as a GRU (Russian: Главное разведывательное управление Генерального штаба Вооружённых сил Российской Федерации) analyst.

In a meeting between conference sessions, prof. Koch encouraged prof. Starak to mention prof. Walewicz's financial problems and introduce dr M. Varshavsky to him. Prof. Koch acquainted prof. Starak with dr M. Varshavsky's informal position, suggesting that he might try and encourage prof. Walewicz to cooperate with the intelligence service of the Russian Federation for money, which might help him solve his financial problems. Casually and craftily, he added that if prof. Starak's aversion to prof. Walewicz was so strong, then he might notify the Polish special services as soon as he learned that prof. Walewicz had already entered into a collaboration.

Exhilarated by his colleague's advice and the relaxed atmosphere of the meeting, prof. Starak decided to act on the advice by the end of the conference. The next day he approached prof. Walewicz and brought up the subject of cooperation with the Russian intelligence service, planting in his mind an idea that such a move might prove to be the panacea for all his financial problems.

On the very same day, after the conference meeting, prof. Walewicz met his life partner, dr Ksenewicz, told her about the matter, and concluded that he had made up his mind because it was worth a try. Dr Ksenewicz did not have a problem with that – after

all, she would break up with prof. Walewicz anyway, having had enough of him. Still, she told her partner the following: “why not, you can do it, and you’ll make enough money to go on holiday in the Dominican Republic.”

On the third and last day of the conference, at a table in one of the restaurants in Poznań Old Market Square, where the conference’s concluding sessions were held, prof. Walewicz spoke to dr M. Varshavsky, made him an offer of work, i.e., cooperation for the benefit of the Russian intelligence. Surprisingly, Varshavsky admitted having worked for the services, which he by no means tried to hide, but by his account, he had never been involved with recruitment or work against the eastern bloc countries and only worked in the capacity of a strategy data analyst. Furthermore, for a long time now, he had not worked for the Russian services, and so could do nothing to help prof. Walewicz. Prof. Walewicz turned red and asked Varshavsky to forget about the whole matter like they had never had the conversation.

But the matter was not forgotten by the Polish counterintelligence service because prof. Koch, prof. Starak, prof. Walewicz, dr Ksenewicz, and dr Varshavsky were subsequently placed under arrest due to a counterintelligence operation and based on the evidence obtained and recorded in the process of operational surveillance.”

The presented story, which concerns individuals engaging in what might fulfill the criteria for various types of offense, is elaborate, and so the individual cases require the establishment of the actual states, legal problems, legal grounds, legal interpretation, and eventually legal classification (association of the facts with legal norms).

## 2.2. Legal Assessment of the Individual Characters’ Acts in the Case Study

The case study under consideration presents the behavior of five persons – prof. Koch, prof. Starak, prof. Walewicz, dr Ksenewicz and dr Varshavsky. It is noteworthy that next to the application of the provision criminalizing the offense of espionage, the analysis needs to take into account and consider the legitimacy of including in the legal classification forms of accessory liability and stages of commission.

The first person whose behavior needs to be considered is prof. Koch, the driving spirit behind further behavior of the other characters in the case study. Consideration of prof. Koch’s behavior leads to the conclu-

sion that he tries to exert some influence on prof. Starak, who in turn is supposed to influence prof. Walewicz's behavior. Prof. Koch's behavior can therefore be seen as urging directed at prof. Starak, who in turn is expected to urge prof. Walewicz to at least partakes in foreign intelligence activity, i.e., commit an act prohibited under Art. 130 § 1 of the Criminal Code. According to the Polish Criminal Code, urging a person to commit a prohibited act constitutes an offense of instigation (Art. 18 § 2). According to the Polish Criminal Code (Art. 24), urging a person to commit a prohibited act to have criminal proceedings directed against them constitutes an offense of incitement. Therefore, this juncture calls for the establishment of the actual state and the legal problem concerned with the offense of instigation and incitement.

