<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Purpose of this guide</td>
<td>3</td>
</tr>
<tr>
<td>2. Asia</td>
<td>4</td>
</tr>
<tr>
<td>a. China</td>
<td>6</td>
</tr>
<tr>
<td>b. Japan</td>
<td>13</td>
</tr>
<tr>
<td>3. Europe</td>
<td>18</td>
</tr>
<tr>
<td>a. France</td>
<td>20</td>
</tr>
<tr>
<td>b. Germany</td>
<td>24</td>
</tr>
<tr>
<td>c. Italy</td>
<td>28</td>
</tr>
<tr>
<td>d. Netherlands</td>
<td>33</td>
</tr>
<tr>
<td>e. Russia</td>
<td>38</td>
</tr>
<tr>
<td>f. Spain</td>
<td>42</td>
</tr>
<tr>
<td>g. UK</td>
<td>48</td>
</tr>
<tr>
<td>4. North America</td>
<td>52</td>
</tr>
<tr>
<td>a. United States</td>
<td>54</td>
</tr>
<tr>
<td>b. Mexico</td>
<td>59</td>
</tr>
<tr>
<td>5. Trade Secrets and Confidential Know-how</td>
<td>64</td>
</tr>
</tbody>
</table>
Preface

Businesses are increasingly turning to trade secrets as a mechanism to protect their innovations and know-how. In some cases, trade secrets offer an attractive alternative to patent protection. Companies also recognize the significant strides taken by lawmakers in some regions to strengthen the rights of innovators, from the implementation of the EU Trade Secrets Directive, to IP reform in China with amendments to its Anti-Unfair Competition Law.

However, over recent years, significant threats to trade secrets protection posed by a new generation of connected devices and mobile workforces have presented new challenges for rights holders. Combined with uncertainties created by inconsistent enforcement regimes in different countries, businesses must learn to navigate this diverse and rapidly evolving legal and regulatory landscape.

Looking forward, macro-economic developments and trade negotiations, the most obvious of which have been the trade tensions between the United States and China, suggest that swift legislation and regulatory changes could also be expected for 2020. We will share details of any changes and what they mean for you as they are revealed.

Our guide

We are delighted to introduce the 2020 edition of our guide to trade secrets legislation and legal developments around the world. This edition contains new chapters examining Japan and Mexico, and the latest developments across China, France, Germany, Italy, Netherlands, Russia, Spain, UK, and the United States.

Understanding the law and how it can help you can mitigate potential losses and save vast amounts in legal fees and potential loss of revenue.

We hope you find this guide useful as a reference point.

Steven Levitan
Co-head of Trade Secrets Practice, Partner, Silicon Valley
T +1 650 463 4032
steve.levitan@hoganlovells.com

Dr. Anna-Katharina Friese
Co-head of Trade Secrets Practice, Counsel, Hamburg
T +49 40 419 93 0
anna-katharina.friese@hoganlovells.com
Asia Pacific
The current landscape

China is often seen as "the world's factory". Over the last decade, however, Chinese companies have continued to use and develop more sophisticated technology to produce high tech products, as China's manufacturing industry moves up the value chain. With this emphasis on acquiring and developing high technology, trade secret misappropriation can be a major issue for businesses operating in China.

Trade secrets are protected in China primarily under the Anti-Unfair Competition Law ("AUCL"), the Criminal Law, various provisions under the Contract Law, the Foreign Investment Law ("FIL"), the Labor Law and Labor Contract Law, as well as the corresponding judicial interpretations and implementing regulations. The category of trade secrets that can be protected is broad, and comprises technical know-how, business information and other commercial information. Criminal, civil and administrative sanctions or liabilities can apply against acts of trade secret misappropriation.

What constitutes a trade secret?

The definition of a “trade secret” under the Chinese law is consistent with Article 39.2 of
the Agreement on Trade-Related Aspects of Intellectual Property Rights (“TRIPS Agreement”). Paragraph 3, Article 9 of the AUCL defines a trade secret as “technical, business or other commercial information” possessing the following features:

1. Not known to the public;
2. Having commercial value; and
3. Protected by the rightful holder with corresponding confidentiality measures.

**Evidencing infringement-Burden of Proof**

The trade secret holder bears the burden of proof to identify the “technical, business, or other commercial information” asserted as a trade secret, to show that such information meets the three pre-requisites mentioned above, and to prove the infringer’s acts of misappropriation, which might include:

1. Acquiring the trade secret through unfair means (including both physical and electronic means, e.g. hacking);
2. Disclosing, using, or allowing a third party to use the trade secret so acquired; or
3. Disclosing, using, or allowing a third party to use the trade secret in violation of his or her obligation of confidentiality.
4. Acquiring, disclosing, using or permitting the use by a third party of the trade secret by instigating, inducing or assisting others in breaching confidentiality obligations (e.g. employee trade secret theft 'on assignment').

However, importantly, under the latest version of the AUCL (last amended in April 2019), there are circumstances under which the burden of proof is shifted to the defendant, i.e. the person who allegedly misappropriated the trade secret.

The first situation in which the burden of proof is shifted is where the rights holder of the trade secret provides preliminary evidence demonstrating: (a) its protective measures; and (b) the misappropriation of its trade secret. In that case, the defendant needs to prove that the trade secret asserted does not qualify as a protectable trade secret (see the three requirements for trade secrets mentioned above).

The second situation in which the burden of proof is shifted is where the rights holder of the trade secret provides
preliminary evidence of misappropriation along with any of the following elements:

1. evidence demonstrating that the suspected infringing party had the means or opportunity to acquire the trade secret, and that the suspected infringing party used the information that is essentially identical to the trade secret in question;

2. evidence demonstrating that the trade secret has been disclosed or used by the suspected infringing party, or is at risk of being disclosed or used; or

3. any other evidence demonstrating the misappropriation of the trade secret by the suspected infringing party.

IP right owners should discuss with their counsel how to use the above burden-shifting provisions to alleviate their burden of proof especially in cases where the evidence available to the IP right owners is not straightforward in showing trade secret infringement.

For infringements committed by a third party who did not obtain the trade secret directly from the rights holder, and did not directly instigate or facilitate the misappropriation, the rights holder would additionally also need to prove that the third party has acquired, disclosed, or used such information knowingly or they should have known that it is a misappropriated trade secret.

The evidentiary requirements are also different depending on the type of procedure used by the IP right owners. In civil proceedings, the plaintiff (trade secret holder) has to carry the burden both to establish that the information is a trade secret and to prove infringement. There is no common-law system type of discovery/disclosure in China (although, discovery is available in civil proceedings in Hong Kong), but a Chinese civil court can order the preservation of evidence against the infringer, and may collect evidence from the defendant or a third party. It could also issue a preliminary or interim injunction, provided that the plaintiff shows a high chance of success, urgency and irreparable harm.

In criminal or administrative proceedings on the other hand, the relevant enforcement authority would itself need to investigate the infringement. However,
usually, in order to accept a case and initiate proceedings, such authorities would generally first require the rights holder to provide evidence to establish an eligible trade secret and its ownership, and at least some preliminary evidence to prove existence of misappropriation of the trade secret. In practice, the rights holder is often additionally required to prove that the accused infringement has caused losses.

Civil remedies
A civil court in China may typically provide the following remedies against trade secret misappropriation:

1. A declaration that the defendant’s act has violated the plaintiff’s trade secret, and an order for the defendant to cease such infringement, such as stopping use of the plaintiff’s confidential technical know-how or business information, etc.;

2. Damages and reasonable costs of enforcement. The damages amount should be equal to the amount of the rights holder’s loss caused by the misappropriation, the infringer’s illegal gain if the rights holder’s loss is difficult to quantify, or if there is no evidence to show either of the above, statutory damages up to RMB five million (around US$725,000) to be determined by a court at its discretion, taking into consideration various factors, such as the value of trade secret, the seriousness of the infringing act, the unlawful profits made etc.

Other civil remedies (for example, a public apology) are less likely to apply in trade secret misappropriation cases because the general conditions for such remedies to apply (in the case of public apology, the loss in the rights holder’s personal or business reputation) might not be present.
Criminal law

Criminal penalties are available under the Criminal Law of China, including a fine and/or up to seven years of imprisonment. Article 219 of the Criminal Law provides essentially the same definition of “trade secret” and acts of trade secret misappropriation as the AUCL, but criminal liability applies only if the acts of misappropriation at issue cause a substantial direct loss to the rights holder – currently, the threshold is set at RMB500,000 (around US$80,000).

The threshold amount is not high, but rights holders can face challenges in establishing a criminal case if the misappropriation act has not caused a direct loss (for example, the stolen technical know-how is not put into actual use), and in proving the causation between the alleged misappropriation (for example, a competitor has unfairly acquired and used its trade secret) and its loss (for example, a loss in the rights holder’s sales of the relevant product).

A criminal action is often the most powerful way to collect evidence of infringement, which is frequently a major challenge in trade secret enforcement.

