POLISH LAW ON RIGHT TO INFORMATION AND CLASSIFICATION

Adam Bodnar[1]
Irmina Pacho[2]

Helsinki Foundation for Human Rights, Poland
May 2011

I. Introduction

The Polish classification regime is currently undergoing significant changes and transformations. In January 2011 a new legal act came into force bringing an entirely new system of classification. Such a radical amendment derived from an assumption that the previous law was out-of-date, not adapted to the modern technology and did not comply with current problems of classification. The first twelve months after the new act became binding, it will be a time of transformation. Within this time limit authorities are obliged to introduce executive orders outlining the execution and implementation of the new law completed. Until that moment some of the former classification system's regulations will still be applicable. Therefore, it is yet too early to determine the consequences of introducing the new classification system, since the effectiveness will have to be verified by future practice. The aim of this paper is to highlight the most important shifts in the law, problems that appeared under previous regulations, as well as the main areas of concern, uncertainty and challenges remaining under the new act.

II. Outline of current relevant legal regimes, including significant shifts

1. National legal authority for right to information

Among the rights guaranteed in a democratic country is the right to have access to information on the activities of state bodies. The right to information is perceived as having fundamental value, since it enables citizens to participate in public life and, thus, empowers democracy. It also guarantees transparency and public control over organs of public authority.[3]

In Poland the right to public information is established in the Constitution.[4] Article 61(1) of the Constitution states, "*A citizen shall have the right to obtain information on the activities of*

---

[1] Adam Bodnar is the secretary of the Board and head of the legal division of the Helsinki Foundation for Human Rights, Warsaw. He is also an associate professor in the Human Rights Chair of the Faculty of Law, Warsaw University. E-mail: a.bodnar@hfhr.org.pl.

[2] Irmina Pacho is the head of the Observatory of the CIA Activities in the Territory of Poland, a program operated by the Helsinki Foundation for Human Rights, Warsaw. She is also participant of the doctoral studies in the Institute of Legal Sciences of the Polish Academy of Sciences. E-mail: i.pacho@hfhr.org.pl.

[3] In Poland the rule was broadly expressed by the judiciary and the doctrine of law. See, *inter alia*, judgment of the Supreme Administrative Court of 11.04.2005, ref. no. I OPS 1/05; J. Zaleśny „*Dostęp do informacji niejawnych w sferze spraw publicznych*" (Access to classified information in public affairs; authors' translation) [in]: „*Obywatelskie prawo do informacji"* (Citizens' right to information; authors' translation), Ed. T. Gardocka, Warsaw 2008, p. 41.

[4] The Constitution of the Republic of Poland (*Konstytucja Rzeczypospolitej Polskiej;* authors' translation*)*, 2.04.1997, the Journal of Laws no. 78, sec. 483.

organs of public authority as well as persons holding public functions. Such right shall also include receipt of information on the activities of self-governing economic or professional organs and other persons or organizational units relating to the field in which they perform the duties of public authorities and manage communal assets or property of the State Treasury."[5] Article 61(2) provides further, "*The right to obtain information shall ensure access to documents and entry to sittings of collective organs of public authority formed by universal elections, with the opportunity to make sound and visual recordings."*[6]

Further, the Freedom of Information Act (hereinafter "FOIA") expounds on the right set out in Article 61 Constitution.[7] First, FOIA clarifies the definition of public information – stating that any reference to public affairs constitutes public information[8] and providing a non-exhaustive index of categories of public information.[9] Second, FOIA states that, as a general rule, anyone has the right to immediately obtain public information including current data regarding public issues, without any requirement that the requester prove a legal or non-legal interest.[10] Third, FOIA provides that citizens, foreigners, stateless persons, legal persons and organizations without legal personality all have the right to information. Lastly, FOIA imposes an explicit obligation on the specified state authorities to disclose information.[11]

2. National security regime

The Constitution states that restrictions on the right to information "*may be imposed by statute solely to protect freedoms and rights of other persons and economic subjects, public order, security or important economic interests of the State".*[12] According to the FOIA, access to public information might be limited due to the need to protect classified information[13]. Open public information is the rule, and restrictions are the exception. As such, exceptions must be explicitly defined, narrowly applied and consistent with the general principle of access to information.[14]

The Protection of Classified Information Act of 5 August 2010, (hereinafter "PCIA 2010") came into force on January 2, 2011[15] replacing the prior law, the Protection of Classified Information Act of 22 January 1999 (hereinafter "PCIA 1999")[16]. It also supplements other

---

5 Authors' translation.

6 Authors' translation.

7 *Ustawa o dostępie do informacji publicznej* (Freedom of Information Act; authors' translation), 6.09.2001, the Journal of Laws no.112, sec. 1198.

8 FOIA Art. 1.

9 FOIA Art. 6.

10 FOIA Arts. 2, 3.

11 FOIA Art. 4 (defining state authorities as organs performing public tasks). Constitutional Court in the judgment of 20.03.2006, ref. no. K 17/2005, characterized the obligation of state bodies as a direct result of the constitutional right to information.

12 Constitution Art. 61(3).

13 FOIA Art. 5(1). Apart from FOIA, some other laws regulate access to public information and introduce secrecy provisions including, for instance, information regarding national records and archives [*Ustawa o narodowym zasobie archiwalnym i archiwach* (Law on National Resources and Archives; authors' translation), 14.07.1983, Journal of Law no. 38, sec. 173], meetings of the Council of Ministers [*Ustawa o Radzie Ministrów* (Law on Council of Ministers; authors' translation), 8.08.1996, Journal of Laws of 2003, no. 24, sec. 199], and functioning of Sejm and Senate [Constitution Art. 61(4)].

14 Judgment of the Supreme Administrative Court, 2.07.2003, ref. no. II SA 837/03.

15 *Ustawa o ochronie informacji niejawnych* (Protection of classified information Act; authors' translation), 5.08.2010. Journal of Laws no. 182, sec. 1228.

16 *Ustawa o ochronie informacji niejawnych* (Protection of Classified Information Act; authors' translation), 22.01.1999, Journal of Law no. 11 sec. 95 with further amendments.

legal authorities, including bilateral international agreements on the mutual protection of classified information concluded by various countries[17] and NATO agreements on the protection of information (6 March 1997)[18] and cooperation in the field of atomic information (18 June 1964)[19].

The previous PCIA 1999 created the modern, legal system of classifying documents in Poland. However, after several years, during which it was amended 23 times, the law did not address current problems in the Polish classification regime. In general, the provisions of the PCIA 1999 were not clear, flexible, or functional. They did not provide with sufficient control mechanisms. Nor were they adapted to the possibilities of modern technology[20]. Moreover, the law was not consistent with NATO and European Union standards. This is important because Poland, as a member state of these organizations, participates in the exchange of information within their structures.

This was becoming very important and problematic especially in the light of the Polish presidency of the Council of the European Union due to commence July 1, 2011, and had the Polish government to introduce PCIA 2010. According to given reasoning, the aim of the bill was to update the law and to regulate effectively and comprehensively the protection of classified information in both the domestic and international sphere. PCIA 2010 is also to provide greater simplicity and flexibility in the provisions than PCIA 1999[21].

The classification law required very far-reaching reforms, and so the new legal act brings significant changes and introduces an entirely new system of classification in Poland. PCIA 2010 eliminates the previously existing division between a state secret and professional secrets. This means, first, that the law no longer protects information of citizens' and organizational units' interests, but only information whose unauthorized disclosure would be detrimental to the State's interests. Further, PCIA 2010 provides radical changes in defining classified information by removing specific categories of mandatory classification and replacing them with a malleable standard of the extent of damage to State's interests. Unlike PCIA 1999, the new law abandons the strict protection of circulation and transmission of "restricted" information.

---

17 Agreements concluded with Albania, Bulgaria, Croatia, Czech Republic, Estonia, Finland, France, Spain, Latvia, Norway, Germany, Russia, Romania, Slovakia, Switzerland. Ukraine, USA, United Kingdom of Great Britain and Northern Ireland and Italy. For instance: *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o wzajemnej ochronie informacji niejawnych* (available at http://isap.sejm.gov.pl/Download?id=WDU20071400985&type=2), *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Słowackiej o wzajemnej ochronie informacji niejawnych* (available at http://isap.sejm.gov.pl/Download?id=WDU20041171214&type=2), *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Łotewskiej o wzajemnej ochronie informacji niejawnych* (available at http://isap.sejm.gov.pl/Download?id=WDU20042212242&type=2).

18 *Umową między Stronami Traktatu Północnoatlantyckiego o ochronie informacji* prepared on 6 March 1997 in Brussels; ratified by Poland on 29.12.1999, the Journal of Laws no. 64, sec. 740; available at: http://isap.sejm.gov.pl/DetailsServlet?id=WDU20000640740.

19 *Umową między Stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych*, prepared in Paris on 18 June 1964, ratified by Poland on 16 March 2000, the Journal of Laws no. 143 sec. 1594; available at: http://isap.sejm.gov.pl/Download?id=WDU20011431594&type=2.

20 *Uzasadnienie do projektu ustawy o ochronie informacji niejawnych* (Reasons for the Project of the Protection of Classified Information Act, Governmental project; authors' translation), available at http://orka.sejm.gov.pl/Druki6ka.nsf/0/FF855CD20A1ABBCFC12576CE004227EE/$file/2791-uzasadnienie.doc.

21 *Ibidem.*

Another significant amendment is the change in the declassification system. Automatic declassification is removed and is replaced by non-automatic declassification based on a five-year review. The new law also introduces 'risk assessment' in terms of recordkeeping of classification activity which is a rational use system of physical security measures based on a threat estimate of unauthorized access or loss of classified records. PCIA 2010 also broadens training requirements for all persons dealing with classified information and enhances administrative review procedures.

3. Criminal Code – relevant provisions

According to art. 265 (1) of the Polish Criminal Code, whoever discloses or uses information classified as secret or top secret in violation of law shall be subject to the penalty of a deprivation of liberty for a term of 3 months to 5 years. If the information is disclosed to a person acting for or on behalf of a foreign entity, the perpetrator shall be subject to the penalty of a deprivation of liberty for a term of 6 months to 8 years[22]. A person who discloses information classified as secret or top secret, which became known to him or her while performing a public function or as a result of an authorization, shall be subject to a pecuniary penalty, a penalty of a restriction of liberty or the penalty of a deprivation of liberty for up to one year.

In order for an action to be punishable it must cause an effect – e.g. disclosing information to at least one, not authorized person orally, by giving access to a document or any other classified as secret object is punishable when the person actually becomes familiar with its meaning. Neither repeating nor passing secret information to others qualifies as disclosing a state secret if the information has been already disclosed, especially in the media or is commonly known or anyone can easily learn about it[23]. "Disclosing" by sign, gesture or mimics could not be punishable[24].

Under commentary of Article 265(1), the use of the information in any activity, especially public, economic or scientific (e.g. in publications, research, business negotiations with a foreign partner) qualifies as an unauthorized use[25]. However, it is not a crime to disclose information if it occurs within the limits of the rights and duties of the person who discloses the information[26]. The judgment of the Supreme Court of 26 March 2009, I KZP 35/08, states that an offense under Article 265(1) may be committed by any person who became familiar with the classified information or by whom the information was confined. Thus, it is a universal crime; it is not limited to persons who have an access certificate for classified information. However, this is not a binding interpretation and is broadly criticised[27].

Disclosing information classified as a state secret to a person acting for or on behalf of a foreign entity is an aggravated offense under Article 265(2). It may take the form of cooperating with foreign intelligence; however the nature of the foreign institution and the

---

22 Criminal Code Art. 265 (2).

23 See A. Marek, *Kodeks karny. Komentarz* (Crimial Code. Commentary; authors' translation), LEX, 2010, 5th edition; B. Kunicka-Michalska *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości* (Crimes against protection of information and justice system; authors' translation), C.H. Beck 2000, p. 391.

24 Judgment of Polish Supreme Court, 17.03.1971, ref. no. III KR 260/70.

25 A. Marek, *Kodeks karny. Komentarz.*

26 Judgment of Polish Supreme Court, 8.03.2007, ref. no. I KZP 30/06.

27 The universal nature of the crime is highly criticized. See section IV.2.

awareness of the perpetrator are the decisive factors[28]. Two types of the offence can be committed with either direct or conceivable intent.