Undoubtedly, prof. Koch urges prof. Starak to urge prof. Walewicz to fulfill the criteria for a prohibited act criminalized at least in Art. 130 § 1 of the Criminal Code. Both the urgings fulfill the condition of individualization, i.e., the realization of influence concerning the person and the act – the individualization is visible both in the relationship between prof. Koch and prof. Starak, as well as prof. Starak and prof. Walewicz. Given the distinction between instigation and incitement, it ought to be assumed that prof. Koch instigates incitement to the offense of espionage (an act oriented directly at prof. Starak) while prof. Starak, through his act, fulfills the criteria for incitement to the basic type of the offense of espionage (an act oriented directly at prof. Walewicz). Regarding the act performed by prof. Koch, Polish criminal law features an important issue, i.e., the admissibility of the so-called chain instigation in the legal classification of an act. Generally, it is assumed that it is possible to apply legal classification based on the construct of instigation to instigation, but also instigation to incitement or instigation to aiding and abetting (Kulik, 2013, pp. 127–143; Tokarczyk, 2017b; Pohl, 2019, pp. 202–211; Bojarski, 2020, pp. 288–292).

The doctrine also raises the problem of the moment at which the criterion for urge is fulfilled. By extension, one can point to different moments at which this criterion is fulfilled – (1) the moment at which urging is over, (2) the moment an intention to commit an offense has been instilled in another person, (3) the moment at which the act has been performed, or an attempt at performing the act has been made by the instigated person (who has already been urged on). Generally, the basis for distinguishing between these three concepts lies in a specific attitude of the doctrine towards the effectiveness of urging (i.e., whether instigation or incitement



is with or without consequences) (Pohl, 2001, pp. 67–74; Kulik, 2013, pp. 127–143; Tokarczyk, 2017b, pp. 225–300; Pohl, 2019, pp. 202–206; Mozgawa, 2020, pp. 397–399, 404).

Accepting that instigation or incitement either has consequences or has no consequences results in various legal classifications of the act. For instance, in the no-consequence concept instigation of the offense of espionage without the instigated person yielding to it, the legal classification of the act will follow Art. 18 § 2 (instigation) in conjunction with Art. 130 § 1 (the basic form of espionage) of the Criminal Code, while in the concept with consequences – Art. 13 § 1 (an attempt) in conjunction with Art. 18 § 2 (instigation) in conjunction with Art. 130 § 1 (the basic type of espionage) of the Criminal Code. Regarding the assessment of the actions performed by prof. Koch and prof. Starak, it is noteworthy that regarding the former, the proper legal classification of the act is Art. 18 § 2 (instigation) in conjunction with Art. 24 (incitement) in conjunction with Art. 130 § 1 (the basic type of espionage) of the Criminal Code. Regarding the latter one, the proper legal classification of the act is Art. 24 (incitement) in conjunction with Art. 130 § 1 (the basic type of espionage) of the Criminal Code.

We can also consider a situation in which prof. Walewicz does not undertake an activity for the benefit of a foreign intelligence service despite prof. Starak's incitement, but we want to adopt the criminal-consequence concept of instigation or incitement. In a case like this, for prof. Starak, the proper legal classification of the act is Art. 13 § 1 (an attempt) in conjunction with Art. 24 (incitement) in conjunction with Art. 130 § 1 (the basic type of espionage) of the Criminal Code. If prof. Starak had not performed the act, which was the subject of instigation on the part of prof. Koch, then the proper legal classification of the act for prof. Koch would be Art. 13 § 1 of the Criminal Code (an attempt) in conjunction with Art. 18 § 2 (instigation) in conjunction with Art. 24 (incitement) in conjunction with Art. 130 § 1 (the basic type of espionage) of the Criminal Code.

