Sławomir Gładysz

Counter-terrorism powers of national authorities

With a provision of the Law on the Counter-Terrorism Operations of 10 June 2016[1] some criticism and anxiety aroused in concern with the powers assigned to the security services, especially the operational powers assigned to the Internal Security Agency. These powers – according to the skeptics of that regulation – have influence on rights and civil freedom and they breach the constitutional principles of protection of the citizen's right of free communication and privacy.

The most frequent foundation of the a/m statements is the anxiety for creation of the law that would justify breaching, by the state's apparatus, all rights constitutionally protected, that under any circumstances should not be touched. It is visible *a priori* to assess the situation from the perspective of the security, in which it is known that no one in their right mind will threat or violate it. Then, the assumption made at the beginning of this paragraph about the inalterability of certain freedoms, and no possibility of suspending them, would be right. Unfortunately, such an approach to security-related issues seems naive.

Rational and at the same time pragmatic attitude in these matters conveys the necessity of going beyond ideals and prepare the state and its institutions to act in the situation of the highest threat or counteract the effects of events that have already taken place. These preparations should include both formal aspects, specifying the basics and scope of actions, and real – by indicating how to use these tools in accordance with the law.

It should be noted that legal structures in the Polish legal system that allow limiting or suspending the use of full civil rights in certain situations have been already existing[2]. They provide that in the event of particular threats preventing the normal functioning of the institution under specific constitutional measures, a state of emergency may be introduced, which may involve a restriction of freedom and human and civil rights.

According to the author, the catalogue of specific threat events shall be supplemented by threats of a terrorist nature, especially those bearing attributes of an offence. The given stance can be reassured i.a. by the regulation on broadly understood anti-terrorist activities discussed in this report.[3]

---

[1] Journal of Laws 2016, item 904.

[2] States of emergency include: martial law – Act of 29 August 2002 on Martial law and on the competences of the Supreme Commander of the Armed Forces and the rules of his subordination to the constitutional organs of the Republic of Poland (Journal of Laws 2017, item 1932); state of emergency – Act of 21 June 2002 on the emergency state (Journal of Laws 2017, item 928); and natural disaster – Act of 18 April 2002 on the Natural disaster state (Journal of Laws 2017, item 1897).

[3] It is possible to discuss whether combating terrorist offences is a "special threat" within the constitutional concept resulting from Journal of Laws art. 228 paragraph 1, nevertheless the logical

It is therefore logical that in order to save the common "greater good" as citizens, we will be ready to give up certain attributes of functioning in the state. No one has or at least no one should have any doubts about it. The common sense of threat felt by citizens, causes flexibility, thanks to which the use of even bothersome restrictions will be accepted by them.

Regardless of the necessity to point out the foundations and scope of the functioning of state institutions in identifying, preventing and counteracting terrorism, the arguments for the implementation of new regulations[4], in the author's opinion, are effective measures recognized by the legislator in the 90's of the twentieth century used by the institutions that are responsible for ensuring security. Operational and procedural work based on "old", proven methods, used for many years, has been supplemented by "new" solutions, i.e. the possibility of operational or process control of mobile communication means, no matter for a specific telephone number, but also for an individual number of the telephone (IMEI), the ability to track the spectrum of telecommunications frequencies or other information that can be obtained from the operational and technical security divisions.

Then, at the turn of 20th and 21st century, it seemed that the saying "criminals are always one step ahead of us" might be outdated for just a moment. At the beginning of the 21st century, while conducting one of the cases, the author determined the way of communication of suspected individuals, who were citizens of neighboring countries. They agreed on a kind of "security system" to keep their criminal activities covert. It consisted of using one SIM card for a maximum of one month, and one telephone did not support more than three SIM cards and after six months it had to be changed. And they were just simple criminals…

This example shows that the development of know-how, technology, communication, especially in relation to the globalization of every area of life, causes that the bodies appointed to recognize, counteract and fight crime will always be behind the criminals aiming for the hermeticity of their environments and the secrecy of their connections, hiding their real plans and intentions. The only question is how far they will be left behind.

It is obvious that the services aren't (or weren't – before June 10th, 2016) helpless in the implementation of their statutory competences, especially in terms of ensuring security. As shown by the various types of publications, the actions taken by the services ensure internal security at a certain, satisfactory level. The criterion of this assessment is based on the existence or not of terrorist incidents. At the same time, the borders between the citizens' awareness that this security was assured, because

---

interpretation of related norms supports such a position. Well, in the regulation of the state of emergency, its introduction was indicated, among others, threat to citizens' security and public order. It should be agreed that a possible terrorist attack would harm these goods. It will be an issue to assess whether a given terrorist, event can cause a situation in which ordinary constitutional measures are not enough to fight or counteract it.

[4] Adapted to new times, technologies, and society, etc.

nobody planned anything, realizing that certain actions were broken by the services at the right moment, and that their potential continuators are deterred by the effectiveness of security services – is (or was) invisible.

The introduction presented above shows two basic points of view of the issues related to the powers of services perceived in the terms of civil rights and freedoms. On the one hand, they are based on the admissibility of certain tools, on the other hand they concern the scope and methods of using them.

Exposing issues related to the state domain in the field of security, in particular protection against terrorist threats, and legal regulations in this area may dispel doubts as to the legitimacy of equipment the state authority in specific instruments of action. The analysis shows that the regulations of this area arise from various legal acts, and their citation, even if signaled, may allow an objective and rational evaluation of the provisions of the Act on anti-terrorist activities.

1. General issues

In accordance with Article 5 of the Constitution of the Republic of Poland of April 2nd, 1997[5] – The Republic of Poland safeguards the independence and inviolability of its territory, ensures freedoms and human and civil rights, and the security of citizens. This standard defines the basic, general functions of the state and its fundamental goals, which mainly consist in the protection of the territory, freedom and security of citizens. The mentioned values are also the basis for the functioning of the state apparatus, and especially its institutions, which were appointed to guard them, regardless of the source of the potential threat.

It is obvious that the most important goods to be protected are: the state as an independent entity with its territory and citizens with their rights, and thus, in fact, the most valuable element of the state. This protection means in fact ensuring a state of security, i.e. creating a situation in which regardless of the level of danger, actions taken by state authorities will rise citizens' trust and understanding of their necessity, and at the same time correctness and effectiveness. The concept of ensuring security, however, requires a narrow interpretation, because it should only be a certain reaction, although also of a preventive nature, to real or potential (but still plausible) threats and attacks.[6]

For the purposes of this article, the focus should be on defining the term citizen security. According to the definitions of the *Dictionary of the Polish language*, the term safety is understood as a state of non-hazard, functioning in the normal mode without the threat of a specific event, negative in its consequences. On the other hand, public safety means all conditions and institutions protecting the state and citizens from dangerous phenomena threatening the legal order, and

[5] Journal of Laws 1997, No 78, item 483.

[6] P. Sarnecki, *Artykuł 5*, in: *Konstytucja Rzeczypospolitej Polskiej. Komentarz I, Wstęp*, Art. 29, L. Garlicki, M. Zubik (scientific editing), Warszawa 2016, p. 234.

protecting the system against attacks on the basic political institutions of the state.[7] However, this definition – excluding from its scope "other people" staying or functioning in the structures of a given state – would be an unauthorized restriction of this concept. "Other people" are also protected; they are also element of public safety.

In the author's opinion, the above entitles to claim that the determination of the security of citizens is a kind of *lex specialis* of public security, which the state has taken upon itself a special legal obligation to protect it.

Another duty of the state under the Article 5 of the Constitution of the Republic of Poland is to ensure freedom and human and civil rights, which expressly lead to the second chapter of the Constitution of the Republic of Poland. It is worth citing here the French *Declaration of Rights of Man and Citizen of August 26th, 1789*[8], especially its article IV, saying that: *Freedom consists in the possibility of doing everything that does not harm another; in this way, the exercise of the natural rights of every human being has no limits other than those that ensure that the same rights are enjoyed by other members of society*. These limits can only be determined by statute. Despite the passage of almost 230 years from this regulation, the commentary to its record is in fact unnecessary.

