

## PROTECCIÓN DEL SECRETO INDUSTRIAL EN EUROPA

Sugerencias para ser usadas por las empresas, particularmente las nuevas participantes en el mercado europeo.

### CONTENIDO

#### VISIÓN DE CONJUNTO

- Importancia de la protección de los secretos industriales
- Diferencias entre patentes y secretos industriales
- Marco legal para la protección del secreto industrial
- Protección internacional del secreto industrial
  - El Convenio de París
  - TRIPS
- Protección europea del secreto industrial

#### ¿QUÉ ES UN SECRETO INDUSTRIAL?

- La confidencialidad
- Valor económico
- Pasos para asegurar la confidencialidad de la información

#### PROTECCIÓN DEL SECRETO INDUSTRIAL

- ¿Qué medidas deberían tomarse por las empresas para proteger sus secretos industriales?

##### Empleados

- Formar a los empleados en cuestiones relativas a la seguridad de la información
- Marcar documentos y restringirlos al acceso público.
- Contratos de confidencialidad y acuerdos de no divulgación.
- Acuerdos de no competencia
- Vigilar las actividades de los empleados
- Otras medidas de seguridad

##### Socios comerciales

- Acuerdos de licencia
- *Joint venture*

#### APROPIACIÓN INDEBIDA DE SECRETOS INDUSTRIALES

- Definición
  - Cuáles son los métodos indebidos para conocer un secreto industrial
  - ¿Qué es la ingeniería inversa?
- Robo de secretos industriales
- Espionaje industrial

#### MEDIDAS CONTRA LA APROPIACIÓN INDEBIDA/VIOLACIÓN DE SECRETOS INDUSTRIALES

- ¿Qué actos constituyen violación o infracción de secreto industrial?
- Litigios
- Recursos
  - Medidas cautelares
  - Recursos penales o administrativos
  - Daños y perjuicios
    - Pérdida de beneficios
    - Enriquecimiento injusto
    - Regalías

#### MÁS ENLACES INFORMATIVOS

## VISIÓN DE CONJUNTO

Es fundamental que las empresas puedan crear y promover la información necesaria para desarrollar o mejorar nuevos productos o servicios que incrementen la competencia y el entorno empresarial global. La información que permite a una empresa competir eficazmente es un "secreto industrial" y, por lo tanto, es un valor comercial que vale la pena salvaguardar.

Famosos ejemplos de secretos industriales son la fórmula de la Coca-Cola o el código fuente de Microsoft. para Windows. Los competidores pueden tener acceso a tal información de forma relativamente fácil, por ejemplo, convenciendo o simplemente contratando a los empleados clave que crearon o tienen acceso a esta información confidencial.

Una empresa de éxito puede salvaguardarse contra la pérdida de un secreto industrial, por ejemplo, firmando acuerdos de no divulgación o tomando medidas de seguridad con los socios comerciales. Las PYMES en particular deben ser conscientes de los riesgos de su crecimiento empresarial y deberían desarrollar un programa efectivo para gestionar los secretos industriales y tomar medidas para proteger los secretos contra la apropiación indebida por medio del robo o espionaje industrial. El mal uso de dicha información (por personas ajenas al propietario del secreto industrial) se considera una práctica desleal y puede ser amparada ante la justicia.

Dependiendo del sistema legal, la protección del secreto industrial se integra en la protección contra la competencia desleal, o bajo disposiciones específicas de la protección de la información confidencial del derecho contractual o penal. No hay una ley del secreto industrial uniforme en la Unión Europea: los principios básicos son similares en los 28 estados miembros, pero la no existencia de un sistema supranacional determina diferentes modos de regulación en cada país.

Esta guía pretende dar una definición general de secreto industrial, su naturaleza y alcance y debería contribuir a una mejor comprensión de las dificultades para identificarlos y de las diferentes formas de protegerlos. La guía explicará qué se entiende por apropiación indebida de un secreto industrial y qué acciones se deben tomar para prevenir la violación de secretos comerciales en diferentes circunstancias. Debido a la normativa específica en la protección del secreto industrial, se aconseja que las empresas comprueben la legislación nacional de cada estado miembro de la UE donde se pida la protección y acudan a expertos profesionales de la

propiedad industrial cuando se desarrolle una estrategia de protección de la propiedad intelectual que incluya la protección de los secretos industriales.

## Importancia de la protección de los secretos industriales

Actualmente, la importancia de la protección del secreto industrial y el desarrollo e implementación de prácticas de protección de la información se ha incrementado debido al desarrollo del entorno empresarial. Ya que todo el marco nacional e internacional sobre derechos de propiedad industrial evoluciona, sobre todo para fomentar la innovación, la legislación de los secretos industriales está alcanzando más atención que nunca. Cuando la protección legal es para productos que son el resultado de inversión en I+D, la protección del secreto industrial es, en algunos casos, la forma preferida de protección.

**Un secreto industrial es una opción diferente a otras opciones de propiedad intelectual, en ésta su protección requiere buena voluntad y mantenimiento y, en algunos casos, es el derecho de propiedad intelectual más atractivo, eficaz y fácilmente disponible.**

## Diferencia entre patentes y secretos industriales

Debido a su carácter confidencial y que se requiere su revelación para obtener protección legal, los secretos industriales no se protegen de la misma forma que otras opciones de propiedad industrial como las patentes o las marcas. Con todo, la protección del secreto industrial ofrece un alcance mucho más amplio que las patentes, las marcas o los derechos de autor.

Una patente requiere que la invención sea nueva, de aplicación industrial y no obvia, ha de ser revelada al público y ser una materia patentable. Las marcas protegen solo la palabra o imagen que hace referencia a un producto o servicio en el comercio. Los derechos de autor protegen solo la forma de expresión pero no el contenido, la idea, la información o el concepto que se quiera transmitir.

A diferencia de las patentes, los secretos industriales pueden proteger materia no patentable. No hace falta que sean nuevos o no obvios. Se protegen sin necesidad de rellenar formularios o cualquier otro requerimiento formal o proceso ante un organismo oficial de protección. Así mismo, un secreto industrial puede estar protegido

sin límite de tiempo, tanto tiempo como se mantenga en confidencialidad.

La protección del secreto industrial es aconsejable:

- Cuando el secreto se refiere a un proceso o invención de fabricación, más que a un producto ya que los productos están más sujetos a la ingeniería inversa.
- Cuando se considera que el secreto no tiene tanto valor como para presentar una patente.
- Cuando el secreto no es patentable.
- Cuando una empresa ha solicitado una patente y está esperando a que se conceda. Por ejemplo, en algunos países una invención se debe mantener en secreto hasta que se decida si continuar como secreto o patentarla.

Sin embargo, la protección del secreto industria es débil y muy difícil de hacer cumplir. Solo protege contra la adquisición indebida, uso o revelación de información confidencial. Si el secreto es revelado, cualquiera puede tener acceso a él. Las desventajas del secreto industrial son también el alto coste que tiene la implementación de la seguridad y las políticas de protección, control y vigilancia. Además alguien puede descubrirlo independientemente o puede patentarlo.

Si el secreto es un know-how patentable hay que evaluar cuidadosamente antes de decidir si patentar la invención o mantenerla en secreto. La empresa propietaria debe considerar qué tipo de conocimiento implica, el uso contemplado, la duración de la ventaja competitiva esperada y la posibilidad de permanecer en secreto por un largo período. Con estas razones, la protección del secreto industrial debe parecer especialmente atractivo para las PYMES.

