EL DELITO DE REVELACIÓN DE SECRETOS EMPRESARIALES. DELIMITACIÓN JURISPRUDENCIAL: TIPICIDAD Y PRUEBA

CRIME OF DISCLOSURE OF TRADE SECRETS. JURISPRUDENTIAL DELIMITATION: CRIMINAL TYPICALITY AND EVIDENCE

CARLOS PEÑALOSA TORNÉ
Abogado asociado a Domingo Monforte Abogados
carlospenyalosa@josedomingomonforte.com

RESUMEN: Se analiza la tipicidad penal de la revelación de secretos empresariales: la delimitación del concepto secreto y la obligación legal o contractual de guardar reserva; la responsabilidad civil derivada de la revelación del secreto empresarial: alcance y concreción del daño; así como los requisitos jurisprudenciales exigidos para la validez probatoria de la información sobre el hecho típico obtenida por el acceso legítimo al ordenador del trabajador, sin vulneración de derechos fundamentales.

PALABRAS CLAVE: delito de revelación de secretos empresariales; responsabilidad civil; prueba ilícita.

ABSTRACT: The criminal typicality of the disclosure of trade secrets is analyzed: the delimitation of the concept of secret and the legal or contractual obligation to keep it confidential, the civil liability from the disclosure of the trade secret: the extent and concretion of the damage, as well as the jurisprudential requirements demanded for the evidentiary validity of the information on the typical fact obtained by the legitimate access to the worker's computer, without violating fundamental rights.

KEY WORDS: crime of disclosure of trade secrets; civil liability; unlawful evidence.

I. LA TIPICIDAD PENAL DE LA REVELACIÓN DE SECRETOS EMPRESARIALES

El *artículo 279 del Código Penal* refuerza la prevención y protección que la normativa mercantil [*Ley 3/1991, de 10 de enero, de Competencia Desleal y Ley 1/2019 de 20 de febrero de Secretos Empresariales*] garantiza sobre la leal competencia entre empresas, y en evitación de actos de revelación de secretos empresariales, dicho precepto prevé y castiga a quien, con obligación legal o contractual de guardar reserva, difunda, revele o ceda información secreta que, precisamente por su carácter secreto, pueda afectar y ponga en peligro la competitividad de la empresa, estableciendo en su apartado segundo un subtipo atenuado cuando la información se utiliza para uso propio.

Se configura el delito de revelación de secretos como un delito doloso, que exige para su comisión la concurrencia del elemento subjetivo del dolo –siquiera eventual– que se concreta en el conocimiento o la intención por parte del sujeto activo de cometer la acción típica, con el daño que ello representa para la competitividad de la empresa; y como un delito de peligro concreto, que no precisa para su consumación la producción de un resultado lesivo, sino que es suficiente con que la información secreta transmitida sea idónea para lesionar el bien jurídico protegido, que es la competencia leal entre empresas.

La norma penal protege el interés económico que el secreto encierra para la empresa y que si es descubierto aumenta la capacidad de competir de los rivales o disminuye la propia capacidad de la empresa cuyos secretos se difunden o emplean fuera de su ámbito.

Concentro mis reflexiones en los elementos del tipo que, a mí juicio, mayor tensión generan en la delimitación y concreción de la conducta típica y que son: de un lado, la interpretación del concepto "secreto de empresa" y de otro, en la medida en que estamos ante un delito especial propio, la obligación legal o contractual de guardar reserva, así como su duración; a la luz de la jurisprudencia que ha resuelto, no con unanimidad, las cuestiones de interpretación de la tipicidad que se plantean.

1. Interpretación y delimitación del concepto y elemento típico: "secreto de empresa"

Para colmar la tipicidad del hecho es necesaria la concurrencia del elemento objetivo "secreto de empresa" cuya interpretación es flexible y modulable bajo los parámetros y contornos establecidos en el *artículo 1 de la Ley 1/2019 de 20 de febrero de Secretos Empresariales* (en adelante LSE) que define y delimita el concepto en los siguientes términos: "*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, y c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto*".