In Polish legislation, freedom is generally understood as the sphere of rights that law does not create, but only defines their limits. In this case, it is the state's duty to prove that the individual has violated these limits. On the other hand, in the case of *law*, the catalogue of which is established by the State, the entity must invoke a specific legal basis in the course of their investigation.[9] It means the freedom of human action wherever the law allows that. This is a total reversal of the situation existing in relation to the state and its organs. The state body operates where it has been authorized by law and acts, citing the legal basis. A citizen can act wherever the law did not introduce bans, and did not forbid certain acts.[10]

Referring to the earlier definition of public security, in which its qualified form was pointed in reference to "citizens", a similar procedure should be indicated, establishing the general rights common for all people, as well as those closely related to formal state affiliation. It is the result of a special obligation of the state to provide protection and a sense of security especially to its citizens, without ignoring the basic, necessary rights belonging to all people residing on the territory of the Republic of Poland, regardless of their state, nationality, racial, religious or political status.

The manifestation of this is the Article 31 of the Constitution of the Republic of Poland, in which legal protection of human freedom was established, but at the same time it was indicated when, and on what basis the indicated rights and freedoms

[7] http://sjp.pwn.pl/slowniki.

[8] Text of the *Declaration* was published on web page http://libr.sejm.gov.po/tek01/txt/konst/francja-18 [access: 23 I 2017].

[9] W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, Warszawa 2013, p. 42.

[10] Ibidem, p. 45.

may be limited. It is obvious that the rights, especially the rights of freedom, cannot be unlimited. The Article 31, paragraph 3 of the Constitution of the Republic of Poland provides guidance on how to determine these boundaries and how far limits can be allowed.[11] These guidelines result directly from the editors of the norm and specify that restrictions that can only be established in statute, and only when they are necessary in a democratic state for its security or public order, or for the protection of the environment, public health, morality or the rights and freedoms of others.

The above provides guarantees for the protection of rights and freedoms, at the same time by introducing clauses limiting these rights and freedoms – the formal ones, setting the minimum rank of a legal act[12] constituting a limitation, and the material ones, dependent on the implementation of a specific task by the state. The tasks listed have been divided into three groups, including: security and public order; environment, public health, public morality; freedom and rights of other people. Restrictions introduced of any of these reasons do not violate the principles of a democratic state ruled by law, but on the contrary – they are necessary.[13]

When discussing constitutional norms, it is worth paying attention to the relevant provision from the point of view of this article, namely Article 37 of the Constitution of the Republic of Poland. It introduces the principle of equal use of freedoms and constitutional rights by all people, both citizens and foreigners in the area covered by the authority of the Republic.

A foreigner, according to the definition of the *Act of 12th December 2013 on foreigners*[14], is anyone who does not have Polish citizenship[15], regardless of whether one has any foreign citizenship (stateless person). Exceptions from the above-mentioned rule, particularly referring to foreigners, can be regulated in statutes. The legislator did not indicate a specific legal act, which could impose restrictions on the enjoyment of rights and freedoms by foreigners, but defined its rank, confirming[16] the necessity of these regulations by means of statutes.[17]

Summing up, the Constitution of the Republic of Poland imposes on the state a special obligation to ensure public safety while guaranteeing the respect of freedoms and human and civil rights. These freedoms may be limited, however, by the legal act issued by the parliament .

One of the reasons for introducing restrictions on the rights of human and citizen freedom is the necessity to ensure security which may jeopardized, among others,

[11] P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997*, Warszawa 2008, p. 48.

[12] As indicated above, this act should have the status of a law, a generally applicable legal act issued by the highest legislative body, in a special mode and having a high position in the structure of sources of law.

[13] P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej…*, p. 49.

[14] Consolidated text: Journal of Laws 2017, item 2206.

[15] Article 3 (2) of the Act on Foreigners.

[16] Article 37 (2) of the Constitution of the Republic of Poland.

[17] Article 31(3) of the Constitution of the Republic of Poland.

by various phenomena and threats of a terrorist character. This threat is important especially now that it defies traditionally understood definitions, and their potential perpetrators act out of the box, often targeting random people, infrastructure or simply striving to make the greatest damage.

To counteract this, the state must comprehensively prepare itself by equipping the competent authorities with instruments and tools that allow to undertake immediate and adequate measures to respond to threats and – in the time of attack – also to remove its consequences.

Precise regulation of the activities of state authorities in the face of terrorist threats, regardless of their level, should be the standard adopted by the state, independently of the political environment from which the ruling party originates.

The effectiveness of such regulations will depend on the close and comprehensive cooperation of all services, bodies and institutions involved in broadly understood anti-terrorist activities with approval – and even support – of the mass media, non-governmental organizations and the whole society.

2. Competent authorities in matters of terrorism

In Poland, bodies appointed directly under the Act to deal with broadly understood issues related to terrorism are the special services: the Internal Security Agency, the Intelligence Agency, the Military Counterintelligence Service and the Military Intelligence Service, as well as the Military Police and the Police. The leading role in the issue of recognition, prevention and detection of terrorism-related offenses has been assigned to the Internal Security Agency, which is reflected in the force-based provisions of competence. The mentioned Article 5 contains a relatively broad approach to the tasks of the Internal Security Agency in the area of terrorist crime.

In fact, it is difficult to overlook also other bodies, whose significance at various stages of phenomena related to terrorism cannot be overestimated, but their tasks do not result directly from the rules, but rather from the logical or systemic interpretation of their powers. Among others the State Fire Service[18], the Polish Border Guard[19], or the Government Protection Bureau[20], however, due to the generality of the subject,

[18] The State Fire Service is the main service responsible for conducting rescue operations in the field of saving lives and human health and protecting property and the environment in the event of an emergency. The tasks of the State Fire Service include undertaking activities in the field of hazard identification, including contamination with chemical and radiation substances, as well as conducting preliminary biological reconnaissance operations. The entities undertaking rescue tasks operate within the framework of the National Rescue and Firefighting System. All rescue operations during a terrorist threat are based on maintaining the priority of saving lives and health and the technology of actions aimed at minimizing the effects of an event.

[19] These activities include protection of state borders, including maritime borders, organization and control of border traffic as well as prevention of illegal crossing of state borders and prosecution of perpetrators of such offenses. The Border Guard also carries out tasks in the area of ensuring security in international communication, including on board aircraft performing air transport.

[20] The Government Protection Bureau is competent in the protection of statutory defined persons,

the author focused on the main organs appointed to deal with the phenomenon of terrorism and the instruments of action assigned to them. Presentation of these tasks and tools, in which the legislator provided organs for their implementation, will create a starting point for discussing and assessing the provisions of the Act on anti-terrorist operational actions.

2.1. *Internal Security Agency (ABW)*

Article 5, paragraph 1, point 2 of *the Act of 24th May 2002 on the Internal Security Agency and the Foreign Intelligence Agency*[21] indicates that the recognition, prevention and detection of crimes, including terrorism is a part of the tasks of the Internal Security Agency. In this respect, the Agency's activity can be carried out both in the country and abroad.

They consist of activities undertaken on four levels, which the legislator has grouped in the terms.[22]

- recognition – according to the definition, it means identification of someone or something, research and undertaking activities aimed at obtaining information about an opponent[23],
- detection – stands for establishing facts about someone's participation in something, disclosing things that were supposed to be secret[24],
- prevention – taking actions aimed at preventing something bad to happen.[25]

In addition, the legislator indicated that the Internal Security Agency is obliged to prosecute the perpetrator of crimes remaining in its material jurisdiction. This means that the Internal Security Agency has the option of legal utilization of its operating materials.[26] This is important at the stage of operational and procedural cooperation, as officers from specific departments can often afford to conduct free dialogue and a loose, informal exchange of comments and needs, aimed at determining the appropriate directions of both the given operational case and the criminal proceedings.

The indicated tasks are the ABW's ability to identify, confirm and taking preventive and procedural measures. The above-mentioned four action plans can occur selectively, individually, and cumulatively. The model situation would be to

facilities and equipment that may become the potential target of terrorist attacks.

[21] Consolidated text: Journal of Laws 2016, position 1897 – therein: the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[22] Perhaps they are obvious, but in the context of the fundamental purpose of this article, i.e. the analysis of the law on anti-terrorist activities, it is worth defining and defining their foundations of meaning.