Administrative penalties

If the criminal threshold is not met, other than filing a civil action, the rights holder has another option of filing a complaint to an administrative enforcement authority. The administrative enforcement authority has certain powers to investigate, but it might be less effective compared to police in criminal proceedings, in particular, in aspects such as seizing personal items, searching private or business premises and seizing evidence when the target is not cooperative.

An administrative authority can issue penalties, including an order to cease infringement, confiscation of illicit earnings, and a fine of up to RMB five million (around US$725,000).
Trade secrets and China's new FIL

China's new FIL, which was adopted on 15 March 2019 and became effective on 1 January 2020, also explicitly addresses and protects trade secrets in the context of foreign investment into China.

The new FIL now dedicates two articles to trade secret protection (namely articles 23 and 39). It specifically provides that administrative organs and their employees must maintain the confidentiality of any trade secrets they learn during the performance of their duties.

The FIL moreover provides that sanctions, including potentially criminal sanctions, will be imposed should these organs and their employees unlawfully disclose trade secrets they learn about in the course of performing their duties. These provisions have been adopted in the context of the trade tensions between China and other nations, which are (partially based on) claims of trade secret theft in the process of foreign investment into China.

Confidentiality measures and agreements

When it comes to trade secret leakage or misappropriation, it is of course better to prevent it from happening in the first place than having to deal with a problem afterwards. Rights holders should always consider the following pre-emptive measures:

1. Non-disclosure agreements – but bearing in mind that for some recipients of trade secrets, this may be viewed as just another piece of paper;

2. Be selective about the information to be disclosed to a current or potential customer, business partner, etc., and the way it is disclosed;

3. Confidentiality and non-compete agreements with employees—and to have them reviewed by a lawyer with experience of Chinese labor and contract law to ensure they are effective and enforceable against both the current employees and ex-employees;

4. Use of access control and IT security measures.
Changes that have happened in the past five years and more changes expected in the future?
Looking back over the past five years, very much has changed in China concerning trade secret protection. To highlight some of these, civil courts started to implement preliminary and interim injunctions in trade secret cases, following changes introduced in the amended Chinese Civil Procedural Law. The amended AUCL came into effect on 1 January 2018, further increased the maximum administrative fine from RMB 200,000 (around US$31,000) to RMB 3,000,000 (around US$470,000). The 2018 version AUCL also made it clear that the administrative organs and their employees have obligations to maintain the confidentiality of trade secrets they learn during the performance of their duties. Most recently in 2019, the newly passed FIL addressed and explicitly prohibits trade secret theft during foreign investment into China. The latest amendments to the AUCL have yet again increased the maximum amount of statutory damages and administrative fines, have adopted burden of proof shifting provisions and have expanded and modernized the categories of trade secret theft (e.g. by including theft through electronic means, such as hacking). We will also continue to keep an eye out for more changes, including the long-discussed proposal to enact a comprehensive Trade Secret Protection Law.

Katie Feng
Office Managing Partner, Shanghai
T +86 21 6122 3826
zhen.feng@hoganlovells.com

Grace Guo
Counsel, Beijing
T +86 10 6582 9488
grace.guo@hoganlovells.com

Julia Peng
Senior Lawyer, Fujian Fidelity (Shanghai) Law Firm & Chinese Lawyer Assigned by Fidelity to Hogan Lovells Fidelity
julia.peng@hoganlovellsftz.com
Japan

The current landscape

In Japan, trade secrets are generally protected under the Unfair Competition Prevention Act (Act No. 47 of 1993, as amended, the "UCPA"). The UCPA was amended in 2015 to enhance trade secrets protection further, following several high-profile trade secret leaks and technological developments.

What constitutes a trade secret?

A "trade secret" is any technical or business information useful in commercial activities, such as manufacturing or marketing methods, which is controlled as secret and not publicly known. The relevant information must:

1. be controlled as confidential information ("Requirement 1");
2. have commercial or technical usefulness ("Requirement 2"); and
3. be unknown to the public ("Requirement 3").
Infringements of trade secrets under the UCPA

Where a person obtains a trade secret from an unauthorized disclosing party and subsequently uses or discloses that trade secret without consent, or uses without consent a trade secret disclosed to that person by the trade secret holder, such use or disclosure constitutes an act of unfair competition in contravention of the UCPA. Such prohibition applies in respect of each unauthorized disclosure and use of a trade secret that may take place in an information chain. In other words, the prohibition is not limited to the primary trade secret discloser-recipient pair.

Moreover, the assignment, delivery, display for assignment or delivery, exportation, importation, and provision via telecommunication of goods resulting from trade secret infringement (such goods being "Infringing Products") are also prohibited by the UCPA.

The UCPA catches a person who either has actual knowledge that the relevant goods were Infringing Products at the time he acquired them, or was grossly negligent in not acquiring such knowledge.

The act of trade secret infringement does not need to be successful to be caught by the UCPA. Certain types of failed attempts to use and/or disclose trade secrets without the consent of the trade secret holder would contravene the UCPA.

The reach of the UCPA can extend beyond Japan in certain circumstances. For example, unauthorized receipt of trade secrets from a server located in a foreign country would contravene the UCPA.

Civil remedies

Civil remedies, including the following, are available to a trade secret holder who suffers loss or damage from a trade secret infringement:

1. Injunction;
2. Compensation; and
3. Measures required to recover any loss of commercial credit incurred by the trade secret holder.
Criminal sanctions

The UCPA imposes criminal sanctions against certain trade secret infringements, including up to 10 years of imprisonment and/or a maximum fine of JPY 30 million for individuals and JPY 1 billion for corporations.

In addition, pursuant to the UCPA, the court can confiscate from the infringer revenues arising from the act of illegal disclosure or use of trade secrets.

Since the 2015 UCPA amendment, the prosecutor can bring an action against an alleged trade secret infringer independent of the relevant trade secret holder. Not even an accusation from the relevant trade secret holder is required for the prosecution. In practice, though, the prosecutor would still need the relevant trade secret holder’s cooperation, in order to gather sufficient evidence to prove the alleged act in criminal proceedings.

Evidencing infringement

To evidence trade secret infringement, the information at stake must be a trade secret within the meaning of the UCPA, i.e. such information must satisfy the three Requirements set out above.

The question of whether a piece of information was handled as "confidential information", and hence satisfying one of the "trade secret" criteria under the UCPA (i.e. Requirement 1), is usually heavily disputed in court. Generally, the Japanese court would have regard to factors including: (i) whether the number and/or category of persons who have access to the relevant information is limited; and (ii) whether the person who has access to the information may recognize, objectively, the confidential nature of the information. The above criteria (i) and (ii), however, are not exhaustive. Determination of Requirement 1 depends on the facts of each case. The court will also consider, for instance, the extent to which the relevant information was handled as confidential information, the size of the company and how its internal documents are ordinarily handled.
As for the requirement of the information to be commercially or technologically useful (i.e. Requirement 2), negative information, such as the data of failed experiments, may also satisfy this criterion, as they help the information holder avoid undue trial-and-error experimentations. On the other hand, information regarding illegality, such as methods for the production or procurement of illegal items like unlawful drugs, is not "commercially or technically useful" information in the eyes of the court.

For information to be unknown to the public (Requirement 3), the Japan Patent Office explains that such information refers to a "state of not being publicly known" or "a state where it cannot generally be obtained, except under the trade secret holder's control". Even where information is known to a person other than the trade secret holder, such information can be considered to be under the trade secret holder's control if such a person is under an obligation to keep the information secret.

As can be seen, proving infringement in trade secret infringement lawsuits is often difficult. To ease the burden of proof on claimants, the 2015 UCPA amendment provides a statutory presumption of unlawful use or disclosure of trade secrets if:

1. an alleged infringer obtains the trade secrets knowing or not knowing (in the latter case by gross negligence) the confidential nature of the trade secret;
2. the trade secret consists of a "method for production"; and
3. the alleged infringer manufactures goods resulting from the use of the trade secrets.

In such circumstances, the alleged infringer has the burden of proof to rebut the presumption. Nevertheless, it typically remains very challenging for the trade secret holder to collect evidence in respect of infringement.
In addition, a court may issue an order, upon a party's request, to cause the counterparty to submit currently existing document(s) which is necessary to establish the alleged infringing acts, or to calculate the amount of damages. However, the counterparty is not under a duty to submit the requested document(s) to the court, if the counterparty has a sound reason to refuse the requested submission. In this case, the court may cause the counterparty to disclose the requested document(s) in order to judge whether such document(s) are necessary to (a) establish the alleged infringing acts or to calculate the amount of damages; or (b) prove that the counterparty has a sound reason to refuse the requested submission (the "Conditions"). The court may disclose such document(s) to the parties to the infringement action, their agents, employees, or attorneys, or the court's expert advisors, so that the court may hear their opinions on whether the documents satisfy either of the Conditions.

The statutory limitation period applicable to any request for injunction against certain use of trade secrets is three years from when a trade secret holder becomes aware of:

- an infringing act; and
- a person or a legal entity who commits the infringing act,

if the alleged infringer continues such infringing act.

