DOI : 10.14746/pp.2024.29.3.1

Remigiusz ROSICKI
Adam Mickiewicz University in Poznań
https://orcid.org/0000-0002-1187-5895

# Criminal Policy on Prevention and Combating of Espionage Activity in Poland. An Aanalysis Illustrated with the Statutory Amendments Adopted in 2023

**Abstract:** The research problem addressed in the text concerns the criminal policy concerned with preventing and combating espionage offences in Poland in 1998–2023. A criminal policy is understood as a particular form of legal policy, encompassing the programming of anti-crime measures through penalties and other legal measures, criminalisation and decriminalisation regulations, and the deliberate creation of penal provisions. The main objective of the analysis is to juxtapose the previous legislation with the new legal solutions criminalising and penalising further types of espionage, which were introduced in 2023. The consequence of the comparative purpose thus defined is the presentation of an assessment of the new solutions from the perspective of penal policy. The analysis is based on two approaches: the dogmatic and the historical-comparative one. The dogmatic approach focuses on the analysis of the penal law provisions themselves and their interpretation, while the historical-comparative approach juxtaposes the current provisions with the earlier changes following the diachronic perspective. The study aims to answer questions about the differences between the current and previous legislation concerned with the criminalisation of espionage, and to assess the effectiveness of the 2023 amendments.

**Key words:** criminal policy, offences against the state, espionage, espionage activity, counter-intelligence

## Introduction

The research problem addressed in the text concerns the criminal policy concerned with preventing and combating espionage offences in Poland in 1998–2023. A criminal policy should be understood as a specific type of legal policy involving the programming of the prevention and combating of crime by means of penalties and other criminal law measures, the penalisation and depenalisation of acts, as well as the deliberate creation of criminal law regulations – mainly by means of the criminalisation of acts – which lends them the characteristic of legal relevance (cf. Gardocki, 1990; Wójcik, 2014, pp. 62–101; Warylewski, 2017, p. 75; Kulesza, 2023, pp. 33–35). A criminal policy is intended to fulfil the basic functions of penal law, which include: the protection function (protection against the violation of legal interests), the guarantee function (the guarantee implied by the principles: *nullum crimen sine lege* and *nulla poena sine lege*), the justice function (retribution for the violation of legal interests by means of adequately holding the perpetrator liable) and the prevention function (prevention of and reduction in the recurrence of legally relevant acts) (cf. Warylewski, 2007, pp. 62–69; Pohl, 2019, pp. 30–43; Mozgawa, 2020, pp. 28–31; Bojarski, 2020, pp. 30–34; Kulesza, 2023, pp. 39–46). A penal policy itself, on the other hand, as part of criminal policy, covers such problems as:

(1) laying down the penal law, (2) applying the penal law, (3) assessing the effects of the laid-down and applied law, (4) assessing the effectiveness of the laid-down and applied law (Lande, 1958, pp. 229–265; Podgórecki, 1962, pp. 122–190; Ziembiński, 1975, pp. 123–141; Pikulski, 2009, pp. 13–21; Stańdo-Kawecka, 2020, pp. 11–43).

The content of the analysis undertaken in the text is concerned with the solutions adopted by the Polish legislator with regard to the criminalisation of the prohibited act defined by the doctrine as espionage, i.e. the content of Article 130 of the Penal Code in force since 1998. This analysis also takes into account the changes to the penalisation and criminalisation of the offence of espionage, which came into force on 1 October 2023 (Article 130, Journal of Laws 1997, no. 88, item 553, as amended; Journal of Laws 2023, item 1834). In order to present the processes concerned with the criminal policy in a more insightful manner, the analysis takes into account selected issues concerning the change in the scope of criminalisation arising during the legislative work initiated by the submission of the *Parliamentary bill amending the Act – the Penal Code and certain other acts of* 17 April 2023 (*Parliamentary bill*..., EW-020-1196/23; Paper no. 3232; *Own amendment*..., Paper no. 3232-A; *Supplementary report...*, Paper no. 3358; *Supplementary report...*, Paper no. 3358-A; *Resolution...*, Paper no. 3553; *Report...*, Paper no. 3596; Journal of Laws 2023, item 1834).

The main purpose of the analysis is to juxtapose the new legal solutions, which criminalise further types of espionage, and which were introduced in 2023, with the legislation in force previously. The consequence of the comparative purpose thus adopted is the presentation of an assessment of the new solutions from the perspective of penal policy, i.e. mainly in the context of: (1) laying down the penal law, (2) assessing the effects of the laid-down and applied law, (3) assessing the effectiveness of the laid-down and applied law. In order to elaborate the objective scope of the research problem, the following questions have been presented in the text: (1) *What are the differences between the legislation concerned with the criminalisation of the offence of espionage under Article 130 of the Penal Code introduced in 2023 and the previous legislation also regarding Article 130 of the Penal Code?*, (2) *What is the effectiveness of the 2023 changes with regard to the criminalisation of the offence of espionage under Article 130 of the Penal Code?*

The following approaches have been used to analyse the two types of legislation: the dogmatic and the historical-comparative one. The dogmatic approach justifies citing, in a descriptive form, the legal solutions as established by the legislator, along with the practices of their application. The main elements of the prohibited acts (the subject of the offence, the subjective side, the objective side, and the object of the offence) will be analysed. The dogmatic approach itself assumes reliance on legal interpretations, which include linguistic and functional interpretations. The historical-comparative approach, on the other hand, is based on the juxtaposition of the legal solutions present in the content of Article 130 of the Penal Code, which have been in force since 1998, with the amendments adopted in 2023, allowing for the perspective of following the diachronic logic of the changes (for more on this see Ankersmit, 1983; Wronkowska, Ziembiński, 1997, pp. 147–179; Dubber, 1998, pp. 159–162; Zielińsk, 1998, pp. 1–20; Samuel, 2014, pp. 57–60; Pohl, 2019, pp. 77–84; Bekrycht, Leszczyński, Łabieniec, 2021, pp. 187–215).

## 1. Legal solutions with regard to espionage activity in Poland in 1998–2023

The new codification of the penal law, which resulted in the entry into force of the Penal Code in 1998, prepared amendments to replace the legal regulations laid down in the late 1960s, under the conditions of the Polish People’s Republic. The new socio-economic and political conditions forced a change in the philosophy of criminal policy, which also came to be reflected in the changes concerning offences against the state, including the offence doctrinally referred to as “espionage” (for more on this see Kuczur, 2012; Kuczur, 2020a, pp. 301–331; Kuczur, 2020b; Kuczur, 2020c, pp. 57–78). Despite the changes, if only in the extent of penalisation, it must be said that the changes to the criminalisation of the offence of espionage, introduced in 1998, fall within the compass of the diachronic legislative logic evinced by the then legislator.

A literal reading of the content of the prohibited act criminalised under Article 130 of the 1997 Penal Code makes it possible to distinguish its various types – the basic type (§ 1) and two aggravated types (§ 2 and § 4), as well as *sui generis* preparation, referred to by some representatives of the doctrine as the mitigated type (§ 3) (Article 130, Journal of Laws 1997, no. 88, item 553, as amended).

According to the wording of Article 130 § 1, which criminalises the basic type of espionage offence, the perpetrator is one who takes part in the activities of a foreign intelligence service against Poland. The aggravated type, as specified in § 2, criminalises providing a foreign intelligence service with information, the passing of which might harm the state of Poland, and where providing the said information is related to playing a part in a foreign intelligence service or acting for the benefit thereof. The aggravated type, as specified in § 4, criminalises organisation or management of a foreign intelligence service. On the other hand, in Article 130 § 3, the legislator describes, in an unusual way, a kind of preparation for espionage, constructed as an independent offence, which is by some commentators referred to as the mitigated type. In this type, the legislator criminalises collecting or storing information, the passing of which to a foreign intelligence service might harm the state of Poland. It is noteworthy that later on the criminalisation scope under Art. 130 § 3 was extended to include accessing the IT system in order to obtain information the passing of which to a foreign intelligence service might harm the state of Poland. Next to collecting or storing specific information, or accessing the IT system, this type of the offence encompasses declaring oneself ready to act for the benefit of a foreign intelligence service (Art. 130, Journal of Laws 1997, no. 88, item 553, as amended; Hoc, 2013, pp. 80–100; Hoc, 2002; Giezek, 2021, pp. 121–127).

