Teka Kom. Praw. – OL PAN, 2017, 289–298

CLASSIFIED INFORMATION AND ITS PROTECTION IN POLISH ARMED FORCES. GENERAL ASSUMPTIONS

Paweł Zając

Department of Theory and Philosophy of Law
War Studies University

Summary. Nowadays, continuous technological progress, especially in the fields of telecommunications, information becomes the primary and most important source of knowledge. In the structure of the armed forces, it takes on special significance, since its disclosure may be dependent on the internal security of the state, and thus on its sovereignty and independence. Information becomes too valuable to allow for it uncontrolled disclosure. Therefore, the Polish legislator, in order to safeguard against any intervention by foreign services in the field of obtaining classified information, introduced into the legal order certain legal tools and institutions which protected them.
The aim of the article is to show what is a classified information, together with a cross-sectional presentation of concrete legal solutions, as provided in Polish legislation in relation to armed forces, in the matter of mechanisms blocking access to classified information.

Key words: national security, sensitive information, army, security clause

The issue of protecting classified information in the armed forces is undoubtedly one of the most important aspects of national security. Often in the nomenclature we meet with the notion of "information advantage" constitu ting the principle rule in practicing the art of war[1]. Information processed in military structures is one of the most sensitive in the state, therefore, regardless of the form of information and the ways by which it is processed should always be properly secured[2]. In the case of soldiers, the protection of classified information takes on special significance because it comes from two sources. First, from the statutory injunction, contained in Art. 51 sec. 1 of Act on the

[1] R. Kawka, *Organizacja systemu ochrony informacji niejawnych w siłach zbrojnych RP*, in: *Ochrona informacji niejawnych i danych osobowych. Wymiar teoretyczny i praktyczny*, eds. S. Topolewski, P. Żarkowski, Wydawnictwo Uniwersytetu Przyrodniczo–Humanistycznego, Siedlce 2014, p. 47.

[2] K. Chałubińska–Jentkiewicz, *Ochrona informacji niejawnych a organizacja służby żołnierzy i funkcjonariuszy zatrudnionych w strukturach obronności i bezpieczeństwa państwa* , in: *Prawo wojskowe*, eds. W. Kitler, D. Nowak, M. Stepnowska, Wolters Kluwer, Warszawa 2017, p. 576.

military service of professional soldiers[3] and Art. 64 of Act on the universal duty of defence of the Republic of Poland[4], according to which, professional soldiers are required to keep confidential all classified information they have been acquainted with during or in connection with active military service, including information that is a secret of another state protected on the basis of reciprocity under international agreements. The second source is moral responsibility and duty, which each soldier imposes upon himself making military oath declaring that he will: "to serve the Republic of Poland faithfully, to defend its independence and borders"[5]. Classified information in the armed forces will always be related to the defence of the State, so their disclosure will be a denial of fidelity and misappropriation against the Republic of Poland.

1. DEFINITION AND CLASSIFICATION OF CLASSIFIED INFORMATION

In Polish law system, the role of the "constitution" in the protection of classified information, including those created and processed in military structures, fulfills the Act on Protection of Classified Information of August 5, 2010[6], in which the legislator normalized such issues as:

- classification of classified information,
- organise the protection of classified information,
- the proceedings of the screening to be carried out in order to determine whether or not a person covered by it, will give you a guarantee of secrecy,
- personnel security,
- physical security measures.

A number of executive acts have been issued on this basis, which specify the statutory provisions. Important legal solutions are also included in international law. We can not forget that Poland, through its presence in international organizations, including the military, is obliged to observe the legal norms issued by institutions like European Union or NATO[7].

---

[3] "Journal of Laws" of 2003, No. 179, item 1750, as amended.

[4] "Journal of Laws" of 1967, No. 44, item 220, as amended.

[5] Act on military oath of October 3, 1992, "Journal of Laws" No. 77, item 386, as amended.

[6] "Journal of Laws" No. 182, item 1228, as amended [hereinafter referred to as the "Act"].

