

THE TRADE SECRETS PROTECTION IN U.S. AND IN EUROPE: A COMPARATIVE STUDY

CHIARA GAIDO*

I. INTRODUCTION

“Fatti non foste a viver come bruti ma per conseguir virtue e canoscenza” (Dante Alighieri, La Divina Commedia, 1321, Inferno, Canto xxvi). Dante Alighieri, the famous Italian poet who is considered the father of the Italian modern language, wrote in his masterpiece that humans are created for the pursuit of virtue and knowledge. In the modern society, perfect tools that consent the acquisition of knowledge and that enhance its improvement are the Intellectual Property Rights (IPRS).

It is in fact well established that the main purpose of IPRS and their consequent protection is to allow the progress of society through knowledge, innovation and new works of art. And this is particularly true with respect to know-how and information which has a special commercial value for the owner (i.e. trade secrets). The aim of this paper is to give a legal comparative analysis of the new laws that govern trade secrets protection in the United States and Europe related to the impact that such laws may have on the business decisions adopted by companies. In fact, only by understanding deeply these new legal regimes, companies will be in the position to effectively protect their own trade secrets.

In light of the above, the purpose of the present paper is to highlight the similarities and the dissimilarities between the two recently adopted regulations in order to give useful guidelines to international companies who deal in both geographical areas and to offer food for thought on how companies should render the protection of their trade secrets more efficient.

* Chiara Gaido is an Italian attorney whose practice is focused on IP matters and who earned an LLM that was jointly organized by the World Intellectual Property and the University of Turin –Italy as well as another LLM from Benjamin N. Cardozo Law School – New York. Milán, Italia. Fecha de recepción: 28 de septiembre de 2017. Fecha de aceptación: 24 de octubre de 2017. Para citar el artículo: GAIDO, CH. “The trade secrets protection in U.S. and in Europe: a comparative study”, *Revista La Propiedad Inmaterial* n.º 24, Universidad Externado de Colombia, julio-diciembre 2017, pp. 129-144. DOI: <https://doi.org/10.18601/16571959.n24.06>

The potential impact of trade secrets in the modern economy is undeniable. In the form of know-how, they do not only form an alternative to patent protection for an invention, but even if a patent is granted there is complimentary know-how that is not included in the patent application. That know-how is then kept and protected as a trade secret¹. Just an example: the value of the Google algorithm for search engine is without any doubt one of the most important asset of the tech company and its loss would probably undermine the whole company, making it for her almost impossible to recoup from such loss.

Therefore, the present paper will focus first its attention on the economic value of trade secrets in our economy and the costs related to cybercrime and cyberespionage, then, on the following two paragraphs, it will analyze the U.S. and E.U. historical legal backgrounds that brought to the adoption of the two recent laws. Subsequently, the heart of this article will be the comparative analysis of the provisions of the laws at issue, pointing out the existing similarities and dissimilarities, giving few highlights on a recent U.S. case law that represents the first concrete application of the federal statute, to conclude finally with some potential suggestions for companies that deal in both U.S. and E.U.

2. THE ECONOMIC VALUE OF TRADE SECRETS

The increased importance of IPRs, including trade secrets, is nowadays indisputable. Businesses, irrespective of their size, value trade secrets as much as patents and other forms of intellectual property rights. They use confidentiality as a management tool for business competitiveness and research innovation, covering a diversified range of information, which extends beyond technological knowledge to commercial data such as information on customers and suppliers, business plans or market research and strategies. Small and medium-sized enterprises (SMEs) –particularly – value and rely on trade secrets more, because the use of intellectual property rights tends to be expensive and SMEs often do not have sufficient specialized human and financial resources to manage and protect such rights.².

The importance of trade secrets has increased through the years. David S. Almeling perfectly depicts some of the reasons of such increase in the U.S. market. In the author's opinion, two elements of such increase are: 1) the fact that the improvement of technology is making the misappropriation of trade secrets easier (i.e. not only increasing the risk for those with a legitimate access to them but also

1 TORREMANS, L. C. The road towards the harmonisation of trade secrets law in European Union. *Revista La Propiedad Inmaterial*. Bogotá: Universidad Externado de Colombia, 2015, (20), p. 27-38 (p. 37). ISSN: 1657-1959.

2 European Parliament. *Report on the proposal of a Directive of the European Parliament and Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, 2015, 7.

and especially for the unlawful access to them, meaning hacking attacks) and 2) the increasing economic value of trade secrets which is always quite hard to establish³.

The economic value of trade secrets lies in the competitive advantage gained by its proprietary from its use, coupled with the exclusion of others from such use. But unlike the right to exclude others from using a patent for a limited period of time, which arises from a government granted monopoly tied to disclosure, the right to exclude others from the use of a trade secret arises from limited disclosure and reasonable efforts to maintain secrecy⁴. The relevance of trade secrets is also proved in the U.S., for example, with the increase through the years – even before the current law was adopted – of trade secret litigation in federal courts, while federal litigation has decreased overall⁵.

