TRADE SECRET PROTECTION IN THE U.S. AND EU.

LL.M. INTERNATIONAL BUSINESS LAW
OSMAN DAVID MEJIA HERNANDEZ
STUDENT NUMBER: U1271042
ANR: 135928
SUPERVISOR: PROF. MR. E.P. M. VERMEULEN
AUGUST 23, 2016
TILBURG, THE NETHERLANDS

ABSTRACT

The purpose of this study is to denote the importance of trade secrets in the U.S. and EU. The scope and duration of trade secrets are probably its most prominent feature, as a result, companies use trade secrets to protect information that otherwise could not be protected by patents. For this reason, the thesis identifies the differences between trade secrets and patents and the advantages in both cost and protection that makes trade secret the common mean of protection used by companies, mostly start-ups. Several reports demonstrate the value of trade secrets and its importance for the proper functioning of the internal market, promotion of innovation and economic growth of countries. However, they also expose the damage and losses generated by the theft and misappropriation of trade secrets. This data exposes the need for security and protection systems in business and the importance of strengthening legislation concerning trade secrets legislation concerning trade secrets.

Keywords: Trade Secrets, Misappropriation, Impact, U.S. legislation, EU Directive, Espionage

TABLE OF CONTENTS

1 CHAPTER 1: INTRODUCTION

The business world that we live in is highly competitive. Companies are obliged to persistently innovate in order to maintain or increase their dominance or status in the market. The companies that stand out are the ones that possess something different, including valuable information or a sense of know-how that gives them an advantage over others, which is why increasingly companies are investing in their Research and Development (R&D) departments.

In this technological era, R&D is of vital importance for a company's growth through the creation of new technologies and the finding of new possibilities for improvement in their products and/or services. The know-how, or information, that companies obtain through their R&D departments constitutes a valuable asset worth protecting. Companies protect this information through intellectual property, like patents, copyrights and trademarks, but it is in the way of trade secrets that companies safeguard most of their business information. The Coca-Cola recipe, KFC recipe or the Google algorithm are some examples of trade secrets in which these companies have generated millions in revenue, enforcing companies to take cautious measures to safeguard their secret commercial information especially in regard to the constant use of digital technology for data storage and communication, which may increase the risk of misappropriation and industrial espionage.

Globalization leads companies to be more engaged in cross-border transactions, which can present itself as an alluring target for information theft and sabotage.

The Report of the Commission on the theft of American Intellectual Property states "*In many ways, trade-secret theft is a foreseeable outgrowth of expanding international markets…"* (as

cited in Yeh, 2016). The risks posed by the theft of commercial information may discourage collaboration between companies from different countries. This collaboration is an important factor for innovation and competitiveness, especially for Small and Medium-sized Enterprises (SME) whom benefit from the sharing of information with larger companies. A weak protection on trade secrets can bring strict measures regarding information sharing, leading to subsequent detrimental effects on a company's growth and economic performance.

In order to safeguard the aforementioned information from theft or misappropriation, serious measures have to be taken into account. However, a large amount of unawareness persists in companies in regard to the protection of valuable information that should be protected and enforced in regards to trade secrets[1]. In his paper "Revealed: Operation Shady RAT (Alperovitch, 2011) states "that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly), with the great majority of the victims rarely discovering the intrusion or its impact".[2] Either by unawareness of the theft of commercial information, fear of bad reputation, or weak legislation in the protection of trade secrets, industrial espionage is a problem that hinders innovation and increases further losses in revenue for the company.

[1] http://www.wipo.int/export/sites/www/sme/en/documents/wipo_magazine/04_2002.pdf

[2] Dmitri Alperovitch, Revealed: Operation Shady RAT "An investigation of targeted intrusions into more than 70 global companies, governments, and non-profit organizations during the last five years"(2011)

2 CHAPTER 2: TRADE SECRETS AND THE TRIPS

Although the definition of 'trade secret' varies according to each individual legislation, the WIPO (World Intellectual Property Organization) provides us with a broad explanation of *"any confidential business information which provides an enterprise a competitive edge may be consider a trade secret*." [3]

Trade secrets constitute maybe the most value and important intangible asset of a company and there are some common rules and regulations about trade secrets. But as Pooley (2013) argue its regulation is under the scope of national laws which in most cases produces vagueness in its enforcement.

The Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) negotiated at the end of the Uruguay Round in 1994, can be considered as the first international legal instrument which provides for the definition of undisclosed information "often treated as synonym of trade secret" (Nair, 2002). The similarities among countries with regarding the concept of trade secrets corresponds to the definition set forth in article 39 TRIPS[4].

Which established that the information must contain this three requirements:

(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

[3] http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm

[4] Enquiries into Intellectual Property's Economic Impact, Chapter 3: Approaches to the Protection of Trade Secrets,pg.131OECD 2015, available at https://www.oecd.org/sti/ieconomy/Chapter3-KBC2-IP.pdf

(c) Has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[5]

The TRIPS provides protection for disclosure, acquisition or use contrary to honest commercial practices. For the purpose of clarifying, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.[6]

Even with a standard definition established by the TRIPS, we can say that there is still not a complete uniformity in the protection of trade secrets, as Sandeen (2011), stated "The TRIPS Agreement requires that WTO members put in place national systems to protect trade secrets against acts of unfair competition" (as cited in Schultz & Lippoldt, 2014, pg.8).[7] Since the TRIPS allows countries to establish mechanisms of protection according to their national law, some variation in the means of protection exist between countries. Apart from the basic standards for defining a trade secret that the TRIPS provide, there should be more uniformity in the coverage about the protection and enforcement of trade secrets between countries.

[5] Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS). Art.39.2

[6] "a manner contrary to honest commercial practices" defined in note 10, Art.39 to the TRIPS Agreement

[7] Mark F. Schultz and Douglas C. Lippoldt. Approaches to Protection of undisclosed information (Trade Secrets). (2014). OECD Trade Policy Paper No.162, pg.8. Available at http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2013)21/FINAL&docLanguage=En

3 CHAPTER 3: WHICH MECHANISM TO USE TO PROTECT MY IDEAS?

3.1 Differences between Trade Secrets and Patents

Innovative ideas or new technologies constitutes a fundamental part of a company's intangible assets and are protected by intellectual property. When it comes to the protection of information by enterprises the most common used mechanisms are patents and trade secrets.

The question that many entrepreneurs ask themselves is whether they should protect their innovative ideas by patent or trade secret law. It can be a common belief that companies prefer to protect their ideas through patents, but "some surveys indicates that in many industries, secrecy is considered more important than patents as a means of protecting IP." (Scherer, et al., 1959; Taylor and Silberston, 1973; Mans_eld, 1986; Levin, et al., 1987; Cohen, Nelson and Walsh, 2000, as cited in Dass, Nanda, & Chong Xiao, 2014). It is of great importance for companies to assess the advantages and disadvantages of the use of patent or trade secret regarding the protection and development of their innovative ideas. By doing so, companies can determine the most appropriate instrument for protection according to the specific case.

3.1.1 Subject Matter

To begin with, trade secrets provide a wider scope with regards on what type of information can be protected, as stated by Beckerman-Rodau (2002) "almost anything that is maintained in secret, that is not generally known to competitors and which provides a competitive advantage is potentially protectable via trade secret law". Given that there are no subject matter constraints "trade secret laws apply to areas that patent law cannot, allowing the protection of business plans, customer's lists, and so-called "negative know-how" (Lemley, 2008 as cited in International Chamber of Commerce, 2014).

On the other hand, it is more difficult when an idea falls into the scope of patentability as it has to meet the requirements of novelty, utility, and non-obviousness. Also, this latter requirement could be viewed as a barrier to obtaining patent protection because some inventions could not be considered inventive enough, especially by a typical person skilled in the relevant technology (Beckerman-Rodau, 2002, para.70-73).

3.1.2 Scope of Protection.

Another essential difference is the level of protection which is different between trade secrets and patents. For one thing, patents usually provides protection for up to 20 years counting from the filing date.[8]Nevertheless, this does not always happen, given that the market is very competitive and is in constant innovation, new and better products may adversely change the value of the patent (The University of Melbourne, Melbourne Institute of Applied Economics and Social Research, 2004). Therefore, as the value of the patent diminishes so it does the interest of preserving the protection.

On the contrary, the protection that trade secrets provide is unlimited as long as secrecy is maintained. Although, it may sound great to have unlimited protection this comes at a certain cost, there are still ways to lose protection. For instance, a product containing a trade secret can easily lose it secrecy by reverse engineering, independent discovery or by disclosure either by mistake or by improper means. Before making the decision of whether to protect an innovative idea through patent or trade secret, it is important to assess the type of product and its value, considering that if the trade secret contained in the product is easily accessible by reverse

[8] Article 33 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) available at https://www.wto.org/english/docs_e/legal_e/27-trips.pdf

engineering or it can be obtained by independent discovery, it would be more convenient to protect the idea with a patent.

Choosing the right strategy can be of significant importance in determining a company's value, as Beckerman-Rodau, (2002) argues that determining the economic value of a company that possesses trade secrets is much more difficult compared with other in possession of patents, due to unavoidable factors that may affect the trade secret. The lack of valuation of a company can be an adversity in selling the company or in obtaining funds.

The length of protection also applies between trade secrets and patents is when it comes to licensing. The difference is simple, the licensing through patents expires when the patent protection term comes to an end, while trade secrets can be license almost in an unlimited term even if the information has been disclose to the public, as it happened in the famous Listerine case (American Bar Association, 2010).

3.1.3 Protection Procedure and Costs.

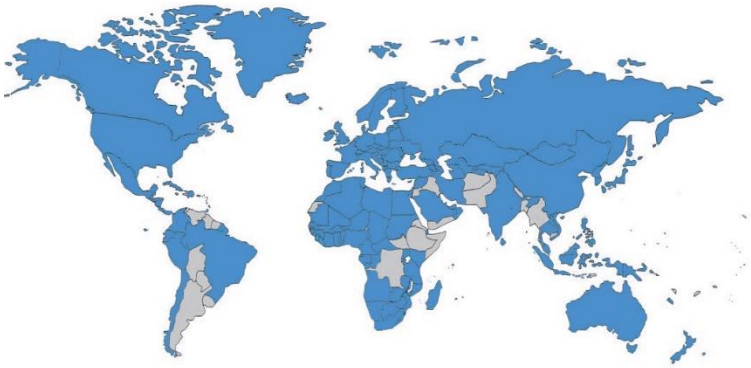
When it comes to obtain patent protection, the process can be long and expensive both in the United States and the European Union, due to the disclosure and registration requirements which includes government and attorney fees which make the patent holder to incur in more expensive costs.

