The Protection of Classified Information in Western Europe and the USA

István László Gál*

Abstract

Regulations for the protection of classified information are extremely similar in developed Western countries. The XXI. century, these states are struggling in a close political and military alliance to meet the security policy challenges of the present and the future. For this reason, the mutual protection of their diplomatic and military secrets plays a key role. The present study presents the secrecy systems of three of NATO's most important member states, primarily in terms of criminal law regulation.

Keywords: *classified data, secrecy, NATO, national security, press, NSA, Five Eyes, need to know*

I. The concept of classified information

In my view, secrecy, in the broadest sense, is a category inherent in human nature that appears at a certain quality of the process of becoming human. A secret is anything that only a certain number of people know about, and whose secrecy for a specified period of time, regardless of its value, is in the interest of one or more people or society, and the holder of the secret has taken appropriate measures to keep it secret. If we examine the secrecy of secrecy, which is also protected by law, as a kind of special legal relationship, we can make the following conclusions about it: – always present in humans, – an absolute legal relationship (everyone is obliged to tolerate that the secret owner only shares the secret with whom he wishes), – always exists within a specified time frame, – its subject-matter is information of a valuable nature which requires and deserves legal protection, and – the loss, destruction, disclosure or making available to an unauthorized person of this information has legal consequences governed by different rights. After defining the general concept of secrecy, we turn to the examination of state secrecy, first also in general. The three indispensable components of the concept of state are territory, population, and sovereignty. Preserving the security and integrity of all three essential components today is closely correlated with the ability and efficiency of the state to preserve information whose disclosure or acquisition by unauthorized persons or bodies could harm or jeopardize the legitimate interests of the state. Already Max Weber points out, every bureaucracy strives to strengthen the sense of superiority of its members with professional knowledge by

* Phd. Head of Department, full professor, University of Pécs, Faculty of Law, Department of Criminal Law. Contact: gal.istvan@ajk.pte.hu.

keeping their knowledge and intentions secret. The bureaucratic administration always strives to be the "administration of secret meetings" as much as possible, hiding its knowledge and actual activities from possible criticism.

The concept of "official secret" is a specific invention of the bureaucracy, which is why it is also fanatically defended by the bureaucracy[1]. Other types of secrets, such as economic secrets, can be conceived as personal secrets, but one of the distinguishing features of state secrets is that they are of a social nature, directly or indirectly affecting the security of the state, and therefore inconceivable only as personal secrets. Nowadays, the developed legal systems use the category of "classified data" instead of the concept of state secrets. Classified data is, in the most general terms, any information that a state or group of states considers to be sensitive in some way and which is therefore subject to an obligation of confidentiality based on national, regional or even international security needs. Access to classified information is restricted by law or regulation, and misuse can often result in criminal sanctions. A security certificate is usually required to manage or access classified information. This can typically be issued after a person's security check. Classified data typically has several hierarchical levels in each legal system, and access to them usually requires different levels of security requirements. The classification level of the data is determined in the framework of the qualification procedure[2]. These characteristics are usually found in the regulations of all countries, but the specific practice and terminology of course differs from country to country. In order to one of the secret type be classified as classified information today, it must fulfill the following requests:

- there is at least one public interest that can be protected by the rating and in the course of the procedure the rating agency has ascertained that the misuse of the data in question directly harms or threatens the public interest that can be protected by the rating,
- conducted by an authorized person,
- a qualification procedure that fully complies with the formal requirements, which qualifies the data for a specified period of time[3].

The appearance of classified information may also vary in practice:

- classified data recorded or transmitted by a data carrier;
- written information, classified data;
- an object or technical device carrying classified information;
- classified information, procedures or knowledge presented in an intangible form;
- finally, there is classified information provided orally[4].

According to the tasks of the application level of information protection, the protection system of classified data includes the following elements: physical protection,

---

[1] M. Weber, *Essays in sociology* [Szociológiai tanulmányok] pp. 233-234 (H.H. Gerth & C. Wright Mills trans. and eds., 1946), *apud* H. Kitrosser, *Classified information leaks and free speech*, University of Illinois Law Review no. 3/2008, p. 889.

[2] https://www.definitions.net/definition/classified+information (accessed on 21.04.2020).

[3] L. Szőke Gergely, *Gondolatok a hazai titokvédelmi szabályozás rendszeréről* [Thoughts on the system of Hungarian secrecy regulations], JURA no. 2/2018, p. 253.