The importance recognized to such IPRS is also highlighted by the costs that companies and countries have to face due to cybercrime and cyberespionage. Just few data to consider: with its 2014 Report on Net Losses, the international company McAfee showed that U.S., China, Japan, and Germany, have reached \$200 billions in losses due to cybercrime.⁶ Such report takes into account direct and indirect costs, losses of intellectual property rights, theft of financial assets and sensitive business info, opportunities costs, additional costs for securing network, and costs of recovering cyberattacks, including reputational damages to hacked companies.

Another important factor that lead to the conclusion that trade secrets require an effective and strong protection is the impact that their violation could have on international relationships between countries such as between U.S. and China when the U.S. charged six Chinese nationals, including some University professors for the alleged theft of technology used in mobile phones⁷.

3 ALMELING, DAVID S. Seven reasons why trade secrets are increasingly important. *Berkeley Technology Law Journal*. Berkeley, CA: U. de Berkeley, 2012, 27(2), pp. 1098-1106. ISSN: 1086-3818.

4 PURDUE, GLENN. Understanding the economic value of trade secrets. *American Bar Association Journal*. Chicago, IL: ABA., 28 March 2014. ISSN: 0002-7596.

5 ALMELING, DAVID S. et al. A statistical analysis of the trade secret litigation in federal courts. *Gonzaga Law Review*. Spokane, WA: Gonzaga University School of Law, 2010, 45, pp. 291-293.

6 MACAFEE. *Net losses: Estimating the global cost of cybercrime, economic impact of cybercrime II*. Washington: Center for Strategic and International Studies, 2014. Available at https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

7 BBC. *US charges six Chinese nationals for stealing trade secrets*. Available on <http://www.bbc.co.uk/news/world-us-canada>. See also cyber-espionage by members of China's People's Liberation Army ("PLA"). Unit 61398 that has received widespread press coverage due to the scale of the conduct and value of the proprietary information allegedly stolen. SANGER, DAVID E. et al. China's Army seen as tied to hacking against U.S. *The New York Times*, Feb. 19, 2013. ISSN: 0362-4331; see also MANDIANT. *APT1: Exposing One of China's Cyber Espionage Units*. 2013. Available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf and other information available and cited by SEAMAN, CHRISTOPHER B. The case against Federalizing Trade Secrecy. *Virginia Law Review*. Charlottesville, VI: University of Virginia, School of Law, 2015, 101(2), pp. 317-394 (p. 320). ISSN: 0042-6601.

In a critical scenario as described in the paragraphs above, the loss due to IP theft is also the most difficult component of the cost of cybercrime to estimate. Valuing IP is an art form, based on estimating the future revenue IP will produce, or the value the market places on IP (which are not always the same). The cost to companies varies from among sector and by the ability to monetize stolen data (whether it is IP or business confidential information). Although all companies face the risk of loss of intellectual property and confidential business information, some sectors—finance, chemicals, aerospace, energy, defense, and IT—are more likely to be targeted and face attacks that persist until they succeed. Losses are higher for sectors where it is easier to monetize the stolen data, as with the chemical industry where proprietary formulas can be easily duplicated or with sensitive business information on business negotiations.⁸

Therefore, due to the need of facing new unlawful behaviors that put at risk the IPRS through new technology (often with cross borders relevance that renders the prosecution of such wrongdoings even harder) and the increase in the use of trade secret protection as an alternative to patents law (with the unfortunate flip side of such protection that in case of breach, the value to be recoup will be very hard to be determined) countries felt the need to adjust their laws in accordance with such demands. This is why both the U.S. and the E.U. adopted in 2016 new laws that govern the protection of trade secrets, which will be analyzed in the following paragraphs.

3. THE U.S. LAW ON TRADE SECRETS PROTECTION – HISTORICAL BACKGROUND

To understand the actual body of law governing the trade secrets protection in U.S., we have to look, briefly, at the historical background that brought the U.S. to the adoption of these rules. Unlike other forms of intellectual property that can trace their origins back several hundreds of years, trade secret law is a creation of state court opinions from the middle of the 19th century⁹. As noted by one legal scholar, the principles of trade secret law

evolved out of a series of related common law torts: breach of confidence, breach of confidential relationship, common law misappropriation, unfair competition, unjust enrichment, and torts related to trespass or unauthorized access to a plaintiff's property. It also evolved out of a series of legal rules—contract and common law—governing the employment relationship¹⁰.