It should be noted, that there are procedures that are aimed at simplifying patent applications and cost reduction, as can be seen in the regulations agreed by the Council of the European Union and the European Parliament for a Unitary Patent Protection and a Unified Patent Court. This new unitary system of patent protection will allow patent protection in the 25 member states that

signed the agreement and reduce cost by means of a single renewal fee, it will also simplify the process of conflict resolution through the unified patent court.[9]

At an international level there is the Patent Cooperation Treaty which consists of 150 contracting states and through an international patent application can provide protection in a considerable number of countries. (See map below)

Figure 1: Contracting Countries of the Patent Cooperation Treaty



Source: World Intellectual Property Organization (WIPO), available at http://www.wipo.int/pct/en/pct_contracting_states.html

While these procedures are intended to simplify the process of obtaining a patent and reduce costs, acquiring protection through patentability remains the most expensive and exhausting way. Instead to the method of protection of trade secrets in which there is no need for disclosure or payment of fees and where the only expense that will be incurred is in applying reasonable measures to maintain the secrecy of the trade secrets. "The fact that trade secrets may be protected without governmental help, as well as their attractiveness to resource-constrained firms, suggest that they may play an important role on the innovation strategies in developing-country firms" (Linton, 2016, p. 8). Companies both in developed and developing countries,

[9] http://www.government.se/articles/2015/06/member-states-meet-users-in-patent-reform/

especially entrepreneurs and SMEs often pursue a vast and economic protection for their innovative products and processes. In addition, "trade secrets can apply to a range of approaches use by SMEs to capture the value of their innovations, reinforcing strategies such as lead-time, product complexity, and close customer relationships" (International Chamber of Commerce, 2014). The broad scope of protection plus the low costs compared to patents, allures companies to use trade secrets as their protection mechanism.

3.1.4 Enforcement of Rights.

The enforcement of patent rights presents differences from that of trade secrets. For instance, patents grants an exclusive right, which means that there is a prohibition for third parties to manufacture, use, offer for sale, sell and import the patented product without a license or express consent from the patent owner. Because the exclusive right is maintained throughout the duration of the patent, a violation of that right by good faith cannot be used as an argument by the defendant in a patent infringement case (Beckerman-Rodau, 2002). In contrast, trade secrets do not provide an exclusive right, due to the fact that trade secrets can be obtained by legal means such as reverse engineering or independent discovery.

3.1.5 Infringement

Patent infringement occurs when there is a violation of the patentee's exclusive right. In their work, W. Kintner & L. Lahr, (1975) argue about the three types of infringement encompassed in the US Patent Act [10], which are: direct, active inducement and contributory.

[10] 35 U.S.C. Section Index; Part III: Patents and Protection of Patent Rights; Chapter 28: Infringement of Patents Section 271 Available at http://www.bitlaw.com/source/35usc/271.html

Fisrt, literal reading of the claims and doctrine of equivalents can be used to prove direct infringement. To understand the first one, we can address to the explanation provided in the Engel Industries, Inc. v. The Lockformer Company, (1996), which states that "Literal infringement of a claim exists when every limitation recited in the claim is found in the accused device, i.e., when the properly construed claim reads on the accused device exactly". The infringement can be noted if the elements of the device that infringes the patent falls within the patent claim.

As regarding the doctrine of equivalents, W. Kintner & L. Lahr, (1975), manifest that the doctrine is a result of the efforts of the courts to protect patent rights in the cases when there was not a literal infringement. To provide a clear understanding, the authors cite the interpretation of the Supreme Court in the Sanitary Refrigerator case (1929) stating that "one device is an infringement of another… if two devices do the same work in substantially the same way, and accomplished substantially the same result,…even though they differ in name, form or shape."

Second, active inducement can be define as the act of persuading or convincing a third party to infringe a pantent. For an active inducement infringement to occur, the compliance of the following assumptions is needed: first, that the defendant acted with scienter giving as a result an infringement of the patent right by a third party and second, that the third party infringed the patent.

Finally, regarding the definition of contributory infringement ,W. Kintner & L. Lahr, (1975) establish that given the difficulty of understanding the concept as a whole and with the finality of getting a clear idea, it is advisable to look at Mr. Pasquale Federico's explanation who breaks down the concept in five subsections. First, it is neccesary that the sold accused device must be a "component" of the patented product or process. Second, it must "constitute a material part of

the invention". Third, the manufacture or adjustment of the sold accused device must be "used in an infringement of the patent". Fourth, the seller must have knowledg of third requirement, and fifth the sold accused device must not be "staple product or commodity of commerce suitable for substantial noninfringing use" (W. Kintner & L. Lahr, 1975).

In contrast, trade secret infringement occurs when it has been a breach of duty or a misappropriation. Regarding the breach of duty Lippoldt & Schultz., (2014) argue about two types of breach of duty: express and implied. In relation to the first one, the authors express that most trade secrets owners turn to written documents such as contracts as the most common form of protection of trade secrets, another example could be non-disclosure agreements. When it comes to the implied duty, they point out that the infringement falls into a breach of trust, in which this gap is particularly true in labor and business relationships. The fact that these relationships occasionally develop which such celerity in various situations, makes it complicated to sometimes settle written agreements in order to safeguard the trade secret, which must rely on the factor of trust. Finally, the lack of knowledge of the implied duty should not be an issue given the justifiable efforts in which the trade secret owner incurred in pursuance of maintaining secrecy (Lippoldt & Schultz., 2014). In relation to misappropriation, it is important to note that "liability for trade secret misappropriation … is generally limited to cases of wrongful conduct or violation of honest commercial practices" (Linton, 2016). Infringement by misappropriation does not require a close relationship with the trade secret owner. They are usually actions of rival firms that maliciously intend to acquire trade secrets of its competitors in the interest of gaining an advantage in the market.

3.1.6 Remedies

In relation to the remedies that can be applied, the American Bar Association, (2010) suggests that trade secret offers more options than patents. The objective of the remedy obtained by the patent is to recover actual losses when there has been a violation but it cannot request the return of profits illegally obtained by the infringer, different from trade secret which allows the recovery of "unjust enrichment". Moreover, when the plaintiff in a trade secret case cannot provide enough evidence to proof damages or unjust enrichment, it can be subject to a reasonable royalty.

4 CHAPTER 4: THE IMPACT OF TRADE SECRET THEFT

The digital age in which we live allows us to have all kinds of information at our fingertips with just one click and it has changed the way we interact. Jorgenson & Vu, (2016) argue that the way in which people relate to each other in the world today is thanks to the Information and Communication Technology (ICT). ICT brings along transformations in the economic and social sphere that impacts and influences all industries as well as our way of life.

Companies' worldwide benefit from the speed in which information can be exchanged, giving, as a result, an improvement in the ease that their business activities are developed. ICT allows storage of trade secrets digitally, as a result trade secrets may be contained in the many national or cross-border activities that companies carry on a daily basis with their business partners, which can be a target of theft.

The ease of acquiring information facilitates the theft of trade secrets, as an illustration, we can refer to the case United States of America, Plaintiff-Appelle, v. Joya Williams, Defendant-Appellant (2008), Williams was an executive assistant at Coca-Cola. In late December 2005, she

contacted Edmund Duhaney, who also worked at Coca-Cola, to discuss some copies of confidential documents that may be interesting to Coca-Cola competitors. The confidential information acquired by Williams contained marketing documents and a sample of the product, such information was acquired using a USB device. Since she had signed a nondisclosure agreement with Coca-Cola, for this reason, she asked Duhaney to be in charge of seeking possible buyers of information. To which, Duhaney contacted a friend, Dimson, that was interested in the documents since they were of great value. The three filed a meeting to refine details, in which Williams suggested that Pepsi could be interested in acquiring information. After Dimson sent an email to a purchasing executive of Pepsi offering and detailing the documents that he had in his possession, Pepsi sent a fax to Coca-Cola, containing the mail Dimson had sent them. During the investigations by the FBI, Dimson tried to sell the documents at an approximate price of $ 1.5 million to one FBI agent posing as a buyer.

Dimson, Duhaney, and Williams were arrested and charged with conspiracy to steal trade secrets. Dimson pleaded guilty without a plea bargain, while Duhaney pleaded guilty with a written plea bargain and agreed to testify against Williams, while Williams pleaded innocent. After a lengthy trial, Williams was sentenced to 96 months in prison and Dimson to 60 months. Whilst, Duhaney received 2 years because of his collaboration.

4.1 A tendency on the rise.

Theft of trade secrets is a threat that is increasing, as argued by Villasenor (2015), cybercriminals aim to find vulnerabilities in order to breach into a security system and hijack "valuable trade secrets". There are many factors that make feasible digital theft of trade secrets, according to Pellegrino (2015)"the plethora of information moving over IT networks, the ease of

access to cyberspace and the difficulties in attributing malicious attack have all contributed to this shift".

There are risks to trade secrets of all kinds and forms. As noted by Almeling (2012) most of the information that people acquire is now digitally. "Cloud computing" is a very common method nowadays to store information used by individuals, businesses and bureaucracy. Although these systems provide protective measures, fully reliance should not be taken, on the grounds that there are always risks.

The risks are greater because not only people who have access to trade secrets can be a threat. Highly skilled criminals are a greater threat, taking into consideration the ease in which they can acquire information without being discovered, as a result victims are not often aware of the attacks.

However, not everything is bad news, as well as there are methods of acquiring information illegally, there are also measures that can be used to detect misappropriation of trade secrets. Establishing a system for monitoring information as well as a method to retrieve and implementing an employee monitoring system are some steps that can be taken. (P.1099-1101)

This is an issue that is not only affecting businesses but also countries, undermining their technological sectors, consequently affecting the economy. For instance, the General Intelligence and Security Service, Ministry of the Interior and Kingdom Relations, (2014) in their Annual Report AIVD states that:

> The Dutch economy is one of the most competitive and innovative in the world. It is also the most digitized, which makes it particular vulnerable to digital espionage. The digital economic espionage damages the Netherlands' earning potential and so represents a

growing risk to the innovative and competitive ability of the entire national economy. (P.24-25)

Digital espionage is an issue that affects both the public and private sector, in which is important that governments and businesses take steps to prevent substantial threats. With this in mind, joint efforts have been made by the European Union (EU) and the United States (U.S.) in order to confront this problematic through the EU-U.S. cooperation on cyber security and cyberspace that addresses transnational cybercrime and other cyber threats.[11]

The U.S. and the EU are the regions most affected by trade secret theft. For instance, as Pellegrino (2015) noted "20% of the European companies have been breach, but actual figures may be much higher", which should be of concern especially since the EU contains four of the top ten companies that generated more revenue in 2015.[12]

The situation is even more worrying if we look at the data supplied by the report on Impact Assessment of the European Commission, (2013) which shows that "in Germany, estimations made in 2010 considered the actual damage caused by industrial espionage in Germany "*is in the region of 20 billion euros*", although other experts consider that the real damage could be closer to 50 billion". The same report notes that in March 2012, a survey of 600 mid-sized businesses among 6 EU countries (DE, ES, FR, HU, NL and UK) concerning business data or theft, exposed the main impacts that businesses experienced, which were: professional liability/exposure (54%); reputational impacts (48%); financial impacts/including loss of business (33%) and regulatory penalties or sanctions (25%). (European Commission, 2013, p.175)

[11] European Union External Action, Fact Sheet "EU-US cooperation on cyber security and cyberspace", Brussels, 26 March 2014 140326/01 available at https://eeas.europa.eu/statements/docs/2014/140326_01_en.pdf