First of all, the subjective side of the different types of the offence of espionage should be presented. This is because it is one of the main characteristics of the offence, as well as because of the attempt to criminalise a new type of espionage offence based on the inadvertent action of the perpetrator in 2023. S. Hoc and M. Budyn-Kulik assume that the basic and the first aggravated type of the offence of espionage can be committed intentionally with both direct and oblique intent. The same position is held by K. Lipiński, I. Zgoliński and K. Wiak. A different position on the admissibility of both intentions within the intentionality in the basic type of the offence of espionage was represented by J. Kulesza, who accepted only direct intent. On the other hand, the mitigated type of the offence of espionage, due to the indicium of acting with intent (including the double

intent in the case of accessing an IT system), according to S. Hoc, M. Budyn-Kulik and I. Zgoliński, can be committed intentionally with deliberate direct intent. As regards the other aggravated type of the offence of espionage, both S. Hoc, M. Budyn-Kulik, K. Lipiński, I. Zgoliński, and K. Wiak accept that it can be committed intentionally with direct intent (for more see Hoc, 2002, pp. 77–79; Mozgawa, 2010, pp. 291–293; Mozgawa, 2017, pp. 431–433; Dukiet-Nagórska, 2018, pp. 368–371; Grześkowiak, Wiak, 2019, pp. 840–843; Konarska-Wrzosek, 2020, pp. 727–732; Giezek, 2021, pp. 121–127; Grześkowiak, Wiak, 2024, pp. 1085–1090).

It should be assumed that in order to fulfil the indicium of participating in foreign intelligence, which is the main indicium in the basic type of the offence, it is sufficient to carry out at least one task commissioned by a foreign intelligence service, and targeted at the state of Poland. Thus, the fulfilment of the indicia of the basic type of the offence of espionage can be, for example, execution of an order to pick up a letter or parcel, passing information, operating contact points, conducting human intelligence, carrying out thematic searches, spreading misinformation in cyberspace (Mozgawa, 2017, pp. 431–433; Grześkowiak, Wiak, 2019, pp. 840–843; Giezek, 2021, pp. 121–127). Following S. Pikulski, it should therefore be assumed that the main constitutive elements of participation in foreign intelligence are: an understanding between the perpetrator and a foreign intelligence service, and execution by him or her of at least one task at the behest of a foreign intelligence service. Of course, participation in foreign intelligence can also take the form of fulfilment of formal functions in it, due to the fact of working within its structure (Pikulski, 1987, pp. 65–134).

Given the practice of detecting espionage offences, participation in foreign intelligence activity “against the state of Poland” seems to be an ambiguous indicium. This is due to the fact 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. This also means that participation in foreign intelligence that is not related to activity against Poland is beyond the bounds of criminalisation pursuant to Art. 130 of the Penal Code. Therefore, by way of illustration, participation in the Azerbaijani intelligence activities targeted at Armenia does not fulfil the indicia specified in the basic type of espionage offence (Gardocki, 2002, pp. 209–211; Hoc, 2002, pp. 64–65; Rosicki, 2021, pp. 49–73). The problematics concerned with the criminalisation of espionage activities targeted at Poland or other states became relevant in the course of the work on changes to the scope of criminalisation in 2023.

Another characteristic that is problematic with regard to the detection practice of espionage offences is the very category of “intelligence” for which the perpetrator is supposed to act. In the legal subject matter, the very term ‘intelligence’ seems ambiguous, because we can speak about foreign (external) intelligence, internal one (counter-intelligence) and criminal intelligence. Depending on the state, special services may fall within any one of the three above-mentioned models, regarding the civilian and military specificity, or constitute mixed models (Minkina, 2014, pp. 27–208). On the other hand, within the legislation in force in 1970–1997, S. Pikulski assumed that intelligence should be understood as: (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 with a view to increasing security, but also with a view

to conducting 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). Nevertheless, this author’s classification of the organs of international institutions as intelligence should be considered debatable. Still, it can undoubtedly be assumed nowadays that intelligence is: (1) a specific institution with a particular type of organisation and structure, which is assigned the task to achieve intelligence objectives and perform intelligence functions (collection, often in a clandestine manner, of information, including storage, processing and analysis; acting in a clandestine manner, including performance of operational and investigative activities), (2) a specific process comprising the so-called intelligence cycle involving the acquisition of information, as well as its transmission, confirmation, reliability checking, interpretation and delivery, usually to specific decision-makers (cf. Knorr, 1964; Kent, 1965; Pikulski, 1987, pp. 49–57; Hoc, 2002, pp. 44– 94; Minkina, 2014, pp. 27–208).

It is noteworthy that the Polish legislator, by using the category of “foreign intelligence,” has narrowed the scope of criminalisation of espionage activities. This is because a frequent solution used by other legislators is a more general indicium, e.g. the category of a foreign state, foreign power or foreign government (cf. Hoc, 1985, pp. 67–78; Pikulski, 1987, pp. 49–57; Rosicki, 2018, pp. 180–201). Such a narrowed category of the entity for which the offender is supposed to render his or her services leads to evidence problems, as in proceedings it is often up to the enforcement authorities to prove that he or she has been acting for the benefit of a specific institution. Also, this problem was not solved by the legislator in the course of the amendment work in 2023.

The aggravated type, as specified in § 2, criminalises providing a foreign intelligence service with information, the passing of which might harm the state of Poland, and where providing the said information is related to playing a part in a foreign intelligence service or acting for the benefit thereof. The Polish legislator did not choose to introduce a division into categories: all information and information protected by a particular type of confidentiality. Nor did the legislator choose to elaborate the characteristics of information, which typifies some other legislators (cf. Hoc, 1985, pp. 78–91; Pikulski, 1987, pp. 96–102; Konarska-Wrzosek, 2020, p. 729; Giezek, 2021, p. 124; Grześkowiak, Wiak, 2024, p. 1088). Thus, as with the indicium of “intelligence,” so in the case of the “information” that might cause harm, law enforcement authorities may encounter difficulty in demonstrating the said characteristic. The consequence of such criminalisation is the assumption that the harm referred to in § 2 does not have to occur, but only may occur; still, the possibility of its occurrence should not be abstract but real (Hoc, 2013, pp. 92–93; Hoc, 2018, pp. 368–371; Giezek, 2021, pp. 121–127). Nonetheless, it should be noted that in the case of the transmission of information that does not meet the criterion for being capable of harming Poland, the perpetrator will be criminally liable, but under the legal classification of § 1. For it is considered that the transfer of information constitutes the performance of a task for the benefit of a foreign intelligence service.

The aggravated type, as specified in § 4, criminalises organisation and management of espionage activity. From the point of view of the logic of action assessment, it must be assumed that both organising and managing are nothing other than specific forms of participating in or acting for the benefit of foreign intelligence. Interestingly, organising and managing espionage activity, as a prohibited act, appeared only with the codification of the penal law in 1969, and then that solution was also adopted in the 1997 codification (cf. Article 124, Journal of Laws 1969, no. 13, item 94, as amended; Bafia, Mioduski, Siewierski, 1977, pp. 124–318; Andrejew, 1978, pp. 98–99). While organising intelligence activity is an offence with no criminal consequences, managing such activity is a material offence. This is because, in the case of organising intelligence activity, the effect of a functional structure is not required. S. Hoc notes that a person who creates and develops a spy ring, as well as recruits new members can be recognised as an organiser. However, a problem concerned with distinguishing between organisation and management arises, as S. Hoc also reckons among the indicia of organisation the following: assigning roles, issuing instructions, and setting contact points. However, some of these actions are classified as management, especially collecting information from others and processing it. In some situations, assignment of roles may better fulfil the indicia of management rather than organisation, which depends on the stage of the development of the intelligence structures. S. Hoc stresses that these indicia are most often likely to be fulfilled by foreign intelligence residents, especially at diplomatic posts, where they perform the functions of information collection and analysis. Nonetheless, it is important to take into account the dynamics of the phenomenon of espionage activity, in which the organisers or even the managers will not only be intelligence service staffers, but its collaborators (Hoc, 1985, pp. 91–97; Pikulski, 1987, pp. 65–134; Hoc, 2002, pp. 74–77; Konarska-Wrzosek, 2020, p. 730; Giezek, 2021, pp. 121–127; Stefański, 2023, pp. 907–908; Grześkowiak, Wiak, 2024, p. 1089).

