Marcin BUDZYŃSKI
Command and Management Faculty
Academy of Military Art

CONTEMPORARY THREATS TO SOLDIERS SERVING ABROAD ASSOCIATED WITH THREATS FOR SOLDIERS SERVING ABROAD CONNECTED WITH LOSS OF CONTROL OVER PERSONAL DATA

SUMMARY

Poland as a country that actively participates in maintaining and opening peace in the world is exposed to various threats to the security of our country. The Polish government sends soldiers of the Polish Army to different regions of the world with the mission to create, maintain and create peace on all continents. Polish soldiers serve in peace-keeping, training and stabilization missions all over the world under the auspices of the UN and NATO, and are exposed to various threats. One of these threats is the loss of personal data of Polish Armed Forces soldiers. Loss of these data affects the safety of our soldiers performing tasks outside the country and their families remaining in Poland, and thus affects the safety of our country.

Keywords:
Soldiers of the Polish Army personal data, performing service outside the country by soldiers of the Armed Forces

INTRODUCTION

Soldiers serving abroad as part of Polish Military Contingents are particularly exposed to various insecurities. One of them is the danger of losing control over personal data of soldiers of the Armed Forces of the Polish Armed Forces and the threat arising from the influence of intelligence services of foreign armies on our soldiers performing tasks outside the borders of our country. This state of affairs causes the desire to draw attention to the risks associated with the loss of personal data of soldiers serving in the country, as

well as abroad. Therefore, the purpose of this article is to draw attention to the risks arising from of losing the personal data of soldiers of the Polish Army.

MODERN THREATS RELATED TO THE LOSS OF CONTROL OVER PERSONAL DATA

Poland, despite strong security guarantees obtained as a result of membership in many international organisations such as NATO, the European Union, currently as a non-permanent member of the United Nations, is not free from many contemporary threats. One of them is the threat of losing control over the personal data of soldiers in the Polish Armed Forces, in particular over the personal data of soldiers serving in Polish Military Contingents (PKW) due to the place and nature of their tasks. How serious this problem is, is evident from several examples of leaks of personal data of soldiers of the United States Army, who actively participated in military operations around the world, often cooperating with soldiers of the Polish Army.

The stability and security of the State requires, among other things, effective protection of the personal data of soldiers going to serve abroad, especially on peacekeeping missions. The protection of such personal data is important from the point of view of the security of the Republic of Poland and the creation of ideal conditions for cooperation with allied forces in international operations.

No country in the world directly discloses the circumstances of loss of control over the personal data of its citizens, such facts are most often scrupulously concealed, and information about the above incidents is most often provided by journalists. Nevertheless, in Poland, in November 2015, the personal data of Polish police officers, customs officers, border guards, Government Protection Bureau officers and soldiers, including those going on missions abroad and staying there, ended up in the databases of a German company from Ulm. This fact was revealed by the editors of *Dziennik Gazeta Prawna*. The reason for this was a situation in which a soldier, a participant in foreign missions, was diagnosed with leukaemia. His life was saved by an urgent bone marrow transplant. The soldier's wife used the social networking site Facebook to ask for bone marrow donors to register at various centres near their homes. She informed that this was the procedure to find a bone marrow donor for her husband and encouraged as many people as possible to participate. She suggested the more people to take part in this campaign, the better the chances for her husband and others waiting for a bone marrow donor will be. In this way, the process of searching for a bone marrow donor was set in motion. The DKMS foundation, which specializes in finding bone marrow donors, joined the action. The search process involves collecting

genetic material, i.e. a swab from the mouth, from a potential donor. During the examination, potential donors filled in a questionnaire, in which they provided the following personal data: name, surname, Personal Identification Number (PESEL), address of residence, telephone number and e-mail. The DKMS foundation also organised recruitment among soldiers on a mission of the Polish Military Contingent KFOR. According to the editors of the aforementioned, there was no legal possibility to recruit in a military base, so the recruitment took place in the hospitable surroundings of the Polish embassy. 44 of our soldiers plus the Polish ambassador, became a potential donor[1].

Another example of revealing personal data of Polish soldiers and representatives of other uniformed services is the fact of receiving faxes with the aforementioned data by a woman, a resident of one of the towns near Warsaw. She repeatedly received letters from the Police Headquarters on her private fax number. The faxed letters contained information on personal data of various persons who were subordinated to various official positions in the police and the army. Among the letters she received there was also information concerning tenders for weapons and granting access to classified information to individual functionaries from the army and police. Incoming documents to the wrong fax number, could include sensitive information including Personal Identification Number (PESEL) and other identification numbers. A spokesman for the Police Headquarters said that the reason for this was the distraction of the person sending it, who mistook the prefix numbers[2].