### Marco legal para la protección del secreto industrial

El sistema de la UE para la protección del secreto industrial no está totalmente armonizado. Los TRIPS (Acuerdos sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio) y otros acuerdos internacionales dan unos estándares mínimos legales para la protección del secreto, dejando a los países suficiente espacio para abordar el tema por sí mismos. La legislación en la Unión Europea se basa en estos principios, pero no ha abordado la cuestión directamente. Así pues, las PYMES debería tener cuidado con las posibles diferencias entre países.

## La protección internacional del secreto industrial

### El Convenio de París

El Convenio de París para la protección de la propiedad intelectual de 20 de marzo de 1883 puede encontrarse en:

[http://www.wipo.int/wipolex/es/wipo\\_treaties/text.jsp?file\\_id=287557](http://www.wipo.int/wipolex/es/wipo_treaties/text.jsp?file_id=287557).

Prohíbe las prácticas comerciales ilegales entre sus miembros; especialmente es inaceptable "todo acto de competencia contrario a los usos honestos en materia industrial o comercial". Los ejemplos de competencia desleal que da el Convenio de París no hacen mención explícita a la infracción de secreto industrial. Pero se podría pensar que el espionaje industrial y otros medios desleales, en el caso del secreto industrial, se consideraría como competencia desleal bajo los términos del Convenio de París.

### TRIPS

El Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio está basado en las disposiciones del Convenio de París para la protección de la propiedad intelectual y el Convenio de Berna para la protección de las obras literarias y artísticas y que puede encontrarse en:

[http://www.wipo.int/wipolex/es/treaties/text.jsp?file\\_id=190791](http://www.wipo.int/wipolex/es/treaties/text.jsp?file_id=190791).

**La disposición más relevante de los TRIPS es la sección 7: Protección de la información no revelada. El artículo 39 (2) establece:**

**2. Las personas físicas y jurídicas tendrán la posibilidad de impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honestos, en la medida en que dicha información:**

**b) tenga un valor comercial por ser secreta; y**

**c) haya sido objeto de medidas razonables, en las circunstancias, para mantenerla secreta, tomadas por la persona que legítimamente la controla.**

Otra característica relevante de los TRIPS es su disposición para la aplicación de los derechos de propiedad intelectual. Los miembros deben garantizar un trato justo e igualitario a los titulares de derechos de propiedad intelectual, incluida la autoridad suficiente para requerir la presentación de pruebas, y soluciones como las medidas cautelares y la compensación por daños.

Los estándares legales para la protección del secreto industrial así como otros derechos de la propiedad intelectual protegidos por los TRIPS son objeto del sistema internacional de solución de controversias de la Organización Mundial del Comercio.

### La protección europea del secreto industrial

La Unión Europea no tiene ninguna disposición legal específica para proteger el secreto industrial o la información no divulgada, aunque la legislación en algunos países europeos tienen una larga tradición en la protección del secreto industrial. Algunos estados miembros de la UE como Italia, Alemania o Bulgaria proporcionan una fuerte protección a los secretos industriales. En Francia, Alemania, Reino Unido, etc. existen medidas cautelares, daños y responsabilidad de terceros para los litigante privados.

En general, la mayoría de los estados miembros no tienen legislación específica para los secretos industriales. Dependiendo del sistema legal, la protección del secreto industrial se basa en disposiciones específicas sobre la protección de la información confidencial, sobre la protección contra la competencia desleal, así como en otras disposiciones del derecho mercantil y penal. Por ejemplo:

- **derecho mercantil, cuando el acuerdo entre las partes busca proteger el secreto industrial usando cláusulas de no divulgación o confidencialidad o a través de cláusulas de ingeniería inversa, etc.**
- **legislación contra la competencia desleal, cuando la apropiación indebida se ha hecho por competidores que no tienen ninguna relación o acuerdo contractual, en un acto de robo o espionaje.**
- **Derecho penal, cuando un empleado roba secretos de una empresa o está implicado en actos que se pueden considerar como invasión de la privacidad, espionaje electrónico, etc.**

El estado y la forma de protección del secreto industrial, incluido el know-how, y el tratamiento de los actos de competencia desleal es muy diferentes entre los estados miembros. A nivel europeo una empresa puede aplicar la directiva europea de la ejecución de los derechos de propiedad industrial (Directiva 2004/48/EC del Parlamento Europeo y del Consejo del 29 de abril de 2004 de ejecución de los derechos de propiedad intelectual) solo si los secretos se protegen como derecho de la propiedad industrial a nivel nacional. La Directiva europea da las disposiciones del procedimiento que conciernen a cualquier infracción de la propiedad intelectual como dispone la legislación comunitaria y/o la legislación nacional del país europeo al que le afecta. Esta Directiva contiene disposiciones sustantivas e incluye las soluciones disponibles en un tribunal civil, pero no los delitos penales.

La Directiva se puede encontrar en:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:es:PDF>

### ¿QUÉ ES EL SECRETO INDUSTRIAL?

Basándonos en los acuerdos TRIPS se define en términos generales en muchos países como cualquier información, incluyendo pero no solo, los datos técnicos o no técnicos, una fórmula, patrón, recopilación, programa, dispositivo, método, técnica, proceso de elaboración, datos financieros, o un listado de clientes o proveedores actuales o potenciales que:

es suficientemente secreto como para obtenerse un valor económico actual o futuro, por el hecho de que no es conocido por las personas que pudieran obtener un valor económico por su uso o divulgación; y

el secreto del cual se mantiene gracias a los esfuerzo de su titular.

Los secretos industriales tienen **3 elementos principales**: la información debe ser secreta en sí misma, debe tener valor económico comercial, y el titular debe mostrar esfuerzos razonables para mantener la información en secreto (por ejemplo acuerdos de confidencialidad). Estos principios se han reconocido desde hace tiempo por los estados miembros de la UE.

Un **secreto industrial es un proceso o dispositivo para uso continuo en operaciones empresariales y es importante y/o vital para el funcionamiento de una empresa**. Son secretos técnicos, tecnológicos y de fabricación. A continuación se ofrecen unas ideas de la amplia gama de lo que podrían ser:

- recopilación de datos, por ejemplo listas de clientes (cuanta más información contenga la lista más protección como secreto industrial), listas de proveedores especiales.
- Diseños, dibujos, planos arquitectónicos, proyectos y mapas, instrumentos, patrones
- Información valiosa empresarialmente como estrategias de negocio, métodos de hacer negocios y planes de marketing, por ejemplo el plan de una empresa para lanzar un nuevo producto, planes de negocio
- Costes e información sobre precios, precios de adquisición de materias primas
- Información sobre actividades de investigación y desarrollo
- Incluso los resultados negativos, por ejemplo en la I+D, pueden formar parte del secreto industrial ya que tienen un valor significativo si no lo conocen los competidores. Otros ejemplos de resultados negativos pueden ser los detalles de los esfuerzos fallados para remediar los problemas de producción de ciertos productos, ideas de investigación, proyectos abandonados, estrategias de marketing fracasadas, etc.
- Los algoritmos y procesos implementados en programas de ordenador, los programas de ordenador en sí mismos, software, códigos fuente
- Tecnología de fabricación (los detalles) o técnicas y procedimientos de reparación, los detalles del proceso
- Procesos de seguimiento de documentos
- Esquemas, manuales, ingredientes, croquis, dibujos de ingeniería
- Prototipos
- Características de un producto
- Fórmulas, ensayos, procesos
- Estructura salarial de una empresa, paquetes de compensación
- Estrategias de promoción o material de marketing en desarrollo
- Know-how
- Datos de tests, libro de notas de laboratorio
- Canales de distribución

- Acuerdos que contengan detalles de vínculos de comercialización

Como es imposible definir con precisión qué es un secreto industrial, a menudo los tribunales tienen en cuenta una lista no exclusiva de factores que determinan si la información es un secreto industrial. Estos factores son:

- grado en el que la información es conocida fuera de la PYME
- grado en el que la información es conocida por los empleados y otras personas involucradas en la PYME
- medidas tomadas para guardar en secreto la información
- valor de la información para la empresa y sus competidores
- cantidad de esfuerzo o dinero que el propietario ha necesitado para desarrollar la información
- facilidad o dificultad con la que esta información podría ser obtenida o duplicada por otros.