[7] This is related to Art. 91 sec. 3 of the Constitution, according to which "If an agreement, ratified by the Republic of Poland, establishing an international organization so provides, the laws established by it shall be applied directly and have precedence in the event of a conflict of laws" [The Constitution of the Republic of Poland of 2nd April, 1997, "Journal of Laws" No. 78, item 483, as amended]. For more see: L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, ed. 4, Wolters Kluwer Polska, Warszawa 2017, pp. 164–171; J. Kusociński, *Ustrój konstytucyjny Rzeczypospolitej Polskiej*, Difin, Warszawa 2013, pp. 42–45.

The classified information is defined as information, "whose unauthorized disclosure of which would or might result in harm to the Republic of Poland or would be from the point of view of its adverse interests, also in the course of their development, and regardless of the form and the way in which they express" (Art. 1 of the Act). Classified information may be generated in the form of a document or presented by presentation or verbal content[8].

The legislator has introduced a classification of classified information which is based on an assessment of the effect that their non-legitimate declassification may have[9]. The nature of the clause must therefore remain in close relation with one of the four categories of damage provided in the Act. In this way classified information is classified as: top secret, secret, confidential, reserved.

The clause "top secret" is given to those classified information, which disclosure will cause exceptionally grave damage for State. For example: threaten the internal security or the constitutional order of the Republic of Poland; weaken the defensive readiness of the Republic of Poland; lead or may lead to the identification of officers, soldiers or employees of the service responsible for implementation of the tasks of intelligence or counterintelligence, who perform emergency operations reconnaissance (Art. 5 sec. 1 of the Act).

Information classified "secret" clause is given when the unauthorized disclosure of which would cause serious damage to the Republic of Poland by prevents the implementation of tasks connected with the protection of sovereignty or the constitutional order of the Republic of Poland. In such a situation may also occur: interfere with the preparation of the defence of the State or functioning of the armed forces of the Republic of Poland. Violation of the clause can also will make more difficult to perform emergency operations carried out reconnaissance in order to ensure the security of the State or prosecution of perpetrators by the departments or institutions authorized to do so (Art. 5 sec. 2 of the Act).

Information classified "confidential" clause is suitable if the unauthorized disclosure of which would cause harm to the Republic of Poland by the fact that, will make difficult implementation of defensive measures, or negatively affect the combat capacity of the armed forces of the Republic of Poland or will impede the execution of the tasks of the departments or institutions responsible for the protection of the essential interests of the security of the Republic of Poland (Art. 5 sec. 3 of the Act).

---

[8] T. Szewc, *Ochrona informacji niejawnych. Komentarz*, Wydawnictwo C.H. Beck, Warszawa 2007, p. 65.

[9] R. Kawka, *Bezpieczeństwo dokumentów*, in: *Ochrona informacji niejawnych. Teoria i praktyka*, eds. M. Kubiak, S. Topolewski, Wydawnictwo Uniwersytetu Przyrodniczo–Humanistycznego, Siedlce 2013, p. 53.

The lowest classified clause is "restricted". Applies to information not previously assigned a higher classification, and which the unauthorized disclosure of which could have a detrimental effect on the performance of the public authorities or other organizational units tasks in the field of national defence, foreign policy, public safety, respect for the rights and freedoms of citizens, criminal justice or economic interests of the Republic of Poland (Art. 5 sec. 4 of the Act).

At this point, the question arises whether the legislator in the above classification did not use too general wording, because it is hard to determine the difference between "interference of the preparation of the defence" and "making difficult the implementation of defensive measures", because in fact they form a single semantic category.

Therefore, it should take into account the possibility of detailed regulations, what information strictly related to for eg. military service, should be classified into the category of classified information.

According to the Act, about classification of information decides the person who is authorized to sign the document or other material (Act art. 6 § 1). Therefore, the entire responsibility rests with the concrete human individual. It is widely known that what is important for some, for others may not have any significance – therefore, the legal structure may raise some doubts. However, the legislator has protected himself against the possibility of making a mistake by a person by introducing a response system, assuming that the recipient of the materials in the case statement understatement or overstatement of classification may ask the person who gave it, or her supervisor with a request for a change. In case of refusal, the matter should be submitted to the Military Counterintelligence Service [MCS] (Art. 9 of the Act). As a result, the document is suspended and until it settles, it does not exist in circulation. Another form of control is the obligation of military commanders to review materials to determine whether they meet the statutory protection requirements, not less than once every five years (Art. 6 § 4 of the Act).