8 MACAFEE. *Op. cit.*, p. 12.

9 YEH, BRIAN T. *Protection of trade secrets: Overview of Current Law and Legislation*. Congressional Research, 2016, p. 5. Available at <https://fas.org/sgp/crs/secrecy/R43714.pdf>

10 LEMLEY, MARK A. The surprising virtues of treating trade secrets as IP rights. *Stanford Law Review*. Stanford: Stanford Law School, 2008, (61), 311-316. ISSN: 0038-9765.

Regardless on how the protection was granted to such IPRs, it has been always very difficult to establish a precise definition of trade secrets. In any event, whether information qualifies as a “trade secret” under federal or state law is a question of fact. For this reason, it is determined by a jury¹¹ who then normally consider several factors in assessing if certain material is in fact a trade secret such as (i) the extent to which the information is known outside of the company; (ii) the extent of measures taken by the company to guard the secrecy of the information and (iii) the value of the information to the company and to its competitors¹². Therefore, originally such IPRs were protected from misappropriation under state law and therefore its owners could seek civil damages in state courts by pursuing a common law tort action for misappropriation or through a specific state statute.

In 1939 the American Law Institute (ALI) published the “Restatement of Torts” with the aim of providing “a clear formulation” of common law and its statutory elements, which included Section 757 and 758 that specifically regulated trade secrets and their misappropriation. Later, in 1979, the National Conference of Commissioners on Uniform State Law (NCCUSL) issued the Uniform Trade Secrets Act (UTSA), which represents the first comprehensive effort to codify the law of trade secrets protection in a harmonized way. The UTSA was adopted by several states, however, the problem here was that the NCCUSL lacked direct legislative authority itself and by consequence its acts became law only to the extent that state legislatures chose to adopt them.

Finally, the federal government adopted the Economic Espionage Act (EEA) in 1996. It defined then two separate criminal offenses: (1) theft of a trade secret for the benefit of a foreign entity (economic espionage, 18 U.S.C. Section 1831), and (2) trade secret theft intended to confer an economic benefit to another party (theft of trade secrets, 18 U.S.C. Section 1832). As a threshold matter, to trigger an action under either provision of the EEA, the information had to be as a trade secret. While 18 U.S.C. Section 1831 regulated the misappropriation of trade secrets pursued with the intent to benefit a foreign government, instrumentality, or agent, the 18 U.S.C. Section 1832 was of more general application. In fact, the main elements of the latter provision, focused on the simple “trade secrets theft or misappropriation”, were: (1) the intentional and/or knowing theft, appropriation, destruction, alteration, or duplication of (2) a trade secret related to a product or service used in or intended for use in interstate or foreign commerce (3) with intent to convert the trade secret and (4) intent or knowledge that such action will injure the owner.

Some observers urged Congress to adopt a comprehensive, federal trade secret law in order to promote uniformity in trade secret law throughout the United States¹³. Supporters of such legislation argued that a federal trade secrets law would

11 MILGRIM, ROGER M. *Milgrim on Trade Secrets*, 2015, §15.01, pp. 4-15.

12 Restatement (First) of Torts §757, comment b.

13 LAO, MARINA. Federalizing trade secrets in an information economy. *Ohio State Law*

create procedural and substantive standards for the trade secret misappropriation offense on a uniform nationwide basis, in response to the current situation of state trade secret laws in which there are “fundamental differences about what constitutes a trade secret, what is required to misappropriate it, and what remedies are available” due to state-by-state variations in statutory text and state court interpretations¹⁴.

On May 2016, the Defend Trade Secrets Act (DTSA) was enacted and created a private cause of action in federal courts for trade secret owners. According to the DTSA, a trade secret owner may now bring a civil action of a trade secret that is misappropriated if it is related to a product or service used in, or intended to be used in, interstate or foreign commerce.

In order to have a better and well-balanced overview of the current U.S. legislation, it is essential to give space to those authors who expressed criticism towards the federalization of trade secrets. With this respect, Christopher B. Seaman perfectly explains why that federalization will not necessary create uniformity¹⁵. The arguments that are brought by the author can be summarized as the following: (i) the fact that forty-seven states have adopted the Uniform Trade Secrets Act (“UTSA”) and therefore a common foundation for state trade secret law already exists; (ii) trade secrecy likely would not accomplish uniformity if the legislation does not preempt parallel state trade secret law¹⁶ and (iii) federalizing trade secrecy may undermine patent law’s objective of promoting the disclosure and widespread dissemination of information regarding new inventions because it will likely cause more inventors to opt out of the patent system¹⁷.

Additional problems are related to the fact that federalization would not resolve the choice-of-law problems because the resolution of trade secret claims often depends upon other areas of state law, including contract, employment, and tort. Similarly, breach of a fiduciary duty that can give rise to a misappropriation claim as well as the scope and enforceability of restrictive covenants like non-disclosure agreements and non-compete clauses that are commonly used to protect trade secret information are governed by state law: as a result, even if trade secret protection

Journal. Ohio: The Ohio State University, 1998, 59(5), pp. 1633-1696. ISSN: 0048-1572.

