COLLECTING INFORMATION FROM HUMAN SOURCES FOR COMPETITIVE INTELLIGENCE

Răzvan GRIGORESCU*

Abstract

The collection of information has evolved continuously throughout history, undergoing a series of transformations closely related to the development of the information sources. Over the last decades, these evolutions have been observed not only at the level of the intelligence community, but also at the level of the business environment, with the development and implementation of the competitive intelligence functions within the companies, on a larger scale.

It is a known fact that many competitive intelligence professionals claim that they use HUMINT in their daily activity, often without clearly explaining what they are referring to. With regard to this topic, we believe that more transparency is needed, due to the fact that HUMINT is being also used by the government intelligence agencies to designate the secret human sources.

This paper briefly analyses how business information should be collected by the competitive intelligence professionals, the types of sources with which they operate, as well as the way in which HUMINT must be approached in competitive intelligence, in order to align with the applicable Romanian legislation and the SCIP Code of Ethics.

Keywords: *competitive intelligence, collection, elicitation, HUMINT, SCIP, ethics*.

Introduction

Collecting information is at the very basis of any actionable intelligence product. In competitive intelligence, the quality of the collected information directly influences the quality of the intelligence product.

*PhD Candidate, "Mihai Viteazul" National Intelligence Academy, Romania, e-mail: grigorescu.razvan@animv.eu.

The temptation to quickly obtain information that will differentiate between companies can sometimes be absolutely tremendous. Under these conditions, in some cases, there may be different business people willing to do almost anything to achieve their goals, even by ignoring the core principles of professional ethics or certain legal provisions, risking their credibility and their freedom.

The motivation for writing this article is of an intrinsic nature and seeks to correctly identify the legal way in which human sources can be used in Romanian competitive intelligence practice, independent of any other international existing practices.

The premise of the research is that all activities carried out by the public or private companies must be in accordance with the principles of professional ethics and the Romanian legislation in force. Thus, the research question was: "How can information for competitive intelligence are collected from human sources in Romania, in a legal and ethical manner?"

Several other questions arise from the research question, this paper answering them as well: What legal provisions influence the competitive intelligence activity in Romania? Is the competitive intelligence activity regulated, from a legal point of view, in Romania? What key elements must be taken into account by any person engaged in competitive intelligence activities, on the Romanian territory, from a legal point of view? What are the main ethical benchmarks of competitive intelligence? Can certain practices carried out in competitive intelligence operations be considered illegal in Romania? What collection methods and techniques are unethical and / or illegal? Is competitive intelligence synonymous with espionage? What categories of sources are used in government intelligence? What categories of sources are used in competitive intelligence? What kind of primary and secondary sources are used in competitive intelligence? How is HUMINT defined? Is it right to use HUMINT in competitive intelligence? What is the difference between secret human sources and non-secret human sources? How is the competitive intelligence function organized, in private companies? Is it possible to use elicitation techniques in competitive intelligence? What kind of proposals could be

made, in order to accelerate the development of competitive intelligence in our country?

In order to answer the research question, we mainly used the social research method of document analysis, accessing a wide range of validated open sources from which we collected information. This was then filtered and processed, accordingly, in order to conduct the later analysis and synthesis. The sources are mentioned at the end of the research paper.

The title we have chosen, even if it may seem too general, reflects our concerns about clarifying some important aspects regarding how information is collected from human sources, in competitive intelligence. We would like to mention that we did not start our research from the premise that collecting information from human sources in competitive intelligence is illegal. We were only interested in analysing how the activities of collecting information from human sources should be carried out, so that they do not contravene the codes of ethics and the Romanian legislation in force (by its specificity, competitive intelligence must meet both the ethics and legal criteria).

We consider that this research paper will have a positive impact with regard to the understanding of competitive intelligence, its results being able to represent a starting point in various debates and future research, having as central element the collection of information from human sources, in the private companies.

This paper is structured into three main chapters, which are complemented by the conclusions and the bibliography. The first part of the paper highlights the main ethical landmarks and the legislative framework, characteristic of competitive intelligence. In the second part, we approach the sources used by the competitive intelligence professionals to obtain the necessary information, as well as the sources used by the state intelligence services. In the third part, reference is made to the main aspects related to the use of human sources in competitive intelligence, proceeding to a more detailed analysis of the HUMINT concept and its usefulness in the field of competitive intelligence, highlighting different approaches proposed by experts. The results of the research, in relation to the stated research question, are reflected in the conclusions, these being the basis for

formulating several recommendations to the competitive intelligence professionals.

Competitive Intelligence: legal aspects

In Romania, the competitive intelligence activity is not delimited by laws or regulations, this being considered unnecessary, until recently. No less important, however, given that competitive intelligence also involves the collection of various information, aimed at obtaining actionable intelligence products, special attention should be paid to the way in which the collection activities are carried out. Like other business practices, competitive intelligence must be conducted in compliance with applicable Romanian legislation and professional ethics.

