The crime of espionage in new terms, i.e. in light of the amendment to the Criminal Code of 17 August 2023

PIOTR BURCZANIUK

Institute of Legal Sciences,
Cardinal Stefan Wyszyński University
https://orcid.org/0000-0002-6685-8769

Internal Security Review, 2024, no. 30: 305–334

https://doi.org/10.4467/20801335PBW.24.013.19615

ARTICLE

Abstract

The study analysed the scope of changes in the criminalisation of the crime of espionage in Poland that took place with the amendment to the Criminal Code of 17 August 2023, as well as the systemic changes introduced by it in eight other laws, including the competency laws of all Polish special services. The amendments were introduced to increase the powers to combat this type of crime. The primary objective of the analysis was an attempt to answer the question of whether the scope of the changes introduced corresponds to the demands made by legal doctrine as well as practitioners involved in combating espionage in Poland, consequently adjusting the legal state to the current geopolitical situation, mainly related to aggressive non-military actions described in the doctrines of war. The analysis of the introduced changes was shown against the background of the legislative process of the indicated law, and especially the discussion that took place within its framework, without which a proper understanding of the changes would not be possible.

Keywords

espionage, intelligence activities, secret services

On 17 August 2023, the Sejm of the Republic of Poland passed the Act on amending the Act Criminal Code and certain other acts (hereinafter: the Act), which fundamentally changed the way in which the crime of espionage is criminalised in Poland. As indicated in the explanatory memorandum to the Act:

> (…) the main objective of the proposed project is the need to adapt the provisions of the Criminal Code concerning the crime of espionage to the constantly changing geopolitical situation, technological progress and constant modifications of the modus operandi of the potential perpetrators of the offences currently described in Article 130 of the Criminal Code. Also of significance is the current high threat of new open armed conflicts and aggressive non-military actions, which intensifies the undertaking of espionage activities by foreign intelligence and others[1].

In addition to the amendment of criminal provisions, by means of this act systemic changes were made in eight other acts, including the competence acts of all Polish special services. The need for changes in the penalisation of the crime of espionage and the competences and powers of the special services in this respect, aimed at the effective neutralisation of this type of crime, has been postulated for more than ten years both by the legal doctrine (including the author of this study) and by practitioners dealing with this criminal act.

The aim of this study is to analyse the scope of the changes introduced and to try to answer the question whether it is relevant to the demands being made and meets the practical problems encountered by the Polish law enforcement authorities when recognising the crime of espionage. The analysis of the course of the legislative process occupies an important place in these considerations. The discussion that accompanied it is important for the proper understanding - as a kind of authentic interpretation - of the new regulation.

Rationale for the changes

In the postulates formulated, concerning regulatory changes to the crime of espionage, it was pointed out that the manner of defining the elements of the prohibited act, contained in the previous wording of Article 130 of the *Act of 6 June 1997 - Criminal Code* (hereinafter: the Criminal Code), in many dimensions is not very

[1] Explanatory Memorandum to *the Parliamentary Draft Act on amendments to the Criminal Code and certain other acts*, print no. 3232, 17 IV 2023, https://orka.sejm.gov.pl/Druki9ka.nsf/0/F53D07E65F-8EC17AC12589B1003F2A96/%24File/3232.pdf, p. 13 [accessed: 28 VIII 2023].

accurate, often insufficient and, above all, unclear and vague. This has fostered different interpretations of the elements of this offence by the doctrine and often led to different qualification of acts by the prosecution. The just amended regulation of the crime of espionage corresponded directly to the threats to Poland's external security identified in the 1990s. They were based on the concept, developed still in the period of the Cold War, of the bipolarity of the international system, based on two opposing blocs of states competing with each other by military means. From this perspective, the scope of the elements of the prohibited act included in this provision did not correspond to the challenges associated with contemporary threats to the external security of the state, including the phenomena collectively referred to as asymmetric threats.

During the parliamentary debate on the draft act, MP Jarosław Krajewski rightly pointed out that (…) *the crime of espionage is one of the gravest crimes against the Republic of Poland, and if committed by a Polish citizen is de facto treason against our country.* (…) *This is particularly important from the perspective of the current geopolitical situation, which also changes the modus operandi of foreign intelligence services acting against our country*[2]. This geopolitical situation is also referred to in Polish strategic documents, including the *National Security Strategy of the Republic of Poland 2020*. They indicate, among other things, that:

> (…) the most serious threat is the neo-imperialist policy of the Russian Federation authorities, also implemented through military force. (…) The Russian Federation also conducts activities below the threshold of war (of a hybrid nature), carrying the risk of a conflict (including unintentional, resulting from a sudden escalation as a result of an incident, especially a military one), and also undertakes comprehensive and complex actions by non-military means (including: cyber attacks, disinformation) with the aim of destabilising structures of Western states and societies and causing divisions among allied states. It should be assumed that the Russian Federation will continue its policy of undermining the current international order, based on international law, in order to rebuild its superpower position and spheres of influence[3].

[2] Speech by Jarosław Krajewski on 13 June 2023, during the first reading of the parliamentary draft act amending the Criminal Code and certain other acts (prints 3232 and 3232-A), iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=9#1C429C6BE7B92E29C12588FB0033AB2F [accessed: 28 VIII 2023].

[3] *National Security Strategy of the Republic of Poland 2020*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, p. 6 [accessed: 28 VIII 2023].

Indicated in this strategy are actions below the threshold of war, also referred to as fourth-generation warfare, hybrid warfare, non-linear warfare, special warfare, asymmetric conflict as well as the Gerasimov doctrine[4]. It implies that:

> (…) the 'rules of war' themselves have changed significantly. The role of non-military methods in achieving political and strategic objectives has increased, in some cases far outstripping the effectiveness of weapons. The methods of confrontation are shifting towards the extensive use of political, economic, informational, humanitarian and other non-military measures, implemented using the protest potential of the population. All this is complemented by covert military measures, including the implementation of information countermeasures and the actions of special operations forces. The overt use of force is often used under the guise of peacekeeping and crisis management only at a certain stage, mainly to achieve ultimate success in the conflict[5].

In this concept, non-military means are not only to create and provide the conditions for the effective use of military force, but often even to replace it. The axis of the presented concept is thus the coordinated use - in order to defeat the opponent or gain an advantage over him - of the full spectrum of non-military means, including diplomatic, political, economic, technological, humanitarian and informational, while using a wide sphere of psychological and sociological influence on the population of the attacked state. It is (…) *a vision of guerrilla warfare waged on all fronts using a wide variety of tools and people: hackers, media, businessmen, information leaks and, of course, fake news and traditional conventional and asymmetric military means*[6]. Asymmetric measures of a non-military nature are therefore not only used to support military action, but are a pillar of the presented concept of new generation warfare. They are treated as an element of warfare, which is intended to create chaos by maintaining a state of permanent unrest and social tensions in the opponent, and are an assumed strategic objective aimed at achieving victory in

[4] It is named after the Chief of the General Staff of the Armed Forces of the Russian Federation, General Valery Gerasimov, who in the article *Ценность науки в предвидении* (Eng. The value of science lies in prediction) published on 27 II 2013 in the newspaper "Военно-промышленный курьер" (Eng. Military-Industrial Courier) reported on the concept of next-generation warfare. Translations in the article are from the author (editor's note).

[5] В. Герасимов, *Ценность науки в предвидении*, "Военно-промышленный курьер", 27 II 2013, https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html [accessed: 28 VIII 2023].

[6] M.K. McKew, *Doktryna Gierasimowa, czyli rosyjski sposób na wojnę: chaos, a nie bomby* (Eng. The Gerasimov doctrine, or the Russian way to war: chaos, not bombs), Onet, 6 IX 2017, https://wiadomosci.onet.pl/swiat/doktryna-gierasimowa-czyli-rosyjski-sposob-na-wojne-chaos-a-nie-bomby/svh4p0h [accessed: 28 VIII 2023].

war. At the same time, the principles of the use of military force are changed. It has been assumed that (…) *frontal clashes of large groupings of troops (forces) at the strategic and operational level are gradually becoming a thing of the past* (…) *they are being displaced by non-contact, long-range precision strikes, combined with the actions of special forces in conjunction with internal opposition forces*[7].

