Revista Jurídica vol. 03, nº. 52, Curitiba, 2018. pp. 199-224

DOI: 10.6084/m9.figshare.7371080

INTELLECTUAL PROPERTY LAW IN THE FOURTH INDUSTRIAL REVOLUTION: TRADE SECRETS RISKS AND OPPORTUNITIES

DIREITO DE PROPRIEDADE INTELECTUAL NA QUARTA REVOLUÇÃO INDUSTRIAL: SEGREDOS E OPORTUNIDADES DOS SEGREDOS COMERCIAIS

MARCELO NEGRI SOARES

Pós-Doutorado pela Uninove/SP (2017). Doutor pela Pontifícia Universidade Católica de São Paulo (2013). Mestre pela PUC-SP (2005). Graduado pela Universidade Estadual de Maringá/PR (1997). Especialista em Direito Processual pela Universidade Paulista (1998), em Direito Comercial pelo Mackenzie (2006), em Direito Público pela Escola Federal de Direito (2008). Formado em Contabilidade pelo IEEM - Maringá (1989). Advogado e contabilista. Professor e Pesquisador do Programa de Mestrado em Direito UniCesumar - Centro Universitário Cesumar, na linha de pesquisa Efetividade da Justiça e Direitos da Personalidade, lecionando a disciplina Acesso à justiça e Meios adequados de solução de conflitos. Funcionário do Banco do Brasil S.A. por mais de 20 (vinte) anos (última função: advogado pleno).

MARCOS EDUARDO KAUFFMAN

Doutorando em PhD Programme Coventry University, CU, Inglaterra. Graduado em Law - LLB Honours University Of Buckingham, Inglaterra.

ABSTRACT

Intellectual Property (IP) is increasingly recognised as a paramount intangible asset influencing the value of companies, as well as their corporate strategies and management. This article focuses on the risks and opportunities associated with the implementation of new technologies on the protection of trade secrets. The study concludes that Intellectual Property Law and Contract Law solutions must be

DOI: 10.6084/m9.figshare.7371080

underpinned by the business strategy and the business model. In addition, changes to organisational structures are necessary to bring together functions that typically operate in silos in many manufacturing businesses, namely: Engineering, Information Technology, Commercial and Legal departments. The present study was guided by the inductive and hypothetical-deductive methods, using bibliographical research.

KEYWORDS: Business Law; Intellectual Property; Industry 4.0; Risks and Opportunities.

RESUMO

A Propriedade Intelectual (PI) é cada vez mais reconhecida como um ativo intangível primordial que influencia o valor, as estratégias corporativas e a gestão da empresa. Este artigo enfoca os riscos e oportunidades associados à implementação de novas tecnologias na proteção de segredos comerciais. O estudo conclui que o Direto de Propriedade Intelectual e o Direito Contratual devem ser sustentados pela estratégia de negócios e pelo modelo de negócios. Além disso, mudanças nas estruturas organizacionais são necessárias para reunir funções que normalmente operam em silos em muitas empresas, por exemplo: engenharia, tecnologias da informação, departamentos comerciais e jurídicos. O presente estudo foi orientado pelos métodos indutivo e hipotético-dedutivo, utilizando pesquisa bibliográfica.

PALAVRAS-CHAVE: Direito Empresarial; Propriedade Intelectual; Indústria 4.0; Riscos e Oportunidades.

INTRODUCTION

In the postmodern society, the proliferation of conflicts of interest coupled with the culture of judicialization are emerging as a result of an immense demand for jurisdictional provision, a phenomenon widely recognized by all legal operators.

DOI: 10.6084/m9.figshare.7371080

The State, as guarantor of peace in the social context, has accepted the resolution of legal crises envisaged in intersubjective relations, to the extent that the doors of the Judiciary are open for any injury or threat to law. Nevertheless, there is excessive litigation and the extension of this power. That is why the lawyer's work is increasingly being redirected to minimize conflicts and offer safer solutions in the extrajudicial sphere.

Thus, in the contemporary world, the importance of information for business is undeniable (CITRARO, 2014, pp. 5-34). It also becomes a matter of central importance to devise mechanisms that allow companies to safeguard any kind of developed information, insofar as they can, and indeed – as it usually happens in many cases – their future and survival in the market depend on it.

As a necessary development, the direct conclusion is reached because there are different natures in the information that is generated within a company and its different classes have different levels of relevance for each company and their levels of relationships and access to information.

This information can take the form of innovative scientific developments with its applicability in the market, which by its definition and extent can be catalogued within those developments that national and international standards have recognized and protected under patents.

However, it is also possible that the characteristics of the information do not lead to the possibility of it being patented, but for this reason it must not be concluded that it does not deserve protection, as it is a special form of intangible property.

It should be noted that it is not only the impossibility of patenting the information or development that leads companies not to carry out this procedure, but that the latent and recurring possibility was also recognized by the doctrine as a factual impediment. Thus, even potentially patentable developments are not, in fact, patented, due to the lack of interest of the companies themselves in doing so. This is what happens when the strength of the advantage offered by development extends in a very short time (given the constant mobility and rapid development of the sectors in industries all over the world), and the information to be protected can also be reduced to the application and other developments they can provide.

DOI: 10.6084/m9.figshare.7371080

In short, companies consider that the procedures to obtain the patent are time-consuming, heavy and costly, and also the level of confidentiality of the development and its application allow them to keep it completely isolated from the public, making it unnecessary or too risky to share this information in a traditional patent office (MELGAR, 2005, p.147).

