CHAPTER 3
MODERN MANAGEMENT TECHNOLOGIES

THE MAIN WAYS OF LEAKING COMMERCIAL SECRETS AND MEASURES TO PROTECT THEM

Hisham Jadallah Mansour Shakhatreh[1], Esraa Mohamed Ababneh[2]

[1]Ph.D. (Law), Assistant Professor, Faculty of Law, Jadara University, Jordan, e-mail: dr_hisham_shakhatreh@yahoo.com, ORCID: https://orcid.org/0000-0001-8693-5744

[2]Faculty of Business, Autonomous University of Barcelona, Barcelona, Spain, e-mail: esraaababneh99@gmail.com ORCID: https://orcid.org/0009-0007-1586-1646

Citation:
Shakhatreh, H., & Ababneh, E. M. (2023). The main ways of leaking commercial secrets and measures to protect them. *Economics, Finance and Management Review*, (2), 76–82. https://doi.org/10.36690/2674-5208-2023-2-76-82

Received: May 26, 2023
Approved: June 29, 2023
Published: June 30, 2023

Abstract. *The study is devoted to the study of international experience in the protection of trade secrets in the leading countries of the world. The purpose of the study is a comparative analysis of the features of international experience in protecting the commercial secrets of corporations. The methodological basis of the study was the use of methods of comparative analysis, methods of analysis and synthesis, as well as an expert survey and a graphic method for presenting the results of the study. The main results of the study are the systematization of commercial information according to the degree of protection, as well as the generalization of the practice of the EU member states regarding the protection of commercial secrets. The main ways of disclosing information constituting a commercial secret are classified: communication of the specified information to other persons, in particular to competitors; providing documents containing information constituting a commercial secret to other persons for perusal; notification of the above-mentioned information in mass media, etc. Systematized measures for the protection of confidential information constituting a commercial secret, namely: organizational, legal, physical, technical and psychological. Organizational measures include a set of measures to protect information that is important for the enterprise by restricting access to it. Technical means involve the use of special programs and equipment that make it impossible to view and/or copy important electronic information. Legal measures involve bringing the internal documents of the corporation into compliance by making appropriate additions to them. The study presents the results of a survey of representatives of EU commercial structures regarding the leakage of trade secret information and tools for protection against leakage.*

Keywords: *corporation; information; commercial information; trade secret; flow of information; information protection.*

JEL Classification: K12, K33, K42

Formulas: 0; fig.: 3; tabl. 1; bibl.: 10

Introduction. The first consequence of the lack of a harmonised system for the protection of trade secrets is the lack of a uniform definition of "trade secrets" within the European Union, Switzerland, Japan and the United States. The general definition of "trade secrets" is provided by Article 39.2 of the TRIPS Agreement:

"Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:

a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

b) has commercial value because it is secret; and

c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."

This definition is often acknowledged by the case law of the EU countries which do not have a statutory definition. Nevertheless, the requirements provided therein can indirectly be found in many of the definitions adopted by the other EU jurisdictions. In Italy, Portugal and Sweden, a statutory definition of trade secrets is provided by the respective specific laws.

By way of an example, the definition of "trade secrets" provided by the Swedish law, included in Section 1 of the Trade Secret Act, reads as follows: "For the purpose of this Act a trade secret means such information on business relations or operating conditions of a business in somebody's business which is kept secret and of which the disclosure is aimed at causing damage to the business proprietor from a competition point of view".

A statutory definition of trade secrets is also available in the unfair competition provisions of Bulgaria, Czech Republic, Greece Poland and the Slovak Republic. In Hungary and Lithuania, the statutory definition is provided in their respective Civil Code. In Slovenia, information is deemed to be a trade secret if so determined by a company in a written resolution. In all the other EU Member States, where no formal definition of trade secret exists (i.e., Austria, Belgium, Cyprus, Denmark, Estonia, Finland, France, Germany, The Netherlands, Republic of Ireland, Latvia, Luxembourg, Malta, Romania, Spain and to a certain extent UK), this has been developed by courts and commentators.

The review of the different definitions has shown the presence of some common requirements. In general, a trade secret is defined as:

i) technical or commercial information related to a business;

ii) which is not generally known or easily accessible;

(iii) which has economic value (i.e., it confers a competitive advantage to the owner); and

iv) which disclosure to a competitor, could cause a prejudice to the owner's interest.

The review has also shown that in almost all countries, the (statutory or jurisprudential) definition of trade secrets is very broad and suitable to encompass

different types of information. In principle, any type of information is potentially capable of being protected as a trade secret, as long as the above criteria are met. We also noted that often, commentators and courts tend to categorise trade secrets into two main types:

i) Technical secrets, which include any type of technical information, as manufacturing processes, technical drawings and designs, prototypes, inventions (not patentable or not patented), technical know-how, formula or recipes, genetic materials, fragrances, etc.

ii) Commercial secrets, which include customers and suppliers list; information on business strategies and plans, business models, cost and price information, other marketing information, etc.