[23] http://sjp.pwn.pl/szukaj/rozpoznawanie.html.

[24] http://sjp.pwn.pl/szukaj/wykrywanie.html.

[25] http://sjp.pwn.pl/szukaj/zapobieganie.html.

[26] The author met with numerous voices of representatives of other services who do not have these capabilities, indicating that the investigations frequently conducted on their operational materials did not have proper operational support, which put the unsatisfactory process results.

have operational and analytical capabilities that would make the recognition process the fastest, the most effective and the most accurate. It depends on further activities of an operational nature, and actions taken in the last phase of the process. Recognition gives the advantage, time and possibilities to take effective and adequate responses to a specific threat. The next stage, detection, is the consumption of identification activities. It is at this stage that the Internal Security Agency will confirm the existence of reasonable suspicion of committing a crime. Then the verification of the collected operational material and its possible process of legal utilization take place. Depending on the type of threat identified, its scale and timeliness, further activities of the Internal Security Agency may take the form of a response adequate to the threat aimed at its leveling or liquidation. This can be achieved both by the dynamic use of force[27] and in long-term activities of a preventive nature. Such activities should, however, lead to a certain goal – which means either to prevent the escalation of the threat or to gather evidence to apprehend the perpetrators and prepare the charge indictment for the court.

According to the Article 21 of the Act on the Internal Security Agency and the Foreign Intelligence Agency, to perform their duties, i.a. in the CT aspect, officers conduct operational, as well as investigate activities. Despite the fact that these three kinds of activities are basically different from and dependent on each other, such division of work is fundamental for the functioning of ABW. To sum it up briefly: the more information is gathered at the operational stage, the better assumptions can be made later by the investigators which results in more effective legal proceedings.[28]

The described relation resulted in granting investigative powers (similar to these used by the Police, resulting from the provisions of the Code of Criminal Procedure) to the ABW officers.[29] The importance of this provision was already mentioned at the beginning of this chapter. It is systematically linked with the Article 22a (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, which – if the gathered material indicates the probability of a perpetration of a crime – allows the Head of ABW to present it to the prosecutor to decide if any further legal proceeding should be initiated. Therefore, it can be supposed that ABW should be the first institution tasked by the prosecutor's office to conduct an investigation[30], whenever the presented material is considered valid and the investigated crime lies within the remit of the Agency.

A certain exception from the rule stipulated in Article 22a (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency has been made by the legislator. Whenever the Head of ABW gets in possession of information indicating

[27] That is why it is so important to be able to use them, and according to the author, within the framework of criminal proceedings or directly at the disposal of the Head of the Internal Security Agency.

[28] Interesting is that his "obviousness" is not so clearly visible for the ABW officers.

[29] Art. 21 (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[30] According to art. 303 of the Code of Criminal Procedure this happens when there is a good reason to suspect that an offence has been committed, and the act can be described, as well as its legal classification can be set forth.

a possible terrorist activity he may – for national security reasons – renounce from informing the prosecutor about the justified suspicion of this crime or its suspected perpetrator.[31]

Another amendment allows the ABW officers[32] to cooperate with a person suspected of committing a crime of a terrorist nature. It can be done only if all circumstances of the committed crime or conducted activity have been deliberately and voluntarily revealed by the mentioned person, and a commitment to cooperate with ABW was signed.[33]

The decision of the Head of ABW of not informing the local prosecutor must be reviewed by the General Prosecutor, as well as by the member of the Cabinet competent in the matters of coordination of special services.[34] The mentioned exceptions are first tools provided by the act of law that can be used by ABW to perform its duties, especially to investigate, detect and prevent crimes of a terrorist nature.

As it was mentioned earlier, the legislator created an exact catalogue of activities that can be done by the state (represented in this case by the officers of ABW) to fulfill its tasks. The analysis of the service's competences shows that they can be divided into three fields: administration and public order[35], covert operational activities, and investigative powers.[36] Due to the fact that the goal of this publication is to describe the provisions of the Law on the Counter-Terrorism Operations, the author focuses only on these covert operational activities of ABW which are essential in fighting terrorist crimes, this means:

- to request blockade of telecommunication;
- to request blockade of accessibility of certain data in IT system;
- to perform a security check of IT system;
- to initiate operational control;
- to collect personal data (also in a covert manner);
- to make use of information described as bank secrecy and information from agreements on cash accounts, insurance or other agreements related to financial instruments, money services or investment funds;

---

[31] Art. 22b (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, added by the Law on the Counter-Terrorism Operations. Such exception cannot be executed when the suspected terrorist committed a crime against a person resulting with death or serious detriment to the health of a person, was involved in committing such crime or instigated to commit it. It involves also a person who – while being a covert informant – has not revealed all relevant information and continues to conduct activities against the Republic of Poland, or committed any of the above-mentioned offences despite his covert cooperation with the service.

[32] There has been no such possibility since the establishing of the UOP and, later, the ABW, neither in the CI nor in the CT field.

[33] It remains unclear how such cooperation should be initiated – by the person, as a "walk-in" or by the officers of the Agency, after the person was identified and offered to cooperate ("to cooperate or to be persecuted").

[34] Art. 22b (4) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[35] A right to issue an instruction to behave in a requested manner, to check a person's identity, to conduct personal searches, to photograph and record fingerprints, and to use firearms and means of coercion.

[36] Based upon the legal procedure code, supported by an internal "instruction on investigation".

- to covertly buy or seize objects from an offence;
- to request a covert oversight of production, transport, storing and trading of subjects from an offence;
- to accept the assistance of informants who are not officers of ABW.

The first of means presented above, the blockade of telecommunication[37], is used as a reaction on a high threat level in a certain field. The indicators of such threat are listed in the empowering measure of the Internal Security Agency; they are: threats to internal security of the state and its constitutional order, as well as most serious offences threatening the state. Despite such broad definition of conditions allowing to use the blockade of telecommunication this procedure seems to be related exclusively to the defined and probable threats, like an act of violence directed against the constitutional institutions of the state or an attempt of a terrorist attack. In such a situation (like in the case of a terrorist attack) the blockade of telecommunication becomes a tool enabling to gain time for mobilization of means and powers which can be later directed to the venue to perform the official duties. It is not difficult to imagine that using this power could mitigate the spreading of potential destruction or prevent the criminal activities aimed at public security.

To use this power the Head of ABW first defines its territorial range and then informs of this fact the President of the Office of Electronic Communications. The lack of precise definition of the time period for which such decision may be valid, seems significant here. The legislation uses only an unclear expression "for the time necessary to perform the duties" which is a result of an unpredictable nature of situation when the blockade of telecommunication is vital. The only limitation in such activities is minimization of the results stemming from the lack of possibility to use means of telecommunication.

The activities described above are linked with an ability to block the accessibility of certain data or services in IT system, in case of a terrorist incident.[38] It can be performed on request of the Head of ABW to block the accessibility to "prevent, counter and detect offences (…) and to pursue the perpetrators"[39] which should be addressed to the District Court in Warsaw, entitled to decide in this matter.

To formalize the request there is a need to obtain a written permission of the General Prosecutor. There is also an option to put the request into power immediately. In such a case the Head of ABW may request to establish a blockade of accessibility after receiving the permission of the General Prosecutor, and in the same time the request is passed to the court to get the final approval. If the court refuses to approve the request within five days since the blockade has been put into power, these activities must be stopped. The blockade of accessibility can be requested for no longer than 30 days with a single option of extending this period for three months.

---

[37] Art. 26a of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[38] Art. 32c (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[39] The quotation marks were used intentionally, due to the opinion of the author that a legal inaccuracy happens here – according to Art. 5 (1) (2) the tasks of ABW are "to investigate, prevent and detect offences". "Countering" is a new kind of tasks described by the Law on the Counter-Terrorism Operations. The issue will be elaborated later on.

Another IT tool that remains at the disposal of the Head of ABW is the ability to perform a security check of mentioned IT systems, allowing to verify the vulnerability to attacks which may harm their integrity, confidentiality, accountability and accessibility.[40] Interesting is that the legislator granted ABW the right to design or acquire devices or software mentioned in Art. 269b of the Criminal Code[41], as well to use them.