As a consequence of the abovementioned, national legislation – and even international or supranational organizations – has led to the conclusion that such information should be protected. It thus arises as an industrial property right whose protection is not granted from the register, nor even subject to any registration granting exclusivity, as with industrial property rights submitted to registration. In this respect and derived from the nature of the so-called trade secrets, it seems important that a registration or publicity, before protecting, ultimately makes the right of intellectual property evaporate with its disclosure, that is, the disclosure registration is what makes it impossible to protect, and not the other way around, as it would be imagined by the records and ostentation of the patent (SEGADE, 2015, p.129).

From the above, as it will be seen later in this article, we are beginning to reflect on the need for intrinsic protection of such information elements, particularly an element that, although not unique, is of great importance, namely the secret nature of information.

There is a risk of providing data to unscrupulous companies that engage in unfair competition from the access to such information. In fact, the patentable information is secret and the adviser or lawyer who issues the opinion to the company must inform what are the necessary and sufficient measures so that it remains confidential.

Thus, it is first necessary to understand business secrets as intangible assets, separating them from the mere material assets of the company, and then deriving their importance in the protection of competition law, through contractual agreements with wordings that allow the protected flow of this type of intangible assets. In particular, jurisprudence gives us equally important clues to problems that can be stalled in the face of the improvements that can be provided in the drafting of the clauses regulating this right, by minimizing potential violations.

DOI: 10.6084/m9.figshare.7371080

It is therefore the purpose of this article to succinctly present the challenges and opportunities in relation to new technologies being implemented as part of the Fourth Industrial Revolution, and also to discuss the various mechanisms for the protection of trade secrets as part of the intangible assets owned by companies, emphasizing the inexorable link between legal protection and economic and strategic importance for entrepreneurs to define and implement mechanisms to protect their investments and companies more efficiently.

2 TRADE SECRETS: ASSETS TO BE PROTECTEDPROTECTED

A trade secret is a kind of intangible asset. Nevertheless, it should be noted that, given the undeniable Roman tradition of some countries in South America (e.g. Brazil, Argentina, and Colombia), the historical background of property rights goes back to the historical conception of real rights that fall solely on material goods:

> Among the Romans, property existed only in bodily things; the man was aware of the right of domination, which is the power over corporeal things. Through occupation, he acquired mastery, that is, all the powers he could aspire to over things. If through occupation he was the owner, and it could not occur, but over corporeal things, the figure of corporeal things could not be dissociated from the notion of property. Thus, following the Roman doctrine, ownership or dominion is the right over a corporeal thing. (GOMEZ, 2001, p.55).

So, business secrecy, despite having productive, industrial or commercial application, whether in the production of raw material, manufacture of goods or in the provision of services, sometimes, as it is more common, can interact as specific means of production, including information that can be patented, new ways of developing an industry, translating into information of an entrepreneurial nature.

Thus, from a business point of view, a secret is a list of clients or suppliers of a company, production strategies or product formulation, or anything that is not public and influences production, either in quality or in expertise to decrease costs.

Notwithstanding the foregoing, we must be concerned with the nature of the information that makes up the secret. If exceeded, for a detailed description in the

DOI: 10.6084/m9.figshare.7371080

patent application, this may sound as impossible to the protection of the information, even if it is framed in that susceptible conception of being an industrial secret. Therefore, the standard of identifying commercial information that has to be protected by secrecy is one that involves secrecy, value and need for protection, as the doctrine points out:

> a) secrecy in the sense that, as a whole or in the precise configuration and assembly of its components, it is not generally known or easily accessible by those in the circles who normally deal with their information; b) has commercial value because it is secret; and (c) has been the subject of reasonable measures taken by its lawful proprietor to keep it secret. The information of a trade secret may be related to the nature, characteristics or purposes of the products; to production methods or processes; or to the means or forms of distribution or commercialization of products or services. (RODRIGEZ, 2011, pp 207).

This definition is directly related to that contemplated in the multilateral regulations of the World Trade Organization, which also provides for the obligation of member states to protect undisclosed information[1].

Now, with respect to the definition itself, one can then verify that the standard establishes the three requirements mentioned, where conditions are imposed separately for the protection and characterization of information as an industrial secret.

Thus, of course, information must naturally have the character of secrecy, in the sense that this – or the sum of its components – is not widely or easily known to other persons acting in the system. However, it should be noted that when referring to the "precise configuration and assembly of its components", the standard allows us to consider a special combination of potentially known market factors as a secret; that is, even information or public knowledge may be an industrial secret, specifically in the form in which the configuration given to that information is private and secret to the proprietor.

To clarify the previous point, it is convenient to give an example. In terms of customer lists, it is well known that trader A is a regular purchaser of a particular material or because it is part of the inputs that companies of this type acquire it frequently. However, the configuration of the entire list, with several traders, as

[1] Agreement on the aspects of intellectual property rights related to trade (Geneva: WTO, 1995, art. 39).

DOI: 10.6084/m9.figshare.7371080

mentioned, in their buying routines, mechanisms, forms of acquisition, prices, people, contact details and frequency of purchase, among others, may well have been required by the standard in sufficient specificity.

Moreover, information must have commercial value, but this must come from its secret nature. That is, if the information in question does not lose its value by the fact of being disclosed, but, on the contrary, remains unchanged to such a situation, it is not considered an industrial secret. Therefore, the standard does not only require that the information has a value, but that it must be derived from its secret nature.

Finally, as it will be seen more specifically in the treatment received from the point of view of the law for the case of unfair competition, it is necessary that the businessperson holding the information has had reasonable and sufficient reasons to keep it a secret. Therefore, a diligent little trader cannot expose their confidential information to third parties (and even employees) without properly defining confidentiality, accountability or, in general, without setting sufficient parameters to safeguard the protection of the information.

This definition is directly applicable to trades secrets, although this is also mentioned in several regulatory bodies, especially in terms of protection mechanisms, which will be discussed below, based on the regulation of unfair competition, its application and its effects on labour issues, leaving aside the penal regulation also in force, which will not, however, make part of this analysis.