It is also worth considering the relationship between prof. Walewicz and dr Ksenewicz. Above all, it is noteworthy that in connection with the urging by prof. Starak, prof. Walewicz took the decision, i.e., willingness to commit the offense was aroused in him. In the conversation with his partner, prof. Walewicz becomes reinforced in his resolve, thereby confirming his intention to commit a prohibited act or in his decision to commit it. There may be a problem in the doctrine concerned with the dis-

inction between instigation and aiding and abetting as two forms of accessory liability. In general, dr Ksenewicz's words are a form of urging, but at the same time, they can be defined as mental aiding and abetting in the commission of the offense (cf. Pohl, 2019, pp. 206–209; Bojarski, 2020, pp. 288–297; Mozgawa, 2020, pp. 399–403). Mental aiding and abetting can be substantiated because dr Ksenewicz does not evoke the intention to commit the offense of espionage, which is what prof. Starak did, and she only keeps up prof. Walewicz's intention. At the same time, dr Ksenewicz is aware that her life partner intends to or has decided to commit a prohibited act. In this case, the proper legal classification of the act committed by dr Ksenewicz is Art. 18 § 3 (the mental form of aiding and abetting) in conjunction with Art. 130 § 1 (the basic type of espionage) of the Criminal Code.

One might also consider a situation in which dr Ksenewicz urges her partner on, unaware that he has already made the final determination to commit the offense of espionage. According to Ł. Pohl, in a situation where a person has been previously and objectively reinforced in their intention or decision to commit a prohibited act, without the reinforcing person's knowledge of that, the objectively reinforcing person ought to be treated as one ineffectually attempting to instigate a given act; e.g., regarding the offense of espionage, the act committed by the reinforcing person should be associated with the legal classification under Art. 13 § 2 of the Criminal Code (an ineffectual attempt) in conjunction with Art. 18 § 2 (instigation) in conjunction with Art. 130 §1 (the basic type of espionage) of the Criminal Code (cf. Pohl, 2001, pp. 67–74; Kulik, 2013, pp. 127–143; Tokarczyk, 2017a, pp. 95–106; Pohl, 2019, pp. 202–209).

Prof. Walewicz's behavior concerning the influence directly exerted on him by prof. Starak and dr Ksenewicz consists in aiming to realize participation in foreign intelligence activity against Poland. However, his actions stop at the stage of declaring his readiness to act for a foreign intelligence service, which comes to be expressed in extending a specific offer to dr Varshavsky. The doctrinal problem concerned with the criterion for declaring readiness was discussed earlier, so here it is only worth mentioning the interpretations of the declaration of readiness may go in three directions: (1) declaring readiness as preparation *sui generis* in reference to one of the forms of preparation – establishing an agreement with another person (for the perpetrator to be liable there needs to be a mutual agreement), (2) declaring readiness as preparation *sui generis* (the perpetrator's liability does not require mutual agreement), (3) declar-

ing readiness as preparation *sui generis* in reference to one of the forms of preparation – establishing an agreement with another person (the perpetrator is not held liable in a situation in which there has been no mutual agreement on account of non-criminalization of ineffectual preparation).

As for prof. Walewicz, it is noteworthy that he offered cooperation, directed at dr Varshavsky. The person he chose to be the recipient of his offer had been a special services operative for a foreign state, even though now he no longer performed this function, and earlier had not been engaged in direct intelligence activity against the state of Poland, because he had only acted as an analyst for the Russian intelligence. Therefore, there remains the question of whether prof. Walewicz's behavior fulfilled the criteria for declaring readiness under Art. 130 § 3 of the Criminal Code. It results from choosing a person incompetent as regards the further proceedings concerned with looking into intelligence cooperation. Therefore, prof. Walewicz's offer did not reach a proper person or organ related to the Russian intelligence.