[4] Z. Kuris, E. Pándi, *Komplex információbiztonság megvalósítási lehetőségeinek megközelítése* [Approaching the possibilities of implementing complex information security], Hadmérnök no. 2/2009, p. 312.

hardware and software, as well as encryption, IT protection of transmission paths, protection against compromising radiation, document protection, personal protection, and procedure protection as well[5].

The characteristics of classified information to be protected in the broadest sense may be the following:

- confidentiality (information can only be accessed by an authorized person);
- authenticity (the characteristic of the information that represents the originality);
- availability (those entitled to it will have access to the information in accordance with the provisions of the relevant regulations);
- integrity (a properly functioning information system represents the data in an appropriate form)[6].

II. United States of America

In the United States, a number of laws and regulations govern the qualification process. In the 1980s, at the initiative of President Reagan, a comprehensive regulation was established on the classification and protection of information relevant to national security[7]. The regulation defines national security as the protection of the national and foreign policy interests of the United States. It defined three rating levels according to a damage-based rating system: top secret, secret, and confidential[8].

President George W. Bush was prone to intensive encryption before September 11, 2001, but this trend intensified in the years that followed. Thus, among others, President Bush set up a secret military court after 9/11, expanded the scope of closed court hearings, further widened the executive's special powers, widened the protection of classified information in court proceedings, banned access to former presidents' files, congressional requests refused to release documents requested under the NSA, kept the NSA's U.S. citizenship surveillance program secret, and in many cases reclassified previously declassified documents. The number of classified data in the United States showed an upward trend in those years: 8.6 million in 2001, 11.3 million in 2002, 14.2 million in 2003, and 15.6 million in 2004[9]. This is already considered by American experts to be a lot, although comparing the population with the Hungarian data, more than twice as much qualified data is generated in Hungary today, with an intensity ratio of 1,000 inhabitants. However, the U.S. legislature also considers the number of its own classified data to be excessive, so a law was passed in 2010 to reduce[10] over-classification. Section 2 (3) of this Act states: "An over-classification

[5] K. Kassai, *Az információvédelem rendszerszintű feladatai* [System-level tasks of information protection], http://193.224.76.2/downloads/konyvtar/digitgy/20014/tartalom.html (accessed on 2020.04.30).

[6] Z. Kuris, E. Pándi, cited, p. 312.

[7] Exec. Order No. 12, 356, 3 C.F.R. 166 (1983).

[8] B.E. Fein, *Access to Classified Information: Constitutional and Statutory Dimensions,* William and Mary Law Review no. 5/1985, p. 807.

[9] D.A. Silver, *National Security and the Press: The Governments ability to Prosecute Journalists for the Possession or Publication of National Security Information* Communication Law and Policy 13(4)/ 2008, p. 450.

[10] Reducing Over-Classification Act [A túlminősítés csökkentéséről szóló törvény] (https://www.congress.gov/111/plaws/publ258/PLAW-111publ258.pdf (accessed on 30.08.2020).

causes significant confusion as to what information can be shared with, and also has a negative impact on the flow of information within the federal government and between individual Member States and local authorities, as well as the private sector". The concept of classified information is currently contained in Enforcement Order No. 13526, signed by President Obama and effective in the United States on December 29, 2009. It defines classified information as information that must be retained in the interests of national security "in order to protect the security of our citizens, our democratic institutions, our country and our relations with foreign nations"[11]. According to a textbook definition, classified information is "news that is so sensitive that its dissemination may be restricted to persons who meet certain specific security requirements and who have a clear need for that information in order to perform their duties. Each organization develops its own rating system, but in the United States, all agencies in the federal intelligence community must adhere to the rules set forth in the implementing instructions, most recently approved by President Obama"[12].

In October 2011, President Obama issued Implementing Decree No. 13587 on "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Protection of Classified Information". It includes a nationwide program (insider risk program) designed to prevent, detect, and mitigate internal risks, including the protection of classified information from unauthorized disclosure, taking into account the levels of risk and individual needs of each agency[13].

The regulation of classified information in the United States is the sole responsibility of the federal government. Although individuals or organizations may be granted access to classified information in certain cases, such information is always the property of the federal government under applicable U.S. law. The rating level reflects the degree of national security risk: the higher the risk, the higher the rating level[14]. The rating level is indicated at the bottom and top of the page on that document, but only the rating level is listed on the document, not the rating name, position, and term of protection. You can classify a document in smaller sections at different levels, or you can specify the classification level for that paragraph or figure by paragraph[15].