Moreover, art. 265(3) Criminal Code provides for the prosecution of non-intentional disclosure, i.e. reckless or negligent disclosure of state secrets. However, the wording of the provision indicate that this provision can only be applied as a *delicta propria* where the subject of the offense is a person holding classification authority.

III. Application of national security secrecy and freedom of information in Poland

1. Procedures for classifying and declassifying

1.1. Classification levels

PCIA 2010 redefines classified information, removing categories of mandatory classification as discussed above.

Classified information can be marked at one of four levels[29]: in descending order, "top secret", "secret", "confidential" and "restricted". Information is classified at a level based on the harm that unlawful disclosure would cause: "top secret" causes an "exceptionally grave harm" to the state's legal interests; "secret" causes "grave harm"; "confidential" causes "harm"; and "restricted" causes a deleterious effect on the ability of public organs or public organizational units to perform their duties.

PCIA 2010 calls for "top secret" classification when unauthorized disclosure may lead to "exceptionally serious harm" because it would a) threaten the independence, sovereignty or territorial integrity of Poland, b) threaten the internal safety or constitutional order of Poland, c) threaten foreign relations or activities of Poland, d) weaken Polish defense ability, or e) lead to the identification of intelligence officers or endanger their lives or the lives of a protected identity witness[30]. Information classified as "secret" may cause "serious harm" to Poland, in that it a) prevents the performance of tasks connected to the protection of the sovereignty or constitutional order of Poland, b) leads to the deterioration of relations between Poland and other countries or international organizations, c) disturbs the functioning of military forces, d) hinders the functioning of services for national safety or prosecution of perpetrators of crimes, e) disturbs the functioning of prosecution agencies or justice system, or f) leads to grave losses in the economic interests of Poland[31].

"Confidential" information's disclosure must "harm" an interest of Poland; as such it must a) hinder the conduct of foreign affairs of Poland, b) hinder the fulfillment of defensive projects or have a negative influence on the military ability of Poland, c) disturb public order or citizen safety, d) hamper the functioning of services and institutions aiming to protect national safety, the fundamental interests of Poland, public safety, citizen safety, or prosecution agencies and justice, or e) threaten financial stability or negatively influence the national economy[32]. Information is classified as "restricted" when it is not classified at higher level, but its unauthorized disclosure can lead to a deleterious effect on the functioning of public

28 A. Marek, *Kodeks karny. Komentarz.*
29 PCIA 2010 Art. 5.
30 PCIA 2010 Art. 5(1).
31 PCIA 2010 Art. 5(2).
32 PCIA 2010 Art. 5(3).

authorities or other organizational units fulfilling obligations regarding national defense, foreign affairs, public safety, justice or economic interests and abiding of rights and freedoms of citizens[33].

The law says that classified information from international organizations or other states under international agreements must be marked with an appropriate classification level in Polish law[34]. This means that such information must be classified in the above-mentioned definition that corresponds to the level of security granted by the international organizations or other states.

1.2. Classification process

In order to possess authority to classify information, a person is obliged to meet three criteria. First, the individual must be the person who is entitled to sign the document or who created the information[35]. Second, the person must have the authority to access classified information as demonstrated by security clearance and special training. Third, the competence to classify, declassify or change the level of classification is strictly determined by the level of classification to which a person has security clearance. For instance, a person holding "confidential" level security clearance cannot classify information at a higher level than "confidential."[36]

Moreover, PCIA 2010 allows for the demarcation of different parts of a single document with different classification levels allowing for partial disclosure[37]. PCIA 1999 had a similar provision; however, in practice it did not work properly.[38]

An issue has arisen regarding the classification of documents prepared by an identity-protected witness, i.e. individuals who are criminal suspects granted protection by the state because they have agreed to testify against members of criminal gangs or other serious

---

33 PCIA 2010 Art. 5(4).

34 PCIA 2010 Art. 5(5).

35 PCIA 2010 Art. 6(1).

36 S. Hoc „*Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych",* Opole 2006, p. 68.

37 PCIA 2010 Art. 6(8).

38 See *Opinia Helsińskiej Fundacji Praw Człowieka o projekcie ustawy o ochronie informacji niejawnych (wersja robocza z dnia 15 lipca 2009 roku* [Opinion of the Helsinki Foundation for Human Rights (hereinafter "HFHR") on the Project of the Protection of Classified Information Act; author's translation], 26.08.2009, available at http://www.hfhrpol.waw.pl/precedens/images/stories/opinia_niejawne.pdf. An example of the practical difficulties can be seen in the decision of 30 April 2009 of the Head of Central Anticorruption Bureau (hereinafter: "CBA"; decision is available at: http://www.hfhrpol.waw.pl/precedens/images/stories/cba_odpowiedz_1.pdf) not to provide public information concerning the statistical data on the application of 'operational control' used by CBA in response to an HFHR freedom of information request. Operational control, in the meaning of *Ustawa o Centralnym Biurze Antykorupcyjnym* (Central Anticorruption Bureau Act; authors' translation), 9.06.2006, the Journal of Law no. 104 sec. 708 with further amendments CBA Act (CBA Act of 9.06.2009, The Journal of Law no. 104, sec. 708 with amendments) is defined as, *inter alia*, application of technical means that enable security forces secretly obtain information and evidence, in particular, the content of telephone conversations and other information transmitted via IT networks (CBA Act Art. 14(1)(6)). The CBA decision was justified under PCIA 1999, as operational control data was protected due to the security of Poland. Further, statistics are included in a special document containing operational control records. Since the document is entirely classified and the statistical information is an integral part, a statistic cannot be physically separated from the whole document without violating the law on classification. According to the Head of CBA, FOIA in such a case is not applicable.

criminals.[39] Documents of an identity-protected witness, such as a motion or other request, that touch upon serious state interests might need classification. Under Polish law these criminals do not fall within the scope of individuals having authority to classify and are not granted any additional power to classify documents. The issue is not yet settled in Polish law. To solve this issue some analysts have suggested that police authorities who receive a document should have the authority to classify it when it properly needs classification.[40]

It is important that the classification of information does not result from an administrative process. Further, the law requires no justification for classification. Likewise, there is no external control at the time of classification. These three factors lead to serious problems in judicial oversight and identifying executive overreach of the classification authority[41].

1.3. Access to classified information

1.3.a. Prerequisites to have access to classified information

In general, classified information is protected according to the applicable law on the protection of classified information, namely PCIA 2010. This means that such information might be disclosed only to a person authorized by the law to access classified data of a certain classification level. Second, information must be created, processed and stored in conditions preventing its unlawful disclosure and within compliance with the law, including the law concerning the standards of the organization of secret chancelleries and other measurers of physical protection corresponding with a certain level of classification. Third, such information must be protected accordingly to the level of classification of the information[42].

In reference to the first prerequisite, PCIA 2010 enumerates two standards that are necessary to be met by an individual in order to see classified information[43]. First, access to national security secrecy might be given to a person when access is necessary to hold an office or to perform a public service or delegated work connected to the classified information. Second, a person must guarantee the proper protection of classified data. Therefore, to view "confidential", "secret" and "top secret" information it is necessary to obtain the appropriate security clearance[44] and to undergo proper training relating to the protection of national security information[45].

Article 1(2) PCIA 2010 catalogues in general terms the state entities that are bound by the law on protection of classified information, meaning handling classified data, classifying, and declassifying information. However, there is no official document enumerating with greater specificity the names of particular government agencies subject to this regime. Public authorities included under the regime are expected to perform tasks strictly connected with

---

39 Protected identity witness program is regulated by the *Ustawa o świadku koronnym* (Identity- Protected Witness Act; author's translation) of 25.06.1997, the Journal of Laws no. 26 sec. 232 with amendments.

40 M. Szczawiński „*Uprawnienie do nadania klauzuli tajności dokumentowi sporządzonemu przez osobę objętą ochroną świadka koronnego*"(Powers to classify a document prepared by protected identity fitness; author's translation), Biuletyn Prawny Komendy Głównej Policji no. 34, p. 10-11.

41 See section III. 1.6.2.b. and IV.4.

42 The prerequisites are stipulated in PCIA 2010 Art. 8.

43 PCIA 2010 Art. 4(1).

44 PCIA 2010 Art. 21(1).

45 PCIA 2010 Art. 19.

national security information requiring classification.[46] In practice, according to an expert on classified information, Stanisław Zarodkiewicz,

> within the branch agency, the head of the agency is responsible for providing a list of posts which are connected to classified information and require security clearance. It is usually a security officer of particular unit that prepares such a list which is subsequently approved by the head of the agency.[47]

Apart from government entities, PCIA 2010 (chapter 9) extends the national security classification regime to contractors with the Polish state, who perform contracts or other tasks that involve dealing with classified information. Each contractor is obliged to undergo a background check prior to obtaining security clearance.[48]

There are, however, officials in certain posts who are granted access to classified information automatically, without the need to obtain security clearance. These are the President, Prime Minster, and Members of the Council of Ministers in most cases. Furthermore, all Polish parliamentarians (i.e., members of the Sejm and the Senate) are exempted from the background check to view classified materials[49]. However, security clearance is required for parliamentarians to access "top secret" documents[50] and information of international organizations or records that are derived from Polish international agreements.[51] PCIA 2010 Article 34(10)(15) also exempts most judges' and prosecutors' procedures from security clearance.[52]

When government officials leave office their access to classified information is excluded. However, there are no procedures in PCIA 2010 that directly regulate the nondisclosure obligations of former government agents. Neither is there a practice to conclude nondisclosure agreements with former officials.[53] However, the analysis of the law on classified information

---

46 S. Hoc „*Ochrona informacji niejawnych…",* p. 35.

47 Interview on 8.10.2010 with Stanisław Zarodkiewicz– President of the *Ogólnopolskie Stowarzyszenie Menedżerów Bezpieczeństwa* "*Clausula Securitatis*" (Polish Association of Security Managers "Clausula Securitatis"; author's translation) gathering experts of the areas of protection of, *inter alia*, classified information, business secrecy, official secrecy or protection of personal data. Website: http://clausec.com. Note: the obligation to designate professionals, which require security clearance, is regulated by acts regarding particular agencies, i.a., art. 116(3) *Ustawa o Agencji Bezpieczeństwa Wewnętrznego* (Internal Security Agency Act; authors' translation), 24.05.2002, the Journal of Laws no. 74, sec. 676 with further amendments; Art. 27 CBA Act.

48 In a shift from PCIA 1999 Art. 1(2)(5), PCIA 2010 Art. 1(2)(6) restricts the scope of government contractors eligible for security clearance to exclude those engaged in scientific and research pursuits. Taking into consideration the range of activities that these units might deal with, this limitation may be perceived as a serious loophole.

49 PCIA 2010 Art. 34(10).

50 PCIA 2010 Art. 34(12). This obligation refers mostly to the members of the Parliamentary Commission on Secret Services.

51 PCIA 2010 Art. 34(11).

52 Judges of the civil courts, military courts, Supreme Court, administrative courts, Supreme Administrative Court, Constitutional Tribunal and Tribunal of the State, lay judges of the civil and military court, and prosecutors are exempt from security clearance requirements. Under PCIA 1999 a question arose concerning the issue whether judges should be subjected to the background check process under the law on protection of classified information. This problem was a source of many legal debates and controversies. Finally, the Supreme Court delivered a judgment of 28 September 2000, ref. no.III ZP 21/00, stating that under the respective law no provisions are stipulated that judges are obliged to undergo the background check process.

53 Interview on 24.09.2010 with Mr. Piotr Niemczyk– Polish politician, former undersecretary of state in Ministry of Economy, former Director of the Analyze and Information Office (*Biuro Analiz i Informacji*;

leads to a conclusion that a person remains under an obligation to protect classified information as long as it has the status of classified information.

1.3.b. Characteristics of background check proceedings

In a shift from PCIA 1999, according to PCIA 2010 the background check can be normal or extended[54], depending on the type of classified information that the person is going to deal with or the office that the individual is going to hold.[55] Further, PCIA 2010, like PCIA 1999, also provides for a control background check when new information undermining the individual's ability to hold state secrets appears. If irregularities are found, the security clearance might be withdrawn[56].