In consequence, while assessing prof. Walewicz's behavior, it needs to be indicated that he does not realize that the commission of a criminal act is impossible because of a lack of an object of a prohibited act – in this situation, the object of the offense committed is dr Varshavsky, the supposed Russian intelligence operative. This situation directly corresponds to the criteria for an ineffectual attempt under the Polish law, Art. 13 § 2 of the Criminal Code. However, the doctrine provides that the content of Art. 130 § 3 of the Criminal Code is entirely concerned with preparation *sui generis*, while under Polish criminal law, the construct of ineffectual preparation is impossible. As a result of these findings, it needs to be assumed that prof. Walewicz cannot be brought to justice on criminal charges under Art. 13 § 2 of the Criminal Code. The situation would be different within the legislation in force in 1970–1997. At the same time, if the concept with criminal consequences were to be adopted with regard to instigation and incitement, then it would be necessary to consider appropriate changes to the legal classification of the acts performed by the persons earlier accused of such offenses (on the grounds of ineffectuality as a criterion).

The last person whose behavior needs to be considered is dr Varshavsky. Undoubtedly, he used to work for a foreign intelligence service, but – as mentioned before – he was not involved in any activity targeted at Poland, or at least the presented facts do not allow such an interpretation. In a situation like this, no charges can be pressed against dr Varshavsky in

the context of the non-fulfillment of the criteria for any prohibited activities related to espionage.

### Conclusion

The subject of analysis is the problem concerned with the content and sense of the statutory criteria for the offense of espionage criminalized under Art. 130 § 1–4 of the Polish Criminal Code. The institutional and legal analysis is performed with textual, functional, and historical interpretations, supplemented with the author's conclusions and opinions. The institutional and legal analysis is also enriched with an abstract case study constituting a thought experiment. The thought experiment is necessary for considering selected legal problems and legal classifications of the described acts related to espionage activity.

There is no doubt that the offense of espionage poses a threat to state security. Within the characterization of the offense of espionage, state security constitutes a protected interest because this kind of offense is reckoned among offenses against the state. According to the doctrinal approach, the interest protected by the criminalization of espionage is exactly the internal and external state security. The state defense system is also indicated as the protected interest. Therefore, identifying threats to state security related to assessing the effectiveness of the law in force and the law in the making concerning espionage activity constitutes an important dimension of analysis in security studies. In order to elaborate the material scope of the analysis and to present the conclusions in the text, the following research questions have been formulated:

***(1) To what extent are the de lege lata legal solutions in Poland effective in counteracting espionage offenses?***

With regard to the analysis of the offence of espionage in the context of the legislation in force, attention should be focused on the following problems that might affect the effectiveness of counteracting espionage offences in Poland: (a) the use by the Polish legislator of the category “intelligence” which significantly narrows espionage acts down to activity for the benefit of a specific entity, (b) the use by the Polish legislator of the category “intelligence” that may be vague because of various ways in which to understand it in the context of the studies of intelligence, (c) the use by the Polish legislator of the category “messages” characterized by

the potential for damage, which gives rise to the problem concerned with the assessment of the character of a threat to interests (an abstract or concrete threat), (d) the use by the Polish legislator of the category “messages” whose characteristic is the potential for harm, which gives rise to the problem concerned with the assessment of harm itself (subjectivization and objectivization of damage), (e) the use by the Polish legislator, for the criminalization of one of the mitigated types of the offence of espionage, of the criteria with non-uniform interpretation in the doctrine (“declares readiness to act for the benefit of a foreign intelligence service”).

***(2) What de lege ferenda solutions ought to be proposed to improve effective counteraction of espionage offenses?***

With regard to the identification of the problems within the analysis of the effectiveness of the law in force and the law in the making concerning espionage activity, as well as within the abstract case study, attention should be focused on the following remarks, the consideration of which may give rise to improved effectiveness of the counteraction of espionage offences in Poland: consideration should be given to (a) replacing the category of “intelligence” with, for instance, a foreign state or a foreign authority, (b) whether to criminalize participation in any foreign intelligence service, which can be axiologically grounded in the citizen’s obligations towards his or her homeland and state security (criminalization might consist in distinguishing two different types of espionage connected with participation in foreign intelligence activity or activity for the benefit of a foreign state – against Poland and without indicating activity against Poland), (c) whether to criminalize passing any messages to a foreign intelligence service (criminalization might consist in distinguishing two different types of espionage connected with transferring messages – any messages and messages bound by special clauses), (d) whether to change criminalization of the mitigated type of espionage offence in the form of declaring readiness to act for the benefit of a foreign intelligence service or state (the change might consist in criminalizing the act not as preparation sui generis, but at least as an attempt sui generis, which would enable criminalization of, say, an ineffectual attempt), (e) whether to change the scope of criminalization of individual forms in the mitigated type of espionage offence with regard to new threats and technological changes taking place in society, (f) whether to criminalize specified forms of espionage offence in relation to the breach of the principle of caution, (g) whether to criminalize acts consisting in public misinformation on

