Current issues of espionage in the new Hungarian criminal law

PhD. István László Gál[1]
Full professor
Head of department of Criminal Law
Faculty of Law
University of Pécs
Hungary

Abstract

It is not an easy task to prove beyond reasonable doubt the commitment of espionage with the help of the toolbox of criminal law. Until now, in the Hungarian legal practice only such cases happened when the perpetrator gave classified information to the foreign organization (as well).

Nowadays we have to count with national security risks arising from forwarding information collected, classified, analysed and concluded through opened sources (such as Internet, national and local mediums) that can be available for foreign powers or organisations (counter-interested secret services). The question arose during a criminal procedure whether such action can be classified as criminal act of espionage according to the Criminal Code, or going further: can it be a crime according to Hungarian criminal law? This article aims to answer this question.

Key words*: crime, OSINT, spy, espionage, criminal law.*

1. Introduction

"Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime."[2]

According to the official statistics, hardly any case of espionage comes to cognizance of the authorities in Hungary. No wonder. On the one hand, it is true that just a very few espionage become known before the authorities since agents are not some amateur criminals, they take (criminal) actions as part of high conspiracy. On the other hand, it is not really effective to call to account criminally a caught agent, or if it is, then it

[1] Contact: gal.istvan@ajk.pte.hu.

[2] Klass v. Federal Republic of Germany case: European Court of Human Rights: Judgement (Strasbourg 6. September 1978. Council of Europe Reports, 1978. p. 18).

might be more practical to charge such agent with a crime against public order (which is usually easy to do because they commit a complex illegal series of acts) and sentence this person as a convict for crimes against public morality turpitude. By so doing possible international diplomatic complications can be avoided as well. In certain cases, „turning back" the caught agent can serve more the national security interest of a country, meaning to employ such agent as a double agent, whereby the secret service of the other interested party can be misled. Besides to replace agents caught abroad with Hungarian agents can make it necessary to not to institute criminal procedures. However, sometimes, even in Hungary agents are brought to criminal justice. With a criminal procedure an international propaganda can be created which can render the bargaining position of the country better, if the exchange of agents of Hungarian interest comes up.

"The protection of national security requires the repression of espionage even in a democratic society. Consequently, counterespionage by secret surveillance constitutes a necessary restriction of freedom of information for the protection of national security."[3] Nowadays we have to count with national security risks arising from forwarding information collected, classified, analysed and concluded through opened sources (such as Internet, national and local mediums) that can be available for foreign powers or organisations (counter-interested secret services). The question arose during a criminal procedure whether such action can be classified as criminal act of espionage according to the Criminal Code, or going further: can it be a crime according to Hungarian criminal law? This short study aims to answer this question.

2. The concept and interpretation of OSINT

The concept of intelligence gathering consists of the following areas according to the traditional classification of the secret service[4]:

a) HUMINT (*Human Intelligence*): In order to collect secret and private information every state owened and private secret service establishes human sources abroad and with a foreign interest at home. The range of human sources starts from occasional information sources to institutionalised (foreign agents) co-operation. The secret circle of connections consists of persons who already have or can create possibilities to obtain foreign secrets.

b) *TECHINT (Technical Intelligence):* Technical Intelligence is a comprehensive designation that ranges from the traditional tools of secret service (*e.g.* tapping the phone) to intelligence gathered through electronic devices and procedures created by scientific methods. The concept of technical intelligence includes gathering information from telecommunication channels and data communication systems, furthermore from attacking cyphering and office equipment by technical tools and methods. Intelligence gathering from telecommunication channels usually realized by attacking international – mainly foreign governmental- telecommunication channels. Cyphering and office equipments are attacked by receiving and processing certain concomitants that is resulted from their functioning or which were induced by certain technological intervention, furthermore the attack can be the restoration of open information on the

[3] John Kish, *International Law and Espionage*, Kluwer Law International, Netherlands, 1995. p. 29.