Access to classified information is based on the principle of the necessary knowledge[16], ie a person holding a "Top Secret" personal security clearance may only access top secret information that is relevant to his or her own work. These limitations are intended, among other things, to protect resources and methods[17].

In the first two decades of the XXI. century, the issue of state secrets has been the subject of extensive debate in the United States. One of the central issues in the debate

---

[11] Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009); *ld még: The President Executive Order 13526.*

[12] C.J. Jensen, D.H. McElreath, M.Graves, *Bevezetés a hírszerzésbe* [Introduction to Intelligence], Antall József Tudásközpont [József Antall Knowledge Center], Budapest, 2017, p. 205.

[13] J.K. Elsea, *The Protection of Classified Information: The Legal Framework*, Congressional Research Service 18 May 2017, p. 19.

[14] B.M. MacKay, *The use of classified information in terrorism trials*, Southern Illinois University Law Journal Vol. 42/2017, pp. 67-68.

[15] Marking Classified National Security Information as Required by Executive Order 13526, 4 January 2018.

[16] Exec. Order No. 13526 § 4.1(a), 75 Fed. Reg. 707 § 4.1(a).

[17] A. Rossmiller, *Adjudicating Classified Information,* St. John's Law Review, vol. 85, no. 4/2011, p. 1301.

is what should be done with government employees leaking classified information to the press, who most often want to inform the public about government action. Whether their act is unlawful, unconstitutional or, where appropriate, even justified in order to enforce the controlling role of the public[18].

However, freedom of the press is a very important constraint on the practical application of classified data regulations in the country. In 1971, the United States Supreme Court ruled against the famous New York Times et al. United States case ruled that the press in some cases may publish classified information with impunity: this was the famous Pentagon Files lawsuit.

The Supreme Court rejected the government's position that 7,000 classified documents related to the Vietnam War should not have been released by 6-3 votes. The court argues that only a free press can uncover abuses by the government and prevent the government from misleading people. In any case, the stakes were high, and under the laws in force, decades of imprisonment could have been imposed. Nowadays, many laws and court decisions have been made that could lead to criminal prosecution of a journalist who publishes classified information with the intent to harm the United States. However, although journalists working for the largest, leading newspapers have been published on a number of occasions in recent decades, no criminal proceedings have been instituted, according to a 2008 study[19].

A 2019 study confirms this finding ten years earlier: media workers are not being prosecuted in the United States, even today, solely against government officials who leak classified information. Snowden could face up to 30 years in prison until he was charged with the newspaper The Guardian, even though they also broke the law. One reason for this, according to the author, may be that the press has special rights based on the principle of freedom of the press or because of its role, as many now consider the media to be the fourth branch of power. The second argument is that leaks cause more damage than the press. The author notes that current U.S. criminal practice is inconsistent: prosecutors should prosecute both, or neither[20].

Under President Obama, five prosecutions have been filed against incumbent and former government officials for violating nationally sensitive information in the press under the espionage law. In one such case, a journalist was put under pressure to testify and reveal the source of the information he published. Attempts were made to persuade the journalist to testify on the grounds that he was the only witness to the crime in which he orally received classified information from his source, that is, a government official. This new practice is significantly different from the previous one, and some authors believe it threatens the right of U.S. citizens to know what their government is doing[21].

It should be noted here that "leakage", ie the disclosure of classified information during the term of protection in the press or on the Internet, is not clearly a negative or positive phenomenon in the literature. In this regard, the UN Johannesburg Principles

---

[18] R. Clark, *Classified Information in the Public Sphere: An Examination of Legal Issues Surrounding the NSA Leaks,* (2013) 41:4 DttP: Documents to the People, p. 7.

[19] D.A. Silver, cited, pp. 447-483.

[20] D. Mokrosinska, *Why Snowden and not Greenwald? On the Accountability of the Press for Unauthorized Disclosures of Classified Information,* Law and Philosophy no. 39/2020, pp. 203-238.