Practical guidelines for the control background check are included in the instruction of the Internal Security Agency (which is responsible for the check, hereinafter: "ABW").[57] It states that the procedure might be initiated in 3 situations: if improper handling of classified information (negligent behavior, leading to a real threat of disclosing information to unauthorized individuals) is discovered, if an official is charged and convicted for an offense or if the authorities receive untrue information during the background check.

In case of denying security clearance or withdrawing security clearance, it is possible to challenge the competent authority's decision[58]. Although lodging a complaint does not prevent the execution of the decision, the authorities are bound by the three-month time limit to consider the motion.

1.4. Declassification process

The definition of "declassification" is inextricably linked to the need to estimate the possible harm to Poland's interests and may be found in various circumstances: declassification of information that does not constitute a national security secret, declassification of data, although it possesses characteristics of classified information, or declassification of information that lost the character of state secrecy.[59]

---

author's translation) and former Deputy Director of the Foreign Intelligence Board (*Zarząd Wywiadu*; author's translation) within the Office of State Protection (*Urząd Ochrony Państwa;* authors' translation), authority subordinated to the Minister of Internal Affairs and further to Prime Minister, expert of the Parliamentary Commission on Secret Services (since 2007); Mr. Piotr Niemczyk runs business activity "Niemczyk i Wspólnicy Sp. z .o.o" providing consultation in the areas concerning security issues and detective services. Website: http://niemczykiwspolnicy.pl.

54 PCIA 2010 Art. 22(1).

55 PCIA 2010 brings significant changes in relation to the background check. It simplifies and clarifies the procedure through, i.e., limiting the check to two types (normal and extended), providing details of the conduct of the procedure, its stay, discontinuance and results of its completion as well as clear division of authorities' competences in the check process (PCIA 2010 Art. 23).

56 PCIA 2010 Art. 33(11). As a result of the control background check process under PCIA 1999, ABW decided on 10.10.2008 to withdraw the security clearance of Antoni Macierewicz having access to "top secret" data at the time of being a Member of Parliament.

57 Brochure "*Postępowanie sprawdzające*" ("Background check", author's translation) prepared by ABW, p. 9-10; available at: http://www.abw.gov.pl/download.php?s=1&id=613.

58 PCIA 2010 Arts. 35(1), 37(1).

59 Judgment of the Constitutional Court, 15.10.2009, ref. no. K 26/08 delivered under PCIA 1999.

PCIA 2010, like PCIA 1999, provides a system of declassification that is controlled by the agency that created the information.[60] According to PCIA 2010 Article 6(3), declassification or changing classifications can only be done after obtaining written consent either from the person who marked the information as classified or from that person's superior. In a situation where information is marked "top secret", it is necessary to obtain the approval of the head of the organizational unit in which the classification originated.

When an agency is subjected to e.g. liquidation or reorganization, declassification and change of the classification level is performed by the legal organizational successor. In a case where there is no legal successor, information is declassified by the national security authority: the Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego*, hereinafter "ABW") or the Military Counterintelligence Service (*Służba Kontrwywiadu Wojskowego,* hereinafter "SKW")[61]. According to Piotr Niemczyk, "In Poland, declassification of certain materials in a situation of e.g. liquidation may appear difficult. It might be thus a part of the political game resulting from the alteration of political forces in power."

An important shift from PCIA 1999 to PCIA 2010 is that the new law does not stipulate a time limit after which data is automatically declassified[62]. Instead, PCIA 2010 provided for the obligatory review of information not less that every five years to check whether the information continues to fulfill the prerequisites to be protected under the classification regime[63]. PCIA 2010 also grants a classifier the competence to identify a date or specific event for declassification or alteration of classification level[64]. The shift abandons a strict time limit and introduces a more flexible system of declassification that is, however, based on the discretion of declassification authority.

In general, information must be declassified eventually; no indefinite classification is permitted. There is, however, one exception[65]: information that leads to the identification of officers, soldiers, or other persons competent on the ground of law to participate in operational activities as well as data that might result in the identification of persons who assisted in operational actions can be withheld indefinitely. The indefinite protection also covers data obtained from international organizations or foreign authorities, if such a provision of protection was a condition for receiving the information[66]. In this respect, PCIA 2010 follows the regulations of PCIA 1999, withholding the possibility of indefinite classification of certain sensitive data. The exception does not, however, cover information

60 In the judgment of 22.02.2007 (ref. V KK 181/06), the Supreme Court confirmed that only officials who classified the information or their superiors have the competence to declassify or to consent for the declassification of information. The PCIA 1999 and PCIA 2010 provisions in this respect are analogous.

61 PCIA 2010 Art. 6(7). In the past few years, there were several significant reorganizations of the secret service in Poland. The State Security Office (*Urząd Ochrony Państwa)* was liquidated on 29 June 2002, and the ABW and Foreign Intelligence Agency (*Agencja Wywiadu*) were created in its place. Furthermore, as a result of the reform of military services on 30 September 2006, the Military Information Service (*Wojskowe Służby Informacyjne*) was replaced by both the Military Counterintelligence Service (*Służba Kontrwywiadu Wojskowego)* and Military Intelligence Service *(Służba Wywiadu Wojskowego).*

62 See section IV.3.2.

63 PCIA 2010 Art. 6(4).

64 PCIA 2010 Art. 6(2).

65 More information in this respect is available IV.3.2.

66 PCIA 2010 Art. 7(1).

regarding the ex-communist regime in Poland being in the possession of the Institute of National Remembrance[67].

1.5. Selected protections for classified information to protect national security

The law on classified information provides various measures to protect classified information and, thus, to protect national security and prevent against abuses. Apart from provisions stipulating who may access classified data, PCIA 2010 also states that classified information must, first, be processed according to its level of classification and, second, in conditions preventing its unauthorized disclosure[68]. Below, we present the most significant protective mechanisms: the so-called physical security measures, namely secret chancelleries where the information is kept, processed and disclosed managed by security officers; proper trainings for classifiers and declassifiers; and measures against abuses including protective measures in the Parliament.

1.5.a. A new approach to recordkeeping on classification activity

Regulations on physical security measures are designed to protect classified information from disclosure to individuals not granted security clearance, foreign secret services or from any form of terrorist attack, sabotage, theft or destruction[69]. The new act introduced a system of rational use of physical security measures, which provides sufficient protection of classified information but at the same time diminishes restrictive measures provided by PCIA 1999. This means that the head of an agency is obliged to perform a risk assessment, i.e., estimating the threat of unauthorized access or loss of classified records. Subsequently, the head of an agency adapts security measures according to the level of risk. This new approach will be executed according to detailed guidelines that will outline technical standards; these guidelines are to be established in a separate executive order of the Council of Ministers[70].

PCIA 2010 requires the establishment of at least one secret chancellery in each branch agency that holds information classified at "secret" and above. The chancellery is a separate unit, managed by a security officer who is responsible for the registry, storing, circulation and issuing of documents to authorized persons[71]. According to PCIA 2010, "confidential" data are held in other protection units[72], but "confidential" or "restricted" information may also be kept by chancelleries[73]. According to experts, *"this approach will soften requirements for organization of chancelleries in agencies which deal exclusively with information classified at a low level. Only "secret" or "top secret" information will meet strict procedure's requirements."*[74] Further, to reduce costs while still providing sufficient protection of classified information, PCIA 2010 allows for one chancellery to guarantee protection of

---

67 PCIA 2010 Art. 7(2). The Institute of National Remembrance - Commission for the Prosecution of Crimes against the Polish Nation (IPN) was established by the Polish Parliament on December 18, 1998. It has been established to, inter alia, prosecute crimes against peace, humanity and war crimes and to compensate for damages suffered by the repressed and harmed people in the communist regime.

68 PCIA 2010 Art. 8(2).

69 PCIA 2010 Art. 45(1).

70 PCIA 2010 Art. 47(1)(2). Within 12 months after PCIA 2010 came into force new execution orders are to be established. Until then execution orders binding under PCIA 1999 remain in force (PCIA 2010 Art. 189(1)).

71 PCIA 2010 Art. 42.

72 PCIA 2010 Art. 43(2).

73 PCIA 2010 Art. 42(5).

74 Interview with Piotr Niemczyk.

multiple branch agencies, with the consent of the national security authority[75]. However, as Stanisław Zarodkiewicz indicated,

> due to the provisions of PCIA 2010, many of the secret chancelleries lose the right to exist. However, it is not possible to predict what will be the practical impact of the new provisions, meaning it is not known whether the existing chancelleries that under the PCIA 2010 would not have been created will be liquidated or not[76].

1.5.b. Broadening training requirements for classifiers/declassifiers

The new PCIA 2010 extends the scope of persons that need to undergo proper training. First, the new law mandates trainings for heads of organizational units, so they learn to adhere to the necessary, updated classification regime and rules of protection. Such training is held by the national security authority in cooperation with security officers[77]. Second, training is required for individuals dealing with all classified data, including those having access to only "restricted" information[78]. Further, trainings have periodical character[79] and need to be conducted not less than every 5 years[80].

1.5.c. Two levels of supervision over the proper protection of national security

PCIA 2010 provides for two levels of the supervision over the classification regime. First, it is conducted by the national security authority (which is ABW and, in military cases, ABW). This includes, *inter alia*, checking the premises of the organizational units, controlling documents relating to the protection of classified information, and demanding clarifications from the heads and employees of branch agencies[81].

Second, supervision is performed at the level of the branch agency by the head of the entity and, in particular, the security officer that is responsible for abiding by the law on the protection of classified data within the agency.[82] The latter one inspects violations of the classification regime, informs the appropriate authorities about the misconduct (head of the organizational unit and national security authority) and finally undertakes actions necessary to limit any negative consequences. Every branch agency establishes its own internal, classified information security policy that stipulates the rules, methods and measures of protection of information. Internal security policy also indicates that the rule ISO/IEC 17799 of the International Organization for Standardization might be especially useful for performing the

---

75 PCIA 2010 Art. 42(3). Interview with Stanisław Zarodkiewicz ("On the grounds of PCIA 1999, there were cases that secret chancelleries were created in order to provide protection to a single classified document that was in a possession of local government's agency. Under PCIA 2010, such a situation would be eliminated, since secret chancelleries in a small organizational units will not be created.").

76 Interview with Stanisław Zarodkiewicz.

77 PCIA 2010 Art. 19(2)(2).

78 PCIA 2010Art. 19(2).

79 PCIA 2010 Art. 19(4). However, as it is stated in the Reasoning for Project of PCIA 2010, a time period of 5 years is relatively long, especially in case of officials who do not deal with classified information in the course of their daily work.

80 Interview with Piotr Niemczyk ("The amendment of training requirements aims at raising qualifications of officials. Therefore, it might have a significant impact at elimination of possible violations in respect of classification and declassification of national security secrecy information.").

81 PCIA 2010 Art. 12.

82 PCIA 2010 Arts. 14(1),(2), 15. PCIA 2010 does not impose on these persons any liability for infringements committed by individual officials.

control. It determines, for instance, the definition of "risk assessment", which is new in the Polish classification regime and might benefit from conducting the security audit.[83]

1.5.d. Access to classified information in Parliamentarian proceedings closed to the general public to protect national security

National security is protected within the Parliament by restricting access to both parliamentarians without special security clearance and the general public. Polish parliamentarians may deal with all classified information, with one exception: to view "top secret" information they need to obtain a security clearance. The practice shows that "*it is rare that Parliament deals with "top secret" data. Model issues that might arise in Parliament are usually not classified at the level higher than "secret". The practice is that when a commission must consider "top secret" data, those parliamentarians who do not possess respective security clearance are obliged to leave the hearing".*[84] However, there is a risk that the system might be seriously undermined; e.g. according to the information provided by the Chancellery of the Sejm (lower chamber), parliamentarian authorities do not know the exact number of current Parliamentarians having "top secret" security clearance.[85]

Furthermore, to protect national security, general public access to Sejm hearings might be restricted. This can relate to sessions of a particular parliamentary commission[86] or of the entire chamber[87]. For instance, proceedings of the Commission on Secret Service are always secret and closed to the general public. Only press releases regarding the course of the sittings might be published, which still need prior approval from the respective ministers and heads of services[88]. This necessary precaution results from the scope of the issues dealt with by the Commission, which is, *inter alia*, financing and functioning of secret services, giving opinions on candidates for head of the services or their possible law violations, and the possibility of classifying documents as "top secret"[89].

