COMO ACTUAR CUANDO SE SOSPECHA QUE UNA PERSONA TRABAJADORA ESTA LLEVANDO A CABO CONDUCTAS QUE PUEDAN COMPROMETER LOS SECRETOS DE EMPRESA

1. INTRODUCCIÓN

Se van a analizar las pautas esenciales que cualquier empresa debería seguir ante la sospecha de que alguna de sus personas trabajadoras está "llevándose información confidencial" y ello por cuanto las primeras decisiones que se adopten van a marcar el devenir de los distintos procedimientos judiciales que puedan acabar incoándose.

La cuestión no resulta baladí ya que la reacción de la empresa podría entrañar una intromisión en los derechos fundamentales de los que es titular la persona trabajadora, tales como el de su intimidad o el secreto de las comunicaciones, por lo que cualquier precaución será poca a la hora de investigar, en el seno empresarial, la conducta de la persona trabajadora.

2. SUPUESTO DE HECHO

El sencillo supuesto de hecho del que vamos a partir es el siguiente: La persona trabajadora Sr. X era Director Comercial en la empresa Z, tenía a su cargo a 4 comerciales, disponía de un portátil y un teléfono móvil facilitado por la empresa y, su superior jerárquico era el Director General a la par que Administrador Único de la sociedad.

La empresa Z, que se dedicaba al sector de la automoción, contaba con 120 trabajadores distribuidos en distintos departamentos y su actividad era la de diseñar y fabricar distintas piezas para el motor de determinados turismos.

La empresa Z tenía una red de clientes, marcas de turismos de alta gama, a quienes vendía las piezas de motor que éstos solicitaban, siendo sus comerciales en plantilla los que tenían, como laboral principal, la captación y ampliación de esa red de clientes.

La persona trabajadora Sr. X, por razón de su cargo, tenía acceso a los listados de clientes y proveedores, a las facturas emitidas por la empresa y a los presupuestos, información que se encontraba colgada en la intranet de la mercantil, a la cual se accedía con una contraseña y un usuario. Esta contraseña y usuario se facilitaba a todas aquellas personas trabajadoras que, por la tarea que desempeñaban, requerían tener acceso a esa información.

Más allá de la contraseña y usuario, la empresa Z no disponía de medidas adicionales de seguridad.

Durante los meses de enero y febrero de 2025, desde el departamento de IT de la empresa Z se detectó que la persona trabajadora Sr. X entraba en más de cincuenta

ocasiones diarias a la intranet, siendo absolutamente desproporcionado y fuera de toda lógica.

Igualmente, en febrero de 2025, un tercero advirtió al Director General de la empresa Z que la empresa V, competidora directa, había entablado negociaciones con el Sr. X para contratarlo como Director Comercial, idéntico cargo al que ostentaba en la empresa Z.

A partir de lo expuesto, debemos plantearnos cómo puede actuar la empresa desplegándose, en primera instancia, la represión laboral y, si fuere pertinente, la penal.

3. DESARROLLO DEL SUPUESTO HECHO

a. ANALISIS FORENSE DE LOS MEDIOS TECNOLOGICOS FACILITADOS POR LA EMPRESA A LA PERSONA TRABAJADORA

La cuestión esencial que se va a tener que plantear la empresa ante las sospechas de "robo" o "fuga" de información confidencial por parte de la persona trabajadora, es cómo llevar a cabo el análisis forense del ordenador de la misma, al ser éste el instrumento mediante el cual, en nuestro ejemplo práctico, habría perpetrado la conducta ilícita.

Con el fin de evitar una posible intromisión ilegítima en la esfera personal de la persona trabajadora, lo que supondría un atentado contra su intimidad, su esfera más privada, lo primero que debe valorar y analizar la empresa es si existe una política de empresa mediante la cual se advierte a las personas trabajadoras de la posibilidad de realizar controles aleatorios del uso de los bienes informáticos y tecnológicos puestos a su disposición por parte de la empresa.

