

## **Towards a better protection of trade secrets**

**In today's world, knowledge is the key to innovation and success. For companies, the protection of trade secrets has become a major challenge as the unlawful disclosure of information concerning a company is likely to undermine such company's ability to compete in a market where competition has dramatically increased.**

**French law, as it currently stands, only partially protects business information and savoir-faire of companies, despite the high commercial value that such information may have. The expression "trade secrets" is, however, frequently referred to in French legal and regulatory texts (it is mentioned in no less than 150 codified articles!) and by judicial and administrative courts, but it is neither defined nor regulated by a specific legal framework.**

**In the absence of any specific text, trade secrets are currently protected by a series of scattered civil and criminal law provisions (1).**

**EU Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (the "Directive") addresses this issue. It was adopted by the European Parliament and the**

**European Council on June 8, 2016 and must be transposed by Member States into national law by June 9, 2018 (Article 18 of the Directive). The question facing law practitioners is now to identify how the protection of trade secrets will henceforth be ensured (2).**

## **1. Protection of trade secrets under French law**

### **1.1. Under criminal law**

While there is no specific criminal offense addressing the protection of trade secrets, various offenses can be relied upon to afford some form of specific but fragmented protection through several causes of action:

- infringement of a manufacturing secret: Article L811-3 of the French Intellectual Property Code<sup>[1]</sup> that deals with manufacturing secret infringements affords a very limited protection that concerns employees only and that exclusively targets manufacturing secrets (to the exclusion of business information); as such, the company is only protected *a posteriori*, i.e. after the manufacturing secret has been disclosed.
- Economic espionage, addressed in Article 411-6 of the French Criminal Code<sup>[2]</sup>, is punishable if it serves the interests of a foreign power or company and if the fundamental interests of the French Nation are threatened.
- Intrusion and interference in the operation of an automated data processing system<sup>[3]</sup> constitute an offense that has a limited scope of application as it only concerns the data contained in data processing systems, and requires that the intrusion in such systems be established.

The protection of trade secrets can also be achieved through offences under ordinary criminal law, such as, according to the circumstances:

- theft, i.e. the “*fraudulent appropriation of something that belongs to another*” (Article 311-1 of the French Criminal Code), is an offense that is hardly applicable in relation to information because of the intangible nature of information. Some courts refuse to recognize the offense of theft of intangible property wherever a material medium (cd-rom, hard drive, etc.) has not been stolen. However, a change seems to be underway and a few isolated decisions – that are not, however, landmark decisions – start to retain the concept of “theft-reproduction” as opposed to the standard concept of “theft-appropriation”<sup>[4]</sup>.
- Breach of trust<sup>[5]</sup> requires the prior transmission of the misused property. If confidential data have not been transmitted, the offense cannot be established.

### **1.2. Under civil law**

In addition to criminal sanctions, companies that are the victim of a violation of their trade secrets are entitled

to bring civil actions to seek damages.

French courts admit that the unfair acquisition of sensitive information constitutes a civil offense. To cover such information, French courts use the concept of “savoir-faire” which is defined (by French legal writers and courts) as the “*information of a technical, industrial or commercial nature that is identified and substantial, not immediately available to the general public, and transmissible.*” This designation, even though much wider than that of “manufacturing secret” or “professional secret”, remains only a part of the concept of trade secrets.

The abusive exploitation of another’s know-how is most of the time sanctioned through a tort action that takes the form of an unfair competition claim. For such a claim to be admissible, it must be established that the employee/competitor/third-party has committed a breach/fault that has caused a damage to the company which holds the know-how.

Apart from litigation, it should be noted that companies may also guard against infringements of their trade secrets through contractual arrangements which are, however, limited because of the principle of privity of contracts.

As such, despite their economic importance, trade secrets are not *per se* efficiently protected under French law. This gap should be closed by the transposition of the Directive, at least from a civil law perspective. Indeed, while many draft Bills (such as the so-called Carayon bill or Macron Bill) submitted in the past to the French Parliament provided for a protection under both civil and criminal laws, the Directive focuses only on civil aspects.

## **2. The protection of trade secrets under the Directive**

### **2.1. The definition of “trade secrets”**

The “trade secrets” protected under the Directive are defined as the valuable know-how and business information that is undisclosed and intended to remain confidential (Article 2 of the Directive). This definition is directly inspired by Article 39 of the Agreement on Trade Related Intellectual Property Rights (TRIPS) of the World Trade Organization.

To be referred to as a trade secret, information must meet the three following requirements:

- *“it is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
- *it has commercial value because it is secret;*
- *it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.”*

As such, the information does not need to be absolutely secret; it suffices that the information is unknown to

*“persons within the circles that normally deal with the kind of information in question”*. There will probably be difficulties in assessing whether this requirement is met, in particular when it will be necessary to determine who are the persons concerned, to what extent they should be considered as being aware of the relevant information, and how should this be evidenced.

In addition, companies will be able to act efficiently wherever their trade secrets are infringed, provided, however, that they can prove that the information in their possession is valuable and that they anticipate infringements through the implementation of reasonable steps intended to keep such information secret.