In any case, considering that the concept applicable in Colombia to industrial secrecy is in line with current international trends, it is worth highlighting the definition of trade secrecy given in the most recent European Union directive on the subject:

> For the purposes of this Directive, the following definitions shall apply: 1) "trade secret" means information that meets all of the following requirements: a) is secret in the sense that it is not as a whole or in the precise configuration and assembly of its components, generally known by persons belonging to the circles in which the type of information in question is normally used or easily accessible to them; b) has commercial value due to its secret nature; c) has been subject to reasonable measures, in the circumstances of the case, to keep it secret, taken by the person who legitimately exercises control (OMPI, 2016).

This is the definition of business secrecy. Therefore, business secrecy is secret information, with commercial value and subject to protective measure by its

DOI: 10.6084/m9.figshare.7371080

holder, information that is difficult to access in the environment in which it circulates or is used, unknown to most of the people who have contact with the product, good or service linked to the information.

3 TECHNOLOGICAL INNOVATION, FOURTH INDUSTRIAL REVOLUTION AND CHALLENGES

3.1 INDUSTRY 4.0

Industry 4.0 (I4.0) is a term utilized internationally to refer to the Fourth Industrial Revolution. Despite the popularity and focus given to I4.0, since its conception it has arguably struggled to achieve a clear definition by the myriad of publications in both academic and practitioner domains and has varied massively and accomplished little (Bauernhansl et al., 2014). Therefore, we begin with an overview of a key concept at the core of I4.0, the Internet of Things (IoT).

A simple way to explain the IoT is to use the widespread, well-understood technological concept known as the Internet. The Internet is comprised of a global network of interconnected computer servers, which can be accessed simultaneously by multiple users via a range of endpoint devices (mobile phones, laptops, tablets, PCs, etc.). These connected users access the internet and use the information contained in those servers.

The next step then is to expand the concept of connecting these users and imagine that everyday objects containing embedded sensors capable of communicating information are also connected to networks and to the Internet. Such objects can include mobile phones, wearable devices, washing machines, light bulbs, vehicles, etc. In an industrial setting, these devices include robots, machines, jet engines, etc.

All of these “things” are now “smart” objects which are capable of communicating and exchanging data with the wider network about themselves (e.g., what, where, when, temperature, pressure, acceleration, speed, status, etc.), making this network the Internet of Things.

DOI: 10.6084/m9.figshare.7371080

In the same fashion as the concept of I4.0, there is still no consensual definition for IoT. Nonetheless, one of the most enlightening definitions was presented by the ISOC report (ROSE et al., 2015, p. 12) as:

> Internet of Things" and "IoT" refers broadly to the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers. These "smart objects" require minimal human intervention to generate, exchange, and consume data; they often feature connectivity to remote data collection, analysis, and management capabilities.

Thus, with a basic understanding of IoT, one can relate to the concept of I4.0, which can be characterised as a form of "Industrial Internet of Things" (IIoT) (Leber, 2012). This alludes to the IoT applied in the industrial context, as already mentioned above in the form of connected robots, machines, jet engines, other equipment, etc.

This characterisation is similar to the one made by Kirazli & Hormann (2015, p. 864), which provides the following definition for I4.0: *Industry 4.0 is the systematic development of an intelligent, real-time capable, horizontal and vertical networking of humans, objects and systems.*

Therefore, I4.0 can be characterised as the deployment of IIoT within the boundaries of an individual business, also known as *Vertical Integration*, as well as across the value chain, industry or even cross-industry, also known as *Horizontal Integration* (KAGERMANN et al., 2015, pp. 8-37).

To conclude this section, we note that the deployment of IIoT within individual businesses can undoubtedly lead to operational gains and other benefits such as increased speed, control and overall productivity. It is argued, however, that the deployment of IIoT across value chains and industries, crossing individual business boundaries, will pose particular challenges, especially with regards to the strategic sharing, or not, of data and knowledge. To this end, the next few sections will explore the key implications of IIoT for manufacturing businesses, as well as the need for the businesses to adapt their IP strategies in order to mitigate risks and secure value.

DOI: 10.6084/m9.figshare.7371080

3.2 THE IMPACT ON IP STRATEGIES

According to the World Intellectual Property Organization (WIPO), Intellectual Property (IP) can be characterised as creations of the mind (WIPO, 2011). These include inventions, literary and artistic works, symbols, names, images, and designs used in commerce. IP can be categorised, according to the subject matter it covers, into two main categories: industrial property, which includes inventions, industrial designs, integrated circuit topographies, trademarks, and geographical indications; and copyright, which includes literary, dramatic and artistic works.

This section explores IP protective measures and the difference between formal and informal protection measures. Protecting IP can be understood as a prohibition, which is intended to ensure that no one uses IP in a way that is contrary to the owner's will.

The protective measures can take effect in various forms, from trade secrets to copyright protection, which forbids someone to reprint a book, remix a song, or patent protection, which prevents the use an invention, or trademarks, which protect the use of logos, among many other possibilities. As shown by these examples, the protection of IP can mean quite different things.

4 THE IMPLICATIONS FOR INTELLECTUAL PROPERTY

The Made Smarter Review issued in the second half of 2017 recognises the importance of IP as a key intangible asset, which can make up over 80 percent of the value of a company (Ocean Tomo, 2015) and it is often the key to securing a competitive advantage in globalised value chains.

Furthermore, the review led by Professor Juergen Maier (CEO Siemens UK) also recognised that IP theft is one of the key threats related to the digitalisation of businesses (Made Smarter. Review 2017, 2017). The review also points out that due to the intangible nature of IP, which is typically found in digital information, it is susceptible to digital piracy.