It is emphasised in security sciences that there is no single pattern of hybrid warfare, especially in its practical version. At most, it is possible to speak of a certain framework within which specific undertakings are implemented that are adapted to the changing circumstances and the external and internal situation of the target state. These activities involve - to varying degrees - many institutions and organs of the state in question or entities dependent on it, with the leading role of the special services being obvious. Importantly, the role of these services is not limited to information gathering, but also includes active intelligence activities known as influence operations. Information gathering, in this case, is combined with disinformation and propaganda, and sometimes with activities bearing the hallmarks of diversion and sabotage, in the form of cyberattacks, covert actions of a provocative nature, aimed at destabilising the socio-political situation or introducing chaos. Dynamic technological progress, especially in the area of communications, mass media and social media, undoubtedly facilitates such activities[8]. *Thanks to the internet and social media, it is now possible to do things that the former Soviet specialists in psychological warfare could only dream of: changing the internal politics of other countries with information alone*[9].

In the context of the described change in the modus operandi of foreign secret services, a significant problem of their qualification within the framework of the description of the elements of the espionage crime in force in Poland arose. This is

---

[7] П. Фельгенгауэр, *Добиться превосходства над остальным человечеством. Начальник российского Генштаба формулирует программу подготовки к масштабной войне* (Eng. In order to achieve superiority over the rest of humanity, the head of the Russian General Staff is formulating a programme of large-scale war preparations), Новая газета, 9 III 2019, https://novayagazeta.ru/articles/2019/03/09/79808-dobitsya-prevoshodstva-nad-ostalnym-chelovechestvom [accessed: 28 VIII 2023].

[8] See in more detail: M. Wojnowski, *Mit "wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku* (Eng. The myth of 'hybrid war'. Conflict on the territory of the Ukrainian state in the light of Russian military thought of the XIX-XXI centuries), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, special issue: *Wojna hybrydowa*, p. 25; Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia* (Eng. Hybrid warfare - the challenge of the future? Selected issues), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, special issue: *Wojna hybrydowa*, pp. 46–47.

[9] M.K. McKew, *Doktryna Gierasimowa*…

because the repealed regulation of Article 130 of the Criminal Code covered only four types of this crime:

- the basic type, which criminalises participation in the activities of a foreign intelligence service (Article 130 § 1),
- the qualified type, where the qualifying circumstance is providing, while participating in or acting for a foreign intelligence service, information to a foreign intelligence service, the transmission of which could cause damage to the Republic of Poland (Article 130 § 2),
- the qualified type, in which aggravated responsibility is connected with the fact of organising or directing the activities of a foreign intelligence service (Article 130 § 4),
- the privileged type, which consists in collecting, storing or entering an information system in order to obtain information for the purpose of providing it to a foreign intelligence service, or declaring readiness to act for a foreign intelligence service against the Republic of Poland (Article 130 § 3).

Legal doctrine and jurisprudence have developed a fairly unambiguous understanding of the key concepts - 'taking part in the activities of a foreign intelligence service' and 'acting for the benefit of a foreign intelligence service'. As Piotr Kardas points out:

> (…) "participation" should be understood as any form of active collaboration with a foreign intelligence service consisting in belonging to the organisational structure of the intelligence service (…) "participation" in the activities of an intelligence service means both the performance of the function of an agent or resident of a foreign intelligence service and the performance of any other function within its organisational structure, such as e.g. the function of a person who recruits collaborators, conducts training of agents, provides or prepares technical means used in the intelligence activity, collects and elaborates information, operates the so-called contact or transfer points, supplies the espionage network with materials and means used in the intelligence activity, etc.[10]

On the other hand, (…) *acting for the benefit of a foreign intelligence service means any form of active cooperation with a foreign intelligence service that does not yet take the form of functioning within its organisational structures, which can be defined as taking part in it. Acting for the benefit of a foreign intelligence service does not require the existence of an organisational link between the perpetrator and the foreign*

[10] P. Kardas, in: *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-211a* (cz. 1) (Eng. Criminal Code. Specific part. Volume II. Commentary to Articles 117-211a (Part 1)), W. Wróbel, A. Zoll (eds.), Warszawa 2017, Article 130.

intelligence service[11]. It is important to note that from the point of view of the elements of the offence previously provided for in Article 130 § 2 of the Criminal Code, only such action in favour of foreign intelligence which took the form of providing it with the information specified in this provision was criminalised. In view of the regulatory scope of Article 130 of the Criminal Code thus drafted, an important practical problem arose with regard to the qualification of criminal behaviour which did not fulfil the cited definition of "taking part in the activities of a foreign intelligence service". This is because they did not contain elements of active cooperation with a foreign intelligence service combined with affiliation to organisational structures of this service (or such activities where such affiliation could not be substantiated by evidence, which in the case of espionage activities - conducted secretly by definition - is a practically impossible task), and which in fact took the form of 'acting for a foreign intelligence service', but were not combined with the transmission of messages to a foreign intelligence service as part of this cooperation (which was penalised by the Criminal Code), but involved the undertaking of various other types of activities, including what are referred to as influence operations, in line with the Gerasimov doctrine described above. During the debate in the Senate on the act, Senator Magdalena Kochan pointed out that:

> (…) none of us in this room can afford to underestimate Russia's special services. None of us who know, have read (…) have familiarised ourselves with the Gerasimov doctrine can afford to underestimate this doctrine and the disinformation that underpins it. We are all aware of its role during the U.S. elections, we know what role this disinformation played during Brexit, we know what enormous attention Poland probably enjoys, as the fall of the USSR did not cure Russia's great power inclinations. In view of this, and in view of the war going on right next to our border, no threats of espionage in our country can be ignored[12].

Legislative work – historical background

The discussion on the need for regulatory changes to the crime of espionage was initiated back in December 2016 by Piotr Pogonowski, then Head of the Internal

[11] Ibid.

[12] Speech by Magdalena Kochan of 26 VII 2023 during the debate at the 65th session of the Senate of the Republic of Poland of the 10th parliamentary term, https://av8.senat.pl/10Sen651 [accessed: 28 VIII 2023].

Security Agency (hereinafter: ABW). The assumptions he presented became the basis for the development of a draft amendment in the first half of 2017, in cooperation with the Minister of Justice. Firstly, it envisaged supplementing the element of the prohibited act defined in Article 130 § 1 of the Criminal Code in the form of 'taking part in the activity of foreign intelligence' with the element of 'conducting intelligence activity', defined as an activity or a set of activities undertaken, even indirectly, in the interest of a foreign state or a foreign organisation. These activities consist of the acquisition or transmission of information, the disclosure or use of which may damage the interests of the state insofar as this includes, in particular, the protection of the state's independence, territorial integrity, external and internal security, defence, foreign policy, natural or cultural heritage and scientific or economic potential, or the conduct of activities against these interests. Secondly, it provided for the introduction of the issue of so-called hybrid threats into the Criminal Code by adding definitions of the offences of state sabotage and acts of aggression. In addition, the draft provided for the criminalisation of espionage activities conducted on the territory of the Republic of Poland and not directed against it. It also assumed the addition of Article 113a to the Criminal Code, which would regulate the applicability of the Code with regard to offences committed with the use of an ICT system, regardless of the geographical location of the perpetrator or the ICT system used by him. With regard to the offence of espionage, the draft introduces a solution suggested by the author of this article[13], consisting in separating the concept of actual conduct of intelligence activities, i.e. performance of specific actions (objective element) from the concept of participation in the activities of a foreign intelligence service, understood as formal membership in the structures of this service (subjective element). Thus, the proponent has included in the presumption of punishability both the behaviour which amounts to performing certain activities in the interest of a foreign state or foreign organisation, without the need to link it directly to a structurally separate entity - the intelligence service, as well as the very membership of such structures. The presented definition of 'intelligence activities' corresponded with the so-called French model of criminalisation of espionage, shaped by the wording of Articles 411-4 and 411-5 of the Criminal Code of the French Republic. However, a negative position towards this project was presented by the National Public Prosecutor's

[13] P. Burczaniuk, *Przestępstwo szpiegostwa – rys historyczny, aktualne regulacje na tle doświadczeń praktycznych i analizy prawno-porównawczej wybranych państw* (Eng. The crime of espionage - historical background, current regulations against the background of practical experience and comparative legal analysis of selected countries), in: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, P. Burczaniuk (ed.), Warszawa 2017, pp. 106–107.