[12] Fortune, Global 500 2015, available in http://fortune.com/rankings/

The case of the U.S. is not very different. There has always been concerns about factors that may affect its position as world leader. With regard to theft of trade secrets, U.S. have given much importance to the issue. As noted in the Special 301 Report by the The Office of the United States Trade Representative, (2015), the report suggests, that there is an increased awareness of businesses in the necessity to protect their trade secrets, taking into consideration that trade secrets may be considered a company's most valuable assets and that cybercrime is a tendency on the rise. Also, theft of trade secrets can generate high impact consequences for the economy and security. Companies who are victims of theft of trade secrets by a rival company may notice how its investment in R & D is affected, resulting in the need to incur more costs, reducing the budget for new ingenious ideas. Attacks on trade secrets in sectors that handle technology aimed at to improve defense may jeopardize the U.S. national security. In the economic sphere employment opportunities and U.S.'s business performance at international level may be affected by this phenomenon. (The Office of the United States Trade Representative, 2015, p.20)

The protection of trade secrets is a fundamental part in order to foster innovation. President Obama in the State of the Union Address (2012) stated that "After all, innovation is what America has always been about. Most new jobs are created in start-ups and small businesses". [13] But there are struggles that make this hard to accomplish. Companies from large multinationals to start-ups are been victims of constant attacks. As stated by the The Commission on the Theft of American Intellectual Property, (2013)"Start-ups and small businesses are an indispensable

[13] **The White House,** Office of the Press Secretary, January 24, 2012, Remarks by the President in State of the Union Address, available at https://www.whitehouse.gov/the-press-office/2012/01/24/remarks-president-state-union-address

part of the United States' culture of innovation, are being increasingly targeted by IP thieves, and have fewer resources to defend themselves."(p.67)

Another report by the United States International Trade Commission (USITC) (2011) in which it obtain results of responses to USITC questionnaire sent to 5,051 U.S. firms in sectors considered IP-Intensive, showed "that firms estimated losses due to reported Chinese trade secret misappropriation of $1.1 billion during 2009". The report also noted that in the majority of firms, the losses from trade secret misappropriation occurred outside the Chinese market with a 47.9% of losses in the U.S. market and 46.4% in third country markets.

The report established that the possible cause that contributes trade secret losses occurring outside China could be the quickness that trade secrets can circulate through "mobile telecommunication devices". Regarding the impact of trade secret misappropriation, during the period of 2007-2009, 52.7% of firms that suffered misappropriation in China said it became a bigger problem.

Finally, in relation to trade secret infringement and enforcement challenge, 60% of the firms reported that did not incur in expenses to address the misappropriation. The grounds can be in the fact that some firms reported difficulties with the requirements for trade secret enforcement, in addition, that proving trade secret misappropriation is a challenge since Chinese law requires a written evidence that the trade secret misappropriation took place. Only 0.6% of the firms pursued trade secret misappropriation proceedings in China in 2007-2009. (United States International Trade Commission, 2011)

4.2 How to mitigate the problem

Why should companies assess this complication? Well, for instance, according to a report produced by Forrester Consulting (2012) it states that intellectual property represents a large part of the information contained in their portfolios. The report realizes a comparison between secrets and custodial data, giving as a result that secrets are more meaningful for businesses. This rationalism is completely understandable since secrets are linked to the corporation's purpose. The report noted in a survey in which they asked 305 IT companies to rate 5 of 17 most valuable property in their portfolio, the results were astonishing stating that two-thirds of the value come from the secrets. (P.3-5)

So, since it has been established that trade secrets are an important factor for businesses, now we have to establish the possible measures that could be applied to protect trade secrets and reduce the risk of being misappropriated. Companies use different strategies for the protection of their business secrets, however, some do not have a starting point on how to protect them.

A report prepared by the Center for Responsible Enterprise and Trade, (2014) establish the elements of a trade secret protection program which consist of 8 categories. First, the implementation of policies in how to protect trade secrets internally and outside the company, applying management procedures, separation, and specification of trade secrets, development of standard agreements such NDA (non-disclosure agreements) and the creation of an inventory with the finality to verify the activity, use, disclosure and management of trade secrets. Second, in order to maximize synergies, the allocation of a responsible group, with its own budget and supervisor in order to handle the surveillance of trade secrets in the company and the identification of the actors who handle trade secrets. Third, risk assessment, stating which trade

secrets are the most vulnerable of being misappropriated and the impacts that this could bring, likewise the implementation of a plan to alleviate risks, classifying them according to their degree of volatility. Fourth, the management of trade secrets by third parties, requiring them to act with due diligence, and to maintain constant communication in order to ensure that third parties comply with the policies of the company regarding the use of trade secrets. Additionally, ensure that agreements with third parties are in writing and that those contains a complete coverage of how to handle trade secrets. Fifth, maintain security and confidentiality of trade secrets, increasing digital security prioritizing the protection of trade secrets and limiting access to them only to authorized persons. Sixth, training, and staff training on how to properly handle trade secrets providing theoretical education and practical information. Seventh, constant review internally and to third parties, furthermore, establish a comparison of the measures taken by the company with those of strongest competitors and apply the best practices or aspects thereof. Finally, apply corrective measures to find the source of the problem, have the ability to problem analysis and decision making. Rate the performance of the company in relation to the protection of trade secrets and use regularly and annual reviews to establish improvements. (P.14-17)

In conclusion, attacks on trade secrets are constant to this day. The loss of trade secrets has a negative impact on the promotion of innovation and competitiveness. Companies invest much of their resources on R & D, as noted above, trade secrets represent a very important asset for companies, hence the importance of protecting them. There is no doubt that a strategy for the safety and handling of trade secrets is an essential part of a company that can bring benefits to avoid big losses and mitigate risks.

5 CHAPTER 5: TRADE SECRET PROTECTION IN THE U.S. AND EU

In the case of the U.S. and EU trade secret protection, we can find that there have been legislative proposals that have already been adopted, all with the intention to strengthen and harmonize the legislation on trade secrets in these regions.

In relation to the U.S., the recent legislative act, the Defend Trade Secret Act[14] (DTSA), signed by President Obama on May 11 2016, creates a private civil action against misappropriation of trade secret and contains some amendments to the Economic Espionage Act, being the civil seizure the most distinct feature. With reference to the EU, we can argue that the diversity of laws existing in the EU makes it really difficult and costly for companies that engage in cross-border transactions to seek enforcement of their trade secrets, for this purpose, in November of 2013 the European Commission proposed a draft directive with the intention of harmonizing the laws around trade secrets, which was approved on May 27 2016.

5.1 U.S. Trade Secret Protection

5.1.1 Uniform Trade Secret Act 1985 Amendments

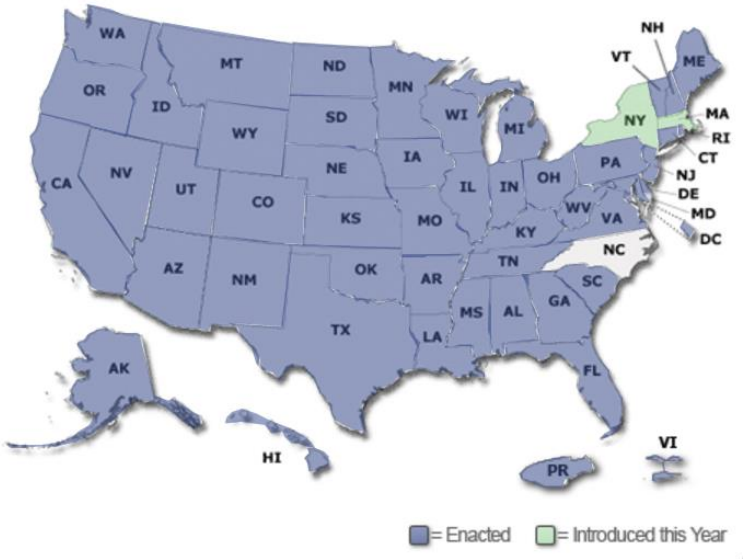
The Uniform Trade Secret Act[15] (UTSA) provides a legal framework for the protection of trade secrets. The Act was first published by the Uniform Law Commission (ULC) in 1979 and amended in 1985. This legal instrument come out as a solution for the variation in State laws that created confusion about what law should be applied. The adoption of the UTSA have provided a

[14] S.1890 - Defend Trade Secrets Act of 2016. Available at https://www.congress.gov/bill/114th-congress/senate-bill/1890/text

[15] Uniform Law Commission. The National Conference of Commissioners on Uniform State Laws. Uniform Trade Secret Law with 1985 amendments. Available at http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf

certain legal uniformity between States. **(Uniform Law Commission, 2016)**[16]. Given the importance of having a codified legislation regarding trade secret protection, "47 states in the US have adopted the UTSA in some form" (Bevitt, Timner, & Westerman, 2014). In 2016, the states of New York and Massachusetts introduced the bills SB3770 and HB37 in order to enact the UTSA,[17] resulting in almost a complete uniformity nationwide regarding trade secret protection (see map below).

Figure 2: Number of States that have enacted the UTSA.



Source: Uniform Law Commission. The National Conference of Commissioners on Uniform State Laws. (2016). Legislative Enactment Status. Retrieved from http://www.uniformlaws.org/LegislativeMap.aspx?title=trade%20Secrets%20Act

[16] Uniform Law Commission. The National Conference of Commissioners on Uniform State Laws. (2016). Why States Should Adopt the Uniform Trade Secret Act. Retrieved from http://www.uniformlaws.org/Narrative.aspx?title=Why%20States%20Should%20Adopt%20UTSA

[17] Uniform Law Commission. The National Conference of Commissioners on Uniform State Laws. (2016). Legislation. Retrieved from http://uniformlaws.org/Legislation.aspx?title=Trade%20Secrets%20Act

Even though some states have not adopted the act entirely, however their legislation is similar and it stills provides a high percentage of legal harmonization regarding the basic issues of trade secret, such as: Definition of trade secret misappropriation, preservation of secrecy and remedies for trade secret misappropriation, which includes: Injunctive relief, damages and attorney's fee only in some cases.

The definition of trade secrets contained in the UTSA served as a basis for the definition laid down in the TRIPS. The definition provided in the Act needs to "derive independent economic value, actual or potential from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use". Also another important aspect is that it has to be subject of efforts that are reasonable under the circumstances in order to maintain its secrecy. As Klitzke (1980) argues, the definition is very broad in scope as to include "economic value" which can be extended to information that companies do not use in their business activities on a daily basis. Continuing with the explanation, he noted that "a secret could have economic value without having commercial value", providing, as an illustration, the "negative know-how", knowledge of a process or product that does not work, and that can have economic value but does not directly generates revenues.(p.288-289)

As for the reasonable efforts to maintain secrecy, the comments to the Act establish that:

> "The courts do not require that extreme and unduly expensive procedures be taken to protect trade secrets against flagrant industrial espionage…it follows that reasonable use of a trade secret including controlled disclosure to employees and licensees is consistent with the requirement of relative secrecy".[18]

[18] Uniform Trade Secret Act, Comment, pg.7

The Act establish that the term “proper means” provides with the legal justifications in the circumstances in which a trade secret can be ascertainable, such as: 1) Discovery by independent inventions; 2) Discovery by reverse engineering; 3) Discovery under a license from the owner of the trade secret; 4) Observation of the item in public use or public display and, 5) Obtaining the trade secret from published literature.