If the trade secret holder is not aware of the infringing act or the infringer, the trade secret holder's claim for injunction shall expire 20 years after the infringing act.
Europe
On 31 July 2018, France passed legislation implementing the EU Trade Secrets Directive. This implementation goes beyond the harmonization threshold set by the Directive and creates a full statutory basis for trade secrets enforcement in France.

What constitutes a trade secret?
The new law defines a trade secret as any information that meets the following criteria:

- information which is not, in itself or in the exact configuration and assembly of its elements, generally known or easily accessible to persons familiar with this type of information because of their field of activity;
- information which has commercial value, actual or potential, because of its secrecy; and
- information which is subjected by its legitimate holder to reasonable protective measures, taking into account the circumstances, to keep them secret.
This definition does not significantly change the current approach taken by French courts but it clarifies that the information should be kept secret and that economic value is derived from it not being generally known.

In practice, it is up to the trade secrets holders to organize the identification, concealment and transmission of such information, both inside and outside of their organization to ensure that reasonable protective measures (technical and legal) are set.

**What constitutes an unlawful acquisition or use?**

Obtaining trade secrets is unlawful when it is carried out without the consent of its rightful holder and it results from:

- unauthorized access to, appropriation or copying of any document, object, material, substance or digital file which contains the secret or from which it may be deduced;

- access to the secret through any other behaviour considered, given the circumstances, as unfair and contrary to commercial practice.

Trade secrets misappropriation may also be judged to have occurred where, despite a contract or a general duty of care, the unauthorized recipient of trade secrets obtains access by going beyond what was authorized by contract. The use or disclosure of trade secrets is therefore unlawful when it is carried out without the consent of its lawful holder by a person who has obtained unauthorized access to the secrets under the conditions provided by French trade secret law or by a person who acts in violation of an obligation not to disclose the secret or to limit its use.

In addition, the new trade secret law anticipates a situation where one receives, possibly in good faith, previously misappropriated information. Obtaining, using or disclosing a trade secret is considered unlawful if a person knew or should have known that the secret was obtained, used or disclosed unlawfully by the person that they acquired it from.
Permitted disclosure
In a move to protect whistle-blowers, French law allows the acquisition, use, and disclosure of trade secrets by each of:

- judicial and administrative authorities for investigative purposes;
- employees to their representatives as part of the legitimate exercise by those representatives of their functions; and
- journalists within their right to freedom of speech.

How to evidence unlawful acquisition or use?
Trade secret owners can use the general provisions of the French Code of Civil Procedure to try and secure evidence of trade secret infringement either in ex parte or inter partes proceedings. The Code provides that if there is a legitimate reason to preserve or establish evidence, legally permissible preparatory inquiries may be ordered by the court.

Remedies and provisional measures
Unlawful use of trade secrets opens the user or recipient up to civil liability claims. However, French law imposes a specific limitation period for bringing proceedings in trade secret misappropriation cases of five years from the occurrence of the wrongdoing.

A party may request ex parte that provisional or freezing measures be ordered if there is a risk of imminent disclosure or misuse of trade secrets, or to ensure the secrecy of information.

Preliminary measures are available where imminent misappropriation or misuse is expected. Similar permanent measures are available on the merits, allowing the trade secrets holder to:

- prohibit a party from appropriating, using or disclosing trade secrets;
- prohibit a party from manufacturing, offering, placing on the market or using of the products resulting substantially from the breach of trade secrets, or from importing, exporting or storing of such products for these purposes;
– proceed with the destruction of the documents, objects, materials, substances or digital files containing trade secrets, or order their total or partial surrender to the plaintiff; and

– recall from trade channels, or confiscate products derived from trade secret misuse.

**Confidentiality in judicial proceedings**

The new law sets specific guidelines for proceedings dealing with or including a discussion about trade secrets.

Hearings and judgement rendering may take place behind closed doors, at the initiative of the Court or at the request of one or more party.

Decisions may be redacted before being published and circulated to the parties and third parties.

If evidence including trade secrets needs to be filed, a two-step process is set to ensure confidentiality:

– First, the judge will review this exhibit alone or with the parties' litigators, (the judge may also decide to order an expert, under confidentiality undertaking, to conduct a review) to decide if protection measures under this article should be applied.

– If protection measures should be applied, the judge will be able to:
  – limit the communication or redact said exhibit to some of its elements,
  – order the communication or production of said exhibit in a summary format; or
  – restrict access for each of the parties to at most one natural person and one person authorized to assist or represent them.

The Court of Appeal of Paris has already applied this process for having contracts confidentially filed to a recent case.

Stanislas Roux-Vaillard
Partner, Paris
T +33 1 53 67 18 87
stanislas.roux-vaillard@hoganlovells.com
The new GeschGehG

On April 26, 2019, the new "Trade Secrets Protection Act" ("Gesetz zum Schutz von Geschäftsgeheimnissen - (GeschGehG)") came into force in Germany. The act implements the EU Directive 2016/943 (Trade Secrets Directive), which harmonizes the definition of trade secrets as well as the associated claims and procedures, into German law. The GeschGehG is the first statute, whose exclusive purpose lies in the protection of trade secrets in Germany. The previously applicable §§ 17 to 19 of the German Unfair Competition Act have, consequently, been superseded.

New definition of "trade secret"

According to the new definition of § 2 no. 1 GeschGehG, the term "trade secret" means information which meets the following requirements cumulatively: (a) it is, secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question and therefore is of economic value; and (b) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the
information, to keep it a secret; and (c) where a legitimate interest in keeping it confidential persists.

**Uncertainties of the new definition**

The new definition of a trade secret in the GeschGehG is problematic, in particular, with regard to two points: First, it is unclear what is meant by "reasonable steps under the circumstances...to keep [the trade secret] a secret", which was directly implemented from the Directive. The ambiguous wording, especially the use of the term "reasonable", is likely to become a controversial issue in future litigation and, ultimately, the courts will have to establish precedent which, in particular, more closely defines which steps are "reasonable" in their case law. Until settled case law is established, it is advisable to implement strict protective measures in order to ensure the effective protection of trade secrets.

Second, the German legislator has, deviated from the Trade Secrets Directive, by additionally introducing the requirement of a "legitimate interest in confidentiality". The official justification for the act does not provide an elaborate explanation for the introduction of this additional requirement, but it very likely stems from existing German case law before the GeschGehG came into force. Presumably, the legislators in Germany deemed certain interests to be undeserving of protection. It remains to be seen how the case law will develop in this respect.

**Civil law**

Under the new GeschGehG, the owners of trade secrets are entitled to various claims against infringers. They can assert claims for removal and (interim) injunction (§ 6 GeschGehG), destruction, surrender and recall (§ 7 GeschGehG) and for accounting (§ 8 GeschGehG). Furthermore, a trade secret holder may be entitled to claim damages (§ 10 GeschGehG). In general, a theft of trade secrets requires the plaintiff to establish that: (1) a trade secret exists; (2) the applicant is the trade secret holder or a licensee, if applicable; and (3) the trade secret has been acquired unlawfully, is being unlawfully used or disclosed, or where the case of unlawful acquisition, use or disclosure of the trade secret is imminent.
Trade secret claims, however, may also be actionable on the basis of breach of contract, e.g. on the basis of a non-disclosure agreement, a confidentiality clause or a confidentiality duty resulting from a duty of loyalty. Contractual confidentiality obligations remain a powerful tool to protect a trade secret even after the introduction of the GeschGehG.

**What has changed with the GeschGehG?**

The new act implements the Trade Secrets Directive almost seamlessly. This means that the protection of trade secrets in Germany has changed dramatically and, therefore, the enforcement of remedies for infringement of trade secrets in court has been facilitated considerably.

**Reverse engineering**

Under the GeschGehG, reverse engineering is also explicitly allowed. However, the GeschGehG provides the possibility to contractually exclude the admissibility of reverse engineering which, if possible and necessary, the trade secrets holders should make use of.

**(Interim) injunction**

The GeschGehG also provides a catalogue of circumstances which have to be considered to determine the proportionality of the (interim) injunction which is a new concept in German law.

According to German procedural law, it is possible to revoke an (interim) injunction upon the respondent's request if the claimant does not start a main proceeding within a certain time period.

**Confidentiality in court**

In order to ensure that trade secrets, or any other confidential information, remain confidential during and after litigation, German Procedural Law allows the exclusion of the public from the court room. The GeschGehG goes even further, by providing the option to exclude the other party (with the exception of one person from the other party and their attorney) from having access to the confidential information. This is new to German law and, for now, will only apply to trade secret litigation. It will be interesting to see if this new provision
will have an impact on other types of litigation, e.g. patent infringement cases, where such a provision has often been requested, but, as of now, not yet provided by German legislators.

**Penal sanctions**

As a remnant stemming from the old German concept of trade secret protection, the GeschGehG also contains, unlike the Directive, criminal sanctions for unlawful trade secret use.