Igualmente, tendrá que tenerse en cuenta si, en dicha política, se hace mención a la posible utilización de dichos bienes para fines particulares o si, por el contrario, únicamente es posible el uso para fines profesionales. Además, se deberá analizar si la propia política prevé la posibilidad de aplicar un régimen disciplinario en tales supuestos.

Asumiendo que la empresa dispone de una política en los términos descritos, la primera actuación que deberá llevar a cabo la empresa es citar a la persona trabajadora, requiriéndole que aporte el ordenador (o el bien objeto de análisis).

Es importante darle la posibilidad de ser asistido por un miembro de la representación legal de las personas trabajadoras, en caso de existir, para así dotar de más garantías al proceso.

Acto seguido, se debería exponer a la persona trabajadora los motivos por los cuales ha sido citado y se le debería informar de la apertura de un proceso de investigación a los efectos de esclarecer los hechos.

Con el fin de asegurar la licitud de las evidencias que se obtengan tras el análisis forense del ordenador, o del objeto de análisis, se recomienda que en el momento de la entrega del objeto de análisis también estén presentes, un perito informático experto en la materia, así como un notario, los cuales asegurarán que no se rompe la cadena de custodia (el perito suele ser el que precinta el ordenador u el objeto de análisis) y que tampoco se manipula (el notario custodiará el aparato electrónico).

La entrega del ordenador por parte del trabajador para su posterior análisis forense constituirá la prueba angular sobre la que pivotará el eventual despido que pretenda llevar a cabo la empresa, así como el procedimiento penal que considere incoar, de ahí que se recomiende que el proceso de recepción se realicé ante notario que levante oportuna acta y lo detente en custodia.

Una vez quede depositado en la Notaría, garantizando de este modo que no ha habido manipulación previa desde la entrega del ordenador por parte de la persona trabajadora hasta su análisis forense, cobrará protagonismo el perito informático correspondiente, el cual, en síntesis, clonará el disco duro del ordenador y llevará a cabo una investigación mediante un procedimiento de "búsquedas ciegas" de palabras.

Este análisis permite seleccionar por palabras lo que, a su vez, permite evitar una búsqueda indiscriminada en el ordenador de la persona trabajadora e incurrir, de este modo, en una vulneración de derechos fundamentales (esencialmente, intimidad y secreto de las comunicaciones).

Pese a que no es una obligación ineludible, no está de más citar a la persona trabajadora el día y hora en la Notaría para que esté presente en el clonado y, en su caso, pueda asistir el perito designado por la misma a los efectos oportunos.

La obtención de las evidencias informáticas debe pasar el filtro de licitud probatoria a fin de garantizar su impugnabilidad en el seno de un eventual procedimiento, poniendo especial relevancia en la forma en que se obtienen y el resultado que se alcanza.

Posiblemente, esta sea la actuación más relevante de todo el concadenado de actos que van a llevar a plantear las distintas acciones contra la persona trabajadora ya que, como hemos expuesto, puede determinar el éxito o el fracaso de las mismas en función de cómo se haya llevado a cabo.

Al respecto, no podemos dejar de reseñar la STEDH, Gran Sala, Caso Barbulescu contra Rumania, Demanda nº 61496/08, de fecha 5 de septiembre de 2017. (CASO BARBULESCU II), la cual señala una serie de puntos a tomar en consideración a la hora de valorar el derecho que puede tener el empresario a ejercer una supervisión sobre la correspondencia y otras comunicaciones de las personas trabajadoras y la protección de la intimidad de estas últimas.