DOI: 10.6084/m9.figshare.7371080

Historically, the focus of IP practitioners has been to use IP rights as the traditional “Shield and Sword” to protect the physical things, devices, structures, or the configuration of physical systems, physical outputs, or the operation of physical systems, physical connections, etc. However, with the implementation of I4.0, the focus needs to be expanded to the IP protection of intangible things, such as methodologies, configuration of virtual systems, data ownership, handling and storage, processing algorithms, brand recognition, etc.

The implementation of I4.0 challenges the current understanding and use of IP protection and commercialisation strategies, justifying the development of new approaches that will be better suited to the rapidly changing, highly integrated business networks.

As a result of the implementation of interconnected communications and the utilization of application programming interfaces (APIs) to more collaborative inter-company models, businesses must carefully consider how to protect their IP, whilst at the same time facilitating the interoperability of connected businesses.

The sub-sections below present a non-exhaustive list of challenges for IP strategy in the face of this new highly collaborative and interoperable environment emanating from I4.0.

4.1 THE INTEGRATED LIFE CYCLE – MODEL BASED DEFINITIONS

In order to achieve the levels of integration across the product life cycle from design to recycling, the I4.0 will require a change in the nature of proprietary files. This will undoubtedly impact manufacturers who will be pushed due to efficiency and market pressures, whether they like it or not, towards migrating to a “Model Based Enterprises” (MBE) where manufacturing businesses will move away from utilising 2D engineering drawings and specifications, to utilising digitalised 3D product drawings and definitions (i.e., Model Based Definitions “MBD”) (Vezzetti et al., 2011). These files can be shared across the supply chain (Hedberg, 2016).

In fact, as highlighted by Hedberg, studies have demonstrated that manufacturing businesses could save millions and reduce their time to market and new product introduction time by almost 75% in average by utilising MBD.

DOI: 10.6084/m9.figshare.7371080

Thus, the MBE digital files, also known as the "digital thread" or "source of truth" as referred to by Siemens (Richer, 2017), will be produced by 3D Computer Aided Design (CAD) software which will contain the specifications for components and final products including dimensions, tolerances and materials, as well as bills of materials and manufacturing information.

It is not difficult to imagine the potential damage caused if such files were to fall into the wrong hands, as this confidential information would enable a rapid copying of the product. As such, the potential loss of valuable IP obviously increases as manufacturing businesses migrate to the integrated life cycle model of I4.0 and begin to utilise the MBD files.

4.2 DIGITAL BUSINESSES AND THE HUMAN CLOUD

Despite the trend towards digitalization of businesses, one part of the organization will remain unchanged, that is the reliance on human beings to setup, coordinate and make decisions regarding critical activities.

Of particular importance in this context is the fact that in the current technological setting, more and more technical work is being done by suppliers, contractors or even the employees themselves, working remotely; this is the so called "human cloud."

This trend is a key factor in the I4.0 labour environment, where programmers, data scientists, IT professionals, statisticians, etc. provide specialized services to hundreds of projects scattered across a virtual cloud. These workers can perform their task from anywhere in the world; and the only thing necessary is to have internet access (O'CONNOR, 2015).

Furthermore, the available literature (AURIGA, 2015) points out that IT employment has the highest turnover of any industry, reaching 20–30% annually and only lasting from one to four years of tenure. Showing an even more concerning picture, a report by Symantec Corp. (2013) presents evidence from a survey showing that nearly 60 percent of software developers based in the United States believe that they have the right to reuse code that they have written in previous assignments for

DOI: 10.6084/m9.figshare.7371080

the purposes of their next employment, and over 40 percent believe that they should have the IP in their inventions.

This challenge was illustrated by the legal case between Formula One teams and a service provider, namely *Force India vs. Malaysia Racing [2012] EWHC 616 (Ch)* and *Force India vs. Aerolab [2013] EWCA Civ 780*.

A key issue raised on paragraph 61 was the need to distinguish between the personal skill and knowledge of the employees of the service provider and the corporate trade secrets of its clients. A concern was expressed that the development contract should not "unduly restrict the ability of Aerolab's employees from making use of their skill and knowledge, even if that skill and knowledge had been enhanced by information that they had acquired in the course of working on the Force India project". This dispute shows the difficulties in defining the scope of protection of trade secrets in an era characterized by employee mobility and by open innovation models.

In conclusion, the confluence of digitalised business and high labour mobility, in combination with the above MBD files and the vertically integrated businesses carrying a vast amount of aggregated expertise and technical information, gives rise to one of the biggest risks to a business IP due to unclear ownership of rights and knowledge spillover as a result of a subsequent competitor employment.

4.3 HORIZONTALLY INTEGRATED BUSINESSES AND THE VALUE OF DATA

In the typical pre-I4.0 environment, IP strategies have focused on protecting hardware and software that process and store data. However, the data itself, especially in the newly interconnected environment, is of high value and worthy of protection. This value emanates from the ability to perform analytics on data from integrated smart objects, generating new knowledge, which can be the source of competitive advantage and innovation. As such, the rights to these data sets, as well as the bigger aggregated data sets and the knowledge and insights emanating from them, are of critical importance to businesses.

Data, in its more simplistic form, is typically protected by trade secrets and copyright law, saved in databases under EU jurisdiction via the "sui generis" protection

vol. 03, nº. 52, Curitiba, 2018. pp. 199-224

DOI: 10.6084/m9.figshare.7371080

scheme provided by the EU Directive 96/9/EC (Directive 96/9/EC, European Parliament and Council, March 11, 1996).

Although the above methods of data protection can be useful in many circumstances, they very often fall short in scope and are considered by many as non-adequate DLA Piper, Rights in Data Handbook (2013). In this case, it is very likely that businesses and IP practitioners will have to resort to contractual agreements in order to govern the operation and the inter-company relations in the I4.0 environment.