14 ALMELING, DAVID S. Four reasons to enact a Federal Trade Secrets Act. *Fordham Intellectual Property, Media & Entertainment Law Journal*. New York, NY: Fordham IPLJ, 2009, 19(3), p. 769-798 (p. 774). ISSN: 1079-9699.

15 SEAMAN, CHRISTOPHER B. The case against Federalizing Trade Secrecy. *Virginia Law Review*. Charlottesville, VI: University of Virginia, School of Law, 2015,101(2), pp. 317-394. ISSN: 0042-6601.

16 Under the Supremacy Clause of the U.S. Constitution, any state law that conflicts with federal law is preempted and thus is “without effect”. As pointed out by Seaman, the current legislation would not preempt state trade secret law, expressly or implicitly, thus permitting a federal civil cause of action to coexist with state law and therefore, in the author’s opinion, Federal legislation that does not preempt state law ultimately will undermine harmonization, rather than promote it, by creating a federal regime that exists in parallel with state trade secret law.

17 *Id.* at pp. 321-322.

were federalized, a federal court frequently would have to engage in a choice-of-law analysis regarding such issues¹⁸.

4. THE E.U. LAW ON TRADE SECRETS PROTECTION

– HISTORICAL BACKGROUND

As for the U.S. a long process has been required in order to enact a federal claim for trade secrets theft, in E.U. as well the path that brought to the adoption of the EC Directive 2016/943 has been very long and very complex. Originally, the protection against the unlawful acquisition, use or disclosure by third parties of trade secrets was already included in some provisions of the Agreement on Trade-Related Aspects of Intellectual Property (the TRIPS Agreement) and all Member States, including the European Union itself were bound by this Agreement. s ever adopted.

According to Art. 39 of the TRIPS Agreement, the foundation of the protection of such IPRS was related to the protection against unlawful competition. Such agreement established that in order to be protected, such information must be confidential with a commercial value that derived directly from its confidentiality and from the measures that the owner has adopted in order to protect it¹⁹.

The problem was that, besides such provision, there was no international treaty on the protection of trade secrets²⁰. Therefore, everything was left to the national rules of each Member State and, by consequence, substantial differences existed with regard to the protection of trade secrets. Thus, for example, not all Member States have adopted national definitions of trade secrets and/or unlawful acquisition, use, or disclosure of a trade secret, so that the scope of protection was not readily accessible and differed throughout the Member States. Furthermore, there was no consistency regarding the civil law remedies available in cases of unlawful acquisition, use, or disclosure of trade secrets, as cease and desist orders are not always available in all Member States against third parties who are not competitors of the legitimate trade secret holder. Divergences also existed across with respect to the treatment of third parties who acquired the trade secret in good faith but subsequently came to learn that their acquisition derived from a previous unlawful acquisition by another party²¹.

18 *Id.* at pp. 322-323.

19 GUZMÁN DELGADO, DIEGO F. *Secreto empresarial*. In E. RENGIFO GARCÍA (dir.). *Derecho de patentes*. Bogotá: Universidad Externado de Colombia, 2016, pp. 938-940. ISBN: 9789587725599.

20 Different countries, such as Colombia, started to grant protection to trade secrets with a protection that reflected the standards provided by the TRIPS Agreement (first with the Código de Comercio of 1971 and then finally with the Decisión Andina 344 of 1993). For a deep analysis of the trade secrets protection in U.S. and in the Andean Community, see GUZMÁN, *supra* note 21 at p. 938 and following.

21 European Parliament Report, at pp. 9-10.

The differences existing in the various national regimes were even more substantial in two cases. The first one, for what concerns the opportunity granted to a legitimate trade secret holder to seek the destruction of goods manufactured by third parties who use such trade secrets unlawfully. The second one, for the calculation of damages since not all the Member States allowed such calculation to be determined by the reasonable royalty or fee which could have been granted through a license with the trade secrets holders.

The existing split of the trade secrets protection within the E.U. territory has certainly affected through the years the internal market by lowering companies' incentives to undertake R&D activity that could eventually lead to trade secrets protection. In fact, without harmonized regulations on this matter, the risks of facing conflicting courts' decisions in order to effectively protect such IPRs together with the need of meeting different standards of protection in each Member States, these factors probably brought companies not to pursue trade secrets protection beyond their national borders and this is probably one of the main reason that brought to the adoption of the Directive EC 2016/943 on May 2016 for the protection of trade secrets²².

5. DIFFERENCES AND SIMILARITIES BETWEEN THE U.S. AND THE EU REGIMES

The U.S. have always been a model for the European Union for what concerns the legislation for the protection of trade secrets. Just think about the fact that the earliest cases discussing trade secrets in U. S. occurred in 1837²³ and in 1868²⁴.