Partiendo de que toda medida de supervisión debe satisfacer cuatro criterios: transparencia, necesidad, equidad y proporcionalidad, el TEDH reseña aquellos factores que las autoridades nacionales deberán tomar en consideración:

1. "Si se ha notificado a la persona trabajadora la posibilidad de que el empresario adopte medidas para supervisar la correspondencia y otras comunicaciones, y la implementación de esas medidas, debiéndose tratar de una notificación clara y efectuada con antelación".
2. "El alcance de la supervisión por parte del empresario y el grado de intrusión en la intimidad de la persona trabajadora, debiéndose distinguir entre la monitorización del flujo de comunicaciones y su contenido".
3. "Si el empresario ha proporcionado razones legítimas para justificar la monitorización de las comunicaciones y el acceso a su contenido real".
4. "Si hubiera sido posible establecer un sistema de supervisión basado en métodos y medidas menos intrusivos, que el acceso directo al contenido de las comunicaciones de la persona trabajadora".
5. "Las consecuencias del control para la persona trabajadora y la utilización de los resultados obtenidos por el empresario mediante la monitorización, especialmente, si eran los pretendidos con la medida".
6. "Si se habían proporcionado a la persona trabajadora las garantías adecuadas, especialmente cuando las operaciones de supervisión del empresario eran de carácter intrusivo".

En consecuencia, si bien el empresario tiene un "interés legítimo en garantizar el buen funcionamiento de la empresa" y ello puede llevarse a cabo estableciendo mecanismos para comprobar que "sus personas trabajadoras cumplen sus obligaciones profesionales de manera adecuada y con la diligencia necesaria", deberá valorarse, esencialmente:

- La política de uso de medios tecnológicos que disponga la empresa.
- La información que se le hubiera facilitado a la persona trabajadora sobre la posibilidad de monitorizar su ordenador o acceder a su correo corporativo.
- El consentimiento dado por éste.

En definitiva, se sitúa en el centro del debate el equilibro entre la expectativa de privacidad que la persona trabajadora tenía a la hora de utilizar sus herramientas de trabajo y la posibilidad del empresario de utilizar otras medidas que impliquen una menor injerencia en la vida privada de la persona trabajadora.

Como hemos indicado, cuanto más regulada esté la expectativa de la persona trabajadora, más sencillo será para la empresa tomar medidas sin que supongan atentar contra la intimidad y el secreto de comunicaciones de la misma.

b. REPERCUSIONES EN EL AMBITO LABORAL DE LAS CONCLUSIONES ALCANZADAS TRAS LA INVESTIGACION INTERNA

Dicho cuanto antecede y por proseguir con el caso práctico, el Informe Pericial tecnológico determinó que la persona trabajadora Sr. X accedió a la intranet de la empresa y durante los últimos quince días del mes de febrero de 2025 reenvió, indiscriminadamente, la información allí contenida: listado de clientes, de proveedores, presupuestos y facturas, desde su email corporativo a su email personal. Todo ello, como se ha expuesto, sin que tuviera consentimiento expreso para ello.

Si bien es cierto que en el presente supuesto de hecho no estamos entrando a valorar, desde la perspectiva del derecho laboral, la finalidad que perseguía la persona trabajadora al remitirse la información referida a su correo personal, la realidad es que, tanto si en la política existente se prohíbe expresamente dicha actuación, como si el fin que persigue la persona trabajadora es ilícito (por ejemplo, remitir la información a la competencia o para uso propio en un potencial futuro negocio particular), la actuación llevada a cabo por la misma se consideraría una transgresión de la buena fe contractual, siendo la buena fe uno de los pilares básicos de cualquier relación laboral.

Estaríamos, por tanto, ante un supuesto de despido disciplinario justamente por la actuación dolosa y voluntaria de la persona trabajadora de incumplir con sus obligaciones de confidencialidad y uso de medios de la empresa, en relación con el deber de actuar diligentemente y de buena fe (artículo 5 del Estatuto de los Trabajadores).

En el propio Estatuto de los Trabajadores, artículo 54.1.d) se prevé como causa de despido disciplinario la transgresión de la buena fe contractual. Este tipo infractor se complementará, en la mayoría de los casos, con la propia infracción por los mismos motivos que el convenio de aplicación de la compañía seguramente recogerá (la transgresión de la buena fe contractual es un tipo infractor comúnmente llamado entre los compañeros de profesión como “el cajón de sastre” en el que se engloban todas las conductas parecidas a la descrita en este artículo).