Therefore, IP strategies will have to take account of the required contractual agreements surrounding data exchange, particularly addressing the types, rights, and licensing constructs related to I4.0 interconnected data.

5 TECHNOLOGY AND THE INCREASED RELIANCE ON TRADE SECRETS AS A PROTECTION METHOD

In the United States of America, many companies have changed their approach to technology protection due to the U.S. Supreme Court decision in the 2014 case of *Alice Corp. Pty. Ltd. vs. CLS Bank International 573 US _ (2014)*. This case has reduced the patent protection available for software and business methods. As a result, in many cases companies are instead relying on trade secrets as a more guaranteed and lower cost solution when compared to patents in these cases.

In addition, the U.S. Supreme Court decision in the 2017 case of *TC Heartland LLC vs. Kraft Foods Group Brands LLC 137 S. Ct. 1514 (2017)* narrowed the potential options for patent case jurisdiction. As a result of this decision, patent litigants can no longer start a patent case in a place where infringement had occurred, on the contrary, the decision limits that the action be initiated in a jurisdiction where the defendants are incorporated or have a physical place of business. In its turn, it limits the claimant's options to select a suitable jurisdiction or a friendly court for this particular type of case, resulting in further expenses by potentially requiring the enforcement of patents in distant and less suitable jurisdictions.

vol. 03, nº. 52, Curitiba, 2018. pp. 199-224

DOI: 10.6084/m9.figshare.7371080

When combined, the result of these decisions increases the costs and the unpredictability of patent litigation, which makes trade secret protection a more appealing option.

In the U.S. alone, there has been an increase in trade secret litigation cases of 14 percent per year from 2001 to 2012 according to an analysis produced by Willamette Management Associates in 2016. Furthermore, such litigations typically concern the type of newly available and easily transportable technologies related to Industry 4.0. This is shown by recent studies pointing out an increase of 50 percent from 2001 to 2015, on federal and state trade secret litigations related to technical expertise and software.

Furthermore, the success rate for trade secret litigations has also increased, reaching a record of 69 percent of success on cases that have made it to the trials (Law 360, 2017). The dismissal rate is also lower than the average for civil litigation in federal courts at 22 percent compared to the average 27 percent (Lex Machina 2017).

6 THE PROTECTION OF TRADE SECRETS: AN INHERENT DUTY ON THE HOLDER OF SECRETS

Having defined the subject of protection analysis, it is necessary to carry out a specific analysis of existing and developed protection mechanisms to protect these rights.

As mentioned, one of the most important elements for the protection of industrial secrets is the protection against unfair competition. The issue of breaching industrial secrecy, therefore, is a cause of unfair competition, and in different parts of the world, the protection afforded to confidential business information is regulated by unfair competition.

The breach of secrecy consists in the disclosure or exploitation of industrial secrets or any other kind of business secrets that have been legitimately accessed without authorization of the owner, but with a reservation obligation, or illegitimacy, as a result of predestined breach behavior secrets in attitudes that result in disloyalty,

DOI: 10.6084/m9.figshare.7371080

such as accessing secrets through espionage or similar procedures, without prejudice to the sanctions established by other norms (COLOMBIA, 1996).

As it can be seen, disclosing information considered as trade secrets constitutes a true unlawful act in the light of competition law, even if such acts are not done with the intention or effect of maintaining or improving the position of an agent in the competing market. If the wrongdoing doesn't have the potential for harm, then it is not properly measured in the effects, but it is objective: in the case of undue disclosure of business secrets, the civil wrongdoing will already be characterized.

So two objectives are presented in modern legislations: a) to guarantee free and fair economic competition; b) to prohibit acts of unfair competition, for the benefit of all market participants and agreement. This is the wording of the Article 10 of the Paris Convention.

First of all, it should be pointed out that commercial secrecy arises as an inherent right to its owner, inseparable from them by the ability to segregate information, therefore it is independent of registration or any formalities, and is therefore an intangible asset as part of the company in its industrial property, which is not subject to registration.

Secondly, the rule contemplates the possibility that the violation occurs by persons who had legitimate access to information and had a duty to keep it private (as it may happen in the case of company employees or potential business allies who have been delivering this information in order to analyse a future alliance), also regarding the access to third parties, who end up obtaining illegally access to confidential information, the core that makes up the secret (Mendez, 2006, 202).

We are talking about people, in the plural. In the past, the protection of intellectual creativity was much simpler, involving a single employee who held business secrets. Nowadays, the operation of a company involves complex relationships, with the participation of many real actors in the process. Creations subject to secrecy are often improved by using several employees. Something similar happens in the protection of great intellectual works in the literary branch that no longer can be created by a single author – several authors participate (BETTIG, 2018, p.7).

Lastly, it is precisely the obligation of the possessor of information to make sufficient efforts to keep information secret in the case of litigation concerning the

DOI: 10.6084/m9.figshare.7371080

protection of secrecy through unfair competition. However, in the case where the owner does not seek to protect the information under the judgment of business secrecy, then the protective right disappears.

7 RELEVANT CONTENT OF TRADE SECRETS IN THE ACT OF PROTECTION

The content of the acts of registration intended for the protection of business secrecy must be carefully and efficiently measured, otherwise the registration itself may sometimes be misused, inciting unfair competition and thus attracting the risk to the owner of the secret, very often in case of leakage of information by itself, to bear the burden of using disproportionate mechanisms in the purpose of protection. Therefore, the holder of business secrecy has the burden of seeking reasonable and appropriate mechanisms for the protection purpose, depending on the nature, extent and characteristics of the object to be protected, weaving strategies for each specific case, in order to prevent that a third party has an easy access to the information.