### La confidencialidad

La información sobre la que trata un secreto debería ser confidencial. La información es secreta cuando no está a disposición del público o no es fácilmente accesible. Ocurre que a parte de su propietario, otras personas pueden conocer el secreto. Sin embargo si estas revelaciones fueran confidenciales (por ejemplo para los empleados o para los socios de la empresa) o sometidas a secreto, no se destruiría el status de secreto industrial.

### Valor económico

El segundo elemento es el valor económico del secreto industrial para la empresa. Es un factor interconectado con la confidencialidad. El valor de un secreto industrial debería ser importante y aportar algún tipo de beneficio económico a la empresa.

### Pasos para asegurar la confidencialidad de la información

El tercer elemento incluye los pasos para asegurar el secreto de la información. Este elemento es también una característica muy importante. En las demandas el tribunal examina si el propietario ha tomado o no, precauciones para salvaguardar la información. Esto quiere decir que le corresponde al demandante del secreto industrial tener una política de confidencialidad

dentro de los procesos normales de la empresa. Puede ser algún tipo de marcaje de la información como "confidencial", algunas restricciones para acceder a esa información, quizá disposiciones u otros acuerdos negociados con los empleados sobre esta información, etc.

Sin embargo, debería existir un procedimiento escrito con respecto a la revelación a empleados y otros, que defina cuál es la información y cómo y bajo qué circunstancias se puede usar y por quién. El procedimiento escrito demuestra que se ha garantizado la protección, lo que juega un papel importante en un litigio

## PROTECCIÓN DEL SECRETO INDUSTRIAL

### ¿Qué medidas se deben tomar en la empresa para proteger sus secretos industriales?

**Aunque ya se ha expresado que la UE carece de unos estándares uniformes para la protección de los secretos industriales, en general se busca la protección legal para parar o prevenir que el secreto se adquiera indebidamente, se divulgue o se use por otros que, o bien están ligados por un deber de confidencialidad (incluidos los empleados), o por personas que han firmado un acuerdo de no divulgación, o incluso por personas que adquieran el secreto industrial a través de medios impropios (como el robo, el espionaje industrial, el soborno, etc.).**

El propietario de un secreto industrial debería tomar medidas para proteger y mantener su confidencialidad. Una manera común de hacerlo es incluir acuerdos de confidencialidad en los contratos de los empleados, firmar acuerdos de no divulgación con los empleados durante y después del empleo y también obligarles a no usar el secreto industrial con un propósito de competencia (por ejemplo con vistas a crear una empresa competidora). También firmar acuerdos de confidencialidad con socios empresariales, siempre que se revele la información confidencial a licenciatarios y socios financieros.

Para restringir el acceso a la información, se pueden aplicar medios técnicos de protección: se recomienda que la empresa tome medidas físicas de seguridad como chequeos periódicos de seguridad, monitores de circuito cerrado, escuchas, o acceso restringido a los datos de ordenador almacenados y acceso restringido a los ordenadores y a áreas clasificadas.

## Empleados

### Formar a los empleados en cuestiones relativas a la seguridad de la información

Durante el tiempo de la relación laboral, los empleados deben ser conscientes de sus deberes fiduciarios para proteger la información confidencial y ser formados periódicamente sobre las situaciones que podrían resultar de la divulgación del secreto industrial. La formación de los empleados debe ser una parte integrada en cualquier programa de confidencialidad comercial. Un empleado que tenga acceso legítimo a un secreto industrial del empresario tiene que tratar esta información con mucho cuidado. Por esta razón deberían existir procesos en marcha para notificar a los empleados sobre los derechos del secreto industrial de la empresa y para proteger los secretos industriales que se utilizan en las operaciones comerciales de la compañía. La formación en los aspectos relativos a la seguridad de la información hace que la protección del secreto industrial forme parte de la cultura empresarial y entrena a los empleados en las políticas de seguridad de la información. La formación y la concienciación son sin duda los aspectos más rentables de un programa de protección.

### Marcar los documentos y restringir el acceso público

Otra medida que se debe tomar para proteger los secretos industriales es restringir el acceso público a la información confidencial. Es necesario limitar la información al personal clave y solo cuando haya necesidad de conocimiento. La protección del secreto industrial también puede conseguirse limitando el acceso a los archivos y otras estancias donde estén almacenados los papeles confidenciales, y restringir el control de acceso a través de autorizaciones adecuadas. Las restricciones físicas, con especial atención a los visitantes u otros externos, con acceso limitado a las instalaciones de la empresa y a áreas que contengan información valiosa, especialmente secretos industriales por supuesto, son esenciales. Además se pueden tomar otras medidas para restringir el acceso público a las instalaciones:

- libro de entradas y pases de visitantes
- acompañar a los visitantes
- hacer las zonas visibles a cualquiera que vaya por las instalaciones de la empresa, por ejemplo, tipo de maquinaria, planes, manipulación física del trabajo en progreso, etc.

- Control con contraseña para accesos, grabar los documentos accedidos por los empleados, lector biométrico de la mano, donde sea necesario.
- Guardias y cámaras de vigilancia, escuchas de conversaciones, documentos abandonados a simple vista, papeleras desatendidas.
- Otra buena manera de proteger los secretos industriales es marcar claramente los documentos, por ejemplo con "Confidencial".

### Contratos de confidencialidad y acuerdos de no divulgación

Un acuerdo de no divulgación (también conocido como acuerdo de confidencialidad) es una de las mejores herramientas del propietario de un secreto industrial para proteger la información confidencial y ayuda a facilitar la carga de la prueba en caso de litigio.

**Un acuerdo de no divulgación es un acuerdo donde una parte acepta la obligación clara y explícita de no divulgar o usar indebidamente la información confidencial que se ha compartido con él.**

Estos acuerdos normalmente cubren un extenso periodo de tiempo, así un empleado que otorgue un acuerdo de no divulgación acuerda no usar o divulgar la información por un mínimo período de tiempo, incluso después de que el empleado haya dejado el trabajo.

Para que tal acuerdo se pueda hacer cumplir debe estar claramente definida qué información entra en esta protección. Por lo tanto es extremadamente importante mantener la confidencialidad o el secreto de la información que tenga valor comercial específico. Un empresario con secretos industriales valiosos, requiere que todos los empleados con acceso a esos secretos industriales entren en un acuerdo de no divulgación.

Bajo la legislación de muchos estados miembros de la UE, no es siempre necesario firmar un acuerdo aparte porque en muchos países la ley que rige las relaciones entre empleados y empresarios requiere que el empleado mantenga la confidencialidad sin estos acuerdos.

Generalmente, los empleados están bajo un deber implícito de no usar los secretos industriales que hayan adquirido durante su contrato. Un deber implícito existe cuando las circunstancias de una situación particular sugieren que ambas partes la consideran confidencial. No obstante, este deber implícito solo existe si el empleado conoce o ha tenido acceso a un secreto industrial sin firmar un acuerdo de confidencialidad. Si el empresario

informó al empleado de la naturaleza confidencial de la información, y el empleado lo comprende, un tribunal podría imponer un deber implícito de confianza y confidencia en el empleado, haciéndole responsable de apropiación indebida de secreto industrial, si después usara o divulgara esta información sin consentimiento del empresario.