With regard to the “improper means”, Klitzke (1980) argues that the use of the term "improper means" is successful and provides a wider scope that if the term "illegal conduct" were used because they can acquire trade secrets without incurring in a criminal action or civil liability. The Act defines "improper means" but does not limit it to those establish in the UTSA, because it is not possible to list all the circumstances that could be considered improper, as a result other sources may be used as a complement to establish the scope and definition. (p.294)

The scenarios listed by the Act in which misappropriation by improper means can occur, can be theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy or espionage through electronic or other means.

Regarding to this term, Klitzke (1980) argues that the misappropriation can be divided into two categories, the first, in connection with the acquisition of a trade secret and the second, voluntary disclosure. He argues that the Act provides protection against someone who received a trade secret of a third person, who obtained it by improper means, but there is a condition, that the person who acquired the trade secret through a third person, had knowledge or should have known that the trade secret was obtained by improper means. With regard to the requirement of "knowledge", the author argues that the Act follows the same parameters as the Restatement of Torts in its section 757, suggesting that "a reasonable man would infer the facts in question" or "would be put on inquiry and an inquiry pursued with reasonable intelligence and diligence

would disclose the facts. " Finally, in the cases where there is an acquisition by accident or mistake, the position who uses a trade secret must change materially once the user becomes aware that the information constitutes a trade secret, although at the time of the acquisition did not have knowledge, otherwise the user will be liable for trade secret misappropriation. (Klitzke, 1980, p. 295-300)

The remedies for misappropriation are also established in the act which includes: 1) Injunctive relief that can still be effective for a reasonable amount of time even after the trade secret ceased to exist, in order to prevent commercial advantage acquired by the misappropriation.

In relation to the injunctive relief, Klitzke (1980) argues that is "the most potent weapon against misappropriation". The purpose of the injunction is to take away the advantage over competitors that a misappropriator obtained by improper means. By setting the duration of the injunction, the court takes into account the maximum time that it would have taken the offender to discover the trade secret by own means, although there are some cases where the court has granted perpetual injunctions. And in cases where you cannot determine the time, it would have taken an offender to discover the trade secret by own means? Well, the author argues that setting a certain duration of the injunction in these cases presents a great difficulty. Klitzke (1980), notices that any injunction with limited lifetime is preferable than to establish a perpetual injunction, only if there is certainty that the trade secret could have been discovered or acquired by proper means sooner or later. In the cases where it is unreasonable to prohibit the use of a trade secret by a third party, the measure to apply is the payment of a reasonable royalty.

As an illustration, the author provides the example that if a third party that uses a trade secret that was obtained through a misappropriator, but the third party acquired it in good faith and without

reason to suspect that was acquired by improper means, then the payment of a reasonable royalty could suffice. (Klitzke, 1980, p.301-304)

2)Damages, complainant is entitled to: 1) recover damages for misappropriation, and 2) disgorgement of profits acquired by unjust enrichment caused by misappropriation that was not taken into account in calculating damages for actual loss.

Finally regarding damages, Klitzke (1980), argues that in cases where both injunctive relief, as well as damages, are granted as remedies, monetary payment will be made only by the time that the injunction is not effective, besides the monetary compensation applies only when the trade secret is subject to protection, which includes the time when the misappropriator has an advantage over other competitors in good faith. Where there is more than a trade secret owner, it presents a problematic and a legal loophole, since the Act does not provide a clear solution to the problem and leaves it to interpretation by judges. The Act finally provides the granting of punitive damages when the misappropriation was on purpose and there was an intent of committing a damage. (p.304-306)

And finally, 3) Attorneys fee; in some cases the court may award reasonable attorney's fees to the prevailing party.

With regard of the preservation of secrecy, the Act establish an obligation to the court in order to protect and preserve the secrecy of trade secrets in trade secret litigation cases.

5.1.2 Economic Espionage Act 1996

The Economic Espionage Act[19] (EEA), was introduced in 1996 with the aim of strengthening the legislation against the increase threat or misappropriation of trade secrets. As noted by Senator Kohl, "trade secret theft and economic espionage continue to pose a threat to U.S. companies to the tune of billions of dollars a year." (as cited in Quinn Emanuel Urquhart and Sullivan LLP, 2012) These issues constitutes a topic of great relevance to the United States especially with constant threats of theft of trade secrets by foreign governments and enormous losses in U.S economy. In order to address this issue, the EEA established two provisions in which criminalizes the theft or misappropriation of trade secrets.[20] First it criminalizes foreign economic espionage (sec.1831) by establishing penalties with a fine up to $500,000 for individuals and $10,000,000 for organizations or imprisonment up to a maximum of 15 years or both to whom commits theft or misappropriation of trade secrets in benefit of a foreign government. The second provision focuses on the common commercial theft of trade secrets (sec.1832), regarding a product produced or placed in interstate or foreign commerce, with the scienter that the offense would prejudice the owner of the trade secret. This illegal activity is punishable with fine up to $5,000,000 for organizations and imprisonment up to a maximum of 10 years for individuals. As for this section, Spencer (1998) argues that it does not provide complete protection of trade secrets since it is limited only to products, leaving, as a result, without protection trade secrets encompassed in services. In other words, James H.A. Pooley et al (1997) noted that "[t]his means that the EEA arguably does not cover either 'negative know

[19] Public Law 104- 294 Economic Espionage Act. Available at https://www.gpo.gov/fdsys/pkg/PLAW-104publ294/pdf/PLAW-104publ294.pdf

[20] United States Department of Justice. Introduction to the Economic Espionage Act. Update June 2015. Available in https://www.justice.gov/usam/criminal-resource-manual-1122-introduction-economic-espionage-act

how' or information discovered but not [currently] used by a company" (as cited in Spencer, 1998). Governmental entities are exempt from the ban if their activities are within the framework of the law (sec.1833). The EEA consent the confiscation of any property derived from the proceeds obtained as a result of the crime, and any property used or intended to be used in the commission of the crime (sec.1834). This represents another limitation established in the EEA, since it does not provide a way for obtaining losses that the victim of a theft of trade secrets has suffered, which would result in relying on state law in order to seek recovery of damages, incurring the victim in more costs due to an exhaustive process. (Spencer, 1998)

Spencer (1998) notices that:

> "A federal law should specifically and adequately address the losses sustained by victims of trade secret theft in the same manner that the EEA protects the U.S. economy, in general, by imposing such stiff penalties for acts of foreign economic espionage."(p.316)

In regard of the preservation of confidentiality of trade secrets relating judicial proceedings, the courts are in the obligation to address the secrecy of such trade secrets (sec1835). The EEA permits that the Attorney General may obtain injunctive relief against any violation (sec.1836). Respecting, where an illegal activity has been committed outside the United States, the EEA sets an extraterritorial jurisdiction provisions, that contains the circumstances in which the act can be enforce, if the offender is a citizen or resident of the United States; if the offender is an organization constituted under the law of the United States or if the punishable act was committed in the United States (sec.1837). In the last two provisions (sec.1838 & sec. 1839), the EEA provides definitions of the terms of "foreign instrumentality", "foreign agent", "owner",

and “trade secret”. The definition of the latter is define as "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing…” In relation to this, Spencer (1998) argues that “the definition of trade secrets under the EEA is broader than that contained in the UTSA because it includes the new technological methods by which trade secrets can now be created and stored.”(p.311). While the term “owner” is define in (sec.1839(4)) as “the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed”

5.2 EU Trade Secret Protection.

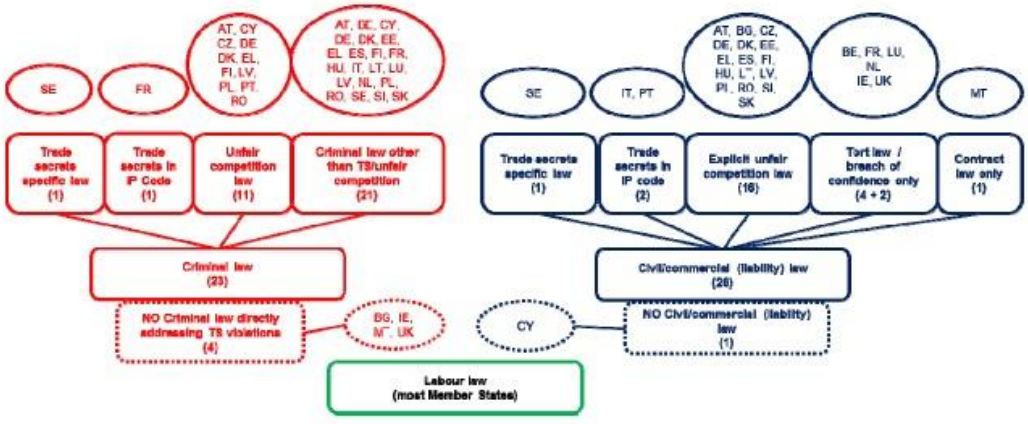
As already stated before, there is no specific law in the EU to deal with misappropriation of trade secrets. Protection relies on national law, which provides civil and in some cases criminal liability. The existence of legislative differences in criminal and civil matters in the EU has created under those circumstances, great obstacles when protecting trade secret misappropriation. The graphic below exposes the problematic as a result of a not harmonized legislation on the protection of trade secrets.

Figure 3: *Uneven and fragmented legal protection of trade secrets against misappropriation within the Internal Market*

Source: (European Commission, 2013) p.19 available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013SC0471

As mentioned above, many Member States use different instruments in civil matters for the protection of trade secrets, the chart below gives us a clearer explanation of how trade secrets are protected according to national laws.

Figure 4: Main protection against trade secret misappropriation by national law



Source: (European Commission, 2013) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013SC0471 pg.179

5.2.1 Civil Protection

The only country in the EU that has a special Act regarding the protection of trade secrets is Sweden, in the case of Italy and Portugal their codes of industrial property contains provisions that protects trade secrets. In relation to the other Member States, more general legislation applies. For instance, Austria, Bulgaria, Czech Republic, Germany, Denmark, Estonia, Greece, Spain, Finland, Hungary, Latvia, Lithuania, Poland, Romania, Slovenia and Slovakia relies on unfair competition law when addressing trade secrets. While in Belgium, France, Luxembourg and Netherlands, trade secrets are addressed through Tort law (liability for non-contractual responsibility). Some other countries rely on Case-law (breach of confidence) such as Ireland and the United Kingdom. Malta relies exclusively on contract law, meanwhile Cyprus have no civil liability for trade secret misappropriation.

The disclosure of trade secrets by employees is covered almost in all countries at least for the duration of the employment relationship. (European Commission, 2013, p. 181). The box below provides further details on the civil rules that governs in the Member States. (Hogan Lovells (2012), *Report on Trade Secrets for the European Commission*)

Figure 5: **Civil rules in Member States**

AT (Austria): Austria's Unfair Competition Act provides civil (and criminal) sanctions against trade or business secret misuse by employees and those who exploit such information without consent for the purposes of competition. Other legislation such as the Patents Act and the Criminal Code also provides legal remedies in particular circumstances, such as disclosure of inventions by employees or in cases of industrial espionage. In addition, the Austrian courts have held that obtaining trade or business secrets by breach of confidence (in the course of contractual negotiations) falls within the Unfair Competition Act.