A título orientativo, destacar que la teoría gradualista, que debe operar en todos los despidos disciplinarios, respecto de la buena fe, tiene una aplicación más limitada, en tanto que la confianza que se tiene depositada en una persona trabajadora se tiene o no se tiene, no pudiéndose en muchas ocasiones modular esa pérdida de confianza por la transgresión de la buena fe contractual.

Por consiguiente, ante una conducta como la aquí descrita, y siempre que se siga el procedimiento detallado, el empresario podrá proceder al despido disciplinario, previa apertura del expediente previo, de acuerdo con la doctrina reciente del Tribunal Supremo (vide Sentencia del Tribunal Supremo núm. 1250/2024, Sala 4ª, de fecha 18 de noviembre de 2024, ponente: Ilma. Sra. Dª Mª Luz García Paredes).

c. REPERCUSIONES EN EL AMBITO PENAL DE LAS CONCLUSIONES ALCANZADAS TRAS LA INVESTIGACION INTERNA

i. CUESTIONES GENERALES

Analizada la conducta de la persona trabajadora Sr. X desde una óptica laboral, procedemos ahora al análisis de la misma desde una perspectiva penal, preguntándonos si la empresa puede accionar penalmente contra la persona trabajadora y, en consecuencia, si nos encontramos ante una conducta subsumible en el tipo de los delitos de violación de secretos empresariales.

La respuesta a estas cuestiones no puede ofrecerse sin antes analizar, si quiera sucintamente, los tipos delictivos cuya aplicación al presente supuesto podemos plantearnos.

Nos estamos refiriendo a los delitos relativos a la violación de los secretos de empresa. Este elenco de delitos se encuentra previstos en los arts. 278, 279 y 280 del CP, integrándose dentro de la Sección 3ª "De los delitos relativos al mercado y a los consumidores", del Capítulo XI "Delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores" del Título XIII "Delitos contra el patrimonio y el orden socioeconómico" del Libro II del CP.

Los delitos comúnmente conocidos como de descubrimiento y revelación de secretos dentro del ámbito del orden socioeconómico – no en el de la intimidad respecto a los que se refieren los arts. 197 y ss del CP – tutelan "la capacidad competitiva de la empresa en una economía de mercado", es decir, la capacidad competitiva que tiene el titular de la información confidencial dentro de la economía de mercado, entendiendo ésta como un "interés patrimonial individual".

El sujeto activo de estos delitos será "el que" "se apodere", "utilice artificios técnicos de escucha, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación", "difunda, revele o ceda" o "utilice en provecho propio" información que pueda catalogarse de secreto de empresa.

La referencia en los tipos penales a ese "el que" nos lleva a considerar que nos encontramos ante un delito común cuando se trate de las conductas previstas en el art. 278 y 280 del CP y de un delito especial en el caso del art. 279 CP ya que solo puede cometer el delito el que tenga "legal o contractualmente la obligación de guardar reserva".

El sujeto pasivo de estos delitos será el titular del secreto empresarial exigiéndose, para su persecución, el requisito de procedibilidad que impone el art. 287.1 CP "denuncia de la persona agraviada o de su representante legal".

En relación con el objeto material del delito, debemos distinguir entre el soporte físico que contiene el secreto de empresa, el cual puede ser desde un papel hasta un fichero informático, de lo que propiamente es el secreto de empresa el cual, si bien su

naturaleza es inmaterial, puede materializarse en un soporte físico.

ii. ¿QUE SE ENTIENDE POR SECRETO DE EMPRESA?

Pese a la utilización de dicha terminología por parte del Código Penal, lo cierto es que nuestro código punitivo no ofrece una definición sobre qué debe entenderse por secreto empresarial.

Se trata, por tanto, de un concepto jurídico indeterminado, que exige su remisión a la normativa extra penal para su interpretación, concretamente, a la Ley 1/2019 de Secretos Empresariales, la cual ofrece una definición legal al respecto y, si bien no es vinculante para el operador jurídico penal, podrá ser utilizada por el mismo como referente.