**Sin embargo, un contrato de no divulgación bien redactado es un medio preventivo muy recomendado de hacer frente a la mala conducta del empleado y facilita la carga de la prueba en caso de litigio. Un acuerdo de no divulgación es detallado e inequívoco, y limita las restricciones temporales y territoriales después de abandonar el empleo.**

Los acuerdos de no divulgación constituyen, así pues, una medida barata y efectiva para prevenir el mal comportamiento del empleado, y debería usarse con proveedores, contratistas, empleados potenciales o temporales, internos, visitantes, no empleados que trabajan en las instalaciones y clientes en prácticamente todos los niveles de la empresa donde se divulgue la información confidencial.

### Acuerdos de no competencia

Una vez que la relación laboral ha terminado legalmente, existe una restricción de la movilidad económica del empleado y una limitación de su libertad personal para seguir su carrera profesional preferida.

En el nuevo lugar de trabajo el empleado está todavía obligado a guardar el secreto industrial, así, está limitado, por su gran experiencia, a avanzar en el sector en el que es más productivo. Cabe señalar que el conocimiento general, las habilidades y la experiencia de un antiguo empleado no se pueden limitar.

Por lo tanto, a los empleados que dejan la empresa se les debe recordar que sus responsabilidades continúan y que deben devolver cualquier información o documento que pueda contener secretos industriales.

Deben también firmar un documento diferente en el que conste que ha devuelto toda la información confidencial y secreta. Este tipo de acuerdo de no competencia impide a un empresario independiente competir con la empresa o robar sus ideas.

**Cuando se requiera a los empleados que firmen un acuerdo de no competencia, los empleados deben estar de acuerdo en no trabajar para un competidor directo, por un cierto tiempo después de abandonar la empresa. La razón es que con el tiempo, los secretos industriales pueden ya no tener valor o pueden haber cambiado como los avances de la empresa.**

En otras palabras, la duración de un acuerdo de no competencia debe ser razonable en cuanto a duración, territorialidad y el alcance de la actividad. Un año de restricción para la competencia, es lo normal. En general, esta restricción se hace cumplir para proteger completamente los secretos del empresario.

### Vigilar las actividades del empleado

Otra medida de protección es presentar auditorias periódicas de la seguridad de la información, de la forma siguiente:

- vigilar el cumplimiento, procesar a los empleados infractores que se van
- realizar entrevistas de despedida para avisar a los empleados de sus obligaciones cuando abandonan la organización, especialmente en temas relacionados con la confidencialidad, los secretos industriales, etc.
- Mandar cartas a los nuevos empleados informándoles sobre algunos aspectos del área en la que el empleado se va a implicar de manera que el empleado no se ponga en este tipo de proyectos en la nueva organización
- Tratar a todos los empleados justamente y compensarlos razonablemente por cualquier derechos de propiedad intelectual generado por su trabajo

### Otras medidas de seguridad

El programa de protección debería incluir esfuerzos para identificar y salvaguardar los sistemas digitales y la información a través de medidas de seguridad integradas en toda la red de la empresa donde las intranets, extranets e Internet se usen para obtener ventaja competitiva. Puede ser de la forma siguiente:

- seguridad en las transacciones en línea, en la intranet y la web

equipar la entrada a la producción o a investigación y desarrollo con un pase de seguridad, autorización (clave), control de accesos

aislar físicamente y cerrar con llave: las cintas de los ordenadores, discos y otros medios de almacenamiento

no permitir pen-drives y puertos USB

vigilar el acceso remoto a los servidores

incluir medidas de seguridad interna con control externo y función de vigilancia: instalación de claves y accesos a datos informáticos encriptadas, así como antivirus y protección de las comunicaciones por e-mail.

### Socios comerciales

Una empresa puede mantener su información confidencial a los competidores requiriendo a los socios comerciales que firmen acuerdos de no divulgación, prohibiéndoles que divulguen secretos industriales. Estos contratos que previenen la divulgación pueden también usarse cuando se contrata con una empresa una licencia u otros acuerdos comerciales.

**Si el socio comercial ligado a un acuerdo durante el curso de las negociaciones, divulgara o hiciera mal uso de los secretos comerciales, violando el contrato, puede estar sujeto a penas económicas, así como a medidas contra las violaciones de secreto industrial impuestos por la ley nacional de cada estado miembro de la UE.**

### Acuerdos de licencia

Los acuerdos de licencia, contratos de know-how u otros métodos legales de transferencia comercial y adquisición de tecnología son medios importantes de proteger los secretos industriales dentro de la relación entre una empresa y su socio comercial.

Para empresas pequeñas, las ventajas incluyen la capacidad de aprovechar los recursos de la empresa. En este contexto, las PYMES pueden promover más fácilmente y más eficientemente sus esfuerzos en I+D con socios comerciales en vez de acometer la I+D independientemente. Un licenciante se encuentra en posición de poder entrar en mercados en los que no podría entrar sin la licencia. A veces sin personal suficiente para desplegar o utilizar un secreto industrial, las pequeñas empresas y *start-ups* pueden conceder licencias para obtener grandes beneficios.



**Si una empresa tiene un secreto industrial, puede licenciar sus secretos a otros.**

Las empresas deberían tener en consideración los siguientes aspectos cuando redacten acuerdos de licencia:

- Una licencia permite al propietario del secreto industrial imponer unas condiciones en cómo y bajo qué circunstancias la información se usará. Lo que más a menudo se introduce explícitamente es el deber de custodia y confidencialidad. Por ejemplo, si una empresa licencia su secreto industrial a un tercero y el acuerdo de licencia contiene una disposición de confidencialidad, el licenciario tiene el deber explícito de custodia y confidencialidad. En cualquier momento que tan explícito deber se incumpla, la parte incumplidora comete apropiación indebida del secreto industrial.
- Los tribunales europeos consideran que la parte que recibe la información de un secreto industrial a través de un acuerdo de licencia, ha recibido tal información legalmente.
- Los acuerdos de licencia también incluyen los aspectos de defensa de la competencia. La UE tiene estrictas leyes de competencia que afectan a la licencia de tecnología. Se ha emitido reglamentación detallada que rige los acuerdos de licencias de patentes y know-how, así como disposiciones adicionales relativas a otros derechos de propiedad intelectual. Las más importantes son el Reglamento de la Comisión (EC) nº 772/2004 de 27 de abril de 2004 en aplicación del artículo 81 (3) del Tratado (ahora artículo 101 (3) del TFEU) de las clases de acuerdos de transferencia de tecnología (TTBER) y el Aviso de la Comisión. - Directrices de la aplicación del artículo 81 de Tratado EC (ahora artículo 101 del TFEU) de los acuerdos de transferencia de tecnología (Directrices de Transferencia de Tecnología).

Estos reglamentos deben ser cuidadosamente considerados por cualquiera que actualmente licencie o contemple licenciar tecnología en la UE.

Las empresas pueden prever exenciones a las restricciones territoriales en sus licencias de know-how hasta que el know-how licenciado ya no sea secreto o hasta la finalización del acuerdo, en el caso de que se haya formalizado una licencia. Licenciar secretos industriales requiere de un especial cuidado porque una vez el secretismo se rompe, los secretos industriales dejan de tener valor, y el licenciante, en general, desea tener un

buen control sobre lo que el licenciario puede o debe hacer. Las empresas deben tener claro cuál es la legislación que rige para poder preparar un proyecto adecuado de acuerdo de licencia. Las PYMES tienen que ser conscientes de que las diferentes legislaciones sobre secretos industriales pueden crear problemas en el contenido de los acuerdos de licencia, por si alguna información confidencial, da derechos en un Estado Miembro pero no en otro. Esto podría impedir la transferencia de tecnología. Las discrepancias en las legislaciones nacionales de los secretos industriales podrían crear barreras comerciales, por ejemplo, un producto que es legal en un país puede violar las leyes del secreto industrial en otro Estado Miembro. Por consiguiente, las empresas deberían tener cuidado en aquellas potenciales diferencias y estar preparadas para los problemas que pueden aparecer.