---

**Christian Stoll**  
Partner, Hamburg  
T +49 40 41993 215  
christian.stoll@hoganlovells.com

**Anna-Katharina Friese**  
Counsel, Hamburg  
T +49 40 41993 173  
anna-katharina.friese@hoganlovells.com
Current landscape

The Italian provisions on trade secrets have been recently amended by Legislative Decree 63/2018, to implement Directive 943/2016 on the protection of undisclosed know-how and business information ("Trade Secrets Directive"). Even before the implementation of the Trade Secrets Directive, Italy provided a strong protection – through specific provisions both under civil and criminal law – to secret business information. The legislator has thus adopted a "minimalist" approach in updating the Italian Intellectual Property Code ("IPC") and the Italian Criminal Code ("ICRC"), as the Italian legal system was already regarded as an advanced model in this area of law, within the EU.

What constitutes a trade secret?

Article 98 IPC specifies the requirements for trade secret protection, while Article 99 IPC sets out the exclusive rights granted to the trade secret holder.

In line with the TRIPs agreements and (now) the Trade Secrets Directive, Article 98 IPC defines "trade secrets" as "business information and technical-industrial experience, including commercial information and experience, subject to the
Trade secret holders are entitled to prevent third parties from abusively acquiring, disclosing or using their trade secrets without consent, except for cases where such information has been achieved autonomously by the third party in question (e.g. by way of reverse engineering).

Legislative Decree 63/2018 introduced three relevant amendments to Article 99 IPC, namely:

a) **Responsibility for unlawful acts of third parties.** When a trade secret is obtained through a third party (e.g. a new employee), the person acquiring, using or disclosing it (e.g. the employer) will act unlawfully if he knows or ought to know that said trade secret was unlawfully used or disclosed in the first place.

b) **Infringing goods.** The production and marketing of infringing goods is *per se* unlawful if the person carrying it (e.g. manufacturer, distributor) knows or ought to know that trade secrets are unlawfully used for those purposes. According to the new provision, infringing goods are those that derive a "*significant benefit*" from the unlawful use of a trade secret.
c) **Limitation period.** The limitation period to bring substantive claims and actions for trade secret violations is now set to five years. The 5-year limitation period also applies to cases of trade secret infringement involving a breach of a confidentiality agreement or similar contractual duties, whereas the general statute of limitation for breach of contract is 10 years.

Legislative Decree 63/2018 did not introduce provisions on lawful uses and exceptions to trade secrets protection further to Articles 3 and 5 of the Directive, although compliance with both is mandatory. The Italian legislator declared that the national case law was already fully aligned with the content of Articles 3 and 5 of the Directive and that there was no need to regulate these cases expressly.

**Protection and enforcement of trade secrets in civil proceedings**

Legislative Decree 63/2018 also introduced a number of new provisions to protect trade secrets in the context of civil proceedings and to ensure that the remedies awarded by the Courts to the rights holder are proportionate.

The Instructing Judge in civil proceedings concerning trade secrets can now impose, upon request of the parties, a confidentiality obligation on any person having access to the case file (including the parties, Court-appointed experts, attorneys of record, Court clerks) against the use or disclosure of secret information. The Judge can also limit access to the hearings (some of which are otherwise public in Italy) and order the redaction of public orders or decisions to preserve confidential information (see Article 121-ter IPC).

Even before the implementation of the Trade Secrets Directive, it was generally recognized that Instructing Judges had ample powers to protect trade secrets, but there were no specific norms in the IPC. These new provisions are deemed to apply not only to proceedings concerning the unlawful acquisition, use and disclosure of trade secrets, but also to all kinds of IP proceedings involving confidential information.

In the course of urgent proceedings, the Judge can also decide – instead of issuing a preliminary injunction – to allow the alleged infringer to continue using the
trade secret against the payment of a security deposit and when there are no risk of further disclosure of the trade secret. In turn, if the preliminary measures obtained by the trade secret holder are later revoked because: (i) he does not initiate ordinary proceedings within the legal time limits; or (ii) in the proceedings on the merits it is ascertained that there was no trade secret worth of protection, the trade secret holder must compensate the damages suffered by the alleged infringer (see Art. 132, 5-bis and 5-quarter, IPC).

Unfair competition

In cases where the requirements set forth by Articles 98 IPC for trade secret protection are not met, the misappropriation, unauthorized use or disclosure of trade secrets may amount to an act of unfair competition under the general clause of Article 2598, No. 3, ICC, which condemns all conducts that are not compliant with professional fairness. Violation of Articles 98-99 IPC and 2598, No. 3, ICC may be claimed cumulatively.

The provisions on unfair competition, however, do not apply to all kinds of information. According to the case law, the information at stake must still:

(i) allow a competitive advantage to the holder; and (ii) it shall not be generally known or easily accessible outside of the company/business.

Moreover, unfair completion rules presuppose that both the infringer and the holder of the confidential information are entrepreneurs and that they are also competitors. However, the Italian case law developed also special liability regime according to which the unfair employee (i.e. a natural person) and the competitor that benefitted of the former's unfair competition conduct are jointly and severally liable if they have acted together (or if it is reasonable to assume so).

Employee's duty of loyalty

In regards to employees, Article 2105 ICC provides that during employment they are subject to a general duty of loyalty to their employer. This includes not disclosing the employer's trade secrets to a competitor. After the end of the employment relationship, the employee is free to use information which has become part of his general skill and knowledge, but he may not use copies of documents or trade secrets in his new job.
Criminal law

The Italian Criminal Code provisions that apply to trade secrets have also been amended by Legislative Decree 63/2018. In particular:

a) Article 623 ICRC now punishes the disclosure or use, for one's own profit or for that of others, of unlawfully acquired trade secrets. The criminal sanctions may be raised of 1/3 if the violation is carried out with the use of computer tools. As most trade secrets violations imply the use of computer tools – which may include also simple hardware and software applications – this provision is likely to apply to numerous cases.

b) Art. 388 ICRC, instead, provides criminal sanctions against the circumvention of a Court order enjoining or otherwise prohibiting the unlawful use of IP rights (not only trade secrets). This also applies to confidentiality orders imposed by the Court in the course of the proceedings.
The Netherlands

Legal basis
The Netherlands has implemented the EU Trade Secrets Directive in the new Trade Secrets Protection Act, as well as changes to procedural law. The Trade Secrets Protection Act protects trade secret holders against misappropriation of their trade secrets. Trade secret misappropriation is a form of tort. Misappropriation of trade secrets can also be addressed under contract law, if the use or disclosure is in violation of a contract.

Trade secret misappropriation can be considered a violation of the employee's duty to act as a good employee. Preferably, the duty to protect trade secrets is laid down specifically in the employment agreement as well as internal policies. The employer may under circumstances terminate the employee's contract with immediate effect if the employee has disclosed a trade secret of the employer without permission.

Trade secret misappropriation is also a criminal offense. The offender can be punished by up to six months jail time or a fine of up to 20,000 euro. In practice though, trade secret misappropriation is mostly dealt with as a civil law matter.
What constitutes a trade secret?
The Trade Secrets Protection Act contains a definition of 'trade secret', which corresponds with the definition of the EU Trade Secrets Directive. This means that it must concern information which meets all of the following requirements:

a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

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

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

What constitutes reasonable steps in the sense of requirement (c) is very case specific. There are examples in case law where the requirement was held not to be met, \textit{inter alia} in situations where certain technical documents were provided to third parties without confidentiality obligations or situations where access to a certain space with technical machinery was not sufficiently restricted. This meant that no trade secret protection was available for that information. It is thus very important for companies to consider what constitutes a trade secret and how to protect such trade secret.

What constitutes misappropriation?
The acquisition of a trade secret without the consent of the trade secret holder is unlawful whenever carried out by unauthorised access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced, or any other conduct which, under the circumstances, is considered contrary to honest commercial practices.

The use or disclosure of a trade secret is unlawful whenever carried out, without the consent of the trade secret holder, by a person who acquired the trade secret unlawfully, acted in breach of a confidentiality agreement or any other duty not to disclose the trade secret, or acted in breach of a contractual or any other duty to limit the use of the trade secret.
The acquisition, use or disclosure of a trade secret is also unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully.

The production, offering or placing on the market of infringing goods, or the importation, export or storage of infringing goods for those purposes, is unlawful if the person carrying out such activities knew, or ought, under the circumstances, to have known that the trade secret was used unlawfully. Infringing goods means goods, the design, characteristics, functioning, production process or marketing of which significantly benefits from trade secrets unlawfully acquired, used or disclosed.

What does not constitute misappropriation?
The acquisition of a trade secret is lawful when the trade secret is obtained by independent discovery or creation, reverse engineering, exercise of the right of workers or workers' representatives to information and consultation, and any other practice which under the circumstances is in conformity with honest commercial practices.

The acquisition, use or disclosure of a trade secret is lawful to the extent that it is required or allowed by Union or national law.

Injunctions and other relief
The trade secret holder, who proves that his trade secret was unlawfully acquired, used or disclosed, can claim a preliminary injunction against the person who unlawfully acquired, used or disclosed a trade secret. The injunction can cover both the (further) use and/or disclosure of the trade secret, as well as an injunction with respect to the further production of and trade in infringing goods. A preliminary injunction can be obtained in about 6-8 weeks.