BE (Belgium): There is no one piece of legislation on the protection of trade secrets as such in Belgium but there are several provisions of Belgian law which can be used against the misuse or disclosure of trade secrets. Trade secret owners generally rely on the general law of tort (Article 1382 of the Belgian Civil Code), unfair competition and specific provisions in Belgian labour law.

BG (Bulgaria): There is no specific legislation on trade secrets in Bulgaria but various laws including the Law on Protection of Competition and the Law on Access to Public Information contain general provisions which may be used to protect trade secrets. In fact, there are over 60 such statutory and non-statutory provisions (including criminal liability under the Criminal Code).

CY (Cyprus): There is no specific legislation governing trade secret misuse in Cyprus but there are a number of different laws which mention trade, business and professional secrets. For example, the Commercial Descriptions Law, the General Product Safety Law and the Competition Law. However, liability is criminal; there is no civil liability for trade secret misuse.

CZ (Czech Republic): The Czech Commercial Code defines a trade secret and provides remedies for trade secret infringement. The TRIPS Agreement is directly applicable in Czech law and thus the definition of a trade secret under Article 39(2) of the TRIPS Agreement also applies in Czech law. The basis of trade secret protection in the Czech Commercial Code, however, is the civil law of unfair competition.

DE (Germany): There are a number of provisions in German legislation protecting trade secrets. The most important statutory provisions for the protection of trade secrets are found in the Act against Unfair Competition. These provisions apply to employees and to third parties. Many of the statutes protecting trade secrets under the criminal law also have civil law provisions. These provisions allow for damages and injunctive relief if one of the relevant criminal law provisions is violated. Civil law remedies are also available under the Civil Code (tort law). German contract law also provides effective protection where there is a contractual obligation to maintain the secrecy of trade secrets. Special rules relating to the protections of trade secrets apply to stock corporations (AG) and limited liability companies (GmbH). As for stock corporations, pursuant to art. 93 sec. 1 of the Stock Corporation Act (Aktiengesetz - AktG), the members of the management board shall keep confidential any information and secrets of the company, namely trade or business secrets. If they fail to comply with this duty, they are liable to the company for any resulting damage.

DK (Denmark): In Denmark there is no statutory definition of trade secrets; however case law has clarified the types of information that are protectable to include both technical and commercial information. Several statutes, both civil and criminal, are used to protect the rights of trade secret owners as well as legal principles derived from contract law, competition law, employment law and

unfair competition law. Most notably, the Criminal Code and the Marketing Practices Act contain provisions protecting trade secrets.

EE (Estonia): Estonian legislation provides specific provisions on the protection of trade secrets, most notably in the Competition Act, the Commercial Code, the Employment Contracts Act and the Penal Code. The Competition Act includes an illustrative list of information considered to constitute trade secrets. The Supreme Court has also held that in addition to this definition, the definition of trade secrets provided in the TRIPS Agreement can also be used to interpret the term "trade secrets" under Estonian law.

EL (Greece): Greek Unfair Competition Law provides specific provisions on the protection of trade secrets. More general protection is found in the Greek Civil Code which includes general tort provisions.

ES (Spain): Trade secrets are mainly protected in Spain under the Unfair Competition Act and the Criminal Code. The Act contains provisions specifically aimed at trade secrets. There are also other laws which deal with trade secret protection indirectly, for example, the laws establishing the obligations of directors and other employees. [In addition, Law 14/2011 on science, technology and innovation also refers to the protection of the results of R&D (Article 35(2))].

FI (Finland): There are a number of Acts which include provisions for the protection of trade secrets, most importantly the Unfair Business Practices Act, the Employment Contracts Act and the Criminal Code. Finland does not have one piece of legislation directed specifically to the protection of trade secrets. Although the Finnish law encompasses the protection of trade secrets under the Unfair Business Practices Act, trade secrets are not considered to be intellectual property rights.

FR (France): There are a number of references to trade secrets in French law and case law but no statutory definition of trade secrets. Trade secret owners generally rely on the unfair competition law (against competitor) and the general law of tort (against any third party) which correspond to the same reference of the French Civil Code, namely Article 1382. However the only specific trade secrets legislation is dealing with protecting "manufacturing secrets" in the Intellectual Property Code (Article L. 621-1) in link with the Labour Code, which provides criminal liability for trade secret violations by employees or former employees. When parties are bound by a contractual obligation not to disclose secret information, an action lies for breach of contract.

HU (Hungary): Hungarian law provides specific provisions on the protection of trade secrets. The main general rules are established in the Civil Code as part of the moral rights section. Besides, rules on the protection of know-how are currently laid down separately in the Civil Code, within the general provisions on the protection of intellectual property. The unfair competition law aspects of trade secret protection (based on the definition of trade secrets enshrined in the Civil Code) are regulated in the Unfair Competition Act. Provisions also exist in the Labour Code and in various financial/banking laws.

IE (Ireland): There is no specific legislation in Ireland directed to the protection of trade secrets. However, proceedings may be brought under laws relating to breach of confidence, data protection and specific sectorial pieces of legislation. As in England, Irish law has the equitable principle that a person who has received information in confidence cannot take unfair advantage of it. Generally, Irish law imposes a duty of confidentiality in both non-employment cases and employment cases. In both situations, there must be an obligation of confidence and once it is established that such an obligation exists then the person to whom the information is given has a duty to act in good faith

and only use the information for the intended purpose. Again, as in England, an obligation to keep information confidential may either be imposed by contract; implied because of the circumstances of the disclosure or implied because of the special relationship between the parties.

IT (Italy): Specific provisions on the protection of trade secrets are contained in the Italian Code of Industrial Property (IPC). Secret information may only be protected if the requirements set out in the IPC are met. There are also general tortious obligations and unfair competition provisions in the Civil Code which can be employed to compensate for trade secrets misuse.

LT (Lithuania): Lithuanian legislation provides specific provisions on the protection of trade secrets, most importantly in the Civil Code, the Law on Competition, the Labour Code and the Criminal Code. Under the Civil Code, anyone unlawfully acquiring a commercial secret is liable to compensate the owner for the damage caused. There are also express provisions in the Labour Code regarding disclosure by employees who disclose a commercial secret in breach of their employment contract.

LU (Luxembourg): There are no specific legal provisions protecting trade secrets in Luxembourg. However, trade secrets can be protected by unfair competition law, criminal law, tort law and contractual law.

LV (Latvia): Latvia has a number of pieces of legislation which provide specific provisions on the protection of commercial secrets. The Commercial Law is the main Act regulating commercial activities. It defines "commercial secrets" and provides express protection for them. The Labour Law also includes provisions regarding use of commercial secrets by employees. Latvia also has an Unfair Competition Act which expressly provides that the acquisition, use or disclosure of commercial secrets of another competitor without their consent is a form of unfair competition.

MT (Malta): There is no specific legislation on the protection of trade secrets in Malta. Trade secrets may be protected contractually, by express or implied terms, and, an employee is presumed to be under an obligation not to disclose confidential information. If no contract exists there will be no civil law right to protect a trade secret.

NL (Netherlands): There are no specific provisions on the protection of trade secrets in Dutch legislation. In the Netherlands, the protection of trade secrets is based on the general principle of tort law i.e. an unlawful act. In 1919, the Dutch Supreme Court held that the provision in the Dutch Civil Code on unlawful acts could be used to secure protection against trade secret infringement. Contract law also provides some protection in contractual relationships if there are confidentiality obligations in the contract.

PL (Poland): There are specific provisions on the protection of trade secrets in Polish legislation, notably in the Unfair Competition Act. A number of other Acts mention trade secrets, for example, the Civil Code, the Labour Code, the Act on Competition and Consumer Protection, the Code of Commercial Companies and Partnerships etc. The Labour Code includes express provisions requiring employees to maintain the confidentiality of information the disclosure of which could cause damage to their employer.

PT (Portugal): The Portuguese Industrial Property Code has specific provisions relating to the protection of trade secrets. The Industrial Property Code is directed towards unlawful acts against competitors. A violation is punished, not as a crime, but as an administrative office punished by a fine. The Labour Code also contains provisions which stipulate that an employee may not disclose

information, while employed, relating to his employer's organization, production methods and company business.

RO (Romania): There is specific legislation in Romania on the protection of trade secrets. Provisions regulating protection of trade secrets have been included in the Law for the Prevention of Unfair Competition ("Law on Unfair Competition") and specify that the unfair use of a competitor's trade secrets is regarded as contrary to honest commercial practices.

SE (Sweden): Sweden is the only country in the EU to have an Act specifically protecting trade secrets. The Act provides a definition of trade secrets, penalizes trade secret espionage and contains provisions on civil liability.

SI (Slovenia): Trade secrets are specifically protected in Slovenia by a number of pieces of legislation, in particular, the Companies Act, the Employment Relationship Act, the Protection of Competition Act, the Penal Code and the Code of Obligations.

SK (Slovakia): Civil protection of trade secrets in the Slovak Republic is regulated by the Commercial Code. The relevant fields of protection are civil law, commercial law, intellectual property law, non-contractual liability and unfair competition law.

UK (United Kingdom): There is no legislation providing specific protection for trade secrets. Trade secrets are protected by contract and/or by the law of equity.

Data retrieve from (European Commission, 2013) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013SC0471 p.181-184

5.2.2 Civil remedies

In relation to the civil remedies, it varies according each member state, the table below elaborated by Baker & McKenzie (2013), p. 29 with information submitted by Member States, provides a listing of the civil remedies in the EU.

Figure 6: Available civil remedies

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Injunctions (cease and desist orders: ordinary action	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Injunctions (cease and desist orders: interim relief	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: ordinary action	✓	✓			✓	✓	✓			✓		✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: interim relief	✓	✓			✓	✓				✓		✓	✓	✓	✓			✓		✓			✓				✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓		✓		✓	✓	✓		✓	✓	✓	✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: interim relief		✓			✓		✓		✓	✓		✓	✓		✓			✓		✓	✓	✓				✓	✓
Withdrawal from the market of goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓		✓		✓	✓	✓	✓	✓			
Withdrawal from the market of goods produced using misappropriated trade secrets: interim relief		✓			✓				✓	✓		✓	✓		✓			✓				✓	✓	✓			
Damages	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Publication of decisions: ordinary action		✓	✓		✓		✓			✓	✓	✓	✓		✓		✓			✓	✓	✓	✓			✓	✓

Publication of decisions: interim relief		✓											✓			✓												
Restraint measures (e.g. penalty for future breach of the Court's order): ordinary action	✓	✓	✓	✓	✓				✓		✓	✓			✓	✓	✓			✓				✓				
Restraint measures (e.g. penalty for future breach of the Court's order): interim relief		✓		✓	✓				✓		✓	✓			✓		✓							✓				
	AT	**BE**	**BG**	**CY**	**CZ**	**DE**	**DK**	**EE**	**EL**	**ES**	**FI**	**FR**	**HU**	**IE**	**IT**	**LT**	**LU**	**LV**	**MT**	**NL**	**PL**	**PT**	**RO**	**SE**	**SI**	**SK**	**UK**

Source: (European Commission, 2013) p.198-199

5.2.3 Criminal Protection

As the European Commission (2013) stated, Member States use different legal mechanisms that contain provisions that punish trade secret infringement. Most legal systems have as the legal basis the protection of the following interests: First, "the protection of the owner's right to exploit the confidential information and to gain, an advantage over competitors". Second, "the company's right to privacy" and third "the proper functioning of the market". In the aspect of criminal law, there are several points to be analyzed. To begin with, the definition of trade secret in criminal law varies in each State, in fact, few legislations provide a definition in that aspect, as a result, and the courts have to refer to a standard definition of trade secret. The trade secret must be information that generates a competitive advantage to its owner, which is known or disclosed to a limited number of people and the owner must have taken reasonable steps to maintain its

secrecy. For the criminal protection to be granted, the secret must generate an interest in the owner to exploit it and gain a competitive edge in the market. However, in some cases, it must establish the requirement of economic value and reasonable measures to keep it secret. In addition to the above, the conduct to sanction is not defined, as a consequence, there is a broad scope on what activities are legal and which ones are not (p.206-207). The table bellows provides a clear illustration of criminal provisions applying to trade secret misappropriation in the EU.