#### Joint venture

Los acuerdos de licencia, contratos de know-how u otros métodos legales de transferencia comercial y adquisición de tecnología se pueden integrar como formas de acuerdos de Joint venture. Una Joint venture es una forma de alianza entre dos empresas independientes. La información debe ser más valiosa cuando se licencia a otros, o es la base para una Joint venture o un acuerdo de cooperación similar. Antes de entrar en una Joint venture o acuerdo similar, las partes deberían negociar y firmar un acuerdo detallado indicando la propiedad y la protección de la información confidencial.

Las Joint ventures normalmente implican dos tipos de información confidencial: la información aportada por los participantes y la información desarrollada como resultado de la participación. Los acuerdos de Joint venture debería indicar la propiedad y la protección de cada tipo de información, durante y después de la Joint venture. La Joint venture desarrolla una unidad diferente de negocio para permitir a dos o más partes, trabajar juntas en la realización de las actividades empresariales especificadas. El establecimiento de Joint ventures se considera como una oportunidad para las PYMES para mejorar sus capacidades internas y adquirir know-how técnico de socios más avanzados en países más desarrollados.

## APROPIACIÓN INDEBIDA DE SECRETOS INDUSTRIALES

### Definición

**La apropiación indebida del secreto industrial ocurre cuando alguien adquiere, usa y/o divulga un secreto industrial sin permiso y de una manera inapropiada. Los ejemplos típicos incluyen actos ilegales como el robo, soborno u obtención fraudulenta de información protegida, o a través de vigilancia ilegal, falsificación, incumplimiento o inducción al incumplimiento de un deber de mantenimiento de secreto, o espionaje electrónico u otros medios.**

La apropiación indebida del secreto industrial normalmente se da en dos áreas: cuando el secreto ha sido apropiado indebidamente por alguien que tiene acceso a él (robos internos) y cuando ha sido apropiado por externos (robos externos). Esto es porque cuando se transfiere un secreto industrial su propietario debería prestar mucha atención a las disposiciones de confidencialidad y a la eficiencia de los mandamientos judiciales que se pueden obtener a nivel local para prevenir la divulgación no autorizada.

### Cuáles son los métodos indebidos para conocer un secreto industrial

**El titular de un secreto industrial solo está protegido de la divulgación no autorizada y del uso del secreto, si la otra parte no tiene permiso para usar o divulgar la información o si el secreto industrial es adquirido por medios impropios o bien otra persona sabe, o tiene una razón para saber, que se adquirió por medios impropios. Si fuera inocente de estos hechos (por ejemplo, un tercero adquirió por error el secreto y lo vendió sin darse cuenta de que era secreto), esa inocencia se podría usar como defensa en una demanda por apropiación indebida.**

Por lo tanto, el propietario de un secreto industrial debe tomar acciones legales solo en aquellos casos en los que, habiendo tenido un cuidado adecuado para proteger el secreto industrial, alguien se apropiara indebidamente de un secreto, por ejemplo cuando un ex empleado transmite secretos del empleo anterior a un nuevo empleador, o usa el secreto del empleo anterior en una nueva empresa

o nuevo trabajo. Es también importante poner en conocimiento de los empleados, contratistas y socios comerciales el tipo de información que tienen obligación de respetar como secreto. Muchas veces, la gente tiene acceso legítimo y permitido a un secreto industrial. Cuando alguien con legítimo acceso usa su secreto para su propio beneficio o lo revela a otros ha cometido apropiación indebida de secreto industrial, lo que quiere decir que el propietario del secreto puede pedir ayuda legal a los tribunales.

La cuestión importante sobre la apropiación indebida es si tienen o no deuda de confianza y confidencia los que violaron usando y/o divulgando el secreto industrial.

Uno de los ejemplos mejor conocidos de una manera legal pero impropia de obtención, es el de una empresa que construye una nueva planta de fabricación. Mientras la planta se está construyendo todavía, una empresa rival sobrevuela la zona de construcción y toma fotos de cómo se está haciendo. Haciendo esto, el rival no quebranta ninguna ley. Sin embargo, el proceso de construcción de la empresa original es un secreto y los tribunales encontrarían que la empresa rival ha tratado de conocerlo de manera inadecuada sobrevolando la planta. El rival, en ese caso, sería responsable de apropiación indebida de secreto.

La razón por la que el tribunal llega a esta conclusión es que no tendría sentido para la empresa original cubrir el lugar de la construcción mientras se construye la planta. La forma inapropiada usada para adquirir o conocer el secreto no tiene que ser necesariamente ilegal para reconocerse como impropia.

Si alguien toma medidas activas en un intento de superar las medidas del propietario del secreto para mantener la confidencialidad, es suficiente para constituir modo inapropiado.

Mientras tales intentos pueden encontrarse impropios, es importante entender que hay medios para enseñar un secreto industrial que son correctos. La forma correcta para que alguien conozca y use un secreto industrial es a través de la ingeniería inversa de productos, que no se califica de apropiación indebida de secreto (lo que significa que no se tiene derecho a usarlos o a conseguir que paren en sus acciones).

Si el secreto es un producto, se le puede hacer ingeniería inversa o si ha sido descubierto independientemente, sin usar medios ilegales o sin violar ningún acuerdo, ley, etc.

## ¿Qué es la ingeniería inversa?

**La ingeniería inversa es resolver la información secreta de alguien, examinando y probando públicamente la información disponible.**

La ingeniería inversa sucede cuando alguien obtiene legalmente un producto y descubre cómo funciona ese producto o cómo está formado, mediante un estudio cuidadoso, desmontándolo, experimentando con él, etc. Estos medios legales incluirían obtener la información de fuentes públicas o publicaciones públicas, licencias del propietario del secreto, creaciones independientes, ingeniería inversa, etc. La ingeniería inversa es una actividad industrial muy común, y siempre que el secreto industrial se haya obtenido de forma legal, es un medio apropiado para conocer el secreto de alguien. Es obvio que tan pronto como la nueva información, producto o equipo está accesible en el mercado, los competidores pueden analizarlo para conocerlo e imitarlo o reproducirlo. Es importante darse cuenta de que el secreto está protegido el tiempo en que permanece en secreto. Por medio de contratos adecuados, se logra que las personas asociadas con el secreto industrial no lo divulguen a otros sin consentimiento explícito del propietario. Sin embargo, si alguien sin acceso legal a la información del secreto, descifra o llega a la información usando medios legales, como la ingeniería inversa o la invención independiente, entonces no se puede evitar que se use la información. Bajo estas circunstancias, el propietario del secreto industrial no puede tomar acciones legales.

Esta es una de las razones por la que una patente es a veces preferible a un secreto industrial. Incluso si alguien hace ingeniería inversa de un producto patentado, no puede usarla sin el permiso del titular. Sin embargo, son libres de usar la ingeniería inversa de un secreto sin pedir permiso al propietario del secreto. Si una persona ha conocido o adquirido el secreto de alguien por medios apropiados, no ha cometido apropiación indebida de secreto industrial. Igualmente, si una persona recibe la información de otro y no sabe o no tiene motivos para saber que esa persona ha obtenido de manera inapropiada la información, no es responsable de apropiación indebida. Aunque el propietario de un secreto puede presentar una demanda contra esa persona, en última instancia no será responsable de los daños. Pero de nuevo, esto pasa si esa persona no sabe que la información se obtuvo de forma indebida o no tiene motivos para saberlo.

