NORMATIVA

# Cómo evita una compañía que le roben sus secretos más valiosos

Se cumple un año de la entrada en vigor en España de la Ley de Secretos Empresariales, que refuerza la protección de la información reservada de una compañía, un bien inmaterial y, en ocasiones, poco identificado.

**Mª José G. Serranillos** Madrid

El año pasado un exempleado de Google fue acusado de robar información confidencial del coche autónomo y de filtrársela a Uber. Se descubrió que había descargado cerca de 14.000 archivos relativos al vehículo sin conductor del gigante tecnológico, una información jugosa y de alto valor económico para cualquier compañía. Un caso similar, también en 2019, puso el foco en la firma automovilística Tesla, que sufrió el robo de documentos secretos sobre el coche autónomo por parte de un exdirectivo, antes de que se marchase a una empresa china que fabrica el mismo tipo de vehículos.

Dreamstime

Son sólo dos muestras de los cientos de sucesos sobre robo de información secreta de productos, sistemas o fórmulas desarrolladas por las compañías, una lacra que les cuesta unas pérdidas de 3.000 millones de euros anuales, según un informe de PwC.

Con el fin de reforzar la protección jurídica de estos conocimientos en febrero del año pasado echó a andar en España una ley específica sobre secretos industriales que obliga, desde entonces, a que las empresas identifiquen qué información secreta tienen en sus manos y a que tomen acciones firmes de defensa ante posibles fugas.

El primer paso es saber qué conocimiento es valioso y cuál no lo es. Debe ser confidencial, algo que muchas empresas no tienen identificado, algo que pueden hacer mediante estudios internos o bien acudiendo a auditores externos.

"Además, debe tener un claro valor para la compañía", indica José Piñeiro, socio de Cases & Lacambra, que ilustra con varios ejemplos este tipo de información: "Fórmulas químicas, procesos o métodos de fabricación; información sobre la organización en una planta industrial, cuestiones técnicas de un producto, datos comerciales o financieros, planes de negocio o información de clientes y proveedores". Cristina Villasante, directora de nuevas tecnologías y propiedad intelectual de Ecija, lo resume en "cualquier conocimiento tecnológico, científico, industrial, comercial, organizativo o financiero que sea confidencial y tenga un alto valor económico".

## ¿Qué datos son reservados?

**Confidencial**
Es cualquier información o conocimiento que tenga, como primer condicionante, la confidencialidad.

**Valor empresarial**
Debe ser una información sobre una materia o desarrollo que suponga un alto valor económico para la compañía.

**Protección**
La empresa tiene que haber desarrollado medidas para protegerlo con el fin de que no salga a la luz y pueda ser copiado por otros.

### A prueba de fugas

El siguiente paso es tomar medidas para blindar el *know how* empresarial. ¿Cómo hacerlo? "Dotando a los empleados de formación y herramientas para que protejan la información e implantar sistemas físicos de protección como copias de seguridad, herramientas de encriptación y la restricción de acceso a ciertos empleados configuran algunas pautas eficaces para hacer frente a robos", detalla Miguel Ángel Martínez, agente de patentes europeas en Hoffmann Eitle. Otras medidas que apunta son "los acuerdos ante notario de la documentación relevante y de protocolos de confidencialidad por parte de los trabajadores en caso de que rescindan el contrato". La clave para este profesional es que esas acciones de seguridad "sean adecuadas y eficaces según el tipo de compañía y el producto".

Muchos directivos son ya conscientes del valor de este bien intangible. Un informe de Baker McKenzie realizado con encuestas a directivos refleja que el 82% de los consultados considera los secretos como parte esencial de su negocio, más valiosos incluso que sus patentes y marcas.

Identificar riesgos futuros forma parte también de la estrategia de blindaje, especialmente para firmas tecnológicas. Como apunta Villasante, buena parte de la innovación de estas compañías se debe a algoritmos asociados a la inteligencia artificial, un valioso conocimiento. Hay que saber protegerlo convenientemente porque estos datos están aún más expuestos a posibles fugas o robos por la Red.

## El robo de 'Súperlópez'

A mediados de los años 90 aconteció el que, para muchos, es el caso de espionaje industrial más conocido en España. José Ignacio López Arriortúa, apodado como 'Superlópez', fue acusado por General Motors (GM) de haberse apoderado de forma ilícita de documentos del grupo automovilístico donde trabajaba y de haber revelado secretos a la empresa de la competencia que le contrató, Volkswagen.

López y sus colaboradores planearon apoderarse de los documentos cien días antes de firmar con Volkswagen. Estos papeles contenían datos muy valiosos de papeles de GM sobre investigación, planificación, fabricación y compras de vehículos y su clara intención era aprovecharlos para su trabajo en la nueva compañía y, finalmente, destruirlos.

## Dos hoteleras en liza

En el año 2009 salió a la luz un caso de espionaje empresarial entre dos grandes cadenas del sector hotelero: Starwood demandó a Hilton por robarle secretos de alto valor económico. La primera acusó a su rival y a dos exejecutivos –Ross Klein y Amar Lalvani–, que pasaron a trabajar en Hilton, del hurto de más de 100.000 archivos con información secreta, que contenían los planes estratégicos de la compañía, información sensible sobre acuerdos comerciales y detalles clave de varios establecimientos de lujo de las marcas 'Luxury' y 'Lifestyle' de Starwood.

Esta compañía protagonizó una de las mayores operaciones corporativas en el sector al ser adquirida por el grupo Marriott en 2016.

## Huawei, en el punto de mira

Con la guerra comercial entre China y Estados Unidos en plena ebullición, a principios del año pasado el Gobierno de Donald Trump presentó varios cargos criminales contra el grupo chino Huawei, fabricante de móviles y otros productos tecnológicos. La fiscalía general de EEUU acusó al gigante asiático de robo de propiedad intelectual a la operadora T-Mobile US, entre otras cuestiones, como fraude financiero.

La sustracción de documentos estaba relacionada con desarrollos ligados a la robótica, en concreto con una tecnología llamada 'Tappy' que imita dedos humanos. Estos hechos coincidieron, además, con la detención en Polonia de un directivo chino de Huawei por las autoridades de este país, que fue acusado de cometer un delito de espionaje industrial.