European Commission

LATIN AMERICA
IP SME HELPDESK

FACTSHEET

Trade secrets in Brazil

1. What is a trade secret?

Most companies use secrecy to protect their intangibles from competitors. Lists of customers, the secret ingredient of a recipe, the optimum proportion of a mixture or certain techniques implemented by employees are examples of trade secrets.

The Brazilian law does not have a specific definition for trade secrets. The former Brazilian Intellectual Property Law made a generic reference to 'confidential business information' and 'confidential industrial information' while the current Intellectual Property Law broadened the definition of confidential information to include 'confidential knowledge, information or data, usable in industry, commerce or the provision of services'.

Furthermore, the new Data Protection Law, which sets out the rules and guidelines for persons, companies and public entities to observe in the treatment and provision of private or personal data, created the National Data Protection Authority. This body will be responsible of ensuring the proper protection of commercial and industrial secrets, among other functions. The law also makes several references to the need to protect commercial and industrial secrets when treating and handling data.

Therefore, trade secrets may be defined as confidential information used in order to conduct a business (industry, commerce or provision of services). In practice, trade secrets may be technical or commercial.

TECHNICAL	COMMERCIAL
• know-how • unpatented technologies • special manufacturing or business techniques • formulae • tools, etc	• commercial strategy • sales strategy • financial information • supplier lists • customer lists • distributor lists • marketing and advertising strategies • databases • business plans • other relevant know-how

2. How can you protect your trade secret in Brazil?

Although most companies handle secret information, n ot all information can be protected as a trade secret. National regulations demand a number of requirements for the information to be qualified as trade secret and to enable owners to protect it against misappropriation.

The rules governing the protection of trade secrets in Brazil do not differ substantially from those of the EU. These requirements are aimed at preserving the confidential nature of the information and limiting the access to it. They also require documentary evidence to prove that the company had the information in their possession at the time of the misappropriation, disclosure or infringement.

Contrary to EU legislation, Brazilian law does not require the information to have commercial or potential commercial value to be protected as a trade secret.

SCOPE OF PROTECTION

The main disadvantage of a trade secret is that it does not provide the SME with an exclusive right (monopoly) to the secret information. Hence, any person that discovers it legally, e.g. through reverse engineering, will be entitled to use it.

A. What cannot be protected as a trade secret in Brazil?

The Brazilian Intellectual Property Law, and the few precedents on this matter, consider that the following knowledge or information are not protectable as trade secrets:

- those that have fallen into the public domain, or
- those that are either generally known or obvious in a specific field.

B. What steps should I take to keep the information secret?

You should take certain measures to keep the information safe.

a) Confidentiality policy

Having a strategy is a key factor to preserve the safety of your trade secrets. Including a confidentiality clause in contracts (e.g. an annex) and training your employees to treat information as an asset are some examples of essential protection measures.

Creating a confidentiality policy is a very useful tool to articulate the rest of the confidentiality measures, regardless of their nature. A comprehensive confidentiality policy should include, at least, the following:

- Guidelines on identifying confidential information and intangible assets.
- Steps to take:
  - Who should be informed of the existence of confidential information? E.g. any disclosure of confidential information should be reported to the legal department.
  - Who should be able to access the information? E.g. only employees that deal with the confidential information regularly in the course of their duties.
  - What additional measures should be taken? E.g. an NDA should be signed before including any confidential information in a communication with third parties.
  - Can the information be protected as an IPR? E.g. patents.
- Obligations on employees. For example, the information should only be disclosed to others when authorised by senior management; confidential information must not be replicated and stored on insecure devices…
- Liability and penalty clauses in case of breach of confidentiality.
- Term and scope of the confidentiality obligations.

OWN DISCLOSURE

Take into account that, in most cases, the disclosure of confidential information does not take place in complex industrial espionage operations but in informal conversations, internal or external emails or because of negligence.

b) Contractual measures: non-disclosure agreements

Non-disclosure agreements (or NDAs) are very useful to ensure that the information remains confidential in those cases that are not covered by the confidentiality policy, namely, disclosures to third parties such as business partners, researchers, customers, etc.