The operational control is defined as acquiring and recording: communication with use of technical means, including IT networks; video footages or sound recordings from means of transport or places other than public; correspondence (also from the electronic channels); information from IT data carriers, terminals, informational and IT systems, as well as acquiring access to postal letters and packages to control their content.[42]

After years of discussions, the mentioned power was adjusted to follow the reality. The operational control gives a lot of opportunity to intrude into someone's privacy, however in the first place it should be assumed that national entities uphold the rule of law. A hypothesis – known to the author from the case of introducing the "posteriori approval" procedure – saying that "it is easily imaginable that an officer illegally uses acquired data" is, in the author's opinion, inadmissible. The main rule is to use granted powers accordingly with their intention, after fulfilling appropriate criteria and with due diligence. The author's experience from his service in ABW allows to conclude that such standards (sometimes even more restricted ones) are being met whenever the power of Article 27 of the Act on the Internal Security Agency and the Foreign Intelligence Agency is executed. In other words, it cannot be imagined that an officer misuses information acquired by the operational control.[43]

To perform its duties related to investigate, detect and prevent crimes, i.a. of a terrorist nature, the court, on a written request made by the Head of ABW, may issue the decision to start the operational control.[44] An additional criteria to fulfil while requesting the operational control is to prove the ineffectiveness or uselessness of other covert means.

[40] Art. 32a (1) and (6) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[41] The described provision seems inaccurate – the referred point of the Criminal Code relates to destroying, deleting or changing IT records that have a particular significance for national defense, transport safety, operation of the government or other state authority or local government, or interferes with or prevents automatic collection and transmission of such information. It may be assumed that this provision may allow to perform simulation of potential results of an attack, however the point 8 of the article stipulates: "(…) to acquire access to data (…) by breaking or passing by its electronic, magnetic, IT or any other means of protection", which suggests a possibility of using more offensive actions.

[42] Art. 27 (6) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[43] To avoid idealization, the violation of the mentioned rule cannot be fully excluded, but it remains exceptional. It is commonly thought that the surveillance materials (especially stemming from tapped wires) are sensational, uncover the deepest secrets and keep the thrill from the beginning to the very end. In real life these sensational recordings are rather a tedious, exhausting and psychically-burdening toil, demanding to listen, re-write and verify enormous amounts of data to gain a potential result.

[44] Art. 27 (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

The request for operational control must be verified at two stages. First, the request of the Head of ABW needs the approval of the General Prosecutor, made in written form. Such legitimization of the request for the operational control entitles the Head of ABW to reach the court. The court may, however, deny such form of control, if the operational materials used as the basis for the request deem insufficient.

There is also an urgent mode of this procedure. According to the Article 27 (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, in case of a risk of losing the information or of destruction of evidence the Head of ABW may run the surveillance – the need to acquire a written agreement from the General Prosecutor is in such a case still pending, and the request for the decision must be presented to the court at the same time.[45]

As it was earlier mentioned, the operational control gives the opportunity to i.a. tap telephone lines, install hidden video cameras and microphones in buildings[46] and vehicles[47], control the correspondence (also electronic one), acquire and store data on electronic carriers, as well as to get access to the content of postal letters and parcels. Despite the fact that some of the mentioned covert means of surveillance are formally incomplete, they seem to allow to record activities of an ABW's person of interest in a multidimensional way – from traditional means of communication to the contemporary ones, including Internet and personal electronic devices. In the era of global network services the legal provisions of data access in different countries are not always compatible, however in Poland this question has been, in most part, formalized.[48]

While discussing the matter of operational control, the ABW's ability to acquire and process communication data[49], i.a. telephone billings[50], postal packages[51], internet

[45] If the court does not allow the operational control in the five-day period since the procedure has started, the Head of ABW stops the surveillance immediately and any acquired materials are to be formally destroyed.

[46] Differently from the regulation of Art. 23 (1) (6) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, these activities are conducted in private spaces.

[47] Executive provisions are still lacking.

[48] There are still some misunderstandings with Polish Internet services' providers but the current practical cooperation positively influences the level of mutual understanding.

[49] Art. 28 (1) and art. 34 (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[50] Especially when there is a need to obtain information on network terminal, IT terminal, end user, call initiator, call receiver, date and time of connection and its duration, kind of connection or localization of the terminal – art. 180c and 180d of the Telecommunications Act of 16 July 2004 (Journal of Laws 2017, item 1907).

[51] To get information about the postal operator, provided services, as well as information allowing to identify the clients, to acquire the packages for communication or content control, to seize the package in case of a suspicion that it contains objects from a crime (for a formal inspection procedure), to admit a crime-related package for the further transport (either untouched or after substituting the content completely or partly, according to other regulations – Art. 82 (1) (1) of the Postal Law of 23 November 2012 (Journal of Laws 2017, item 1481).

data[52], as well as any personal information[53] related to the Agency's persons of interest in the context of its tasks enumerated in Article 5 of the Act on the Internal Security Agency and the Foreign Intelligence Agency should also be mentioned. In such cases, especially in those related to telecommunication, postal or Internet data, the judicial review was also introduced. This means that the proper court has the right to be provided with all materials justifying the ABW's access to this kind of information.[54]

The scope of information ABW is entitled to acquire has recently been broadened by the access to information protected by the bank secrecy and derived data.[55] Such information can be acquired to effectively prevent crimes enlisted in Article 5 (1) (2), to detect them or to establish their perpetrators and gather evidence. The access procedure includes a formal agreement made by the District Court in Warsaw determining the kind and the scope of provided data, as well as the entity obliged to grant the access.[56] It needs to be pointed out that the Head of ABW has 120 days to inform the entity about the fact of obtaining the data related to it. If such information could harm the ongoing covert actions[57] the court – on the Head of ABW's request – can postpone this date[58]. The ability to pass to an entity information about acquiring data related to it and protected by the bank secrecy and derived data also depends from gathering material allowing to initiate legal proceedings – or the lack of such possibility.[59] If the material has been gathered the prosecutor informs the entity before the investigation closes (it can also be done by the Head of ABW, on the prosecutor's request) or – with no hesitation – after it had been closed. If there is no sufficient material it is done immediately after the local prosecutor's office rejects to open the investigation.

Whenever ABW obtains credible information concerning a crime that remains within its remit, it may initiate activities to covertly buy or seize objects from an offence or other objects that cannot be legally produced, owned, transported or traded. Such procedure also relates to controlled acceptance or giving a material benefit.[60] These activities cannot be understood as playing leading role in the criminal process – they are designed to detect perpetrators and gather sufficient evidence.

[52] Especially when it relates to surname and family name(s) of the client, personal identification number or the passport number, personal ID or other identity document, permanent or postal address, verification data of client's e-signature – Art. 18 (1-5) of the Act on Electronic Services of 18 July 2002 (Journal of Laws 2017, item 1219).

[53] Especially the personal identification number and data related to racial or ethnic background, political opinions, religious or ethical beliefs, religious or political or trade-union affiliations, health data, DNA, addictions or sexual relations, information concerning previous convictions, penalties and fines, as well as other decisions issued in court or administrative proceedings – Art. 27 and 28 of the Act on the Protection of Personal Data of 29 August 1997 (Journal of Laws 2016, item 922).

[54] Art. 28a (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[55] Art. 34a (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[56] Art. 34a (6) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[57] Such risk must be considered probable.

[58] Art. 34a (9) and (10) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[59] Art. 34a (11) and (12) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[60] Art. 29 (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

The Head of ABW is designated as authority to order the a/m measures, after being granted a written permission by the General Prosecutor, who is also provided with all covertly acquired material, if the fact of crime perpetration has been confirmed.

Covert oversight of production, transport, storing and trading of subjects from an offence can be initiated in the same manner – after receiving a permission from the General Prosecutor.[61] The only condition in this context is to prevent any risks to human life or health. In this case the legislator obliges national entities (especially the custom entities and the Border Guard), as well as postal and cargo entities to cooperate closely with ABW.