In this respect, it is clear that the mere development of information will not be sufficient for protection, and an average duty of prudence and responsibility in the maintenance of such information will also be required. Besides, you cannot protect someone who only makes a meeting or sum of several potentially public information in their individuality. Sneaky information, which deserves protection, has a high degree of originality.

Thus, trade secrets, as a form of intangible assets and subject to protection, may have an indefinite time, reaching a goal of granting permanent protection without time constraints, unlike the case, for example, of the patent (20 or 25 years old), or, in the case of trademarks, where, although the ten-year renewal period may be consecutive and unlimited, they depend on the actual procedure for renewal and, where appropriate, can be cancelled if, for example, they are not used effectively.

None of this is intended in industrial property that relates to trade secrets, since it must have perennial protection. In this line, the law often does not conform to the facts, as the doctrine has already emphasized:

DOI: 10.6084/m9.figshare.7371080

> While IP laws may be written in a formally neutral way, their substantive application can exacerbate economic and societal divisions. Such imbalances can have wider impacts on how society develops and the monetary and social value placed on certain types of creativity and innovation. With its intrinsic link to new technologies and creative expression, IP law is fundamentally linked to the future, human development and progress. (Auchmuty, 2018, p. 150).

That is why the disclosable content of business secrecy in the act, term or contract in which it is precisely intended needs to obtain protection, as well as, on the other hand, needs the perpetuation of such protection; precisely such protective objectives may be stronger and based more on the limitation of information than on another strategy.

8 TRADE SECRETS PROTECTION CHALLENGES

As a corollary of the brief analysis above, it should be recognized that the importance of trade secrets, as a manifestation of intangible assets and whose use is increasingly recurrent in the contemporary commercial world, is extremely difficult, since its secretive nature focuses on mental ingenuity and, the more it is translated into a written object, the more it goes far away from the materialization of its essence. The result is that the vast majority of claims do not condemn the defendant for lack of evidence or lack of evidence of a causal link.

This is due to the intrinsic difficulty of protecting and proving both the existence of the secret with all its characteristics, such as the diligence of its rightful owner to protect it. Why, in the end, was this information obtained by a specific person unequivocally? Does the one who says they own the business secret really own it?

On the characteristics of intangible assets (IA) within which industrial secrets can be located, it is observed that property rights are not clearly defined and, in counterpoint, it is observed in the ownership of physical and financial assets that they have well-defined properties, and this feature facilitates the settlement of disputes in the field of property law or even possessory.

Then, because the property is not well-defined, business secrecy can be transferred to another company, although the investments have been made to train a

DOI: 10.6084/m9.figshare.7371080

certain employee, now holder of that secret, who simply decides to change jobs or retire, to establish their own company.

The problem is that companies have no legal control over intangible assets, especially business secrets that interfere with human capital, unpatented expertise, and commercial or industrial practices.

It is evident that the conception of the difficulties related to the economic and accounting nature of intangible assets in companies, which means what it means for entrepreneurs in the development of their businesses, replies in the legal aspect, as to the desired protection in the delicate balance between investment in research and development, an element of great contemporary importance, and the protection of non-patentable knowledge arising from this, including investment in the training of their own employees.

Therefore, in the unfinished form of determining the protection of trade secrets against unfair competition, it becomes more relevant for entrepreneurs to know and invest, not only in obtaining and creating this important knowledge, but also in sufficient mechanisms to guarantee them the protection of their secrets in the future from the legal and material point of view.

Therefore, to protect such sensitive information, entrepreneurs need to find ways to create such knowledge, minimizing the risk of becoming non-existent after disclosure.

From a legal point of view, it is necessary, first of all, that entrepreneurs clearly identify what is relevant, secret and of economic value in business information, considering that, in many cases, the information may have arisen from years of work, or spontaneously, as part of the company's ongoing growth and effort.

Once the relevant information is clear, measures must be taken, both in electronic locks, software tracking and information use, without prejudice to limiting direct access, as well as establishing internal parameters that provide traceable access, all this to avoid the free flow of information to be protected.

It is not by chance that in Spain, with a focus on the lessons of Silvia Barona Vilar, the following is said:

DOI: 10.6084/m9.figshare.7371080

> The need to preserve those who are illegally affected in their personal progress in their efforts, in their economic development, who may find coverage in the existence of their own industrial secrets or in general business, in addition to the need to favour the very activity of the market, competition, among which is the need to avoid monopolistic situations, static positions due to the consolidation of large ones and the impossibility of admitting small ones in the sector. (Vilar, 2008, p.564).

Thus, in protectionist legal strategies and times of Industry 4.0, it is important to draw up a term or agreement in which employees who need information that involves business secrecy keep it confidential, and confine themselves to the correct exercise of their work. Also, the employer, holder of business secrecy, must identify what information will be provided, in whole or in part, because if it is partial, it may be sufficient for the development of the work, and an important mechanism to protect the right to secrecy of business secrecy.

Finally, in legal terms, this term to be signed with the employee takes the form of a confidentiality agreement, which specifically determines the secret information that will be delivered to the employee, together with mechanisms within that agreement that allow its subsequent execution, in losses and damages at a minimum previously stipulated, without leaving aside the possibility of a penalty clause (fine), which must be as high, to the maximum extent practicable, as to deter the violation of the obligation.

The contractual strategy never comes alone, the administration must also work, prioritizing the hiring of young talents, who wish to grow with the company, so that adequate salaries and benefits can enhance the willingness to protect the company, reducing the occurrence of corruptible practices, inhibiting the alignment of employees with the competition. Note that there has always been a tension between the monopolistic character of intellectual property to better remunerate the employer, interested in the secrecy of the secret of their business. Now, more and more, this thinking starts to migrate to cover the one who was employed with access to privileged information, to be a partner, thinking as an owner as well, in order to achieve a normative goal of improving the flow of information and protection of ideas.