El art. 1 de la Ley 1/2019 define lo que se entiende por secreto empresarial de la forma siguiente:

"A efectos de esta ley, se considera secreto empresarial cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones:

a. Ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas.
b. Tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto.
c. Haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto".

Así mismo, dicha definición legal se completa con los rasgos que los distintos autores han ido exigiendo, abalados por los órganos judiciales, para dotar de reservada, confidencial o secreta una información.

De este modo, debe tratarse de (i) "información cuya detentación constituya un activo patrimonial o genere una expectativa de ganancia", (ii) "que sea desconocida por el competidor medio, actual o potencial del mercado relevante (reservada)", (iii) "que la detentación de dicha información suponga tener una ventaja competitiva frente al competidor medio", (iv) "que se trate de una información relacionada con la actividad empresarial" y, finalmente (v) "que el titular del secreto adopte medidas de autoprotección razonables".

Una concepción funcional-práctica de secreto empresarial considera como secretos los propios de la actividad empresarial que, de ser conocidos contra la voluntad de la empresa, podrían afectar a su capacidad competitiva.
Pese a que no se trata de un numerus clausus, el Prof. Dr. Albert Estrada clasifica en tres los tipos de secretos empresariales: "Los de carácter técnico – industrial (planos, diseños

industriales, procesos de producción, fórmulas químicas, etc…), los de carácter comercial (listados de clientes, listados de precios, ofertas, cálculos y estrategias de mercado, etc…) y los relativos a la organización, gestión y relaciones de la empresa con terceros (salarios e incentivos a los trabajadores, porque tengan valor patrimonial, se encuentren relacionados con la actividad empresarial y tengan carácter reservado)".

Por lo tanto, quedan excluidos de lo que se entiende por secretos de empresa:

1. Los datos de acceso público.
2. La información que conoce el sujeto por su experiencia y puede ser conocida por cualquier competidor del sector (vide Sentencia núm. 539/2018, 14 de septiembre de 2018, Ilma. Sección 3ª de la Audiencia Provincial de Valencia, Ponente: Ilma. Sra. Dª. Maria del Carmen Melero Villacañas-Lagranja, (JUR 2018\319234).
3. La información que es pública (vide Sentencia núm. 679/2018 de 20 diciembre de 2018 del Tribunal Supremo (Sala de lo Penal, Sección 1ª), Ponente: Excma. Sra. Dª. Susana Polo García, (RJ 2018\5855).
4. La información que está al alcance de todos los trabajadores (vide Auto núm. 562/2019 de 23 octubre de 2019 dictado por la Audiencia Provincial de Lleida (Sección 1ª), Ponente: Ilmo. Sr. D Víctor Manuel García Navascués, (JUR 2020\44384), Auto núm. 341/2023 de 14 junio de 2023 dictado por la Audiencia Provincial de Lleida, Sección 1ª, Ponente: Ilma. Sra. Dª María Ángeles Andrés Llovera (ECLI: ES:APL:2023:563A).
5. Asimismo, se excluyen las competencias y habilidades adquiridas por los trabajadores durante el curso de su carrera profesional (Preámbulo de la Ley 1/2019).

En el supuesto de hecho que se ha expuesto ab initio y sobre el que se ha ido desarrollando el presente artículo, se indicaba que la documentación que la persona trabajadora Sr. X había reenviado desde su correo corporativo a su correo personal era información alojada en la intranet de la empresa y que consistía en listados de clientes, proveedores, presupuestos y facturas.

La pregunta que nos debemos hacer es si esa información debe ser calificada de secreto de empresa, esto es, si reúne los requisitos de secreta, de tener valor comercial por ser precisamente secreta y de estar debidamente protegida.
La respuesta no es en absoluto sencilla, ya que debe atenderse a la casuística, debiéndose analizar cada caso en concreto.