The ability (stemming from a major rule named *argumentum a maiori ad minus*) to apply the operational control both by "covert acquisition" and "covertly supervised package", needs additional attention.[62] The reason for that is the high probability of the fact of a crime and the need of an efficient control of all participants of such activities. It allows to obtain evidence from multiple sources that confirm the reason of criminal inspiration or perpetrators' motivation, often leading to discovering the true principals and initiators of the transactions.

All of the a/m activities are based on the cooperation with informants[63] assisting the ABW officers in performing their duties. It is considered an essential element of building the informational competence of a service. The activity is – paradoxically – underestimated by "newcomers" and overrated by the "old hands". The true power of this operational tool is its apparent simplicity and directness of obtaining knowledge. This form of work can also be easily modified and planned: from individual tasking to long-term undertakings concerning multiple aspects.

The presented instruments may be used by officers to investigate, prevent and detect i.a. terrorist crimes. Additional means are the ABW's analytical abilities, as well as its coordination powers, directly pointed in Art. 40 of the Act on the Internal Security Agency and the Foreign Intelligence Agency: (…) *the Head of the ABW coordinates all covert activities of special services that may influence national security*.

2.2. *Foreign Intelligence Agency (AW)*

According to Art. 6 (1) (5) and (7a) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, the tasks of AW are: (…) *to investigate international terrorism, extremism and international groups of organized crime, as well as* (…) *to investigate, counter and prevent terrorist incidents aimed at citizens or property of the Republic of Poland abroad, with exclusion of terrorist incidents aimed at personnel or property of the Polish Armed Forces*.

[61] Art. 30 (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency – according to provisions of Article 27.

[62] Art. 31 of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[63] Art. 36 (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

In addition to the previously described and defined terms (while describing the tasks of the ABW), "to investigate" and "to prevent" terrorist incidents or other incidents of such a nature, AW undertakes activities aimed at countering them.

To counter, according to the definition, means to prevent a negative phenomenon by undertaking certain activities[64]. In the context of the AW's competences it can be understood as gathering data and analyzing it for further distribution and utilization by other entities.

The main criteria enabling the AW activity is the threat for Polish citizens or property abroad. In this context, officers of AW initiate covert actions and conduct analytical activities.

As far as the activities related to administration and public order, as well as strictly informational ones[65] are common for both of the described Agencies, the very AW has only limited possibilities to engage in covert operations.

What is more, the operational activities of an offensive nature[66] can be undertaken on the territory of the Republic of Poland, however (...) *only through the Head of ABW.*[67]

The obligation imposed on the governmental authorities to inform the Head of AW about events relevant to the external security and international position of Poland, especially regarding international terrorism, extremism and international groups of organized crime[68], seems to take an increasingly central place.

2.3. ***Military Counterintelligence Service (SKW) and Military Intelligence Service (SWW)***

Article 5 (1) (2a) and Art. 6 (1) (2b) and (3a) of the Act on the Military Counterintelligence Service and the Military Intelligence Service of 9 June 2006[69] concern duties imposed on the services in the field of counter-terrorism.

SKW is in charge of identifying, preventing and detecting crimes connected with terrorist activities threatening security of the defence potential of the country, the Armed Forces of the Polish Republic and organizational units of the Ministry of National Defence. On the other hand, SWW is designated as the authority for the identification, counteracting and prevention of terrorist threats to personnel and property of the Armed Forces of the Polish Republic outside the country, as well as dealing with the consequences resulting thereof.

---

[64] http://sjp.pwn.pl/szukaj/przeciwdziałanie.html.

[65] Consistently with the role of AW – they are: gathering (also in a covert manner) any kind of personal data.

[66] Thus: operational control, purchase, in an implicit manner, or the takeover of objects, power to order covert surveillance of the manufacturing, transportation, storage and trafficking of objects from an offence.

[67] Art. 6 (9) (3) (editorial note).

[68] Art. 41 (1) (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

[69] Consolidated text: Journal of Laws 2017, item 1879.

In analogy to the civil security services operating in Poland, SKW[70] is the competent authority to carry out the a/m tasks, whereas SWW fulfills them outside the country. The operational capacity of SKW was regulated similarly to ABW – however, with a few exceptions.[71] The first and probably the major difference concerns the way of execution of appointed tasks by undertaking operational and exploratory activities, as well as analytical and informative, but excluding investigative activities. Thus, SWW plays an active role in recognition of the given issue remaining its responsibility until information justifying the suspicion that a crime has been committed becomes available. The next step – pursuant to Art. 27 of the Act on the Military Counterintelligence Service and the Military Service – is to inform the competent Prosecutor's Office or pass on the information to other competent authority.

The exceptions concerning the a/m similarity are: no access to data provided by banks, falling under the category of bank secrecy and tools used to block accessibility of specified IT data. The other activities i.e. the power to block telecommunications, operational control, obtaining telecommunication, mailing and internet data, collection (also in a covert manner) of all personal data, purchase, in an implicit manner, or the takeover of objects from an offence, power to order covert surveillance of the manufacturing, transportation, storage and trafficking of objects from an offence, request for assistance from any person, as well as the procedure of their implementation, fall within the remits of ABW.

SWW is the military counterpart of AW in the area of competences, which also performs operational and exploratory, as well as analytical and informative activities. The offensive operational activities might be undertaken on the territory of the Republic of Poland only by SKW or ABW.

2.4. *Military Gendarmerie and Police*

The given uniformed services are a part of the governmental administration system established for the purpose of dealing with CT issues. Both, Military Gendarmerie and the Police, were granted the competences pursuant to the Law on the Counter-Terrorism Operations.

The powers of Military Gendarmerie are regulated by Art. 4 (1) (3a) of the Act on the Military Police and the Military Law Enforcement Bodies of 24 August 2001.[72] Pursuant to the Law, Military Gendarmerie is entitled to perform counter-terrorism operations

[70] Military Counterintelligence Service is in charge of identifying, preventing and detecting crimes committed by soldiers fulfilling the active military service, officers of the Military Counterintelligence Service and the Military Intelligence Service, as well as the staff of the Armed Forces of the Republic of Poland and other organizational units of the Ministry of National Defence, as well as collaborates with i.a. Military Gendarmerie but only in performing the a/m activity. Interestingly, this new competence (referred to in point 2a) lacks the possibility to carry out the given tasks, whereas ABW has been granted such a possibility.

[71] These are of crucial importance for identifying the position of the service within the CT system.

[72] Consolidated text: Journal of Laws 2016, item 1483, as amended.

over areas or facilities owned by offices and agencies subordinate to the Minister of National Defence or supervised by him, or administered by these offices and agencies.[73]

Noteworthy is the range of activities undertaken by Military Gendarmerie within their statutory powers, which include operational and exploratory, as well as investigative activities.[74] Those powers, exercised to fulfill own duties, correspond to the competences of SKW i.e. the power to block telecommunications, operational control, obtaining telecommunication, mailing and internet data, collection (also in a covert manner) of all personal data[75], purchase, in an implicit manner, or the takeover of objects from an offence, power to order covert surveillance of the manufacturing, transportation, storage and trafficking of objects from an offence and request for assistance from any person.

According to the author[76], granting investigative powers to Military Gendarmerie means in effect that the service has a leading role among entities under the Ministry of National Defence. Interestingly, it is not one of the special military services mentioned earlier, which in the light of the rules and powers perform strictly informative duties.[77]

On the other hand, pursuant to Art. 1 (3a) of the Act of 6 April 1990 on the Police[78], police is carrying out counter-terrorist activities and therefore becomes the executive authority responsible for the physical elimination of threats.

3. The Law on the Counter-Terrorism Operations

Thus far, in this paper the author described the government administration bodies with appropriate competences, which pursuant to the Law were granted with certain measures and tools for identification, detection, prevention and countering of terrorist threats. The new powers, despite the interference with particular human and citizen rights and freedoms, were adopted with the aim of providing the national security in the widest meaning of the term. Granting the power to use these measures in order to execute statutory tasks by security services should not raise any doubts.

The general picture which emerges from the a/m observations is that security services are authorized to perform operational and exploratory, as well as investigative activities, hence are equipped with instruments enabling identification of a given issue at all stages

[73] The definition of counter-terrorism operation, as well as the source will be provided in the further part of the report.