[21] M.H. Halperin, *Criminal Penalties for Disclosing Classified Information to the Press in the United States,* https://www.right2info.org/resources/publications/Halperin_CriminalPenaltiesforDisclosingClassifiedInformationtothePressintheUnitedStates.pdf (accessed on 22.08.2020).

on National Security[22], Freedom of Expression and Access to Information contain the following in Principle 15: "General Rules for Disclosure of Confidential Information No one shall be penalized for reasons of national security for disclosing information if (1) the disclosure is not likely to have a real effect on the legitimate interests of national security, or (2) the public interest served by disclosure outweighs the harm caused by disclosure".

In my view, this can only be accepted in a very narrow, very exceptional way. In general, the risk of unauthorized disclosure of classified information during the term of protection is much greater than the benefit to the public interest of disclosure in an open, democratic society. Nonetheless, we must acknowledge that such a case may occur. Examples of this can be found in the case of major social changes, such as a change in the political and economic system, as we will see in the historical section. The position of Károly Kassai is in line with this, according to which opinions that the law should not hinder the work of investigative and fact-finding journalists and that journalists should not be prosecuted if classified information is disclosed are completely devoid of professionalism[23].

Also of great interest in the relevant United States legislation is the provision for the reclassification of data that has already been released and declassified. This is called "retroactive rating" or "downgrading" by U.S. regulations. The legitimacy of the provision has been a concern in the past, but in the age of the Internet, it is already completely questionable, as a study published a few years ago suggests. Once something has been uploaded to the Internet as public material, it is almost impossible to remove it from there. The only consequence of the provision is that any public discourse regarding such reclassified data will become impossible[24].

The United States has a strong culture and literature on confidentiality, and they also pay close attention to training employees of organizations handling classified information during training. A good example of this is one of the Ministry of Energy's educational materials, which emphasizes the need to prepare in advance about how to respond during public hearings, including press conferences, lectures, and other events. The English term "No comment" is a worldwide, popular answer, but its use should be avoided because it would confirm that the respondent may be in the background of the question, and in the case of a question to be decided, such an answer may infer the content of the classified information. Therefore, you should not choose any of the following answers:

Are there nuclear weapons in country x? " No".

Is there a nuclear weapon in country y? "No".

Are there nuclear weapons in country x? "No comment".

The correct use of "No comment", on the other hand, is as follows*: „Are there nuclear weapons in country x?"* We recognize that nuclear weapons are or have been in many countries. I cannot provide more detailed information on the location of nuclear

---

[22] The Johannesburg Principles on National Security, Freedom of Expression and Access to Information U.N. Doc. E/CN.4/1996/39.

[23] K. Kassai, *A Magyar Honvédség információvédelmének – mint a biztonság részének –* feladatrendszere [Task system of information protection of the Hungarian Armed Forces as a part of security], Doctoral (PhD) dissertation, Budapest, 2007, p. 7.

[24] J. Abel, *Do you have to keep the government's secrets? Retroactively classified documents, the first amendment and the power to make secrets out of the public report,* University of Pennsylvania Law Review Issue 163, no. 4/2015, pp. 1038-1039.

weapons. " And if the person in possession of the classified information is talking to his friends, according to the educational material, be humorous, articulate, and change the subject as soon as possible[25].

In summary, breaches of classified information are referred to in the U.S. literature as "unauthorized disclosure". There are four typical types:

1. the deliberate leakage of classified information (mainly by government officials, primarily to the media),
2. outflow of classified information (usually through electronic data transmission systems, whether intentionally or negligently, such as an e-mail message, classified information is also sent between open data),
3. espionage,
4. Inadequate security measures (in this case, the security breach of classified information is typically negligent, such as someone forgetting a page containing classified information in a copier)[26].

In the United States, federal criminal law includes the most serious federal offenses, but for less serious offenses, each state has created its own criminal code. In addition to all this, military criminal law and Native American reserves have their own criminal law, meaning that there are more than 500 systems of criminal law in force in the country, and it is almost impossible for a university professor of criminal law to review and understand them. However, the regulation of misuse of classified information is easy to review, as it is a federal crime. A federal employee or official who makes classified information intentionally inaccessible without permission is punishable by one year's imprisonment and a fine of up to $ 1,000. The penalty is imprisonment for up to 10 years and a fine of up to $ 10,000 if that employee or officer knowingly transfers classified information to a person who is known to work for a foreign government. The same penalty applies if a federal employee or official or anyone else discloses classified information, makes it available to an unauthorized person, or uses classified information used by the United States, encryption, and intelligence to the detriment of the United States. Finally, a person entitled to use classified information is punishable by up to 15 years' imprisonment if he or she intentionally commits the offense and, as a result, the identity of one or more undercover agents is disclosed. Other classified cases of the offense are all related to the disclosure of classified information about covered agents, with a maximum penalty of 15 years imprisonment[27].