Prior to drafting your own NDA, you should seek professional advice. In any case, an NDA should include, at least, the following provisions:

- Scope of the confidentiality duty: in most cases, a general mention to the exchange of all information during the transaction or research may suffice. However, sometimes it is advisable to explicitly identify information that may not be considered sensitive at first.
- Restricting the use of the information for a specific purpose. For example, if you use an NDA to protect the information you exchange while negotiating a licence agreement, you might want to impose to the receiving party the obligation to use the information only to evaluate whether or not to enter into the agreement.
- List the information not covered by confidentiality obligations. For example, information that belongs to the public domain at the time of disclosure.
- Measures to take following the termination of the relationship. For example, the obligation to return or destroy prototypes, files or other support with the information, non-competition terms, i.e. a stipulation that the party may not engage in a competing business for a stipulated amount of time.
- Liability and penalties: in the event of infringement.
- Length of the confidentiality obligation: the Brazilian law does not include any specific term for the confidentiality duty.
- Applicable law and jurisdiction: especially if the parties are from different countries.

EXTERNAL STORAGE OF INFORMATION

TIn recent years, companies have shown a tendency to store their information in external servers (such as HostGator or HostEurope), or on cloud computing platforms (such as Dropbox or Google Drive). Before using any of these platforms to share or store your confidential information, make sure that the general terms of the server/platform grant you at least the same degree of protection as your internal standards.

Otherwise:

- sign a contract with the service provider in order to ensure adequate levels of protection, or;
- if this is not possible (which is the case with big providers) make sure that no confidential information is stored in such platforms.

In 2019, the Data Protection Law (LGPD) was signed by the Brazilian Federal Government addressing key aspects for the management and treatment of information, including trade and industrial secrets by data storage services. This law, entered into force in September 2021, shedding light on the obligations and responsibilities of storage service providers, including the obligation to pay damages and the possibility of inverting the burden of proof against these service providers, in some cases for data mistreatment. Specific enforcement provisions (e.g. application of penalties) are still expected to come into force (last tentative date: 1 August 2021).

Thus, it is important to verify if the service provider is up to date regarding the latest legal requirements and, in case of doubt, seek specialised legal counsel.

c) Technical measures

Nowadays, information is stored, shared and used using IT (information technology). Failing to employ the appropriate technical measures may put your confidential information in the wrong hands.

Some examples of technical measures are:

- storage of documents containing the confidential information or trade secrets in a secure server or database;
- restrictions imposed on copies (physical or digital), digitalisation and access to virtual connections;
- creation of different profiles for the employees with different access privileges;
- establishment of an effective security system to handle digital information on the company's intranet (including, for example, software encryption) that limits access to classified information;
- implementation of a system that monitors communications and disclosures.

d) Physical measures

Limiting or restricting access to the confidential information or to the places where the information is stored is still one of the most effective measures to prevent undue disclosures. The most common physical measures are:

- mark documents containing trade secrets with the expressions **'confidential'** and **'do not copy';**
- limit the access of employees to those areas involving confidential information in the normal course of their professional activity;
- restrict the access to areas where confidential information is managed, used or stored, and lock them outside business hours;
- even if it seems obvious, file and store any confidential information that will not be needed.

3. When is it advisable to protect your information as a trade secret?

Maintaining and protecting information or an invention as a trade secret may be an alternative to IPRs:

- when the invention does not comply with the patentability requirements;
- when the time and territorial limitations imposed by the patent system do not compensate the risks that arise from the disclosure of the information to competitors (which is what happens when a patent is published), taking into account that a trade secret exists as long as it remains secret;

In other cases, combining both protections (IPRs and trade secrets) jointly or successively may be the best strategy. For example:

- developments, prototypes and tests of a yet-to-be patented invention will require protection through trade secrets at this phase in order to avoid disclosure;
- in those cases in which the SME has complementary know-how to its IPRs that improves its performance.