[74] Art. 4 (2) of the Act on the Military Police and the Military Law Enforcement Bodies.

[75] Taking into account constraints deriving from the Act on the Protection of Personal Data.

[76] The author is aware that there are many opponents of the given stance.

[77] It is difficult to assess whether it is a disadvantage or advantage. There are many different opinions on the given matter, thus the saying "one's point of view depends on where one is sitting" seems accurate. However, experience shows that the farther apart the source is, the more distorted information or the emphasis put in an improper manner. This in turn reinforces the likelihood of its incomplete or improper use. In this situation, not only the structure of one institution at the operational level will be horizontal, but also the procedure will be repeated at the further procedural stage, however from top to bottom.

[78] Consolidated text: Journal of Laws 2017, item 2067.

and its further proceedings. At the same time, taking operational and exploratory, as well as analytical and informative measures – thus, oriented only at obtaining information and its appropriate operation. The same selection and ranking of government institutions have been set out in the specific provisions relating to terrorist offences.

With regard to the Laws stipulating the competencies of the Internal Security Agency, Foreign Intelligence Agency, Military Counterintelligence Service, Military Intelligence Service, Military Gendarmerie and Police, on 10 June 2016 the Law on the Counter-Terrorism Operations was adopted – a lex specialis in the context of terrorist threats. The Law is the response to a long-expected legal regulation in the given matter, adopted to provide a solution to be used in a situation of a real threat, mobilize forces and resources and to respond effectively in the event of a terrorist incident and counteract its impact.

It should be noted, that the act of law regulating the identification, detection and prevention of terrorist threats helped to stipulate the roles and responsibilities of authorities, their capacities and actual tasks by putting the emphasis on the effective functioning of the state in a situation of a real threat.

The need for this regulation can be reaffirmed by *de lege ferenda* arguments put forward a few years ago by collegial bodies of the Criminal Proceedings Department of ABW.[79] At that time, it was proposed to consider taking up steps towards establishing new rules of statutory ranking, providing for a comprehensive regulation on identification, prevention, counteracting, neutralization and dealing with the effects of terrorist attacks, as well as specifying tasks and responsibilities to be taken immediately at the scene of incident by authorized services and institutions.

In order to discuss the content of the Law on the Counter-Terrorism Operations several definitions need to be clarified, thus confirming the validity and relevance of the regulation.

3.1. *Definitions*

Terrorist offence (Art. 115 par. 20 of the Criminal Code)[80] – a terrorist offence is a prohibited act with a sentence of imprisonment for at least five years, committed with the aim of: 1) seriously terrorizing a large number of people, 2) forcing a public authority of the Republic of Poland, or another state or international organization, to take or not to take a certain course of action, 3) cause a serious disturbance in the political system or economy of the Republic of Poland or another state or international organization, – or a threat to commit such an act.[81]

Such definition of a terrorist offence can be also found in other definitions of the offences embodied in the Criminal Code, i.a. in sections XVI-XXII, in which

---

[79] Task Force for developing a proposal for cooperation and management of tasks to be undertaken at the scene of a terrorist incident, established in 2013.

[80] Act of 6 June 1997 – the Criminal Code (Journal of Laws 2017, item 2204).

[81] The motives of a potential perpetrator can be various i.a. religious, political or racial.

the most characteristic crimes are described in Art. 163[82], 164[83], 165[84], 165a[85], 166[86] and 167[87]. The given offences may or rather, as a rule, will include the actual concurrence with other crimes. Thus, there is no possibility to commit a terrorist crime without any connection to other illegal activity stipulated by criminal law provisions. However, it may occur only after a certain period of time that the given criminal offence was committed in relations to a terrorist crime.

Terrorist incident[88] refers to a situation when there are sufficient reasons to believe that it has arisen from a terrorist offence or a threat of such a situation.

While describing an incident, we can specify a scene of the event of a terrorist nature, which can be understood as an open or closed area where an event of a terrorist nature has taken place, or where its effects have taken or were to take place, as well as a space where threats related to the event of a terrorist nature are present.[89] The activities undertaken at a scene of the event by particular services immediately after the incident will represent very significant, but only a part of all measures to be taken by the competent authorities in relation to the incident that might have been of a terrorist nature. According to the a/m definitions, a scene of the event, as well as activities undertaken on site, are only components of a greater whole related to the complex examination of a terrorist offence (i.e. operational and exploratory, as well as investigative).

The act in question regulates the activities of the organs of public administration which are aimed at preventing events of a terrorist nature, preparations to take control over such events by means of planned undertakings, reaction in case such events occur and removal of their effects, including the recovery of the resources aimed at reacting to such events, referred to as antiterrorist activities.[90]

The list of tasks includes also counter-terrorist activities mentioned before. The term should be understood as activities against perpetrators, as well as persons preparing or assisting in committing an offence of a terrorist nature, performed with the aim to eliminate the immediate threat to life, health or property, with the use of specialist forces or means, as well as specialist operational tactics.[91]

3.2. *Terrorism – identification, prevention and counteracting*

The Head of ABW and the minister competent for internal affairs have been given the central role in the provisions. By working together, the authorities are responsible for

[82] Causing a life-threatening event.
[83] Immediate endangerment.
[84] Other endangerment.
[85] Financing terrorist activity.
[86] Piracy.
[87] Dangerous devices or substances.
[88] Art. 2 (2) of the Law on the Counter-Terrorism Operations.
[89] Art. 2 (6) of the Law on the Counter-Terrorism Operations.
[90] Art. 2 (1) of the Law on the Counter-Terrorism Operations.
[91] Art. 2 (2) of the Law on the Counter-Terrorism Operations.

prevention of terrorist incidents, as well as taking control over events of a terrorist nature in case of the occurrence of such events by producing response adequate to the threat.

By increasing emphasis on combating terrorism, the legislator imposed on the a/m authorities the responsibility for the effectiveness and professionalism of activities undertaken by services and institutions in a threat situation or in case of a suspicion of committing an offence of a terrorist nature.[92]

While discussing certain stages of an operation, we have to focus on those resulting from the Law on the Counter-Terrorism Operations, which are: identification, prevention and counteracting. The legislator designated the Head of ABW as the authority responsible for the prevention of terrorist incidents. The Law on the Counter-Terrorism Operations is a specific law referring to threats and incidents of terrorist nature, thus the majority of activities that can be carried out by ABW have been regulated in the Law on the Internal Security Agency and the Foreign Intelligence Agency. Designating the given powers to ABW supports the argument that there is a need for one centre responsible for gathering all information concerning terrorist incidents and giving instructions, in order to ensure efficient, quick and adequate response. The given responsibilities were assigned to the Head of the Internal Security Agency, who within the remits of analytical and informative, as well as operational and exploratory activities gathers information and coordinates activities undertaken by other authorities and public institutions, while at the same time conducting operational activities against individuals suspected of being involved in terrorism.[93]

The Head of ABW is authorized to coordinate analytical and informative activities of Polish external and internal security services i.a. Military Counterintelligence Service, Foreign Intelligence Agency, Military Intelligence Service and Central Anticorruption Bureau, as well as other authorities i.a. Police, Border Guard, Government Protection Bureau, State Fire Service, Customs Service, General Inspector of Financial Information, General Inspector of Fiscal Audit, Military Gendarmerie and Government Centre for Security. The coordination arrangements include exchange of information on possible terrorist threats[94], as well as persons associated with terrorist activities.

Individuals of particular interest are divided into four categories:

- persons involved in activities on behalf of terrorist organizations or organizations connected with terrorist activities or members of such organizations;

---

[92] Art. 3 (1) and (2) of the Law on the Counter-Terrorism Operations.

[93] Particular attention should be drawn to categorical statements, such as: “the Head of ABW coordinates”, which impose the obligation to take such actions. There is no room for an independent decision to take certain actions. This implies a need for taking coordinating measures by the Head of Internal Security Agency in the event of threat.

[94] In particular, incidents described in the catalogue of incidents and events of a terrorist nature included in the Directive of the Minister of the Interior and Administration of 22 July 2016 on the open catalogue of terrorist incidents (i.e.: Journal of Laws 2017, item 1517).