Both legislations present many similarities, which therefore make it easier for international companies to understand how to effectively protect their valuable information. Nonetheless, important differences exist especially for what concerns the protection of whistleblowers and the remedies the plaintiff can seek in case of misappropriation or unlawful use. In this paragraph, the similarities will be examined first and then we will focus our attention on the existing dissimilarities.

First of all, both laws have a very similar definition concerning trade secrets. In fact, pursuant to 18 U.S.C. § 1839(3):

22 The Directive does not have a direct effect in the EU member states and therefore it must be incorporated in their national laws in order to be effective: deadline to be compliant is June 9, 2018.

23 *Vickery vs. Welch*, 36 Mass. (1 Pick.) 523, 524 (1837). (Holding that there is an implied duty of confidentiality in shared trade secrets).

24 *Peabody vs. Norfolk*, 98 Mass. 452, 457-458 (1868). (Holding that one who invents and keep secret a process of manufacture has a property right in it against one who in breach of confidence attempts to use it or disclose it to third parties). Both cases cited by ALMELING, DAVID S. *Seven reasons why trade secrets are increasingly important*. *Op. cit.*

[The term] ‘trade secret’ means all forms and types of financial, business, scientific, technical, economic, or engineering information, ... whether tangible or intangible, and whether or how stored, compiled, or memorialized ... if-

- (A) the owner thereof has taken reasonable measures to keep such information secret, and

- (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information [.]

Instead, according to Art. 2 Sec. (1) of the E.U. Directive:

[The term] trade secrets mean information which meets all the following requirements: (a) 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 person within the circles that normally deal with the kind of information in question;

(b) it has commercial value because it is secret and

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

Thus, while the DTSA and the E.U. Directive define trade secrets similarly, relatively minor differences include: (i) the fact that while the DTSA specifies that information must not be readily ascertainable *through proper means*; the E.U. directive does not expressly include such language in the context of the legal definition, but it does separately establish lawful acquisition, use, or disclosure, as exemptions to misappropriation (E.U. Directive Art.3, §§ 1, 2); (ii) while according to the DTSA, trade secret information must not be generally known to or readily ascertainable by “another person *who can obtain economic value from the disclosure of use of the information*” (18 U.S.C. § 1839(3)(B)), pursuant to art. 2 § (1)(a) of the E.U. Directive, the other person has to be “*within the circles that normally deal with the kind of information in question.*” In practice, however, this distinction may not be significant. A person who can obtain economic value from the information’s disclosure or use generally also will be a person within the circles which normally deals with the kind of information in question and vice versa²⁵.

25 AKENBRANDT, BRIAN; VORMANN, THORSTEN & HERTLIN, RICHARD. *Comparing U.S. and EU Trade Secrets Laws*. Washington/Brussels: Trans-Atlantic Business Council, 2016, available on www.transatlanticbusiness.org, at p. 6.

Therefore, the definition of trade secrets includes: (i) all technical aspects pertaining to the company such as the production processing and manuals, patents and all form of scientific inventions, industrial designs; (ii) the commercial aspects of the company (ex. customers' lists) and (iii) any other internal company's aspects that could be commercially valuable for its competitors (such as the relationship with the employees, the financial situation of the company or its intent to enter into a specific contract)²⁶.

Another slight difference concerning between DTSA and the E.U. Directive is that, according to the latter, a trade secret must be ascertainable "*as a body or in the precise configuration and assembly of its components.*" E.U. Directive art. 2, § (1)(a). This simply means that information still may be a trade secret even if its components are known or readily ascertainable, as long as their precise configuration is not. Although the DTSA does not expressly include similar provision, the distinction should be considered insignificant as well as the law in U.S. jurisdictions generally recognize that unique combinations of generally known components or concepts still can be trade secrets²⁷.

For what concerns the unlawful behaviors that both laws aim to punish, despite variations in language, the definition of misappropriation through "improper means" given by the DTSA is mostly consistent with the E.U. definition of unlawful acquisition, use or disclosure of trade secrets (See 18 U.S.C. § 1839(5)(A) and E.U. Directive Art 4, § 2).

However, the provisions on misappropriation by acquisition diverge for what concerns the required knowledge of the person acquiring the trade secret information. In fact, while the DTSA requires actual or constructive knowledge before imposing liability for acquisition of a trade secret, regardless of whether the trade secret is acquired directly from the trade secret owner or indirectly from a third party. (18 U.S.C. § 1839(5)(A)); the E.U. Directive distinguishes between information acquired directly from the trade secret holder and information acquired from a third party. If the information is acquired while lawfully under the control of the trade secret holder, unlawful acquisition simply must be "unauthorized" or otherwise contrary to honest commercial practices E.U. Directive art. 4, § 2.

