SSOAR

Open Access Repository
www.ssoar.info

Information Security as Exemplified by Clandestine Collaboration and Influence Exerted by the Polish Internal Security Agency Officers on Journalists - de lege lata and de lege ferenda regulations

Rosicki, Remigiusz

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Rosicki, R. (2014). Information Security as Exemplified by Clandestine Collaboration and Influence Exerted by the Polish Internal Security Agency Officers on Journalists - de lege lata and de lege ferenda regulations. *Przegląd Strategiczny (Strategic Review)*, 7, 145-154. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-450599

Nutzungsbedingungen:
Dieser Text wird unter einer CC BY-NC-ND Lizenz (Namensnennung-Nicht-kommerziell-Keine Bearbeitung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de

Terms of use:
This document is made available under a CC BY-NC-ND Licence (Attribution-Non Comercial-NoDerivatives). For more Information see:
https://creativecommons.org/licenses/by-nc-nd/4.0

gesis
Leibniz-Institut
für Sozialwissenschaften

Mitglied der
Leibniz-Gemeinschaft

Remigiusz ROSICKI
Adam Mickiewicz University in Poznań

DOI 10.14746/ps.2014.1.11

INFORMATION SECURITY AS EXEMPLIFIED BY CLANDESTINE COLLABORATION AND INFLUENCE EXERTED BY THE POLISH INTERNAL SECURITY AGENCY OFFICERS ON JOURNALISTS – *DE LEGE LATA* AND *DE LEGE FERENDA* REGULATIONS

OBJECTIVE SCOPE

The aim of the analysis is information security which will be illustrated with the example of the *de lege lata* and *de lege ferenda* regulations as part of the legal acts setting down the operation of the *Internal Security Agency* (ABW) in Poland. The analysis of the issues of information security, from the perspective of the activity of one of the Polish special services, is of particular importance given the relevance of continual institutional changes of individual special services in Poland since the 1990s, as well as with regard to the abuse of the services for political purposes.

The starting point for the analysis is the category of information security which should be approached objectively (Rosicki, 2010: 24–32; Zięba, 2008: 15–39). Given the escalation of manifold threats of international and national character, the plane of objective approaches to security is expanding; all the more so because of the ever-broadening spectrum of security studies, which have long surpassed the issues of military threat (Czaputowicz, 2012; Rosicki, 2010: 24–32). Still, the military paradigm is so sturdy that even information security is looked into from the angle of national security (Lidel, 2005) – with the recommendation and/or substantiation of significant prerogatives of the State in this scope. The discourse on the way information is acquired by both the State and the citizens may serve as an example. As for the former, state institutions invoke the priority of security, which came to be particularly noticeable in the case of war on terrorism or other kinds of asymmetrical threats (Koziej, 2011: 21–49; Madej, 2007). As for the latter, activities undertaken by such persons as Edward Snowden or Julian Assange are of major importance. The activities engaged in by these two persons, and aimed at information freedom follow from various problems, and yet they share a common core that can be boiled down to the following questions: (1) Where are the global and national security boundaries that can be invoked by the State and/or international community? (2) How much freedom can be sacrificed for the sake of security? (3) How much information can the State gather about its own (and not only its own) citizens? (4) On what principles and within what scope may the citizens break the restrictions imposed on the access to confidential, top secret and other kinds of classified information?

On the one hand, we are dealing here with the issue of the infringement of the principles related to the functioning of contemporary democratic systems, that is the evaluation of the abuse of state structures (Edward Snowden); on the other hand, we are dealing with transparency and the fight for access to information, which takes on the form of hacktivism (Julian Assange). These issues are very interesting because of the clash of two values – freedom and security; nevertheless, they will not come under closer scrutiny. Still, it is worthy of note that the problems, particularly within the context of activism, have already been addressed in academic literature and literature directed at the general public, as well as in opinion journalism (Cf. Jordan, 2008; J. Assange et al., 2012; J. Assange, 2013).[1] Also, it is worth mentioning the significance of information within the context of the reconfiguration of tools of governance against the backdrop of historical development of societies, which was put forward by M. Foucault as part of his concept of discipline, as well as critiqued by, inter alia, Mathiesen (Foucault, 1975; Mathiesen, 1997: 215–234; Węgrzecki, 2011: 331–484; Herer, 2012: 237–264).