Figure 7: Criminal provisions applying to trade secrets misappropriation

Table A9.1 – Criminal provisions applying to trade secrets misappropriation[584]

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Criminal code	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	
Unfair competition / commercial law	✓			✓	✓	✓	✓		✓		✓											✓	✓				
Specific law on trade secrets																								✓			
Intellectual Property Code												✓															

Source: (European Commission, 2013) p.185 retrieve: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013SC0471

5.3 New Legislation

5.3.1 The Defend Trade Secret Act 2016

The days when you could only get a civil action in cases of trade secrets misappropriation through State law have come to an end. The Defend Trade Secret Act would create a federal private civil cause of action for trade secret misappropriation. Subsequently, we will analyze the most relevant aspects of this law.

Section 2 of the DTSA, established that an owner of a trade secret that has been misappropriated, is entitled to bring civil action if the trade secret is related to a product or service used in or intend for use in, interstate or foreign commerce[21]. The terms "misappropriation" and "improper means"[22] are define in the DTSA and are in consonance with the definition provided in the UTSA. The court may, upon ex parte and only in extraordinary circumstances, order for seizure of property, if it is necessary to prevent the propagation or dissemination of the trade secret[23]. With the intention of preventing abuses of this provision, the DTSA established requirements for its application. Some of this requirements include: 1) existence of an immediate and irreparable injury; 2) The harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom seizure would be ordered and substantially outweighs the harm to any third parties; 3) The applicant successfully demonstrated, that the information is a trade secret and that the person against whom seizure would be ordered, misappropriated the trade secret by improper means; 4) Risk that the person against whom seizure would be ordered, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person.[24]

The order for the seizure shall contain some elements such as:

a) Findings of fact and conclusions of law required for the order;

b) Provide for the narrowest seizure of property necessary to achieve the purpose and to be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret;

[21] S.1890 sec.2(a) inserting new sec. 1836 (b)(1)
[22] S.1890 sec.2(b), amending 18 U.S.C. §1839
[23] S.1890 sec.2(a) inserting new sec.1836 (b)(2)(A)(i)
[24] S.1890 sec 2(a) inserting new sec.1836(b)(2)(A)(ii)

c) Order protecting the seized property from disclosure;

d) Set a date for a hearing at the earliest possible time, and not later than 7 days after the order has issued;

e) The person obtaining the order needs to provide the security, which will be determined by the court for the payment of the damages in the case of a wrongful or excessive seizure or wrongful or excessive attempted seizure.[25]

The DTSA contains a provision for cases in which a wrongful or excessive seizure occurs.[26] the person shall be entitled to the relief provide under section 34 (d) (11) of the Trademark Act of 1946, which "includes damages for lost profits, cost of materials, loss of good will, and punitive damages in instances where the seizure was sought in bad faith, and, unless the court finds extenuating circumstances, to recover a reasonable attorney's fee".

The Seizure Provision has generated mixed reviews, for example, according to the Senate Judiciary Committee report, "[t] he ex parte seizure provision is expected to be used in instances in which a defendant is seeking to flee the country or planning to disclose the trade secret to a third party or immediately is not amenable to the otherwise enforcement of the court's orders" (cited in Yeh, 2016).

In regards of this issue, Goldman (2015) argues that the ex-seizure provision can have serious consequences for competitiveness and provide collateral damage to third parties that are not liable. While it is true that there are safeguards that are supposed to prevent abuses, the author argues that these will not be accurate and may not achieve the desired level of protection.(p.287)

Also, Goldman (2015) notice that the ex-parte seizure provision may affect information that was not misappropriated and that is essential to the defendant's business, also he argues that because

[25] S.1890 sec 2(a) inserting new sec.1836(b)(2)(B)

[26] S.1890 sec 2(a) inserting new sec.1836(b)(2)(G)

of the ease in which information is disseminated, any device that may contain information that was misappropriated may be affected, giving as a result business closures. The fact, that in the law there is a measure for the narrowest seizure is not much help since it will be a long and arduous task. With regard to the wrongful seizure, he argues that because the scienter requirement is not clearly established, this will bring as a result, a disincentive factor for owners of trade secrets to not use the measure because of the fear of making a mistake and being accused of wrongful seizure (p.290-291). Finally, Goldman (2015) argues that the U.S. legal system is not designed for ex-parte proceedings because it is based on the discussion of lawyers who uses their best arguments to convince the judge, and because the ex-parte provision will allow only one part to expose the arguments favoring him, this would result in withdrawing the possibility to the defending party to provides his version and to indicate the flaws of the indictment (p.299). To bolster his argument, Goldman states that "in an ex-parte action, the plaintiff's claim that the information is a trade secret goes unchallenged." (p.304)

Another argument against the ex-parte seizure is provided in the Professors' Letter in Opposition to the Defend Trade Secret Act of 2015 (Goldam, et al., 2015). The scholars argue that this provision would mainly affect small businesses, start-ups, and entrepreneurs because of its content that would cause anticompetitive harm. Another point they criticize is that it does not specify the property can be seized and the scope, resulting in damages to the alleged offenders affecting their business operations, even with the provision of narrowest seizure.

They also argue that ex-parte seizure is pro-plaintiff since it does not allow the defendant to present evidence to discredit the provision. Finally, they establish that in opposing the provision, this will bring an increase in the process costs, which would affect mostly start-ups in cases

against large companies, since the former would yield before incurring large costs. (Goldam, et al., 2015).

Just as there are arguments against, there are also arguments in favor of ex parte seizure. For instance, Halligan (2015) argued that the ex parte seizure orders are an advantage and an important legal mean today, given the fact that trade secrets can be disseminated so easily, plus adding the possibility that the defender can destroy the evidence proving misappropriation trade secrets. He also argues that the main purpose of this provision is the preservation of evidence and in order to prevent abuses, that is why the provision of the Safeguards exists.

Another argument in favor of ex-parte seizure is provided by Prof. Crouch (2016) who notices that in order to avoid damage, federal courts may be more effective when to enforce the law. Regarding that the system is not prepared to ex-parte seizure, Crouch (2016) argues that the U.S. legal system has already used seizure procedures before, as an illustration, he states that Texas allows the provision of ex-parte sequestration. Also, he notes that the DTSA imposes restrictions on the ex-parte seizure and is limited only to property "necessary to prevent propagation or dissemination of the trade secret." Furthermore, the court is obliged to carry out the narrowest seizure in a way that does not affect business operations of the defendant that are not related to the alleged misappropriation. It is important to establish that the plaintiff needs to prove that the information is a trade secret and that if given notice the defendant could get rid of trade secrets by destroying evidence. In the case of wrongful or excessive seizure, Crouch (2016) argues that this provision is important for reducing the risk of abuse for several factors. First, it would be very difficult that a federal judge would grant an ex parte seizure provision, especially since they are characterized by being "tough". Second, taking into consideration the difficulty of obtaining the seizure and adding the consequences that the DTSA establish for wrongful seizure, surely

these factors will serve to prevent abuses. Litigants wishing to obtain an ex parte seizure must make a detailed and careful analysis of risks involved, discouraging unfounded applications. (Crouch, 2016)

Finally, in relation that some provisions of the DTSA could affect smaller companies, (Almeling, Four Reasons to Enact a Federal Trade Secrets, 2009) states that "There is evidence ... that trade secret theft threatens small businesses more than large ones" (p.788). He notices two reasons. First, in the smaller companies, labor relations are more turbulent compared to those in big companies, which makes them vulnerable to misappropriation of trade secrets by employees. Second, small companies do not handle well the loss of trade secrets due to lack of resources. (p.788). Thus, we could say that the DTSA could become a powerful weapon for smaller companies in order to protect their trade secrets nationwide.

The DTSA contains provisions regarding the custody of material, in which the court shall secure the seized material from physical and electronic access.[27] With reference to civil remedies for trade secret misappropriation, the court may grant injunction relief, damages for actual loss and unjust enrichment caused by the misappropriation of the trade secret, or the imposition of a reasonable royalty, the concession of punitive damages in an amount not more than 2 times the amount of the damages if the trade secret is willfully and maliciously misappropriated and attorney's fees in cases where a claim of misappropriation or a motion to terminate an injunction are made in bad faith or the trade secret was willfully and maliciously misappropriated.[28]

[27] S.1890 sec 2(a), inserting new sec.1836 (b) (2) (D).
[28] S.1890 sec 2(a), inserting new sec. 1836(b)(3)

In relation to the order of injunction, it shall not prevent a person from entering into an employment relationship and be in conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business.[29]

The DTSA establish a whistleblower immunity. In which anyone who discloses a trade secret to a Federal, State, or local government official, either directly or indirectly, or to an attorney, with the solely purpose of reporting or investigating a suspected violation of law, or filed it in a lawsuit or other proceeding, if such filing is made under seal, shall not be held criminally or civilly liable.[30]

There is also a requirement that in any contract or agreement with an employee that governs the use of trade secret or other confidential information, an employer shall notify the employee about this immunity. The non-compliance of this requirement shall result in the failure to grant the employer punitive damages and attorney's fees in an action against an employee.[31]For the purpose of the DTSA the term "employee" includes individuals working as contractor or consultant.[32]

The DTSA clarifies that nothing in this Act modifies the rule of construction in section 1838 of the EEA, and, as a result State trade secret laws are not preempted or affected by this Act. Further, nothing in this Act affects an otherwise lawful disclosure under the Freedom of Information Act.[33] Finally, the DTSA provides a Statue of Limitations that sets a deadline of 3

[29] S.1890 sec 2(a), inserting new sec, 1836(b) (3) (A) (i) (I) (II)
[30] S.1890 sec 7, inserting new sec. 1833(b) (1)
[31] S.1890 sec 7, inserting new sec. 1833 (b) (3) (C)
[32] S.1890 sec 7, inserting new sec. 1833 (b) (4)
[33] Senate. 2016. Report 114-220. Defend Trade Secret Act 2016. Available at https://www.congress.gov/congressional-report/114th-congress/senate-report/220/1

years after the date on which the misappropriation is discovered or by the exercise of reasonable diligence should have been discovered. [34]

Trademarks, copyrights, and Patents are all governed by U.S. federal legal system, the only one missing are trade secrets. Trade secrets are complex in several aspects, are important for the economy of many businesses and essential for innovation, hence arises the intention to regulate by federal law.