One of the biggest scandals over the misuse of classified information in recent years has erupted in the 2016 U.S. presidential election campaign in America. Donald Trump and Hillary Clinton once engaged in a fierce battle of words during the campaign over alleged misuse of classified information by Hillary Clinton during the 2016 presidential election campaign. Hillary Clinton told CNN about the illegal transfer of classified information: "It was a mistake that I used my personal email. I'm sorry". Then he reacted again to the topic in the presidential debate on October 9, 2016: "It is terribly good that not a man of temperate Donald Trump is controlling our country" Donald Trump replied, "because you would be in prison by then". Incidentally,

[25] https://fas.org/sgp/othergov/doe/gen-16-rev2.pdf (accessed on 15.08.2020).

[26] https://www.cdse.edu/documents/student-guides/IF130-guide.pdf (accessed on 15.08.2020).

[27] J.K. Elsea, *The Protection of Classified Information: The Legal Framework,* Congressional Research Service 2017, pp. 14-15.

no criminal proceedings have been instituted in the case to date, but an assessment of this circumstance would already be a political decision.

III. United Kingdom

In Europe, the UK is one of the most important geopolitical and military factors, so it's a good idea to briefly review its privacy regulations. The UK rating system is simple and easy to review, currently using only three rating levels: Official, Secret, Top Secret. The Official rating level is commonly used for most information created or processed by the public sector. such as economic data, which could have harmful consequences if lost, stolen or published in the media. At the Secret classification level, highly sensitive information is protected for which enhanced security measures are warranted. For example, data the disclosure of which could seriously damage military defense capabilities, international relations, but also data related to the fight against organized crime. The Top Secret rating level is the highest. This protects the Queen's Government's most sensitive information, the data that requires the highest level of protection against the most serious threats. For example, data may be included where disclosure or unauthorized acquisition by a person could endanger life or endanger the security or economic well-being of the country or Allied nations. Access to classified information is also based on the need-to-know principle under the British system. However, the regulation also allows for the application of the need-to-share principle in specific situations, ie the possibility of sharing classified information with persons who do not have the appropriate personal security clearance, for example where immediate action is required to protect life or commit a serious crime. to prevent the commission of such offenses. In such circumstances, a reasonable approach under UK law should be followed: if time permits, individual alternatives should also be considered and steps taken to protect the source of the information[28].

The UK is also a member of the Five Eyes intelligence community, which is still operating in SIGINT[29] today with the participation of five states, with a high degree of efficiency. The Five Eyes came into being during World War II. The United States and Great Britain also worked closely on SIGINT during the war to effectively intercept enemy communications. The British hacked Germany's super-secret Enigma system, and the United States hacked Japanese encryption. This cooperation was institutionalized in 1946 by an agreement between the United Kingdom and the United States. In intelligence against the Soviet Union in the ensuing Cold War, it was already considered necessary to maintain and strengthen intelligence cooperation in peacetime, in order to anticipate potential conflicts. Canada joined the alliance in 1948, and Australia and New Zealand in 1956, creating a global intelligence-sharing organization[30]. The relationship between members of the Five Eyes community is now so close that

[28] Government Security Classifications (Kormányzati minősítések) May 2018, p. 4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf (accessed on 10.07.2020).

[29] SIGINT, or Radio Electronic Signaling, refers to the interception and processing of electronic communications signals.

[30] J.E. Dailey, *The Intelligence Club: A Comparative Look at Five Eyes*, Journal of Political Sciences & Public Affairs no. 5/2017, p. 1.

participating governments are putting requests from the United States National Security Agency, or NSA, to protect the privacy of their own citizens[31].

IV. Germany

In Germany, the protection of classified information under the current legislation includes any measure by which a public body may declare certain facts, objects or knowledge to be classified information in the context of a specific procedure. Many provisions of German federal and state law govern the subject of classified information. The legal basis for the security of the federal state is primarily the Security Control Act (SÜG) and related administrative regulations. Confidentiality also has personal and physical requirements in Germany, in line with international practice. The key concept in German privacy law is classified information (V*erschlusssache*). Four rating levels are used:

- *VS-Nur für den Dienstgebrauchs (VS-NfD)* – for service use only (this corresponds to the restricted distribution rating level),
- *VS-Vertraulich (VS-Vertr.)* – confidential,
- *Geheim (Geh.)* – secret, and
- *Streng Geheim (Str. Geh.)* – top secret.