The organization of the protection of classified information is based on several basic principles. The most important were grouped in art. 8 of the Act stipulating that classified information to which a security classification has been assigned:

- can only be made available to an authorized person,
- they must be processed under conditions that prevent their unauthorized disclosure;
- they must be protected according to the security classification provided.

2. INSTITUTIONAL PROTECTION OF CLASSIFIED INFORMATION

Institutional protection includes the creation of special organizational units, the main task of which is to protect classified information[10]. According to the Act, the function of the National Security Authority fulfill the Chief of the Integral Security Agency. However, in the context of the functioning of the armed forces, it performs its tasks through the Chief of MCS.

Therefore, the first defence mechanism is entrusting the supervision of the functioning of the systems of protection of classified information in military units to the Military Counterintelligence Service – a special State protection service, competent to protect against internal threats to the defence of the State[11]. Within its framework, was created a special division, which only deals with the study of movement and the protection of classified information. As a result, the protection system is not fragmented between the various institutions, resulting in a better response in the detection of pathological situations.

In individual units of the armed forces, the commanders of military units are responsible for the information protection in coordination with MCS (commanders, bosses or directors). They are assisted by a agent for the protection of classified information appointed by them for the protection of classified information (Art. 14 of the Act)[12]. Agents of individual divisions of the Polish armed forces like Chief of the General Staff of the Polish Armed Forces, Commander of the Operational Type of Armed Forces or Armed Forces Support Arms, are designed to coordinate and oversee the implementation of tasks in the field of protection of classified information and are committed to information security risk management – the process of analysis and evaluation of the combination of the probability of an adverse event and its consequences[13].

Agents are also responsible for carrying out training course, which is completed with the positive transition of the screening process, is a condition *sine qua non* for access to classified information. Training, in addition to the aspect

[10] It should be noted here that the Act refers to all state structures in which classified information is processed. However, in view of the accepted subject matter of the article, only the provisions concerning military structures will be discussed, with their content adapted to the specificities of the armed forces.

[11] Act on Military Counterintelligence Service and the Military Intelligence Service of June 23, 2006, "Journal of Laws" No. 104, item 709, as amended, art. 1. See: S. Topolewski, *System ochrony informacji niejawnych*, in: *Ochrona informacji niejawnych. Teoria i praktyka*, pp. 34–35.

[12] A. Jędruszczak, *Odpowiedzialność kierownika jednostki oraz pełnomocnika do spraw ochrony informacji niejawnych*, in: B. Nowakowski, A. Jędruszczak, A. Gałach, *Ochrona danych osobowych, informacji niejawnych i systemów teleinformatycznych w sektorze publicznym*, Wydawnictwo C.H. Beck, Warszawa 2013, pp. 135–136.

[13] R. Kawka, *Organizacja systemu ochrony informacji niejawnych w siłach zbrojnych RP*, p. 48.

of gaining and expanding knowledge, it also helps the teacher training discern whether the participant has the character traits allowing it to work with information containing secret military[14].

The second stage of the admission of a soldier or employee of armed forces units to contact with the classified information is a positive transition of the investigating procedure (the ordinary authorizing the processing of information classified as "confidential" or "restricted"; or extended – with a "secret" and "top secret" classified clause), the aim of which is to check whether the person subject to give a pledge of secrecy (in other words, whether it is capable of ensuring the protection of information)[15]. In the case of soldiers in active military service and reserve soldiers, they are obliged to undergo such a procedure if they have or will have access to classified information in connection with the allocation of emergency or mobilization allowances[16]. The investigation verifies that there are any doubts about participation, cooperation or support by a person being screened, espionage, terrorism, sabotage or other action against the Republic of Poland (Art. 24 sec. 1 of the Act). This procedure starts with a questionnaire which is then verified by the relevant service.

Competence to conduct the proceedings is provided by the Military Counterintelligence Service, which implements them against officers, soldiers and employees, as well as persons applying for admission to the service or work in MCS and to: the Chief of the ICA, the Chief of the MIS, the Chief Commander and the persons assigned to these positions, the security agents and their deputies, as well as the persons envisaged for these positions in the ICA, MCS and MIS. In addition, it conducts extensive investigations on soldiers and civil servants of the Ministry of National Defence and organizational units subordinated to or supervised by the Minister of National Defence, defence atheists in foreign missions and soldiers in active service assigned to service posts in other organizational units (Art. 23 of Act).