a specific scale, (h) whether to criminalize illegal foreign support, e.g., in the form of illegal material support, illegal support of agents of influence, or illegal influence exerted on the public opinion in matters of essential significance for the state.

The selection of the presented proposals for changes to the scope of criminalization of acts related to espionage activity *sensu largo* should include goals to be attained in the penal policy serving the state security. Besides, while making the changes, one should weigh the state interests and individual interests so that the new law is not repressive or does not interfere with citizens' lives through excessive criminalization and penalization. From the systemic viewpoint, consideration should be given to comprehensive changes allowing for the relationship between the offense of espionage and the offenses against information security (inter alia, those classed as the so-called cyber-terrorism).

### Bibliography

- Act of 19 April 1969 – *The Criminal Code*, Journal of Laws 1969, no. 13, item 94.
- Act of 6 June 1997 – *The Criminal Code*, Journal of Laws 1997, no. 88, item 553, as amended.
- Aichele G., Phillips G. A. (1995), *Introduction: Exegesis, Eisegesis, Intergesis*, “*Se-meia*”, no. 69–70.
- Andrejew I. (1978), *Kodeks karny. Komentarz*, PIW, Warszawa.
- Announcement by the President of the State Council of 16 February 1976 on the publication of the consolidated text of the Constitution of the Polish People's Republic passed by the Legislative Sejm on 22 July 1952, Journal of Laws 1976, no. 7, item 36.
- Bafia J., Mioduski K., Siewierski M. (1977), *Kodeks karny. Komentarz*, WP, Warszawa.
- Bojarski M. (ed.) (2020), *Prawo karne materialne. Część ogólna i szczególna*, Kluwer, Warszawa.
- Constitution of the Polish People's Republic passed by the Legislative Sejm* (legislature) on 22 July 1952, Journal of Laws 1952, no. 33, item 232, as amended.
- Decree of 13 June 1946 *on crimes posing especial danger in the period of the reconstruction of the State*, Journal of Laws 1946, no. 30, item 192.
- Dukiet-Nagórska T. et al. (eds.) (2018), *Prawo karne. Część ogólna, szczególna i wojskowa*, Kluwer, Warszawa.
- Gardocki L. (2002), *Prawo karne*, C.H. Beck, Warszawa.
- Gardocki L. (ed.) (2013), *System prawa karnego. Przestępstwa przeciwko państwu i dobrom zbiorowym*, vol. 8, C.H. Beck, Warszawa.