The German system is also a damage-based rating system, determining the potential hazards assigned to each rating level in almost the same way as the Hungarian regulations. Classified data may only be created and managed for the time and at the level required. The German legislation also emphasizes the principle of need-to-know (*'Kenntnis nur, wenn nötig'*) in relation to access to classified information[32].

All in all, it can be stated that perhaps the closest is the German regulation to the Hungarian, we most likely used it as one of the examples during the codification. German criminal law contains criminal provisions in other sectoral laws, but the most important part of criminal law (*Kernstrafrecht*) can be found in the German Criminal Code, and the ancillary criminal law provisions (*Nebenstrafrecht*). According to the German legislature, the protection of classified information is so important that:

1) the Criminal Code contains all relevant criminal law provisions,
2) several facts protect the legal objects related to the classified information, and
3) these provisions can be found relatively at the beginning of the Special Part, in the second chapter, and the legislator also indicates their importance. The facts related to the protection of classified data can be found in the second chapter of the German Criminal Code, under the title "Trafficking and endangering the external security of the state". In doing so, German criminal law clearly states that it considers these behaviors to be crimes against the state that endanger national security.

Section 93 contains the definition of state secrets:

(1) *State secrecy is any fact, object or knowledge to which a limited number of persons have access and which must be kept secret from foreign powers in*

[31] G. Greenwald, *A Snowden-ügy. Korunk legnagyobb nemzetbiztonsági botránya* [The Snowden case. The biggest national security scandal of our time], Hvgkönyvek, Budapest, 2014, p. 164.

[32] M. Vogt, D. Wahlen, *Geheimschutzrecht Voraussetzungen und Folgen der Einstufung von Informationen als Verschlusssachen,* Deutscher Bundestag [Protection of secrets Prerequisites and consequences of the classification of information as classified information, German Bundestag], WD 3-3010-036/15. 2015, pp. 4-9.

order to avoid any serious threat to the external security of the Federal Republic of Germany.

(2) *Information which infringes the interests of a free, democratic state, the constitutional order of the Federal Republic of Germany or of the contracting parties to international arms control agreements is not a state secret*. The German legislation is interesting in that it states *expressis verbis* what cannot be classified as a state secret, ie what should not be classified. In this respect, this is the most democratic regulation I have examined, as in the event of such anti-democratic classified information, citizens are protected by the Criminal Code itself if they are prosecuted for disclosure.

Section 94 of the Criminal Code contains the provisions of the betrayal:

(1) *Who discloses a state secret to a foreign power or one of its representatives* or *is making a State secret available to an unauthorized person for the purpose of harming the Federal Republic of Germany or gaining an advantage over a foreign power shall be punishable by a term of imprisonment of one year or more.*

(2) In particularly serious cases, the sentence shall be imprisonment for a term of imprisonment of at least five years.

A particularly serious case is usually when the perpetrator *1. Abuses his official position in which he would be bound by professional secrecy;* or *2. Poses a particularly serious threat to the external security of the Federal Republic of Germany by committing the offense.*

Another important fact related to the protection of classified data of the German Criminal Code is the offense of disclosure of state secrets in 95 §:

(1) *Whoever makes or discloses a state secret classified by an official body to an unauthorized person, thereby endangering the external security of the Federal Republic of Germany with the possibility of serious harm, shall be punishable by a term of imprisonment of six months to five years.*

(2) An attempt to commit a criminal offense shall be punishable.

(3) In particularly serious cases, the penalty shall be one to ten years imprisonment.

With regard to the concept of a particularly serious case, the second sentence of Section 94 (2) shall apply. In addition to these, there are eight other facts about the extremely thorough, casuistic system of criminal law rules. Studying these, it may occur to us that extremely thorough, strict criminal law provisions may have been the criminal means of combating East German intelligence at the time, and one of the reasons for the strict regulation may have been the decades-long secret service struggle between the two former German states.

References

Abel, J., *Do you have to keep the government's secrets? Retroactively classified documents, the first amendment and the power to make secrets out of the public report,* University of Pennsylvania Law Review Issue 163, no. 4/2015.