The trade secret holder can also claim an injunction in proceedings on the merits, as well as damages. Proceedings on the merits generally take about 18 months to 24 months. Proceedings on the merits provide more opportunity for evidence gathering.

The duration of the injunction must be sufficient to eliminate any commercial or economic advantage that the infringer could have derived from the misappropriation.
The Court can also order the destruction of all or part of any document, object, material, substance or electronic file containing or embodying the trade secret or the delivery up of all or part of those; recall of the infringing goods from the market; depriving the infringing goods of their infringing quality; destruction of the infringing goods or, where appropriate, their withdrawal from the market, provided that the withdrawal does not undermine the protection of the trade secret in question (which in practice means the full legal costs or a very substantial part thereof).

The party that loses the proceedings can be ordered to pay the reasonable and equitable legal costs of the proceedings.

**Damages**

The misappropriating party can be ordered to pay damages in proceedings on the merits, provided that it knew or ought to have known that it was engaging in unlawful acquisition, use or disclosure of a trade secret. In appropriate cases, the Court can order a lump sum payment.

**Evidence gathering**

The trade secret holder has the possibility to conduct an evidentiary seizure under the alleged misappropriating party for safeguarding evidence. Permission for the evidentiary seizure is granted *ex parte*, i.e. without the alleged infringer being heard on the request. If permission is granted, a bailiff accompanied by technical and IT experts can enter the premises of the misappropriating party and make copies of relevant physical and digital documents and other types of evidence. The bailiff may also make a detailed description of the infringing goods, the production processes and relevant materials and machinery of the alleged misappropriating party (Supreme Court 28 September 2018, *Organik Kimya v. Dow Chemical*). The seized evidence will be kept in custody by the bailiff. Release of the seized evidence must be claimed in separate proceedings.

The trade secret holder can also claim disclosure of relevant documents, either in the context of proceedings on the merits or in separate proceedings for disclosure. The trade secret holder must show that it concerns specific documents relating to the alleged misappropriation. In order to be successful, the trade secret holder must be able to show a reasonable suspicion of misappropriation. The Supreme Court has held that in disclosure proceedings the trade secret holder does not have to specify its trade secrets in detail, because
at that stage it is not yet clear to what extent the defendant has said trade secrets in its possession and the trade secret holder is entitled to protection of its trade secrets (Supreme Court 28 September 2018, Organik Kimya v. Dow Chemical).

It is established case law that evidence gathering in the Netherlands can be conducted for use of the obtained evidence in foreign proceedings (Supreme Court 8 June 2012, ADIB/ABN). This means that, depending on the specific circumstances, the Netherlands can be a very attractive jurisdiction for evidence collection in international disputes.

**Seizures**

The trade secret holder can file an *ex parte* request for the seizure of suspected infringing goods.

**Confidentiality**

The Court can impose various measures to safeguard confidentiality:

- The Court can order that anyone involved in the proceedings is not permitted to use or disclose any trade secret or alleged trade secret which the Court has identified as confidential;
- The Court can restrict access to certain documents to a limited number of persons, including at least one person from each party as well as the attorneys or other representatives of the parties. Under circumstances, access can be lawyers only; and
  - The Court can restrict access to the hearing to a limited number of persons.
  - The Court can publish a redacted version of the decision.
  - The Court can also appoint an expert to review documents and select (redacted) documents for disclosure (Supreme Court 28 September 2018, Organik Kimya v. Dow Chemical).
Russia

Under Russian law, a trade secret can be defined as information of any type (production-related, technical, scientific research, business, organizational etc.) that has real or potential commercial value by virtue of it being unknown and hidden from third parties.

To be protected as a trade secret, certain measures need to be taken, including:

a) preparing a list of the information considered as a trade secret;

b) adoption of internal regulations within the company on trade secrets protection, handling and control;

c) appointment of persons having access to trade secrets or to whom trade secrets have been transferred;

d) provision of trade secrets to third parties only under non-disclosure agreements and to employees under labor agreements; and

e) implementation of technical measures aimed at protection of trade secrets from unauthorized use and labelling of all material carriers of trade secrets with the respective mark "Confidential".
Implementation of the above measures creates a so-called "regime of trade secret". Unless the regime is not established, a company's trade secret is considered to be unprotected.

Russian Civil Code also provides for a separate regulation for know-how. The owner of the know-how must take reasonable measures to protect the confidentiality of information considered as know-how. These measures may include implementing a trade secret regime, however, this is not a mandatory measure for know-how protection, but is recommended to help prove that certain information is know-how.

Before 1 October 2014 introduction regime of trade secret was a mandatory condition for legal protection of know-how. Therefore, if regime of trade secret was not introduced with respect to the know-how created before 1 October 2014, such know-how would not be protectable. Thus, based on current court practice, legal protection of know-how created before 1 October 2014 remains dependant on introduction regime of trade secret.

**Russian civil law perspective**

Unless an agreement with a disclosure penalty clause is in place, the owner of a trade secret may seek to recover damages from an individual or a company that has illegally disseminated or used the trade secret. In particular, such an agreement may provide for a specific penalty for dissemination of trade secrets in a fixed amount or calculated otherwise.

**Evidence**

As with many other countries, trade secrets litigation in Russia can be very complex. Due to lack of disclosure proceedings, the plaintiff is expected to provide solid evidence of a breach himself. There are very limited legal tools available to the plaintiff seeking the court's assistance in obtaining evidence from the defendant. Collection of evidence requires patience and precise compliance with the requirements of Russian procedural rules.
An owner of a trade secret should demonstrate to the court that the trade secret regime was established for the disputed information. Most recent precedents state that if there is no trade secret regime established by a company (i.e. there is no approved policy, list of information constituting trade secret, etc.), it is not possible to clearly define the information constituting a trade secret regime, and, therefore no liability for breach of a non-disclosure obligation may be imposed. The burden of proof that the trade secret regime was established and subsequently breached rests on the plaintiff. Nevertheless, Russian court practice is developing and in some rulings the courts have confirmed that information constituted a trade secret, even in the absence of a formally established trade secret regime. These successful cases give hope for a breakthrough in streamlining trade secrets litigation in Russia.

Confidentiality

Russian procedural law allows court proceedings to be kept confidential in as far as they relate to a trade secret regime or other information protected by law. An interested party can file a motion and request that the court conducts closed court proceedings. The courts may grant this request if the requesting party can show that the information being disclosed in the court proceedings is confidential (i.e. that a trade secret regime has been established).

Closed court proceedings allow attendance by only the parties to the case, as well as experts, translators and witnesses (if any), and all attendees are obliged not to disseminate confidential information received during such closed court proceedings.
Russian criminal law perspective

Criminal liability of up to seven years of imprisonment – depending on the peculiarities of a case – may be imposed on an individual that illegally collects, shares or uses information protected by a trade secret regime or information that can be constituted as a trade secret.

Russian employment law perspective

Disciplinary liability may be imposed by an employer on an employee who illegally shares information protected by a trade secret regime, which had become known to him/her in the course of work. Dissemination of information protected by a trade secret regime is considered by law as a gross violation of labor obligations and may serve as a ground for the employee's dismissal.
Spain

The current landscape
Spain implemented Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (the Directive) by means of the Ley 1/2009, de 20 de febrero, de Secretos Empresariales entering into force on 13 March 2019 (LSE). Trade secrets were previously protected in Spain by, inter alia, Article 13 of the Unfair Competition Act which is now amended and reverts to the LSE.

What constitutes a trade secret?
The new law provides for the first time a definition of trade secret (and the description of the nature of information which may be a trade secret), in line with the one included in the Directive and in Article 39.2 of the TRIPs Agreement, and building on established Spanish case law. In this sense, a piece of information shall be deemed a trade secret if the following requirements are met:

– The information is secret in the sense that it is not generally known or easily accessible to persons within the circles that normally deal with the kind of information in question (those interested in having it);
The information has commercial value (granting its owner an actual or future competitive advantage) because of its secrecy; and

The information has been subject to reasonable measures under the circumstances, by the person lawfully in control of the information, to keep it secret.

**What constitutes infringement?**

According to the provisions of the LSE (Article 3), the following acts (all independent from each other) are considered unlawful:

- The acquisition of trade secrets, without the consent of the holder, carried out by the unauthorized access to, appropriation of, or copying of any documents or other media containing the trade secret or from which the trade secret can be deduced, or by any other conduct contrary to honest commercial practices.

- The use or disclosure of a trade secret carried out, without the consent of the holder, by anyone who:
  a) has acquired the trade secret unlawfully;
  b) is in breach of a confidentiality agreement or any other duty not to disclose the trade secret; or
  c) is in breach of a contractual or any other duty to limit the use of the trade secret.

The acquisition, use or disclosure of a trade secret is also considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought to know under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully.

The commercialization of infringing goods also constitutes an unlawful use of a trade secret where the person carrying out such activities knew, or ought to know, under the circumstances, to have known that the trade secret was used unlawfully.