Next, we would like to mention the main ethical benchmark of competitive intelligence, as well as to make a brief analysis of the national legislation in force, relevant to both public and private companies, in order to identify the key elements to be considered by any person carrying out competitive intelligence activities in Romania.

With regard to the professional ethics, in competitive intelligence, The SCIP Code of Ethics[1] is an important benchmark and mentions the following guidelines: "to continually strive to increase the recognition and respect of the profession; to comply with all applicable laws, domestic and international; to accurately disclose all relevant information, including one's identity and organization, prior to all interviews; to avoid conflicts of interest in fulfilling one's duties; to provide honest and realistic recommendations and conclusions in the execution of one's duties; to promote this Code of Ethics within one's company, with third-party contractors and within the entire profession; to faithfully adhere to and abide by one's company policies, objectives and guidelines". (SCIP, n.d.)

Referring to our national legislation, we note that not much effort has been made, so far, to analyse the main elements of legislation to be considered in the practice of competitive intelligence, especially

[1] Strategic & Competitive Intelligence Professionals – a global society of strategic and competitive intelligence professionals.

when we refer to the collection of information from human sources. Therefore, we would like to try to identify these elements.

For a start, we should emphasize that from a competitor's point of view, the information of interest, planned to be collected, could be a publicly available one or a confidential one, such as a trade secret (whose obtaining is unlawful, without the consent of its rightful owner, as it is not meant to be publicly available).

A trade secret could be defined as know-how or business information that is not widely known, being undisclosed and intended to remain confidential. (Directive (EU) 2016/943, 2016)

In order for any piece of information to be protected as a trade secret, it must meet the following conditions: it must be a secret, meaning that it is not known or accessible to many people; it must have a commercial value; it must be the subject to protection measures, in order to maintain its secrecy. (European IPR Helpdesk, n.d.)

It is a well-known fact that crime presupposes the existence of intent. According to the article 16 of the new Criminal Code, the following are provided regarding guilt:

"(1) The action is an offense if committed under the form of guilt required by the criminal law.

(2) Guilt exists when an offense is committed with direct intent, with basic intent or with oblique intent.

(3) An action is committed with direct intent when the perpetrator:

a) can foresee the outcome of their actions, in the expectation of causing such outcome by perpetrating the act;

b) can foresee the outcome of their actions and, while not intending to produce it, nevertheless accepts the likelihood that will occur.

(4) An act is committed with basic intent when the perpetrator:

a) can foresee the outcome of their actions but does not accept it, believing without reason that such outcome will not occur;

b) does not foresee the outcome of their actions, although they should and could have foreseen it.

(5) Oblique intent exists when an act, consisting of a deliberate action or inaction, produces unintended more serious consequences and is attributable to the perpetrator.

(6) The act consisting of an action or inaction shall constitute an offense when committed intentionally. The act committed with basic intent constitutes an offense only when the law expressly establishes it as such." (Criminal Code, 2009)

From the Criminal Code perspective, the intention can be substantiated if different entities, such as the competitors of a company, plan and carry out activities of collecting information of interest, with secret or confidential character, regarding a target company.

Trying to identify the most important legislative provisions, related to the field of competitive intelligence, following a brief analysis of the relevant Romanian legislation, we chose to focus on the following: *Constitution of Romania* (1991), as amended and supplemented; Law no. 31/1990 on companies, as amended and supplemented; Law no. 11/1991 on combating the unfair competition, as amended and supplemented; Law no. 51/1991 on the national security of Romania, amended by Law no. 187/2012, republished, under art. 107 (3) From the Law no. 255/2013; Law no. 14/1992 on the organization and operation of the Romanian Intelligence Service, as amended and supplemented; Law no. 8/1996 on copyright and neighbouring rights, as amended and supplemented; Law no. 21/1996 of competition, amended and supplemented by Law no. 149/2011 and Law no. 347/2015 on approving Government Emergency Ordinance no. 31/2015; Law no. 84/1998 on marks and geographical indications, republished; Law no. 298/2001 on the amendment and supplementation of Law no. 11/1991 on combating the unfair competition; Law no. 324/2003 on approving Government Emergency Ordinance no. 57/2002 on scientific research and technological development, amended and supplemented by Government Emergency Ordinance no. 6/2011; Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communication sector, that transposes Directive 2002/58/CE of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic

communications sector (Directive of privacy and electronic communications), amended and supplemented; Law no. 535/2004 on prevention and combating terrorism, as amended and supplemented by Law no. 187/2012, Law no. 255/2013, Government Emergency Ordinance no. 78/2016 and Law no. 58/2019; Order no. 1.832/856/2011 on the amendment to the classification of occupations in Romania – Level of Occupation (six characters); Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); Government Emergency Ordinance no. 25/2019 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, as well as on the amendment and supplementation of legislation, that transposes Directive 2016/943/EU of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