MCS also conducts screenings before issuing security clearances for authorizing access to classified information international (NATO, the European Union and the European Space Agency)[17].

---

[14] See: A. Turek, *Casus Wikileaks, a wybrane zagadnienia informacji niejawnych*, in: *Ochrona informacji niejawnych. Teoria i praktyka*, p. 212.

[15] A. Jędruszczak, *Udostępnianie informacji niejawnych*, in: B. Nowakowski, A. Jędruszczak, A. Gałach, *Ochrona danych osobowych*, pp.143–144; see: J. Szydłowski, *Postępowania sprawdzające*, in: *Ochrona informacji niejawnych i danych osobowych. Wymiar teoretyczny i praktyczny*, pp. 72–73; more: R. Wądłowski, *Stosowanie przepisów ustawy o ochronie informacji niejawnych – wybrane zagadnienia*, in: *Ochrona informacji niejawnych. Teoria i praktyka*, pp. 79–92.

[16] K. Chałubińska–Jentkiewicz, *Ochrona informacji niejawnych*, pp. 580–581.

[17] It should be noted, that information provided by international organizations or other countries is subject to the Polish classification of security clause. Issuing guidelines for dealing with such information belongs to the Chief of the ISA. See: The Intelligence Security Agency, Guide-

3. PROPER PROTECTION OF CLASSIFIED INFORMATION

The Act and ordinance of Ministry of National Defence No. 47 from December 20, 2012[18], provide for the designated special registry (*kancelaria tajna*) in each armed force unit in which the information classified as "top secret" and "secret" are stored and processed[19]. A registry is a separate organizational unit, subordinate to the security agent, serviced by security staff. It provides the possibility to determine, in all circumstances, where material with a given clause remains and who has read this material[20]. According to the regulation of the Ministry of National Defence, registry should, as far as possible, be arranged in a place consisting of at least three rooms intended for:

– workroom for staff,
– rooms for storage of classified materials,
– rooms intended for acquaintance with classified documents.

Entrance to the registry should lead through a protective zone – a separate area that prevents unauthorized access.

The Act also provides physical security mechanisms of the system which is a system of interrelated organizational projects, human, technical and physical for the protection of the information. Components of the system in particular consist of: preparation of plans, instructions, regulations and procedures; arranging the internal security service or using the services of a licensed security agency; separation, organization and implementation of architectural and building security; protection and surveillance of appropriate protection zones using anti-burglary and attack systems[21].

The safest way to store classified information is their physical form – the form of a document that we can secure in a safe in a special room, which makes access to it difficult. But nowadays it is practically impossible, as most of the documents are created in teleinformatic systems, so that you can quickly send them to authorized persons. Therefore, the armed forces were equipped with appropriate teleinformatic systems such as MIL-WAN. Competencies for admitting ICT systems in military structures are provided by MCS[22].

---

lines for dealing with international classified information, https://www.abw.gov.pl/pl/zadania/ochrona-informacji-nie/7,Ochrona-informacji-niejawnych.html [accessed: 17.10.2017].

[18] "Official Journal of the Ministry of the National Defence" of 2013, item 79.

[19] See also: Council Decision of 23 September 2013 on the security rules for protecting EU classified information, "Official Journal of the European Union" 2013/488/EU; L 274/1.

[20] See: K. Gawęda, *Kancelaria tajna w jednostce organizacyjnej*, in: *Ochrona informacji niejawnych. Teoria i praktyka*, pp. 89–90.

[21] https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-fizyczn/150, BEZPIECZENSTWO-FIZYCZNE.html#16 [accessed: 14.10.2017].