Office[14], which may have influenced the lack of continuation of the related legislative work. It was resumed on the initiative of the Parliamentary Committee for Special Services. This was mentioned during the debate in the Sejm by Marek Biernacki MP, who recalled that:

> (…) the current definition of espionage does not meet its requirements, it does not serve effectively for the action - protection of Polish interests, it does not serve the Polish state, this has been known for a long time. We also know that in our other neighbours, our partners (the French, other countries), they are working on changing these provisions, and we also started working from 2018 in the Committee for Special Services - I remind you, because this is important. We worked with the then heads of the ABW Prof. Pogonowski and Col. Loba. The prosecution and the judges also participated. Everyone showed that the bill was needed, that the law had to be amended. Suddenly, through the fault of the prosecution, the national prosecutor withdrew this draft, withdrew the work[15].

Work on regulatory changes concerning the crime of espionage was resumed by the Minister of Justice at the end of February 2022, due to the geopolitical situation caused by the armed aggression of the Russian Federation against Ukraine and the related threat to Poland's security. Developed at that time, in cooperation with the Ministry of Internal Affairs and Administration, the National Public Prosecutor's Office and the heads of the special services, the draft focused on making the offence of espionage more severe in terms of punishment, adding the stage form of preparation and introducing its unintentional form. The proposed wording of the provision of Article 130 of the Criminal Code was intended to cover with its scope the criminal activities of entities participating in the activity of foreign intelligence or other intelligence activity against the Republic of Poland. At the same time, the draft provided for the introduction of a definition of intelligence activity, understood as an activity or a set of activities undertaken in the interest of or for the benefit of a foreign state or foreign entity by a person who does not participate in foreign intelligence. These activities would consist of: 1) obtaining or transmitting information, the disclosure or use of which infringes or is likely to infringe the interest of the state in protecting its independence, territorial integrity, external and internal security, defence,

[14] Letter of 21 June 2017 no. PK I BP 0280.122.2017.

[15] Speech by Marek Biernacki on behalf of the parliamentary club on 6 VII 2023 during consideration of the Commission's report on the parliamentary draft act amendingthe Criminal Code and certain other acts (prints nos. 3232, 3232-A and 3358), iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=2#0CD6003114C05652C12588FB0033AD73 [accessed: 28 VIII 2023].

foreign policy, international position, scientific or economic potential, or 2) carrying out disinformation or propaganda activities that infringe the interest of the state within the scope specified in item 1, aimed at destabilising the political system or the economy or exerting pressure on public authorities in order for them to undertake or abandon specific actions. Importantly, as the Minister of Justice pointed out, the concept of intelligence activities referred not only to entities emanating from a foreign state, but also to other disguised forms[16], such as companies, foundations and other organisations, formally unrelated to state structures. In addition, it was assumed that the threat of punishment for espionage would be of a preventive nature, which was to justify the clarification and setting the amount of the sanction at a very high ceiling, including life imprisonment in the qualified type. The draft also contained amendments to, inter alia, the *Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency* (hereinafter: the ABW and AW Act) and the *Act of 10 June 2016 on anti-terrorist activities* (hereinafter: the AT Act), in which the competences of the ABW concerning the prevention and combating of terrorist crime were to be extended to crimes of an espionage nature. According to the assumption of the Ministry of Justice, the draft was to be submitted as an auto--amendment to the government's draft law on amendments to the Criminal Code and certain other laws (print no. 2023), which, however, did not happen. This work was returned to in October 2022 by Deputy Minister of Justice Marcin Warchoł, who indicated: (…) *we are after arrangements between the Ministry of Justice and the Ministry of Internal Affairs and Administration. We have worked out the shape of solutions ready for parliamentary work. I hope that the Sejm will deal with them immediately. The decision on this matter is up to the Marshal of the Sejm*[17]. As announced, the proposal was to take the form of a parliamentary motion.

The materialisation of this announcement took place on 17 April 2023, when a parliamentary draft act amending the Criminal Code and certain other acts (print no. 3232) was submitted to the Marshal of the Sejm by a group of Law and Justice MPs, represented by Jarosław Krajewski. The analysis of this draft leads to the conclusion that in terms of direction it coincided with the drafts under consideration earlier, with two significant changes. Firstly, it dropped the element of conducting intelligence activities (and its definition) as a component of the prohibited act

[16] *Amendments to the Criminal Code related to threats to state security*, Ministry of Justice, 29 III 2022, https://www.gov.pl/web/sprawiedliwosc/zmiany-w-kodeksie-karnym-zwiazane-z-zagrozeniem-bezpieczenstwa-panstwa [accessed: 28 VIII 2023].

[17] M. Mikowski, *Wiceszef MS: zmiany ws. surowszych kar za szpiegostwo są już gotowe* (Eng. Deputy Minister of Justice: amendments on tougher penalties for espionage are ready), PAP, 23 X 2022, https://www.pap.pl/aktualnosci/news%2C1460354%2Cwiceszef-ms-zmiany-ws-surowszych-kar-za-szpiegostwo-sa-juz-gotowe.html [accessed: 28 VIII 2023].

of espionage. Secondly, it introduced the criminalisation of a specific type of intelligence activity consisting in disinformation, sabotage, diversion and activities of a terrorist nature. The draft was supplemented by amendments to the *Act of 11 March 2022 on the Defence of the Homeland* (hereinafter: the Homeland Defence Act), providing for a ban on photographing, filming and recording the image of objects of particular importance for the security and defence of the state, as well as of persons and movable property located in these facilities.

The Panoptykon Foundation and the Helsinki Foundation for Human Rights submitted their position on the draft, in a letter dated 16 May 2023. They criticised, first of all, the introduction in the draft of criminal liability for unintentional espionage and the penalisation of the preparation of this crime. The doubts raised in this regard probably influenced the introduction, within the framework of the first reading of the draft (13 June 2023, 77th sitting of the Sejm), of amendments removing the criminalisation of unintentional espionage and narrowing the preparation only to an act within the scope of sabotage, diversion or defined in Article 115 § 20 of the Criminal Code. The National Council of the Judiciary[18] and the Supreme Court[19] also submitted their comments to the draft, and an assessment of the impact of the regulation was provided by the Analyses Bureau of the Sejm[20].

Further parliamentary legislative work proceeded very smoothly, as already at the 78th sitting of the Sejm, on 6 July 2023, the draft was considered at second reading (accepting the majority of amendments of a legislative nature tabled by the Law and Justice parliamentary club), and on 7 July 2023, the law was passed by an overwhelming majority of votes[21]. On 28 July 2023, the act was considered by the Senate of the Republic of Poland[22] by tabling five amendments, only one of which was adopted when the Act was reconsidered by the Sejm of the Republic of Poland on 17 August 2023. The adoption of this amendment resulted in the formal re-enactment of the Act and the change of its date to 17 August 2023. The Act was signed

[18] Opinion of 16 VI 2023.

[19] Comments of the Office of Studies and Analyses of the Supreme Court of 12 June 2023 no. BSA. II.021.29.2023.

[20] Regulatory impact assessment of 22 May 2023 to print no. 3232.

[21] According to the results of vote no. 46 at the 78th sitting of the Sejm, 271 MPs were in favour of the law (all of the Law and Justice club, the majority from the Polish Coalition club and the Confederation club), 1 was against and 179 abstained (the Left club and the majority from the Civic Coalition club), https://www.sejm.gov.pl/sejm9.nsf/agent.xsp?symbol=glosowania&NrKadencji=9&NrPosiedzenia=78&NrGlosowania=46 [accessed: 28 VIII 2023].