## Robo de secretos industriales

Los secretos industriales son un área potencialmente crítica especialmente en una economía de la información cuando hay una gran rotación de empleados dentro de una empresa, una mano de obra más móvil, incremento de contratistas y consultores e incremento de externalización de la infraestructura, lo que incrementa las posibilidades de que sean robados. Los datos y la información valiosa se roban con medios electrónicos de alta densidad como los CDs, memorias USB, etc., así, ya no es necesario cargar con la información física lo que hace más fácil transportarla. De esta manera los ordenadores han hecho mucho más fácil crear y robar secretos industriales. Cada vez más, Internet, las tecnologías de intercambio de archivos hacen más fácil transmitir fácilmente un gran volumen de información. Combinado con el incremento de la movilidad de los trabajadores hay una gran posibilidad de que los secretos industriales se roben. Cerrar bajo llave los secretos industriales contra los externos ya no es suficiente.

Por lo tanto, no es sorprendente que a día de hoy la mayoría de violaciones de secretos industriales sean por robos internos. Mientras las empresas hacen todo lo posible para protegerse contra la revelación de externos, es un hecho reconocido que más del 80% de los delitos de información vienen de dentro de la empresa y están ligados a empleados, contratistas, internos de confianza y son el resultado de destrucción maliciosa, borrado de datos de I+D por empleados descontentos o despedidos, robos por empleados en formación y, en muchos casos, debido a ignorar las obligaciones relativas al secreto industrial de empleados actuales, en formación o jubilados. Estos robos internos se pueden evitar. Las empresas pueden y debe esforzarse en proteger sus secretos comerciales promulgando medidas de seguridad empresariales y cláusulas de confidencialidad con los empleados, licencias de tecnología, acuerdos con los transportistas y acuerdos de *joint venture*. Aquí ponemos algunos ejemplos de medidas de seguridad física: chequeos periódicos de seguridad, monitores de circuito cerrado, acceso restringido o control a los datos informáticos almacenados y acceso restringido a las áreas de ordenadores y clasificadas. Estos métodos preventivos son necesarios y rentables y ayudan mucho a proteger los secretos comerciales del robo por personas a quienes las empresas deben revelar el secreto para que puedan realizar su trabajo: empleados, vendedores y asesores.

El robo interno por empleados descontentos o empleados en formación también es intencional. Algunas de estas personas se permiten a sí mismos ser explotados por

operativos de inteligencia competitiva, por dinero. En efecto, se puede decir que la principal actividad empresarial de muchas empresas actualmente, es la creación de información de secretos industriales – toda la gama desde sobre qué se trabaja o sobre qué no se trabaja, qué pasó en el pasado y qué planea para el futuro. Los ladrones de esos secretos industriales y las infracciones de los competidores es una amenaza para el valor de los accionistas de la empresa.

## Espionaje industrial

El espionaje industrial es otro método común para la apropiación indebida de un secreto industrial. El espionaje industrial es propio de ladrones externos de secretos de una organización o empresa.

El robo externo incluye el espionaje de empresas por criminales profesionales, focalizándose en tecnología específica, iniciando ataques de red (hackers), robos en ordenadores portátiles accediendo al código fuente, diseños de productos, planes de marketing, listas de clientes, acercándose a los empleados para revelar información empresarial, etc.

La intensa competencia en los mercados nacionales e internacionales ha dado lugar a un alarmante incremento del robo por intrusos. El espionaje industrial está aumentando debido a que la competencia global produce ciclos más cortos de los productos, márgenes de beneficios más pequeños, disminución de la lealtad de los empleados. La posibilidad de que el secreto industrial sea un activo de alto valor que pueda ser usado, vendido o comercializado en las empresas líderes en tecnología, ha llevado progresivamente a que muchas empresas pongan coto a la identificación de sus secretos y a gestionar políticas, programas, procesos y medidas prácticas y actividades para el día a día. La feroz competencia en los mercados interiores y exteriores ha hecho aumentar el sabotaje y el espionaje industrial pues los secretos pueden perderse fácilmente si no se ponen en marcha medidas adecuadas de protección para empleados, socios, páginas web y sistemas físicos o electrónicos que sean propiedad de o se usen en una empresa. Con una competencia creciente en los mercados y el aumento de los costes de I+D, la pérdida de secretos cobra mayor importancia.

La típica respuesta para mantener seguros los secretos es usar mejor y más formas sofisticadas de guardarlos. Las empresas tienen gastos enormes al año en tales métodos. Claves, instalaciones seguras, guardias de seguridad y tarjetas de identificación y cortafuegos para Internet,

todo sirve para tener encerrados los secretos de forma más segura. Todos esos métodos de seguridad protegen contra la revelación de forasteros.

## MEDIDAS CONTRA LA APROPIACIÓN INDEBIDA/VIOLACIÓN DE SECRETOS INDUSTRIALES

Los secretos industriales se regulan de manera diferente en cada uno de los 28 estados miembros de la UE: las autoridades nacionales y las leyes rigen la concesión, el alcance, la aplicación y validación en el territorio nacional. Las infracciones de los secretos industriales por terceras partes se consideran normalmente como delito.

En esos casos cuando los secretos son protegidos como un derecho de propiedad intelectual a nivel nacional, se entiende que están cubiertos para el ámbito de la UE por la Directiva de aplicación de los derechos de la Propiedad Industrial. Las empresas han de tener en cuenta que los principios generales de sanciones contra la obtención, los procesos y medidas que garantizan el cumplimiento de los derechos de la propiedad intelectual a nivel europeo están previstos en la Directiva de aplicación.

Las empresas han de ser conscientes que el alcance de la Directiva no se limita a los derechos armonizados a nivel europeo, sino que también cubren los derechos protegidos como derechos de propiedad intelectual por la ley nacional. La Directiva, así pues, solo prevé la armonización en cuanto a las medidas de ejecución se refiere. Las empresas han de conocer el derecho sustantivo en propiedad industrial, las obligaciones internacionales de los Estados Miembros (sobre todo los Acuerdos TRIPS) incluyendo las disposiciones de la ley criminal de los Estados Miembros porque como derecho procesal la Directiva no afecta a lo arriba mencionado.

## ¿Qué actos constituyen violación o infracción de secreto industrial?

**El propietario de un secreto comercial puede protegerse a sí mismo contra la divulgación no autorizada y el uso del secreto comercial, así como contra el uso por una persona que lo adquiere por robo, fraude o incumplimiento de obligación de confidencialidad.**

Los actos prohibidos deben incluir la obtención y uso de secretos industriales, y la divulgación por una tercera parte sin autorización. La divulgación pública por equivocación o accidental de un secreto, en general ya no es un secreto. Debería también prohibirse la obtención a

sabiendas o por negligencia y utilizar indebidamente los secretos adquiridos.

Además, la divulgación prematura de la información valiosa comercialmente, incluido el know-how, puede ser perjudicial o fatal para los intentos posteriores de protección mediante una patente o diseño.

Un invento o diseño puede permanecer como secreto industrial hasta que se decida si continuar manteniéndolo más tiempo como secreto o patentarlo o registrarlo como diseño. De este modo cuando una empresa divulga por equivocación o accidentalmente su secreto, esto hará imposible el registro de la patente o diseño y la empresa puede perder sus ventajas.

Para establecer la violación de los derechos del secreto industrial, el propietario del secreto ha de ser capaz de mostrar:

- la infracción cometida o la ventaja competitiva adquirida por la persona/empresa que se ha apropiado indebidamente del secreto industrial.
- El propietario ha tomado todos los pasos razonables para mantenerlo en secreto.
- Hay un mal uso si la información obtenida ha sido usada o divulgada violando las prácticas comerciales honestas.

## Litigios

A diferencia de las demandas por infracción de las patentes, marcas y copyright, las demandas de secreto industrial requieren que el demandante pruebe la existencia de un secreto industrial y que él tiene los derechos de propiedad.