1.6. Challenges to classification to protect access to information

1.6.1. Internal challenges

PCIA 2010 gives a procedure to challenge improper classification by the classified authority. PCIA 2010 introduces an enhanced, complex procedure aiming at providing more mechanisms for internal review of information asserted as improperly classified to limit such abuses[90]. Proper and meaningful internal review mechanisms serve to limit individual discretion that causes improper manipulation of purported national security secrets. This is obviously crucial for the protection of a state secret since the information should be protected not solely due to the intention of the state official, but because of the need to protect national security and public interest.

---

83 S. Hoc „*Ochrona informacji…*, p. 64-65.

84 Interview with Piotr Niemczyk.

85 Letter of the Chancellery of Sejm of 10.03.2010; the letter was a response to the Helsinki Foundation for Human Rights freedom of information request dated on 2.02.2010 regarding the number of Member of Parliament having "top secret" security clearance, available at: http://www.hfhrpol.waw.pl/precedens/images/stories/file/odp%20kancelaria%20sejmu.pdf.

86 Statute of Sejm Art. 156.

87 Statute of Sejm Art. 174.

88 Statute of Sejm Arts. 139(1), 141(3).

89 Statute of Sejm Art. 141.

90 See: Reasons for the Project PCIA 2010, p.3.

1.6.1.a. Enhanced procedure under PCIA 2010

The aim of the legislature was to introduce provisions guaranteeing that "the new law provides the procedure of challenging the level of classification which is very precise."[91] According to PCIA 2010, the first mechanism to challenge the classification level (whether it is not too high, too low or when information should not have been classified) is that the recipient of the information may claim that the information was wrongfully classified in a motion to the official who classified the information or to his or her superior. In the motion a recipient may demand a change of the classification level[92]. PCIA 2010 allows a further level of appeal and therefore introduces a mechanism of legal repression. If the motion remains unexamined for 30 days or the decision to change the classification level is negative, the recipient of the information may lodge a motion to the national classification authority or the Prime Minister also requiring an unappealable examination within 30 days. However, there are no sanctions detailed and included in the PCIA 2010 for officials' abuses.

The procedure under PCIA 1999 constituted a serious loophole. For instance, PCIA 1999 limited the ability to challenge the classification level to situations of "excessive" misclassification, a vague term. PCIA 2010 does not include the "excessive" limitation and instead refers to all instances of misclassification of information. The need to introduce such an alteration was underlined, inter alia, by legal commentary.[93]

1.6.1.b. Remaining ambiguities

Although serious amendments have been introduced, certain ambiguities remain in the above procedure leading some, including by the Helsinki Foundation for Human Rights (a Polish rights organization, hereinafter "HFHR") and the Sejm Office of Analysis, to conclude that PCIA 2010 does not constitute an effective remedy of reviewing the correctness of classification. First, PCIA 2010 does not specify who is the "recipient of the information" that is granted the exclusive right to question the level of classification. Some have urged that it should even include those refused access to information on secrecy grounds.[94] Second, PCIA 2010 does not guarantee a right to challenge the decision of the Prime Minister or the national security authority before a court. Additionally, an element that might undermine the effectiveness of the procedure to challenge classification decisions is the lack of responsibility and sanction for improper classification of information. Although sanctions may be interpreted from the legal system, this may cause problems in enforcing the law and holding officials responsible for their abuses.[95]

1.6.2. External challenges

---

91 Reasons for the Project PCIA 2010, p. 13.

92 PCIA 2010 Art. 9(1).

93 J. Zaleśny "Dostęp do informacji…", p. 41.

94 The concern is expressed in the opinion of the Helsinki Foundation for Human Rights on the project of the protection of classified information Act, 26.08.2009 and in the opinion of the Sejm Office of Analysis [*Biuro Analiz Analiz Sejmowych]* on the project of the protection of classified information Act, 6.04.2010, available at: http://orka.sejm.gov.pl/rexdomk6.nsf/0/E18F3B1615B6C9D8C12576E3003B09CE/$file/i432-10.rtf.

95 More information about the problem of lack of sanctions for excessive classification available in section IV.3.1.

The right to access to public information is considered a fundamental value in a democratic state respecting the rule of law. It is important that the process of making information secret is conducted in accordance with the law, and therefore, it is crucial to ensure judicial review of categorizing information as classified[96]. However, in Poland, the question has arisen whether abuses in classification might be successfully challenged by the courts at all. Under Polish law, there is lack of clear, unambiguous legal procedure that would regulate the court's powers in this respect. That is why the problem is subjected to a serious ongoing dispute in legal commentary and jurisprudence. Until now, issues such as the grounds of judicial control, the circumstances in which the court might *ex officio* order this procedure and the scope of the court's examination remain unsettled. As a result, court's capacity to combat abuses and to order, *inter alia*, declassification or a change in the classification level is uncertain.

1.6.2.a. The right of public access to information

In the right of access to information procedure, pursuant to FOIA, a person requesting public information does not have to show any legal or factual interest[97]. The only restriction relates to the right to obtain "processed information", whose disclosure requires additional efforts of the authorities (for instance, preparation of some comprehensive, detailed compilations of data) and of the individual; the individual who seeks to obtain such a data must demonstrate that it is highly important for the public interest[98]. If the authorities refuse to publish information upon public request due to the classified nature of the information, they are required to provide a written decision denying the request[99] together with a basic justification for the non-disclosure[100]. It is indicated that authorities should identify what type of information is protected and on what grounds[101]. In practice, however, the government justification might exclusively state that information cannot be disclosed because it is classified without providing any further explanation, in particular, what kind of damage to state interest it may cause.[102] The decision denying the request is judicially reviewable.

---

96 It is indicated that the lack of an effective instrument of control may lead to several abuses of the classification authorities including instances of unlawful classification of information. (J. Zaleśny *„Dostęp do informacji*…", p. 41. More about the importance of judicial control in reference to PCIA 2011 in section IV.4.

97 FOIA Art. 2(2).

98 FOIA Art. 3(1)(1). Such a regulation is a consequence of the principle of subordination of private interest to the public interest. It is designed to protect authorities from providing public information that demands their reorganization of the structure and working rules to individuals for their private purposes (e.g. scientific work). M. Kłaczyński, S. Szuster „*Komentarz do art.3 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.01.112.1198)"* (Coomentary to Article 3 of the Freedom of Information Act; authors' translation*)*, LEX/el. 2003.

99 FOIA Art. 16(1). The form of a decision must be a guarantee that the refusal is not arbitrary. Judgment of the Constitutional Tribunal, 15.10.2009, ref. no. K 26/08; In the judgment of 12.02.2004 (ref. no II Sa/Ka 2024/03) the District Administrative Court in Gliwice stated that filing the decision on the refusal to disclose information is obligatory when the data requested falls within the scope of the FOIA, and it cannot be made public in order to protect one of the secrecy, e.g. state secrecy. Lately, in a case concerning the inaction of the ABW regarding disclosure upon Helsinki Foundation for Human Rights of the statistical data of operational activities, the Supreme Court in its judgment of 7.07.2010 (ref. I OSK 592/10) ruled that ABW is obliged to act and provide information on HFHR requests in the form of a decision.

100 District Administrative Court in Gdansk in its judgment of 26.05.2004 (ref. no 3 II SA/Gd 1339/02) emphasized that each decision denying access to public information must be justified.

101 Judgment of District Administrative Court in Warsaw, 7.05.2004, ref. no. II SA/Wa 221/04.

102 For instance: decision of the ABW of 26.06.2010, ref. no P-3012/2010. On the day of 31 May 2010 the HFHR filled freedom of information request in order to obtain information about secret agreement concluded between American and Polish intelligence on creation of CIA secret prisons in Poland where terrorism suspects were allegedly detained and tortured. In response, the Internal Security Agency refused

Further, practice also showes that there are cases where the classifying authority will neither confirm nor deny the existence of certain records that include classified information[103]. This is not regulated under FOIA and is definitely in need of further changes and elaborations.

1.6.2.b. Judicial control

Although unregulated, the concept of judicial control is being slowly elaborated by the judiciary. Recently, there have been important developments in the case law pointing to a need for courts to have effective power to exercise control and to be entitled to change the level of classification. It should be noted that information is not classified by an administrative decision which would legitimize the issue of challenging the classification before the administrative court.

The question presented for judicial review of the legality of classifying information is whether such a control is within the powers of a court. In the judgment of 15 October 2009, ref. no. K 26/08, the Constitutional Tribunal[104] expressed a general rule that when a court is considering a case involving classified information, it should also possess the ability to review the fulfillment of the requirements for classification. According to the judgment, if judicial control is limited only to confirming that particular information is or is not classified (without the review of whether the classification was performed in compliance with legal prerequisites), it will undermine the effectiveness and aim of judicial review.

In the most up-to-date judgment, 14 September 2010, ref. no. I OSK 1047/10, the Supreme Administrative Court quashed a judgment of a lower court that has sustained a refusal to publish information about the number of persons protected and costs of protecting identity witnesses program in Poland. The decision was given by the Head of Police Headquarters (*Komendant Główny Policji*) in response to the HFHR freedom of information request.[105] The case is an example of the abusive interpretation of secrecy - justifying the refusal to provide public information. It is now to be reconsidered by the District Administrative Court. What is

---

to disclose this information stating solely that it is a state secrecy and not explaining the reasons for classification. Available at: http://www.hfhr.org.pl/cia/images/stories/odpowiedz%20abw_24_06-2010.pdf.

103 It appears that this conundrum results from the assertion that even the disclosure of whether something is classified or not is itself classified information. For instance, in the course of one of the latter freedom of information cases litigated by the Helsinki Foundation for Human Rights, the Prosecutor Service investigating the alleged existence of CIA prisons in Poland refused to confirm or deny whether a document was authentic or not (Letter of Appeal Prosecutor Office in Warsaw *(Prokuratura Apelacyjna w Warszawie;* auyhors' translation*)*, 30 June 2010 (ref. no. Ap V Ds 37/09), available at: http://www.hfhr.org.pl/cia/images/stories/Odpowiedz_prokuratura.pdf). The document is a two-page piece of a flight book from Szymany airport obtained by a Polish journalist. It confirmed several landings of the planes that are commonly believed to collaborate with the CIA in the extraordinary rendition program created within the "war on terror" at the above-mentioned airport. The authority stated that the document is part of evidence material of a criminal investigation marked with a state secrecy clause. Since it is part of classified information, the authority reported that is not entitled either to confirm or deny the authenticity of its existence.

104 The judgment of the Constitutional Tribunal was delivered under the PCIA 1999 and was a result of the motion filed by the Polish Ombudsman, who claimed that the extensive classifying of information, resulting from the improper construction of the PCIA 1999 Article 21(3) (stipulating who was responsible for classification), led to an unconstitutional restriction of citizens' access to public information.[104] Although the Constitutional Tribunal did not find this particular provision unconstitutional, it confirmed that in practice, under PCIA 1999, there was a real threat of manipulation of classified information that caused numerous abuses.

105 Request available on: http://www.hfhrpol.waw.pl/precedens/images/stories/wniosek_o_informacje_sk.pdf

important is that the Supreme Administrative Court expressed a general opinion that judicial review should be possible. The court allowed for judicial control to check whether the information was classified in accordance with binding law in cases where documents based on classified information are considered (such as a decision refusing to disclose information). This recent judgment should be regarded as an important step towards recognition of the court's competence to review the merits of classification.

The above approach of 2010 is supplemented by earlier legal commentary that provides a firm justification for allowing courts to analyze the basis for classification. Some claim that there are no obstacles to the court's examination of whether the information was classified correctly.[106] It is also indicated that the court's competence in this respect is inevitable since it is necessary for the proper performance of FOIA provisions[107].

Questions arise also as to which types of cases judicial review can be performed in. Pursuant to FOIA, there are guarantees of the public right to access information, enforceable before the court. Judicial control in administrative cases might thus be initiated in cases of a refusal of a state authority to disclose information of a freedom of information request due to, *inter alia*, national security measures or in cases of not answering such a request[108]. It seems, however, that judicial control is not limited solely to freedom of information cases examined by administrative courts; it appears that it can be taken into consideration in any other case pending before the court when the case files include classified information and are considered by the court[109] (see the above-mentioned judgment in a criminal case).