[4] http://www.mkih.hu/hivatal_hirszerzes.shtml, accessed 2.10.2011.

attacked systems by combining the application of various scientific methods and technical tools.

c) *OSINT (Open Source Intelligence):* secret services are watching the open source intelligence as well. Open sources of information: press releases, programmes of mass media, open databases and information systems and the internet. The necessary information must be filtered off this mass of facts.

d) *International Co-operation:* certain national secret services take part in several multilateral secret service so-operations. Our partner relations are usually based on reciprocity, mutual interest and equal rights.

From among the above mentioned areas of espionage, the OSINT[5] deserves a more thorough introduction. In a general term, the OSINT deals with the search, analysis, collection, systematization and evaluation of information that can be gathered from not classified sources with legal tools but which constitute assets for the intelligence services. This type of data collection uses sources that are accessible for anyone (Internet, written and online media, commercial databases). The gathering, analysis and evaluation of unconcealed information are nut traditional tasks of the intelligence services[6], but such information is searched for intentionally[7], it is differentiated and identified individually[8], filtered and which is going to be used subsequently.[9]

The OSINT plays a great role in military intelligence as well: „The Open Source Intelligence – OSINT has grown to be a modern type of intelligence gathering. It shall mean the analysis of newspapers, radio and television broadcasts, and mostly the expedient use of the news on the Internet. The processing of open source intelligence – as always in history -, if it is executed in a professional manner and with an appropriate knowledge, can be of a great value. In the 70's there were already official estimations saying that 60-70% of the information of the intelligence services was collected from open source intelligence."[10]

3. The regulation on espionage in the new Hungarian Criminal Code

The new Criminal Code of Hungary, Act C of 2012 determines the crime of espionage basically the same as it was in Act IV of 1978:

---

[5] Open Source Intelligence. Its definition and types can be found in scientific literature on the Internet. See, *e.g.*, the NATO OSINT *Handbook,*
http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf, accessed 30.12.2013.

[6] See in detail: Lévay Gábor: *OSINT (OPEN SOURCE INTELLIGENCE), Nyílt információs hírszerzés.* Zrínyi Miklós *Nemzetvédelmi Egyetem, egyetemi jegyzet* http://osint.gportal.hu/gindex.php?pg=20201555&nid=3320934, accessed 29.12.2013.

[7] The secret service agency searches for information expediently which it has an interest in, and are necessary for the analysis, evaluation and the determination of assessment and prospective developments.http://osint.gportal.hu/gindex.php?pg=20201555&nid=3320934 accessed 29.12.2013.

[8] For the sake of fast retrieval and evaluation of the truthfullness and reliablity of information, the author, place of invention, subject matter, keywords, references to other sources are also recorded.http://osint.gportal.hu/gindex.php?pg=20201555&nid=3320934 accessed 29.12.2013.

[9] Izsa Jenő, *Nemzetbiztonsági alapismeretek (A titkosszolgálatok működése)* [*Fundamentals of national security (Operation of secret services)*] ZMNE, Kossuth Lajos Hadtudományi Kar, Budapest, 2009, pp. 49-50.

[10] Hajma Lajos, *A katonai felderítés és hírszerzés története (egyetemi jegyzet) [The history of military intelligence (lecture notes)]* ZNME Budapest, 2001, p. 212.

Section 261

"(1) Any person who engages in gathering intelligence for a foreign power or foreign organization against Hungary is guilty of a felony punishable two to eight years of imprisonment.

(2) Any person who commits the espionage defined in (1) by disclosing top secret information shall be punishable by five to fifteen years of imprisonment.

(3) Any person who engages in preparations for espionage shall be punishable by one to five years of imprisonment.

(4) Any person who – before having performed any further act of espionage – reports his or her engagement or undertaking to the authorities or the relevant state bodies and fully discloses his or her foreign contact shall not be liable for prosecution for offering or undertaking to participate in espionage operations".