[22] During the legislative work, the Ombudsman (letter of 19 July 2023 no. II.510.565.2023.PZ) expressed his critical position towards the Act, and the President of the Personal Data Protection Office (letter of 21 July 2023 no. DOL.401.362.2023.WL.RB) submitted his comments.

into law by President of the Republic of Poland Andrzej Duda on 28 August 2023 and entered into force on 23 September 2023, with the exception of selected provisions which entered into force on 1 October 2023.

Scope of changes to the Criminal Code

There is no doubt that the most substantively significant element of the changes covered by the adopted Act is the redefinition of the offence of espionage by giving a new wording to the entire Article 130 of the Criminal Code. All other changes covered by the adopted amendment remain in systemic relation to this very change. For this reason, the adopted law was often referred to as the anti-spying law during legislative work.

For the correct interpretation of the indicated changes, it is extremely important to conclude that all the above-described drafts, submitted in 2016-2022, assumed the necessity to introduce into the Criminal Code as an element of the criminal offence of espionage the behaviour consisting in conducting intelligence activities, while defining this concept by referring to the so-called French model. This legislative procedure was to be a remedy for the criminalisation of criminal activities related to the activity of foreign special services being an element of hybrid activities. The passed law was the first draft that did not provide for this solution. Pursuant to the finally adopted wording of the provision of Article 130 § 1 of the Criminal Code, the offence of espionage in the basic type may take the form of: taking part in the activities of a foreign intelligence service or acting on its behalf, while in both situations it must be a criminal act directed against the Republic of Poland. Therefore, from 1 October 2023, the basic type of the offence of espionage is fulfilled by conduct taking the form of active cooperation with a foreign intelligence service, consisting in belonging to its organisational structures (taking part), or any active cooperation with a foreign intelligence service, which does not yet take the form of functioning in its organisational structures (acting for its benefit), as long as these activities are directed against the Republic of Poland, i.e. threaten or violate the external or internal interests of the Polish state. Obviously, what is at issue is the potential - albeit demonstrated in a specific state of facts - possibility of causing damage to the Polish state (under the repealed wording, it was already assumed that it was not necessary to demonstrate actual damage).

The adopted solution should be assessed as a step in the right direction and a way out of the reported practical problems. The difficulty, however, is the openness of interpretation of the adopted provision, which, mainly due to the presumption of *in dubio pro reo* and the accompanying prohibition on the use of broad

interpretation in criminal law, may, in the course of consideration of individual cases by courts, encounter a narrowing understanding of the concepts used (mainly the concept of cooperation with foreign intelligence). The consequence of this will be the impossibility to criminalise a certain spectrum of behaviours recognised by the services as hybrid threats conducted by foreign special services. It seems that the definition of intelligence activities formulated in earlier drafts was less prone to such a risk, due to its higher level of definiteness.

The second fundamental change covered by the Act is a significant increase in the amount of criminal sanctions for particular types of espionage offences. As the drafters indicated in the explanatory memorandum to the Act:

> The increase in criminal sanctions is justified by the fact that, in the case of the crime of espionage, the threat of punishment is mainly intended to have a preventive value. 'Professional' spies most often analyse the criminal threat in the laws of individual countries when deciding to take the risk of conducting their activities on the territory of those countries. It is therefore justifiable to set the criminal threat at a very high level, as under this assumption, general prevention will have a more effective impact than in the case of other types of crime, where criminals do not take into account the level of the criminal threat[23].

In the Criminal Code of 1969, the offence of espionage in the basic type was punishable by imprisonment for a term of not less than 5 years or by the death penalty. In the now repealed regulation of Article 130 of the Criminal Code, the basic type of the offence of espionage was punishable by imprisonment for a term of between 1 and 10 years. On the basis of an analysis of 13 sentences passed by criminal courts in espionage cases after the entry into force of the current Criminal Code, the author of this article concluded that the sentences actually oscillate around the lower limit of the prescribed prison term. Only in three cases sentences of more than 3 years imprisonment were passed:

1) to a sentence of 4 years' imprisonment, the Regional Court in Warsaw sentenced in March 2016 the defendant to participate in the activities of the intelligence service of the Republic of Belarus against the Republic of Poland, i.e. an offence under Article 130 § 2 of the Criminal Code, in the period from an undetermined date to 17 February 2014[24];
2) to a sentence of 6 years' imprisonment, deprivation of public rights for 5 years, forfeiture of material evidence and financial gain The Military

[23] Explanatory Memorandum to *the Parliamentary Draft Act amending the Act*…, pp. 13–14.

[24] Ref. no. XVIII K 110/15.

Regional Court in Warsaw sentenced in April 2016 the defendant for taking part in foreign intelligence activities against the Republic of Poland, i.e. an offence under Article 130 § 1 of the Criminal Code[25];

3) to a sentence of 7 years' imprisonment, the Court of Appeal in Warsaw sentenced the defendant for the offence of Article 130 § 1 of the Criminal Code in November 2017[26].

At the same time, in the cases under consideration, there were four convictions with a sentence of 3 years' imprisonment[27]; a sentence of 2 years and 2 months' imprisonment[28]; a joint sentence of 1 year and 6 months' imprisonment[29]; a joint sentence of 1 year and 4 months' imprisonment; forfeiture of an object used to commit a crime and forfeiture of material evidence specified in the list of evidence[30]; a total sentence of 1 year and 2 months' imprisonment[31]; a conviction of two persons, the first to a sentence of 1 year's imprisonment with a conditional suspension of its execution for a probation period of 3 years, the second to a sentence of 1 year's imprisonment[32]; a conviction to a sentence of 6 months' imprisonment, the execution of which was conditionally suspended for a probation period of 2 years, and a fine in the amount of PLN 6,300[33].

Referring to analogous analyses, the legislator decided to significantly increase the criminal sanction for the offence of espionage in the basic type. It established it as a punishment of imprisonment for a term of not less than 5 years (up to 30 years).

In addition, the legislator in the amendment retained the two existing qualified types:

– the first, in which more severe responsibility is attached to providing, while taking part in the activities of a foreign intelligence service or acting on its behalf, to a foreign intelligence service information the transmission of which may cause damage to the Republic of Poland (Article 130 § 2).

[25] Ref. no. So 1/16.

[26] Ref. no. II AKa 269/17.

[27] Subsequently: judgment of the Military Regional Court in Warsaw of 11 April 2001, ref. no. So 24/00; judgment of the Military Regional Court in Warsaw of 3 November 2005, ref. no. So 37/05; judgment of the Regional Court in Warsaw of 22 December 2010, ref. no. VIII K 272/10; judgment of the Regional Court in Warsaw of 8 March 2019, ref. no. XII K 176/18.

[28] Judgment of the Court of Appeal in Białystok of 28 XI 2016, ref. no. II AKa 96/16.

[29] Judgment of the Regional Court in Warsaw of 11 August 2022, ref. no. XVIII K 78/22.

[30] Judgment of the Regional Court in Warsaw of 21 II 2022, ref. no. XVIII K 58/20.

[31] Judgment of the Regional Court in Gdańsk of 17 May 2005, ref. no. IV K 86/05.

[32] Judgment of the Regional Court in Katowice of 19 X 2015, ref. no. V K 141/15.

[33] Judgment of the Military Regional Court in Warsaw of 29 IV 2019, ref. no. So 5/19.

However, it significantly increased the limits of the criminal sanction, from the previous sentence of imprisonment for a term of not less than 3 years to a sentence of imprisonment for a term of not less than 8 years (up to 30 years) or life imprisonment;

– the second, in which the qualification is related to organising or directing foreign intelligence activities (Article 130 § 4). Similarly, the limits of the criminal sanction have been increased from the previous sentence of imprisonment for a term of not less than 5 years or 25 years to a sentence of imprisonment for a term of not less than 10 years (up to 30 years) or life imprisonment.