The indicia of “organising” and “managing” come close to the indicia specified for the offence of organised crime, but in this case the Polish legislator used the indicia of “establishing” and “managing” an organised criminal group or association (see Article 258 § 3 and 4, Article 130, Journal of Laws 1997, no. 88, item 553, as amended). The use in Article 130 § 4 of the category of intelligence activity rather than any organisational structure results in the irrelevance of the number of individuals involved by the offender organising or managing foreign intelligence. Still, the assumption is that if espionage activity is to be organised and managed, it should have a more complex structure, also in terms of the number of participants. However, the size of the structure of the organised or managed intelligence activity is not a formal requirement determining the content of the second type of espionage offence. Hence, it follows that, for this type of offence, it is not necessary to fulfil the condition of, for example, managing a group of at least three persons (cf. Giezek, 2021, pp. 1073–1093; Grześkowiak, Wiak, 2024, pp. 1620–1630). However, it should be noted that in this type of espionage offence, the offender organises or manages the foreign intelligence activities, which implies the performance of a specific type of task for a larger structure such as a foreign intelligence service. It follows from the above that, under certain factual circumstances, it will be possible to bring charges against the offender under Article 130 in the concurrence of offences or even in a cumulative concurrence with Article 258 of the Penal Code.

## 2. Legal solutions concerned with espionage activity in Poland introduced in 2023

The discussion of the need for changes to espionage laws has been going on in Poland for a long time, but it was only Russia’s armed assault on Ukraine in 2022 that provided a stronger rationale for such changes. The biggest proponent of the changes was the Polish counter-intelligence service, which drew attention to the incompatibility of the provisions criminalising espionage with the new challenges. The services’ lobbying efforts came to be reflected in the work undertaken by the Ministry of Justice. It is to be assumed that the coincidence of the Russian threat with the instrumental use of the law in domestic politics paved the way for a change in the scope of criminalisation of espionage acts, and in the increase in criminal liability for these acts (Rosicki, 2023, pp. 252–281).

Undoubtedly, the exploitation of the atmosphere of threat and a kind of spymania has more than once in history implied legislative changes and their particular use by the apparatuses of both democratic and non-democratic states. Such a state of affairs seems to be adequately represented by an excerpt from Alexander I. Solzhenitsyn’s *The Gulag Archipelago*, which refers to the provision criminalising espionage in Stalinist Russia: “[It] was interpreted so broadly that if one were to count up all those sentenced under it one might conclude that during Stalin’s time our people supported life not by agriculture or industry, but only by espionage on behalf of foreigners, and by living on subsidies from foreign intelligence services. Espionage was very convenient in its simplicity, comprehensible both to an undeveloped criminal and to a learned jurist, to a journalist and to public opinion” (see Solzhenitsyn, 1975, p. 63). We faced a similar situation during the Stalinist period in Poland. The atmosphere of obsession with secrets, spy camouflage and the paranoia of spy conspiracies is parodically conveyed in Stanisław Lem’s *Memoirs Found in a Bathtub* (Lem, 1973). Of no little relevance for the atmosphere of suspicion is also the public perception of the phenomenon, which occurs in synergy with its depiction in many spy novels which present complex intelligence games, and which include, for example, the works by John le Carré: *Call for the Dead* (1961), *The Spy Who Came in from the Cold* (1963), *The Looking Glass War* (1965), *Tinker, Tailor, Soldier, Spy* (1974) and many others.

One cannot fail to note that the very Russian-Ukrainian conflict has increased the threat, thereby enforcing the argumentation advocating a change in the degree of penalisation and the scope of criminalisation of espionage activity in Poland. Certain events are also significant. For instance: (1) in February 2022, just three days after the Russian invasion of Ukraine, the Polish intelligence services apprehended, near the Polish-Ukrainian border, a Spanish citizen who, by their own account, was allegedly spying for Russia while practising as a journalist; (2) in March 2022, the services apprehended a Polish citizen, an employee of the archives of the Warsaw Registry Office and previously one of the subordinates of S. Cenckiewicz, the chairman of the Committee for the Liquidation of the Military Information Services; (3) in April 2022, a Russian citizen I. J. Petrov was taken into custody on charges of spying for the Russian intelligence; (4) in November 2023, the prosecutor’s office brought espionage charges against sixteen people for espionage activities targeted at Poland, and undertaken in the first quarter of that year. The core of this group comprised Ukrainian citizens who were also alleged to have organised acts of sabotage on behalf of Russia’s intelligence services; (5) in March 2024, the Polish

counter-intelligence services, in cooperation with other European services, including the Czech Republic, carried out procedural acts in connection with the documented activities aimed at organising pro-Russian initiatives and media campaigns in the European Union countries (*Dziennikarz…*, 2022; Kacprzak, Zawadka, 2023; Rosicki, 2023, pp. 339–351; *Report of the Internal Security Agency of 28.03.2024*, 2024).

Preliminary work on amending the espionage legislation got underway at the Ministry of Justice, but the draft amendments were submitted to the Sejm by a group of MPs on 17 April 2023. Under the new structure of Article 130 of the Penal Code proposed by the authors, the working names of the different types of espionage can be as follows: § 1 – activity on behalf of foreign intelligence, § 2 – providing information to foreign intelligence, § 3 – activity on behalf of foreign intelligence, undertaken by a public official or a person performing flexible territorial military service, § 4 – disinformation as part of espionage activity, § 5 – sabotage, subversion and activities of a terrorist nature as part of espionage activity, § 6 – espionage activity without the consent from the competent authority, § 7 – inadvertent provision of information to persons or entities participating in foreign intelligence activities, § 8 – *sui generis* preparation, § 9 – preparation (for § 1–3), § 9 – organising and managing foreign intelligence activities (*Parliamentary Bill*..., EW-020-1196/23).

In its original version, the bill drew criticism both on account of its poor legislative technique and the controversial solutions significantly widening the prelude aspect of the offence of espionage. The most criticised solution seems to have been the attempt to criminalise the so-called unintentional espionage, which took the form of the criminal transmission of a particular type of information by the offender to a person or other entity which, on the basis of the surrounding circumstances, he or she should and could assume to be involved in the activities of a foreign intelligence service. It is noteworthy that the bill’s initiator has drawn the construct of unintentional passing of information to persons and entities associated with foreign intelligence from the offence of unintentional receiving. Whereas in the new type of espionage unintentionality was to be concerned with obligation and ability to recognise circumstances indicating that the persons and entities were connected with foreign intelligence, in the offence of unintentional receiving, the perpetrator should and may presume, on the basis of the surrounding circumstances, that a specific item has been obtained by means of a prohibited act (cf. Budyn-Kulik, 2013, pp. 33–61; Theuss, 2020, pp. 93–96). It seems right that the legislator abandoned the criminalisation of unintentional espionage, as the scope of its criminalisation, i.e. of the subjective side, established above-average requirements for the average person as regards suspicion of the espionage activities undertaken by his interlocutor (cf. *Own amendment*..., Paper no. 3232-A). Such requirements may rather be imposed in regard to a public official or a person who has become acquainted with the information while performing a public function, rather than in regard to the average person, which anyway is reflected in the provisions concerned with another offence, already present in the Polish penal law, i.e. inadvertent disclosure of information bound by “secret” or “top secret” clauses (see Art. 265 § 3 and also § 2, Journal of Laws 1997, no. 88, item 553, as amended; Grześkowiak, Wiak, 2024, pp. 1650–1653).