Instead, if a trade secret is "obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully" the European Directive does require actual or constructive knowledge that the trade secret was obtained from someone who was using or disclosing it unlawfully (See. E.U. Directive Art. 4 § 4).

26 PAYÁN RODRÍGUEZ, C. FELIPE. Secreto empresarial, vigencia como mecanismo de protección en la propiedad intelectual (Trade secrets, validity as an intellectual property). 2011. In *Revista La Propiedad Inmaterial*. Bogotá: Universidad Externado de Colombia, 2011, (15), p. 211. ISSN: 1657-1959.

27 *Id.* at supra note 27 at p. 7 and see also *Restatement (Third) of Unfair Competition* § 39 cmt. (f).

Again, both laws can be considered mostly consistent for what concerns misappropriation by use or disclosure as well as for the definition of a lawful acquisition of trade secrets lawful (i.e. when the trade secret is obtained by any of the following means: reverse engineering, independent derivation, as well as “other lawful means of acquisition” (according to the DTSA) or “other honest commercial practices” (according to the E.U. Directive).

Similarities between the two laws also regards:

- the measures that must be granted during court proceeding in order to maintain the trade secret information confidential 18 U.S.C. § 1835(b) and E.U. Directive art. 9, §§ 1-2.;

- the provisional remedies that a court can grant in such proceeding. See 18 U.S.C. § 1836(b)(2) and E.U. Directive art. 10, § 1 together with similar factors that courts should consider before granting or denying such precautionary reliefs such as (i) Balancing of harms and public interest § 1836(b)(2)(A)(ii) and E.U. Directive art. 11, § 2. and (ii) Target in possession of trade secret and likelihood of success on the merits. 18 U.S.C. § 1836(b)(2)(A)(ii), and the E.U.- art. 11, § 1.

- the fact that both laws include provisions allowing for the imposition of a reasonable royalty to compensate the trade secret owner or holder as an alternative to a preliminary injunction or other preliminary measures. 18 U.S.C. § 1836(b)(3)(A)(iii); E.U. Directive art. 10, § 2;

- the liability for misappropriation by a downstream customer or supplier (See 18 U.S.C. § 1839(5)(B)(iii) and E.U. Directive Article 4, section 5). While under the DTSA such person will be liable only if, before a material change in his position, he has actual or constructive knowledge both that the information is a trade secret and that he learned of the trade secret by accident or mistake, under the E.U. Directive any person who while marketing, importing, exporting or storing goods, infringes a trade secret, such conduct constitutes unlawful use only where the actor has actual or constructive knowledge that the trade secret was used unlawfully--regardless of whether the information was received from the trade secret holder or indirectly from any other person.

With respect to damages, and in particular to compensatory damages, the DTSA and the E.U. Directive have similar and consistent provisions. Both in fact permit damages for actual loss or prejudice suffered by the claimant including: the claimant’s lost profits, *see* 18 U.S.C § 1836(b)(3)(B)(i)(I), E.U. Directive art. 14, § 1; and (non-duplicative) damages based on benefits unfairly received by the misappropriator (“unjust enrichment” under U.S. law, *id.* § 1836(b)(3)(B)(i), and “unfair profits made by the infringer” under E.U. Directive art. 14, § 2). Alternatively, they both provide damages based on a reasonable royalty for the misappropriation. 18 U.S.C. § 1836(b)(3)(B)(ii); E.U. Directive art. 14, § 2.12: in addition, the E.U. law also allows Member States to limit employee liability toward their employers if the misappropriation was without intent. See art. 14, § 1 of the Directive.

Finally, both the DTSA and the E.U. Directive allow for sanctions against a party that initiates misappropriation claims in bad faith. On one side, the DTSA specifically provides for an award of attorneys' fees to a party that prevails against a bad-faith misappropriation claim. 18 U.S.C. § 1836(b)(3)(D). On the other side, the E.U. Directive compels Member States to allow for the imposition of sanctions on the applicant or the award of damages to the prevailing respondent if the legal proceedings were initiated abusively or in bad faith. See art. 7, § 2.

Furthermore, other main differences that exist between the laws at issue can be summarized as it follows:

1. Standing requirement: such difference depends on the definition given by the E.U. and the U.S. laws of trade secret owner and described above. In fact, while in U.S. only the owner may have standing under the DTSA, under the E.U. provisions, it seems that anybody who is lawfully in control of a trade secret (i.e. licensee) may bring a law suit.