La tendencia general de nuestros Tribunales es la de considerar que dentro del concepto de "secreto de empresa" debe incluirse "los datos comerciales, tales como la catalogación de productos, descripción gráfica, precios de adquisición y venta al pública, listado de proveedores y clientes" (vide Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, Núm. 285/2008, de 12 de mayo, Ponente: Ilmo. Sr. D. Francisco Monterde Ferrer).

Ahora bien, para tildar de "secreta" la información, deberá analizarse cómo se han confeccionado esos listados, quién tenía conocimiento de ellos, dónde se encontraban alojados, qué medidas de protección ha adoptado el titular del secreto empresarial para salvaguardar la información de terceros, entre otras.
Y es que no en todos los casos la lista de clientes e información sobre precios tiene la consideración de secreto de empresa (vide Sentencia núm. 539/2018 dictada por la Audiencia Provincial de Valencia, Sección 3ª, de fecha 14 de septiembre de 2018, ponente: Ilma. Sra. Mª Del Carmen Melero Villacañas – Lagranja).

Analizada una de las cuestiones nucleares de estos tipos delictivos, cual es el objeto material de los mismos, procedemos ahora a abordar las conductas penalmente típicas.

4. DELITO DE ESPIONAJE INDUSTRIAL

El art. 278 del CP tipifica el delito de espionaje industrial, previendo su tipo básico en el apartado primero y el tipo cualificado en el segundo.

La conducta típica se describe con los verbos "apoderarse por cualquier medio" de toda clase de objetos que se refieran al secreto empresarial, enumerando, a título meramente ejemplificativo, "datos, documentos escritos o electrónicos, soportes informativos u otros objetos que se refieran al mismo" o "emplear alguno de los medios o instrumentos señalados en el apartado 1 del art. 197".

Se trata de un tipo doloso que exige la concurrencia del elemento subjetivo del injusto, consistente en que la finalidad que guía la conducta sea la de "descubrir un secreto de empresa", siendo penalmente atípicos aquellos descubrimientos fortuitos o casuales.

Ese "ánimo de descubrir un secreto de empresa" ha sido interpretado como "un ánimo de divulgar" o como "un ánimo de conocer", siendo esta última interpretación la mayoritaria, implicando, la misma, el dejar fuera del círculo de posibles sujetos activos del delito aquellos sujetos que, aun cometiendo la conducta típica, tengan un conocimiento previo y lícito de la información confidencial.

Pese a que ésta es y ha sido la interpretación mayoritaria en la doctrina y la jurisprudencia, discrepa de la misma el Prof. Dr. Albert Estrada i Cuadras indicando, al respecto, lo siguiente: "Tal forma de interpretar el tipo obliga a dejar impune la conducta de quien, a pesar de tener acceso legítimo a la información, tiene prohibido su aseguramiento. (…) Cuando la complejidad del secreto ya sea por razones cualitativas o cuantitativas, impida o haga muy difícil su memorización, el aseguramiento ilegítimo de los soportes materiales por parte de quien tiene acceso legítimo a la información no es menos grave que el aseguramiento ilegítimo por parte de cualquier tercero".

Por lo tanto y siguiendo el criterio mayoritario, en el caso propuesto, se descarta, a priori, la aplicación de esta modalidad delictiva - art. 278.1 CP - dado que la

información que el Sr. X se reenvió a su cuenta de email personal era información a la que ya tenía acceso por razón de su cargo.

Debemos resaltar que la conducta de "apoderamiento" debe ser entendida tanto como apoderamiento material como apoderamiento intelectual, es decir, "el acceso al dato que permita conocer el secreto de empresa".

La consumación se sitúa con la conducta de "apoderamiento, interceptación o utilización de artificios técnicos", sin que se exija que concurra el efectivo descubrimiento del secreto, siendo admisible su ejecución en grado de tentativa.
El tipo cualificado previsto en el art. 278.2 CP parte de la siguiente premisa: los secretos empresariales ya han sido descubiertos por una persona que no tenía acceso a los mismos a través de alguna de las conductas que se tipifican en el apartado anterior y, con posterioridad a su descubrimiento, los "difunde, revela o cede" a terceros.