These advanced actions, tending to obtain the adequate protection of the information of the companies with respect to their employees with access to the information of business secrecy, will not ipso facto guarantee a real protection, but will

DOI: 10.6084/m9.figshare.7371080

be based on confidence that will build environment with less worries arising from the possibility that the hard work of the entrepreneur may be frustrated by the unauthorized disclosure of developed knowledge and information that makes up the business secret.

CONCLUSION

The phenomenon of I4.0 will reach businesses of all sizes and across all industries. It will generate rich data, which, when coupled with analytics, will enable more efficient monitoring and controlling of operations leading to increased levels of flexibility and efficiency.

While these new technology offerings and business models have no effect on IP rights themselves, they do affect how IP strategies should be formulated. That is, the basic requirements for the registration and enforcement of IP obviously remain unchanged. However, the practices and strategies for securing and commercialising IP in such an environment are completely different.

A flexible and multi-faceted IP strategy informed by the business strategy and business model must be implemented to ensure control over the business value offering, as well as the brand, technology ownership, reputation and joint technological innovation.

Furthermore, patents will continue to be the dominant form of intellectual property protection in certain industries. Nevertheless, today's legal and technological demands require a higher degree of importance in relation to trade secrets, which will increase in relevance over the next decades.

Finally, companies must be aware of the challenges regarding the management and protection of confidential information. As the number of cases and the size of the damages awarded in recent trade secret litigation indicate, defendants should take trade secret matters seriously.

DOI: 10.6084/m9.figshare.7371080

REFERENCES

AURIGAÇ. **Employee Tenure Becomes Hot Topic for Tech Companies**. 15 June 2015. http://auriga.com/blog/employee-tenure-becomes-hot-topic-for-tech-companies/ (Accessed on 14 May 2018).

ALICE CORP. Pty. Ltd. v. **CLS Bank International** 573 US _ (2014)

AUCHMUTY, Rosemary. **Great Debates in Gender and Law.** New York: Macmillian Publishers, 2018.

BAUERNHANSL, Thomas; TEN HOMPEL, Michael; VOGEL-HEUSER, Birgit (Ed.). **Industrie 4.0 in produktion, automatisierung und logistik:** anwendung, technologien und migration. Wiesbaden: Springer Vieweg, 2014.

BETTIG, Ronald V. **Copyrighting culture:** The political economy of intellectual property. Routledge, 2018.

BOTTHOF, A. (2015) Zukunft der Arbeit im Kontext von Autonomik und Industrie 4.0. In A. Botthof, & E.A. Hartmann (Eds.) **Zukunft der Arbeit in Industrie 4.0** (pp. 3-8). Berlin, Heidelberg: Springer.

BRETTEL, M., FRIEDERICHSEN, N., Keller, M., & Rosenberg, M. (2014) How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. **International Journal of Mechanical, Aerospace, Industrial and Mechatronics Engineering** 8(1): 37-44.

COLOMBIA. *Constitución Política De Colombia*. **Law 256 of 1996 article 16**.

GREENOUGH, Jhon; CAMHI, Jonathan. The Internet of Things. In: **Business Insider (2015)**. Disponível em: http://uk.businessinsider.com/internet-of-things-2015-forecasts-of-the-industrial-iot-connected-home-and-more-2015-10. (Accessed on 3 July 2017)

CITRARO, L. Torres. *La importancia de los activos intangibles en la sociedad del conocimiento.* ***Revista La Propiedad Inmaterial n.° 18 (2014):*** 5-34.

SHAW, Josephine; CREMONA, Marise. **Law of the European Union.** Basingstoke: Macmillan, 1996.

DOI: 10.6084/m9.figshare.7371080

WILKS, John. Rights in Data Handbook 2013. In: **DLA Piper.** (2013) https://www.dlapiper.com/en/uk/insights/publications/2013/01/rights-in-data-handbook-2013/ (Accessed on 5 July 2017).

EMMRICH, V., DÖBELE, M., Bauernhansl, T., Paulus-Rohmer, D., Schatz, A., & Weskamp, M. (2015) **Geschäftsmodell-Innovation durch Industrie 4.0:** Chancen und Risiken für den Maschinen- und Anlagenbau. München, Stuttgart: Dr. Wieselhuber & Partner, Fraunhofer IPA.

SWARB.CO.UK. **Force India Formula One Team** Ltd v. 1 Malaysia Racing Team SDN BHD and others [2012] EWHC 616 (Ch)

SOUTH SQUARE. **Force India Formula One Team** Ltd v. Aerolab SRL and others [2013] EWCA Civ 780

FOROOHAR, R. (2016) The 1 Thing on Everybody's Mind at Davos. **Time.** (20 January 2016). http://time.com/4186599/davos-2016-technology-jobs/. (Accessed on 14 April 2018)

GAITAN, M. G.; PAYAN, C. F. y Velazcp, P. ***El Nuevo Derecho de Marcas:*** *Perspectivas en Colombia, Estados Unidos y la Unión Europea.* Bogotá: Universidad Externado de Colombia, 2016.

GOMEZ, José J. ***Bienes***. Bogotá: *Publicaciones Universidad Externado de Colombia*, 2001.

HEDBERG, T. (2016) Testing the Digital Thread in Support of Model-Based Manufacturing and Inspection. **ASME Journal of Computing and Information Science in Engineering** (Mar. 8, 2016) at p.1.

JONDA, M. (2007) ***Innovation „Geschäftsmodell“:*** *Analyse - und Planungsprozesse der strategischen Unternehmensführung*. Saarbrücken: VDM Müller.