Analysing the content of the above mentioned laws and regulations, several key elements have emerged, considering that they must be taken into account, by any person who carries out competitive intelligence activities, in Romania. The key elements we found have been summarized, among which we would like to mention the following: "the right to information shall not be prejudicial to the measures of protection of young people or national security", as mentioned in Art. 31 (3) of the Constitution of Romania (Constitution of Romania, 1991); all the carried out activities must comply with the General Data Protection Regulation; the disclosure, collection or use of trade secrets by third parties, as a result of a commercial or industrial espionage action, which infringes a legal person, is illegal and is punishable (Law no. 298, 2001); the attainment of a trade secret, as well as its use or disclosure, without the consent of its rightful owner is illegal (Government Emergency Ordinance no. 25, 2019); the attainment, use or disclosure of a trade secret is unlawful if the person

acquiring the trade secret knew or should have been aware that the trade secret was obtained from a person who was not allowed to disclose that trade secret. (Government Emergency Ordinance no. 25, 2019)

Sources of information in competitive intelligence

Most business people use competitive intelligence responsibly, in compliance with applicable laws and codes of ethics. It is well known that competitive intelligence is incompatible with the following ways of collecting information, deeply illegal, which must be strictly avoided by everyone, the list being not limited to: violation of individuals' privacy and the infringement of their fundamentals rights; blackmail and various types of threats; corruption of civil servants or competition employees; illegal entry into the spaces where the competitors carry out their daily activity or into their employees homes, in order to gather information; phishing; wiretapping etc.

Unfortunately, there is still an ongoing confusion regarding the term competitive intelligence, which is sometimes considered synonymous with espionage. In order to clarify things, it should be noted that competitive intelligence activities take place in full legality and in accordance with the ethical principles, having nothing in common with espionage, which is unethical, being a crime, according to the Criminal Code.

Without going into too much detail, we will continue by briefly referring to the competitive intelligence sources, comparing them with the ones used by the governmental intelligence agencies. According to the Explanatory Dictionary of the Romanian Language, the term source is defined as "the place where information or a novelty emanates" (Romanian Academy, 2016, p. 1191).

Regarding government intelligence, the sources of information can be divided into the following main categories: secret sources (HUMINT and TECHINT) and open sources (OSINT), non-secret. Although the use of HUMINT is being often invoked, mostly by foreign experts, competitive intelligence is not using secret sources, but open sources (to obtain secondary or primary information).

Presently, there are different approaches in regard with secondary and primary sources of information. Generally speaking, the secondary sources used in competitive intelligence can be represented by traditional media, new media, grey literature, books, official reports, brochures, conferences, academic papers, images from commercial satellites etc., while the primary sources being used are generally represented by non-secret human sources, original documents publicly available etc.

We would like to point out that some categories of sources can be both primary and secondary sources (UNSW Library, n. d.). Primary sources are those that have not been altered and have not been edited (e.g. speeches, telephone interviews, press releases etc.), while secondary sources have been edited, in various ways (e.g. newspaper articles, magazines etc.). (Cook, Cook, 2000, p. 39)

Reviewing the different categories of open sources, the Open Source Centre also mentions the press conferences or the conferences and symposia in professional or academic settings (Open Source Centre, n.d.), that can represent both secondary sources and primary sources. The information obtained from these categories of open sources could be also primary information (for example, the public information obtained by an investigative journalist to the question he asked a person that is holding a press conference).

Jay Liebowitz shows us that the primary sources used in competitive intelligence can be individuals, data sets or various documents, noting that interviewing people at fairs and exhibitions or conferences can prove useful. As for secondary sources, they are described either as the person who knows the individual who holds the information of interest, or as an article in a newspaper, a report on a particular industry, or someone quoting someone else. (Liebowitz, 2006, p. 60)

The primary sources used in competitive intelligence are the sources from which first-hand information is collected. Larry Kahaner gives examples the CEO of a company, the president, a governmental agency, or another person who has access to the right information. (Kahaner, 1996, p. 53) "Human intelligence is derived from human sources". (Interagency OPSEC Support Staff, 1991)

Ionel Nițu describes HUMINT as "the use of secret human sources" (Nițu, 2012, p. 37). Secret human sources are people who provide information that is generally not intended for the general public. Among the possible secret human sources are intelligence officers, agents (spies), military attachés, soldiers, emigrants, tourists, war deserters, prisoners, dissidents etc. (Petrescu, 2011, p. 168)

Peter Gill and Mark Phythian emphasize that intelligence operates with both secret and open sources, HUMINT being part of the secret sources category. (Gill, Phythian, 2011, p. 64) Various competitive intelligence practitioners invoke the use of HUMINT, without making certain clarifications, which would eliminate the uncertainties regarding the legality of these approaches, which can end up by creating the false impression that competitive intelligence is synonymous with espionage, when, in fact, competitive intelligence is a legal activity, useful to the business environment. Next we will show why this can happen.