El delito se consuma cuando se lleva a cabo el acto de comunicación que tenga la potencialidad suficiente para lesionar la capacidad competitiva de la empresa, sin que sea necesaria la producción de ningún perjuicio.

Finalmente, debemos indicar que es doctrina mayoritaria el considerar que el tipo del art. 278. 2 CP no puede cometerse en grado de tentativa.

5. UTILIZACION O COMUNICACIÓN DE UN SECRETO POR PARTE DE UN SUJETO QUE TIENE ACCESO AL MISMO DE FORMA LICITA

El art. 279 CP tipifica el delito de violación del secreto de empresa por persona obligada a guardar reserva (terminología empleada por el Prof. Dr. Carlos Martínez – Buján Pérez) o de disposición desleal del secreto empresarial (Prof. Dr. Albert Estrada i Cuadras), o de utilización o comunicación de un secreto lícitamente conocido (Prof. Dr. Jacobo Dopico Gómez-Aller).
Se trata de un delito especial propio cuyo sujeto activo solo puede serlo el que "tuviere legal o contractualmente la obligación de guardar reserva".

La interpretación que se realiza de esta previsión no es unánime en nuestra jurisprudencia pues si bien una parte de ella se decanta por considerarla incluida dentro de las obligaciones genéricas derivadas de la buena fe contractual o del deber de diligencia previsto en el art. 5.a), otro sector considera que debe aplicarse de forma restrictiva, en aras a preservar el principio de taxatividad que debe regir en el Derecho Penal y, por lo tanto, estar específicamente recogida en el Convenio Colectivo o en el contrato laboral (vide Sentencia de la Audiencia Provincial de Barcelona, Sección 3ª, de fecha 7 de junio de 1999, ponente: Ilma. Sr. Luis Fernando Martínez Zapater; Auto núm. 113/2019 de la Audiencia Provincial de Barcelona (Sección 5ª), ponente: Ilma. Alicia Alcaraz Castillejos).

En cuanto a la obligación de guardar reserva, hay unanimidad en que ésta puede extenderse más allá de finalizada la relación laboral, debiendo analizar el caso en

concreto, por ejemplo, si se había firmado un pacto de confidencialidad con la correspondiente compensación económica, si la información puede seguir aportando un plus a la empresa competidora, etc.., no debiéndose confundir con un posible pacto de no competencia.

La conducta descrita en el art. 279 párrafo primero CP consiste en la "difusión, revelación o cesión" de un secreto de empresa a terceros por parte del sujeto que tiene "legal o contractualmente obligación de guardar reserva".

Se configura como un delito de peligro en el que su comisión requiere que las conductas de "difusión, revelación o cesión" comprometan la capacidad competitiva de la empresa sin requerir, para su consumación, la lesión de la misma, admitiéndose su comisión por omisión, así como su ejecución en grado de tentativa.

El párrafo segundo del art. 279 CP regula el segundo subtipo básico consistente en la utilización en provecho propio del secreto empresarial.

La condición del sujeto activo es la misma que la exigida en el párrafo anterior, debiéndose añadir que, este segundo subtipo, el sujeto obligado que infringe el deber es el sujeto al que la utilización del secreto debe reportar un beneficio.

La consumación del delito se produce en el momento en que el sujeto utiliza el secreto en provecho propio, siendo posible la ejecución en grado de tentativa (vide Sentencia núm. 17/2024 dictada por la Audiencia Provincial de Valencia, Sección 3ª, en fecha 7 de enero, ponente: Ilma. Sr. D. Lamberto Juan Rodríguez Martínez).