The commercial value of the information may be either actual or potential (cf. (14) of the Directive). The secret information should be considered to have a commercial value wherever any infringement thereof is likely to harm the economic, scientific and technical interests of the person lawfully controlling it, and to undermine that person’s strategic positions or ability to compete.

Even though not clearly defined, the *“reasonable steps intended to keep [the company’s information] secret”* appear to include, for examples, the recording of the confidential information, the drafting of confidentiality clauses, the negotiation of non-disclosure agreements, the control of access to information, the encryption of the information, etc. The reasonableness of such steps can, however, remain open to interpretation.

## **2.2. The legality or illegality of the acquisition, use and disclosure of trade secrets**

### **• Lawful acquisition, use and disclosure of trade secrets**

Article 3 of the Directive provides certain instances in which the acquisition, use and disclosure of trade secrets are lawful. Such instances notably arise when the trade secret is obtained by means of an *“independent discovery or creation”* or any other practice which is *“in conformity with honest commercial practices”*.

The acquisition of a trade secret is also lawful when it results from the reverse engineering<sup>[6]</sup> of a product that is lawfully in the possession of the acquirer of the information, provided, however, that this person be free from *“any legally valid duty to limit the acquisition of the trade secret”*.

The acquisition, use or disclosure of a trade secret shall also be considered lawful to the extent that such acquisition, use or disclosure is required or allowed by EU or national law.

### **• Unlawful acquisition, use and disclosure of trade secrets**

Article 4 of the Directive defines the unlawful acquisition, use and disclosure of trade secrets. It should be specified that such unlawful actions are always made without the consent of the trade secret holder. They include the *“unauthorized access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files [...] and any other conduct which, under the circumstances, is considered contrary to honest commercial practices.”*

The use or disclosure of a trade secret shall also be considered unlawful whenever it is carried out by a person having acquired the trade secret unlawfully, i.e. in breach of a confidentiality agreement or contractual duty.

In addition, the acquisition, use or disclosure of a trade secret shall also be considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought to have known that the trade secret had been obtained from another person who was using or disclosing the trade secret unlawfully.

Lastly, *“the production, offering or placing on the market of infringing goods, or the importation, export or storage of infringing goods for those purposes, shall also be considered as an unlawful use of a trade secret wherever the person carrying out such activities knew or [...] ought to have known that the trade secret was used unlawfully”*.

### **2.3. Exceptions to the protection of trade secrets**

The Directive does not infringe freedom of expression and information and does not undermine the possibility to reveal such secret information for reasons of public interest (Articles 1 and 5 of the Directive). Indeed, the right to freedom of information prevails over the protection of trade secrets when it serves to protect public interest or a *“legitimate interest”* recognized by EU or national law.

The voice of journalists and whistleblowers - who strongly opposed to the adoption of the Directive because it would allegedly infringe freedom of expression and information - has thus been heard with the introduction of such exceptions that limit the scope of the afforded protection. Yet, here again, we can expect that the concepts of *“public interest”* and *“legitimate interest”* will likely raise debates and controversies as to their interpretation...

Other exceptions to the protection of trade secret have been introduced, in particular in order to respect as much as possible freedom of labor and *“the mobility of employees”* (Article 1.3 of the Directive).

### **2.4. Judicial actions that can be undertaken in case of infringement of trade secrets**

Prior to June 9, 2018, Member States must make available to *“trade secret holders”* lawfully controlling a trade secret *“measures, procedures and remedies necessary to ensure the availability of civil redress against the unlawful acquisition, use and disclosure of trade secrets”*. These measures must comply with the proportionality principle, and be fair and equitable, effective and dissuasive. They must not be unnecessarily complicated, costly, or time-consuming (Article 6 of the Directive).

- **Provisional and precautionary measures**

The competent judicial authorities of the Member States may, at the request of the trade secret holder, order provisional and precautionary measures, such as:

- the cessation or, as the case may be, the prohibition of the use or disclosure of the trade secret on a provisional basis;

- the prohibition of the production, offering, placing on the market or use of infringing goods, or the importation, export or storage of infringing goods for those purposes ; or
- the seizure or delivery up of the suspected infringing goods, including imported goods, so as to prevent their entry into, or circulation on, the market.

To prevent abuses, Article 11 of the Directive stipulates that the competent judicial authorities of the Member States have the authority to require the plaintiff to provide any piece of evidence that would satisfy themselves with a sufficient degree of certainty that a trade secret exists, that the applicant is the trade secret holder, and that the trade secret has been acquired unlawfully. This Article requires the competent judicial authorities to take into account the specific circumstances of the case, such as the conduct of the defendant, the impact of the unlawful use or disclosure of the trade secret, the value of the trade secret or the interests of third parties.

Member States shall also ensure that the judicial authorities may, as an alternative to the measures referred to above, make the continuation of the alleged unlawful use of a trade secret subject to the lodging of guarantees intended to ensure the compensation of the trade secret holder. On the other hand, disclosure of a trade secret in return for the lodging of guarantees shall not be allowed (Article 10 of the Directive).