At the same time, the legislator introduced three new qualified types:

– the first, related to the aggravation of responsibility of the basic type in the situation of perpetration of the offence of espionage by a public official and a person performing territorial military service. In doing so, it provided for a criminal sanction in the form of imprisonment for a term of not less than 8 years (up to 30 years) or life imprisonment (Article 130 § 5);
– the second, in which the qualifying circumstance is the commission, during conduct falling within the basic type, of diversion, sabotage or the commission of a terrorist offence. It has provided for a criminal sanction in this case in the form of imprisonment for not less than 10 years (up to 30 years) or life imprisonment (Article 130 § 7). Significantly, in the case of this criminal act, the legislator has also provided for the criminalisation of its preparation, punishable by imprisonment from 6 months to 8 years (Article 130 § 8);
– the third, in which the qualifying circumstance is the carrying out, in the course of conduct falling within the basic type, of disinformation, consisting in the dissemination of false or misleading information with the aim of causing serious disturbance to the system or economy of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member, or inducing a public authority of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member to take or refrain from taking specific actions, punishable by imprisonment for a period of not less than 8 years (up to 30 years) (Article 130 § 9). It is clear - and this was confirmed during the debate on the Act in the Senate of the Republic of Poland[34] – that the disinformation activity described in the elements does not constitute a separate crime from

[34] Debate during the 65th session of the Senate of the Republic of Poland of the 10th parliamentary term, 26 July 2023, https://av8.senat.pl/10Sen651 [accessed: 28 VIII 2023].

espionage, but is its qualified type. Conducting disinformation is therefore an element of intelligence activity falling within the category of participating in the activities of a foreign intelligence service or activities for its benefit. It is noteworthy that this provision introduces, for the first time in the Polish legal system, the concept of disinformation - which has so far been used mainly in the security sciences - with a simultaneous attempt to construct a definition of activities falling within the scope of its conduct. However, it should be clearly emphasised that the scope of this definition falls within the colloquial understanding of the term. According to the dictionary understanding, disinformation is 'to mislead by giving false information'[35]. This understanding, in Article 130 § 9 of the Criminal Code, has been narrowed down by the legislator by the notion of a public purpose connected with causing serious disturbance to the system or economy of the Republic of Poland, an allied state or an international organisation, or inducing a public authority of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member to take or refrain from taking certain actions. In this context, it should be added that two regulatory approaches to the issue of disinformation are evident in the European Union: horizontal (e.g. Malta) - prohibiting the dissemination of disinformation in any context as long as there is a threat of public harm, and vertical (e.g. Hungary and France) - combating disinformation only in specific areas, e.g. during the electoral process. Two models of liability are also applied - criminal (e.g. Malta) or administrative (e.g. France). Thus, the solution adopted in the Criminal Code duplicates the model of horizontal regulation (albeit narrowed - constituting an element of intelligence activity) with the adopted criminal type of responsibility.

Within the framework of the privileged types, the legislator has retained the previously occurring variant of the offence of espionage, which consists of collecting, storing or entering an information system in order to obtain messages with a view to providing them to foreign intelligence, or reporting a readiness to act for foreign intelligence against the Republic of Poland (Article 130 § 3).

In addition to the aforementioned privileged type, the legislator added a new type of espionage, consisting in taking part in activities of a foreign intelligence service not directed against the Republic of Poland, conducted on its territory without the consent of a competent body granted under separate regulations, punishable by imprisonment from 6 months to 8 years. This is a significant regulatory change with

[35] *Słownik języka polskiego PWN* (Eng. PWN Dictionary of the Polish Language), vol. 1, M. Szymczak (ed.), Warszawa 1999, p. 365.

regard to the offence of espionage, as previously the Criminal Code did not penalise activity consisting in taking part in activities of foreign intelligence not directed against the Republic of Poland, i.e. not threatening or violating the external or internal interests of the Polish state. During the debate on the draft, as an example of such activities, Minister Stanisław Żaryn pointed to activities of a foreign intelligence service conducted on the territory of the Republic of Poland focusing on the recognition of a national minority originating from that country[36]. It should be noted that the legislator introduced into the regulation in question a peculiar counter-type, excluding criminal liability of persons participating in the activities of foreign intelligence, covered by the so-called primary consent of an authorised body. These authorities include the Head of the ABW and the Head of the Military Counterintelligence Service (hereinafter: SKW), as well as the Head of the Foreign Intelligence Agency (hereinafter: AW) and the Head of the Military Intelligence Service (hereinafter: SWW). As indicated in the explanatory memorandum to the draft act (…) *a necessary condition for the issuance of such consent will be that the Head of the relevant service obtains information on the objectives and course of the activity conducted and that such activities are not harmful to the interests of the Republic of Poland*[37]. With regard to the issuance of primary consent, several important issues should be noted. Firstly, the legislator narrowed the elements of the offence specified in Article 130 § 6 of the Criminal Code exclusively to taking part in the activity of a foreign intelligence service not directed against the Republic of Poland conducted on its territory. This was confirmed in the terms of expressing this consent, providing in Article 8a, Section 1 of the ABW and AW Act and in Article 9a of the *Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service* (hereinafter: the SKW and SWW Act) that the heads of these services may grant consent for participation in foreign intelligence activity conducted on the territory of the Republic of Poland in a situation where it is conducted by an organ or service of another state, guided by the premise of not infringing the interest of the Republic of Poland indicated in these provisions. The formulation constructed in this way means that both the privileged type itself and, consequently, the primary consent do not cover conduct consisting in acting for the benefit of foreign intelligence. Secondly, the use of the phrase "taking part in the activity of foreign intelligence services"

[36] Statement of 14 VI 2023 by Stanisław Żaryn, Secretary of State in the Chancellery of the Prime Minister, Government Plenipotentiary for the Security of the Information Space of the Republic of Poland, during the meeting of the Extraordinary Committee for Changes in the Codifications considering the draft law, iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?rok=2023&month=06&page=5#D535320871BCC086C12589CC00473889 [accessed: 28 VIII 2023].

[37] Explanatory Memorandum to *the Parliamentary Draft Act amending the Act*…, p. 14.

in the description of the attributes causes a clear distinction between the primary consent and the subsequent consent referred to in Article 22b(2a) of the ABW and AW Act and Article 27a(2a) of the SKW and SWW Act, which were added by the act. When interpreting these regulations linguistically, it is clearly stated that the primary consent may be granted with regard to the activity of foreign intelligence conducted on the territory of the Republic of Poland if it does not infringe upon the interest of the Republic of Poland, whereas the subsequent consent may be granted only in the situation when such activity is conducted by intelligence of an allied state (more about which later in this article). The obvious result of the linguistic interpretation in this respect is in conflict with the content of the justification to the draft act, in which it is indicated that (…) *the draft also allows for the possibility of conducting on the territory of the Republic of Poland by allied services activities not aimed at the interests of Poland*[38]. Adopting the reasoning presented in the explanatory memorandum would, however, stand in clear contradiction to the fundamental principle of the prohibition of synonymous interpretation[39], with the result that the only acceptable understanding of the norm is the result of linguistic interpretation presented. Thus, in the case of primary consent, the heads of services authorised to give consent are not subjectively limited to allied services only, and the only premise they must be guided by is the potential effect of not infringing, by such activity, the interest of the Republic of Poland. Thirdly, in the context of the wording of the above-mentioned premise, the possibility of withdrawal of the granted consent by the service that issued it in the situation of ascertaining the occurrence of potential infringement of the interest of the Republic of Poland in the course of conducting the activity of a foreign intelligence service also seems obvious. The service issuing the consent is thus forced to constantly monitor intelligence activities. This may, however, be difficult, as this consent lacks solutions analogous to follow-up consent in the form of, inter alia, (…) *ongoing information on the scope of the intelligence activities conducted*. As it seems, this differentiation indicates a certain oversight on the part of the legislator. Withdrawal of consent is also connected with the risk of criminal liability for a person who, despite its withdrawal, continued intelligence activities currently assessed as interfering with the interests of the Republic of Poland. Fourthly, the request for primary consent must precede the initiation of the person's participation in the foreign intelligence activity and must be made not by the person but by an authority or service of another state, through bilateral contacts between the services. That authority or service, through the same contacts, should be informed of the withdrawal of consent.

[38] Ibid.

[39] The prohibition on attributing the same meaning within an act or branch of law to different phrases and concepts.