- wanted persons involved in terrorist activities or persons suspected[95] of committing offences of a terrorist nature, with regard to whom an arrest or a search warrant has been issued or a wanted letter has been decided on, as well as persons who are wanted and subject to the European Arrest Warrant;
- persons with regard to whom there is a justified suspicion that they are involved in activities aimed at committing an offence of a terrorist nature, including persons who might present a threat to civil aviation;
- persons participating in a terrorist training or undertaking journey with the aim to commit an offence of a terrorist nature.[96]

The Head of ABW maintains a register including the a/m information.

Officers of ABW, Police and the Border Guard are entitled to take fingerprints or record the face image of individuals included on the list or a person who is not a citizen of the Republic of Poland in case when there is a doubt as to the identity of this person or there is a suspicion that the border of the Republic of Poland has been crossed illegally, or there is a doubt as to the declared purpose of the person's stay on the territory of the Republic of Poland. The organ, which has taken the fingerprints or recorded the person's facial image, shall transmit to the Commander in Chief of the Police the obtained data which are then entered in the Police databases.[97]

In order to prevent events of a terrorist nature, the Head of ABW has free access to the data and information gathered in public registers and records that is kept in particular by: Military Counterintelligence Service, Foreign Intelligence Agency, Military Intelligence Service, Central Anticorruption Bureau, Police, Border Guard, Government Protection Bureau, State Fire Service, Customs Service, General Inspector of Financial Information, General Inspector of Fiscal Audit, Military Gendarmerie, Government Centre for Security, Head of the Office for Foreigners, President of the Office of Electronic Communication, President of the Office for Civil Aviation, President of the National Atomic Energy Agency, Social Insurance Office, President of the Agricultural Social Insurance Fund, Financial Supervision Authority, Land Surveyor General, local authorities and General Prosecutor.[98] The scope of the data includes also the image of events recorded by image recording equipment located in public venues, by public roads and other public places.[99]

Pursuant to Art. 4 of the Law on the Counter-Terrorism Operations, organs of public administration, owners and holders of facilities, installations, and equipment of public administration infrastructure, as well as critical infrastructure[100], are obliged

[95] Whereas the Act refers to presumed suspects, what was probably meant were suspects toward whom there was sufficient evidence to issue a decision to present charges (not necessarily announced to the a/m persons).

[96] Art. 6 (1) of the Law on the Counter-Terrorism Operations.

[97] Art. 10 (1–6) of the Law on the Counter-Terrorism Operations.

[98] Art. 11 (1) of the Law on the Counter-Terrorism Operations. It should be emphasized, that this power encompasses also units subordinated and supervised by the a/m organs.

[99] It is worth mentioning that it concerns on-line streams.

[100] In particular, any potential threat to the functioning of energy, water and sanitation, heating and

to convey to the Head of ABW information they possess about terrorist threats to the infrastructure of public administration or the critical infrastructure and the Head of ABW can issue orders[101] to them aimed at counteracting, removing or minimizing the threats.

Another area of activities imposed on the Head of ABW includes coordination of operational and exploratory activities undertaken by the special services and authorities mentioned in the previous paragraph, as well as activities performed by customs officers of observing and recording vision and sound of events in public spaces[102]. The operational and exploratory activities have to concern incidents of a terrorist nature. The Head of ABW can issue recommendations[103] to the entities, with the aim to remove or minimize the terrorist threat which has occurred.

Article 9 of the Law on the Counter-Terrorism Operations deserves particular attention. It refers to the extended scope of activities of ABW and includes, apart from prevention, also identification and counteracting of terrorist offences. The new competence of the Head of ABW, which has not been indicated previously, is counteracting, which according to a dictionary definition means any action against a person or object, overcoming an obstacle by taking long-term steps.[104]

The given regulation stipulates that the Head of ABW may order covert activities (such as obtaining and recording the content of conversations by technical means, including with the use of telecommunication networks; image and sound of persons from premises, means of public transportation and other venues from public spaces; content of correspondence, including correspondence kept by means of electronic communication; data from data storage devices, telecommunication terminal devices; as well as information and IT systems and finally obtaining access and controlling the content of consignments)[105] with regard to a person who is not a citizen of the Republic of Poland, and with regard to whom there is a fear of possible involvement in terrorist activities.

The Head of ABW shall, without delay inform the Minister Coordinator of Special Services, as well as the General Prosecutor about the undertaken actions, who may order to stop the activities[106]. These actions might be ordered for a period of no longer than three months with a possibility of extension, however under Art. 27 of the Act on the Internal Security Agency and the Foreign Intelligence Agency.[107]

IT systems and networks, relevant for the national security.

[101] These will likely be legally binding notices to take specific actions.

[102] Art. 8 (1) of the Law on the Counter-Terrorism Operations.

[103] Although it is only a "recommendation" it is difficult to imagine a situation in which either authority – not having a comprehensive view of the situation – would refuse to follow such a recommendation.

[104] http://sjp.pwn.pl/szukaj/zwalczanie.html.

[105] These bring about associations with the operational control described in Art. 27 of the Act on the Internal Security Agency and the Foreign Intelligence Agency, which make complete sense.

[106] Art. 9 (4) of the Law on the Counter-Terrorism Operations.

[107] It refers to judicial control of the validity of the extension.

The decision to undertake activities equivalent to the operational control[108], which is a single-stage procedure, comes to the fore. What is more, it should be emphasized that the procedure has been limited to foreigners who are not citizens of the Republic of Poland, and the powers of the Head of ABW were granted by a legal act of statutory rank. Thus, there are no grounds for questioning this legal basis and powers to carry out the given tasks.

By defining a specific threat, the legislator provided the Head of ABW with a possibility to undertake offensive operational activities. Having in mind that it refers to the concern for undertaking terrorist activities by foreigners[109], the normal procedure of initiating the operational control, on the basis of Art. 27 of the Internal Security Agency and the Foreign Intelligence Agency, could be hampered or even impossible. In order to apply the given procedure, any other operational measures would have to be ineffective or useless. The ever-evolving nature of terrorism makes it impossible to apply the standard operational activities that include a variety of actions from simple methods and measures to more sophisticated solutions, which very often require complex combinations or operational games. Time is of the essence[110] when it comes to the implementation of the procedure. There is no place for hesitation when intelligence on a possible terrorist threat is obtained and an immediate and rational decision has to be made.[111] That is one side of such statutory solutions.

On the other side, the common perception of terrorism as homogenous is not always that obvious.[112] Terrorist activities include also logistical actions related to individuals against whom further procedural steps are to be taken and evidence is to be collected in order to take the case to court. Therefore, it gives possibility to identify the actual masterminds and other participants, as well as clarify their roles and identify potential targets. This, in turn, as it was mentioned before, gives advantages and possibilities to security services.

The aforementioned arguments indicate that the decision to grant the Head of ABW with the ability to undertake offensive operational activities in the light of the terrorist threat was correctly taken.

---

[108] Although supervision over the proper application of these activities is the responsibility of the General Prosecutor by the power to finish them, according to the provisions, the Head of ABW has the duty to immediately inform about the taken actions, which in practice might mean that they will be in force for a certain period of time.

[109] It refers to individuals, whose identity is very difficult or even impossible to be verified, as well as other data such as place of residence or criminal records.

[110] Truly, the author did not want to mention that argument but that is the reality of any public administration body. In order to introduce certain actions, time in organization unit first is needed, then its implementation must be accepted by the unit, department and appropriate documents have to be passed to the other institution etc. Before sending a motion concerning the implementation of surveillance procedure to the Regional Court in Warsaw documents goes through a few organizations units (not even mentioning the supervisors, who have to accept these documents).

[111] This includes also taking responsibility for the decisions made.

[112] A suicide bomber, one faith believer, armed with explosives attached to a specified uniform.