Due to the significance of judicial control in cases concerning the restriction of access to public information, there still exists the need to provide an explicit clarification either by statute or further case law concerning judicial control over the classification regime, the scope of judicial control and the possible power of declassification. These issues remain uncertain, and such a state of affairs should be regarded with due seriousness.

2. Applicability of secrecy laws for the public

2.1. Access to classified information to general public

Under Polish law, persons eligible for security clearance are only those individuals who hold an office or perform a public service or the delegated work connected to classified information, and government contractors dealing with this kind of information[110] who guarantee its proper protection. As Piotr Niemczyk stated,

> in general there always needs to exist a justified reason, provided by the legal act, that should be proved in order to deal with classified data. The procedure leading

106 Rodziewicz, *Ochrona informacji niejawnych – analiza przepisów*, Przegląd Prawa i Administracji, t. 51, Wrocław 2003, s. 207.

107 J. Zaleśny *„Dostęp do informacji…*", p. 41.

108 FOIA Art. 16.

109 See the judgment of 10.09.2009 of the civil Appellate Court in Cracow (case ref. no. II AKa 139/09). The context of the judgment was a charge of committing the crime of disclosing confidential information. The court pointed out that judicial review is possible as an exception, only when it is reasonable. It should not be performed by courts in all circumstances, but only when serious doubts as to whether the classification complied with the law arises.

110 PCIA 2010) Art. 4(1).

to obtain a security clearance in most of the cases is initiated upon a request of an appropriate state official. The general rule is that it is not granted institutionally.[111]

PCIA 2010 does not provide any means for broader public to access to classified information. The practice shows, however, that there is a need to introduce provisions that would allow others with a legal interest to obtain a security clearance when justified.[112] For instance, HFHR might well illustrate the issue. The Foundation was involved in the case of Jan Kuriaty, a Member of Parliament at time, who was subjected to vetting proceedings regarding his alleged collaboration with authorities of the former communist regime. In the proceedings, the Foundation, as a Non-Governmental Organization, was granted the status of a third party and, as such, could participate in the trails, demand certain procedural actions and access case files. However, this became impossible once state secrecy was invoked in the course of proceedings. Consequently, representatives of the Foundation could not enter a number of sessions nor could they access files when the court considered classified information. According to the information provided by the Internal Security Agency, in Polish law it is not possible for a civil society's representatives to obtain a security clearance in cases where the organization possesses a direct interest. Such a conclusion derives from the letter to HFHR of Director of the Department of the Protection of Classified Information of the Internal Security Agency, 16.04.2010, ref. no. D-III-1009/2009.

2.2. Applicability of secrecy laws to journalists

Polish law does not specifically protect journalists by shielding them from prosecution for disclosing classified information. The Press Law[113], however, stipulates the "professional secrecy" of journalists, which provides journalists with several rights and obligations. One of them is the right to keep their name secret and a use nick-name[114]. Journalists are also under obligation to protect and keep secret data identifying the authors of press materials, letters to the editor, and other similar materials as well as other persons providing information to journalists on the condition not to disclose their personal data[115]. They also have to restrain from disclosing data that might violate the rights of third persons[116].

Furthermore, the professional secrecy of journalists results in certain procedural rights in criminal proceedings. Under the Criminal Procedure Code journalists may refuse to testify in circumstances falling within journalist's professional secrecy, unless the court orders an exemption, a decision that the journalist can appeal. The exemption is possible only when the court determines that a journalist's testimony is indispensible for the proper functioning of the justice system[117] and in the circumstances of the case, when the information cannot be

111 Interview with Mr. Piotr Niemczyk.

112 The concern was expressed in the opinion of the HFHR on the project of the protection of classified information Act, 26.08.2009, available at: www.hfhrpol.waw.pl/precedens/images/stories/opinia_niejawne.pdf.

113 *Ustawa prawo prasowe* (Press Law; authors' translation), 26.01.1984, the Journal of Laws no. 5 sec. 24 with further amendments.

114 Press Law Art. 15(1). The obligation is extended to other editorial staff, employees of publishing houses and other press organizational units.

115 Press Law Art. 15(2)(1). The obligation is extended to other editorial staff, employees of publishing houses and other press organizational units.

116 Press Law Art. 15(2)(2).

117 The notion of proper functioning of the justice system should be primarily understood as the need to establish an objective truth. When facts falling within the scope of journalist's professional secrecy can be established otherwise, the exemption from the secrecy is *ex lege* forbidden. Judgment of the Supreme Court, 22.11.2002, I KZP 26/02.

determined otherwise[118]. It is limited, as the court cannot order an exemption to compel the journalist to provide certain types of information, including information that would lead to the identification of anonymous sources or authors of articles or other data that might violate the rights of third persons[119]. However, the law overrides the exemption designed to protect anonymous sources or authors where the information sought relates to the certain offences enumerated in art. 240 Criminal Code – *inter alia* genocide, terrorist attack, murder, coup d'état, espionage, threat to public safety, assassination of a head of state, piracy and taking of a hostage[120].

It is the journalist's informant, not the journalist, who remains the holder of information. Between the journalist and the informant there is a relation of confidentiality. Therefore, in response to a judicial challenge, a journalist cannot force a source to reveal information or his or her identity; however, the journalist can appeal to the informant, or conclude an agreement allowing the journalist to release the information.[121] Furthermore, the professional secrecy of journalists does not mean that it is not possible for a journalist to testify on issues falling within his or her professional secrecy, intentionally violating the secrecy. It results from the assertion that journalists' professional secrecy is not covered by an absolute prohibition of an examination of evidence.[122]

Apart from the above, there are no explicit provisions shielding journalists from the criminal liability. On the contrary, the law says that a journalist's refusal to disclose information protected by professional secrecy does not prevent him or her from liability for an offence committed by publishing certain information[123]. Journalists who, in the course of their professional obligations, disclose classified information may be, therefore, at risk of criminal liability for the offence of unauthorized disclosure and use of classified information[124]. Journalists are also exposed to criminal liability when disclosing information concerning ongoing criminal investigations containing classified information[125]. However, there are presently efforts to amend Polish law to protect journalists from criminal liability for disclosing such information, *inter alia*, in order to protect a socially justified interest.[126]

Moreover, concerning journalists' professional secrecy, there is uncertainty as to state authorities intercepting phone billings or e-mail messages of journalists. According to Criminal Code Article 218, e.g. phone billings, mails, and e-mails are to be submitted by the possessing units upon a court's request for criminal proceedings and investigations. However, a recent case revealing the invigilation of journalists brought to light several abuses of the

118 Criminal Procedure Code Art. 180(1)-(2).

119 Criminal Procedure Code Art. 180(3).

120 Criminal Procedure Code Art. 180(4).

121 I. Dobosz "*Prawo Prasowe. Podręcznik" (Press Law. Workbook*; author's translation*)*, Wolters Kluwer 2006, p. 228-229.

122 Judgment of the Supreme Court, 15.12.2004, III KK 278/04.

123 Criminal Procedure Code Art. 180(5).

124 The issue of the scope of individual criminal liability for the offence stipulated in art. 265 Criminal Code, including journalists, is further elaborated in the section IV.2.

125 Criminal Code Art. 241(1).

126 *Założenia Projektu Ustawy o Zmianie Ustawy – Kodeks Karny* (Project of assumptions for the project of the act amending the Criminal Code; authors' translation*)* of 30 June 2010 prepared by the Ministry of Justice. The project is currently subjected to the debate within the Council of Ministers and has not been submitted to Parliament yet. The project available at http://bip.ms.gov.pl/Data/Files/_public/bip/projekty_aktow_prawnych/prawo_karne/proj100324c.rtf.

secret services and Police[127]. The incident displayed clear insufficiencies in Polish law preventing effective control over the surveillance activities of the Police and special services. The case also showed insufficiencies in regulations concerning confidentiality of the proceedings, as journalist's constitutional right to access information about oneself and to destroy such information gathered unlawfully was ineffectively rendered in the case[128].

2.3. Participants in Legal Proceedings – access to case files

Invoking state secrecy during court proceedings and preparatory proceedings might, in some instances, effectively hinder parties of a particular case from accessing case files. The European Court of Human Rights (hereinafter "ECHR"), for instance, has repeatedly found violations in vetting proceedings. The ECHR stated that Polish law implies restrictions on a defendant to access classified, archived case files containing information on his or her connections with communist regime authorities. This, in the opinion of the Court, significantly impedes the right to defense and violates the right to a fair trial.

The opposite conclusion was found by the Provincial Administrative Court in Warsaw in an expulsion case of a Moroccan citizen who had been living in Poland for eight years and who was accused of engaging in terrorist activity in Poland. He was refused a prolongation of a temporary resident permit and deported from Poland pursuant to an administrative decision, based on a restricted document of the Internal Security Agency. The court upheld the decision, even though the document that constituted the basis of the deportation was unseen by both the defendant and his attorney. This case shows that there are no procedural guarantees such as the accused person's right to see classified documents in administrative hearings .

Another limitation in access to case files is stipulated in Criminal Procedure Code. It provides that a party to proceedings has the right to view classified materials only in the secret chancellery and does not have the right to make notes or copies. This applies also to vetting procedures. Lately, the ECHR, in the judgment of 1 March 2011, in case *Welke and Bialek v. Poland* (Application no. 15924/05), ruled that the above-mentioned restriction does not violate the fair trail standards derived from Article 6 of the European Convention of Human Rights. The applicants complained about the unfairness of criminal proceedings brought against them convicting them of drug trafficking. Among other things, they alleged that their right to defense was violated. The Court stated that access to case files only in secret chancelleries and with the note-taking restriction is not contrary to the Convention.

2.4. Protection of Whistleblowers

---

127 The case was reported by media (Article „Dziennikarze na celowniku służb specjalnych" by Wojciech Czuchnowski, Gazeta Wyborcza, 8.10.2010, available at http://wyborcza.pl/1,75478,8480752,Dziennikarze_na_celowniku_sluzb_specjalnych.html?as=1&startsz=x.). It indicated that between 2005 and 2007, Polish secret services and police investigated the phone records of ten, top Polish journalists, uncovering information, including protected information regarding journalists' informers. According to media, the case files show that the services gravely abused their obligation of combating serious crimes. Prosecutor Service in Zielona Góra investigated the case on the charges that ten Polish journalist were invigilated. However, in May 2010 the prosecutor discontinued the investigation stating that the secret services' and Police's conduct did not violate the law and did not fulfill the prerequisites constituting an offence of abuse of powers. Only a small part of the documents were published, since most of them were classified as "secret" and "top secret".

128 An amendment to the law regulating the operational activities of secret services was proposed some time ago and was submitted to Parliament. However, it is imbalanced and protects the privileges of the security services more than the rights of citizens and as such will not provide the desirable law amendments.

Under the Polish legal system, there are no laws that provide specific protections of persons who acting in good faith disclose violations or unethical behavior in their workplace or any other professional environment. Such persons, whistleblowers, by taking action for the protection of the public interest, guarantee that irregularities are detected and prevented as early as possible and exposes themselves, *inter alia*, to mobbing, risk of dismissal and when disclosing classified information, criminal liability. In Poland, this group of persons is not granted any statutory protection that would take into account the specificity of their action.[129] Neither are there laws regulating whistleblowers who reveal the above-mentioned irregularities and, at the same time, commit an offense like the violating the law on classified information[130]. This issue has sparked a debate in Poland where there have been calls to introduce legal protection for whistle-blowers.

IV. Selected current areas of uncertainty, controversy and challenge

1. Change in classification definitions

PCIA 2010 introduces a new system of defining classified information. Certain information should be classified when the authority body determines that it falls within one of the definitions of the classification levels. To do so, the body needs to assess the possible harm to the Republic of Poland that might be caused by the unauthorized disclosure of the information. Apart from the definitions, there is no list of categories of information that need to be classified.