INFORMATION SECURITY EXEMPLIFIED BY POLAND

The issue of information security as exemplified by Poland will be reduced to the relation between the *Internal Security Agency* officers and journalists. Hence, the text will only address a fragment of the question in hand, which thus will not represent all the complex issues related to the circulation of information within the context of the activities of the Polish special services. In particular, the issues raised here will not be examined in connection with the applicability of the *Classified Information Protection Act* (Journal of Laws of the Republic of Poland, 2010),[2] the *Personal Data Protection Act* (Journal of Laws of the Republic of Poland, 1997) or the *Act on Access to Public Information* (Journal of Laws of the Republic of Poland, 2001; Aleksandrowicz, 2002; Jabłoński, Wygoda, 2002; Taradejna, Taradejna, 2003).

Therefore, the approach presented in this article will not be characterized by systematic analysis – in any case such an analysis might only demonstrate the dispersion of the issues related to the "circulation" of information as illustrated by various legal acts, which is the ramification of poor legislative culture of the Polish lawmakers. A lack of transparency and a proliferation of various institutions have been characteristic traits of the Polish lawmaking processes since the beginning of the 1990s. It neither positively affects the transparency of the law, nor – what is more important – the ease of its application.

The objective scope of the analysis concernes the *de lege lata* and *de lege ferenda* regulations as part of the activity of the *Internal Security Agency*. With regard to the *de lege lata* regulations, we are dealing with the *Internal Security Agency and Foreign Intelligence Agency Act* of 2002 (Journal of Laws of the Republic of Poland, 2002),

---

[1] It is also worth mentioning the program featuring J. Assange, entitled "The Julian Assange Show: Cypherpunks", which was broadcast by the Russian TV station Russia Today in 2012.

[2] Dziennik Ustaw [Journal of Laws of the Republic of Poland] 2010, No. 182, Item 1228, as amended.

whereas in the case of the *de lege ferenda* regulations, we are dealing with the *Bill of Internal Security Agency* of 1 August 2013 (hereandafter: 2013 Bill). As for the former, the penal provisions of the Act, that is Articles 153b–153d (Chapter 10a) are applicable, whereas as for the latter, the applicable regulations are the Bill Articles numbered 197–199 (Chapter 10). In broad outline, these regulations concern the issues related to the special service officers' (or former officers') responsibility for the use of information gathered while fulfilling official duties and engaging in the so-called clandestine collaboration.

POLISH SPECIAL SERVICES – THE CONTEXT OF STATUTORY CHANGES

The official reason for the changes to the regulations concerned with the structure and operation of the *Internal Security Agency* is the "Amber Gold" scandal. Nevertheless, this excuse should be recognized as rather implausible, since by all accounts the services kept the executive (including Prime Minister D. Tusk) advised about the potential threats following from the operation of this company (a peculiar pyramid scheme). The accusation levelled at the Polish special services that they neglected to take any action in this respect must be viewed as an attempt at excusing the inaction on the part of other state authorities, including the executive (the *Council of Ministers* and the Prime Minister); all the more so because the "Amber Gold" case and the airlines that belonged to the company were connected with the Prime Minister's son (at least in the media accounts). The "Amber Gold" case tarnished the Prime Minister's image, as well as undermined his veracity regarding the information he obtained from the *Internal Security Agency.*

Another major issue that might have affected the government's decision concerned with the work on the changes to the regulations on the *Internal Security Agency* (ABW) is the case of J. K. Bielecki (one of the advisers to Prime Minister Tusk), who was accused by a newspaper of lobbying for a Russian company Acron, which was reputedly vying to take over the *Grupa Azoty* – a Polish company of strategic significance. According to a newspaper, the Prime Minister was informed about this by the head of ABW. The Agency itself denies the existence of such a report (Cf. *Lobbing*, 2013).