It is worth noting that although the TRIPS Agreement qualifies "undisclosed information" as a type of intellectual property right, and despite a close relationship between trade secrets and intellectual property rights has been pointed out in many countries, most of the EU Member States do not attach the status of intellectual property rights to trade secrets. Exceptions can be found in some EU Member States such as Italy, France, Latvia, Romania (only with regards to know-how), Slovak Republic and Spain (at least formally).

Considering a trade secret as an IP right under national legislation would trigger the application of the remedies provided by the Enforcement Directive for intellectual property rights, however, due to the different form of implementation adopted by Member States, this does not automatically foster the creation of a more uniform legal system. The Enforcement Directive is applicable to trade secrets only in Italy, Portugal (to the extent the law implementing the Enforcement Directive is applicable to unfair competition conduct), Slovak Republic and to a certain extent in Romania.

Outside Europe, a statutory definition of “trade secrets” is provided by the Japanese Unfair Competition Prevention Act and by the US UTSA. Switzerland does not have a statutory definition, but case law and scholars have generally accepted the criteria identified by Article 39.2 of TRIPS. Furthermore, in Japan and the United States, trade secrets are generally considered to be intellectual property rights, but not in Switzerland.

Aims. The purpose of the study is a comparative analysis of the features of international experience in protecting the commercial secrets of corporations.

Methodology. The methodological basis of the study was the use of methods of comparative analysis, methods of analysis and synthesis, as well as an expert survey and a graphic method for presenting the results of the study.

Results. To understand the sources of the information leak, we offer the results of a study conducted by the company to identify the persons involved in it.

One of the first steps in the direction of classification of persons who disclose trade secrets was made by the international research company IDC, which presented its view on the problem in 2006. According to IDC, the system of insiders has four levels: "citizens", "violators", "renegades", "traitors" (Fig. 1).

The top tier consists of "citizens" — loyal employees who very rarely (if ever) violate corporate policy and are generally not a security threat [4].

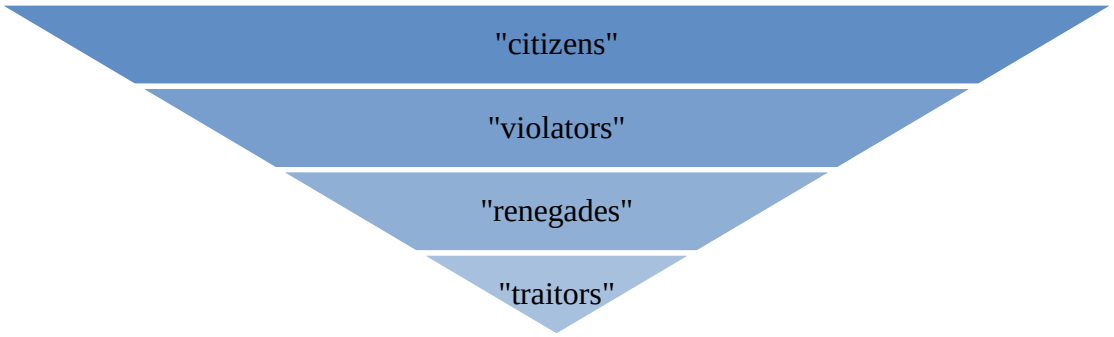

Figure 1. Classification of insiders according to IDC studies [4]

Source: developed by authors

At the second level are "violators", who make up a large part of all employees of the enterprise. These employees allow themselves small familiarities, work with personal web mail, play computer games and make online purchases. Representatives of this level of violators pose a threat to information security, but these incidents are random and unintentional.

At the next level are "renegades" - employees who spend most of their working time doing things they shouldn't be doing. These employees are abusing their Internet access privileges. Moreover, such employees can send confidential information of the company to external recipients interested in it. Thus, "renegades" represent a serious security threat.

At the lowest level, there are "traitors" - employees who deliberately and regularly put confidential company information at risk (usually for a financial reward from an interested party). Such employees represent a real threat, but they are the most difficult to catch [139].