Many problems under PCIA 1999 led to the introduction of changes in PCIA 2010. The former law protected classified information that included both state secrets and professional secrets. The first one, according to PCIA 1999 Article 2(1), is information that can endanger the fundamental interest of the state of Poland regarding public order, security, defense, international or economic relations if disclosed. Additionally, apart from this specification, classified information being a state secret was enumerated in an exhaustive list of explicit categories as Attachment no 1 to the PCIA 1999. Professional secrets, on the other hand, were defined in PCIA 1999 Article 2(2) as classified information that does not fall under a state secret gained in the course of performing public functions. Unauthorized disclosure of professional secrets connected to the functioning of a governmental units can lead to harm of state interests, public interests or legally protected interests of citizens or organizational units.

On the one hand, according to Stanisław Zarodkiewicz, "the prerequisites to classify information was very precise, therefore there was no ambiguity as to what data should be

---

129 See: A. Wojciechowska-Nowak „Jak zdemaskować szwindel? Czyli krótki przewodnik po whistle-blowingu." (How do unmask abuses? Short Guide on Whistleblowing; author's translation) , Fundacja Batorego, Warsaw 2008, available at: http://www.batory.org.pl/doc/Poradnik_Jak_zdemaskowac_szwindel_grudzien_2008.pdf.

130 The construction of the offence of unauthorized disclosure of a state secret (Criminal Code Art. 265) is such that does not include any circumstances which depenalise the offence. There are no exceptions, such as disclosure of a state security secret that does not cause any harm to state interests and national security or overriding public interest, meaning the right of citizens to be aware of any irregularities seriously affecting the public interest. One may seek defense on the grounds of the general provisions of criminal law, such as the lack of guilt or insignificant social noxiousness. A person might argue that they were acting in a state of necessity, as exculpation for breaking the law (according to Criminal Code Art. 26, a person does not commit an offence when acting to avoid an imminent harm to legally protected goods, where the harm cannot be prevented otherwise and the value of a good that is rescued is higher than the one that is sacrificed).

classified."[131] On the other, according to the Reasons for the Project of Protection of Classified Information Act, the practice shows that the requirements in PCIA 1999 led to classification of the large amount of information which in many cases did not require the protection prescribed for classified data. Moreover, much information was given too high a level of classification, not justified by its factual content. The reason being that the information was listed under one of the obligatory categories for classification.

Another problem identified in the Reasons for the Project of Protection of Classified Information Act was the fact that PCIA 1999 enforced classification when information that should have been granted a certain level of protection was not classified at all due to the need of fast processing and transmission of the information to the recipients. This resulted because state secrets were protected only at the level of "secret" and "top secret", thus the highest levels of classification, which imply serious restrictions. "Confidential" and "restricted" levels that guaranteed sufficient protection while allowing for access that was not as strict as in the case of "secret" information were designed only for professional secrets. As practice showed, not all information important for state secrecy needed such a high protection level, which significantly restricted its access.

The above issues were a reason to introduce the new system of defining classified information. According to the Reasons for the Project of Protection of Classified Information Act, the aim of PCIA 2010 was to provide more flexible rules allowing authorities rational classification. It no longer required automatic classification of data because the information fit into a particular category, regardless of the analysis of the particular information and the harm that would come from the information's unauthorized disclosure. In consequence, the purported justification of new classification system under PCIA 2010 was to eliminate or significantly limit the problem of excessive classification.

PCIA 2010 removed the anachronistic and difficult-to-apply classified information division between a state secret and a professional secret. The new law stipulates that classification is based on the harm standard relating exclusively to the sphere of state's interests. It does not refer anymore to e.g. the interest concerning the proper functioning of a particular governmental agency. In consequence, information important to state interest and national security can be now classified not only at two but at four levels, including "restricted" and "confidential". This seems to allow for proper protection of information, while simultaneously diminishing the risk of giving too high a level of classification, which would restrict access to information. Additionally, the law abandons the strict control of the circulation of documents with lower classifications, especially data classified as "restricted".

However, under the new law practical problems with application may appear. There is less automatic classification, but at the same time, the vagueness of the definitions leaves much greater discretion to the classifying authorities, and the potential for practical problems in determining appropriate classification increases. Under PCIA 2010, the construction of the definitions of the levels of classification is based on indeterminate, vague terms such as "serious harm", "exceptionally serious harm", thus on a valuation of the harm without a specification of the harm, as well as e.g. "negatively influence national economy". This problem was indicated by the Sejm Office of Analysis who examined the new regulations. The Office pointed to the practical problems that may appear in understanding the law and its interpretation made by officials who are competent to classify, declassify or to change the

[131] Interview with Stanisław Zarodkiewicz.

level of classification as well as to perform overall control over the classification regime.[132] Neither the PCIA 2010 nor any executive order provides more specific guidelines for officials to follow in classifying and declassifying information. As Piotr Niemczyk pointed out,

> under PCIA 2010, it seems that the most serious problem that the officials will face will be the question: how to classify the information? The new law introduces serious amendments in this respect. Beforehand, there were clear rules regarding classification which however lead to automatic classification of [a] big amount of data. The new law complying of indeterminate provisions [makes] this issue for the officials uncertain[133].

The practice of state officials holding classified authority will show whether the amendments introduced by PCIA 2010 fulfill all the aims of the new regulations. The PCIA 2010 came into force on 2 January 2011, and as of now, it is far too early to state what the consequences are of changing the definitions of classified information.

2. Public responsibility to protect information and liability for disclosure

Under the Polish law and practice, there is serious uncertainty regarding who may be held liable for the offense of unauthorized disclosure and sharing of classified information stipulated in Criminal Code Article 265(1). The essence of the highly debated problem focuses on who is the perpetrator of Article 265(1) – whether it is exclusively a state official who is entitled to access and obliged to protect classified information or whether it can be anyone who came into possession of such information[134].

It results from the fact, *inter alia,* that PCIA 1999 and PCIA 2010, unlike the former regulations of 1982[135], do not state *expressis verbis* that every person who is acquainted with classified information is under the obligation to protect it, thus that such a person is liable for its disclosure. Further, the Criminal Code does not provide the legal definition of "state secrecy".[136]

An important voice in the debate was added by the judgment of the Supreme Court of 26 March 2009 in case ref. no. I KZP 35/08[137]. The Supreme Court interpreted Criminal Code Article 265 in a case of two journalists Jarosław J. and Bertold K., who were accused of

---

132 See Legal brief of the Sejm Office of Analysis regarding the project of the protection of classified information act, 6.04.2010.

133 Interview with Piotr Niemczyk.

134 In favour of the opinion that only a state official who is entitled to access to classified information can be perpetrator of art. 265(1) Criminal Code - see *inter alia*, W. Wróbel, *Prawnokarna ochrona tajemnicy państwowej (*Criminal protection on state secret; authors' translation*)* , Czasopismo Prawa Karnego i Nauk Penalnych 2000 no. 1, p. 133-147; P. Burzyński, *Tajemnica państwowa jako przedmiot ochrony regulacji prawnokarnej (*State secret as a subject to protection of criminal law*; authors' translation)*, Czasopismo Prawa Karnego i Nauk Penalnych 2002, no. 1, p. 26-29. Universal nature of art. 265(1) Criminal Code - see S. Hoc, *Kilka uwag dotyczących przestępstwa z art. 265 k.k. (*Few thought on the offence of Crimial Code Article 265; authors' translation*)*, Wojskowy Przegląd Prawniczy 2003, no. 4, p. 90-91. In reference to jurisprudence see the Supreme Court's judgment of 8 March 2007 in case ref. no. I KZP 30/06: "a person may not be indicated as a perpetrator of the offence of art. 256(1) Criminal Code when discloses information within his or her competences and obligations".

135 *Ustawa o ochronie tajemnicy państwowej i służbowej* (Protection of state secrecy and professional secrecy; authors' translation), 14.12.1982, the Journal of Laws no. 40, sec. 271.

136 K. Tkaczyk, *Comments on the judgment…,* p. 271.

137 The judgment was delivered under PCIA 1999, however remains valid under PCIA 2010.

disclosing a state secret in 1999 by publishing series of articles[138]. The court stated that the offence of unauthorized disclosure and using of classified information may be committed not only by state officials authorized by statute to hold classified information, but also by journalist who publish them, since the offense is of "universal nature". Earlier in the practice among justice bodies, the dominant view was that only the official who primarily discloses classified information may be held liable due to their exclusive obligation to protect it. According to the Supreme Court's judgment, all persons who are acquainted with such information, not only those performing public functions that had the information enter their possession legally, may be charged for the offence.

The Supreme Court considered Press Law Article 3a, in saying that in terms of access to information, the Press Law refers directly to FOIA. According to the court, this includes FOIA Article 5 (1) that limits access to information based on the rules in the law on classified information. Therefore, the Supreme Court stated that the scope of the use of information by journalists is limited by the law on classified information. In other words, FOIA exemptions apply to the general public as well as to journalists, meaning that where FOIA exemptions require the state officials to not disclose information, journalists too do not have a right to that information as an exception.

As a result of the Supreme Court judgment, the case was reexamined. The court of first instance found the defendants guilty of the offence of unauthorized disclosure of classified information. However, the court discontinued the proceedings relying on insignificant social noxiousness. The court did not advance procedurally, i.e., in examining testimony or motives, considering the emergency context, etc. Journalist, Jarosław J. and Bertold K., lodged an appeal against the decision to the court of second instance demanding quashing the decision. They raised the defense of acting out of necessity, since they possessed highly probable information that state officials who committed an offence wanted to hush up this fact and evade criminal responsibility. The District Court in Warsaw, however, in the judgment of 10 December 2010, case ref. no. IV K 211/06, did not support such argumentation and sustained the first decision. The result of the proceeding was that the journalists were found guilty of disclosing classified information; however, they did not suffer punishment due to insignificant social noxiousness.

This precedential judgment is very important for the debate on the interpretation of Criminal Code Article 265(1), since previously, this issue has not been subjected to such a broad and deep analysis. Some representatives from the legal commentary speak in favor of the judgment claiming, for instance, that excluding the group of journalists from the applicability of Criminal Code Article 265(1) is not justified under the law, since such an immunity provided for particular group – journalists – may be unconstitutional[139]. However, the

---

138 Two journalists, Jarosław J. and Bertold K. published three articles describing operational activities conducted by the State Security Office (*Urząd Ochrony Państwa*) concerning spy activities of former officers of Polish Army. Journalists also disclosed the source of information that was transmitted to the State Security Office while performing operational activities. The County Court in Warsaw (*Sąd Rejonowy w Warszawie*; court of first instance), on 9 May 2008, dismissed the proceedings claiming that the offence of 265 Criminal Code can be committed only by state officials legally obliged to protect classified information. Subsequently, the case was considered by the District Court in Warsaw (*Sąd Okręgowy w Warszawie*), as a result of Public Prosecutor General's complaint. The court of second instance filed a legal question to the Supreme Court asking whether anyone, including journalists, can be held liable for the offence of disclosure of classified information.

139 S. Hoc *Glosa do uchwały SN z dnia 26 marca 2009 r., I KZP 35/08* (Comments on the judgment of the Supreme Court of 26.03.2009, ref. I KZP 35/08; authors' translation), Prokuratura i Prawo 2010/3/138.

judgment raised serious controversies in the legal commentary, especially taking into consideration the professional activity of journalists[140]. There are various arguments that undermine the significance of the judgment. It is indicated, for instance, that the case raises grave doubts and objections because of the cursory nature of the argumentation and a lack of internal consistency[141]. The debate regarding the interpretation of the provision is still ongoing. Who can be held liable for the offense is highly controversial, and the opinion that all individuals, regardless of whether they were obliged by the law to protect classified information, may face criminal liability is broadly questioned.

The Supreme Court's judgment in case ref. no. I KZP 35/08 might be persuasive to other courts, as they may follow the judgment, relying on the authority of the Supreme Court. Formally, the interpretation does not have a binding effect on all courts, but only binds the court that presented the legal question to the Supreme Court[142]. In reference to that, several other questions arise regarding future judicial practice. First, it is not clear what would be a possible and effective defense to invoke before a court. As the case ref. no. IV K 211/06 showed, the court was not likely to support argumentation based on acting out of necessity to protect the public interest. Further questions concern the issue of what penalties might be ordered by the court. It is yet not certain whether a court would, like in the mentioned case, find an individual guilty, but abandon punishment under the veil of insignificant social noxiousness. All of these questions and issues need further challenging and need to be evaluated.