Con anterioridad a la promulgación de la citada ley, la Sentencia del Tribunal Supremo (Penal) sec. 1ª, de 12 de mayo de 2008 [(nº 285/2008, rec. 1467/2007) Ponente: Excmo. Sr. D. Francisco Monterde Ferrer)] interpretó el concepto de secreto de empresa fijando sus límites y definiéndolos. Estimó la Sala que *"el Código Penal no define qué debemos entender por tal, seguramente por tratarse de un concepto lábil, dinámico, no constreñible en un "numerus clausus". Por ello, habremos de ir a una concepción funcional-práctica, debiendo considerar secretos de empresa los propios de la actividad empresarial, que de ser conocidos contra la voluntad de la empresa, pueden afectar a su capacidad competitiva. Así serán notas características: la confidencialidad (pues se quiere mantener bajo reserva); la exclusividad (en cuanto propio de una empresa); el valor económico (ventaja o rentabilidad económica; licitud (la actividad ha de ser legal para su protección). Y su contenido suele entenderse integrado, por los secretos de naturaleza técnico industrial (objeto o giro de empresa); los de orden comercial (como clientela, o marketing) y los organizativos (como las cuestiones laborales, de funcionamiento y planes de la empresa). Su materialización puede producirse en todo género de soporte, tanto papel como electrónico, y tanto en original como copia, y aún por comunicación verbal. Y cabe incluir tanto cifras, como listados, partidas contables, organigramas, planos, memorandums internos, etc."* [V. en este sentido, sobre el concepto de secreto de empresa, más reciente y con cita en esta Sentencia, la Sentencia del Tribunal Supremo de 20 de diciembre de 2018 [(nº resol. 679/2018) Ponente: Excma. Sra. Dña. Susana Polo].

Por su parte, tras la entrada en vigor de la LSE, la Audiencia Provincial de Madrid Sec. 23ª en Sentencia 17 de marzo de 2020 (nº 222/2020, rec. 126/2020) recordando la doctrina jurisprudencial del Tribunal Supremo sobre el concepto, y con cita en las anteriores resoluciones, concluye que: *"Nos encontramos ante un concepto jurídico penal funcionalizado a evitar comportamientos de competencia desleal que garanticen la capacidad competitiva de la empresa. Podemos así definir el secreto de empresa como toda información relativa a la empresa (técnico-industrial como fórmulas, operaciones o investigaciones de productos, comercial como listados de clientes, estratégica, relacional u organizativa, laboral, financiera, etc.) detentada con criterios de confidencialidad y exclusividad para asegurarse una posición optima en el mercado frente al resto de competidores, es decir, con entidad suficiente de afectar a la capacidad competitiva de la empresa, descartándose aquellas que pese a ser de conocimiento reservado carecen de esa capacidad de afectación".*

Se deduce por tanto que para la integración de una determinada información en el concepto típico "secreto de empresa", que se constituye como elemento objetivo y esencial del tipo, ha de atenderse a la circunstancias concretas del caso: la naturaleza propia de la información, su carácter reservado, esto es, que no sea fácilmente accesible por terceros y en especial, a la actividad de la mercantil y al valor competitivo de la información sobre ideas, productos o procedimientos que el empresario, precisamente por el valor competitivo para la empresa, decide mantener ocultos, siendo información exclusiva. Información que al ser divulgada o revelada será potencialmente lesiva para el bien jurídico protegido: la competencia leal entre las empresas.

Es precisamente por ello que, en la jurisprudencia menor, se encuentran pronunciamientos que integran el listado de clientes en el concepto "secreto de

empresa" mientras que otros lo descartan según el ámbito competitivo de la empresa. Es ilustrativa sobre este particular, la Sentencia de la Audiencia Provincial Valencia, sec. 3ª, de 14 de septiembre de 2018 (nº 539/2018, rec. 1365/2018) que confirma la absolución del acusado de un delito de descubrimiento y revelación de secretos de empresa al entender que, en este caso, la lista de clientes de la mercantil no tiene la consideración de secreto empresarial y con cita en la jurisprudencia del Tribunal Supremo y de las Audiencias Provinciales recuerda que "*las Audiencias Provinciales no mantienen unos criterios de decisión respecto a la condición secreta de las listas de clientes o precios y condiciones económicas de productos mercantiles, siendo diversos sus pronunciamientos, tal y como se expone, por ejemplo en la SAP Madrid, sec. 1ª, núm. 57/2016 de 16 de febrero, rec. 615/2015, en la que se afirma que "Es cierto que no siempre las Audiencias Provinciales y el Tribunal Supremo considera secreto de empresa la cartera de clientes para integrar el objeto del delito sino que se ha de atender a cada caso concreto".* (Respecto de la cartera de clientes, véase, en especial, la STS 864/2008, 16-12, siguiendo expresamente a la STS 285/2008, 12-5 en atención a su carácter reservado frente a terceros y su relación con la actividad de la mercantil).