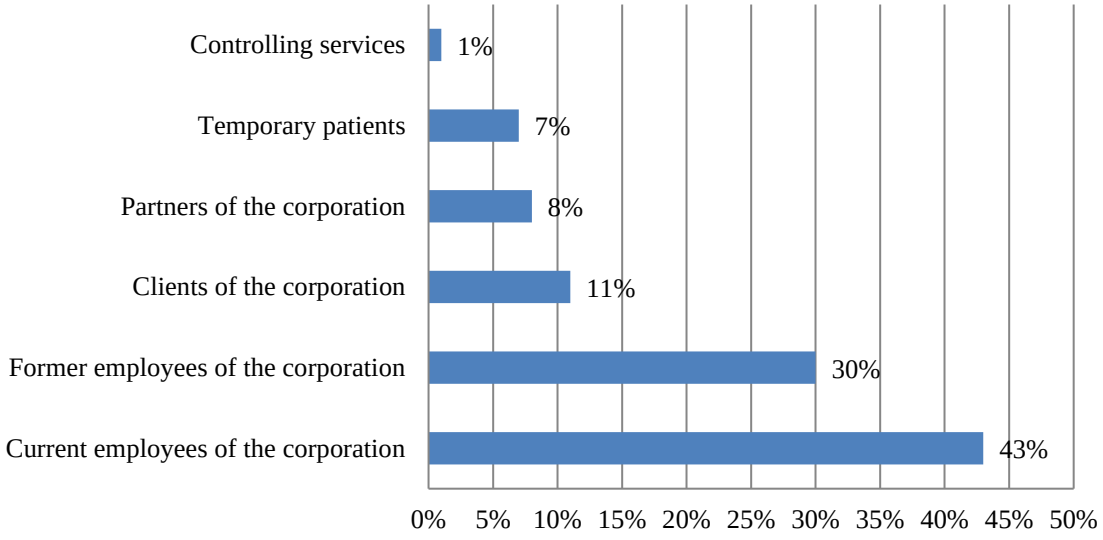

Figure 2. The structure of the subjects of the leak of insider information about the activities of the joint-stock company

Source: [5]

Analysts have estimated that 43 and 30% of incidents are caused by current and former employees, respectively, 11% are caused by part of the company's customers, 8% are caused by partners and, finally, 7% are caused by temporary employees (contract workers, consultants, etc.). This indicates that the problem of leakage of confidential information is at the top of the list of priorities of the company's management [4].

The most common factors for the disclosure of restricted information by employees are shown in Table 1. As can be seen from the table, the disclosure of restricted information by employees is most often carried out due to the fact that the management of companies does not pay attention to the threats of information leakage related to personnel, that is, insiders.

Table 1. Factors of information disclosure by employees [5]

№ п/п	Factors	%
1	Excessive talkativeness of employees	32
2	The desire of employees to earn money by any means and at any price	24
3	Absence of the security service company	14
4	"Soviet" habits of company employees to share with each other (traditional exchange of experience)	12
5	Uncontrolled use of information systems	10
6	The presence of opportunities for conflict situations to arise among employees: lack of psychological compatibility, random selection of personnel, lack of work on team cohesion, etc.	8

Source: developed by authors

Therefore, after analyzing the data privacy threats that are related to personnel, it can be seen that ignoring these threats leads to serious losses in enterprises. It is not only about the financial losses of the company, but also about the sharp drop in its image due to the fact that it cannot protect its own confidential information.

In this connection, the issue of improving the efficiency of the economic security service of joint-stock companies and its interaction with the company's internal divisions and external bodies and administrations is acute.

Protection of confidential information, which constitutes a commercial secret, can be ensured by a complex of legal, organizational, technical and other measures (Fig. 3).

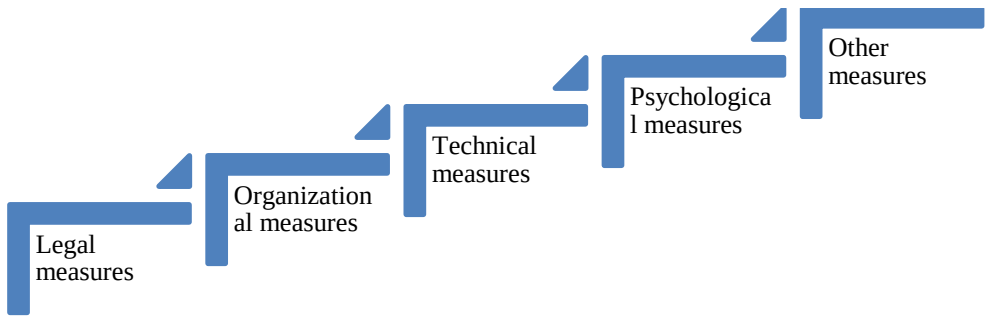

Figure 3. The main measures that are necessary to protect the commercial secret of the corporation

Source: developed by authors

Legal measures - in order to protect commercial secrets, each corporation needs to regulate appropriate measures in its internal documents.