Abram Shulsky and Gary Schmitt put the equal mark on gathering information from human sources, espionage and HUMINT. (Shulsky, 2006, p. 35) Mark Lowenthal highlights that HUMINT means espionage (Lowenthal, 2003, pp. 74-77), involving the manipulation of other human beings as potential sources of information (Lowenthal, 2003, p. 211).

Sergiu Medar and Cristi Lățea point out that, from a theoretical point of view, HUMINT represents "the information obtained by specially prepared and trained personnel by exploiting human sources, officially, semi-officially or unofficially (clandestinely), through informants, collaborators or agents (spies)" (Medar, Lățea, 2007, p. 46).

As for the intelligence officers, who work for the intelligence services, they often act under the cover of employees of embassies, consulates, consular offices, business missions or official diplomatic activities. (Petrescu, 2011, p. 168) Stan Petrescu claims that there is an unwritten law "according to which intelligence officers and military attachés may carry out clandestine activities, on their own, to collect information." (Petrescu, 2011, p. 169)

Although for the general public HUMINT collection remains synonymous with espionage and clandestine actions, most of it is

actually being conducted "by overt collectors, such as diplomats and military attachés". (Operations Security, n.d.)

In turn, TECHINT (Shulsky, Schmitt, 2008, p. 35), technical sources (secret) could provide information in addition to or as a substitute for information from human sources and/or open sources, the collection of information from these sources being done "without the knowledge, agreement or cooperation of the targets." (Petrescu, 2011, p. 65)

Regarding OSINT, Ionel Nițu defines it as "the collection of information from open, public sources, with unregulated access, official or unofficial" (Nițu, 2012, p. 37). Edward Waltz describes the main categories of intelligence sources, dividing them in terms of access and means of collection, OSINT being openly accessible sources, the collection of information from these sources being done by human and technical means. (Waltz, 2003, p. 36) According with NATO, there are four main categories of open sources: open source data (OSD), open source information (OSIF), open source intelligence (OSINT), and open source intelligence validated (OSINT-V). (NATO, 2001, pp. 2-3)

In general, the use of human sources is characteristic to the field of social research, characterized by transparency, in which the application of questionnaires, conducting qualitative interviews, using focus groups, etc., manages to provide answers, scientifically valid, to various research questions. Under these conditions, it is natural for human sources to be also considered in the field of intelligence, even if the methods and techniques that are used to obtain information are more comprehensive.

There is still certain confusion about HUMINT and OSINT, with some people mistakenly believing that the use of human sources is only characteristic to HUMINT. Next, we will show that, to a certain extent, human sources are also characteristic for OSINT (as opposed to HUMINT, in OSINT we are only referring ourselves to non-secret human sources).

Among the open sources mentioned by the NATO Open Source Intelligence Handbook are the open human sources, more precisely, various experts and observers. "The ultimate open source is a human expert or human observer with direct experience. (…) The human

expert is often the most efficient and the most inexpensive means of creating new open source intelligence that is responsive to a specific requirement from the commander or his staff". (NATO, 2001, p. 9)

Stephen Mercado noted that the sharp development of OSINT is transforming the world of intelligence, with the advent of open versions of the covert arts of human intelligence (HUMINT), aerial imagery (IMINT) and signal intelligence (SIGINT). (Mercado, 2004, p. 47)

Practically, OSINT extends to areas of HUMINT, IMINT and SIGINT (Mercado, 2004, p. 48), pervading "all of the collection disciplines", as evidenced by Mark M. Lowenthal, which also stated that today information can be collected including by elicitation, by ordering images from commercial satellites and by "using software to conduct traffic analysis". (Lowenthal, 2001, p. 62) Regarding competitive intelligence, David Jimenez specifies that it is based on open sources, also mentioning the employee interviews, as an example (Jimenez, 2005, p. 171).