Such situations of disclosing personal data and other important non-public information took place not only in Poland, but also in other countries around the world. On the international scene, the most spectacular example of personal data leakage was the case of CIA employee Edward Snowden, who was employed by DELL on NSA contracts. He disclosed to the press several hundred thousand confidential, secret and top secret NSA dossiers, which was treated as the biggest information data leak in US history. The disclosed files showed the whole world how the authorities in Washington massively eavesdrop and track their own citizens and closest allies, as well as millions of foreigners. The above data included the personal data of US citizens in addition to the personal data of millions of people from allied countries. Wanted by US authorities on suspicion of revealing state secrets and espionage, Snowden was granted temporary asylum in the Russian Federation at the beginning of August 2013.

[1]https://wiadomosci.dziennik.pl/wydarzenia/artykuly/506696,niemiecka-baza-polskich-zolnierzy-dane-wojskowych-w-bazie-dkms-w-niemczech.html. dostęp 15.02.2019.
[2]https://www.gazetaprawna.pl/wiadomosci/artykuly/602818,wyciek-danych-z-komendy-glownej-policji-winien-jest-prefiks.html, dostęp 15.02.2019.

Further evidence that personal data is being stolen and obtained illegally is the fact that the data of up to four million employees of various federal agencies may have been illegally obtained from the US Office of Personnel Management (OPM) network. Among these files are the data of personnel employed by the Department of Defence. A special database belonging to the US Office of Personnel Management (OPM) federal became the target of a cyber-attack, as a result of which personal data concerning up to 4 million people was extracted from it. However, it is difficult to say at this point whether these data are social security numbers, identification document numbers of federal officials, or perhaps data relating to financial matters. This is probably one of the largest thefts of this kind in US history. This fact has caused particular concern overseas, as it directly affects a government sector that should theoretically be subject to special protection. The Federal Bureau of Investigation (FBI) has launched an extensive investigation to clarify the matter as quickly as possible. The US Department of Homeland Security also took immediate action. The case has also been widely discussed in Congress, where politicians who sit on the intelligence committees on a daily basis are dealing with it. It is worth noting, that the US Office of Personnel Management (OPM) not only collects information on individuals employed by various federal agencies, but also prepares data necessary in the United States to obtain security clearances. Therefore, there have been unofficial suggestions that some foreign countries may be behind the leaked information. Chinese hackers are considered to be particularly suspicious. However, a spokesman for the embassy of the People's Republic of China, anticipating possible allegations, said that such suggestions are irresponsible and unproductive. One of the structures affected by the data leak is, of course, the Department of Defence. Its employees, whose information may have recently fallen into the wrong hands, are to receive a special, personalised message from the Office of Personnel Management (OPM). At the same time, in order to minimise the risk of the stolen personal data of employees of federal agencies being used in a hostile manner, CSID, a specialist company dealing with data security breaches, has been approached[3].

After World War II, soldiers of the Polish Army participated in many peace missions[4] outside the country. Between 1953 and 2015, over 100,000 Polish soldiers and civilian employees of the army took part in approximately 90 missions. These missions were conducted under the auspices of the United

[3]https://www.defence24.pl/wielka-kradziez-danych-w-USA , dostęp 15.11.2018.

[4]National Defense University definition The USA defines peace missions as "United Nations field operations with international civilian and military personnel deployed with the approval of the United Nations to help resolve existing or potential international conflicts or internal conflicts with a clear international dimension." Def. after: W.H. Lewis, Military Implications of United Nations Peacekeeping Operations, Washington 1993, p. 17.

Nations (UN), the North Atlantic Treaty Organization (NATO), the European Union (EU), and the Organisation for Security and Cooperation in Europe (OSCE). In 2010 Poland participated in 10 missions to which, taking into account the six-month rotation system, it sent approximately 6 thousand soldiers and over 110 military civilian employees. Most of them – over 2,000 soldiers –stationed in Afghanistan, over 400 in Kosovo, and over 250 in Bosnia and Herzegovina.

Issues concerning sending of Polish soldiers on missions abroad are regulated by both national legislation and political documents. In addition, there are many references to international documents, above all the Charter of the United Nations, the Strategic Concept of the North Atlantic Alliance, and the European Security Strategy.