[22] For more see: W. Zagórski, *Zasady bezpiecznego przechowywania i obiegu dokumentów niejawnych*, in: *Ochrona informacji niejawnych. Teoria i praktyka*, pp. 121–148; K. Liderman, *Zarządzanie ryzykiem jako element zapewnienie odpowiedniego poziomu bezpieczeństwa*

Important measures to protect classified information are also the provisions of the Penal Code[23], which provides for a specific category of crime against information. It penalizes conduct that may jeopardize the good of the state by disclosing classified information. The catalog of crimes is included: crime of illegal use of classified and highly confidential information (Art. 265 of Penal Code); crime of disclosure or use of information that he has become aware of in connection with his function, work, public, social, economic or scientific activity (Art. 266 of Penal Code); crime of illegal access to classified information (Art. 267 of Penal Code); crime of destroying classified information (Art. 268 of Penal Code); crime of destroying, damaging, deleting or changing computer data of particular importance to the defence of the country (Art. 269 and 269a of Penal Code); Fraudulent sharing of equipment, computer passwords and access codes for the theft of classified information (Art. 269b of Penal Code). Disclosure of information may also be considered as a foreign intelligence service activity against the Republic of Poland (Art. 130 of Penal Code)[24].

***

In conclusion, the Polish armed forces in the aspect of protection of classified information operate within the limits of the norms provided for in the Act on the protection of classified information. Protection takes two forms: the first institutional, consisting of the appointment of SKW and the agents for the protection of classified information, who are to develop protection plans and anticipate information security risks; and the second one – proper, which includes concrete solutions such as screening, the obligation to conduct specialist training course, the obligation to create special registry, the application of appropriate physical security measures, penalization of pathological behaviors to discourage the disclosure of classified information to unauthorized persons.

It should be emphasized that the system of protection of classified information in the Polish Armed Forces is one of the best in the world, which consists of detailed procedures and multi-dimensional control of individual stages, so that early detection of any irregularities can be detected at an early stage.

teleinformatycznego, "Biuletyn Instytutu Automatyki i Robotyki" 23 (2006), pp. 43–88.

[23] "Journal of Laws" of 1997, No. 88, item 553, as amended.

[24] For more see: M. Leciak, *Karnoprawna ochrona informacji niejawnych. Uwagi w świetle ustawy z dnia 5.08.2010 o ochronie informacji niejawnych*, Wydawnictwo Dom Organizatora, Toruń 2012.

REFERENCES

Chałubińska–Jentkiewicz, Katarzyna. 2017. "Ochrona informacji niejawnych a organizacja służby żołnierzy i funkcjonariuszy zatrudnionych w strukturach obronności i bezpieczeństwa państwa." In Prawo wojskowe, edited by Waldemar Kitler, Dariusz Nowak, and Marta Stepnowska. 575–595. Warszawa: Wolters Kluwer.

Garlicki, Leszek. 2017. *Polskie prawo konstytucyjne. Zarys wykładu*. Ed. 4. Warszawa: Wolters Kluwer Polska.

Gawęda, Krzysztof. 2013. "Kancelaria tajna w jednostce organizacyjnej." In Ochrona informacji niejawnych. Teoria i praktyka, edited by Mariusz Kubiak, and Stanisław Topolewski, 89–105. Siedlce: Wydawnictwo Uniwersytetu Przyrodniczo–Humanistycznego.

Jędruszczak, Anna. 2013. "Udostępnianie informacji niejawnych." In Bogusław Nowakowski, Anna Jędruszczak, and Adam Gałach, Ochrona danych osobowych, informacji niejawnych i systemów teleinformatycznych w sektorze publicznym, 143–144. Warszawa: Wydawnictwo C.H. Beck.

Jędruszczak, Anna. 2013. "Odpowiedzialność kierownika jednostki oraz pełnomocnika do spraw ochrony informacji niejawnych." In Bogusław Nowakowski, Anna Jędruszczak, and Adam Gałach, Ochrona danych osobowych, informacji niejawnych i systemów teleinformatycznych w sektorze publicznym, 135–138. Warszawa: Wydawnictwo C.H. Beck.

Kawka, Robert. 2013. "Bezpieczeństwo dokumentów." In Ochrona informacji niejawnych. Teoria i praktyka, edited by Mariusz Kubiak, and Stanisław Topolewski, 49–70. Siedlce: Wydawnictwo Uniwersytetu Przyrodniczo–Humanistycznego.