1. Clark, R., *Classified Information in the Public Sphere: An Examination of Legal Issues Surrounding the NSA Leaks,* (2013) 41:4 DttP: Documents to the People.

2. Dailey, J.E., *The Intelligence Club: A Comparative Look at Five Eyes*, Journal of Political Sciences & Public Affairs no. 5/2017.

3. Elsea, J.K., *The Protection of Classified Information: The Legal Framework*, Congressional Research Service 18 May 2017.

4. Elsea, J.K., *The Protection of Classified Information: The Legal Framework,* Congressional Research Service 2017.

5. Fein, B.E., *Access to Classified Information: Constitutional and Statutory Dimensions,* William and Mary Law Review no. 5/1985.

6. Government Security Classifications [Kormányzati minősítések] May 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf (accessed on 10.07.2020).

7. Greenwald, G., *A Snowden-ügy. Korunk legnagyobb nemzetbiztonsági botránya* [The Snowden case. The biggest national security scandal of our time], Hvgkönyvek, Budapest, 2014.

8. Halperin, M.H., *Criminal Penalties for Disclosing Classified Information to the Press in the United States,* https://www.right2info.org/resources/publications/Halperin_CriminalPenaltiesforDisclosingClassifiedInformationtothePressintheUnitedStates.pdf (accessed on 22.08.2020).

9. https://fas.org/sgp/othergov/doe/gen-16-rev2.pdf (accessed on 15.08.2020).

10. https://www.cdse.edu/documents/student-guides/IF130-guide.pdf (accessed on 15.08.2020).

11. https://www.definitions.net/definition/classified+information (accessed on 21.04.2020.

12. Jensen, C.J., McElreath, D.H., Graves, M., *Bevezetés a hírszerzésbe* [Introduction to Intelligence], Antall József Tudásközpont [József Antall Knowledge Center], Budapest, 2017.

13. Kassai, K., *A Magyar Honvédség információvédelmének – mint a biztonság részének* –feladatrendszere [Task system of information protection of the Hungarian Armed Forces as a part of security], Doctoral (PhD) dissertation, Budapest, 2007.

14. Kassai, K., *Az információvédelem rendszerszintű feladatai* [System-level tasks of information protection], http://193.224.76.2/downloads/konyvtar/digitgy/20014/tartalom.html (accessed on 2020. 04. 30).

15. Kuris, Z., Pándi, E., *Komplex információbiztonság megvalósítási lehetőségeinek megközelítése* [Approaching the possibilities of implementing complex information security], Hadmérnök no. 2/2009.

16. MacKay, B.M., *The use of classified information in terrorism trials*, Southern Illinois University Law Journal Vol. 42/2017.

17. Mokrosinska, D., *Why Snowden and not Greenwald? On the Accountability of the Press for Unauthorized Disclosures of Classified Information,* Law and Philosophy no. 39/2020.

18. Reducing Over-Classification Act [A túlminősítés csökkentéséről szóló törvény] (https://www.congress.gov/111/plaws/publ258/PLAW-111publ258.pdf (accessed on 30.08.2020).

19. Rossmiller, A., *Adjudicating Classified Information,* St. John's Law Review, vol. 85, no. 4/2011.

20. Silver, D.A., *National Security and the Press: The Governments ability to Prosecute Journalists for the Possession or Publication of National Security Information* Communication Law and Policy 13(4)/2008, p. 450.

21. Szőke Gergely, L., *Gondolatok a hazai titokvédelmi szabályozás rendszeréről* [Thoughts on the system of Hungarian secrecy regulations], JURA no. 2/2018.

22. The Johannesburg Principles on National Security, Freedom of Expression and Access to Information U.N. Doc. E/CN.4/1996/39.

23. Vogt, M., Wahlen, D., *Geheimschutzrecht Voraussetzungen und Folgen der Einstufung von Informationen als Verschlusssachen Deutscher Bundestag* [Protection of secrets Prerequisites and consequences of the classification of information as classified information, German Bundestag], WD 3-3010-036/15. 2015.

24. Weber, M., *Essays in sociology* [Szociológiai tanulmányok] pp. 233-234 (H.H. Gerth & C. Wright Mills trans. and eds., 1946), *apud* H. Kitrosser, *Classified information leaks and free speech*, University of Illinois Law Review no. 3/2008.