The legal object of espionage is the (constitutional) order of the state according to the Fundamental Law (Constitution) of Hungary, explicitly states on the security of the state and every political, military, social or economic interest of our country.

The object of perpetration can be any kind of data that is suitable to be used against the interest of Hungary. The aggravated case of espionage determines a specific object, namely data that is classifies as top-secret information.

The act that establishes the commitment of this crime: intelligence work which includes the following areas according to the formerly introduced traditional classification[11]: HUMINT, TECHNINT, OSINT, international co-operation.

Criminal textbooks after the turn of the millennium interpret the notion of intelligence work in a wider sense: Nowadays, espionage is not limited to secret intelligence gathering and supplying, but it consists of far extensive activities. It includes actions like for example finding the adequate person for the intelligence service, compromising the target person, operating residency for intelligence work. The modern intelligence services have overcome the traditional forms of espionage (recruitment, recording of the statement for recruitment), and they choose looser forms of communication to keep in touch. The statement of facts of this crime renders punishable basically the secret intelligence gathering acts and the promoting thereof."[12]

The open and secret methods of data collection complete each other, secret information gathering follows the open source information collection in order to supplement and complete the knowledge collected in an open manner.

The two basic types of espionage are the offensive espionage and the aversion.

The legal methods of offensive espionage are shadowing the media and internet, analysing the information accessible from open databases (register of companies, register of title deeds, etc.). The proper classification, evaluation and analysis of available mass-information can result in data that can help to legally „figure out" secret information (without committing a criminal offence). Means of operation include the recruitment of agents (collaborators, or with a technical term: source of information).

The intelligence gathering or averting services may establish a system of appointed agents in order to guarantee fast and effective flow of information. A well-trained external member of the service, former contact person or even an agent trained to be an appointed agent can be the appointed agent. The appointed agent keeps in touch with

[11] http://www.mkih.hu/hivatal_hirszerzes.shtml, accessed 2.10.2011.

[12] Belovics-Molnár-Sinku, *Magyar büntetőjog Különös rész* [*Hungarian Criminal Law Special Part*] Budapest, 2005, pp. 35-36.

3-5 agents at their best, and forwards the collected information to the agency through his liaison officer.

According to the Criminal Code, espionage acts can be carried out in two directions: for

a) foreign power, or

b) foreign organization.

Foreign power is usually a state; the foreign organization is usually a foreign secret service agency. Any kind of organization could be mentioned, which functions are carried out of the territory of Hungary. If this foreign organization is a cover company for a foreign secret service, then the fact that among the owners of the company there are Hungarian citizens as well will not change possibility to establish the crime of espionage. (It is another question that the criminal liability of such Hungarian owners should also be examined.)

The Criminal Code does not determine a result regarding this crime, meaning espionage is considered to be committed when the person carries out the specific criminal behaviour according to law. The legislator does not need a purpose or a motive to establish this crime, so it does not matter, if espionage was committed for political or material reasons.

Carrying out intelligence work the crime of espionage is completed. According to judicial practice, carrying out a work cannot mean one act; it necessitates acts isolated in time and space. Intelligence work itself means a continuous line of acts according to the secret service jargon, so the crime cannot be committed by one action. If the perpetrator carried only one conduct, then the attempt of espionage or other crime (like crime violating certain kind of secrets, or other crime against the state) can be established; or if neither attempt nor other crime can be established then the accused must be acquitted for the lack of crime.

(Thus, for example, carrying out a messenger work only one time in favour of a foreign secret service agency, or handing over unclassified information, preparing an analysis-evaluation report thereof only one time for a foreign power or organization does not count as a crime according to the new Criminal Code.) Attempt can only be established, if the perpetrator begins the act in order to acquire information, but he does not obtain it or he prepared only one report including one or more facts, moreover, it can be proven that the connection between the informant and the foreign power or organization was established for a considerable period of time. In the point of view of legal practice this results in an expectation that the activity of the informant must be documented and verified with special thoroughness so the court could establish the commitment of the crime of espionage (and to be able to prove it in court). The Criminal Code renders the preparation of this crime also punishable, expressing the increased threat of espionage to the society.