Kawka, Robert. 2014. "Organizacja systemu ochrony informacji niejawnych w siłach zbrojnych RP." In Ochrona informacji niejawnych i danych osobowych. Wymiar teoretyczny i praktyczny, edited by Stanisław Topolewski, and Paweł Żarkowski, 47–66. Siedlce: Wydawnictwo Uniwersytetu Przyrodniczo–Humanistycznego.

Kusociński, Jerzy. 2013. *Ustrój konstytucyjny Rzeczypospolitej Polskiej*. Warszawa: Difin.

Leciak, Michał. 2012. *Karnoprawna ochrona informacji niejawnych. Uwagi w świetle ustawy z dnia 5.08.2010 o ochronie informacji niejawnych.* Toruń: Wydawnictwo Dom Organizatora.

Liderman, Krzysztof. 2006. "Zarządzanie ryzykiem jako element zapewnienie odpowiedniego poziomu bezpieczeństwa teleinformatycznego". *Biuletyn Instytutu Automatyki i Robotyki* 23:43–88.

Szewc, Tomasz. 2007. *Ochrona informacji niejawnych. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Szydłowski, Jerzy. 2014. "Postępowania sprawdzające." In Ochrona informacji niejawnych i danych osobowych. Wymiar teoretyczny i praktyczny, edited by Stanisław Topolewski, and Paweł Żarkowski, 71–78. Siedlce: Wydawnictwo Uniwersytetu Przyrodniczo–Humanistycznego.

Topolewski, Stanisław. 2013. "System ochrony informacji niejawnych." In Ochrona informacji niejawnych. Teoria i praktyka, edited by Mariusz Kubiak, and Stanisław Topolewski, 25–48. Siedlce: Wydawnictwo Uniwersytetu Przyrodniczo–Humanistycznego.

Turek, Andrzej. 2013. "Casus Wikileaks, a wybrane zagadnienia informacji niejawnych." In Ochrona informacji niejawnych. Teoria i praktyka, edited by Mariusz Kubiak, and Stanisław Topolewski, 199–215. Siedlce: Wydawnictwo Uniwersytetu Przyrodniczo–Humanistycznego.

Wądłowski, Rafał. 2014. "Stosowanie przepisów ustawy o ochronie informacji niejawnych – wybrane zagadnienia." In Ochrona informacji niejawnych i danych osobowych. Wymiar teoretyczny i praktyczny, edited by Stanisław Topolewski, and Paweł Żarkowski, 79–100. Siedlce: Wydawnictwo Uniwersytetu Przyrodniczo–Humanistycznego.

Zagórski, Włodzimierz. 2013. "Zasady bezpiecznego przechowywania i obiegu dokumentów niejawnych." In Ochrona informacji niejawnych. Teoria i praktyka, edited by Mariusz Kubiak, and Stanisław Topolewski, 121–148. Siedlce: Wydawnictwo Uniwersytetu Przyrodniczo–Humanistycznego.

INFORMACJE NIEJAWNE I ICH OCHRONA W POLSKICH SIŁACH ZBROJNYCH. UWAGI OGÓLNE

Streszczenie. W dzisiejszych czasach nieustannego postępu technologicznego, zwłaszcza w dziedzinach teleinformatycznych, informacja staje się podstawowym i najważniejszym źródłem wiedzy. W strukturach sił zbrojnych, nabiera ona szczególnego znaczenia, gdyż od jej ujawnienia zależeć może bezpieczeństwo wewnętrzne danego państwa, a co za tym idzie jego suwerenność i niepodległość. Informacja staje się zbyt cenna, aby można było sobie pozwolić na jej niekontrolowane ujawnianie. Dlatego też polski ustawodawca, chcąc zabezpieczyć się przed jakąkolwiek interwencją obcych służb w zakresie pozyskiwania informacji niejawnych wprowadził do porządku prawnego określone narzędzia i instytucje prawne chroniące do nich dostęp.

Niniejszy artykuł ma na celu ukazanie, czym są informacje niejawne wraz z przekrojowym zaprezentowaniem konkretnych rozwiązań prawnych, jakie przewidziano w polskim ustawodawstwie w odniesieniu do sił zbrojnych, w materii mechanizmów blokujących dostęp do informacji niejawnych.

Słowa kluczowe: bezpieczeństwo narodowe, informacje wrażliwe, wojsko, klauzula bezpieczeństwa