Another example of an attempt at imprudent extension of the criminalisation of the prelude aspect of the offence of espionage, in the Parliamentary Bill of 17 April 2023, is

the criminalisation of preparation for: (1) activity for the benefit of foreign intelligence, (2) providing information to foreign intelligence, (3) activity for the benefit of foreign intelligence, undertaken by a public official or a person performing flexible territorial military service (*Parliamentary Bill*..., EW-020-1196/23; *Own amendment*..., Paper no. 3232). The institution of the preparation for the basic type and selected aggravated types of the offence of espionage could lead to problems concerned with the classification of particular actual states, in a situation where, at the same time, the criminalisation of preparation *sui generis* was preserved (see current Article 130 § 3, Journal of Laws 1997, no. 88, item 553, as amended). Eventually, in the course of the work, the legislator retained only the criminalisation of the preparation for sabotage, subversion and the commission of a terrorist offence as part of espionage activity (see current Article 130 § 8 in connection with § 7, Journal of Laws 1997, no. 88, item 553, as amended). At this point, a remark is due as to why the legislator ultimately decided to criminalise only one of the afore-mentioned aggravated types of offences and not, for example, by way of addition to disinformation as part of espionage activity (see current Article 130 § 9, Journal of Laws 1997, no. 88, item 553, as amended). This remark is well-grounded, as the pursuit of changes in the penalisation and criminalisation of the offence of espionage by the then authorities of the Ministry of Justice was justified by the desire to make the punishment more repressive and to eliminate the threat of disinformation inspired by foreign intelligence or states, while subversion, sabotage and terrorist offences were not a strong talking point in public debate.

The attempt to criminalise subversion, sabotage and terrorist offences involves quite a lot of awkwardness on the part of the initiator, and in the further course of work – on the part of the legislator. In this regard, the main issues include:

(1) the use, in the course of the work, of various indicia to define terrorist acts, while there was already a legal definition of a terrorist offence in the Polish Penal Code (see Art. 115 § 20, Journal of Laws 1997, no. 88, item 553, as amended). In Paper no. 3232 of 17 April 2023, and similarly in Paper no. 3232-A of 26 May 2023, the initiator used the expression “activities of a terrorist nature,” which should be regarded as a mistake, as the Polish Penal Code does not use this type of indicium, but instead uses the above-mentioned term “terrorist offence.” Therefore, in Paper no. 3358 of 14 June 2023, the indicium “activities of a terrorist nature” was replaced with the following wording: “commits a prohibited act as defined in Article 115 § 20,” which in turn in Paper no. 3358-A of 7 July 2023 is replaced with the indicium: “commits a terrorist offence” (*Parliamentary bill*..., Paper no. 3232; *Supplementary report*..., Paper no. 3358; *Own amendment*..., Paper no. 3232-A; *Supplementary report*..., Paper no. 3358-A).

(2) the use by the initiator, and the maintenance by the legislator in the course of its work, of other indicia, i.e. the commission of “subversion” or “sabotage,” may raise all sorts of questions. The first doubt will be the juxtaposition of subversion and sabotage alongside the terrorist offence. This is due to the fact that while the latter category has its own legal definition in the Polish Penal Code, the former two do not. Under the 1946 Decree and the 1969 Penal Code, the Polish legislator used the category of sabotage or doctrinally defined certain criminalised acts as sabotage or subversion (cf. Art. 3, Journal of Laws 1946, no. 30, item 192, as amended; Art. 127,

Journal of Laws 1969, no. 13, item 94, as amended; Andrejew, Pławski, 1953, pp. 33–35 and 50–55; Lityński, 1960, pp. 96–110; Bafia, Hochberg, Siewierski, 1965, pp. 9–14; Chybiński, Gutekunst, Świda, 1965, pp. 36–42; Bafia, Mioduski, Siewierski, 1977, pp. 322–325; Andrejew, 1978, p. 100). It is doubtful, however, whether the modern legislator would want to refer to the significance of subversion and sabotage in the scheme of Stalinist and communist penal regulations, especially since, in both the previous types of legislation, the provisions criminalising sabotage and subversion were often misused and over-interpreted, including practices aimed at combating political opponents. Another doubt is the lack of a clear understanding of the two terms: subversion and sabotage.[1] This, therefore, makes it difficult to make a basic linguistic interpretation in this case. For instance, as regards the term “subversion,” dictionaries provide at least two meanings. The first one is: an armed or propaganda action carried out in the back and rear of the enemy troops with the aim of hampering their actions on the battlefield and reducing their combat value. The second one is: an action aimed at disrupting the political and economic life of a state and weakening its military potential, conducted stealthily, undercover. The same problem applies to the term “sabotage,” which can be understood in two ways: (1) as a deliberate disorganisation of work by evading or performing it defectively, by damaging or destroying machinery, tools, (2) as a disguised, covert action aimed at obstructing some plans (cf. Sobol, 1995, pp. 263 and 986). Undoubtedly, however, the category of sabotage was often linked to espionage itself, an expression of which can be found, for example, in a 1944 study – addressed to German offices, but excluding the German army – which stated that those carrying out their duties concerned with prevention of espionage, were at the same time counteracting sabotage, as the former activity serves to advance the latter, e.g. by means of infrastructure reconnaissance which can be described as essential to security (for more see *Guidelines*…, 1944).

The Act *amending the act – the Penal Code and certain other acts*, which changed, *inter alia*, the degree of penalisation and the scope of criminalisation of the offence of espionage, was passed on 17 August 2023 and, following the President’s signature, came into force on 1 October 2023 (for more see Journal of Laws 2023, item 1834). In the end, the legislator corrected the initial errors in the legislative technique, and the criminalisation of espionage adopted the following structure and scope within Article 130 of the Penal Code: (1) participating in the activities or acting on behalf of a foreign intelligence service (§ 1); (2) providing information to a foreign intelligence service (§ 2); (3) preparation *sui generis*, including declaration of readiness to act for a foreign intelligence service against Poland (§ 3); (4) organising and managing the activities of foreign intelligence (§ 4); (5) participating in the activities of a foreign intelligence service or acting

[1] While analysing the criminalisation of sabotage and subversion as part of espionage activities, S. Hoc cites a government representative’s opinion whereby these are “concepts well described in the security doctrine and science.” Admittedly, it is true that they are described, but it is not true that there is a consensus as to the meaning of these terms. Moreover, security sciences are not the only ones that deal with problematics of sabotage and subversion. Given the above, the argumentation by the government representative in the legislative process must be regarded as misguided as well as logically and substantively flawed (cf. Hoc, 2023, pp. 119–144).

for the benefit of a foreign intelligence service, by a public official or a person performing flexible territorial military service (§ 5); (6) espionage activities without the consent of the competent authority (§ 6); (7) sabotage, subversion and commission of a terrorist offence as part of espionage activity (§ 7); (8) preparation for sabotage, subversion and commission of a terrorist offence as part of espionage activity (§ 8); (9) disinformation as part of espionage activity (§ 9).

Considering that in the first part of the text an analysis was made of the legislation previously in force, as well as of the provisions that were maintained or slightly changed by the legislator, and in the second part at the beginning an analysis was made of the legal solutions that were not maintained in the course of the legislative work, or an analysis of selected problems related to the technique of criminalisation and legislation, it is necessary at this point to review the completely new solutions introduced into Article 130 of the Penal Code.

In Article 130 § 5, the legislator criminalises participation in the activities of a foreign intelligence service, or acting on its behalf by a public official or a person performing flexible territorial military service. The legislator therefore considers that this type of activity deserves a greater punishment because of the function or position held. Noteworthily, this solution is not alien to other European legislators, but there is a variety of ways to single out this type of offence subjects. As regards the Polish legislator, use is made of the figure of a “public official,” the legal definition of which – an exhaustive list of subjects – is included in Article 115 § 13 of the Penal Code (see Art. 115 § 13, Journal of Laws 1997, no. 88, item 553, as amended). Given the cases of officers or officials being recruited by foreign intelligence services, it seems to be an appropriate solution in countries such as the US, Germany and Sweden. However, the creation of an independent aggravated type alongside the basic type of the offence of espionage (i.e. Article 130 § 1 of the Penal Code), but not the creation of an adequate solution for Article 130 § 2 of the Penal Code, may be questionable. It seems that a more coherent solution in this situation would be to include in the criminalisation – due to the specific nature of the subject of the offence – both participating in the activities of a foreign intelligence service or acting on its behalf, and providing that intelligence service with the information the transmission of which might cause harm to Poland. This solution, however, requires more consideration, and at the same time a more rational penal policy by means of an appropriate gradation of sanctions within Article 130 of the Penal Code. However, the Polish legislator does not show any consideration like this.