The statement of facts of this crime does not require a result, which means that behaving in a certain way, so doing intelligence work makes the commitment of this crime complete.

The subject of espionage can be anyone irrespective of citizenship. Foreign citizens usually do intelligence work within embassies, under diplomatic cover. Embassies are in the majority of cases the centres of the appointed agent's group. Foreign diplomats, however, are protected by diplomatic immunity, so in Hungary only Hungarian citizens and non-diplomatic foreign agents can be held criminally liable. (Nevertheless, these agents – even if they were brought to justice – are exchanged to private agents after

some years have passed since the final judgment[13]). Espionage can only be committed intentionally, both with *dolus directus* and *dolus eventualis*.

Aggravated case of the crime is when espionage is committed by handing out top secret information.

Espionage is committed by carrying out a activity, so it is a continuous, prolonged criminal offence. Therefore, if someone does intelligence work repeatedly or continuously for the same organization or foreign power, espionage constitutes natural unity. If espionage is committed for several organization or foreign power then the sameness of the injured party, meaning the Hungarian state creates one continuously committed offence, as a unity created by law. Multiple offences can be established in a rare and unlikely case when the perpetrator does intelligence work for several organization or foreign power and continuously committed offence cannot be established due to the long period of time between the executed partial acts.

The Criminal Code guarantees impunity for the perpetrator who reports his volunteering or undertaking to the authorities and discloses all information on his foreign connection before he had done any intelligence work. This rule can be a useful tool for the Hungarian secret services to „turn back" foreign agents after their identification, thus to employ them as double agents and to mislead the foreign secret service with false information. It is an important issue in practice that the double agent must be given real information as well because such agent could be caught quickly, if he is given only false information. In this case, espionage is committed pro forma, but if the Hungarian colleagues of the secret service hand out real data besides the false information through the double agent in conformity with the professional rules then in my opinion the crime cannot be established due to the lack of danger to society. In such cases, however, the national secret service has to act particularly carefully and in compliance with the professional rules and real information can only be given to the foreign power or foreign organization in the narrowest possible limits.

Crimes violating obligations to keep certain secrets have the following relation to espionage: according to both the principle of specialty and the principle of consumption (meaning that the less serious crime merges into the more serious one) – due to even the more severe punishment – we have to establish espionage in case of seeming multiple offences.

Espionage and the violation of trade secrets can be distinguished according to the following aspects: if the intelligence work can be proven as the act of perpetration (on the basis of later scientific literature, with regard to the widened interpretation of intelligence work this would not be difficult), and this person forwards economic secrets for a foreign power or foreign organization, commits espionage (economic espionage).[14] If someone obtains economic secrets for his own benefit or for a domestic company which cannot be proven to be linked to a foreign secret service, only the violation of trade secrets can be established (in literature it is called industrial espionage). The most important distinguishing element is whether the perpetrator is able to violate the

---

[13] For the exact meaning of legal force see: Elek Balázs, *A jogerő a büntetőeljárásban.* [*Legal force int he criminal procedure*] Monográfia, Debrecen, DE ÁJK, 2012, pp. 74-80.

[14] For the increasing importance of economic data and information, see Kecskés András, *A kezdeti nyilvános részvénykibocsátások árfolyam-stabilizációjának jogi szabályozása* [*Regulation of the stabilization of the current price of initial public issue of shares*], Magyar Jog, 2012. Október, pp. 589-597.

financial, economic other relevant interest of Hungary by managing such data illicitly. [15] If yes, then espionage should be established, if not, then no matter how big the damage is, the perpetrator only violated trade secrets.