2. Protection of free speech and whistleblowers: whereas the DTSA protects a whistle-blower only to the extent he discloses a trade secret "in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney," 18 U.S.C. § 1833(b)(1)(A),⁶ the E.U.-Directive states that misappropriation claims against whistleblowers acting in public interest must be dismissed—without requiring the trade secret to have been disclosed confidentially. E.U. Directive art. 5. Moreover, the E.U. law provides similar immunity from liability where the actor is exercising the freedom of expression, in circumstances involving workers' disclosures to representatives in accordance with Union or national law, and for the purpose of protecting any other legitimate interest recognized by Union or national law;

3. Immunity: the DTSA provides immunity from liability only "for the disclosure of a trade secret." It does not immunize the act of illicitly acquiring the trade secret, even if the disclosure is made for the salutary purposes protected in the law. Therefore, an employee who lacks authorized access to a trade secret and acquires it improperly and then discloses it to an appropriate government agency may not be held liable for the disclosure, but may still be held liable for the illicit acquisition. By contrast, the E.U. Directive expressly states that its immunity provisions apply more broadly to the "acquisition, use or disclosure of the trade secret." And

4. Punitive Damages: while under the DTSA, in cases of willful or malicious misappropriation, punitive damages may be awarded up to 2 times the compensatory damages. 18 U.S.C. § 1836(b)(3)(C), the E.U. Directive does not expressly provide for such punitive damages, but it does provide that judicial authorities may, in appropriate cases, consider non-economic factors such as moral prejudice suffered by the trade secret holder. E.U. Directive art. 14, § 2. (whose amount will be unlikely very hard also because most of the times it is very hard to determine in the complaint).

6. BRIEF NOTES ON THE RECENT U.S. CASE LAW

If as of today, no new litigation has arisen yet under the new E.U. law, this is not the case for the U.S. On February 2017, Waymo, a Google company, filed a law suit in the Federal Court of San Francisco against Otto, a start-up acquired in 2016 by Uber and alleging trade secrets theft by Otto's employees of its technology and design concerning laser-scanning system to guide self-driving cars. It is alleged that the "calculated theft" suffered by Waymo is of more than \$500 Million USD. In my opinion, this case is sure to become one of the first high-profile cases concerning trade secrets litigation, not only because it is the first time that claims under the DTSA has been brought to the attention of a court but also because it underscores the importance of the technology that is at the heart of the legal battle.

Just a few notes on the facts of the case:

Waymo is a "self-driving technology company," which for the past years has been developing technology related to self-driving cars, including a laser system used to help the car navigate known as LIDAR ("Light Detection and Ranging"). In January 2016, one of Waymo's managers left the company and launched Otto, a new company focused on self-driving car technology which was later acquired by Uber on August 2016. Waymo became suspicious that Otto was using its technology when it inadvertently received an email from one of its LIDAR-component vendors which was apparently intended for Otto, and purported to attach a drawing of an Otto circuit board. According to Waymo, the Otto circuit board had "a striking resemblance to" Waymo's LIDAR circuit board. In addition to that, few months after the departure of its key manager, Waymo noted the departure of several other employees for Otto. Waymo in its complaint contends that Waymo's original manager, who first left the company, had taken over 14,000 confidential company's files and uploaded them to a personal hard drive before his departure.

As of September 2017, the litigation is still ongoing. Recently, Waymo tried to postpone the trial by alleging a "mountain of new evidence" to analyze. We will see in the following months how this case will evolve.

7. CONCLUSIONS

In a globalized economy, where threats to exclusive rights can come across the globe, it is essential to grant a harmonized protection throughout the different countries. If for patent, trademark, and copyright law, this goal has been achieved – even maintaining important differences between the various legal systems – this was possible because such exclusive rights have been the object of treaties adopted by the international community, which allowed uniform standards of protection. This is different for what concerns trade secrets. The recent laws adopted by the E.U. and the U.S. are the first important step toward the harmonization of such IPRs and the many existing similarities are an evident proof of this direction. However, in

my opinion, one huge difference still exists between the two laws at issue. In fact, while with the adoption of a federal claim, the U.S. have potentially harmonized the standard of protection for trade secrets throughout their territory, this is not the case with the E.U. By not adopting a self-executing regulation, which would have applied directly in all Member States and, instead, by adopting a directive and therefore by leaving to each Member States the hard work of incorporating such law into their national laws, this may inevitably lead to some discrepancies in the applicable law in the different Member States and by consequence in its application by the national courts.

Therefore, it is essential for companies that deal in both geographical areas to protect their trade secrets in the most effective way, given the legal tools provided by such laws.

Here few suggestions: 1) by providing strong confidentiality – non-disclosure agreements coupled with stringent non-compete clauses; 2) by providing huge liquidated damages in order to avoid any breach of the above referenced agreements; also in consideration to the fact that punitive damages are generally not recognized in E.U.; 3) in case a breach occurred, by evaluating if such conduct does not constitute also a criminal offense under the state law (ex in Italy with Art. 623 of the Italian Penal Code²⁸) and 4) if the company decides to sue in civil court, be aware that in E.U. it will be very unlikely that the amounts awarded as damages due to trade secrets theft are similar to those recognized by the U.S. courts (i.e. meaning the amount will be much lower). On the other hand, one positive aspect in case of civil litigation in E.U. is that in many Member States there are specialized IP courts (for instance in Italy) that have exclusive jurisdiction to hear a case concerning IP violation, where judges have a specialized knowledge of such topics.