The authority or service requesting consent must be covered by the consent to cooperate referred to in Article 8 of the ABW and AW Act and Article 9 of the SKW and SWW Act[40]. It should be noted that, on the one hand, Article 130 § 6 of the Criminal Code speaks of consent to the activity of foreign intelligence, however, it follows from Article 8a(1) of the ABW and AW Act and Article 9a(1) of the SKW and SWW Act that the heads of the services grant consent to participate in the activity of foreign intelligence. In view of the above, these provisions should be read comprehensively - in such a way that an authority or service of another state, while requesting consent for a specific intelligence activity, at the same time indicates the persons participating in it. The consent given thus assumes a concretised character in relation to the intelligence activity in question and an individualised character in relation to the persons involved. The lack of individualised character of consent would exclude its counter-typical understanding in the context of the principle of individualisation of criminal liability expressed in Article 21 of the Criminal Code. An authority or service of another state should inform the person who is to take or is taking part in their intelligence activity of the issue of consent or its withdrawal.

In addition to giving new wording to Article 130 of the Criminal Code, the amendment also introduced other changes to the Criminal Code. Firstly, the rules for the application of the criminal measure in the form of deprivation of public rights have been modified, which, in accordance with the added Article 40 § 3, in the event of conviction for the crime of espionage as defined in Article 130 § 1-5 or 7-9, will be imposed by the court on an obligatory basis. This is a significant regulatory novelty with regard to the application of this criminal measure, which was previously adjudicated solely on the basis of the judge's optional discretion, after fulfilling the conditions set out in Article 40 § 2 of the Criminal Code. Secondly, by the addition of the new Article 112a of the Criminal Code, the previous - set out in Article 112 of the Criminal Code - principles of the absolute application of the Polish Criminal Law were extended. According to its wording, the Polish Act will apply, irrespective of the provisions in force in the place where the offence is committed, to a Polish citizen and a foreigner in the event of committing an offence by means of an IT system, an ICT system or an ICT network, if the act in the territory of the Republic of Poland has had or could have had the effect of prejudicing the interest of the state in protecting its independence, territorial integrity, external and internal security, defence, foreign policy, international position or scientific or economic potential. The amendment thus goes beyond the crime of espionage, extending its scope of application to all acts prosecuted in the Polish legal order,

[40] The indicated provisions under the Act have been extended to include the possibility of cooperation with international organisations.

committed in the manner indicated therein, i.e. with the use of an IT system, an ICT system or an ICT network, if the act may have had or has had an effect infringing one of the state interests indicated therein[41].

The last of the changes introduced by the Act to the Criminal Code gives new wording to Article 131 of the Criminal Code regulating the institution of active repentance, excluding, in strictly defined situations, the punishability of perpetrators of certain offences of foreseeable lower harmfulness. However, this is a purely consequential change, related to the addition of new types of offences in Article 130 of the Criminal Code.

Scope of amendments to other laws

As indicated at the outset, in addition to amending the criminal provisions, eight laws were amended by means of the Act to, notably to the competency laws of all Polish special services. Most of these changes are a direct consequence of the redefinition of the wording of the crime of espionage and are mainly related to the increased powers of the services responsible for combating these crimes.

Article 130 § 6 of the Criminal Code introduced, as already mentioned, a peculiar counter-type, excluding criminal liability of persons taking part in the activity of foreign intelligence, covered at the same time by the consent of an authorised body. Through amendments consisting in the addition of Article 8a in the ABW and AW Act and Article 9a in the SKW and SWW Act, the Head of the ABW, the Head of AW and the Head of the SKW and the Head of the SWW were authorised to give such consent. In the case of the Head of the ABW and the Head of the AW, the only prerequisite considered for such consent is the possible infringement by such activity of the interest of the Republic of Poland within the scope defined in Article 112a of the Criminal Code, i.e. within the scope of protection of independence, territorial integrity, external and internal security, defence, foreign policy, international position or scientific or economic potential. In the case of the Heads of the SKW and SWW, such a premise is the absence of a possible finding of a breach of state defence, security and combat capability of the Polish Armed Forces or organisational units of the Ministry of National Defence. Moreover, each of the Heads has been obliged to keep a register of consents issued by them and to provide the other Heads with information collected in the register kept by them in order to perform their tasks concerning the expression

[41] The manner in which Article 112a was introduced into the Criminal Code was criticised by the Ombudsman, as expressed during legislative work in the Senate of the Republic of Poland (letter of 19 July 2023, no. II.510.565.2023.PZ).

of the consent in question. In this way, the register is intended to perform the coordination function of the services in the process of granting such consent.

The analysed Act also introduced very important modifications to the powers of the ABW, granted to it in 2016 by the AT Act. Under it, the ABW gained a number of powers directed at preventing, counteracting and combating terrorist incidents, set out primarily in Chapter 2 (*anti-terrorist activities preventing terrorist incidents*) – which concern, among others, under Article 9 of that Act, carrying out so-called covert operations against foreigners, and in provisions then added to the ABW and AW Act, including Article 22b (on the secret cooperation with the ABW of a perpetrator of an espionage offence or a suspected perpetrator of a terrorist offence nature), Article 32a (concerning the assessment by the ABW of the security of information and communication systems), Article 32b (concerning the provision, at the request of the Head of the ABW, of information on the construction, functioning and principles of operation of information and communication systems) and Article 32c (concerning the blocking of the availability in an information and communication system of specific information data or information and communication services connected with an event of a terrorist nature). The anti-espionage law analysed extended all the powers indicated, beyond the hitherto exclusive area of terrorist offences, also to the crime of espionage[42]. As indicated in the explanatory memorandum to the draft act, (…) *the adoption of* [this] *legal solution is necessary due to the need to minimise the impact of adverse effects in the regulated matter arising as a result of the armed conflict in Ukraine, in particular the significantly increased activity of intelligence activities directed against Poland by the services of the Russian Federation and Belarus*[43].

As a result of the above changes, according to Article 9(1) of the AT Act, in order to recognise, prevent, combat and detect terrorist offences or the offence of espionage and to prosecute their perpetrators, the Head of the ABW may order, for a period not exceeding 3 months, an undercover operation to be carried out against a person who is not a citizen of the Republic of Poland and in relation to whom there is a concern as to the possibility of his/her conducting terrorist activities or committing a crime of espionage, which may include:

1) obtaining and recording the content of conversations conducted with the use of technical means, including by means of telecommunications networks;

[42] The scope of the amendments in question prompted the Legislative Bureau of the Sejm to submit a proposal to amend the title of the AT Act by extending its material scope to include the offence of espionage. However, the MPs did not approve the proposal.

[43] Explanatory Memorandum to *the Parliamentary Draft Act amending the Act*…, p. 15.

2) obtaining and recording the image or sound of persons from premises, means of transport or places other than public places;
3) obtaining and recording the content of correspondence, including correspondence conducted by means of electronic communication;
4) obtaining and recording data contained on computer data carriers, telecommunication terminal equipment, information and data communication systems;
5) gaining access to and controlling the content of consignments.

Analysing the wording of the provision of Article 22b of the ABW and AW Act, it should be pointed out that, as of 2 July 2016, it provided for the possibility of the Head of the ABW (on the basis of the SKW and SWW Act - the Head of the SKW), where it is justified by reasons of state security, to waive the obligation to notify the competent prosecutor of a justified suspicion that a crime has been committed and of a person who, according to the information or materials obtained by the ABW (SKW), may be its perpetrator, if the information or materials obtained by the ABW (SKW) in the course of performing the tasks referred to in Article 5(1) of the ABW and AW Act (in Article 5(1) of the SKW and SWW Act), indicate the commission of an offence of espionage or make it probable that an activity aimed at committing a terrorist offence has been committed. By virtue of the amended Act, this entitlement has been extended, by sec. 2a added to Article 22b of the ABW and AW Act, by the possibility of this waiver, also in the case of the perpetrator of the offence referred to in Article 130 § 6 of the Criminal Code (i.e. espionage not directed against the Republic of Poland), when the intelligence of an allied state in whose activities the person participated - firstly, discloses the circumstances of the committed act or the conducted activity; secondly, undertakes to continue to conduct it within the framework of secret cooperation with the ABW or to provide current information on the scope of activities conducted by this intelligence - obtaining a subsequent consent in accordance with the principles set forth in Article 8a. The same power was also obtained, by virtue of paragraph 2a added to Article 27a of the SKW and SWW Act, by the Head of the SKW. The legislator did not provide for the possibility of granting the indicated subsequent consent by the Heads of the AW and the SWW, although they grant the primary consent. As it seems, this is a deliberate procedure, as the sequence of events described in the normatively indicated provisions de facto concerns the situation of recognition by the Polish counterintelligence service, i.e. the ABW or the SKW, of persons participating in activities of foreign intelligence services not directed against the Republic of Poland, but conducted in the territory of the Republic of Poland, to whose activities, prior to the formal institution of preparatory proceedings, the intelligence service of an allied state, which is behind these activities, admits and discloses the circumstances