Por su parte, la Sentencia de la Audiencia Provincial de A Coruña, Sec. 6ª, de 29 de junio de 2012 (núm. 80/2012, rec. 241/2012) sostuvo que los hechos enjuiciados no eran constitutivos de un delito del artículo 279 del Código Penal; afirmando que *"en éste concepto es cuestionable, pero admisible, que pueda constituir secreto de empresa el listado de clientes. Lo que no cabe considerar secreto de empresa es el conocimiento de los clientes que un trabajador haya adquirido como consecuencia del desarrollo de su actividad laboral o profesional"* Y matiza que *"la naturaleza secreta de la "lista de clientes" puede permitir la calificación como delictiva la conducta de quien utiliza una lista de esa naturaleza en provecho propio, lo que requiere la previa obtención y apoderamiento de esa lista. Pero no cabe confundir "lista de clientes" con el conocimiento personal de algunos de los clientes que obtiene un trabajador en el desempeño de su labor. Éste conocimiento adquirido por el trabajador que se ha dedicado a la comercialización de los productos de una compañía es personal y no constituye un secreto de empresa. De su uso, con perjuicio para la empresa, pueden proteger las normas legales o contractuales que vedan la concurrencia en la actividad durante la relación laboral o una vez esta ha concluido. Normas que contienen las correspondientes sanciones, laborales o civiles, ajenas al orden penal".*

En consecuencia, el criterio determinante de la tipicidad penal del hecho estará en la calificación de la información revelada, en su carácter reservado y su modo de obtención y conocimiento, así como en la idoneidad de dicha información para poner en peligro la competencia entre empresas, en atención a su contenido y su influencia en el tráfico o mercado en el que se opera.

2. La obligación legal o contractual de guardar reserva y su límite temporal

El segundo de los elementos exigidos por el tipo penal, es la especial condición del sujeto activo, en cuanto a la necesidad de que éste tenga el deber legal o contractual de guardar reserva, sin perjuicio de la responsabilidad del tercero (*extraneus*) según su grado de participación. Por ello, resulta imprescindible determinar si el empleado de una empresa tiene tal obligación por su condición de trabajador, o si por el contrario se exige una expresa y previa cláusula de confidencialidad o de no concurrencia.

En mi opinión, en la medida en que constituye un deber básico y esencial de todo trabajador *ex lege* [*artículos 5. a) y 20.2 del Estatuto de los Trabajadores*] el cumplimiento de sus obligaciones concretas de su puesto de trabajo de conformidad con las reglas de la buena fe y diligencia, es suficiente este deber genérico de buena fe impuesto en el Estatuto de los Trabajadores, sin necesidad de una cláusula contractual de previsión expresa sobre la no concurrencia o no competencia del trabajador.

No obstante, sobre este particular existen también criterios dispares en la jurisprudencia. Así, el Auto de la Audiencia Provincial de Madrid de 18 de febrero de 2009 59/2009, consideró que *"la obligación de guardar reserva, si es expresa convierte al sujeto en garante de protección, pero si es genérica —la derivada de la buena fe y de la diligencia a la que alude el art. 5 a) del ET— sólo dará lugar a una infracción de deberes genéricos originadora, en su caso, de una responsabilidad civil"*. Y a la misma conclusión parece que llega la ya citada Sentencia del Tribunal Supremo de 20 de diciembre de 2018 (ponente: Exma. Sra. Dña. Susana Polo).