BIBLIOGRAPHY

- AKENBRANDT, BRIAN; VORMANN, THORSTEN & HERTLIN, RICHARD. *Comparing U.S. and EU Trade Secrets Laws*. Washington/Brussels: Trans-Atlantic Business Council, 2016.
- ALMELING, DAVID S. et al. A statistical analysis of the trade secret litigation in federal courts. *Gonzaga Law Review*. Spokane, WA: Gonzaga University School of Law, 2010, 45, pp, 291-293, 301-02.
- ALMELING, DAVID S. Seven reasons why trade secrets are increasingly important. *Berkeley Technology Law Journal*. Berkeley, CA: U. de Berkeley, 2012, 27(2), pp. 1098-1106. ISSN: 1086-3818.

28 See also a very interesting analysis on the criminal protection of confidential and privileged information in Colombia by PAYÁN RODRÍGUEZ, CARLOS FELIPE, *supra* note 28.

- ALMELING, DAVID S. Four reasons to enact a Federal Trade Secrets Act. *Fordham Intellectual Property, Media & Entertainment Law Journal*. New York, NY: Fordham IPLJ, 2009, 19(3), p. 769-798. ISSN: 1079-9699.
- BBC. *US charges six Chinese nationals for stealing trade secrets*. Available on <http://www.bbc.co.uk/news/world-us-canada>
- Directive 2016/943 of the E.U. Parliament and Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
- European Parliament. *Report on the proposal of a Directive of the European Parliament and Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, 2015, 7.
- GUZMÁN DELGADO, DIEGO F. *Secreto empresarial*. In E. RENGIFO GARCÍA (dir.). *Derecho de patentes*. Bogotá: Universidad Externado de Colombia, 2016, pp. 938-940. ISBN: 9789587725599.
- LAO, MARINA. Federalizing trade secrets in an information economy. *Ohio State Law Journal*. Ohio: The Ohio State University, 1998, 59(5), pp. 1633-1696. ISSN: 0048-1572.
- LEMLEY, MARK A. The surprising virtues of treating trade secrets as IP rights. *Stanford Law Review*. Stanford: Stanford Law School, 2008, (61), 311-316. ISSN: 0038-9765.
- MACAFEE. *Net losses: Estimating the global cost of cybercrime, economic impact of cybercrime II*. Washington: Center for Strategic and International Studies, 2014. Available at https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf
- MANDIANT. *APT1: Exposing One of China's Cyber Espionage Units*. 2013. Available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
- MILGRIM, ROGER M. *Milgrim on Trade Secrets*, 2015, §15.01, pp. 4-15.
- PAYÁN RODRÍGUEZ, C. FELIPE. Secreto empresarial, vigencia como mecanismo de protección en la propiedad intelectual (Trade secrets, validity as an intellectual property). 2011. In *Revista La Propiedad Inmaterial*. Bogotá: Universidad Externado de Colombia, 2011, (15), pp. 207-224. ISSN: 1657-1959.
- Peabody vs. Norfolk, 98 Mass. 452, 457-458 (1868).
- PURDUE, GLENN. Understanding the economic value of trade secrets. *American Bar Association Journal*. Chicago, IL: ABA., 28 March 2014. ISSN: 0002-7596.
- RENGIFO GARCÍA, ERNESTO. Dir. *Derecho de patentes*. Bogotá: Universidad Externado de Colombia, 2016. ISBN: 9789587725599.
- Restatement (First) of Torts §757
- SANGER, DAVID E. et al. China's Army seen as tied to hacking against U.S. *The New York Times*, Feb. 19, 2013. ISSN: 0362-4331.
- SEAMAN, CHRISTOPHER B. The case against Federalizing Trade Secrecy. *Virginia Law Review*. Charlottesville, VI: University of Virginia, School of Law, 2015, 101(2), pp. 317-394. ISSN: 0042-6601.

- TORREMANS, L. C. The road towards the harmonisation of trade secrets law in European Union. *Revista La Propiedad Inmaterial*. Bogotá: Universidad Externado de Colombia, 2015, (20), p. 27-38. ISSN: 1657-1959.
- Vickery v. Welch, 36 Mass. (1 Pick.) 523, 524 (1837).
- YEH, BRIAN T. *Protection of trade secrets: Overview of Current Law and Legislation*. Congressional Research, 2016, p. 5. Available at <https://fas.org/sgp/crs/secretcy/R43714.pdf>