...and what doesn't?

On the contrary, the acquisition of a trade secret shall be considered lawful when it is obtained by any of the following means:

- independent discovery or creation;
- observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the person carrying out those activities;
– exercise of the right of workers or workers’ representatives to information and consultation in accordance with European Union and Spanish laws and practices;

– any other practice which, under the circumstances, is in conformity with honest commercial practices.

Moreover, the LSE lists the exceptions to trade secret protection, which were not previously provided for under the Unfair Competition Act. In this sense, any measures or remedies provided for in the LSE shall not apply where the alleged acquisition, use or disclosure of the trade secret was carried out under any of the following circumstances:

– in exercise of the right to freedom of expression and information, including respect for the freedom and pluralism of the media;

– in order to reveal, on behalf of the public interest, any misconduct, wrongdoing or illegal activity directly related to the trade secret;

– when the trade secret is disclosed by workers to their representatives as part of the legitimate exercise by those representatives of their functions, provided that such disclosure was necessary for that exercise; and

– for the purpose of protecting a legitimate interest recognized by European Union or Spanish law. In particular, trade secret protection shall not be invoked to impede the application of any law which requires the disclosure of information to administrative or judicial authorities or which allows public authorities to disclose the information they hold.

**Evidencing infringement**

The trade secret holder must show that the trade secret has been disclosed, exploited or appropriated without his/her authorization. However, the LSE does not require the plaintiff to prove the existence of any subjective element (e.g. intention of the infringer to obtain an advantage from the violation of the trade secret, or to harm the holder thereof) in order to declare that the trade secret has been violated.

Under the LSE, the trade secret holder and the licensee (authorized by the former) have active standing to seek protection of a trade secret. The new law has also extended the means to obtain evidence
necessary to prepare the proceedings on the merits. In addition to the already existing *diligencias de comprobación de hechos* (pre-trial inspection proceedings), provided for under the Patents Act and applied in trade secret cases, the LSE allows the trade secret owner to ask the court for the access to sources of (and means to secure) evidence provided for in some of the provisions of the Civil Procedural Act.

**Injunctions and corrective measures**

Under the LSE, the trade secret holder is entitled to request the court to issue a declaration that the trade secret has been violated and that said violation constitutes an unfair practice. Moreover, the new law provides, *inter alia*, for the following remedies:

a) Cease – and abstain in the future from – violating the trade secret;

b) Prohibition to manufacture, offer, commercialize or use infringing products, as well as the importation, exportation or storage thereof with those aims;

c) Remove the effects, by handing over to the plaintiff all or part of the documents or any other means containing the secret, of the violation of the trade secret;

d) Compensate the plaintiff in cases of willful infringement or negligence;

e) Publish the judgment (partially or in its entirety), at the defendant's expense.

In addition, the trade secret holder is also entitled to request the court to order the seizure of the infringing goods, as well as of the means used to produce them.

Finally, courts are allowed to substitute, at the request of a *bona fide* infringer, the abovementioned remedies for a monetary compensation based on the hypothetical royalties that the latter would have had to pay if he or she had been granted authorization for exploiting the trade secret.

The claims under the LSE are time-barred if they are filed later than three years from the moment when the trade secret holder became aware of the identity of the individual who had carried out the violation of the trade secret.
Criteria for assessing damages
In line with the Directive, the LSE provides a set of clear criteria for assessing damages based on lost profits, the unfair enrichment obtained by the infringer, and moral damages, or, alternatively, a lump sum to be calculated applying a hypothetical royalty. Investigation expenses incurred to obtain reasonable evidence of the violation of the trade secret may also be taken into account to assess damages.

Preliminary injunctions
The trade secret holder is also entitled to obtain interim relief subject to the general requirements (that he or she can show likelihood of success of the complaint and irreparable harm or urgency). Some specific rules apply under the LSE: in order to grant or reject the application, the court shall examine the specific circumstances of the case and the proportionality of the measures, taking into account the value and other features of the trade secret, the measures taken to protect it, the conduct of the respondent in acquiring, using or disclosing the trade secret, the impact of the unlawful use or disclosure of the trade secret, the legitimate interests of the parties and the impact which the granting or rejection of the measures could have on the parties, the legitimate interests of third parties, the public interest and the safeguard of fundamental rights.

Preliminary injunctions are generally applied for with the complaint on the merits and handled by the same court although independently. Exceptionally, they may be applied for before the complaint on the merits if the plaintiff shows reasons of urgency or necessity. Interim injunctions may also be ordered ex-parte if the plaintiff provides sufficient evidence of a "qualified" urgency, or justifies that the hearing might have a negative impact on the effectiveness of the preliminary injunction.

Criminal law
The Spanish Criminal Code sets out the circumstances in which the disclosure of trade secrets would be considered a criminal offence:

- disclosure by any person subject to a legal or contractual obligation to maintain confidentiality; or
- the seizure of data (e.g., written or electronic documents, computer media) through any means in order to disclose a trade secret; or
– the disclosure or assignment of trade secrets by a third party not participating in its discovery but acknowledging its illegal origin.

Confidentiality
The LSE includes trade secret-tailored procedural safeguards aimed at avoiding the disclosure of trade secrets in civil proceedings. In particular, the use or disclosure or any information which can constitute a trade secret and which has been declared confidential by the court, by any person who takes part in judicial proceedings regarding the violation of a trade secret or who has access to the documents of said proceedings, is prohibited, even after the conclusion of the proceedings.

Moreover, courts may also establish any measures deemed necessary to preserve the confidentiality of any information which might constitute a trade secret and which has been submitted in the context of the proceedings, or of any other kind for which said information is necessary to issue a decision on the merits. The measures may include, among others which are adequate and proportionate, restrictions to access to documents and hearings, as well as the possibility of publishing a non-confidential version of the judgment.

Specialized courts
In the context of the enactment of the LSE, the Spanish General Council of the Judiciary is currently working on a new pilot project in connection with trade secrets and the LSE to create the new Trade Secret Protection Courts. These courts, which are expected to be based in Barcelona, will specialize in trade secret matters and may even have EU wide competence.

Within this pilot project, the Competition Section of the Commercial Courts of Barcelona has recently adopted the new "Protocol for Trade Secret Protection in the Commercial Courts" ("Protocolo de Protección del Secreto Empresarial en los Juzgados Mercantiles"), which aims at unifying procedural practices regarding the treatment of trade secrets or confidential information in the Commercial Courts of Barcelona.

Ana Castedo
Partner, Madrid
T +34 91 349 82 61
ana.castedo@hoganlovells.com
UK

Legal basis
Prior to June 2018, trade secrets in the UK were protected by the law of confidence. This is based on principles of common (case) law and equity and has been developed over more than 150 years. Since June 2018, trade secrets along with other types of confidential information (such as personal/private information and state secrets) continue to be protected by actions for breach of confidence, but with trade secrets now having protections, remedies, and procedural mechanisms safeguarded by statute as a result of the UK’s implementation of the Trade Secrets Directive.

How has the UK implemented the Trade Secrets Directive?
Substantial and effective protection for trade secrets existed in law already, so the Trade Secrets (Enforcement, etc.) Regulations 2018 (SI 2018 No. 597) did not transpose the Directive in its entirety. The Regulations addressed areas of existing UK law where there were gaps, or where it was necessary to ensure harmonization of the Directive's implementation across the UK's jurisdictions (England and Wales, Scotland, and Northern Ireland).

The 2018 Regulations introduced statutory definitions of "infringer", "infringing goods", "trade secret holder" (each precisely in line with
the Directive), and most importantly, of a "trade secret" This is information which:

- is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

- it has commercial value because it is secret; and

- it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

An "infringer" is a person who has acquired, used or disclosed a trade secret unlawfully, which is determined according to the existing law of confidence.

**Infringement**

Key Regulation 3 states that: "The acquisition, use or disclosure of a trade secret is unlawful where the acquisition, use or disclosure constitutes a breach of confidence in confidential information."

In summary, to succeed in a breach of confidence action (and thus under the 2018 Trade Secret Regulations), the claimant has to show that: (a) the relevant information has the necessary quality of confidence in the sense of not being generally known and not being of a trivial nature; (b) the information was disclosed to the defendant in circumstances of confidence; and (c) the defendant has used or disclosed the information without permission or has threatened to do so.

Except in rare cases, requirement (a) will be fulfilled if the information concerned is already within the Directive definition of a trade secret. In fringe cases, a defendant may be able to escape liability under the 2018 Regulations/Directive by showing that reasonable steps had not been taken by the claimant to keep the information secret, but could still remain liable for breach of confidence. Whether this happens in practice remains to be seen. By the beginning of 2020, no reported case in England and Wales has been determined specifically by reference to the 2018 Trade Secret Regulations, despite frequent actions and judgments for breach of confidence.