With reference to open source data, Robert David Steele also mentions oral debriefing or another form of information, from a primary source. (Steele, 2007, p. 131)

Considering the open sources of information, the same expert mentions the following general categories: traditional mass-media, different commercial online sources, gray literature, overt human experts, commercial imagery and geospatial information, and the Internet. (Steele, 2007, p. 138)

In turn, Ion Călin also includes the human sources (observers, researchers etc.) in OSINT. Basically, the main categories of open sources mentioned by Ion Călin are represented by the traditional media, the Internet, the "grey" literature, the human sources (n. a. non-secret), and the commercial satellites. (Călin, 2015, p. 193)

Ion Călin mentions that the human sources he is referring to should not be confused with the human sources specific to the intelligence activity (HUMINT). (Călin, 2015, p. 196)

Regarding their value and credibility, Ion Călin appreciates the fact that the information collected from open sources have at least the same value as that derived from classified ones. (Călin, 2015, p. 193)

Non-secret human sources are those human sources from which information is obtained for the general public. Non-secret human sources include observers, researchers, "government officials, librarians, archivists, investigative journalists, accredited reporters from governmental institutions, employees of non-governmental organizations." (Călin, 2015, p. 193) At the same time, we consider that public relations experts, academic experts, business people, including specially trained staff to represent companies, at trade fairs and exhibitions, sales staff, customers and their competitors etc., can be also added to the list.

Abram Shulsky and Gary Schmitt (2006, p. 35) include the collection through diplomatic contacts in open sources. Taking into account all these elements, noting the diversity of the available open sources, we can deduct that, in competitive intelligence, the use of the term "HUMINT" cannot be accepted unconditionally, being necessary more clarifications, at least from the legal perspective of our country.

Given the controversies related to the use of primary sources, in competitive intelligence, we will further refer to some aspects related to the use of human sources.

Human sources in competitive intelligence

In competitive intelligence, the use of secondary sources is predominant. No less important, there are opinions that support the idea of using the primary sources, on a larger scale, also by making reference to HUMINT.

One of the people who support this approach is Nir Kaminer, Head of Competitive Intelligence T-Systems International GmbH, and Germany. He considers that although secondary information, used in competitive intelligence activity, already proved its effectiveness, its exclusive use can lead to the loss of the distinctive advantage companies are looking for, believing that it can also be accessed by competitors, as it's not exclusive. (Institute for Competitive Intelligence, 2017)

In this respect, Nir Kaminer is of the opinion that the primary information (obtained from primary sources) makes the difference, not being accessed by everyone. He considers that the information collected and analysed, using HUMINT (through direct contact with human

sources, previously identified, with whom is made conversation), is effective in competitive intelligence, helping businesses to win. Regarding the practices to be avoided when using HUMINT, Nir Kaminer only mentions that it should be borne in mind that "the same situation does not happen within your own organization", emphasizing the importance of communication with employees, in terms of taking all the necessary precautions, in relation to what they communicate to others, in order to avoid the undesirable information leaks. (Institute for Competitive Intelligence, 2017)

Internationally, the private companies choose either to organize their competitive intelligence functions internally, or to outsource them. The competitive intelligence function of a company may be developed in a separate department, included in one or more of the company's existing departments or assigned to one or more trained individuals. In the same time, the competitive intelligence function can be outsourced to various entities, such as freelancers, consulting firms, security companies, private intelligence agencies, private detective agencies and/or various developers of dedicated IT solutions.

Sometimes, the above mentioned entities employ former military people, including former military intelligence personnel, being able to conduct intelligence operations anywhere in the world, being able to access even hidden (n. a. protected) information or personal information, as mentioned by W.E.P.A. Agency, for example. (W.E.P.A. Agency, n.d.)

We consider it to be self-evident that what it is legal in other countries it is not necessarily legal in Romania. Therefore, before starting a new activity, following any other existing foreign model, from elsewhere, all the relevant Romanian legislation should be studied, with a focus on the possible legal implications of the carried out activities, also taking into account the European Union legislation, where applicable.

Taking into account that we gave examples from other countries, referring to the possibility of accessing the competitive intelligence services, offered by different external entities, to various companies on the Romanian market, or to companies that are aiming entering this market in the future, concerning HUMINT, without referring to a

specific case, we consider that we should ask ourselves the following question: "Who guarantees that a foreign entity, such as a private intelligence agency, for example, that is also specialized in competitive intelligence, complies with our national legislation, when collecting information, on Romanian territory"?

In this regard, we would like to highlight a few more conceptual approaches of HUMINT. The CIA defines HUMINT as any information that can be collected from human sources. HUMINT collection is done by clandestinely obtaining photographs or other documents, by collecting overtly by different people overseas, by debriefing of foreign nationals and citizens traveling abroad, as well as by official contacts with foreign governments. (CIA, 2010)

From a certain perspective, HUMINT can be also used in business, but without aiming to obtain secret or confidential information, including trade secrets. A study by Alisa Rubin Peled and Haim Dror, found that corporations could use HUMINT (seen as "counter-terror intelligence techniques based on human sources") to identify patterns of corporate-wide fraud, rather than target individual perpetrators, and educate employees about the information they can share with others. (Peled, Dror, 2010, pp. 320-331)

In turn, trying to define HUMINT, Larry Kahaner briefly refers to it as "what someone tells you", giving examples from the business world such as what salespeople tell their managers about customers, the rumours or notes taken by employees when attending public events, organized by competitors, such as the opening a new factory etc. (Kahaner, 1996, p. 80)

Robert M. Clark is mentioning that HUMINT could be collected clandestinely and overtly. (Clark, 2014, p. 50) Clark emphasizes the fact that in competitive intelligence, HUMINT is mostly done overtly (Clark, 2014, p. 51), noting that he does not state that this collection is totally made in this way, thus understanding that it is also made clandestinely, which is contrary to the Romanian legislation.