The year 2013 witnessed a problem with the workings of another special service – the *Military Counterintelligence Service* (SKW). The problem concerned a personality clash between two generals: the head of the *Military Counterintelligence Service* (J. Nosek) and the deputy minister of national defence (W. Skrzypczak). The mass media announced that the action taken by SKW against General W. Skrzypczak might have been tinged with personal prejudice, and not merely have been driven by willingness to take care of state security: the revocation of Skrzypczak's security certificate, pointing to the likelihood that he might have earned an illegitimate income, accusations of swaying armament sector tenders organized by the Ministry of Defence (Wroński, 2013).

With regard to the above-quoted cases, two problems emerge. The one is the acquisition of information by journalists; the other is the possibilities that the special services

have of collecting information and/or keeping under surveillance both public figures and ordinary citizens. From the perspective of this text's analysis, the first problem is of overriding importance, that is the penal regulations concerned with the flow of information between former and/or current officers of the Polish special services and journalists.

THE INFLUENCE EXERTEDBY INTERNAL SECURITY AGENCY OFFICERS ON JOURNALISTS' ACTIVITY AND CLANDESTINE COLLABORATION BETWEEN OFFICERS AND JOURNALISTS

A teleological-functional justification for the introduction of regulations contained in Chapter 10a of the *Internal Security Agency and Foreign Intelligence Agency Act* of 24 May 2002

The necessity of introducing the regulations presently contained in Chapter 10a (Articles 153a–153d) of the 2002 Act was highlighted, inter alia, in the justification for statutory changes prepared by the representatives of the *Senate* in 2006. The justification reads that the work on the changes is driven by the need to implement transparency regarding holding extra positions by special services officers. This means that the legislators wanted to impose restrictions on holding offices in the business and public spheres by special services officers. Still, it must be pointed out that 3 out of 4 articles in Chapter 10a concern the relations with the media and not the ban on holding offices in specific circles. This in turn means that the justification invoked by the Senators, in the course of legislative changes, is at least dubious as far as its argumentative value is concerned.

It must be noted that the object and function of the implemented regulations are rather connected with "pathologies" concerning informal "links" and relations between officers and the political sphere. The fact of having access to "deficit" information alone might have enabled special services to use the mass media for swaying current politics; for the same reason they might have become the object of political "horse-trading". This served as the rationale for the attempted statutory restriction of easy transfer of all the information that the *Internal Security Agency* and *Foreign Intelligence Agency* (AW) were in possession of.

In the case of the proposed changes of 2006 the Polish legislators did not even try to refer to the existing laws concerned with the circulation of information bearing special clauses (e.g. top secret, secret, confidential, classified) – that is, to the *Classified Information Protection Act* (Journal of Laws of the Republic of Poland, 2010). Following down the "easy path" and leaving aside the systematic approach, the legislator created another type of information, whose circulation has been penalized. It seems that with this "simple" legislative move, the legislator expected to broaden the scope of criminal responsibility, in comparison to the regulations on the responsibility for the breach of state and professional secrecy, and which are addressed in Chapter XXXIII of the *Penal Code* (Journal of Laws of the Republic of Poland, 1997). The expected result of this so-

lution is greater discipline among the officers of the *Internal Security Agency* and *Foreign Intelligence Agency*.

From the perspective of the reason of the State, attention should drawn to the significance of the institution itself – the *Internal Security Agency*. Pursuant to the *Classified Information Protection Act*, its head serves as "national security authority" (Art. 11). In the same vein, the remit of the *Internal Security Agency* delineated in Art. 5, Sec. 1, Para. 3 and 4 of the *Act on the Internal Security Agency* and *Foreign Intelligence Agency* of 2002 should be highlighted. Hence special criminal responsibility of the Internal Security Agency officers who look after the system that safeguards information – including classified information – would be advisable.