**Remedies**

The 2018 Regulations have put on a statutory footing the three primary remedies already available in a claim for trade secret infringement in the UK: (a) preliminary and/or final injunction to prevent further misuse or disclosure; (b) compensatory damages; and (c) an
account of profits. The plaintiff usually has to choose either damages or an account of the infringer’s profits and cannot receive both. An injunction is usually available in addition to the award of damages/an account of profits. However, the grant of an injunction is discretionary and in some cases the court may decide that an injunction is inappropriate.

The interim prohibition of dealings (such as marketing, import and export), seizure and delivery up of infringing goods mandated by the Directive, as well as its permitted final prohibitions, corrective measures (such as market recall and destruction) and destruction remedies, were all available to the courts in trade secret cases already. These are also now expressed in statutory terms. So too are the sets of factors required by the Directive to be considered by the court when considering an application for interim and final remedies.

**Search orders**

English law already goes further than the Directive by including useful measures for the preservation of evidence by means of the search order which are not included in the Directive. Obtaining evidence of trade secret misuse is one of the main hurdles a plaintiff has to overcome in order to enforce his rights and prevent further misuse. It is possible under English law to obtain an *ex parte* court order permitting the plaintiff’s legal representatives to enter the defendant’s premises without notice in order to search for and seize materials containing misappropriated trade secrets. The process is supervised by an independent lawyer who reports directly to the court. It is also possible to obtain an order requiring a person to disclose the whereabouts of such materials. The person subject to such an order may be the wrongdoer himself but can also be an innocent individual who has the necessary information.

These types of order are useful means of obtaining evidence of misuse but, in the case of search orders are only ordered by the court where there is a strong *prima facie* case. As a result, if granted and executed (and not overturned at the first *inter partes* hearing), a search order frequently results in rapid resolution of the action between the parties without the need for a trial.

**Timing**

In very urgent cases, interim injunctions (including search orders) can be obtained within a few hours, but more typically within a matter of days of the misuse or threatened disclosure coming to light. Substantive proceedings on the merits, which are typically decided by specialist IP judges in the High Court, usually take
between one and two years, including fully reasoned judgments.

**Criminal law**

There is no criminal liability as such for the misuse of trade secrets in the UK. However, if documents containing the trade secret are physically removed then this may amount to theft and if a computer system has been accessed or used without authorization in order to obtain the information, criminal liability may attach under the Computer Misuse Act. If no physical material is removed, then the copying of secret information is not a criminal offence under English law although views have been expressed to the contrary.

**Confidentiality of proceedings**

In order to achieve effective protection of trade secrets across the EU, one of the most important provisions of the Directive was the introduction of procedural measures to ensure the confidentiality of court proceedings. The use of confidentiality clubs and private hearings were already common practice in English trade secret cases. So too, the publication of redacted versions of the court’s decision and pleadings so that the trade secret is not disclosed through public access to judgments and court records. The 2018 Regulations have now put these measures on a statutory footing.

**Employees**

The Trade Secrets Directive did not seek to regulate post-employment arrangements concerning trade secrets (which, in the UK, frequently give rise to proceedings). So, since June 2018, the position remains as it was before. Whilst employed, an individual has a duty of good faith to his employer and will be bound to keep all confidential information secret. After employment ends the court will usually only offer protection to high-grade confidential information ("real trade secrets") and not day-to-day information which forms part of the employee’s general skill and knowledge. It may be possible to protect lower grade information after employment by imposing a suitable post-employment contractual restriction (known as a restrictive covenant).

**Effect of Brexit**

Subject to any change of policy by the Government, the changes introduced by the 2018 Trade Secrets Regulations will remain in force in the UK even though the UK has now left the EU.
North America
General concepts

What is a Trade Secret?

All forms and types of financial, business, scientific, technical, economic, or engineering information . . . tangible or intangible . . . if

– the owner thereof has taken reasonable measures to keep such information secret; and

– the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information. (18 U.S.C. §1839)

Key elements: (1) information that is secret; and (2) has been consistently subject to reasonable measures to protect its secrecy; and (3) derives independent economic value from not being publicly known and/or readily ascertainable through proper means.

What constitutes “misappropriation” of trade secrets?

The statutory definition for “misappropriation” of trade secrets (18 U.S.C. §1839):

– The acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
Disclosure or use of a trade secret of another without express or implied consent by a person who:

- Used improper means to acquire knowledge of the trade secret; or

- At the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was:
  
  - Derived from or through a person who had used improper means to acquire it;

  - Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

  - Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

  - Before a material change of his or her position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

**What is meant by "improper means"?**

"Improper Means" includes:

- Theft

- Bribery

- Misrepresentation

- Breach or inducement of a breach of a duty to maintain secrecy

- Espionage through electronic or other means

"Improper Means" is NOT:

- Reverse engineering,

- Independent derivation, or;

- Any other lawful means of acquisition.

Independent development is a common defense to misappropriation claims.
Possible Forums for Litigation

The “misappropriation” of trade secrets may give rise to a civil (or criminal) claim under both federal and state laws. This dual system means there is no federal pre-emption.

– Federal district court
– U.S. state court
– The U.S. International Trade Commission (“ITC”) (in cases involving imported goods)

U.S. State Civil Law Claims

Historically, laws protecting trade secrets were predominantly state laws. Thus, most pre-2016 U.S. trade secret precedent involved application of state laws.

49 of the 50 U.S. states and the District of Columbia have adopted some version of the Uniform Trade Secrets Act (“UTSA”) as their trade secrets law.

There are, however, variations in the language of particular state UTSA statutes, and differences in the interpretation and application of those statutes among the states.

Note that some states may afford whistleblower protection to employees who use trade secrets to report violations of the law or in the context of employment litigation. New Jersey is an example.

U.S. Federal Civil Law claims

The Defend Trade Secrets Act (“DTSA”), 18 U.S.C. §1831 et seq., enacted in 2016, creates a federal civil cause of action for trade secret misappropriation claims:

– Effective for misappropriation occurring on or after May 11, 2016.
– The act provides for greater uniformity across state lines in trade secret definitions and misappropriation standards, as well as national service of process and execution of judgments.
– Among the DTSA’s more notable provisions are:
  – the availability of ex parte seizure orders in “extraordinary circumstances”, both to preserve evidence and as a remedy; and
  – whistleblower protection for employees and contractors
– Interstate or foreign commerce requirement for standing.
– Applies to conduct outside the U.S. if:
  (1) offender is U.S. citizen or company; or (2) an act in furtherance of the offense committed in the U.S.
– Remedies include injunctive relief; monetary damages for actual loss and any unjust enrichment or alternatively a reasonable royalty; enhanced damages of up to two times the amount of monetary damages; and attorneys’ fees, where the misappropriation was willful and malicious, or if the claim of misappropriation was made in bad faith.

– The DTSA does not preempt state law claims; if properly in federal court, plaintiff can pursue both DTSA and parallel state law claims.

U.S. International Trade Commission claims

In 2011, the Federal Circuit held that the ITC’s jurisdiction includes trade secrets misappropriation cases where: (1) the alleged misappropriation took place outside of the U.S.; and (2) the products embodying the allegedly misappropriated trade secrets were unfairly imported into the U.S.

The ITC is to apply “federal common law” standards for trade secret misappropriation (TianRui Grp. Co. v. Int’l Trade Comm’n, 661 F.3d 1322 (Fed. Cir. 2011)). ITC remedies are limited to Exclusion and Cease and Desists orders – the ITC does not award damages.

New Developments

– The US-Mexico-Canada Agreement (“USMCA”) recites that "each Party shall ensure that persons have the legal means to prevent trade secrets lawfully in their control from being disclosed to, acquired by, or used by others (including state-owned enterprises) without their consent in a manner contrary to honest commercial practices." The USMCA provides requirements that each country make available civil and criminal penalties for entities that violate the provisions. The USMCA further contains prohibitions against limiting the term of protection for trade secrets or impeding licensing or transfer of trade secrets, and judicial procedures to prevent disclosure of trade secrets during litigation.
The U.S.-China Phase 1 trade deal has provisions aimed at protection for trade secrets and effective enforcement against misappropriation. Although the agreement’s requirements are bilateral, they mainly consist of commitments by China to take certain steps to enhance its trade secret protection laws to match existing U.S. laws, including enumerating acts of misappropriation to include electronic intrusions, breach of duties not to disclose information that is secret, and unauthorized disclosure or use that occurs after acquisition of a trade secret. The agreement also requires that China authorize preliminary injunctions, criminal procedures and penalties, and burden-shifting in civil proceedings so that “the burden of production of evidence or burden of proof ... shifts to the accused party ... where the holder of a trade secret has produced prima facie evidence ... of a reasonable indication of trade secret misappropriation ....”

There is a “Workplace Mobility Act” presently before Congress (Senate Bill 2614), which, if enacted, would limit the ability of companies to enter into and/or enforce non-compete agreements with their employees. The Bill, however, expressly states that nothing within it precludes employers from entering into agreements with their employees to not share information regarding the employer or the employment that is a trade secret.