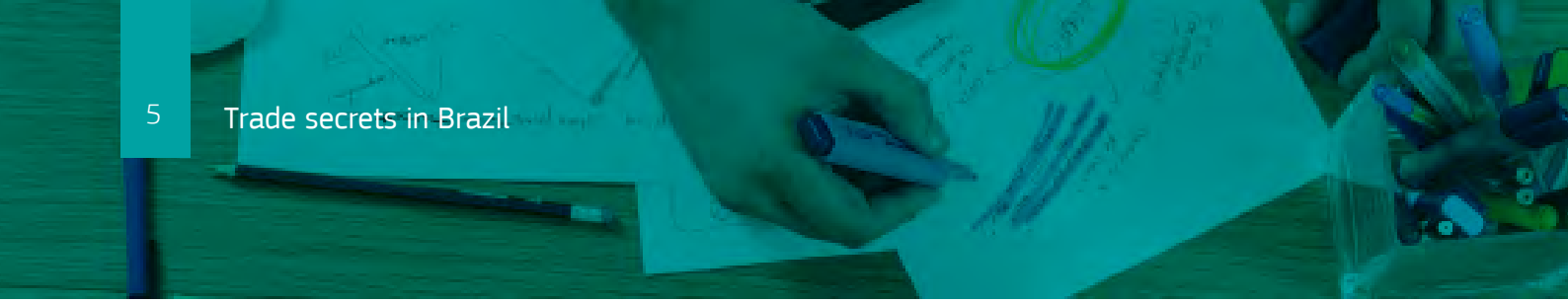
For example, it is a common practice to draft a patent where the quantity of a substance is defined as a range (e.g. between 5 and 10 mg), while protecting the optimum amount (e.g. 7,4 mg) as a trade secret.

For further information on the strategic use of trade secrets, check out our factsheet Trade secrets in a nutshell.

PATENT vs TRADE SECRET in Brazil		
Protection tool	Patent	Trade secret
Duration	20 years from the application date	As long as the information is kept secret
Registration	Mandatory	No
Scope	Exclusive right. Grants a monopoly over the use and exploitation of the invention.	Entitles the owner to take legal action against those who access the information illegally, but not against those who access it legally (e.g. reverse engineering)
Territorial scope	Territorial	Extraterritorial
Requirements	Novelty Inventive step Industrial applicability	Secret information, reasonable measures to protect it
Expenses	€ 49 (official fees) for the application form + € 164 (official fees) as examination fee, up to 10 claims + € 60 for maintenance fees (official fees of annuities increase progressively during the life of the patent)	Secret protection costs (technological protection measures or NDA drafting). The amount depends on the complexity of the measures and the number of people who know about the information

TIPS and WATCH OUTS

According to the latest BPTO's statistics, 70% of the traded technologies in 2017 were non-patentable technologies.



4. What happens if someone steals or discloses my trade secrets?

DISCLOSURE

The disclosure, either by lawful or unlawful means, implies that the information becomes public. Thus, once a third party discloses your confidential information, the information will no longer be protected as a trade secret. However, you are entitled to request civil and criminal remedies, including damages.

A. Criminal remedies

In Brazil, trade secrets are protected by criminal provisions covering unfair competition that establish, in a nutshell, that the unauthorised use, exploitation or disclosure of trade secrets may be subject to criminal actions. Such crimes can be committed by an employee, ex-employee, or a person having, or who has had, a contractual relationship with the owner of the trade secret. Even a third party may be convicted of this crime if they obtained the trade secret committing fraud or through other illicit means.

B. Civil remedies

Sanctions for misappropriation of trade secrets are criminal in nature. However, as a civil tort, the violation of a trade secret entitles you to request an injunction to prevent or suspend the unauthorised use of the confidential information, without prejudice to your right to claim for damages.