of the committed act or conducted activities, undertaking to continue conducting them jointly with the ABW (or SKW) or to provide current information on the scope of their activities. As it seems - the project's explanatory memorandum does not contain such information - the purpose of this regulation, which introduces a kind of 'abolitionist act', is to secure Poland's allied cooperation by giving counterintelligence services the right to 'legalise' such activities in order to pursue common strategic interests. This reasoning is confirmed by the legislature's use of the phrase 'intelligence of an allied state' and not, as in the case of the primary consent, 'foreign intelligence'. It should also be noted that the Act does not define the concept of allied state intelligence (as discussed in more detail earlier). In understanding the concept of an allied state, reference should be made to doctrinal considerations developed on the basis of the so-called reciprocity principle set out in Article 138 of the Criminal Code. As Kardas points out:

> (…) the concept of an allied state is normative in nature, related to regulations contained in acts of public international law. An allied state is a state that, under international agreements or treaties (multilateral or bilateral), has been recognised as a political and military ally of the Republic of Poland. In other words, it is a state with which the Republic of Poland has concluded a political or military alliance. Allied states of the Republic of Poland include, inter alia, all states remaining in the NATO structure since the Republic of Poland's accession to the pact[44].

Thus, primary consent may be granted for participation in the activities of a foreign intelligence service conducted on the Polish territory if this does not infringe on the interests of the Republic of Poland. The subsequent consent, on the other hand, under the same conditions, may be granted only in the situation of conducting activities by the intelligence of an allied state. This consent, similarly to the primary consent, may be withdrawn by the ABW or SKW in the situation of failure to fulfil the conditions of its granting. Its withdrawal may take place: firstly, in a situation where the conducted activity begins to infringe the interests of the Republic of Poland; secondly, when information is obtained indicating the misleading of Polish services with regard to the circumstances of the committed act or the conducted activity; thirdly, when the intelligence of an allied state ceases to conduct further activity jointly with the ABW (or SKW) or ceases to provide current information on the scope of its activities.

In addition, in accordance with the amended wording of Article 32a of the ABW and AW Act, the ABW was given the power to conduct security

[44] P. Kardas, in: *Kodeks karny*…, Article 138.

assessments of ICT systems of public administration bodies or ICT networks covered by the uniform list of objects, installations, devices and services constituting critical infrastructure, as well as ICT systems of owners, sole and dependent owners of objects, installations or devices of critical infrastructure referred to in Article 5b(7)(1) of the *Act of 26 April 2007 on crisis management*, or data processed in these systems. This power has been granted not only, as before, in order to prevent and counteract terrorist incidents and to detect and prevent terrorist offences in this area as well as to prosecute their perpetrators, but also in order to prevent and counteract events that make the commission of the offence of espionage probable and to recognise, detect and prevent the crime of espionage.

In the same scope, the Head of the ABW obtained, by virtue of the amended Article 32b of the ABW and AW Act, the power to demand from the above-mentioned entities to present information on the construction, functioning and principles of exploitation of the ICT systems held, including information containing computer passwords, access codes and other data enabling access to the system and their use, in order to respond to and prevent incidents of a terrorist nature or making it probable that an offence of espionage has been committed, concerning these systems or data, as well as to recognise, prevent and detect offences of a terrorist nature and an offence of espionage in this area and to prosecute their perpetrators.

Similarly, with regard to the offence of espionage, the possibility was extended for the Head of the ABW to apply, on the basis of Article 32c of the ABW and AW Act, for the application by the court, after obtaining the written consent of the Prosecutor General, of the so-called blocking accessibility, i.e. blocking by the service provider supplying electronic services the accessibility in the ICT system of specific IT data connected with an event of a terrorist nature or making it probable that an offence of espionage has been committed, or specific ICT services serving or used to cause an event of a terrorist nature or making it probable that an offence of espionage has been committed. This power becomes particularly important in the context of Article 130 § 9 of the Criminal Code in which the legislator directly included the activities of conducting disinformation as an element of intelligence activities. Until now, only Article 180 of the *Telecommunications Act of 16 July 2004* obliged telecommunications companies to immediately block telecommunications connections or information transmissions, at the request of authorised entities (i.e. Police, the Internal Supervision Bureau, the Border Guard, the Internal Inspectorate of the Prison Service, the State Protection Service, the Internal Security Agency, the Military Counterintelligence Service, the Military Police, the Central Anticorruption Bureau and the National Revenue Administration), if these calls could threaten the defence, state security and public safety and order, or to allow them to carry out such blocking. The amended provision in the ABW and

AW Act - going beyond the previous limitation to offences of a terrorist nature and encompassing within its scope also the offence of espionage - gives a basis for the service provider supplying electronic services to block the availability in an ICT system of specific IT data or specific ICT services, disseminating false or misleading information in order to cause serious disturbances in the system or economy of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member, or to induce a public authority of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member to take or refrain from taking specific actions.

In the context of the changes described above, it should be added that the Act also made changes to Article 32aa of the ABW and AW Act, added to it in 2018 by the *Act of 5 July 2018 on the national cybersecurity system*, obliging the ABW to implement, operate and coordinate the functioning of the early warning system for threats occurring online. Similar to the amendments discussed earlier, the purpose of operating the system has been extended - beyond preventing, countering and preventing terrorist incidents and beyond identifying, detecting and preventing terrorist offences and prosecuting their perpetrators - to preventing, countering and preventing incidents that make it likely that an espionage offence has been committed and to identifying, detecting and preventing the crime of espionage and prosecuting its perpetrators.

In addition, (…) *in order to build a coherent catalogue of sanctions, as well as preventive measures*[45], through amendments to the pension law for officers of uniformed services and professional soldiers, the crime of espionage was added to the catalogue of offences the commission of which, confirmed by a valid court judgment, by a soldier, officer or police pensioner results in the loss of pension rights.

In addition to the changes indicated, the Act introduced several additional changes to the competence acts of the special services, not directly related to the changes in the scope of the crime of espionage, being the result of the experience of the functioning of the services, such as the extension, in the case of the ABW, AW, SKW and SWW, of the authority to undertake cooperation not only with the competent authorities and services of other states, but also with international organisations.

One of these changes is particularly significant from the perspective of overall state security. This is because the Act amended the Homeland Defence Act by establishing, in Article 616a, a prohibition - without a permit - on photographing, filming or otherwise recording the picture or image of facilities of particular importance for the security or defence of the state, facilities of the Ministry of National

[45] Explanatory Memorandum to *the Parliamentary Draft Act amending the Act*…, p. 14.

Defence not recognised as facilities of particular importance for the security or defence of the state, facilities of critical infrastructure, if they have been marked with a graphic sign expressing this prohibition, and persons or movables located in these facilities. The marking of a facility with a sign prohibiting photography is to be decided by the authority competent for the protection of that facility, taking into account the risks to its security. Coupled with this prohibition is a new offence punishable by imprisonment or a fine for any person who, without authorisation, photographs, films or otherwise records an image of an object marked with a 'no photography' sign or an image of a person or movable property within such a facility.