Steven Levitan
Co-head of Trade Secrets Practice, Partner, Silicon Valley
T +1 650 463 4032
steve.levitan@hoganlovells.com
Mexico

The current landscape
Trade secrets are protected in Mexico under the Industrial Property Law (“IPL”) as well as under Criminal Law. Trade secrets can constitute technical know-how, business information and mathematical algorithms. Misappropriations of trade secrets can be sanctioned in Mexico by criminal means, ranging from community services to financial fines up to suspension of profession and imprisonment. Damages can be requested in civil proceedings but only after a misappropriation has been assessed by the criminal authorities.

What constitutes a trade secret?
A trade secret can be any industrial or commercial information kept by an individual or entity which is confidential by nature, has a competitive or economic advantage, and where the owner has adopted sufficient means to preserve its confidentiality and restricted access.

Not considered as trade secret is information that:

1. is already in the public domain;
2. is obvious to a person skilled in the art due to information available in the market; or
3. was disclosed by virtue of a legal provision or court order.
As an exception to information not considered as a trade secret, the IPL provides that information disclosed to authorities shall not be considered as entering the public domain or being disclosed by virtue of a legal provision, where said information is provided for the purpose of obtaining licenses, permits, authorizations, registrations or any other official document.

**Enforcement of trade secrets**

The trade secret holder bears the burden of proof to evidence that the involved information qualifies as trade secret and has been misappropriated. Enforcing a trade secret in Mexico requires that the following facts can be evidenced:

1. The information was always kept confidential;
2. The information provides a competitive or economic advantage over third parties;
3. The trade secret holder applied sufficient means or systems to preserve its confidentiality, including access control;
4. The information is related to the nature, characteristics or purposes of products, to production methods or processes, or to ways or means of distributing or marketing products or rendering services;
5. Third parties in contact with the information were informed about its confidentiality;
6. Disclosure, misappropriation or unauthorized use of the confidential information.

**Criminal remedies**

According to the IPL, the disclosure, misappropriation or unauthorized use of trade secrets can be sanctioned with the following criminal measures:

1. Imprisonment ranging from two to six years;
2. Fines in the range from approximately $422 to $42,245 USD (depending on the annual amount and rate of the Mexican measuring unit for legal fines).
In addition, the Federal Criminal Code set forth provisions for the protection of confidential information. The offenses stipulated under the Mexican Criminal Code are:

1. Disclosing of reserved information known or received by means of employment, title or position to the detriment of a third party, without consent from the trade secret holder. This conduct will be punished with thirty to two hundred days of community service.

2. If the person disclosing the reserved information is a provider of professional or technical services or a public official or when the disclosed or published secret is considered as industrial, the penalty consists in imprisonment from one to five years and fines from fifty to five hundred Mexican Pesos (approximately $2.5 to $25 USD) as well as a possible suspension of profession from two months to one year.

The penalties are increased if the confidential information is used for the infringer’s own benefit or for third parties’ benefits.

Moreover, trade secret holder can request search warrants in criminal proceedings. During the enforcement of the search warrant the public prosecutor can, if there is sufficient cause, order the detention of any good connected to the unauthorized use of trade secrets.

**Civil Remedies**

After a trade secret infringement has been confirmed by the criminal authorities, trade secret holder can seek damages resulting from the infringement through separate civil proceedings.

**Being pro-active**

Trade secrets can be part of one of the most valuable assets of a company. The second the confidential information has been disclosed, the main damage to the business has already been done. It is, therefore, of paramount importance taking adequate measures to prevent the disclosure of trade secrets.
Trade secret holder in Mexico should always take pro-active steps for the protection of their trade secrets, which can include the following measures:

1. Effective Employment Contracts with confidentiality clauses – under Mexican Law it is essential for trade secret enforcement that the disclosing party was aware of the confidential nature of the trade secret, which is why confidentiality clauses should be signed by any person in contact with sensitive company information;

2. Non-Disclosure Agreements – Before entering into any third party negotiation involving sensitive information non-disclosure agreements should be concluded;

3. Trade Secret Protection Policy – It is advisable to have a written declaration and training session to help employees understand what is protected under the company’s trade secrets and what the consequences are in case those will be misappropriated;

4. Warning Notice – Third parties visiting any of your company’s premises should receive a notice informing about your trade secret protection policies. Moreover, all confidential information should be clearly marked as such and indicate ownership;

5. Access control and IT security measures are indispensable.

Bernardo Herrerías Franco
Partner, Mexico City
T +52 55 5091 0163
bernardo.herrerias@hoganlovells.com

Valentina Schmid
Senior Associate, Mexico City
T +52 55 5091 0044
valentina.schmid@hoganlovells.com
To-do List For Trade Secret Protection

A quick reference guide for you to consider when assessing your level of trade secret protection.

(1) Trade Secret Audit
- Review of existing trade secrets of the company
- Review of current agreements and policies
- Review of existing protection measures

(2) Setting up protection system for the trade secrets
- Set up physical security measures
- Improve IT security
- Draft guidelines and provide information
- Review and amendment of all necessary contracts, especially NDAs and employment contracts
- Educate employees
- Ensure proper documentation

(3) Ensure compliance with protection system
- Regular review of protection system and amendments where necessary
- Ongoing education of old and new employees
- Review of "departing procedure" and "arrival procedure" of employees
Trade secrets and other confidential know-how are the lifeblood of every business and protecting such valuable information is no simple matter. Our experienced, technology-focused trade secrets practice can help develop strategies to prevent misuse and will defend quickly against claims of trade secret misappropriation.

Our global trade secrets team has a wealth of experience helping the most innovative companies protect their proprietary information. We help clients implement procedures to identify commercially important proprietary information and take proper care when licensing or selling a trade secret, just as with other forms of intellectual property. To help protect this information, we can help to draft NDAs to use with other companies and employee agreements covering confidentiality and IP rights. We formulate policies and practices, and conduct training, to help prevent the theft of trade secrets by former, current, and future employees.
When it comes to litigation, our lawyers command the experience, scientific knowledge, and geographical reach necessary to handle the relevant proceedings, whether heard in court or by an arbitral tribunal. If necessary, we can seek an injunction to prevent the misuse of information or to recover it from third parties. Because trade secrets litigation often moves rapidly in the courts, we stand ready to quickly assemble in-depth teams and strategies from innovation hubs across the nation and world.

Our team has litigated trade secret disputes stemming from licensing agreements and collaborations, as well as from employment relationships. As part of our leading global IP practice, we understand the important connections and distinctions between patents and trade secrets. We have a wealth of technical and subject matter expertise to draw from and we are ready to vigorously defend your position.

**Areas of focus:**
- Audits and protection policies
- Preservation of evidence
- IP, technology, and know-how licensing
- License disputes
- Trade secret misappropriation actions
- Employee disputes and team moves
- Use of third party information
- Independent development, reverse engineering, and “clean room” guidelines
- Alignment with patenting activities

"Named Managing Intellectual Property’s ‘Global IP Firm of the Year’ for two consecutive years – the only firm ever to do so."

*Managing Intellectual Property Awards, 2019*
Representative experience

- Representing a multinational electronics company in defense of allegations of trade secrets misappropriation in connection with solar cell technology.

- Representing a major pharmaceutical company in trade secret litigation involving the transfer of information by a former employee to a competitor.

- Representing a global high frequency trading business in relation to source code trade secrets, obtaining a multi-site search order and leading a big four computer forensics team executing it in the City of London over a 20-hour period.

- Representing uPI Semiconductor in a defense of Richtek Technology’s complaint for trade secret misappropriation in California state court.

- Conducting a six-month study published by the European Commission on trade secrets law: completing a comparative law assessment of protection against infringement in Member States.

- Acting for a global chemical company in an international dispute relating to industrial secrets of a world leading antibiotic formula. This involved litigation in the UK and U.S. and concerned activities in the U.S., the UK, Sweden, the Netherlands, and Taiwan.

- Advising a petroleum company in relation to protection of confidential know-how licensed to it and possible actions for breach of confidence where one of its plants was in danger of being nationalized and seized without its consent.

- Advising an international medical device company on suspected infringement of its trade secrets by one of its key ex-employees.
– Representing a German machinery company in an investigation and further legal actions against its Chinese former employee on the basis of misappropriation of our client’s technical know-how, which involved working with computer forensic experts to recover deleted digital data.

– Advising Solvay Co. Ltd. in their defense of a trade secret misappropriation action brought in connection with the manufacturing process of the synthetic chemical vanillin.

– Advising a petrochemicals company on restructuring their employee inventions and remuneration program, and designing confidentiality and restrictive covenants to protect client’s intellectual assets.

– Acting for a German chemical company in cross-border civil and criminal proceedings against trade secret theft by an employee and infringing factory in China, including successfully obtaining civil injunctions against infringers in Germany and a court evidence preservation order in China.

– Advising a European lighting designer on suspected trade secret misappropriation by its former Chinese OEM manufacturer and their ex-employees.

“The firm is commended for its deft handling of cross-border mandates, with one interviewee highlighting the firm's "international footprint."

Chambers Global (Intellectual Property), 2019
“Hogan Lovells” or the “firm” is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word “partner” is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2020. All rights reserved. 1148264_0220