- In order to avoid irreparable damages or damages that would be difficult to recover, the judge may grant an injunction to suspend the violation or act before summoning the defendant in return of a monetary caution or fiduciary guarantee, if necessary.
- Loss of profits are determined by the criteria that are most favorable to the injured party:

    I. the benefits of the injured party if the violation had not occurred;

    II. the benefits of the author of the violation of the rights; or

    III. the compensation that the author of the crime would have paid to the owner of the rights for a legally granted licence, allowing them to exploit the subject of the rights.

DAMAGES: What to expect?

Brazilian courts tend to be restrictive regarding the award of potential or theoretical damages. Therefore, it is advisable to provide extensive proof of the actual damages caused and of the eventual loss of profits or revenue.

According to Brazilian case law, moral damages can also be claimed, subject to evidence. However, courts tend to be stricter in granting such claims, especially if the plaintiff is a company, and the plaintiff is usually required to prove that the violation caused damages to the name, reputation or public image of the company.

5. Useful links and additional information

For further information regarding trade secrets in Brazil or any other Latin American country, check out our website:

https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/latin-america-ip-sme-helpdesk_en

General information:

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

http://www.wipo.int/sme/en/ip_business/trade_secrets/patent_trade.htm

http://www.wipo.int/wipo_magazine/en/2013/03/article_0001.html

http://www.wipo.int/sme/en/ip_business/trade_secrets/protection.htm

General information from Brazil (available in Portuguese):

http://www.inpi.gov.br/sobre/arquivos/guia_empresario_iel-senai-e-inpi.pdf/view

http://www.inpi.gov.br/sobre/arquivos/03_cartilhapatentes_21_01_2014_0.pdf/view

www.wipo.int/export/sites/www/sme/en/documents/wipo_magazine_2002.pdf

LATIN AMERICA
IP SME HELPDESK

Trade secrets in Brazil

Download Guide

The **Latin America IP SME Helpdesk** offers **multilingual services** (English, French, German, Spanish and Portuguese[1]), with free information and first-line legal advice on IP related subjects, as well as training, webinars and publications, especially designed for EU SMEs.

HELPLINE First-line advisory service on IP protection and enforcement for EU SMEs working or planning to operate in Latin America.

TRAINING Targeted trainings and webinars on IPR protection and enforcement for EU SMEs (including sector- specific approaches).

IP CONTENT State-of-the-art publications (factsheets, learning modules, videos, IP glossary, info graphics, case studies and newsletters) on the protection and enforcement of IPR in Latin America – specifically addressing IP matters from the SME business needs point of view.

AWARENESS RAISING EVENTS Participation in events attended by EU SMEs to increase the awareness of IP and of the visibility of the services provided by the Helpdesk.

IP ANALYSIS Analysis of IP challenges faced by EU SMEs in the target markets.

IP DIAGNOSTIC TOOLKIT Toolkit for self-evaluation of the IP-status of the user in terms of IP knowledge and management.

IP COST TOOL Online tool that allows the user to pre evaluate the costs related to IP management in every Latin American country covered by the Helpdesk.

[1]The language offer will depend on the specific service and experts' availability.

If you have any queries on how to protect your Intellectual Property in Latinamerica contact our Helpdesk service:

helpline@latinamerica-ipr-helpdesk.eu
+34 96 590 9684
Working Hours: Monday - Friday 9:00 -16:30 (CEST)

If you want more information on additional free services offered by the Helpdesk contact the coordination team:

info@latinamerica-ipr-helpdesk.eu
University of Alicante, Campus San Vicente del Raspeig,
Edificio Torre de Control, 03690 Alicante, Spain
+34 96 590 9684

Follow us on Social Media and stay tuned on new releases of factsheets and other IP content:

@latinamericaipr

https://intellectual-property-helpdesk.ec.europa.eu/

Luxembourg: Publications Office of the European Union, 2022

Print ISBN 978-92-9460-857-4 doi:10.2826/722777 EA-06-21-081-EN-C
PDF ISBN 978-92-9460-856-7 doi:10.2826/838178 EA-06-21-081-EN-N

Publications Office of the European Union

Last update January 2022