In a general way, issues concerning the subordination and use of the Polish Armed Forces (SZ RP) are regulated by the Constitution of the Republic of Poland of 2 April 1997. An important principle is that the Armed Forces are subject to civilian and democratic control and remain neutral in political matters (Article 16(2) of the Constitution of the Republic of Poland). Since the supreme power in Poland belongs to the nation (Article 4(1) of the Constitution of the Republic of Poland), the Armed Forces are ultimately subject to control by society. The nation exercises power through its representatives. In practice, the most important decisions concerning the functioning and use of the Polish Armed Forces are made by the relevant constitutional authorities. Civilian authorities decide, among other things, on sending Polish soldiers on missions abroad. In accordance with the Constitution, the rules for the use of the Polish Armed Forces outside the country are defined by a ratified international agreement or by statute (art. 117)[5].

The Constitution does not specify the circumstances which must exist for the Armed Forces to be used outside the country. The principles governing the sending of Polish military units abroad are regulated in the act on the principles of use or residence of the Armed Forces of the Republic of Poland outside its borders. Within the meaning of the act, military units are operational and tactical associations, as well as divisions and subdivisions. The

[5]The foundation for Art. 117, 229 and other articles of the Polish Constitution referring to an international agreement, is Art. 9 of the Constitution, which states that the Republic of Poland complies with international law that is binding on it. Moreover, Art. 87 point 1 of the Constitution classifies ratified international agreements in the category of sources of universally binding law of the Republic of Poland. This is called principle of favorable international law. See
E. Krzysztofik, Support for Peace in Contemporary International Relations, Warsaw 2009, pp. 158-166. Art. 27 of the Vienna Convention on the Law of Treaties. According to it, a party may not invoke the provisions of its domestic law to justify its failure to perform a treaty. See Vienna Convention on the Law of Treaties of May 22, 1969 (Journal of Laws of 1990, No. 74, item 439, as amended).

Act distinguishes between two different situations, i.e. the use of the Polish Armed Forces outside state borders, and the stay of these forces outside state borders[6]. The use of units outside the borders of the state means their presence abroad in order to participate in three types of undertakings:

- an armed conflict, or to strengthen the forces of the state or allied countries;
- a peacekeeping mission,
- action to prevent acts of terrorism, or their consequences.

The stay of units outside the borders of the state means their presence abroad in undertakings, among others:

- military training and exercises;
- rescue, search, or humanitarian actions, with the exception of rescue actions regulated by the provisions on rescue at sea,
- representational activities.

The use of military units abroad shall be decided by the President pursuant to the Act of 17 December 1998 on the Principles of the Use or Stay of the Polish Armed Forces Abroad, of which he shall immediately notify the Marshals of the Sejm and Senate. In the case of sending soldiers to participate in an armed conflict or to strengthen the forces of the state or of allied countries, as well as in the case of participation in a peacekeeping mission, the President decides at the request of the Council of Ministers. The situation is different in the case of actions to prevent acts of terrorism or their consequences, where the president decides at the request of the Prime Minister. The decision on the stay of military units, however, belongs to the Council of Ministers or its relevant members. According to the act, such a decision is taken by the minister in charge of national defence or the minister in charge of internal affairs with respect to units subordinate to them, regardless of the nature of the stay. An exception is the situation of the stay of military units for training or military exercises if the funds for these undertakings have not been included in the budget of the relevant ministry. In such a situation the stay is decided by the Council of Ministers. Each time the Prime Minister notifies the President about the decision on the stay of military units outside the borders of the state.

In the case of a presidential decision on the use of military units outside the country, the law introduces several formal and legal conditions. The order must contain basic information about the mission itself and, above all, about the Polish units participating in it. The decision must contain information as to which military units, in what number and for how long, will remain outside the

[6]Act of December 17, 1998 on the rules of use or stay of the Armed Forces of the Republic of Poland abroad (Journal of Laws of 1998, No. 162, item 1117; Journal of Laws of 2004, No. 210, item 2135).

borders of the state. In addition, it must specify the objective of sending military units abroad, the scope of their tasks and the area of operations. The body of the international organisation under whose auspices the operation is conducted should be indicated, as well as the system of directing and commanding the units. It is also necessary to indicate the bodies of government administration responsible for cooperation with the relevant bodies of the international organisation within the scope of managing activities and supplying military units. It is also necessary to indicate what equipment the military units will be armed with. In the case of transit, it is also necessary to record information on the routes and time of movement of military unites.