En el ejemplo que ha sido propuesto y que está siendo utilizado como hilo conductor, entendemos que este último tipo penal sería el cuestionable y ello, teniendo en cuenta los siguientes puntos:

- La información que el Sr. X se auto cede es conocida por el mismo por razón de su cargo.
- La información en cuestión, si entendemos que constituye un secreto de empresa, puede ser utilizada por el Sr. X en su nuevo puesto de trabajo, al tratarse de un cargo idéntico en una empresa competidora.
- El uso de esta información puede implicar un beneficio o provecho para el Sr. X.

No se puede ofrecer una contundente respuesta, ya que es preciso analizar el caso en concreto y, en base a sus particularidades, considerar si el tipo delictivo es o no aplicable.

6. APROVECHAMIENTO POR PARTE DE UN TERCERO DEL SECRETO ILICITAMENTE CONOCIDO

El elenco de delitos a analizar concluye con el tipo previsto en el art. 280 del CP llamado "delito de utilización o comunicación de un secreto ilícitamente conocido" (terminología utilizada por el Dr. Jacobo Dopico Gómez-Aller).

Las notas características son las siguientes:

- El sujeto activo realiza alguna de las conductas descritas en los delitos de los arts. 278 y 279 CP.
- No ha tomado parte en la tarea de descubrir el secreto.
- Conocía, empero, su origen ilícito.

Se trata de un delito común y de resultado, admitiendo la comisión en grado de tentativa.

Tal vez lo que resulta destacable de este tipo delictivo, por un lado, es la necesidad de delimitar si todas las conductas previstas en los arts. 278 y 279 CP pueden dar lugar al mismo y, por otro lado, si su comisión sólo puede ser dolosa o se admite la comisión por dolo eventual.

En cuanto a la primera cuestión planteada, la doctrina se divide al considerar que la remisión a los dos preceptos previos es completa y sin excepción, de aquellos autores que consideran que la remisión se limita a la conducta del art. 278.2 y 279 CP. En cuanto a la segunda cuestión planteada, hay unanimidad al considerar la posible comisión de este tipo delictivo por dolo eventual.

En el caso expuesto, la empresa competidora V podría ser llamada a un eventual procedimiento penal si se hubiera aprovechado de los secretos empresariales obtenidos por parte del Sr. X en relación con la empresa Z.

Para ello, deberán tenerse en cuenta circunstancias tales como: si la empresa V se ha dirigido a nuevos clientes que estaban dentro del listado de la empresa Z, si ha rebajado o utilizado precios como instrumento de captación, en definitiva, se trata de analizar qué comportamiento ha tenido la empresa V y si del mismo se desprende que ha podido aprovecharse de la información obtenida por el Sr. X.

7. RESPONSABILIDAD PENAL DE LA PERSONA JURIDICA

Finalmente, debemos hacer alusión a la tipificación expresa de la responsabilidad penal de la persona jurídica según dispone el art. 288 del CP.

De ahí la importancia de que la empresa disponga de un elaborado y completo plan de prevención de delitos, debidamente implementado, así como de una persona encargada de velar por su cumplimento.

8. CONCLUSION

Como conclusión, a los efectos de evitar una fuga de información por parte de las personas trabajadoras, es esencial que la empresa disponga de una política de uso de los medios tecnológicos, así como proteger, de forma adecuada, la información clasificada como confidencial.

Es decir, que no se escatime en adoptar las medidas de prevención necesarias para evitar supuestos como el analizado.

Desde un plano teórico laboral y penal, ello tendrá, ya de entrada, un efecto disuasorio para las propias personas trabajadoras ya que conocerán de la existencia de las limitaciones que les habrán sido impuestas por la propia empresa.

Finalmente, si se advierte alguna de las conductas descritas, la regulación específica de cómo gestionar los bienes tecnológicos puestos a disposición de las personas trabajadoras, la obligación de éstas a mantener la confidencialidad de la información que puedan manejar por razón de su cargo y la garantía de que las evidencias encontradas no puedan ser tachadas de ilícitas, permitirá, a su vez, que las eventuales acciones que la empresa se plantee entablar tengan visos de prosperar.

31 de octubre de 2025