It should be noted that, more often than not, HUMINT is brought into discussions by mentioning the elicitation techniques. We should mention that elicitation could lead sometimes to different ethical and legal issues that should not be ignored, but treated responsibly.

In order to understand what we mean by that, we consider necessary to briefly mention the way in which elicitation is being defined, internationally.

One of the approaches belongs to Cliff Lansley, which defines elicitation as "a process used to draw out information from people, during a communication with a purpose, often without them realizing the elicitor's purpose for doing so". (Lansley, 2017) Lansley emphasizes that you should not abuse of elicitation, if it might harm others. (Lansley, 2017)

At the same time, Wayne N. Taylor defines HUMINT concept as "the subtle art of extracting information from another individual during an apparently normal and innocent conversation". (Taylor, 2010, p. 6) What is important to note is that Wayne N. Taylor further explains that the target of elicitation is the individual that "may or may not be willing to share the information and should not know that you're even interested in the information". (Taylor, 2010, p. 6)

We also consider it appropriate to present the way in which the FBI defines elicitation, as "the strategic use of conversation to extract information from people, without giving them the feeling they are being interrogated." (U.S. Department of Justice, n.d.)

Elicitation has very deep roots in the more or less recent history of Romania, being mainly related with the activity of secret services, an example of definition being the one proposed by the ***National Council for the Study*** of the ***Securitate Archives*** (NCSSA), more precisely, "the operative method of collecting information under the cover of a false identity". (N.C.S.S.A., n. d., p. 5)

From these definitions, it can be seen that, in general, elicitation is being used with the intention of extracting information of interest from a person who holds it, including information that the person would not disclose, voluntarily, in other circumstances, not being aware that he/she transmits information, without being shown any transparency, in relation to the aim pursued, being able to go as far as to use a false identity, if necessary, which contradicts not only the professional ethics, but also the national laws (especially, if the information of interest is secret or confidential).

In order to avoid any confusion, we would like to emphasize that we do not consider unethical and/or illegal any use of human sources in competitive intelligence activities, in regard with elicitation, appreciating that there might be certain ways in which it is neither illegal nor unethical to do it.

However, in order to emphasize the importance of clarifying the way in which elicitation is being carried out in competitive intelligence, we mention that Robert M. Clark points out that, in general, an operation is clandestine if the opponent or target does not realize that it took place, at all, being different from the covert one (hidden), in which the adversary or the target realizes that it took place, not being able to identify the source of the operation. (Clark, 2013)

We would like to mention that, according to the Explanatory Dictionary of the Romanian Language, the term clandestine is defined as having "a secret character, which is done in secret (being forbidden by law)". (Romanian Academy, 2016, p. 211)

Thus, we cannot fail to notice that aiming to extract information of interest from human sources, for a specific purpose, by using different methods and techniques, the target(s) being unaware about that specific purpose, without willing to disclose the information of interest, to others, could be interpreted, at least from a theoretical point of view, to be a clandestine operation, especially if the information intended to be extracted is known to be secret or confidential (referring to trade secrets), possibly falling under the incidence of the Criminal Code, including from the national security perspective, in some cases.

In these conditions, regarding the competitive intelligence activities carried out on the Romanian territory, we consider the use of HUMINT to be inappropriate, due to the multiple concerns of its legality and its compliance with the applicable codes of ethics, recommending the use of non-secret human sources.

Conclusions

Competitive intelligence is being characterized by the use of open sources for collecting information, being incompatible with the use of secret sources; at least from the perspective of the Romanian legislation (competitive intelligence is a business practice, not a military

one, without any regulations to connect it to the intelligence services of the state). Competitive intelligence is using human sources and will continue to do it, provided that the national and international legislation, as well as the ethical codes are complied with.

Answering the research question, there are always legal and ethical ways through which useful information could be collected, from human sources, for competitive intelligence purposes. With regard to the legal provisions in force and the provisions of the codes of professional ethics, they can be respected, for example, by using non-secret human sources and applying those methods and techniques that are more characteristic to the field of social research, such as surveys and questionnaires, qualitative interviews, the use of focus groups etc., that are not violating Romanian laws or the provisions of the codes of ethics, clearly mentioning that we are only referring to the collection of information that is not secret or confidential.