- Giezek J. (2013), *Formy stadialne popełnienia czynu zabronionego w polskim prawie karnym*, "Annales Universitatis Mariae Curie-Skłodowska, sectio G", vol. LX, no. 2.
- Giezek J. (ed.) (2014), *Kodeks karny. Część szczególna. Komentarz*, Kluwer, Warszawa.
- Gill P., Marrin S., Phythian M. (eds.) (2009), *Intelligence Theory: Key Questions and Debates*, Routledge, London.
- Grześkowiak A., Wiak K. (eds.) (2019), *Kodeks karny. Komentarz*, C.H. Beck, Warszawa.
- Hoc S. (1979), *Szpiegostwo w socjalistycznym prawie karnym*, "Wojskowy Przegląd Prawniczy", no. 1.
- Hoc S. (1985), *Zagadnienia odpowiedzialności karnej za szpiegostwo*, ASW, Warszawa.
- Hoc S. (2002), *Przestępstwa przeciwko Rzeczypospolitej Polskiej*, UO, Opole.
- Hoc S. (2019), *Wymiana agentów wywiadu – aspekty prawne i polityczne*, "Studia Prawnoustrojowe", no. 44.
- Johnson L. K. (2003), *Bricks and Mortar for a Theory of Intelligence*, "Comparative Strategy", vol. 22.
- Johnson L. K. (2009), *Sketches for a theory of strategic intelligence*, in: *Intelligence Theory: Key Questions and Debates*, eds. P. Gill, S. Marrin, M. Phythian, Routledge, London.
- Judgment of the Appellate Court in Warsaw of 24 January 2008 (II Aka 404/07).
- Kent S. (1965), *Strategic intelligence for American world policy*, Archon Books, Hamden.
- Knorr K. (1964), *Foreign Intelligence and the Social Sciences*, Princeton University, Princeton.
- Krajewski A. (2014), *Zasluga dla Polski. Pułkownik Kukliński opowiada swoją historię*, E-bookowo, Warszawa.
- Kuczur T. (2012), *Przestępstwa polityczne w uwarunkowaniach systemowych Polski XX wieku*, WUKW, Bydgoszcz.
- Kulik M. (2013), *Formy zjawiskowe popełnienia przestępstwa w polskim prawie karnym*, "Annales Universitatis Mariae Curie-Skłodowska, sectio G", vol. LX, no. 2.
- Kunze E. (1983), *Przygotowanie przestępstwa w jugosłowiańskim prawie karnym*, "Ruch Prawniczy, Ekonomiczny i Socjologiczny", no. 4.
- Kunze E. (1990), *Karalne postacie przygotowania przestępstwa w polskim prawie karnym*, "Ruch Prawniczy, Ekonomiczny i Socjologiczny", no. 3–4.
- Lucas E. (2012), *Deception: Spies, Lies and How Russia Dupes the West*, Bloomsbury, New York.
- Małecki M. (2016), *Przygotowanie do przestępstwa. Analiza dogmatycznoprawna*, Kluwer, Warszawa.

- Marek A. (2010), *Kodeks karny. Komentarz*, Kluwer, Warszawa.
- Mozgawa M. et al. (eds.) (2017), *Kodeks karny. Komentarz*, Kluwer, Warszawa.
- Mozgawa M. (ed.) (2020), *Prawo karne materialne. Część ogólna*, Kluwer, Warszawa.
- Nowacki J., Tabor Z. (2016), *Wstęp do prawoznawstwa*, Kluwer, Warszawa.
- Pawela S. (2003), *Rec.: S. Hoc, Przestępstwa przeciwko Rzeczypospolitej Polskiej, Opole 2002*, "Państwo i Prawo", no. 2.
- Pikulski S. (1980), *Sporne zagadnienia w wykładni unormowania przestępstwa szpiegostwa w kodeksie karnym PRL z 1969 r.*, "Wojskowy Przegląd Prawniczy", no. 1.
- Pikulski S. (1987), *Przestępstwo szpiegostwa w teorii i praktyce*, DSziDZ MSW, Warszawa.
- Pohl Ł. (2001), *Formy stadialne czynu zabronionego w odniesieniu do podżegania i pomocnictwa według kodeksu karnego z 1997 r.*, "Ruch Prawniczy, Ekonomiczny i Socjologiczny", vol. LXIII, no. 1–2.
- Pohl Ł. (2019), *Prawo karne. Wykład części ogólnej*, Kluwer, Warszawa.
- Popławski H. (1983), *Zbrodnia zdrady ojczyzny. Zbrodnia szpiegostwa*, WP, Warszawa.
- Puchała F. (2012), *Pułkownika Kuklińskiego udział w grze wywiadów wielkich mocarstw*, "Przegląd Historyczno-Wojskowy", no. 4.
- Rosicki R. (2016), *Poland's internal security as exemplified by the tasks and activities of the Internal Security Agency in the period 2007–2015*, "Przegląd Polityczny", no. 1.
- Rosicki R. (2018), *Information security as exemplified by the crime of espionage in the Polish and Swedish criminal law*, "Studia Polityczne", vol. 49.
- Sroka T. (2014), *Kodeks karny. Wybór orzecznictwa. Komentarz orzeczniczy*, Kluwer, Warszawa, <http://lex-1amu-1edu-1pl-1015e98wh01f0.han.amu.edu.pl/#/commentary/587375108/172548%20>, 18.02.2021.
- Suspected Russian spies charged in US* (2010), <https://www.bbc.com/news/10442223>, 29.06.2010.
- Świda W. (ed.) (1977), *Kryminologia*, PWN, Warszawa.
- Taras T. (1970), *Przestępstwo szpiegostwa w świetle nowego kodeksu karnego z 1969 r.*, "Palestra", no. 3.
- Tokarczyk D. (2017a), *Podżeganie i pomocnictwo jako typy zjawiskowe przestępstwa*, "Ruch Prawniczy, Ekonomiczny i Socjologiczny", no. 4.
- Tokarczyk D. (2017b), *Podżeganie w polskim prawie karnym. Studium z zakresu teorii i praktyki prawa karnego*, C.H. Beck, Warszawa.
- Wronkowska S. (2005), *Podstawowe pojęcia prawa i prawoznawstwa*, Ars boni et aequi, Poznań.
- Wronkowska S., Ziemiński Z. (1997), *Zarys teorii prawa*, Ars boni et aequi, Poznań.
- Wróbel W., Zoll A. (eds.) (2017), *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117–211a*, Kluwer, Warszawa.