Having familiarized ourselves with the literature on the subject, we can notice few scientific studies that would comprehensively exhaust the subject of the ways and procedures for protecting the identity of soldiers serving in the Polish Armed Forces. This leaves room for ordering this topic in the context of soldiers' personal data security using research methods. For this purpose, I will conduct a diagnosis of the existing state and conduct my own analysis of the existing state of personal data protection procedures in order to present a concept of repair of the organizational and functional sphere of methods of personal data protection of soldiers in the Polish Armed Forces.

The above examples show that, despite many legal acts in force in our country, the security of personal data of Polish soldiers in the country, especially those participating in peacekeeping missions, is at risk.

The most important tasks of any state include protecting the independence and inviolability of its territory and ensuring the security of its citizens. The Republic of Poland performs these duties using a variety of forces and means, which are interrelated and together form the state defence subsystem.

The defence subsystem of the state is one of the operational subsystems of a wider system of national security of the Republic of Poland. According to the National Security Strategy issued in 2014, the state defence system is formed by forces and means which are at the disposal of the security management bodies and are intended for the implementation of statutorily defined tasks related to exploiting opportunities, taking up challenges, reducing risks and countering external threats of a political-military nature[7].

The legal basis for the protection of personal data in Poland is the Constitution, in which in the chapter Freedom and Personal Rights and Article 47 it is written: "Everyone has the right to the legal protection of his private life,

[7]National Security Strategy of the Republic of Poland 2014, approved at the request of the Prime Minister by the President of the Republic of Poland, Bronisław Komorowski, on November 5, 2014.

family life, honour and good name, and to decide on his/her life"[8]. This expresses the will of society that the created legal order, which respects human freedom, should also respect human rights to acquire, transmit, process, or reproduce information.

The Data Protection Act of 10 May 2018 is in force in Poland. The Act sets out:

- personal data protection authorities,
- competences of the Inspector General for Personal Data Protection,
- the principles of securing personal data,
- the principles of transferring personal data to a third country.

In addition, the Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 is in force in Poland d 28.05.2018. on the protection of natural persons in relation to the processing of personal data and on the free movement of such data (RODO), which contains provisions on the protection of natural persons in relation to the processing of personal data and provisions on the free movement of personal data.

RODO is the EU regulation that imposes rules for the processing of personal data in a fully or partially automated manner in the countries of the European Union. In addition, it defines the rules for the non-automated processing of personal data that are part of the data set. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 also contains exclusions from the above rules. These exclusions apply to the activities of entities not covered by EU law or relate to the processing of data by a neutral person in the course of domestic and personal activities. The RODO also describes the specific rights for persons whose data is collected, processed, and transferred. These powers can be divided into four groups. The first group of rights is the broadly understood right to obtain information about data processing and access to this data. However, the next group of rights are corrective powers. The personal data subject to processing should be correct (in accordance with the facts, up-to-date, free of errors). Among the powers granted to the data subject, a special role is played by the powers to decide on the processing of data, which are generally referred to as decision powers. The entity whose rights will be violated as a result of unlawful data processing has the right to use legal remedies and obtain compensation.

An equally important legal act in force in our country, which is related to the protection of soldiers' personal data, is the Act which determines the principles and organisation of the classified information protection system in

[8]Journal of Laws 1997 No. 78, item 483, the Constitution of the Republic of Poland of April 2, 1997, adopted by the National Assembly on April 2, 1997, adopted by the Nation in a constitutional referendum on May 25, 1997, signed by the President of the Republic of Poland on July 16, 1997..

Poland of 5 August 2010 on the protection of classified information. This act is accompanied by a number of executive acts issued on its basis: regulations, orders, decisions. The division and analysis of the legal status in force allows the statement that the system of protection of classified information takes into account the scopes of responsibility of the organisational structures of state institutions.

Also important is the Act on the Military Counterintelligence Service and the Military Intelligence Service. This act specifies in detail the scope of activity of the above mentioned services, the principles of recruitment, and the requirements for candidates. Institutions, which in a natural way coordinate protection and disposal of personal data, are institutions such as: Internal Security Agency (ABW), Military Counterintelligence Service (SKW) and security divisions of organisational units[9].

The security system of an organisation should be a comprehensive system, i.e. all the methods of organisational, physical, personnel and ICT protection must be applied jointly, in a coherent way, otherwise such system will have gaps, synergy of actions is key.