- **Injunctions and corrective measures**

In addition to the above-mentioned measures, whenever a judicial decision rendered on the merits of the case finds that there has been unlawful acquisition, use or disclosure of a trade secret, the competent judicial authorities may order the destruction or delivery to the plaintiff of all or part of any document, object, material, substance or electronic file containing or embodying the trade secret.

In addition, the competent judicial authorities may take corrective measures, such as:

- the recall of the infringing goods from the market;
- depriving the infringing goods of their infringing quality;
- the destruction of the infringing goods or their withdrawal.

When ordering the withdrawal of the infringing goods from the market, the competent judicial authorities may order, at the request of the trade secret holder, that the goods be delivered up to him/her or to charitable organizations.

All these measures shall be carried out at the expense of the infringer, unless there are particular reasons for not doing so (Article 12 of the Directive).

- **Damages**

The competent judicial authorities of the Member States may also order the infringer to pay damages (Article 14 of the Directive). When setting the amount of such damages, they must take into account "*all appropriate*

*factors, such as the negative economic consequences, [...] the moral prejudice caused” or they can alternatively “set the damages as a lump sum on the basis of elements such as, at a minimum, the amount of royalties or fees which would have been due had the infringer requested authorization to use the trade secret in question”.*

Pursuant to Article 7.2 of the Directive, whenever it is found that the plaintiff has initiated the legal proceedings abusively or in bad faith, the competent judicial authorities may, at the request of the defendant, order him/her to pay damages.

It should also be noted that Article 8 of the Directive imposes on the Member States the obligation to lay down rules on the statutes of limitations applicable to trade secret related claims and actions, it being specified that such statutes of limitations may not exceed 6 years.

As a matter of fact, these measures do not really sanction the infringer. They are rather aimed at providing compensation to the trade secret holder whose rights have been infringed. The authors of the Directive did not wish to introduce the notion of punitive damages but when transposing the Directive into national law, Member States may, for example, provide for additional criminal sanctions in order to further deter infringements of trade secrets.

## **2.5. Confidentiality of legal proceedings and publication of judicial decisions**

The use of the various means of actions by a trade secret holder whose rights have been infringed must not entail the risk of negative publicity or disclosure of sensitive and confidential information. In order to avoid these risks, Article 9 of the Directive sets a number of rules intended to protect the confidentiality of trade secrets in the course of legal proceedings.

Member States must ensure that any person participating in legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret, or who has access to documents which form part of those legal proceedings, are not permitted to use or disclose any trade secret which the competent judicial authorities have, in response to a duly reasoned application by an interested party, identified as confidential.

The competent judicial authorities of the Member States may, on a duly reasoned application by a party, take specific measures necessary to restrict the access to any document produced by the parties or even to restrict the access to hearings and the corresponding records or transcripts; in that case, a non-confidential version of the judicial decision, in which the passages containing trade secrets have been removed, can be made available.

In addition, pursuant to Article 15 of the Directive, the publication of judicial decision must preserve the confidentiality of the relevant trade secret.

## **2.6. Conclusion**

The Directive harmonizes the protection of trade secrets within the EU by enabling European companies to

protect themselves against the unlawful acquisition, diffusion or use of confidential business information with strategic value. This is a much needed step forward for the European Union where the protection was fragmented and uneven from one Member State to another and, therefore, unlikely to properly protect companies against unlawful practices that undermine their competitiveness.

[1] *"The fact for a director or an employee to disclose or attempt to disclose a manufacturing secret is punished by 2 years' imprisonment and a fine of EUR 30,000."*

[2] *"Supplying or making accessible to a foreign power, to a foreign company or organization or to a company or organization under foreign control, or to their agents, information, processes, articles, documents, computerized data or files, the use, disclosure or collection of which are liable to prejudice the fundamental interests of the nation is punished by fifteen years' imprisonment and a fine of EUR 225,000."*

[3] *"Fraudulently accessing or remaining within all or part of an automated data processing system is punished by two year's imprisonment and a fine of EUR 30,000."* (article 323-1 of the French Criminal Code)

[4] Criminal Chamber of the *Cour de Cassation*, March 4, 2008, n° 07-84.002 ; Criminal Chamber of the *Cour de Cassation*, May 20, 2015, n° 14-81.336

[5] *"Breach of trust is committed when a person, to the prejudice of other persons, misappropriates funds, valuables or any property that were handed over to him and that he accepted subject to the condition of returning, redelivering or using them in a specified way."* (Article 314-1 of the French Criminal Code)

[6] Reverse engineering consists in obtaining the secret information through the disassembly or observation of a product that has been made available to the public.

**Soulier Avocats** is an independent full-service law firm that offers key players in the economic, industrial and financial world comprehensive legal services.

We advise and defend our French and foreign clients on any and all legal and tax issues that may arise in connection with their day-to-day operations, specific transactions and strategic decisions.

Our clients, whatever their size, nationality and business sector, benefit from customized services that are tailored to their specific needs.

For more information, please visit us at [www.soulier-avocats.com](http://www.soulier-avocats.com).

This material has been prepared for informational purposes only and is not intended to be, and should not be construed as, legal advice. The addressee is solely liable for any use of the information contained herein.