4. Can espionage be committed by only collecting and analysing open source information?

Since OSINT extract newer data in quality from the analysis of open source information, we must pose the question whether the acquisition and forwarding of information coming only from open sources

1) can meet the statement of fact of the crime of espionage, and
2) can establish the crime of espionage.

Ad 1) We have to separate the collection and analysis of data from forwarding data. In our opinion, merely the analysis of open databases and collecting data there from are entirely neutral activities, even if the person obtained new information by means thereof. (Information put on the Internet always constitutes open source information, even if classified data can be or is mixed among them, just think about the scandal regarding Wikileaks.) In case the data gained from open source information is forwarded to foreign power or foreign organization, then the statement of facts of espionage can be met. However, it matters what kind of information and to what kind of foreign organization or power the perpetrator forwards the data. For example, collecting and forwarding medical, technical or scientific open source data to a person working at a foreign research facility does not meet the statement of fact of espionage. However, collecting, analysing, processing and forwarding governmental, political or economic information to an opposed secret service can meet the statement of facts of the crime of espionage.

Ad 2) After examining the statement of facts we must examine the issues of danger to society and guilt. It is not easy to prove the danger to society in this case. The action has to damage or danger the interest of Hungary. In addition, the perpetrator can allude to error in danger to society. With regard to the question of guilt, intention can also be hard to prove for the authorities: since the authorities have to prove that the perpetrator knew that the collected data violates the interest of Hungary and that he also knew that the data is forwarded to a foreign power or organization, and that this activity is suitable to potentially cause damage to Hungary.[16]

This means that espionage can only be verified under multiple qualified circumstances against a perpetrator who gains only open source information but in certain cases it is possible to establish this crime.

---

[15] For the relation between national economic and corporative interests, see: Kecskés András, *The Legal Theory of Stakeholder Protection*, JURA, 2010/ 1. Szám, pp. 67-76.

[16] Regarding this issue a mistake can have a great importance, as a ground for excluding criminal liability see: Polt Péter (szerk.), *Új Btk. kommentár. 1. kötet, IV. fejezet, 1.4. Elek Balázs: A tévedés* [*Commentary to the new Criminal Code Book 1, Chapter IV. para 1.4. The mistake by Balázs Elek*], pp. 137-147, Elek Balázs, *Juris ignorantia non excusat? A jogi tévedés megítélése a gazdasági büntetőperekben.* [*Juris ignorantia non excusat? The evaluation of legal mistake in economic criminal cases*] Rendészeti Szemle, 2009/7-8, pp. 96-109.

5. Conclusion

As it can be seen before, it is not an easy task to prove beyond reasonable doubt the commitment of espionage with the help of the toolbox of criminal law. Until now, in the Hungarian legal practice only such cases happened when the perpetrator gave classified information to the foreign organization (as well). Maybe the most interesting case was the criminal procedure of Steven Belovai (deceased in 2009)[17] who wrote in his memoir – a book titled Code-name: Scorpion[18] – that he decided after a long struggle to contact CIA in order to forestall the new world war. Practically, due to his activities was the Conrad-conspiracy uncovered and circulated in the world press. Clyde Lee Conrad (1948-1998) a U.S. Army non-commissioned officer in Germany sold top secret information to the People's Republic of Hungary between 1974-1988. The most important of these secrets was the draft of the lock of the nuclear shaft that separated East and West Europe, and by which means the soviet tanks could get without difficulty to the La Manche. In 1990 he was convicted of espionage and high treason in a German court and was sentenced to life imprisonment. Belovai was, however, caught earlier in the mid 80's, when he received a document at a hide-out. The manipulates stone to be sued therefore, as a material „mailbox" can still be viewed in Budapest as a museum exhibit in the central office of National Defence Bureau. The prosecutor asked for death penalty against Belovai according to the Criminal Code that was effective back then at the trial, but in the end he was sentenced to life imprisonment and complete confiscation of property, and in 1990 Árpád Göncz the President of the Republic gave pardon to him, so he did not have to serve the remained punishment.