Another approach, which is also significant in the given matter, cannot be ignored. As is was stated by Mr. Lech Paprzycki, who is the President of the Criminal Chamber of the Supreme Court (…) *for many years security services were operating* (…) *under limited prosecutor and judicial control*, he also added that the aspect of control should be in the interest of officers in order to ensure that activities (i.e. of an operational nature), undertaken by them, including counter-terrorist, are conducted in conformity with the law.[113] Giving the Head of ABW the power to execute actions described in Art. 9 of the Law on the Counter-Terrorism Operations, without obtaining the prior consent of the court, may raise certain controversies, in particular in relation to the general obligation of judicial checks on applications for operational control imposed on all security services.

Considering the above, it can be assumed that specific circumstances require specific competences, and these require exceptional professionalism, accuracy and diligence. These qualities will guarantee appropriate and effective use of tools granted to the Head of ABW.

After finishing activities described in Art. 9 the Head of ABW passes all gathered materials to the general prosecutor, who decides about the scope and the way the materials will be utilized. An assessment, if the materials have enough evidence to initiate a criminal proceedings, is conducted by the general prosecutor[114], who, if there is not enough evidence orders destroying the material.

The rules in the Act on anti-terrorist activities refer in a visible way to the proceeding field, which was extended to special opportunities as far as information obtained during conducted operational activities is used, which caused the appropriate reaction to the threat of terrorist nature. The author emphasizes that in case when the operational officer recognizes the terrorist threat it will be almost the end of the potential case at his level, whereas – as far as prevention and combating the above-mentioned threat, including gathering and securing the evidence in the legal process, and further arresting the perpetrators are concerned – the case will just begin.

A novelty in the criminal proceeding regulations are rules allowing to search at any time of day and night premises, including individuals staying in the certain rooms or in the certain premises.[115] The decision is made by the prosecutor, who acts on the basis of the notion containing materials describing the suspicion, attempts to commit a crime or preparation to commit a crime of terrorist nature and justified suspicion basis, that the above mentioned things are there prepared by the appropriate ABW's unit. In an analogical situation the prosecutor can issue a decision to detain the suspected person.

---

[113] L.K. Paprzycki, *Czy Polsce potrzebna jest ustawa antyterrorystyczna?*, in: *Terroryzm – materia ustawowa?*, K. Endecki, P. Potejko (ed.), Warszawa 2009.

[114] It is indicated in Art. 27, para.15 Act on the ABW and AW, according to which the Head of ABW decides if material gathered from surveillance procedure has enough evidence to initiate a criminal proceeding, and if it has, it can be passed to the General Prosecutor.

[115] Article 25 (1) of The Act on anti-terrorist activities.

Analyzing the above regulation it can be assumed that information concerning what or who needs to be found must be limited to justified suspicion[116] and describe precisely according to which criminal case must be gathered and verified. These knowledge not necessarily contains the grounds on the basis of which the investigation may be initiated, in which it is crucial to justify the suspicion of crime[117]. It seems that result of performed activities will set grounds to take the decision of initiating or refusal of instituting a preparatory proceeding. The said activities will be carried out, using trade law terminology, "in organization investigation" that is before the decision about its formal initiation.

If during surveillance and intelligence activities a gathered material indicates the suspicion of committing a crime, the prosecutor, with due regard for the investigation of the alleged offence, can issue a decision on presentation of the charges, based on the operational materials.[118] Furthermore, in case the possibility of committing, attempts to commit or preparation to commit a crime of terrorist nature the prosecutor can issue a decision for provisional detention of the suspected person.[119]

The regulation allows to present charges in a case of "only" suspicion of committing a crime, not necessary justified suspicion, under the condition of activities with regard of further purpose of pre-trail proceedings. Whereas, in case of its probable suspicion[120] it can be a premise for provisional detention.

The above-listed activities of proceeding character before formal investigation begins may have its source in Art. 308 Code of the Criminal Proceedings that is a proceeding in the essential scope, "adjusted" to reality of the terrorist threat. It can be true, especially, when applying to materials gathered accordingly with Art. 9 Act on anti-terrorist activities. It would be more difficult if the mentioned decision were taken on the basis of vague, ambiguous terms, not consulted objectively with ABW's units responsible for cooperation with the prosecutor.

---

[116] It is worth noticing that it is a challenging construction.

[117] As W. Grzeszczak stated that the basis on which the investigation may be initiated can be only such data, which impartially makes committing a crime more likely to happen, whereas subjective emotions arise high suspicion of its appearance. The said basis is a minimum condition, thus the obviousness of crime committing is even more likely to fulfill the condition to initiate the proceeding. The Act on anti-terrorist activities describing justified suspicion of a perpetration of a criminal offence requires it to be based on a rational premise. This condition is not fulfilled by rumor, thought or not close related suspicion regarding the crime because such suspicion would be arbitrary. The justified suspicion must refer to the certain crime, an act, which can be qualified from certain regulation of the Criminal Code or other specific act, but it goes with stadial forms and phenomenal crime, see: W. Grzeszczyk, *Postępowanie przygotowawcze w kodeksie postępowania karnego*, Kraków 1998, p. 48

[118] Article 26 (1) The Act on anti-terrorist activities.

[119] Article 26 (2) The Act on anti-terrorist activities.

[120] The legislator uses not precise phrase "probable suspicion" avoiding a code phrase "reasonably assumed". It seems that before the motion for provisional detention would be better to obtain materials justifying the suspicion of a perpetration of a criminal offence, giving the basis for initiating the investigation as it is stated in Art. 303 of the Code of Criminal proceedings.

Due to variability of methods used by the terrorists, the Services should have adequate instruments that would enable them proper recognition and evaluation of threats and effective counteracting of possible situations of terrorist nature. The instruments, so that they were effective, considering development, need to be adopted to the realities and updated systematically.

At the end the author quoted a fragment of one of the operation cases analyzed a few years ago, in which long before regulation of the Act on the anti-terrorist activities he indicated that:

> (...) in the context of current situation concerning terrorism development in Europe, in the Middle East, Asia and both Americas, the decision whether the given occurrence poses a threat should be made with no presumption of innocence, with any doubt being treated as detriment, at least in terms of verification necessity [and possibilities]. Actually, accordingly to media information, this strategy was accepted in practice with various countries that are particularly exposed to terrorism (the USA, England, Israel, etc.) and this is currently accomplished.

This approach gives an opportunity to fight against organizations and their members, which are aimed at widespreading feeling of threat.

A thorough familiarity with the Act on anti-terrorist activity and other legal acts related to it, gives an answer to the raised question concerning legitimacy of equipping state bodies with certain tools regarding possible special threat to the state security and its citizens and legitimization of the activities in the Polish legal system. In both cases – although, one could say that some regulations are controversial – the answer is “yes”.

Obviously, minor and more serious mistakes were not avoided, however, they will not be verified until situation of direct necessity to use regulations of the Act on anti-terrorist activities appears.

Events of last years, months and even days have reflected the significance of the subject and its regulation requires special attention and accuracy. Increasing number of terrorist acts, including activities supporting such organizations, requires an immediate and effective reaction[121] that simultaneously should be legal.

Since June 10, 2016 we have had a starting point thanks to which the mentioned at the beginning of the article “a step behind the criminal” may become much more shorter.

[121] With a wide range of effective accomplishment of goals imposed to state authorities.

Abstract

Issues concerning terrorism appear to be highly popular and prone to public discussion. This concerns both comments of incidents and occurrences with terroristic backgrounds including looking for reasons of such a situation and attempts to prepare our state for pushing the attack and prevent it.

Unfortunately, as one can notice this discussion takes place, in my humble opinion, in the atmosphere of unnecessary tense and commotion each time evoked by the peculiar character of the commented occurrence and relating it to a current situation in Poland, very often with political connotations. What is noticeable is the lack "cold blood and common sense', which is significantly crucial to assess a particular threat, let alone real actions in the face of it.

This article include a multitude of answers posed by potential participants, observes and listeners of such discussions. These questions especially concern designated organs fighting terrorism and their tasks. Moreover, they concern more advanced issues regarding a range of means and methods f work of operational and reconnaissance as well as investigation teams.

The above considerations were preceded by an attempt to define the role of the state to assure public safety and the significance of this role for both administrational organs and the society itself.

The issues included in this article shall constitute a possibility of, hopefully, objective adjudication of numerous issues cited in the comments in the introductory part.

Keywords: safety, terrorism, counter-terrorism action, operational control, covert activities.