The influence exerted on journalists' activity by *Internal Security Agency* officers

Art. 153b of the 2002 Act and Art. 197 of the 2013 Bill penalize the use by the officers of the information acquired either while fulfilling or in connection with their duties for the purpose of affecting the operation of public authority bodies, entrepreneurs or broadcasters – within the meaning of the *Act on Radio and Television Broadcasting*, chief editors, journalists and persons conducting publishing activity. An *Internal Security Agency* officer who commits such a deed in contravention of the provisions of the Act is liable to imprisonment for the term between 6 months and 8 years. However, if he or she acts with a view to receiving a personal or material benefit, they are liable to imprisonment for the term between 2 and 12 years. As regards the understanding of the term "**journalist**", the legislator refers the reader to the *Act on Press Law*, which defines the journalist as a person who edits, creates and prepares press materials, and who remains in an employment relationship with the editorial board, or who engages in such activity on behalf of and with the authorization of the editorial board (Cf. Dobosz, 2006: 73–90; Ferenc-Szydełko, 2008: 77–86; Sobczak, 2008: 312–347; Sobczak, 1993: 48–49).

Art. 197 of the 2013 Bill does not only differ from the former regulation in respect of the way it is edited, for the said Bill carries "its own definition" of a journalist (Art. 26, Sec. 1, Para. 9): a person who edits and prepares press materials, and who remains in an employment relationship with the editorial board (a unit governing the preparation process, that is gathering, evaluation and development of the materials to be published in the press), or who engages in such activity on behalf of and with the authorization of the editorial board, on the basis of a contract for specific work or a contract of mandate.

Given the above-mentioned legal solution, many questions arise as for its application. The solutions included in the 2013 Bill will give rise to a problem concerned with persons who are not on an employment contract, either for specific work or of mandate, since they are, e.g. student interns or trainees, which – given the Polish reality – is a standard practice rather than an isolated case. This means that in the case of a student who writes a current affairs commentary for an editorial board, and this commentary is later on published without any contract being signed, but the text contents having been affected by an officer, the person's action cannot be penalized (Cf. Ferenc-Szydełko, 2008: 83–84; Sobczak, 1993: 48–49).

Some other issues that ought to be connected with the deed defined in Art. 153b of the 2002 Act and Art. 197 of the 2013 Bill are: (1) What intent will be taken into consideration (a direct intent)?; (2) Will the character taken into account be of material or formal nature?; (3) How in practice will it be possible to point to the feature of a prohibited act in the form of "the use of information to exert influence" on e.g. a journalist? Besides, it is essential to maintain a broad sense of information that an officer obtained while fulfilling or in connection with his official duties.

As for the above-invoked crime, it is worth mentioning its main elements: (1) the subject of a crime (an *Internal Security Agency*/*Foreign Intelligence Agency* officer); (2) the objective aspect (the use of information obtained while fulfilling or in connection with official duties to influence individuals); (3) the object of the crime (the good that must be protected for the sake of the reason of the State – information itself, that is information security, but also the individuals mentioned in the article: inter alia, journalists).

As regards the definition of the crime subject, we shall say that in Article 153b of the 2002 Act and in Article 197 of the 2013 Bill the subject is defined individually (an individual crime). In the case when the kind of intent is defined, it must be pointed out that in a case like this we are dealing with a direct intent (an officer wants to commit a prohibited act, which means that he is aware of it and is willing to accomplish it). The crime defined above is of material character, so there must be an effect in the form of an exertion of influence. In the case of a journalist this effect will take the form of an acceptance of the press material as fit for being published as a press article. It is also worth mentioning Art 128, Clause 3 of the *Penal Code*, which defines the crime as an exertion of influence on "official activities of a constitutional authority of the Republic of Poland" – here the scope of activities has been partially defined though. However, in the case of Art. 153b (of the 2002 Act) and Art. 197 (of the 2013 Bill), the influence scope is quite broad, given the use of the expression of the "influence on activity", inter alia, of the public authority body, **journalists**. In the case of journalists it would be advisable to consider the quite narrow notion of activity, that is the actions of editing, creating and preparing press materials.

Art. 135c of the 2002 Act and accordingly Art 198 of the 2013 Bill penalize the use by a former *Internal Security Agency* and/or *Office for State Protection* (a predecessor of ABW and AW) of the information gathered while fulfilling or in connection with official duties for the purpose of affecting the operation of public authority bodies, entrepreneurs or broadcasters, editors-in-chief, **journalists** and persons conducting publishing activity. Any person engaging in such an act will be liable to imprisonment for the term between 6 months and 8 years, whereas if they act with a view to receiving a personal or material benefit, they will be liable to imprisonment for the term between 2 and 12 years.