In my opinion, open source intelligence (OSINT) can only be prosecuted and the perpetrator can only be punished in the future, if in case of an already caught spy the submission of classified data cannot be proven, but his regular connection to the foreign organization and that he transferred filtered and analysed information that originated from publicly available sources can.

References

1. András, Kecskés, *A kezdeti nyilvános részvénykibocsátások árfolyam-stabilizá ciójának jogi szabályozása* [*Regulation of the stabilization of the current price of initial public issue of shares*], Magyar Jog, 2012. Október;

2. András, Kecskés, *The Legal Theory of Stakeholder Protection*, JURA, 2010/1. Szám;

3. Balázs, Elek, *A jogerő a büntetőeljárásban.* [*Legal force int he criminal procedure*] Monográfia, Debrecen, DE ÁJK, 2012;

4. Belovics-Molnár-Sinku, *Magyar büntetőjog Különös rész* [*Hungarian Criminal Law Special Part*] Budapest, 2005;

[17] An additional interesting tidbit from recent years: According to the prosecutor's office of Bolivia, Eduardo Rózsa Flores kept in touch with the CIA through Stephen Belovai, who organized a terrorist group for the Bolivian separatists. Rózsa Flores and Belovai as an agent of the CIA probably get in touch at the Balkan and Belovai gave Rózsa Flores financial and technical help for hisBolivian activities – indicated the Bolivian press. http://www.mixonline.hu/Cikk.aspx?id=37012, accessed 23.10.2011.

[18] Author's issue, Budapest, 1998. ISBN: 9635506724, p. 604.

5. Gábor Lévay, *OSINT (OPEN SOURCE INTELLIGENCE), Nyílt információs hírszerzés.* Zrínyi Miklós *Nemzetvédelmi Egyetem, egyetemi jegyzet* http://osint.gportal.hu/gindex.php?pg=20201555&nid=3320934, accessed 29.12.2013;

6. http://osint.gportal.hu/gindex.php?pg=20201555&nid=3320934, accessed 29.12.2013;

7. http://osint.gportal.hu/gindex.php?pg=20201555&nid=3320934, accessed 29.12.2013;

8. http://www.mixonline.hu/Cikk.aspx?id=37012 accessed 23.10.2011;

9. http://www.mkih.hu/hivatal_hirszerzes.shtml accessed 2.10.2011;

10. http://www.mkih.hu/hivatal_hirszerzes.shtml accessed 2.10.2011;

11. Jenő, Izsa, *Nemzetbiztonsági alapismeretek (A titkosszolgálatok működése)* [*Fundamentals of national security (Operation of secret services)*] ZMNE, Kossuth Lajos Hadtudományi Kar, Budapest, 2009;

12. Kish, John, *International Law and Espionage*, Kluwer Law International, Netherlands, 1995;

13. Klass v. Federal Republic of Germany case: European Court of Human Rights: Judgement, Strasbourg 6 September 1978, Council of Europe Reports, 1978;

14. Lajos, Hajma, *A katonai felderítés és hírszerzés története (egyetemi jegyzet) [The history of military intelligence (lecture notes)]* ZNME Budapest, 2001;

15. NATO OSINT *Handbook,* http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf, accessed 30.12.2013;

16. Péter, Polt (szerk.), *Új Btk. kommentár. 1. kötet, IV. fejezet, 1.4. Elek Balázs: A tévedés* [*Commentary to the new Criminal Code Book 1, Chapter IV. para 1.4. The mistake by Balázs Elek*], Elek Balázs, *Juris ignorantia non excusat? A jogi tévedés megítélése a gazdasági büntetőperekben.* [*Juris ignorantia non excusat? The evaluation of legal mistake in economic criminal cases*] Rendészeti Szemle, 2009/7-8.