3. Incentives to classify and declassify

3.1. Lack of sanctions for excessive classification

PCIA 2010 stipulates a procedure to challenge the improper classification, namely classifying data with too high or too low a level of classification or classifying information that does not require such a protection under the law[143]. PCIA 2010, like PCIA 1999, does not include

---

140 See K. Tkaczyk, *Glosa do uchwały SN z dnia 26 marca 2009 r., I KZP 35/08 (*Comments on the judgment of the Supreme Court of 26.03.2009, ref. I KZP 35/08; authors' translation), Palestra 5-6/2010, p. 273; J. Raglewski *Glosa do uchwały SN z dnia 26 marca 2009 r., I KZP 35/08* (Comments on the judgment of the Supreme Court of 26.03.2009, ref. I KZP 35/08; authors' translation), LEX/el 2009; M. Leciak *Glosa do uchwały SN z dnia 26 marca 2009 r., I KZP 35/08* (Comments on the judgment of the Supreme Court of 26.03.2009, ref. I KZP 35/08; authors' translation), Prokuratura i Prawo, 9/2009, p. 164-167; J. Skrzydło *Glosa do uchwały SN z dnia 26 marca 2009 r., I KZP 35/08* (Comments on the judgment of the Supreme Court of 26.03.2009, ref. I KZP 35/08; authors' translation), Państwo i Prawo 2010.6.128.

141 It is highlighted that, e.g., the content of Criminal Code Article 265(1) may be reconstructed solely based on provisions of the act on classified information; namely this implies that criminal liability arises only when one violates procedures stipulated in law (See K. Tkaczyk, *Comments on the judgment of the Supreme Court of 26.03.2009, ref. I KZP 35/08,* p. 273; J. Raglewski *Comments on the judgment of the Supreme Court of 26.03.2009, ref. I KZP 35/08,* LEX/el 2009; M. Leciak *Comments on the judgment of the Supreme Court of 26.03.2009, ref. I KZP 35/08,* p. 164-167; J. Skrzydło *Comments on the judgment of the Supreme Court of 26.03.2009, ref. I KZP 35/08,*). Furthermore, the rationality to hold all individuals criminally liable is questionable. It is especially controversial respecting journalists. The Supreme Court's judgment carries a risk of criminal liability for journalists who act to protect public interest by publishing articles that do not negatively affect state interest (K. Tkaczyk, *Comments on the judgment of the Supreme Court of 26.03.2009, ref. I KZP 35/08)*. What brings important doubts is also that the non-disclosure obligation applied to persons who get familiar with classified information beyond the activity of the public sphere might restrict the constitutional freedom of unfettered dissemination of information.

142 Binding interpretation is established when the law was delivered by seven judges.

143 PCIA 2010 Art. 9. More about the procedure in the section III.1.6.1.

provisions stipulating the type of responsibility that a state official might face for excessive classification.

Under PCIA 1999 the lack of sanctions was deeply analyzed by the Polish Constitutional Tribunal[144] in a judgment that resulted from a motion filed by the Polish Ombudsman. The Ombudsman claimed that PCIA 1999 Article 21(3) is unconstitutional since this regulation does not stipulate the nature, prerequisites and type of responsibility that a state official may hold. According to the Ombudsman, the regulation was incomplete and the reason for abuses in classifying data and consequently an extensive restriction of citizens' access to public information. However, the Constitutional Tribunal ruled that PCIA 1999 Article 21(3) was in compliance with the Constitution, since the problem resulted from the official's practice of applying PCIA 1999 rather than directly from the wording of PCIA 1999Article 21(3).

Furthermore, what is crucial is that the Constitutional Tribunal ruled that although the provisions including responsibility and sanctions are not included in the act, it does not mean that no such sanctions exist or apply at all. They are stipulated in separate legal acts and depend directly on the type of responsibility held by an official, which might be disciplinary, official or criminal. As to the latter, the Constitutional Tribunal indicated that liability for unlawful disclosure or use of classified information[145] or abuse of powers by states officials, which is against public or private interest[146], should be taken into consideration.

However, taking into consideration the practical dimension of the law, although lack of sanctions is not unconstitutional, due to the lack of their explicit stipulation in PCIA 2010, problems with enforcing the law and holding the officials responsible for their abuses might still occur. In essence, there is an improved procedure but still no directly mentioned remedy to encourage or command its effective use. According to Piotr Niemczyk,

> The superior is unable to control all classified information generated within the organizational unit and thus is unable to supervise the conduct of all officials. Therefore, it is possible that people, in order to hide their own incompetence, or that of other officials, choose to classify information even where, it is not obligatory. Under PCIA 1999, which also did not provide for sanctions, in practice, officials rarely faced responsibility for misconduct through disciplinary measures. Therefore, it is fair to assume that PCIA 2010 will not provide a significant change in holding officials responsible for their abuses concerning misclassification. Although the procedure exists, it will be difficult to enforce it.[147]

Mr. Niemczyk cited one example of abusive classification: "Under PCIA 1999 special executive order regulated the dispatch procedures of classified information contained provisions that spoke in favor of classifying information as state secret rather than professional secret. In consequence, information falling within the professional secrecy was more likely to mark as state secrecy*".* The executive order*[148]* stipulated that state secret

144 Judgment of the Constitutional Court, 15.10.2009, ref. no. K 26/08; the judgment was delivered as a consequence of the claim submitted on 8 August 2008 by Polish Ombudsman in relation to the refusal of disclosing public information, namely the Report of Julia Pitera on the activities of the CBA.

145 Criminal Code Art. 265.

146 Criminal Code Art. 231.

147 Interview with Piotr Niemczyk.

148 Interview with Piotr Niemczyk; the rules of transportation are included in the *Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie trybu i sposobu przyjmowania, przewożenia,*

information was transported by specially appointed post services (e.g. special post subordinated to Minister of Internal Affairs, special unit subordinated to the Ministry of Foreign Affairs, according to strict procedure, whereas professional secret information could be transported in normal letters via public Post Office.

> A reason for choosing by state officials to dispatch information through those post services was that they preferred to guarantee a better level of protection of transported items than was offered by the public Post Office even if it was connected with classifying information with the level much higher that needed. It was difficult to accept by officials that state secrecy items could be simply send via public Post Office – explains Mr. Niemczyk – However, in practice, the reason to preferably choose specially appointed post units could also have been much more trivial. Under the executive order it was far more convenient to send information using their services. Prepared transportation packages were collected directly from the governmental agency by the post service. Sending letters or other packages containing professional secrecy, however, required the use of public Post Office which obviously did not include such facilitation. It is also possible to presume a situation when classifying with too high level of classification derived from the possible defects within the classification regime and was possible due to insufficient control by superiors[149].

As Mr. Zarodkiewicz pointed to[150], another example of excessive classification under PCIA 1999 was noted in police practice. Internal police guidelines stated that telecommunication data provided by telecommunication companies at the police's request[151] should be classified only when it contains public service secrets. However, practice showed that such information was almost always classified regardless of its factual content.[152]

3.2. Lack of automatic declassification regime in PCIA 2010

When considering incentives under the new law for classification it is necessary to point to the fact that PCIA 2010 brought a significant amendment in declassification. The law no longer mandates mandatory time limits but provides for obligatory periodic review of information.

According to the Reasons for the Project of Protection of Classified Information Act 2010, the aim was not to provide a more flexible declassification regime. Second, the five-year non-automatic review was adapted and now is analogous with European Union regulations. In the Reasons it was pointed out that the results of a mandatory periodic review of all classified documents to determine whether this information continues to meet the statutory requirements set out in PCIA 2010 Article 5 will allow for easier change of classification level or even

---

wydawania i ochrony materiałów zawierających informacje niejawne (Execution order of 29.09.2005 regarding transportation of secret information; authors' translation), the Journal of laws no. 1649 sec. 1650, issued under the PCIA 1999.

149 Interview with Piotr Niemczyk.

150 Interview with Stanisław Zarodkiewicz.

151 *Ustawa o Policji* (The Police Act; *authors' translation)*, 6.04.1999, the Journals of Law no. 43 sec. 277 with further amendments, Art. 20 c.

152 M. Romanowski „*Nadawanie klauzuli tajności informacjom uzyskiwanym w trybie art. 20 c ustawy o Policji*" (Classifying information obtained under the Police Act Article 20 c, authors' translation), Biuletyn Prawny Komendy Głównej Policji, no. 2(37), p. 22. This paper provide with deep analyze of the issue.

declassification. It will, therefore, reflect the real necessity to classify information and bring updated knowledge in this respect. The flexibility was also to be improved by introducing the possibility to declassify after a stipulated event and the possibility to classify with different levels different parts of documents.

System of declassification under PCIA 1999 presumed that a time limit exists after which data is automatically declassified. "Top secret" and "secret" information, namely state secrets, used to be protected for 50 years. "Confidential" professional secrecy was protected for 5 years and "restricted" professional secrecy for 2 years[153]. In reference to professional secrets, time for its protection might have been either shortened or extended; however in no case could it be longer than 20 years[154]. There was an obligation to keep this information classified for the entire duration of the above-mentioned periods and earlier declassification was allowed only under certain conditions. After 20 years information could be declassified by the Council of Ministers in a form of executive order enumerating which "secret" (only) information no longer needed to be classified. This mechanism was thus limited and not flexible.

Practical dimension of applying systemic declassification under PCIA 1999 showed it did not properly protected classified information. It caused a great amount of secret information that should not have been protected at all to remain classified or at certain level of classification. According to the Reasons for the Project of Protection of Classified Information Act, abandoning this system was designed to be a direct answer to such unjustified, excessive classification. On the other hand, legal commentary[155] mentioned that, in some circumstances, automatic declassification led to obligatory disclosure of sensitive information after a certain time period, although taking into consideration its content, it should have remained under protection.

The change might have a good effect, as it will enable a real revision of the archives of classified information. The heads of the agencies are obliged under PCIA 2010 Article181 to review all documents and other materials containing classified information that were created in the agency. This must be done within 36 months after the PCIA 2010 entered into force. As a result, information that does not comply with the prerequisites to be classified due to their content and actual impact on national security but was kept secret under the automatic declassification system are to be declassified or given lower level of protection. However, we have to keep in mind that the new mechanism of PCIA 2010 relies on the discretion of state officials and on the proper fulfillment of their obligations. This always raises a question of possible abuses. Therefore, there is a risk of arbitrary decisions and violations of classification regime by authorities. Perhaps it would be better to allow more flexible provisions of revision while maintaining automatic declassification in the legal scheme. As the law has been in force since January 2011, it is too early to judge what will be the practical application by state officials regarding newly classified information and information that already had been classified.

Additionally, the new law introducing non-automatic declassification based on periodic revision did not exclude from the Polish legal scheme a permanent classification of certain sensitive data, namely identification data concerning officers, soldiers, or other persons

153 PCIA 1999 Art. 25(3).

154 PCIA 1999 Art. 25(4).

155 T. Szewc *„Ochrona informacji niejawnych. Komentarz."* (Protection of classified information. Commentary; authors' translation), Warsaw 2007, p.129.

participating in operational activities. This might seem problematic from the perspective of access to information, since data, for instance, concerning spies could never be declassified and disclosed to the public.

However, there is one exception to that[156]. Information about employees, officers and military officials of ex-communist secret services are publicly available[157] and their files are accessible in the premises of the Institute of National Remembrance. Such information is not eligible for indefinite classification. This provision is strictly connected to the history of Poland and issues of overcoming the legacies of the ex-communist regime in Poland. It is very important for the proper performing of vetting proceedings in Poland concerning clearances required to demonstrate non-collaboration with Poland's communist-era security agencies. There is, however, one exception to this rule[158]. According to Vetting Act 2006 Article 39, to protect national security the head of Internal Security Agency, the head of the Foreign Intelligence Agency, Minister of Defense may order that for certain time period selected archives of the Institute of National Remembrance are classified and only designated persons may access it[159]. In general, these regulations provide clear rules of protection of officers and collaborators of ex-communist regime. In case of ambiguities, vetting proceedings could be significantly disturbed or even not possible. In terms of secret archives, their existence appears to provide for proper protection of national security. On the other hand, the fact that they are in possession of the Institute of National Remembrance, not secret services should prevent form possible abuses of the services.