En las demandas de secreto industrial se suele alegar infracción de un gran grupo de secretos comerciales. Esto es, en parte, por el hecho de que los secretos no están ligados a una revelación, en parte porque en los casos de infracción de patentes, marcas y derechos de autor se lucha por proteger propiedades intelectuales más fuertes del demandante.

Esta misma estrategia se aplicaría en los casos de secretos industriales. El demandante evitaría alegar contra cada secreto al que el demandado ha accedido y pueda haber infringido.

El demandante establece las alegaciones más fuertes generalizando los argumentos a toda la información. Por otro lado al demandado se le ha dado la oportunidad de argumentar contra las alegaciones más débiles y generalizar estos argumentos a toda la información.

Alegando a todas las infracciones posibles debilita seriamente el caso del demandante.

Es posible litigar solo sobre secretos fuertes muy específicos. Esto forzará al demandante a argumentar su tesis más débil. Limitar la demanda a las alegaciones más fuertes parece ser particularmente relevante cuando concierne a los secretos comerciales o know-how.

La carga de la prueba recae normalmente sobre el demandante pero algunas pruebas que establecen la infracción son controladas exclusivamente por el demandado.

En tales casos, parece que los tribunales a menudo tienen dificultades para evaluar y equilibrar los intereses del titular de los derechos de la información y el interés del presunto infractor en la protección de la información confidencial con el fin de prevenir el abuso, en particular cuando las partes son competidores.

La práctica de los Estados Miembros de la UE, por otro lado, muestra que la protección de la información confidencial no significa que no se pueda acceder a ella con medidas provisionales.

Por otro lado, el acceso a la información confidencial a través de medidas provisionales (por ejemplo por búsqueda, descubrimiento, embargo o medida cautelar) pueden revelar secretos comerciales y parece que deben permitirse solo en los casos donde la información es realmente necesaria y donde la información no se puede obtener por otras vías legales.

Además, se puede aplicar un proceso especial (p.ej. audiencia cerrada al público) cuando tal información confidencial ha de ser divulgada incluyendo la limitación de usar esta información solo para el proceso.

También, para la protección completa de los secretos, esos secretos se deben mantener durante el proceso legal de manera que la persona que legítimamente los controla pueda de forma segura encontrar recursos ante el tribunal.

Así es muy importante tener procesos o reglas específicos para proteger los secretos industriales ante un tribunal. Esos procesos o reglas deben venir del código civil o de las reglas del tribunal.

En este momento debido a la falta de información en esta materia incluyendo la aclaración de las condiciones como cuándo y cómo, de acuerdo con la jurisprudencia de los tribunales nacionales, revelar la información confidencial que puede parecer útil, la Comisión Europea no está en posición de juzgar si esta situación presenta un obstáculo

para la aplicación efectiva de los derechos de propiedad intelectual.<sup>1</sup>

## Medidas

Las medidas contra la violación de secretos comerciales incluyen:

- una orden judicial para detener a la persona con más actos ilegales (medidas cautelares)
- una orden judicial para obtener compensación económica (daños y perjuicios, lucro cesante, enriquecimiento injusto)
- orden de embargo (para verificar las instalaciones del demandado, para tomar declaración, etc.)
- confiscación/embargo preventivo de los artículos que incluyen el secreto o productos resultantes de su uso o mal uso.

## Medidas cautelares

A menudo una empresa tendrá derecho a alguna forma de medida cautelar. Si la información es todavía un secreto protegible (por ejemplo, cuando la otra parte no ha hecho una difusión pública) el asesor legal puede pedir una orden judicial y el tribunal puede ordenar a la otra parte que deje de utilizar o compartir la información protegida. Las medidas cautelares pueden ser previstas para actos futuros de violación del secreto industrial\*.

El artículo 9 de la Aplicación de la Directiva obliga a los Estados Miembros a asegurar que el derecho de los titulares esté en posición de aplicar medidas cautelares contra el infractor dirigidas a la prohibición de continuar la infracción (medidas cautelares provisionales o temporales). Las medidas cautelares contra los infractores no son nuevas en los sistemas legales de los Estados Miembros y han sido extensamente usadas incluso antes de la adopción de la Directiva.

<sup>1</sup> Para más información ver Informe de la Comisión al Parlamento Europeo, de 29 de abril de 2004 sobre la aplicación de los derechos de la propiedad intelectual que se puede encontrar en:

<http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0779&qid=1401189420758&from=EN>

\* Para más información ver el documento de trabajo del personal de la Comisión: Análisis de la aplicación de la Directiva 2004/48/EC del Parlamento Europeo y del Consejo de 29 de abril de 2004 sobre la aplicación de los derechos de propiedad intelectual en los Estados Miembros. Documento de acompañamiento al informe de la Comisión al Consejo, el Parlamento Europeo y el Comité Social Europeo de la aplicación de la Directiva 2004/48/EC del Parlamento Europeo y del Consejo de 29 de abril de 2004 sobre la aplicación de los derechos de la Propiedad Intelectual COM(2010)779. <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0779&qid=1401279903293&from=EN>

El incumplimiento de una medida cautelar se sanciona con una multa que se paga al demandante o al tribunal o con sanciones penales en algunos casos. Los informes recibidos de los Estados Miembros sugieren que para la mayoría de ellos la experiencia con los mandamientos judiciales ha sido bastante positiva. Con algunas excepciones, los mandamientos judiciales en general parece que se conceden bastante rápidamente por los tribunales y a menudo conducen a una solución entre las partes de manera que se evitan los procedimientos sobre el fondo del asunto.

Para la mayoría de las partes interesadas, debido a la duración de los procesos judiciales que afectan a la infracción de los derechos de la propiedad intelectual y a los costes de los procesos, que rara vez se reflejan en las indemnizaciones concedidas en el procedimiento principal, las medidas cautelares son el principal remedio a aplicar.

A pesar de esta valoración, normalmente positiva, de las medidas cautelares, la información disponible sugiere que el nivel de las pruebas que requieren los tribunales para conceder las medidas difiere significativamente entre los Estados Miembros y, en general, es bastante alta. Por otra parte, parece que algunos tribunales a veces son reacios a ordenar medidas cautelares a no ser que se haya probado la infracción, en oposición a la concesión de medidas por razones preventivas.

En estos casos el “suficiente grado de certeza” que requieren los tribunales es mayor que los que los solicitantes son capaces de establecer en la práctica. Algunos tribunales no concederán ninguna medida cautelar sobre la base de que la información se divulga. Otros tribunales concederán medidas permanentes contra la otra parte, incluso a pesar de que el público es libre de usar la información, como un castigo por sus irregularidades en la divulgación pública de información.

La mayoría de las jurisdicciones que ven el secreto industrial como un derecho de propiedad tienden a mantener que el derecho solo tiene valor mientras permanece en secreto y que protegen durante el tiempo que permanecen en secreto o durante el periodo de tiempo que ha utilizado el demandado para desarrollar el mismo secreto de manera independiente. Además, en algunos casos, los costes asociados pueden ser significativos, a menudo comprenden las tasas judiciales, los honorarios de los abogados y en muchos casos también las tarifas de expertos técnicos.

## Recursos penales o administrativos

En algunas jurisdicciones para una protección efectiva del secreto industrial razonable y equilibrado, los recursos penales o administrativos pueden ser más importantes que los recursos civiles. Los recursos penales o administrativos pueden jugar un papel en conexión con la disposición de recursos civiles porque a menudo es difícil de establecer, u obtener evidencias, sobre los actos de violación de secretos industriales dentro del marco de procesos civiles en muchas jurisdicciones.