With regard to the use of elicitation techniques, in competitive intelligence, in Romania, the features of our national legislation, as well as the ethical codes, including The SCIP Code of Ethics, should be seriously taken into consideration. We would like to emphasize that, general speaking, elicitation is not being used randomly, but with a prior preparation, based on a collection plan (i.e., with intent). Therefore, if the intended purpose is to obtain secret or confidential information, such as trade secrets, from a theoretical point of view, by using elicitation and extracting such information of interest, a crime would be committed.

Presently, in regard with the concept of competitive intelligence, internationally recognized as a respectable business practice, an unfortunate confusion is still being made, from time to time, by which competitive intelligence is considered synonymous with espionage.

We consider that one of the causes that led to the perpetuation of this confusion might be represented by the use of HUMINT, for collecting information. In order to avoid any future perception errors of competitive intelligence, we would like to propose, to all the competitive intelligence professionals, the use of the non-secret human sources, overtly, as we know that, generally speaking, secret human sources are providing information that is not meant for the general

public. In the same time, we propose to avoid using the term HUMINT in competitive intelligence, the term being much more comprehensive, being used by the state intelligence services, more often, also suggesting the creation of a new concept, as an alternative.

Although it is not absolutely necessary, at this moment, the future regulation of competitive intelligence activity in Romania, could have some positive effects in regard with the perception of this respectable business practice among our private companies, creating the premises for an accelerated development of this field in our country, that could lead to the increase of the competitiveness of our business environment and to the consolidation of the companies with full or majority Romanian capital, as well as to the improvement of some of our macroeconomic indicators.

Last but not least, regulating competitive intelligence could contribute to the increasing of the security culture of the Romanian entrepreneurs, being also useful in preventing and deterring the development of certain illegal practices in our country.

References:

1. Academia Română. Institutul de Lingvistică „Iorgu Iordan – Al. Rosetti". (2016). *Dicţionar Explicativ al Limbii Române, Ed. A 2-a, rev*. Bucureşti: Univers Enciclopedic.

2. Călin, Ion. (2015, March). *Informaţiile din surse deschise – delimitări conceptuale*. *Buletinul Universităţii Naţionale de Apărare „Carol I"*, 192-196.

3. Centrul Surse Deschise. (n.d.). *Ghid OSINT*. Retrieved from https://www.sri.ro/upload/Ghid_OSINT.pdf

4. CIA. (2010). *INTelligence: Human Intelligence,* Retrieved from https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html

5. Clark, Robert M. (2013). *Intelligence Collection* (Kindle Edition). CQ Press.

6. Clark, Robert M. (2014). *Intelligence Collection*. Thousand Oaks: CQ Press.

7. *Constitution of Romania*. (1991). Retrieved from https://www.constitutiaromaniei.ro/art-31-dreptul-la-informatie/

8. Cook, Michelle, Cook, Curtis. (2000). *Competitive Intelligence: Create an Intelligent Organization and Compete to Win*. London: Kogan Page Limited.

9. *Criminal Code*. (2009). Art. 16 Guilt, Retrieved from https:// legeaz.net/noul-cod-penal/art-16

10. Directive (EU) 2016/943. (2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&from=EN

11. European IPR Helpdesk. (n.d.). *Trade secrets: An efficient tool for competitiveness*, Retrieved from https://www.iprhelpdesk.eu/sites/default/ files/newsdocuments/Fact-Sheet-Trade-Secrets.pdf

12. Gill, Peter, Phythian, Mark. (2011). *Intelligence in an Insecure World*. Cambridge: Polity Press.

13. Government Emergency Ordinance no. 25. (2019). Retrieved from https://lege5.ro/Gratuit/gmzdqnbsga4q/ordonanta-de-urgenta-nr-25-2019-privind-protectia-know-how-ului-si-a-informatiilor-de-afaceri-nedivulgate-care-constituie-secrete-comerciale-impotriva-dobandirii-utilizarii-si-divulgarii-ilegale-precu

14. Institute for Competitive Intelligence. (2017). *Insight Expert Interview, Human Intelligence in Competitive Intelligence*, Germany. Retrieved from https://www.institute-for-competitive-iintelligence.com/expert-interviews/ video-channel/expert-interviews/expert-interview-human-intelligence-in-competitive-intelligence

15. Interagency OPSEC Support Staff. (1991, April). *Compendium of OPSEC Terms*, Greenbelt. MD: IOSS, in Operations Security. (n.d.). *Intelligence Threat Handbook, Intelligence Collection Activities and Disciplines*, Retrieved from https://fas.org/irp/nsa/ioss/threat96/part02.htm

16. Jimenez, David. (2005). *Corporate Intelligence* in Carlisle, Rodney P. (Ed.). Encyclopedia of Intelligence and Counterintelligence (Vol. 1). Armonk: Golson Books Ltd.