Summary

Summing up the above considerations, it should be indicated that the Act amending the Criminal Code and certain other acts passed by the Sejm of the Republic of Poland on 17 August 2023, which significantly changed the way in which the offence of espionage is penalised in Poland, must be assessed positively. After several years of legislative work, which resulted from the demands made both by the representatives of the legal doctrine and practitioners dealing with this prohibited act, an amendment appeared, which, in principle, adjusted the provisions of the Criminal Code in this area to the current geopolitical situation, shaped mainly by the high threat of new open armed conflicts and aggressive non-military actions described in the doctrines of war. Furthermore, this amendment corresponds with the threats posed by technological advances and the described modus operandi of potential perpetrators of the crime of espionage.

It is obvious that the adopted changes, including, inter alia, the use of new notions in the attributes of criminal acts, which have not been present in the legal system so far, including many notions which are broad in meaning and susceptible to diverse interpretations, will have to be verified in terms of their effectiveness through the practice of criminal proceedings. This practice will bring an answer in particular, to the question as to whether the practical understanding of the new provisions does not, as a consequence, deprive the criminalisation of a certain spectrum of behaviours recognised by the services as hybrid threats carried out by foreign special services.

In the coming years, analyses of this effectiveness should be undertaken, based on the experience from the practice in applying the new regulations. If the legal solutions adopted prove to be ineffective, then consideration should be given to reconsidering the proposals that were made during the legislative process described above, including the definition of intelligence activities formulated at that time.

Bibliography

Burczaniuk P., *Przestępstwo szpiegostwa – rys historyczny, aktualne regulacje na tle doświadczeń praktycznych i analizy prawno-porównawczej wybranych państw* (Eng. The crime of espionage - historical background, current regulations against the background of practical experience and comparative legal analysis of selected countries), in: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, P. Burczaniuk (ed.), Warszawa 2017, pp. 86–107.

Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-211a (cz.1) (Eng. Criminal Code. Specific part. Volume II. Commentary to Articles 117-211a (Part 1)), W. Wróbel, A. Zoll (eds.), Warszawa 2017.

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia* (Eng. Hybrid warfare - the challenge of the future? Selected issues), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, special issue: *Wojna hybrydowa*, pp. 39–50.

Słownik Języka Polskiego PWN (Eng. PWN Dictionary of Polish Language), vol. 1, M. Szymczak (ed.), Warszawa 1999.

Wojnowski M., *Mit "wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku* (Eng. The myth of 'hybrid war'. Conflict on the territory of the Ukrainian state in the light of Russian military thought of the XIX-XXI centuries), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, special issue: *Wojna hybrydowa*, pp. 7–38.

Internet sources

Amendments to the Criminal Code related to threats to state security, The Ministry of Justice, 29 III 2022, https://www.gov.pl/web/sprawiedliwosc/zmiany-w-kodeksie-karnym-zwiazane-z-zagrozeniem-bezpieczenstwa-panstwa [accessed: 28 VIII 2023].

Consideration of the Commission's report on the parliamentary draft act amending - the Criminal Code and certain other acts (nos. 3232, 3232-A and 3358), iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=2#0CD6003114C05652C12588FB0033AD73 [accessed: 28 VIII 2023].

Explanatory Memorandum to *the Parliamentary Draft Act on amending the Criminal Code and certain other acts* (print no. 3232), https://orka.sejm.gov.pl/Druki9ka.nsf/0/F53D07E65F8EC17AC12589B1003F2A96/%24File/3232.pdf [accessed: 28 VIII 2023].

McKew M.K., *Doktryna Gierasimowa, czyli rosyjski sposób na wojnę: chaos, a nie bomby* (Eng. The Gerasimov doctrine, or the Russian way to war: chaos, not bombs), Onet, 6 IX 2017, https://wiadomosci.onet.pl/swiat/doktryna-gierasimowa-czyli-rosyjski-sposob-na-wojne-chaos-a-nie-bomby/svh4p0h [accessed: 28 VIII 2023].

Mikowski M., *Wiceszef MS: zmiany ws. surowszych kar za szpiegostwo są już gotowe* (Eng. Deputy Minister of Justice: amendments on tougher penalties for espionage are ready), PAP, 23 X 2022, https://www.pap.pl/aktualnosci/news%2C1460354%2Cwiceszef-ms-zmiany-ws-surowszych-kar-za-szpiegostwo-sa-juz-gotowe.html [accessed: 28 VIII 2023].

Recording of the meeting of the Sejm Extraordinary Committee for Amendments to the Codifications - 14 VI 2023, iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?rok=2023&month=06&page=5#D535320871BCC086C12589CC00473889 [accessed: 28 VIII 2023].

Recording of the 77th sitting of the Sejm - 13 VI 2023, iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=9#1C429C6BE7B92E29C12588FB0033AB2F [accessed: 28 VIII 2023].

Recording of the 65th sitting of the Senate of the Republic of Poland of the 10th parliamentary term - 26 July 2023, https://av8.senat.pl/10Sen651 [accessed: 28 VIII 2023].

Vote no. 46 at the 78th sitting of the Sejm on 07-07-2023 at 19:21:18, https://www.sejm.gov.pl/sejm9.nsf/agent.xsp?symbol=glosowania&NrKadencji=9&NrPosiedzenia=78&NrGlosowania=46 [accessed: 28 VIII 2023].

Russian Internet sources

Герасимов В., *Ценность науки в предвидении*, "Военно-промышленный курьер", 27 II 2013, https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html [accessed: 28 VIII 2023].

Фельгенгауэр П., *Добиться превосходства над остальным человечеством Начальник российского Генштаба формулирует программу подготовки к масштабной войне*, Новая газета, 9 III 2019, https://novayagazeta.ru/articles/2019/03/09/79808-dobitsya-prevoshodstva-nad-ostalnym-chelovechestvom [accessed: 28 VIII 2023].

Legal acts

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

Act of 11 March 2022 on the defence of the homeland (consolidated text of Journal of Laws of 2024, item 248).

Act of 5 July 2018 on the national cybersecurity system (consolidated text of Journal of Laws of 2023, item 913, as amended).

Act of 10 June 2016 on antiterrorist activities (consolidated text of Journal of Laws of 2022, item 2632).

Act of 26 April 2007 on crisis management (consolidated text of Journal of Laws of 2023, item 122).

Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service (consolidated text of Journal of Laws of 2023, item 81, as amended).

Act of 16 July 2004 telecommunications law (consolidated text of Journal of Laws of 2022, item 1648, as amended).

Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency (consolidated text of Journal of Laws of 2023, item 1136, as amended).

Act of 6 June 1997 - Criminal Code (consolidated text of Journal of Laws of 2022, item 1138, as amended).

Case law

Judgment of the Court of Appeal in Białystok of 28 XI 2016, ref. no. II AKa 96/16.

Judgment of the Court of Appeal in Warsaw of 24 XI 2017, ref. no. II AKa 269/17.

Judgment of the Regional Court in Gdańsk of 17 V 2005, ref. no. IV K 86/05.

Judgment of the Regional Court in Katowice of 19 X 2015, ref. no. V K 141/15.

Judgment of the Regional Court in Warsaw of 11 VIII 2022, ref. no. XVIII K 78/22.

Judgment of the Regional Court in Warsaw of 21 II 2022, ref. no. XVIII K 58/20.

Judgment by the Regional Court in Warsaw of 8 III 2019, ref. no. XII K 176/18.

Judgment of the Regional Court in Warsaw of 23 III 2016, ref. no. XVIII K 110/15.

Judgment of the Regional Court in Warsaw of 22 XII 2010, ref. no. VIII K 272/10.

Judgment of the Military Regional Court in Warsaw of 29 IV 2019, ref. no. So 5/19.

Judgment of the Military Regional Court in Warsaw of 26 IV 2016, ref. no. So 1/16.

Judgment of the Military Regional Court in Warsaw of 3 XI 2005, ref. no. So 37/05.

Judgment of the Military Regional Court in Warsaw of 11 IV 2001, ref. no. So 24/00.

Other documents

National Security Strategy of the Republic of Poland 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [accessed: 28 VIII 2023].

Piotr Burczaniuk, PhD

Doctor of Law, Assistant Professor at the Institute of Legal Sciences of Cardinal Stefan Wyszyński University, legal counsel, legislator. He specialises in legal theory, business law and IT law.

Contact: p.burczaniuk@uksw.edu.pl