Zieliński M. (1998), *Wyznaczniki reguły wykładni prawa*, "Ruch Prawniczy, Ekonomiczny i Socjologiczny", no. 3–4.

---

## Bezpieczeństwo państwa na przykładzie przestępstwa szpiegostwa w polskim prawie

### Streszczenie

Zakres przedmiotowy problemu badawczego w tekście obejmuje wybrane kwestie dotyczące treści i znaczenia elementów charakteryzujących przestępstwo szpiegostwa w polskim prawie karnym. W obecnym stanie prawnym przestępstwo szpiegostwa kryminalizowane jest na gruncie art. 130 § 1–4 Kodeksu karnego. Głównym celem podjętej analizy jest dokonanie karnomaterialnej analizy przestępstwa szpiegostwa w polskim prawie z uwzględnieniem praktycznego studium przypadku, a także oceny rozwiązań prawnych ze względu na bezpieczeństwo państwa. W celu uszczegółowienia zakresu przedmiotowego problemu badawczego i prezentacji wniosków w tekście przedstawiono następujące pytania badawcze: (1) W jakim zakresie rozwiązania prawne *de lege lata* w Polsce są efektywne w zwalczaniu przestępstw szpiegostwa?, (2) Jakie rozwiązania prawne *de lege ferenda* należy zaproponować w celu zwiększenia efektywności zwalczania przestępstw szpiegostwa? Analiza zawarta w tekście ma charakter poglądowy, w ramach niej wykorzystano głównie analizę instytucjonalno-prawną za pomocą interpretacji tekstualnej, funkcjonalnej i historycznej, które uzupełnione zostały własnymi wnioskami i opiniami dotyczącymi rozwiązań prawnych *de lege lata* i *de lege ferenda*. Analiza instytucjonalno-prawna uzupełniona została o abstrakcyjne studium przypadku czynności szpiegowskich. Zaprezentowane abstrakcyjne studium przypadku pomocne jest do prowadzenia rozważań nad wybranymi problemami prawnymi i w końcowym efekcie prezentacji przykładowych kwalifikacji prawnych opisanych w nim czynów związanych z działalnością szpiegowską.

**Słowa kluczowe:** bezpieczeństwo państwa, bezpieczeństwo informacji, szpiegostwo, przestępstwo szpiegostwa, działalność wywiadowcza