> "By consolidating the four types of IP law at the federal level, an FTSA [Federal Trade Secret Act] would be the final step toward a unified IP regime. This unification would, in turn, help achieve better innovation policy because it would consolidate in one entity—first Congress, and then the federal courts—the power to define the scope of all major categories of IP." (Almeling, Four Reasons to Enact a Federal Trade Secrets, 2009, p. 789-790).

5.3.2 Directive of the European Parliament and of the Council on the Protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

As noted above, the Directive is an attempt to harmonize national laws in EU on trade secrets. It "aims at improving the effectiveness of the legal protection of trade secrets against misappropriation within the Internal Market." (European Commission, 2013,pg.6). Therefore, we analyze the most revelevant and some controversial aspects of the Directive.

[34] S.1890 Sec.2 (d)

5.3.2.1 Subject matter and scope

The directive in Article 1, stipulates the rules for the protection against unlawful acquisition, use and disclosure of trade secrets and, also sets the minimums standards that Member States must meet. But leaves the possibility for Member States to establish a broader protection with the condition that such measures are consistent with certain provisions set out in the directive.

The provisions in this Directive do not apply to certain aspects, such as the exercise of the right of freedom of expression and information established in Article 1. 2 (a) of the Directive and protected by Article 11 of the Charter of Fundamental Rights of the European Union. This issue has been very controversial especially for journalists and whistleblowers, who see affected their right to freedom of expression and information, given that the provision in the Directive states that the alleged acquisition, use or disclosure of a trade secret must have been in aiming to reveal a misconduct, wrongdoing or illegal activity and that the respondent was acting with the purpose of protecting a general interest. [35] As the OSCE's representative for media freedom, Dunja Mijatovic, stated "More particularly the text does not define the legitimate exercise of the right to freedom of expression and information and does not provide a clear notion of public interest in order to properly protect investigative journalism." (as cited in Lahodynsky, 2015).

The problem occurs with the absence of two key aspects. First, of a definition of what public interest concerns and second in what type of information contains a misconduct, wrongdoing or illegal activity. Such ambiguity presents a major obstacle to the existing ones for investigative journalism and whistleblowers. Another aspect to consider is that investigative journalists should ensure that the information they acquire by their informants has been legally acquired. Taking in

[35] Otmar Lahodynsky. EU trade bill threatens media freedom. 15 June 2015. Euobserver. Available in https://euobserver.com/opinion/129103

mind, the provision in Article 4 (4) of the Directive which establishes that the acquisition, use or disclosure of a trade secret will also be considered unlawful, if the person at the time of acquisition knew or was in the obligation to know that the information had been obtained illegally by a third party.

Another aspects that are not affected by the Directive, are the disclosure of trade secrets for reasons of public interest, or to judicial or administrative authorities in the performance of its duties and the rules requiring institutions of the European Union or national public authorities to disclose business-related information. Regarding, the autonomy of social partners and their rights to enter into collective agreements, and no unjustified barriers to workers mobility, the legal affairs of the Members of the European Parliament (MEPs) stated that the Directive should not:

> "Affect the use of information that is not considered a trade secret, or the use of the experience and skills honestly acquired in the normal course of their employment. The new rules must not impose restrictions in the event that a worker wishes to change job, other than those included in employment contracts" (European Parliament News, 2015).[36]

[36] European Parliament News. Trade secrets: freedom of expression must be protected, say legal affairs MEPs. Press release - Citizens' rights / Competition – 16-06-2015 - 12:52. Available at http://www.europarl.europa.eu/news/en/news-room/20150615IPR66493/Trade-secrets-freedom-of-expression-must-be-protected-say-legal-affairs-MEPs

5.3.2.2 Definitions

5.3.2.2.1 "Trade Secret"

The definition of trade secret contained in Article 2 of the Directive is in harmony with the definition of "undisclosed information" provided in Article 39 of the TRIPS. The definition in the Directive consists of three aspects: 1) it 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 circle of that normally deal with the kind of information in question; 2) has commercial value because it is secret; and 3) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

5.3.2.2.2 "Commercial Value"

In this section, the information must contain commercial value to the holder, in contrast to the provisions in the UTSA that requires "economic value", "the commercial value requirement ensures that information without any objective value or trivial information is excluded from protection" (Knaak, Kur, & Hilty, 2014). The recital 14 of the Directive provides clarification to the issue of commercial value by stating the following:

> "Such information or know-how should have commercial value, whether actual or potential. Such information or know-how has commercial value especially insofar as its unauthorized acquisition, use or disclosure is likely to harm the interest of the person

lawfully controlling it in that it undermines his or her scientific and technical potential, business or financial interests, strategic position or ability to compete".[37]

5.3.2.2.3 "Reasonable steps to keep it secret"

Although the directive does not clarify what reasonable measures concerns, many EU countries have in their legislations the provision for taking reasonable measures. "However, there is no checklist of minimally acceptable secrecy precautions; instead, courts require that the precautions be reasonable under the circumstances" (Bone, 1998)[38].

Certain circumstances may depend on the size of the company, for example,

> "A company that performs all its operations within a single building may adequately address misappropriation risks through basic employee agreements and visitor precautions. However, a globally networked enterprise may be expected to deploy sophisticated technologies to detect and prevent cyber-theft, entailing potentially substantial costs." (International Chamber of Commerce, 2014,p.6)

"These measures have to be effective and are of a varying nature: they can be technical (e.g. secured access to rooms, passwords on computers, seals on documents, etc.), or contractual (e.g. non-disclosure agreements)" (Boulay, 2015). Many companies have internal measures that

> "range from the policies, procedures and agreements and other records needed to establish and document protection; to physical and electronic security and confidentiality measures; to risk-assessment efforts to identify and prioritize trade secret risks; to due

[37] Recital 14 Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

[38] Robert G. Bone. A New Look at Trade Secret Law: Doctrine in Search for Justification. California Law Review. Pg. 249. Available http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1592&context=californialawreview

diligence and other ongoing third party management; to management oversight and coordination, employee and supplier training, monitoring and measurement, and corrective actions and improvements". (Center for Responsible Enterprise and Trade, 2015,p.6).

5.3.2.2.4 "Trade Secret Holder"

Article 2 (2) defines trade secret holder as "any natural or legal person lawfully controlling a trade secret". This broad definition could provide doubts about who could be the lawful holder of a trade secret in certain situations. As stated in her text, Prof. Tanya Aplin exposes many questions that have not been evaluated by the Directive. In the case of persons who are entrusted with the creation of a trade secret, who would lawfully control the trade secret? How about, trade secrets created in a joint venture? Are exclusive and non-exclusive "licensees" persons lawfully controlling a trade secret? What about employees to whom the information has been disclosed with consent? And finally what about persons who have lawfully reverse-engineered a marketed product and acquired a trade secret as a result? (Aplin, 2014). It would be advisable that the Council establish a definition related to the concept of trade secret holder to avoid vagueness.

5.3.2.2.5 "Infringing Goods"

According to the Directive, infringing goods means "goods whose design, characteristics, functioning, manufacturing process or marketing significantly benefits from trade secrets unlawfully acquired, used or disclosed". Regarding this concept, a particular aspect draws our attention and in with respect to the element of "marketing". One could establish that their scope is strict, as Knaak, Kur, & Hilty (2014) argues "marketing a good is not connected with the use

of a trade secret" (p.6). The intent of the provision could be considered too rigorous, to put it in another way, "marketing campaigns based on customer lists that were unlawfully acquired, it would by far exceed the legitimate purpose of the provision if the products marketed in that manner were classified as infringing". (Knaak, Kur, & Hilty, 2014). Aplin (2014), illustrates this point by explaining that if a company unlawfully acquires a trade secret consisting of a client list from a rival company, with the purpose of marketing their own products to the clients of their rival company. In this particular case, the products obtains a significantly benefit from the unlawful acquisition of the trade secret, but the products themselves are in no way the result of the unlawful acquisition, use or disclosure of the trade secret.

5.3.2.3 Lawful acquisition, use and disclosure of trade secrets

In Article 3 of the Directive establish a set of lawful ways to acquire a trade secret, which include: a) independent discovery or creation; b) observation, study, disassembly or test of a product or object that has been made available to the public or that it is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret; c) exercise of the right of workers or workers' representatives to information and consultation in accordance with Union and national law or practices; c) any other practice which, under the circumstances, is in conformity with honest commercial practices.

The recital 10 of the Directive reaffirms the possibility of acquiring the trade secret or know-how by independent discovery. In the case of reverse engineering it established that it is a lawful mean of acquiring a trade secret except if is subject to a contractual obligation.

Reverse engineering can be defined as:

> "The observation, study, disassembly or test of a product or object that has been made available to the public or that it is lawfully in the possession of the acquirer of the information, who is free from any legally valid duty to limit the acquisition of the trade secret".[39]

As stated in recital 17 "In some industry sectors, […] products can nowadays be easily reverse-engineered once in the market". Upon the purchase of a product, we also obtain property rights which allow us to dispose of the product in the way we want. The amount of effort that is needed in the process of reverse engineering to obtain information of a product may justify the right to use such information. (Samuelson, 2002). To market a product does not mean that the trade secret holder discloses the trade secret to the public. As stated in (Sinclair v. Aquarius Electronics, Inc., 1974) the court argued that a product containing a trade secret does not lose its character of secrecy by the fact of being marketed and that such statement is based both in law and in reason and logic, also emphasizes the very distinction between a patented and unpatented secret idea, establishing that the latter can be uncovered by reverse engineering.

5.3.2.4 Remedies

In relation to the remedies the Directive established in article 7.1 that the elements in which the measures, procedures and remedies shall be applied, being the following: (a) is proportionate;

[39] Art. 3 (b) Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure

(b) avoids the creation of barriers to legitimate trade in the internal market; and (c) provides for safeguards against their abuse. In the article 7.2, it establish sanctions to an applicant that began proceedings in bad faith.

Article 10, establish provisional and precautionary measures, in which preliminary injunctive relief is permitted. As for the Seizure provision, in contrast with the DTSA, the Directive is not clear if the procedure would be ex-parte. (Ankenbrandt & Vormann, 2016).

The injunctive relief and corrective measure are establish in article 12.1 (a)-(b), which allows judicial authorities to realize the following measures: (a) "the cessation of or, as the case may be, the prohibition of the use or disclosure of the trade secret"; (b) "the prohibition of the production, offering, placing on the market or use of infringing goods, or the importation, export or storage of infringing goods for those purposes"; (c) "the adoption of the appropriate corrective measures with regard to the infringing goods"; (d) "the destruction of all or part of any document, object, material, substance or electronic file containing or embodying the trade secret or, where appropriate, the delivery up to the applicant of all or part of those documents, objects, materials, substances or electronic files".

Damages (article 14.1; 14.2) can be granted for actual loss and any unfair profits that the infringer made. The Directive remains silent on the concession of punitive damages, but it takes into account non-economic factors such as moral prejudice when setting the damages. It is important to mention that there is a feature that the U.S. legislation does not contain, and that is that the limitation of employees' liability when the trade secret misappropriation was realized without intent. (Ankenbrandt & Vormann, 2016).