Today's technologically advanced societies largely depend on information, in particular information processed, stored, and transmitted in information systems. An information security management system is a systemic, comprehensive approach to establishing, implementing and maintaining information security; its elements are:

- information security policy;
- procedures;
- guidelines;
- core and supporting assets[10].

The state security system consists of a command subsystem and executive subsystems. The command subsystem is the basic and essential element of the national security system. and essential element of the national security system. It consists of public authority institutions and managers of organisational units who perform tasks related to national security, together with advisory bodies and administrative apparatus and relevant infrastructure. Its functioning is based on permanent systemic principles. A special role in the national security management subsystem is played by the Parliament of the Republic of Poland, the President of the Republic of Poland, and the Council of Ministers.

[9]S. Topolewski, *Ochrona informacji niejawnych w siłach zbrojnych Rzeczypospolitej Polskiej*, Siedlce 2017, p. 269.

[10]http://www.mrj.uksw.edu.pl/sites/default/files/Konferencje/Normalizacja_a_legislacja , dostęp 15.11.2018.

In order to ensure an adequate level of security in Poland, such institutions have been established as:

a) civilian:
- Internal Security Agency,
- Intelligence Agency
- Central Anticorruption Bureau,

b) military:
- Military Counterintelligence Service,
- Military Intelligence Service.

Soldiers serving abroad, as part of Polish Military Contingents, are particularly exposed to the influence of intelligence services of foreign countries due to the classified tasks they perform. Therefore they should be particularly protected by the binding legal acts. For this purpose, among others, the Act on the Protection of Classified Information of 5 August 2010 was passed by the Polish Parliament.

The unbelievably rapid development of technology that we have been observing for the last quarter of a century, and in particular the development of telecommunications technology, and the avalanche of computerisation in almost every area of life, means that information is the most precious "commodity". It would be a truism to say that it is the key to success in politics, business and war. Therefore, the security system for the protection of personal data of soldiers of the Polish Armed Forces performing tasks outside the country should be a comprehensive system, i.e., all methods of organizational, physical, personnel, ICT protection must be used together, in a coherent way, otherwise such a system will have gaps, the key is the synergy of action. Today's technologically advanced societies largely depend on information, and in particular on information processed, stored, and transmitted in Social Media. Therefore, soldiers of the Polish Armed Forces serving in the country, as well as those carrying out tasks abroad, should obligatorily participate in trainings on modern threats resulting from inadequate protection of their personal data.

BIBLIOGRAPHY

[1] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. *(Dz. U.z 1997 r. Nr 78 poz. 483);*

[2] Ustawa z dn. 17 grudnia 1998 r. o zasadach użycia lub pobytu Sił Zbrojnych Rzeczypospolitej Polskiej poza granicami państwa *(Dz. U. z 1998 r. Nr 162 poz. 1117; Dz. U. z 2004 r. Nr 210, poz. 2135)*;

[3] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014, zatwierdzona na wniosek Prezesa Rady Ministrów przez prezydenta

Rzeczypospolitej Polskiej Bronisława Komorowskiego 5 listopada 2014 roku.

[4] Balcerowicz B. (red.), *Słownik z zakresu bezpieczeństwa narodowego, Warszawa 2002;*

[5] Karta Narodów Zjednoczonych z 26 czerwca 1945 r. (Dz. U. z 1947 r. Nr 23 poz. 90 ze zm.). Odwołania do koncepcji strategicznej z 1999 r.: Koncepcja strategiczna Sojuszu, zatwierdzona przez szefów państw i rządów, biorących udział w posiedzeniu Rady Północnoatlantyckiej, Waszyngton, 23 -24 kwietnia 1999 r. Obecnie obowiązuje: Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, przyjęta przez szefów państw i rządów w Lizbonie, Lizbona, 19 -20 listopada 2010.

[6] Bezpieczna Europa w Lepszym Świecie. Europejska Strategia Bezpieczeństwa, Bruksela, 12 grudnia 2003.

[7] Paszkowski K., Gągor F, *Międzynarodowe operacje pokojowe w doktrynie obronnej RP*, Warszawa 1998.

[8] Zapałowski L., *Operacje pokojowe ONZ*, Warszawa 1989.

[9] Topolewski S., *Ochrona informacji niejawnych w siłach zbrojnych Rzeczypospolitej Polskiej*, Siedlce 2017.