## Daños y perjuicios

En la mayoría de las situaciones dañinas, un tribunal puede ordenar al infractor a pagar los daños de manera ejemplar. Los daños deberían recuperarse a través del agravio o la violación de contrato.

El artículo 13 de la Directiva de aplicación requiere que los Estado Miembros permitan a las autoridades judiciales competentes, ordenar al infractor que a sabiendas o con motivos razonables para saberlo, es cogido en una actividad infractora, a pagar al titular del derecho de manera adecuada al actual perjuicio sufrido por él como resultado de la infracción. Cuando el infractor actuó de buena fe (sin motivos razonables de conocimiento), los Estados Miembros tienen la posibilidad de permitir a las autoridades judiciales que ordenen la recuperación de los beneficios o el pago de los daños, que deben preestablecerse (artículo 13(2)). El artículo 14 requiere que los costes legales razonables y proporcionados y otros gastos incurridos por la parte vencedora, correrán a cargo por la parte perdedora, a menos que la imparcialidad no lo permita.

Ya que el valor económico de la propiedad intelectual puede ser bastante difícil de medir, también debido a su naturaleza "abstracta", la práctica nos muestra que la estimación de los daños por infracción de los derechos de propiedad intelectual, es a menudo complicada. En la mayoría de los casos solo pequeños ajustes de las leyes nacionales que regulan el cálculo y adjudican los daños son necesarios para hacer cumplir a los Estados Miembros con la Directiva. Sin embargo debido al relativamente bajo número y a la considerable duración de los procesos judiciales, no hay todavía una jurisprudencia en la evaluación y la valoración de los daños desde la transposición de la Directiva en los Estados Miembros. Al mismo tiempo, parece que los juicios existentes no han sido demasiado explícitos y detallados en cómo han sido calculados los daños

otorgados. Sin embargo, muchos titulares de derechos informan que prefieren medidas provisionales (cautelares) rápidas y no reclamación de daños como la solución principal. La razón de esto son los altos costes de los procesos que raramente se reflejan en la indemnización concedida y en la gran duración de los procesos judiciales que envuelven las infracciones de los derechos de propiedad intelectual. Además las indemnizaciones concedidas en los casos de propiedad intelectual no son solicitadas por los titulares de los derechos por rutina.

## Pérdida de beneficios

En la adjudicación de daños y perjuicios, parece que todos los Estados Miembros de la UE tengan en cuenta la pérdida de beneficios de los titulares de derechos. La pérdida de beneficios se define en general como beneficios que debería haber ganado el titular del derecho en ausencia de infracciones, o lo que podría haberse esperado justificadamente (excluyendo los beneficios del infractor). Sin embargo, en algunos Estados Miembros no está claro si el precio del producto original o el precio de la falsificación (que debería ser sustancialmente más bajo en algunos casos) deberían tenerse en cuenta cuando se evalúe la pérdida de beneficios del titular del derecho.

## Enriquecimiento injusto

Los tribunales han medido de varias maneras los daños de un enriquecimiento injusto.

Los beneficios obtenidos ilegalmente por el infractor (enriquecimiento injusto) constituyen un nuevo aspecto para evaluar los daños, en los Estados Miembros y ha sido implantado en las legislaciones nacionales de maneras diferentes.

Muchos Estados Miembros requieren un titular de los derechos para probar que los beneficios fueron hechos con o como resultado de los productos infractores (relación de causalidad). Los infractores a veces deben tener mayores beneficios con los productos infractores que el titular del derecho con sus productos de marca. Los titulares de los derechos encuentran muy difícil probar que ellos habrían ganado los mismos beneficios que los infractores, particularmente donde los infractores ofrecen sus productos bajo condiciones que difieren significativamente de aquellas de los canales legales (p.ej. precios más bajos, costes de producción más bajos, ausencia de servicios relacionados, etc.). Además, en algunos Estados Miembros parece que los beneficios de

los infractores pueden tenerse en consideración solo una vez, una de dos como recuperación de beneficios injustos o como daños (o parte de daños), pero no de manera acumulativa. En otros Estados Miembros la transferencia de los beneficios de los infractores se evalúan como una alternativa, cuando los beneficios son mayores que el cálculo de daños del titular de los derechos. Finalmente en algunos Estados Miembros, además de los daños, también se ordena la devolución de los beneficios del infractor.

### Regalías

La Directiva de Aplicación proporciona dos posibilidades para que las autoridades judiciales determinen la cantidad de las indemnizaciones:

Se puede basar la cantidad en los perjuicios actuales (p.ej. los últimos beneficios del titular del derecho, los beneficios ilegales del infractor, el perjuicio moral y otras consecuencias económicas negativas); o pueden adjudicar daños a mano alzada basados en el valor único de los royalties que se habrían pagado si el infractor hubiera solicitado la autorización para usar los derechos de propiedad intelectual en cuestión (p.ej. si un infractor ha concluido un acuerdo de licencia con un titular de derechos).

### MÁS ENLACES INFORMATIVOS

Directiva 2004/48/EC del Parlamento europeo y del consejo de 29 de abril de 2004 sobre la aplicación de los derechos de propiedad intelectual:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:es:PDF>

Regulación de la Comisión (EC) nº 772/2004 de 27 de abril de 2004 sobre la aplicación del artículo 081(3) del Tratado (ahora artículo 101(3) del TFEU) a determinadas categorías de los acuerdos de transferencia de tecnología (TTBER):

<http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32004R0772&from=ES>

Comunicación de la Comisión- Directrices de la aplicación del artículo 81 del Tratado CE (ahora artículo 101 del

TFEU) sobre los acuerdos de transferencia de tecnología (Directrices de transferencia de tecnología):

[http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52004XC0427\(01\)&rid=7](http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52004XC0427(01)&rid=7)

TRIPS (Acuerdo de la Organización Mundial del Comercio sobre aspectos de los derechos de propiedad intelectual relacionados con el comercio):

[http://www.wipo.int/wipolex/es/other\\_treaties/text.jsp?file\\_id=305796](http://www.wipo.int/wipolex/es/other_treaties/text.jsp?file_id=305796)

Decisión del 30 de agosto de 2003 concerniente a la implementación del párrafo 6 de la Declaración de Doha:

[http://www.wto.org/spanish/tratop\\_s/trips\\_s/implem\\_para6\\_s.htm](http://www.wto.org/spanish/tratop_s/trips_s/implem_para6_s.htm)

Convención de la Haya sobre acuerdos de elección de foro:

<http://www.hcch.net/upload/conventions/txt37es.pdf>

Organización Mundial de la Propiedad Intelectual (OMPI)

¿Qué es un secreto industrial?:

[http://www.wipo.int/sme/es/ip\\_business/trade\\_secrets/trade\\_secrets.htm](http://www.wipo.int/sme/es/ip_business/trade_secrets/trade_secrets.htm)

---

Este documento ha sido preparado bajo el proyecto EU-China sobre la Protección de los Derechos de Propiedad Intelectual, del China IPR SME Helpdesk, que es una iniciativa de la Unión Europea para el asesoramiento de las PYMES.

El European IPR Helpdesk está gestionado por la Agencia Ejecutiva para la Competitividad e Innovación (EACI) de la Comisión Europea, con las directrices aprobadas por la Dirección General de la Empresa y la Industria de la Comisión Europea.

Las opiniones expresadas son de los autores y no necesariamente reflejan los puntos de vista de la Comisión Europea.

Este trabajo ha sido traducido por Estrella Alcón, socia de la Red Europea de Empresas en su calidad de Embajadora del European IPR Helpdesk. El folleto traducido deriva originalmente de materiales proporcionados gratuitamente por el IPR Helpdesk. El European IPR Helpdesk no se hace responsable de aquellas modificaciones o eliminaciones significativas del contenido, que se hayan producido en la traducción.