The right of a business entity to commercial secrecy can be formalized by making appropriate additions to the following documents:

• the statute of the enterprise (it is prescribed that the regime of commercial secrecy is introduced);

• founding agreement;

• collective agreement;

• provisions on commercial secrecy and rules for its preservation;

• provisions on the permission system for access of executors to documents and information constituting the commercial secret of the enterprise; on the mode of work of employees with data constituting a commercial secret, or to other local documents.

When drawing up an employment relationship, it will be very useful to provide, for example, the following obligations for employees to protect commercial secrets:

- to keep a commercial secret that becomes known to them in the course of work, and not to disclose it without permission issued in the prescribed manner, provided that the information that constitutes a commercial secret was not known to them before or was not received by them from a third party without obligation to observe their confidentiality;

- comply with the requirements of instructions, regulations, and orders to ensure the preservation of commercial secrets;

- in the case of an attempt by third parties to obtain from them information that constitutes a commercial secret, immediately report this to the relevant official or to the relevant division of the business entity;

- to keep commercial secrets of business entities with which there are business relations; - not to use knowledge of trade secrets to engage in activities that, as a competitive action, may harm the business entity;

- in the case of dismissal, transfer all information carriers constituting a commercial secret (manuscripts, drafts, documents, drawings, magnetic tapes, punched cards, punched tapes, discs, diskettes, printouts on printers, film and photo films, models, materials, etc.) that were at their disposal, the relevant official.

Organizational measures - in order to protect information that is important for the enterprise, it is necessary to limit employees' access to it, that is, each employee gets the opportunity to work only with those data that are necessary for the performance of his duties.

Technical measures – special programs and equipment are used to protect information, which make it impossible to view and/or copy important electronic information. For this, access to the hard disk or the possibility of using removable digital media is blocked. Implementation of such measures is usually entrusted to the system administrator.

Information constituting a commercial secret should be divided into categories according to the level of importance:

1) information that requires maximum secrecy;

2) information, the disclosure of which is possible, but not desirable;

3) everyday working information.

They also compile a list of employees who have access to each group of information.

The ways of disclosing information constituting a commercial secret can be different:

• communication of the specified information to other persons, in particular to competitors;

• providing other persons with documents that contain information constituting a commercial secret;

• notification of the above-mentioned information in mass media, etc.

Conclusions. The analysis has revealed the lack of a uniform definition and scope of protection of trade secrets throughout the European Union. In most of the countries protection is not specific and provisions dealing with trade secrets are scattered over completely different fields of law. According to the contributing countries' opinion, such a fragmentation of legislation might entail a risk of inconsistent interpretation of what is protectable as trade secret and consequently, make trade secrets enforcement difficult and costly to handle.

Author contributions. The authors contributed equally.

Disclosure statement. The authors do not have any conflict of interest.

References:

1. François Dessemontet. Protection of Trade Secrets and Confidential Information. URL: https://www.unil.ch/files/live/sites/cedidac/files/Articles/Protection%20Trade%20Secrets.pdf
2. Study on Trade Secrets and Confidential Business Information in the Internal Market. URL: c
3. Barbe, A. & Linton, K. (2016). Trade Secrets: International Trade Policy and Empirical Research: Draft Version: (August 5, 2016) https://www.oecd.org/sti/144%20-%20OECD%20Trade%20Secrets%202016-8-5.pdf.
4. Information and Data Security. URL: https://www.idc.com/getdoc.jsp?containerId=IDC_P33456
5. Friedman, David D., William M. Landes, and Richard A. Posner. 1991. "Some Economics of Trade Secret Law." *Journal of Economic Perspectives*, 5 (1): 61-72.
6. Linton, K. (2016). The importance of trade secrets: new directions in international trade policy making and empirical research. *J. Int'l Com. & Econ.*, 1.
7. Farouq Ahmad Faleh Alazzam, & Rasha Bashar Ismail Al sabbagh. (2021). The importance of non-tariff barriers in regulating international trade relations. *Public Administration and Law Review*, (1), 92–104. https://doi.org/10.36690/2674-5216-2021-1-92
8. Coe, R. N. (1994). Keeping trade secrets secret. *J. Pat. & Trademark Off. Soc'y*, *76*, 833.
9. Mihus , I., Akimova , L., Akimov O., Laptev , S., Zakharov , O., & Gaman , N. (2022). Influence of corporate governance ratings on assessment of non-financial threats to economic security of joint stock companies. *Financial and Credit Activity Problems of Theory and Practice*, *6*(41), 223–237. https://doi.org/10.18371/fcaptp.v6i41.251442.
10. Alshunnaq, M. F., Alsabbagh, R. . B. I., & Alazzam, F. A. F. (2021). LEGAL PROTECTION OF intellectual property rights under jordanian legislation and international agreements. *Public Administration and Law Review*, (3), 18–32. https://doi.org/10.36690/2674-5216-2021-3-18.