In Article 130 § 6, the legislator has introduced a new type of espionage offence, which might be referred to as a “game changer,” as it is targeted at all espionage activity, and not only the kind that is directed against Poland. Under the previous legislation, espionage was criminalised if it was directed only against Poland, or if the information transmitted, as part of that activity, could harm Poland (cf. Gardocki, 2002, pp. 209–210; Gardocki, 2023, pp. 240–241). However, the exception in the legislation in force back then was the situation specified in Article 138 of the Penal Code, which indicates even now that Article 130 of the Penal Code may be applied if espionage has been committed to the detriment of an allied state, where the state guarantees reciprocity (cf. Giezek, 2021, pp. 159–161; Stefański, 2023, pp. 920–922; Świecki, 2023, pp. 512–514).

The new solution, under Article 130 § 6, criminalises espionage activity that is not targeted at Poland, but is carried out on its territory. At the same time, the provision indicates that an act like this will be punishable only if the perpetrator has not previously obtained consent to this type of activity from the competent authorities (i.e. the Head of the Internal Security Agency, the Head of the Intelligence Agency, the Head of the Counter-Intelligence Service, or the Head of the Military Intelligence Service – each of the aforementioned heads may grant consent within the scope of his or her own jurisdiction) (see Art. 8a section 1, Journal of Laws 2002, no. 74, item 676, as amended; Art. 9a section 1, Journal of Laws 2006, no. 104, item 709, as amended). The limitation with regard to the aforementioned decision is the situation in which the espionage activity does not violate Poland’s interests as described by the legislator in Article 112a of the Penal Code, i.e. it does not violate such interests as the protection of independence, territorial integrity, external and internal security, defence capabilities, foreign policy, international position, or scientific or economic potential (Article 112a, Joural of Laws 1997, no. 88, item 553, as amended; Grześkowiak, Wiak, 2024, pp. 958–960). Some of the categories mentioned are difficult to link to the interests legally protected directly under the Penal Code, the result being that the discretionary decisions of individual heads of the secret services become highly arbitrary. Moreover, the legislation allows the Head of the Internal Security Agency and the Head of the Military Counter-Intelligence Service to “legitimise” *ex post facto* espionage of this type by waiving the obligation to notify the competent prosecutor, but fulfilling the conditions indicated in the Act (for more see Article 22b, section 2a, Journal of Laws 2002, no. 74, item 676, as amended; Art. 27a, section 2a, Journal of Laws 2006, no. 104, item 709, as amended). Despite the comments cited above, it is noteworthy that the criminalisation of espionage activity carried out on the territory of a state and not directed against it is not alien to other European legislators. It can also be pointed out that the criminalisation of this type of espionage fulfils its preventive function, especially with regard to Polish citizens. This follows from the fact that the potential recruitment of a Polish citizen by a foreign intelligence service may take place under the guise of acting not against Poland, but against another state, and steps may then be taken to divert the recruited person’s actions.

At this point, it is also worth considering whether the solution under Article 130 § 6, as well as the supplementary provisions specified by the administrative law (as regards the functioning of the special services) are consistent, if only with regard to the criminalisation of the organisation and management of espionage activities taking place in the Polish territory, but not directed against Poland. This may result in a situation where the verbal features of the indicia specified in Article 130 § 4 have been fulfilled, but there is no activity directed against Poland, nor concomitantly consent has been granted (as specified in Article 130 § 6), and so it will be necessary to apply only Article 130 § 6.

As regards the offence of sabotage, subversion and the commission of a terrorist offence as part of espionage activity, criminalised under Article 130 § 7 of the Penal Code, remarks have been made earlier with regard to the problems of linguistic interpretation of the first two functional indicia. Unfortunately, due to the initiator’s poor justification of the specific indicia and types of offences, enclosed with the bill of 17 April 2023, it is difficult to discern the rationale and the objectives (see *Parliamentary bill*..., EW-020-

1196/23).[2] As it is impossible to effect a proper linguistic and functional interpretation of the indicia of sabotage and subversion, one should recognise that they do not fulfil the maximum specificity of the type of offence, which is required by the principle of *nullum crimen sine lege certa*. Therefore, as far as these indicia are concerned, the provision must be deemed unconstitutional. Moreover, it could also be over-interpreted to the disadvantage of those suspected of such prohibited acts. Vague and insufficiently specified indicia tend to typify legislatures in non-democratic systems, but they should not be characteristic of legislatures in democratic states governed by the rule of law.

Also, it is worth considering the construction of the preparation for Article 130 § 7 of the Penal Code in connection with the indicium of a “terrorist offence” and, more specifically, the situation in which the perpetrator “commits a terrorist offence” by participating in espionage activity (see Article 130 § 8 in connection with Article 130 § 7). This article directly refers to the legal definition of a “terrorist offence,” which is any act that meets the conditions: the objective one and at least one of the three subjective ones. The objective condition is: a specific act carries the maximum penalty of at least five years’ custodial sentence. The subjective conditions are: (1) serious terrorising of many people, (2) forcing a public authority of the Republic of Poland, or another state or international organisation, to take or not to take a certain course of action, (3) causing a serious disturbance in the system or the economy of the Republic of Poland, or another state or international organisation. One must not forget that a threat of acts fulfilling the above-mentioned subjective and objective conditions is a terrorist offence as well (cf. Górniok, 2004, pp. 3–11; Gabriel-Węglowski, 2018, pp. 53–58; Gołda-Sobczak, Sobczak, 2018, pp. 92–119; Michalska-Warias, 2019, pp. 41–49). An interesting fact can thus be noted, which is that the legislator has criminalised through Article 130 § 8, in conjunction with Article 130 § 7, and with reference to Article 115 § 20, the preparation for the threat to commit a terrorist offence as part of espionage activity. At the same time, it must be clarified that the institution of a terrorist offence is so broad that it can also encompass a merely exemplary situation of the following kind: a perpetrator threatens to commit both a selected environmental offence (e.g. pollution of water, air, or the ground – Article 182 of the Penal Code) and a sexual offence (e.g. rape – Article 197 of the Penal Code) in order to force the authorities to make a specific decision (cf. Stefański, 2023, pp. 838–840).

In the years 2022–2023, representatives of the Ministry of Justice reported that disinformation would need to be criminalised (*Ministry of Justice*..., 2022; Woźnicki, 2022). However, despite the announcements, it was not disinformation as such, but disinformation as part of espionage activity that came to be ultimately criminalised. And L. Gardocki would even refer to it as intelligence disinformation, even though the term has already been used by the doctrine for the offence in Article 132 of the Penal Code (cf. Art. 132, Journal of Laws 1997, no. 88, item 553, as amended; Gardocki, 2023, pp. 240–241; Grześkowiak, Wiak, 2024, pp. 1092–1093).