As for Article 153c of the 2002 Act and Art. 198 of the 2013 Bill, it is necessary to point out the same doubts which were raised in relation to Art 153b of the 2002 Act and Art 197 of the 2013 Bill. Besides, one should draw attention to the Polish legislator's inconsistency, since while defining 'the former officer', the legislator refers to the officers of the *Office for State Protection* and of the *Internal Security Agency*, whereas he does not refer to former officers of the Security Service (a main security organization in the People's Republic of Poland). There might emerge a hypothetical situation con-

cerned with possession of "valuable" information, e.g. information about the intelligence agent network under operation or another form of services cooperation which might be continued in the Third Republic of Poland (this only serves as an example of a possible situation, however more cases might be invoked).

Clandestine collaboration between Internal Security Agency officers and journalists

Clandestine collaboration between an Internal Security Agency officer and a broadcaster, an editor-in-chief, **a journalist** or a person conducting publishing activity was penalized in Art. 153d of the 2002 Act, and in Art. 199 of the 2013 Bill. An *Internal Security Agency* officer who chooses to collaborate with the individual entities is liable to imprisonment for the term between 6 months and 8 years. In section 2 of this Article the legislator introduces an exclusion of culpability – the above-mentioned crime is not committed by an *Internal Security Agency* officer who has been granted the Agency Head's permission, which is defined in Art. 37, Section 2 of the 2002 Act. As such, the Act does not contain a definition of **clandestine collaboration**, not to mention the notion of collaboration itself. Still, Art. 37, Section 1 features "a list of persons of various professions or in specific positions, with whom *Internal Security Agency* and *Foreign Intelligence Agency* officers must not engage in clandestine collaboration, e.g. judges, prosecutors, attorneys-at-law, directors general at ministries, central government offices or province authority offices, broadcasters, editors-in-chief, **journalists** or persons conducting publishing activity. At this point, it is worth noting that for a long time the legislator did not include in the "list" – say – legal advisers, who – just like attorneys-at-law – represent, in the Polish legal system, a profession of public trust (changes in this respect are due to come into force as late as 2015). The list also does not feature the authorities of the *Polish Press Agency*, of the *Polish Television* (the supervisory board, the management board, the directors), that is – the persons who directly and/or indirectly exercise influence on the broadcast programming and communication of information. In case of Art. 199 of the 2013 Bill, we are dealing with the same solutions as far as clandestine collaboration is concerned; as far as the exclusion of clandestine collaboration is concerned, the authorities of the *Polish Press Agency*, and of the *Polish Television* (the supervisory board, the management board and the directors) are not included either.

The crime mentioned in Art. 153d (of the 2002 Act) and Art. 199 (of the 2013 Bill) is of individual character – the subject of the crime is defined. The good protected in these articles is the activity of individual entities, including **journalists**. Clandestine collaboration with a journalist may in practice turn into the enlistment of journalists to cooperate as "intelligence agents" for the benefit of the *Internal Security Agency*/*Foreign Intelligence Agency.*

It is also worth noting that in the 2013 Bill, the Polish legislator extends the scope of possible collaboration – the obligation to collaborate, as defined in the existing regulations, essentially used to exist on paper only. The 2013 Bill includes regulations concerned with the collaboration obligation incumbent on government officials and entrepreneurs who "conduct activity of public utility."

* * *

More often than not, information security is analyzed on account of State security. Because it is the State that is in possession of knowledge that is amassed with the aid of special instruments and entitlements. This comes to be reflected in the operation of special services, for whom any occurrence that might constitute a threat to internal or external security, and the constitutional order falls within the scope of interest. Of special significance for the operation of special services is the information which is classified; in the case of Poland this issue is regulated by the *Classified Information Protection Act* as well as acts that govern the operation of individual special services.