6 CONCLUSIONS

As can be seen, trade secrets are critical to the development of enterprises and promotion of innovation. Trade secrets are used by all companies, but especially by small companies, such as start-ups. Trade Secrets can be considered the most common form of protection given the several advantages offer compared to other types of intellectual property, such as patents.

Much of the operations executed by companies and their valuable assets are trade secrets. Trade secrets are not only valuable for businesses but also for cybercriminals and people who intend to misappropriate them with the purpose to make money or to gain an advantage in today's competitive market. These reprehensible actions are the cause of large losses by companies and negative impacts on countries' economy.

The U.S. and EU are the regions most affected by theft or misappropriation of trade secrets. In order to mitigate this problem, businesses in these areas are more aware of implementing security and protective measures of trade secrets in their companies. In the legislative aspect, the U.S. and EU have made proposals that have already been approved in order to generate a high level of harmonization of the rules protecting trade secrets in their respective regions.

While there are still improvements that could be implemented within these laws, efforts to achieve more protection surrounding trade secrets suggest that nowadays trade secrets are valued and are being given the importance they deserves.

7 Bibliography

The Office of the United States Trade Representative. (2015). *2015 Special 301 Report.* Retrieved from https://ustr.gov/sites/default/files/2015-Special-301-Report-FINAL.pdf

AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS (1994).

Almeling, D. S. (2009). Four Reasons to Enact a Federal Trade Secrets. *Fordham Intellectual Property, Media and Entertainment Law Journal, 19*(3). Retrieved from http://law.fordham.edu/publications/

Almeling, D. S. (2012). Seven Reasons Why Trade Secrets Are Increasingly Important. *Berkeley Tech. L.J., 27.* doi:http://dx.doi.org/doi:10.15779/Z38SM4F

Alperovitch, D. (2011). *Revealed: Operation Shady RAT, An investigation of targeted intrusions into more than 70 global companies, governments,and non-profit organizations during the last five years.* McAfee.

American Bar Association. (2010, July/August). Trade Secrets v. Patents: The New Calculus by R. Mark Halligan. *Landslide volume 2, number 6*, p. 3.

Ankenbrandt, B., & Vormann, T. (2016). *Comparing U.S. and EU Trade Secret Laws.* Trans-Atlantic Business Council, Intellectual Property Working Group. Retrieved from www.transatlanticbusiness.org

Aplin, T. (2014). *A Critical Evaluation of the Proposed EU Trade Secrets Directive.* King's College London, Dickson Poon School of Law.

Beckerman-Rodau, A. (2002). The Choice between Patent Protection and Trade Secret Protection: A legal and Business Decision.

Bevitt, A., Timner, H., & Westerman, D. (2014, June). Protecting Trade Secrets Globally: Compating The U.S. and EU. *Employment Law Commentary, 26*. Retrieved from http://www.mofo.com/~/media/Files/Newsletter/140630EmploymentLawCommentary.pdf

Bone, R. G. (1998). A New Look at Trade Secret Law: Doctrine in Search for Justification. *California Law Review, 86*(2). doi:http://dx.doi.org/doi:10.15779/Z38942G

Boulay, C. (2015). *QUESTION B The Protection of Trade Secrets and Know-How Are countries providing enough or too much protection?* University of Neuchâtel, Center for Intellectual Property and Innovation Law.

Center for Responsible Enterprise and Trade. (2014). Safeguarding Trade Secrets and Mitigating Threats: A Five-Step Framework to Identify, Assess and Manage Trade Secrets. Elements of an Effective Trade Secret Protection Program. CREATe.org, PwC. Retrieved from www.CREATe.org

Center for Responsible Enterprise and Trade. (2015). *"Reasonable Steps" to protect Trade Secrets: Leading Practices in an Evolving Legal Landscape.* Retrieved from www.CREATe.org.

Congress, S. a. (2016, May 11). To amend chapter 90 of title 18, United States Code, to provide Federal jurisdiction for the theft of trade secrets, and for other purposes.‘‘Defend Trade Secrets Act of 2016". Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/1890/text

Crouch, D. (2016, January 18). Guest Post: Why we Need a Seizure Remedy in the Defend Trade Secrets Act. *Patentlyo*. Retrieved from http://patentlyo.com/patent/2016/01/seizure-secrets-dtsa.html

Dass, N., Nanda, V., & Chong Xiao, S. (2014, October). Intellectual Property Protection and Financial Markets: Patenting vs. Secrecy. Retrieved from www2.warwick.ac.uk/fac/soc/wbs/subjects/finance/events/.../innoprotect_v4b.pdf

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. (2016, April 26). THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&from=EN

Engel Industries, Inc. v. The Lockformer Company, No.95-1185 (United States Court of Appeals, Federal Circuit September 25, 1996).

European Commission. (2013). *Impact Assessment on a proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against misappropriation.* Commission Staff Working Document, Brussels. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013SC0471

European Parliament News. (2015, June 16). Trade Secrets: freedom of expression must be protected, say legal affairs MEPs.

Executive Office of the President of the United States. (2013). *ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS.* Retrieved from https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf

Forrester Consulting. (2012). *The Value of Corporate Secrets, How Compliance and Collaboration Affects Enterprise Perception of Risk.* Retrieved from www.forrester.com

General Intelligence and Security Service, Ministry of the Interior and Kingdom Relations. (2014). *ANNUAL REPORT AIVD.* Retrieved from www.aivd.nl

Goldam, E., Levine, D. S., Sandeen, S. K., Seaman, C. B., Bambauer, J., Bessen, J., . . . Wiant, S. K. (2015, November 17). Professors' Letter in Opposition to the Defend Trade Secret Act of 2015. Retrieved from https://cyberlaw.stanford.edu/files/blogs/2015%20Professors%20Letter%20in%20Opposition%20to%20DTSA%20FINAL.pdf

Goldman, E. (2015). Ex Parte Seizures and the Defend Trade Secrets Act. *Washington and Lee Law Review Online, 72*(2). Retrieved from http://scholarlycommons.law.wlu.edu/wlulr-online/vol72/iss2/4

Halligan, R. M. (2015). Revisited 2015: Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996. *MARSHALL REV. INTELL. PROP. L.*

International Chamber of Commerce. (2014). Trade Secrets: Tools for Innovation and Collaboration. p.9.

Jorgenson, D. W., & Vu, K. M. (2016, February 5). The ICT revolution, world economic growth and policy issues. *ELSERVIER*, 383-397. doi:10.1016/j.telpol.2016.01.002

Klitzke, R. A. (1980). The Uniform Trade Secret Act. *Marquette Law Review, 64*(2). Retrieved from http://scholarship.law.marquette.edu/mulr/vol64/iss2/2

Knaak, R., Kur, A., & Hilty, R. M. (2014, June 3). Comments of the Max Planck Institute for Innovation and Competition . Retrieved from http://ssrn.com/abstract=2464971

Lahodynsky, O. (2015, June 15). EU trade bill threatens media freedom. *eurobserver*.

Linton, K. (2016, March). The Unexpected Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research.

Lippoldt, D. C., & Schultz., M. F. (2014). Trade Secrets, Innovation and the WTO. Geneva, Switzerland: International Center for Trade and Sustainable Development (ICTSD) and World Economic Forum. Retrieved from www.e15initiave.org/

Meltzer, J. (2013, February). The Internet, Cross-border Data Flows and International Trade. *Issues in Technology Innovation (22)*. Center for Technology Innovation at Brookings. Retrieved from https://www.brookings.edu/research/the-internet-cross-border-data-flows-and-international-trade/

Nair, M. (2002, August 27). Protection of Trade Secrets/Undisclosed Information. *Journal of Intellectual Property Rights, 7*, 527.

Pellegrino, M. (2015, June 5). The Threat of State-Sponsored Industrial Espionage. *European Union Institute for Security Studies*(26). Retrieved from http://www.iss.europa.eu/publications/detail/article/the-threat-of-state-sponsored-industrial-espionage/

Pooley, J. (2013, June). Trade Secrets: The Other IP Right. *WIPO Magazine*. Retrieved from http://www.wipo.int/wipo_magazine/en/2013/03/article_0001.html

Quinn Emanuel Urquhart and Sullivan LLP. (2012, April 2). Spotlight on the Economic Espionage Act. *Lexology*. Retrieved from http://www.lexology.com/library/detail.aspx?g=d7ac3398-5ff9-44ca-ba44-03bc6cd1eb16

Samuelson, P. (2002). *Reverse Engineering Under Seige.* Available at: http://scholarship.law.berkeley.edu/facpubs/2383.

Schultz, M. F., & Lippoldt, D. C. (2014). *APPROACHES TO PROTECTION OF UNDISCLOSED INFORMATION (TRADE SECRETS) - BACKGROUND PAPER.* Organisation for Economic Co-operation and Development (OECD). Retrieved from http://www.oecd.org/trade

Senate and House of Representatives of the United States of America in Congress assembled. (1996, October 11). PUBLIC LAW 104 - 294 - ECONOMIC ESPIONAGE ACT OF 1996. *An act to amend title 18, United States Code, to protect proprietary economic information, and for other purposes.* Retrieved from https://www.gpo.gov/fdsys/pkg/PLAW-104publ294/content-detail.html

Sinclair v. Aquarius Electronics, Inc., Civ.No.31700 (Court of Appeals of California, First Appellate District, Division Two October 2, 1974).

Spencer, S. (1998). The Economic Espionage Act of 1996. *Berkeley Tech. L.J. 305*. doi:http://dx.doi.org/doi:10.15779/Z38X95T

The Commission on the Theft of American Intellectual Property. (2013). *The Report of the Commission on the Theft of American Intellectual Property.* The National Bureau of Asian Research. Retrieved from http://www.ipcommission.org/

The University of Melbourne, Melbourne Institute of Applied Economics and Social Research. (2004). On the Interaction between Patent Policy and Trade Secret Policy.

UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS. (1985). NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS. Retrieved from http://www.uniformlaws.org/Search.aspx?cx=014921086760789645719:at7aeght8rg&cof=FORID%3A9&ie=UTF-8&q=uniform%20trade%20secret%20act&sa=Search

United States International Trade Commission. (2011). *China: Effects of IP Infringement and Indigenous Innovation Policies on the U.S. Economy.* Retrieved from http://www.usitc.gov

United States of America, Plaintiff-Appelle, v. Joya Williams, Defendant-Appellant, 07-12526, 07-12653 (United States Court of Appeals, Eleventh Circuit March 20, 2008).

Villasenor, J. (2015, August). Corporate CyberSecurity Realism: Managing Trade Secrets in a World Where Breaches Occur. *Quarterly Journal, 43*.

W. Kintner, E., & L. Lahr, J. (1975). *An Intellectual Property Law Primer .* New York: Macmillan Publishing Co., Inc.; Collier Macmillian Publishers.

Yeh, B. T. (2016, April 22). Protection of Trade Secrets:Overview of Current Law and Legislation. *Congressional Research Service*. Retrieved from https://www.fas.org/sgp/crs/secrecy/R43714.pdf