In Article 130 § 9, the legislator has criminalised a situation in which the perpetrator, while participating in or acting on behalf of foreign intelligence, engages in disinforma-

[2] The document entitled *An assessment of the legal effects of the regulation contained in the parliamentary bill amending the Act – the Penal Code and certain other acts* (Paper no. 3232) by N. Podraza-Majewska, a legislation expert at the Bureau of Research, dated 22 May 2023, does not contribute anything in this respect either.

tion, disseminating false or misleading information, with the aim of causing serious disturbances in the system or economy of Poland, an allied state or an international organisation of which Poland is a member, or forces a national public authority, an allied state or an international organisation of which Poland is a member to take or refrain from taking certain actions (Art. 130 § 9, Journal of Laws 1997, no. 88, item 553, as amended). With the constitutive elements of the terrorist offence in mind, it is easy to see that two of its three subjective conditions have been used to criminalise this form of disinformation. It is unclear why the initiator of the bill, and ultimately the legislator did not include the first subjective condition of the terrorist offence, namely the serious terrorising of many people. It is clear that one of the many purposes of disinformation is also to cause anxiety and fear in the community, which can ultimately result in confusion and instability. This makes one wonder in general about the point in and rationale for criminalising disinformation, if its indicia intersect with the indicia of a terrorist offence. It is not clear what purpose is served by such a broad criminalisation regarding the negative impact on third countries and international organisations (cf. Hoc, 2023, pp. 138–139). The potential of the Polish counter-intelligence and intelligence is not so high as to deal with this type of cases, and on such a scale. Furthermore, a high level of subjectivity in both what is untrue or misleading, and the nature of the purposes behind such information can result in an instrumental influence of state organs on the freedom of expression. Last but not least, it must be emphasised that the disinformation with manifestations indicated in the new regulation was already criminalised under Article 130 § 1. And this follows from the fact that the fulfilment of the indicia of participation in foreign intelligence against Poland may be manifested by the performance of at least one task for its benefit, which may exactly be engaging in disinformation.

While analysing the sense of criminalising disinformation, technological advancement should be borne in mind as well. In a situation where the majority of disinformation operations are carried out externally, with the involvement or support of foreign intelligence services, which may be using bots, a botnet, troll farms and AI, the effectiveness of applying the new provision to such situations will be rather negligible, or even non-existent (cf. Chałubińska-Jentkiewicz, 2021a, pp. 9–23; Chałubińska-Jentkiewicz, 2021b, pp. 9–18; Grycuk, 2021, pp. 1– 12; Aro, 2022; Chałubińska-Jentkiewicz, 2023, pp. 260–295).

To conclude, it is worth noting a change within the provision that the doctrine has most often referred to as preparation *sui generis* (Article 130 § 3, Journal of Laws 1997, no. 88, item 553, as amended). In the current wording of Article 130 § 3, the perpetrator is the one who declares readiness to act for foreign intelligence against Poland, or in order to provide foreign intelligence with information, the transmission of which may cause harm to Poland; who collects or stores it, or accesses the IT system in order to obtain it. Compared with the previous legislation, the sentence concerning the declaration of readiness for the benefit of foreign intelligence has been moved from the end to the beginning of the provision, which has eliminated the purpose of the action, thereby making the offering of one’s services to foreign intelligence an act independent of the circumstances described thereafter (cf. Hoc, 2023, p. 134; Świecki, 2023, pp. 512–514; Grześkowiak, Wiak, 2024, pp. 1088–1089). It must therefore be assumed that with the benefit of this legislative procedure the legislator wanted to achieve a greater scope of

criminalisation of the initiation of collaboration with foreign intelligence (cf. Rosicki, 2023, pp. 257–271).

## Ending and conclusions

The main objective of the analysis performed in the text was to compare the new legal solutions introduced in 2023, which concern the criminalisation of various forms of espionage, with the previous legal provisions in force in 1998–2023. The comparison served to present an assessment of the new legal solutions from a criminal policy perspective, focusing mainly on three aspects: the process of laying down penal law, the evaluation of the effects of the introduced and applied law, and the effectiveness of the applied legal provisions. Given the need to elaborate the material scope of the research problem, the text features two research questions related to the following conclusions:

***(1) What are the differences between the legislation concerned with the criminalisation of the offence of espionage under Article 130 of the Penal Code introduced in 2023, and the previous legislation also regarding Article 130 of the Penal Code?***

The Act *amending the act – the Penal Code and certain other acts* enacted on 17 August 2023 amended the scope of penalisation and criminalisation of the offence of espionage, presenting the following systematisation of the types of espionage offences under Article 130 of the Penal Code: § 1 – participation in the activities of a foreign intelligence service or acting on its behalf (by and large, the provision maintains the existing solutions introduced along with the entry into force of the Penal Code in 1998; however, the indicium “acting on behalf of a foreign intelligence service” has been added), § 2 – providing a foreign intelligence service with information (the provision maintains the existing solutions introduced along with the entry into force of the Penal Code in 1998), § 3 – *sui generis* preparation (due to the editing of the provision, the fulfilment of the indicium of declaring readiness to act for the benefit of foreign intelligence no longer requires the demonstration that the purpose is to provide information that might cause harm to Poland), § 4 – organising and managing foreign intelligence activities (by and large, the provision maintains the solutions introduced when the Penal Code came into force in 1998, nevertheless the new wording of the provision, with the delegation to § 1, may raise doubts), § 5 – participation in the activities of a foreign intelligence service or acting on its behalf, as a public official or a person performing flexible territorial military service (this is a new solution and does not seem to raise any particular doubts), § 6 – espionage activity without the consent of the competent authority (this is a new solution and significantly changes the scope of the criminalisation of espionage, as it criminalises espionage not directed against Poland), § 7 – sabotage, subversion and commission of a terrorist offence as part of espionage activity (this is a new solution, and at the same time, in part of its indicia it does not comply with the principle of *nullum crimen sine lege certa*), § 8 – preparation for sabotage, subversion and commission of a terrorist offence as part of espionage activity (this is a new solution), § 9 – disinformation as part of espionage activity (this is a new solution, and it should be regarded as inadequate for the new and advanced technologies used in disinformation conducted by foreign entities).

***(2) What is the effectiveness of the 2023 changes with regard to the criminalisation of the offence of espionage under Article 130 of the Penal Code?***

Apparently, the introduction of new types of espionage, particularly aggravated ones, may not be that significant. Some of the actual states described by the indicia of the new types of aggravated offences were criminalised in the previous legislation. This follows from the fact that any task carried out for a foreign intelligence service and directed against Poland fulfilled the indicia of participating in foreign intelligence. Hence, conducting terrorist activities, sabotage or subversion, as well as disinformation, was the object of the indicium of participating in or acting for a foreign intelligence service; moreover, even OSINT activities were covered by it. In this provision, the criminological difficulty in the detection activities undertaken by the Polish counter-intelligence has been, and continues to be the indicium of “intelligence.” However, during the amendment work on Article 130, the entity for whose benefit the offender is to act has been left in place. It seems that in order to better prosecute espionage activities directed against Poland, the number of entities should have been expanded in the first place, or the existing one should have been replaced with another, e.g. a “foreign state” – a move not uncommon among European legislators. However, it should be noted that the Polish legislator has extended the criminalisation of espionage activity to those cases which are not activities against Poland, and which have not at the same time been legalised by the relevant authorities. In addition, one cannot but notice that in the case of the two new aggravated types (i.e. sabotage, subversion and commission of a terrorist offence as part of espionage activity, and disinformation as part of espionage activity), the legislator did not use the indicium “against the Republic of Poland,” which broadens the scope of criminalisation. Despite the absence of the aforementioned indicium in the two new aggravated types, it must be borne in mind that in one case the legislator refers directly to the category of a “terrorist offence,” and in the other uses – almost unamended – two of the three subjective conditions in this category, and in these, after all, various forms of negative impact on Poland are presented. Still, such a broad scope of criminalisation means that cases that do not specifically threaten the country’s interests will fall within the compass of the Polish counter-intelligence.

The initiator of the statutory amendments, while working on them, placed great emphasis on the criminalisation of disinformation; in the end, the initiator only criminalised disinformation as part of espionage activity, and – on top of that – the kind of disinformation that is not targeted at Poland. It seems that in the context of the development of new technologies and the use of botnets, troll farms and AI for disinformation, this provision will become hardly effective. It can only consolidate cooperation in combating this type of threat in the allied countries’ environment, of which Poland is a part.

Some of the solutions seem to act only as a deterrent in connection with the increased scale of criminalisation, which is intended to send a clear signal to potential perpetrators (all the new aggravated types of the offence of espionage). However, it must be borne in mind that in the countries with a high degree of penalisation of this type of offence, this does not eliminate the phenomenon of espionage. Still, as regards the penal policy, the inevitability of the punishment and not just its severity is of greater importance. The inevitability of punishment for espionage is, however, linked to the quality and effectiveness of the counter-intelligence, but this – in a democratic state

under the rule of law – is not achieved through substantive law, but through well-functioning institutions.