The issue of classified information protection has not been the subject matter under consideration in the present article. The article, for that matter, focuses on specific legal solutions which came within the purview of the 24 May 2002 *Act on the Internal Security Agency and Foreign Intelligence Agency*, as well as the 1 August 2013 *Bill of the Internal Security Agency*. In the analysis, only the problem of the relations between the ABW officers and journalists comes under close scrutiny. Hence, the text does not touch upon all the aspects of collaboration or exertion of influence on persons holding public offices or offices of similar nature (for more on this see Art. 37 of the 2002 Act and Art. 26 of the 2013 Bill).

It must be pointed out that the changes which were proposed by the Polish legislator in 2006, and which are reflected in the Act on ABW and AW (Chapter 10a), and which in essence recur in the ABW Bill (Chapter 10), are intended to eliminate the use of special services for current politics. They were also intended to diminish the influence exerted by officers upon political, public and economic life on the mere grounds of being in possession of information that is valuable on account of the way it is acquired. Much too often the public opinion gained access – with the aid of mass media – to classified information. In order to put an end to all kinds of collaboration and the undesirable "transfer" of information – for the sake of the reason of the State – a solution that was resorted to was the one which curbed possibilities for clandestine collaboration with journalists, as well as a possibility of employing information acquired while fulfilling or in connection with official duties performed by the *Internal Security Agency* officers in order to affect the operation of public authority bodies, entrepreneurs or broadcasters, editors-in-chief, **journalists** and persons conducting publishing activity. The official intent was transparency of the workings of the public sphere, and yet it must be noted that it was thanks to the so-called "leaks" from special services that the general public was able to learn about politicians' illegitimate actions. With these regulations in effect, the officer-journalist "game" appears to be quite "costly" on account of criminal liability.

Bibliography

Act of 6 June 1997 – Penal Code, Official Journal 1997, No. 88, Item 553 as amended.

Act of 26 January 1984 – Press Law, Official Journal 1984, No. 5, Item 24 as amended.

Act of 24 May 2002 on the Internal Security Agency and Foreign Intelligence Agency, Official Journal 2002, No. 74, Item 676 as amended.

Act of 6 September 2001 on Access to Public Information, Official Journal 2001, No. 112, Item 1198 as amended.

Act of 29 August 1997 on Personal Data Protection, Official Journal 1997, No. 133, Item 883 as amended.

Act of 5 August 2010 on Classified Information Protection, Official Journal 2010, No. 182, Item 1228 as amended.

Act of 29 December 1992 on Radio and Television Broadcasting, Official Journal 1993, No. 7, Item 34 as amended.

Aleksandrowicz T. R. (2002), *Komentarz do ustawy o dostępie do informacji publicznej*, Wrocław.

Assange J. (2013), *How cryptography is a key weapon in the fight against empire states*, "The Guardian", 9 July 2013.

Assange J., Appelbaum J., Muller-Maguhn A., Zimmermann J. (2012), *Cypherpunks: Freedom and the Future of the Internet*, New York.

Bill of the Internal Security Agency of 1 August 2013.

Czaputowicz J. (2012), *Bezpieczeństwo międzynarodowe. Współczesne koncepcje*, Warszawa.

Dobosz I. (2006), *Prawo prasowe. Podręcznik*, Warszawa.

Ferenc-Szydełko E. (2008), *Prawo prasowe. Komentarz*, Warszawa.

Foucault M.(1975), *Surveiller et punir: Naissance de la prison*, Paris.

Herer M. (2012), *Filozofia aktualności*, Warszawa.

Jabłoński M., Wygoda K. (2002), *Ustawa o dostępie do informacji publicznej. Komentarz*, Wrocław.

Jordan T.(2008), *Hacking. Digital Media and Technological Determinism*, Cambridge.

Koziej S. (2011), *Triada globalnych zagrożeń asymetrycznych: konsekwencja proliferacji terroryzmu, broni nuklearnej i technologii rakietowych*, "Bezpieczeństwo Narodowe", No. 19.

The Julian Assange Show: Cypherpunks (2012), broadcast by the Russian TV station Russia Today (RT) in 2012.

Liedel K. (2005), *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń.

Lobbing na rzecz Rosjan? Bielecki odpiera ataki, a PiS chce komisji śledczej (2013), "Dziennik Gazeta Prawna" 13.05.2013, http://wiadomosci.dziennik.pl/polityka/artykuly/427439,lobbing-na-rzecz-rosjan-bielecki-odpiera-ataki-a-pis-chce-komisji-sledczej.html (access: 18.08.2013).