JOVANI, C. Salvador. ***El ámbito de protección de la patente.*** Valencia: Tirant Lo Blanch, 2002.

KAGERMANN, H. (2015) "Change Through Digitization – Value Creation in the Age of Industry 4.0", in: Albach, H., H. Meffert, A. Pinkwart, and R. Reichwald, eds., **Management of Permanent Change, Springer**, New York, 2015, pp. 23-45.

DOI: 10.6084/m9.figshare.7371080

KIRAZLI, A. & HORMANN, R., (2015). **A conceptual approach for identifying Industrie 4.0 application scenarios**. Proceedings of the 2015 Industrial and Systems Engineering Research Conference.

LEBER, J. (2012) General Electric Pitches an Industrial Internet, **MIT Technology Review** [Online] (28 November 2012). https://www.technologyreview.com/s/507831/general-electric-pitches-an-industrial-internet/ (Accessed on 11 June 2017)

LOEBBECKE, C., & PICOT, A. (2015) **Reflections on societal and business model transformation arising from digitization and big data analytics:** A research agenda. The Journal of Strategic Information Systems 24(3): 149-157.

LONDON. Department for Business, Energy & Industrial Strategy. (2017) **Made Smarter.** Review [Online]. https://www.gov.uk/government/publications/made-smarter-review. (Accessed 11 November 2017).

MANYIKA, J. McKinsey Global Institute. **The Internet of Things:** Mapping the value beyond the hype, 2015. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx (Accessed on 22 April 2018).

MELGAR, S. A. B.. ***Contratos modernos empresariales*.** Quito: Ediciones Legales. 2013.

MENDEZ, R. M. **Lecciones de Propiedad Industrial III**. Medellín: DIKÉ, 2006.

MILLIEN, R., Geoge, C. (2016) **Intellectual Property Lawyering in the Fourth Industrial Revolution (the IoT).** https://www.researchgate.net/publication/313504500_ (Accessed on 14 May 2018).

NEW YORK. Why Trade Secret Litigation Is on the Rise. (2017). **Law 360.** [Online]. https://www.law360.com/articles/983195/why-trade-secret-litigation-is-on-the-rise (Accessed 17 November 2017).

OCEAN TOMO. **Annual Study of Intangible Asset Market Value** (March 2015) http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/ (Accessed on 23 March 2018).

O'CONNOR, S. **The Human Cloud:** A New World of Work, [Online] (8 October 2015) https://www.ft.com/content/a4b6e13e-675e-11e5-97d0-1456a776a4f5 (Accessed 21 April 2018)

OMPI. European Union (EU). Di**rective 2016/943 of the European Parliment and Council of 8 June 2016.** (http://www.wipo.int/wipolex/es/details.jsp?id=16435).

RICHTER, K., Walther, J. (2016) **Supply Chain Integration Challenges in Commercial Aerospace -** A Comprehensive Perspective on the Aviation Value Chain, Springer, Hannover.

RODRIGUEZ, C. Payán. *Secreto empresarial, vigencia como mecanismo de protección en la propiedad intelectual.* ***Revista Propiedad Inmaterial***, n.° 15 (2011): 207-224.

ROSE, K.; ELDRIDGE, S.; CHAPIN, L. **The Internet Society (ISOC),** 2015 https://www.internetsociety.org/resources/doc/2015/iot-overview (Accessed on 23 April 2018).

SCHRIKER, Gerhard. ***Derecho de patentes:*** *Observancia en distintos países.* Buenos Aires: Depalma, 2003.

SCHWAB, K. The Fourth Industrial Revolution: What It Means, How to Respond, **World Economic Forum.** (2016) https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/. (Accessed on 13 April 2018)

SEGADE, J. Antonio Gómez*. "Los bienes inmateriales en el Anteproyecto de Ley del Código Mercantil*". **En Estudios sobre el futuro Código Mercantil**: libro homenaje al professor Rafael Illiescas Ortiz, editado por María José Morillas, 129. Getafe, Madrid: Universidad Carlos III de Madrid, 2015.

SYMANTEC CORPORATION (2013) **Intenet Security Threat Report 2013** – Volume 18 [Online] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (Accessed on 7 April 2018)

SANCHIDRIAN, Guido. What's Yours Is Mine: How Employees Are Putting Your Intellectual Property at Risk. In: **Symatec** (2013) https://www.symantec.com/connect/blogs/what-s-yours-mine-how-employees-are-putting-your-intellectual-property-risk (Accessed on 5 May 2018).

DOI: 10.6084/m9.figshare.7371080

SUPREME COURT OF THE UNITED STATES. **TC Heartland LLC v. Kraft Foods Group Brands LLC** 137 S. Ct. 1514 (2017).

UK. **Intellectual Property Office, Eight Great Technologies, The Internet of Things:** A Patent Overview (August 2014) https://www.gov.uk/government/publications/new-eight-great-technologies-internet-of-things. (Accessed on 3 May 2018)

UNIÃO EUROPEIA. **Directive 96/9/EC**, European Parliament and of the Council (March 11, 1996).

VEZZETTI, E.; DESTEFANIS. F.; ALEMANNI, M. (2011). Model-based definition design in the product lifecycle management scenario. In: **International Journal, Advanced Manufacturing Technology,** pp. 1-14. - ISSN 0268-3768

VILAR, Silvia Barona. ***Competencia desleal.*** *Tutela Jurisdiccional – especialmente proceso civil y extrajurisdiccional. Tomo I.* Valencia, España: Tirant Lo Blanch, 2008.

WIPO. **Intellectual Property Report** (2011) The Changing Face of Innovation http://www.wipo.int/publications/en/details.jsp?id=227 (Accessed on 2 June 2017).