**Author Contributions**

Conceptualization (Konceptualizacja): Remigiusz Rosicki

Data curation (Zestawienie danych): Remigiusz Rosicki

Formal analysis (Analiza formalna): Remigiusz Rosicki

Writing – original draft (Piśmiennictwo – oryginalny projekt): Remigiusz Rosicki

Writing – review & editing (Piśmiennictwo – sprawdzenie i edytowanie): Remigiusz Rosicki

**Competing interests:** The author have declared that no competing interests exist

**(Sprzeczne interesy:** Autor oświadczył, że nie istnieją żadne sprzeczne interesy)

**Bibliography**

Act of 19 April 1969 – *The Penal Code* (Journal of Laws 1969, no. 13, item 94, as amended).

Act of 6 June 1997 – *The Penal Code* (Journal of Laws 1997, no. 88, item 553, as amended).

Act of 24 May 2002 on the *Internal Security Agency and the Intelligence Agency* (Journal of Laws 2002, no. 74, item 676, as amended).

Act of 9 June 2006 *on the Military Counter-Intelligence Service and the Military Intelligence Service* (Journal of Laws 2006, no. 104, item 709).

Act of 17 August 2023 *amending the Act – the Penal Code and certain other acts* (Journal of Laws, 2023 item, 1834).

Andrejew I. (1978), *Kodeks karny. Krótki komentarz*, PWN, Warszawa.

Andrejew I., Pławski S. (1953), *Prawo karne. Część szczególna*, PWN, Warszawa.

Ankersmit F. R. (1983), *Narrative logic. A semantic analysis of the historian’s language*, Martinus Nijhoff Pub., Hague–Boston–London.

Aro J. (2022), *Putin’s Trolls: On the Frontlines of Russia’s Information War Against the World*, Ig Publishing, New York.

Bafia J., Hochberg L., Siewierski M. (1965), *Ustawy karne PRL. Komentarz*, Wyd. Prawnicze, Warszawa.

Bafia J., Mioduski K., Siewierski M. (1977), *Kodeks karny. Komentarz*, Wyd. Prawnicze, Warszawa.

Bekrycht T., Leszczyński J., Łabieniec P. (2021), *Podstawy doktryny prawnej*, Wolters Kluwer, Warszawa.

Bojarski M. (eds.) (2020), *Prawo karne materialne. Część ogólna i szczególna*, Wolters Kluwer, Warszawa.

Budyn-Kulik M. (2013), *Wybrane dogmatyczne i kryminologiczne aspekty paserstwa*, „Prawo w Działaniu. Sprawy Karne”, no. 13.

le Carré J. (1961), *Call for the Dead*, Pub. Victor Gollancz, London.

le Carré J. (1963), *The Spy Who Came In from the Cold*, Pub. Victor Gollancz, London.

le Carré J. (1965), *The Looking-Glass War*, Pub. William Heinemann, London.

le Carré J. (1974), *Tinker, Tailor, Soldier*, *Spy*, Alfred A. Knopf, Inc., New York.

Chałubińska-Jentkiewicz K. (2021a), *Dezinformacja jako akt agresji w cyberprzestrzeni*, „Cybersecurity and Law”, no. 1.

Chałubińska-Jentkiewicz K. (2021b), *Disinformation – and what else?*, „Cybersecurity and Law”, no. 2.

Chałubińska-Jentkiewicz K. (2023), *Prawne granice dezinformacji w środkach społecznego przekazu*, Wyd. A. Marszałek, Toruń.

Chybiński O., Gutekunst W., Świda W. (1965), *Prawo karne. Część szczególna*, PWN, Warszawa.

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, as amended).

Dubber M. D. (1998), *Historical Analysis of Law*, „Law and History Review”, no. 16.

Dukiet-Nagórska T. et al. (eds.) (2018), *Prawo karne. Część ogólna, szczególna i wojskowa*, Wolters Kluwer, Warszawa.

*Dziennikarz z Hiszpanii zatrzymany w Polsce. Był rosyjskim szpiegiem?* (2022), https://www.rp.pl/przestepczosc/art35815071-dziennikarz-z-hiszpanii-zatrzymany-w-polsce-byl-rosyjskim-szpiegiem, 06.03.2022.

Gabriel-Węglowski M. (2018), *Działania antyterrorystyczne. Komentarz*, Wolters Kluwer, Warszawa.

Gardocki L. (1990), *Zagadnienia teorii kryminalizacji*, PWN, 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.

Gardocki L. (2023), *Prawo karne*, C.H. Beck, Warszawa.

Giezek J. (ed.) (2021), *Kodeks karny. Część szczególna. Komentarz*, Wolters Kluwer, Warszawa.

Gołda-Sobczak M., Sobczak W. (2018), *Problem definicji terroryzmu*, „Themis Polska Nova”, no. 2.

Górniok O. (2004), *Przestępstwo o charakterze terrorystycznym w art. 115 § 20 k.k.*, „Przegląd Sądowy”, no. 10.

Grycuk A. (2021), *Fake newsy, trolle, boty i cyborgi w mediach społecznościowych*, „Analizy Biura Analiz Sejmowych”, no. 1.

Grześkowiak A., Wiak K. (eds.) (2019), *Kodeks karny. Komentarz*, C.H. Beck, Warszawa.

Grześkowiak A., Wiak K. (eds.) (2024), *Kodeks karny. Komentarz*, C.H. Beck, Warszawa.

*Guidelines for training on countering espionage, sabotage and corruption in offices* [translated from German] (1944), Ministry of Public Security.

Hoc S. (1985), *Zagadnienia odpowiedzialności karnej za szpiegostwo*, Akademia Spraw Wewnętrznych, Warszawa.

Hoc S. (2002), *Przestępstwa przeciwko Rzeczypospolitej Polskiej*, Wyd. UO, Opole.

Hoc S. (2013), *Przestępstwa przeciwko Rzeczypospolitej Polskiej*, in: *System prawa karnego. Przestępstwa przeciwko państwu i dobrom zbiorowym*, vol. 8, ed. L. Gardocki, C.H. Beck, Warszawa.

Hoc S. (2018), *Przestępstwa przeciwko Rzeczypospolitej Polskiej*, in: *Prawo karne. Część ogólna, szczególna i wojskowa*, eds. T. Dukiet-Nagórska et al., Wolters Kluwer, Warszawa.

Hoc S. (2023), *Szpiegostwo w znowelizowanym Kodeksie karnym*, „Nowa Kodyfikacja Prawa Karnego”, no. 67.

Kacparzak I., Zawadka G. (2023), *Szpiedzy chcą kary bez procesu*, „Rzeczpospolita” 18.12.2023.

Kent S. (1965), *Strategic intelligence for American world policy*, Archon Books, Hamden.

Knorr K. (1964), *Foreign Intelligence and the Social Sciences*, Princeton University, Princeton.

Konarska-Wrzosek V. (ed.) (2020), *Kodeks karny. Komentarz*, Warszawa.

Kuczur T. (2012), *Przestępstwa polityczne w uwarunkowaniach systemowych Polski XX wieku*, UKW, Bydgoszcz.

Kuczur T. (2020a), *Historyczne i prawne uwarunkowania przestępstwa szpiegostwa w Polsce w XX wieku*, „Dzieje Najnowsze”, no. 52.

Kuczur T. (2020b), *Przestępstwo szpiegostwa w Polsce w XX i XXI wieku. Polityka kryminalna, zakres kryminalizacji, uwarunkowania systemowe*, UKW, Bydgoszcz.

Kuczur T. (2020c), *Uwarunkowania normatywne i systemowe przestępstwa politycznego w Polsce w latach 1944/1945–1997*, „Przegląd Sejmowy”, no. 1.

Kulesza J. (eds.) (2023), *Prawo karne materialne. Nauka o przestępstwie, ustawie karnej i karze*, Wolters Kluwer, Warszawa.

Lande J. (1958), *Socjologia Petrażyckiego*, „Przegląd Socjologiczny”, no. 12.

Lem S. (1973), *Memoirs Found in a Bathtub*, trans. Michael Kandel, Christine Rose, The Seabury Press, New York.