3.3. Lack of explicit prescription of information that should be disclosed

Nothing in the Polish law lists specific information or categories of information that would be excluded from classification. Nor does Polish law stipulate specific categories of national security information that are required to be disclosed for oversight purposes. The lack of those exemptions in Polish law may appear problematic, favoring classifying data and not access to information.

In reference to the lack of specific information or categories of information that would fall outside of classification, there is no exemption from classification for, for instance, serious violations of law, statistical data (e.g. concerning operational activities of secret services)[160], "documents concealing abuse of powers especially within secret services, documents preventing to disclose data indicating violations of law or improper functioning of certain agencies and officials, or information which after certain period of time lost its characteristics to be classified (e.g. data on energy supplies to the country)."[161] These are circumstances that should speak for declassification or not classifying them at all. However, as pointed to Mr.

---

156 PCIA 2010 Art. 7(2).

157 Information is published at: http://katalog.bip.ipn.gov.pl/main.do?katalogId=2&pageNo=1&. However, information about informants can be published in such catalogues when they were subjected to terminated vetting proceedings Vetting Act 2006 Arts. 18(5), 63b) or were the highest state officers (Vetting Act 2006 Art. 22(1)).

158 PCIA Art. 7(2).

159 In the judgment of 26.10.2005 r., ref. no. K 31/04 TK Constitutional Tribunal confirmed that it is in conformity with Polish Constitution to create archives with restricted access in the Institute of National Remembrance.

160 In the judgment of the Supreme Administrative Court of 1.10.2010 (ref. no. I OSK 1149/10) the Court stated that the statistical data does not constitute a state secrecy but falls within the scope of public information.

161 Interview with Piotr Niemczyk.

Niemczyk, there are certain information that should be obligatory subjected to classification regime, due to its impact on state interest, inter alia, current functioning of military services, strategy and logistics of military actions (including those fulfilled abroad), details of organization of secret services, data concerning current energy resources, strategic reserves of Polish economy, main directions of work and tasks of Polish diplomacy[162].

3.4. Lack of public interest overrides exception

PCIA 2010 provisions do not introduce a public interest test and a public interest override exemption. No exceptions are therefore granted that would allow disclosure to protect public interest when the information is properly classified. The lack of public interest override might be an important loophole, since in certain instances disclosure of information might better contribute to protecting national security than its continued secrecy.

A good example for the need to introduce the above-mentioned exemptions are grave human rights violations e.g. the case of the alleged existence of CIA secret facilities in Poland established within the frameworks of the "war on terror" commenced by United Stated of America after the September 11, 2001 attacks. Terrorist suspects were to be detained, interrogated and tortured there. Despite the Polish national authorities denying the existence of such secret detention centers, Poland is mentioned in the reports of Council of Europe[163], European Parliament[164] and United Nations[165] as one of the European countries where secret CIA detention centers were created. The criminal investigation concerning Poland's involvement in the extraordinary rendition started in 2008 and from the beginning was classified. At the moment, the investigation is carried out by the V Department of the Appellate Prosecutor's Office and concerns the possible abuse of power by public officers while performing the role of the highest representative of Polish authority, violating Criminal Code Article 231(1)[166].

---

162 Interview with Piotr Niemczyk.

163 Alleged secret detentions and unlawful inter-state transfers involving Council of Europe member states. First Report of June 7, 2006 of the Committee on Legal Affairs and Human Rights PACE, Rapporteur: Mr Dick Marty, available at http://assembly.coe.int/Main.asp?Link=/CommitteeDocs/2006/20060606_Ejdoc162006PartII-FINAL.htm; Secret detentions and illegal transfers of detainees involving Council of Europe member states. Second report of June 11, 2007 of the Committee on Legal Affairs and Human Rights PACE, Rapporteur: Mr. Dick Marty available at http://assembly.coe.int/Documents/WorkingDocs/Doc07/edoc11302.pdf.

164 European Parliament resolution on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners, adopted midway through the work of the Temporary Committee (2006/2027(INI)) of July 6, 2006, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2006-0316+0+DOC+XML+V0//EN.

165 Joint study on global practices in relation to secret detention in the context of countering terrorism of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, the Working Group on Arbitrary Detention and the Working Group on Enforced or Involuntary Disappearances, available at http://www.hfhrpol.waw.pl/cia/images/stories/Rport%20ONZ.doc.

166 Letter of Appellate Prosecutor Office of December 15, 2010 available at http://www.hfhr.org.pl/cia/images/stories/Odpowiedz_Prokuratura_15_12_2010.pdf.

Since there is international pressure[167] to explain Poland's role in extraordinary rendition, a fair and meticulous investigation should become a priority for the national authorities. However, due to the fact that the investigation is covered by state secrecy, for more than two years now, the public has known little about its course or, e.g., an approximate date of its conclusion. State secrecy thus became a condition justifying the refusal to provide public information.

The case regards allegations of serious human rights violations on Polish soil, so it is definitely in the public interest to have at least basic knowledge. Therefore HFHR has been submitting freedom of information requests to several state authorities and received important information on Polish involvement on renditions[168]. Despite constant reluctance of authorities to give information on the case, thanks to the actions taken by the HFHR as well as the Polish media[169], much information about CIA secret prisons in Poland became present in public domain[170]. Finally, in 2010 and 2011, when more and more information was publicly available, in view of the pressure coming from human rights groups, media and international sources, the Prosecutor Service started to provide some procedural facts of the investigation in response to the HFHR requests and letters[171].

---

167 It was indicated by both the Human Rights Commissioner of the Council of Europe, Thomas Hammarberg, and the UN Human Rights Committee in its Recommendations on Poland. They argued that Poland should conduct a thorough investigation concerning extraordinary rendition. Additionally, they said that the state secret argument cannot be raised to justify the refusal to disclose information about human rights violations.

168 For instance, the Foundation obtained flight logs from the Polish Air Navigation Services Agency *(Polska Agencja Żeglugi Powietrznej),* which showed that CIA planes landed in Poland many times and both Polish and US authorities were covering up their flight plans. Data available at: http://www.hfhrpol.waw.pl/pliki/OBS_CIA.zip. In addition, the Border Guard Service disclosed that the planes were carrying passengers. From 5 December 2002, to 22 September 2003, five out of seven planes that landed at the Szymany airport brought passengers and departed with only the crew. The last plane arrived at Szymany with no passengers and departed carrying five people. Data available at: http://www.hfhr.org.pl/cia/images/stories/SKAN%20DOKUMENTU.pdf.

169 Newspapers reported in 2010, quoting an unofficial source within the Prosecution Service, that the prosecutors conducting the investigation had collected evidence sufficient to prosecute top state officials in office during the period when the operation of the CIA prisons in Poland allegedly took place before the Court of State on the charges of committing war crimes (the offence under article 123 (2) of the Criminal Code). The above information was not confirmed by state officials.

170 The Prosecutor Service, though, for more than two years, refused to disclose, upon HFHR requests, information concerning the investigation, such as a confirmation of the existence of a document without disclosing its content, information on whether witnesses had been interrogated or whether a Report of International Committee of the Red Cross was included in the case files –information, of procedural, not of substantive nature. At the same time the Prosecutor Service did not accept the argument that the possibility of grave human right violations justified informing the public about the investigation.

171 For instance, the Prosecutor Service disclosed the date of commencing the investigation; that two men who maintain they were held and tortured in a secret detention center in Poland, were granted victim status. See Article "*Saudyjski więzień CIA otrzymał status poszkodowanego od polskiej prokuratur"*, Polish Press Agency, available at http://wiadomosci.gazeta.pl/Wiadomosci/1,80708,8574539,Saudyjski_wiezien_CIA_otrzymal_status_poszkodowanego.html; INTERRIGHTS and REPREIVE press release *Polish Prosecutor officially recognises Guantánamo prisoner Abu Zubaydah as a victim in Poland's CIA secret prison investigation; decision should allow former 'high-value detainee' to testify against his US torturers and their allies* available at http://www.interights.org/view-document/index.htm?id=609. Prosecutor Service also informed that in 2009, the Prosecutor's Office requested legal assistance from the American judicial authorities that was not granted due to national security or other relevant state interests. See letter of December 15,2010 available at http://www.hfhr.org.pl/cia/images/stories/Odpowiedz_Prokuratura_15_12_2010.pdf. The most comprehensive information on the course of the investigation – mentioning categories of persons that had been interrogated (without providing their names), the fact that the investigation concentrates on a

Taking into consideration declassification mechanisms and the fact that it is based, to a large extent, on the assertion that a document may be declassified by the same person who performed the classification, there is still a risk that when the case will be considered by the court, the court's hearing will not be open to public view, and the justification for court's judgment will be classified too. Assuming such a situation appears, the public will not be able to know the truth about the Polish involvement in the CIA rendition program. Also, it should be noted that serious human rights violations such as torture or illegal detention are linked to the case of Polish involvement in the rendition program. Therefore, from the perspective of national security, providing a comprehensive explanation of the issue might far more contribute to guaranteeing state security and state interest than leaving the case unsolved and not bringing it to the public's attention.

4. Significance of control mechanisms over classification law under PCIA 2010

The situation of excessive classification was detected on the grounds of PCIA 1999.[172] This appeared, *inter alia*, due to ineffective control procedures over the classification regime stipulated in the two acts – the Freedom of Information Act and the Protection of Classified Information Act.[173] The control procedure includes e.g. judicial review and control within the governmental branch agencies. When those mechanisms do not work properly, the consequences of excessive classification might have important impact on democracy.

The new PCIA 2010 brings improvements in the effectiveness of control mechanisms, however no radical changes. The PCIA 2010 does not introduce a system of control or supervision at the time of classification, an obligation to provide a justification or explanation of reasons to classify, it also does not stipulate that information must be classified by an administrative decision (this would facilitate judicial control). A positive change is, however, that PCIA 2010 introduces an enhanced, complex procedure to challenge abuses in classifying information within the branch agency, as it provides for an appeal procedure to higher administration bodies. However, the procedure is still limited, as does not stipulate an appeal to the court. As the superior in the branch agency will not always be able to effectively supervise and control other subordinated officials, judicial control appears inevitable and crucial. Further, in general, under Polish law the issue of judicial control over the classification regime and its scope is not settled yet and thus more likely it will be further developed and elaborated in case law.

The new PCIA 2010 undoubtedly provides for positive, important changes, but introduces provisions relying to a large extend on the discretion of public officials and on imprecise, not yet determined terms. This includes, inter alia, the new system of defining classified information based on yet undetermined terms not specifying clear guidelines as to how to classify and the new system of declassification, not supported by previous practice. It is thus important to provide state officials with enhanced, up-dated knowledge on classification to guarantee that they perform their tasks according to the law. That is why improving and broadening training requirements under PCIA 2010 should be valued positively. On the other

---

verification of flights landing in Poland – was disclosed by the Appellate Prosecutor Service in 2011, approximately three years after the commencement of investigation. See letter of February 4, 2011 available at http://www.hfhr.org.pl/cia/images/stories/odpowiedz_PG_4_02_2011.pdf.

172 Judgment of the Constitutional Tribunal indicated in the judgment of 15 October 2009, ref. no. K 26/08. See supranote 101.

173 Judgment of the Constitutional Tribunal,15.10.2009, ref. no. K 26/08.

hand, there are still some factors that remain room for possible incorrect classification or could be used as instruments to conceal abuses of power by authorities, including secret services. This is a lack of sanctions for excessive classification specified directly in the law on classified information, a lack of explicit prescription of information that should be disclosed or should not fall within the classification regime *ab initio*, a lack of a public interest override exemption. Therefore, the need of effective control procedures and judicial review as well as an effective mechanism of repression is highly desirable.

Taking into consideration the new law of classification provided by PCIA 2010, the question has arisen if its mechanisms and systems will bring radical changes in classification regime. As the law is in force since few months, the further practice will show what are the consequences of introducing more flexibility in the law, whether the control mechanism within the agency is effective and whether the new regulations will successfully prevent and eliminate the practice of excessive classification and deal with the abuses.