Madej M. (2007), *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, PISM, Warszawa.

Mathiesen T. (1997), *The Viewer Society: Michel Foucault's 'Panopticon' Revisited*, "Theoretical Criminology", Vol. 1, No. 2.

Rosicki R. (2010), *O pojęciu i istocie bezpieczeństwa*, "Przegląd Politologiczny", No. 3.

Sobczak J. (2008), *Prawo prasowe. Komentarz*, Warszawa.

Sobczak J. (1993), *Polskie prawo prasowe*, Poznań.

Taradejna M., Taradejna R. (2003), *Dostęp do informacji publicznej, a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego*, Toruń.

Zięba R. (2008), *Pozimnowojenny paradygmat bezpieczeństwa międzynarodowego*, in: *Bezpieczeństwo międzynarodowe po zimnej wojnie*, (ed.) R. Zięba, Warszawa.

Węgrzecki J. (2011), *Wpływ, autorytet, dominacja. Teorie władzy i ich struktura*, Warszawa.

Wroński P. (2013), *Wojna generałów. Generał Nosek musi odejść, bo prześwietlił wydatki wiceministra?*, "Gazeta Wyborcza", 24.11.2013, http://wyborcza.pl/2029020,75478,14664625.html (access: 25.11.2013).

ABSTRACT

The text addresses the issue of information security as exemplified by clandestine collaboration and the influence exerted by the *Internal Security Agency* officers upon journalists. The texts analyzes the *de lege lata* regulations as well as the *de lege ferenda* ones. As for the former, the penal provisions of the Act, that is Articles 153b–153d (Chapter 10a) are applicable, whereas as for the latter, the applicable regulations are the 2013 Bill Articles numbered 197–199 (Chapter 10). In both the 2002 *Act on the Internal Security Agency and Foreign Intelligence Agency* as well as in the 2013 draft *Bill of the Internal Security Agency*, the legislator penalizes the employment by the officers of the information acquired while fulfilling or in connection with official duties for the purpose of affecting the operation of public authority bodies, entrepreneurs or broadcasters, editors-in-chief, journalists and persons conducting publishing activity. Also, the text analyzes regulations concerned with the penalization of clandestine collaboration engaged in by ABW officers with a broadcaster, editor-in-chief, a journalist and a person conducting publishing activity.

BEZPIECZEŃSTWO INFORMACJI NA PRZYKŁADZIE TAJNEJ WSPÓŁPRACY I WYWIERANIA WPŁYWU PRZEZ FUNKCJONARIUSZY AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO NA DZIENNIKARZY – PRZEPISY *DE LEGE LATA* I *DE LEGE FERENDA*

STRESZCZENIE

Tekst podejmuje problematykę bezpieczeństwa informacji na przykładzie tajnej współpracy i wywierania wpływu przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego na dziennikarzy. W tekście analizowane będą przepisy *de lege lata* (Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu) i *de lege ferenda* (Projekt ustawy o Agencji Bezpieczeństwa Wewnętrznego z 1 sierpnia 2013 r.). W pierwszym przypadku znaczenie mają przepisy karne ustawy, czyli art. 153b–153d (Rozdział 10a), natomiast w drugim przypadku adekwatne regulacje od art. 197 do art. 199 Projektu z 2013 r. (Rozdział 10). Zarówno w *Ustawie o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu* z 2002 r., jak i w projekcie ustawy o ABW z 2013 r. ustawodawca penalizuje wykorzystanie przez funkcjonariuszy informacji uzyskanych podczas lub w związku z pełnieniem obowiązków służbowych do wpływania na działalność organów władzy publicznej, przedsiębiorców lub nadawców, redaktorów naczelnych, dziennikarzy i osób prowadzących działalność wydawniczą. W tekście analizowane są również regulacje dotyczące penalizacji tajnej współpracy funkcjonariuszy ABW z nadawcą, redaktorem naczelnym, dziennikarzem i osobą prowadzącą działalność wydawniczą.