17. Johnson, Loch K. (2007). *Handbook of Intelligence Studies*. New York: Routledge.

18. Kahaner, Larry. (1996). *Competitive Intelligence: How to Gather, Analyze and Use Information to Move your Business to the Top*. New York: Simon & Schuster.

19. Lansley, Cliff. (2017). *Elicitation – Would you recognise it?*, Retrieved from https://www.eiagroup.com/elicitation-would-you-recognise-it/

20. *Law no. 298*. (2001, June 7). Retrieved from http://www. cdep.ro/pls/legis/legis_pck.htp_act_text?idt=28203

21. Liebowitz, Jay. (2006). *Strategic intelligence: business intelligence, competitive intelligence, and knowledge management*. Boca Raton: Auerbach Publications.

22. Logan, Keith Gregory (Ed.). (2010). *Homeland security and intelligence*. Praeger.

23. Lowenthal, Mark M. (2001). *OSINT: The State of the Art, the Artless State*. Studies in Intelligence 45, no. 3 in Mercado, Stephen C. (2004). *Sailing the Sea of OSINT in the Information Age*, Studies in Intelligence Vol. 48, No. 3, Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol48no3/pdf/v48i3a05p.pdf

24. Lowenthal, Mark. (2003). *Intelligence: From Secrets to Policy*, 2nd ed. Washington: CQ Press, in Norwitz, Jeffrey H. (n.d.). Disrupting Human Networks: Ancient Tool for Modern Challenges. in Logan, Keith Gregory (Ed.). (2010). Homeland security and intelligence. Praeger.

25. Medar, Sergiu, Lăţea, Cristi. (2007). *Intelligence pentru comandanţi*. Bucureşti: Editura Centrului Tehnic Editorial al Armatei.

26. Mercado, Stephen C. (2004). *Sailing the Sea of OSINT in the Information Age*, Studies in Intelligence Vol. 48, No. 3, Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol48no3/pdf/v48i3a05p.pdf

27. NATO. (2001). *NATO Open Source Intelligence Handbook.* Retrieved from http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf

28. Nițu, Ionel. (2012). *Analiza de intelligence: o abordare din perspectiva teoriilor schimbării*. Bucureşti: Ed. RAO.

29. Norwitz, Jeffrey H. (n.d.). *Disrupting Human Networks: Ancient Tool for Modern Challenges.* In Logan, Keith Gregory (Ed.). (2010). Homeland security and intelligence. Praeger.

30. Operations Security. (n.d). *Intelligence Threat Handbook*, Intelligence Collection Activities and Disciplines, Retrieved from https://fas.org/irp/nsa/ioss/threat96/part02.htm

31. Petrescu, Stan. (2011). *Despre intelligence: spionaj-contraspionaj*. Craiova: Sitech

32. Peled, A., Dror, H. (2010). *HUMINT: Combating corporate crime with a counter-terrorism methodology*. *Secur J* 23**,** 320–331. https://doi.org/10.1057/sj.2008.24

33. *Regulation (EU) 2016/679*. (2016, April 27). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=RO

34. Shulsky, Abram N., Schmitt, Gary J. (2006). *Războiul tăcut: introducere în universul informaţiilor secrete*. Iaşi: Editura Polirom.

35. Steele, Robert David. (2007). *Open source intelligence*. In Johnson, Loch K. (2007). Handbook of Intelligence Studies. New York: Routledge.

36. *Strategic & Competitive Intelligence Professionals*. (n.d.). The SCIP Code of Ethics, Retrieved from https://www.scip.org/page/Ethical-Intelligence.

37. Taylor, Wayne N. (2010). *The Dark Arts of Business, The Lessons Not Taught in the Classroom or Boardroom: Elicitation*. Lulu Enterprises, Inc.

38. *The National Council for the Study* of the *Securitate Archives*. (n.d.). *Index of frequently used terms and abbreviations in Securitate documents*. Retrieved from http://www.cnsas.ro/documente/arhiva/Dictionar%20 termeni.pdf

39. UNSW Library (n.d.). *Primary and secondary sources.* Retrieved from https://www.library.unsw.edu.au/study/information-resources/primary-and-secondary-sources

40. U.S. Department of Justice Federal Bureau of Investigation. (n.d.). *Elicitation*. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiBwriOo6HpAhWMURUIHecfCaoQFjAAegQIARAB&url=htpps%3A%2F%2Fwww.fbi.gov%2Ffile-repository%Felicitation-brochure.pdf%2Fview&usg=AOvVaw0o9xGs2Yy16McK1zFf-1pj

41. Waltz, Edward. (2003). *Knowledge management in the intelligence enterprise*. Norwood: Artech House, Inc.

42. W.E.P.A. Agency. (n.d.). *Humint Services*, Retrieved from https://www.wepa.agency/humint-services/