Lityński M. (1960), *Przestępstwa przeciwko państwu ludowemu*, PWN, Łódź.

Michalska-Warias A. (2019), *Threat to Commit an Offence of a Terrorist Character According to Article 115 § 20 of the Polish Criminal Code – Selected Interpretation Problems*, „Studia Iuridica Lublinensia”, no. 3.

*Ministry of Justice set to combat the wave of online disinformation* (2022), https://www.rp.pl/prawo-karne/art35775701-ministerstwo-sprawiedliwosci-chce-walczyc-z-fala-internetowej-dezinformacji, 15.07.2023.

Minkina M. (2014), *Sztuka wywiadu w państwie współczesnym*, Bellona, Warszawa.

Mozgawa M. (ed.) (2010), *Kodeks karny. Praktyczny komentarz*, Wolters Kluwer, Warszawa.

Mozgawa M. et al. (eds.) (2017), *Kodeks karny. Komentarz*, Wolters Kluwer, Warszawa.

Mozgawa M. (eds.) (2020), *Prawo karne materialne. Część ogólna*, Wolters Kluwer, Warszawa.

*Own amendment to the parliamentary bill to amend the act – the Penal Code and certain other acts* of 26 May 2023 (Paper no. 3232-A), https://orka.sejm.gov.pl/Druki9ka.nsf/0/647F73E3ECF16D6EC12589BE00 416D98/$File/3232-A.pdf, 01.03.2024.

*Parliamentary bill amending the Act – the Penal Code and certain other acts submitted to the Sejm* on 17 April 2023, EW-020-1196/23 (2023), https://orka.sejm.gov.pl/Druki9ka.nsf/Projekty/9-020-1196-2023/$file/9-020-1196-2023.pdf, 14.03.2024.

*Parliamentary bill amending the Act – the Penal Code and certain acts submitted to the Sejm* on 17 April 2023 (Paper no. 3232) (2023), https://orka.sejm.gov.pl/Druki9ka.nsf/0/F53D07E65F8EC17AC12589B1003F2A96/$File/3232.pdf, 14.03.2024.

Pikulski S. (1987), *Przestępstwo szpiegostwa w teorii i praktyce*, Departament Szkolenia i Doskonalenia. Zawodowego MSW, Warszawa.

Pikulski S. (2009), *Polityka karna w Polsce z perspektywy międzynarodowej*, „Białostockie Studia Prawnicze”, no. 6.

Podgórecki A. (1962), *Socjologia prawa*, WP, Warszawa.

Podraza-Majewska N. (2023), *An assessment of the legal effects of the regulation contained in the parliamentary bill amending the Act – the Penal Code and certain other acts* (Paper no. 3232), Bureau of Research of the Chancellery of the Sejm, Warszawa.

Pohl Ł. (2019), *Prawo karne. Wykład części ogólnej*, Wolters Kluwer, Warszawa.

*Report of the Internal Security Agency of 28.03.2024* (2024), https://www.abw.gov.pl/pl/informacje/2471,Komunikat.html, 28.03.2024.

*Report of the special committee on amendments to the codifications on the Senate resolution about the act to amend the act – the Penal Code and certain other acts* (Paper no. 3596) (2023), https://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=3596, 14.03.2024.

*Resolution of the Senate on the act amending the act – the Penal Code and certain other acts* (Paper no. 3553) (2023), https://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=3553, 14.03.2024.

Rosicki R. (2018), *Information security as exemplified by the crime of espionage in the Polish and Swedish criminal law*, „Studia Politologiczne”, vol. 49.

Rosicki R. (2021), *State Security as Exemplified by the Offense of Espionage Under Polish Law*, „Środkowoeuropejskie Studia Polityczne”, no. 3.

Rosicki R. (2023), *Polityka kryminalna w zakresie zwalczania działalności szpiegowskiej w Polsce*, Grupa Wydawnicza FNCE, Poznań.

Samuel G. (2014), *An Introduction to Comparative Law Theory and Method*, Hart Pub., Portland.

Solzhenitsyn A. (1975), *The Gulag Archipelago 1918–1956. An Experiment in Literary Investigation*, vol. I–II, trans. T. P. Whitney, Harper & Row Publishers, New York.

Stańdo-Kawecka B. (2020), *Polityka karna i penitencjarna między punitywizmem i menedżeryzmem*, Wolters Kluwer, Warszawa.

Stefański R. A. (ed.) (2023), *Kodeks karny. Komentarz*, C.H. Beck, Warszawa.

*Supplementary report of the special committee on amendments to the codifications on the parliamentary bill to amend the act – the Penal Code and certain other acts* (Paper no. 3358) (2023), https://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=3358, 14.03.2024.

*Supplementary report of the special committee on amendments to the codifications on the parliamentary bill to amend the act – the Penal Code and certain other acts* (Paper no. 3358-A) (2023), https://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=3358-A, 14.03.2024.

Świecki D. (ed.) (2023), *Kodeks karny. Orzecznictwo*, Wolters Kluwer, Warszawa.

Theuss P. K. (2020), *Prawne i kryminologiczne aspekty paserstwa w polskim prawie karnym i wykroczeń* (praca doktorska), UwB WP, Białystok.

Warylewski J. (2007), *Prawo karne. Część ogólna*, LexisNexis, Warszawa.

Warylewski J. (2017), *Prawo karne. Część ogólna*, Wolters Kluwer, Warszawa.

Woźnicki Ł. (2022), *Nawet dożywocie za szpiegostwo. Wojna w pretekstem do drakońskiej reformy kodeksu karnego*, https://wyborcza.pl/7,75398,28282261,nawet-dozywocie-za-szpiegostwo--wojna-w-pretekstem-do-drakonskiej.html, 16.04.2023.

Wójcik J. W. (2014), *Kryminologia. Współczesne aspekty*, Wolters Kluwer, Warszawa.

Wronkowska S., Ziembiński Z. (1997), *Zarys teorii prawa*, Wyd. Ars boni et aequi, Poznań.

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

Ziembiński Z. (1975), *Socjologia prawa jako nauka prawna*, PWN, Warszawa–Poznań.

---

**Polityka kryminalna w zakresie zapobiegania i zwalczania działalności szpiegowskiej w Polsce. Analiza wzbogacona zmianami ustawowymi przyjętymi w 2023 r.**

**Streszczenie**

Problem badawczy w tekście dotyczy polityki kryminalnej w zakresie przeciwdziałania i zwalczania przestępstwom szpiegostwa w Polsce w latach 1998–2023. Polityka kryminalna jest rozumiana jako szczególna forma polityki prawa, obejmująca programowanie działań przeciwdziałających przestępczości poprzez kary i inne środki prawne, regulacje dotyczące penalizacji i depenalizacji oraz celowe tworzenie przepisów karnych. Głównym celem analizy jest dokonanie porównania poprzedniego stanu prawnego z nowymi rozwiązaniami prawnymi, kryminalizującymi i penalizującymi kolejne typy szpiegostwa a wprowadzonymi w 2023 roku. Konsekwencją tak przyjętego celu komparatystycznego jest prezentacja oceny nowych rozwiązań w perspektywie polityki karnej. Analiza opiera się na dwóch podejściach: dogmatycznym i historyczno-porównawczym. Podejście dogmatyczne koncentruje się na analizie samych przepisów prawa karnego oraz ich interpretacji, podczas gdy podejście historyczno-po-

równawcze porównuje obecne przepisy z wcześniejszymi zmianami zgodnie z perspektywą diachroniczną. Badanie ma na celu odpowiedzieć na pytania dotyczące różnic między obecnym a poprzednim stanem prawnym, dotyczącym kryminalizacji szpiegostwa oraz ocenę skuteczności wprowadzonych zmian z 2023 roku.

**Słowa kluczowe:** polityka kryminalna, przestępstwa przeciwko państwu, szpiegostwo, działalność szpiegowska, kontrwywiad

Article submitted: 16.02.2024; article accepted: 25.02.2024.
Data przekazania tekstu: 16.02.2024; data zaakceptowania tekstu: 25.02.2024.