Distinto es el criterio –que comparto y considero acertado- seguido por la Sentencia de la Audiencia Provincial de Valencia de 7 de enero de 2014 (nº de Recurso: 362/2013, nº de Resolución: 17/2014) que con cita en la Sentencia del Tribunal Supremo citada *ut supra* (Ponente: Exmo. Sr. Francisco Monterde) considera que es suficiente el deber genérico de buena fe impuesto en el Estatuto de los Trabajadores: *"Y en cuanto a esa obligación de guardar reserva, entiende el apelante, con apoyo en algunas resoluciones de Audiencias Provinciales, que tiene que venir impuesta por una específica cláusula contractual (que no se da en este caso) o por una norma legal específica, no bastando con la obligación legal de reserva que impone el Estatuto de los Trabajadores porque ello supondría una interpretación extensiva contraria a la naturaleza penal del precepto.*

Sin embargo, como acertadamente señala el Juzgador de instancia, el Tribunal Supremo ha optado expresamente por esa interpretación que rechaza el apelante.

(…) En la misma línea, la sentencia de fecha 16-12-2008, nº 864/2008, estima cometido el delito por quien "como todo trabajador estaba obligado por su relación laboral a una conducta de reserva respecto de esa lista de clientes que conocía por tal condición".

De este modo, aunque pueda ser razonable la tesis sostenida por el apelante, la doctrina establecida por el Tribunal Supremo es clara y basta con la obligación legal de reserva impuesta a todos los trabajadores para que quede integrado el delito previsto en el artículo 279 del Código penal, sin necesidad, como pretende el apelante, de que esa obligación sea reiterada por otra disposición legal o por una cláusula contractual que redunden en imponer una prohibición de divulgar los secretos de empresa que las normas legales citadas ya establecen para todos los trabajadores"

Sobre la limitación temporal del deber de guardar secreto tampoco existe un criterio jurisprudencial uniforme. Para determinar la duración de la obligación de guardar secreto se ha de estar a la fuente del deber de reserva, esto es, a la norma o al contrato.

Pudiera considerarse que, en la medida en que el pacto de no competencia para después de extinguido el contrato de trabajo, no puede tener una duración superior a 2 años para los técnicos y de 6 meses para los demás trabajadores, y solo es válido si el empresario tiene un efectivo interés industrial o comercial en ello; y si compensa económicamente al trabajador, dicho deber de reserva tendría en los casos de pacto de no competencia una limitada duración de 2 años o 6 meses y, ante la ausencia de cláusula quedaría únicamente obligado a guardar reserva hasta la extinción del contrato.

Sin embargo, en la jurisprudencia del Tribunal Supremo -todavía cuantitativamente limitada en esta materia- parece ampliarse el deber de sigilo independientemente de la finalización de la relación jurídica.

Sobe esta cuestión también se ha pronunciado la Sentencia del Tribunal Supremo de 12 de mayo de 2008 (nº 285/2008, rec. 1467/2007. Ponente: Excmo. Sr. Monterde Ferrer) que consideró que: *"El deber de reserva, no terminó con el fin de la relación laboral, como pretende el recurrente. El tipo del art. 279 aplicado, se caracteriza por la infracción de un deber extrapenal específico de guardar secreto que, -según entiende la doctrina- independientemente de la eventual cláusula de duración contractual determinada, se encuentra vigente, respecto de las personas que cesan en la empresa, mientras esté en condiciones de aportar un valor económico. Y, en este supuesto, a ello se añade el compromiso -pactado por el recurrente, explícitamente, con la empresa- más allá de la extinción laboral, prolongándose durante dos años a partir de tal cese.*

El recurrente incurrió en la conducta típica de cesión (dentro de la que, sin duda hay que incluir la autocesión) de un secreto de empresa, contraviniendo la obligación legal que como fuente de la reserva, le venía impuesta por su condición de empleado de la empresa y por su contrato laboral, accediendo -también con toda lógica- a tal información durante la vigencia del contrato y antes de extinguirse la relación laboral. Ello tal como revela el factum, al decir que: "como empleado de la empresa "Industrias de Fijación Técnica, S.A.", con la categoría de Director Comercial, cuyas relaciones laborales se extinguieron en 31-10-2001 abrigando la idea -junto con otros dos acusados- de instalarse por su cuenta, recopiló datos comerciales de la empresa, tanto en papel como en ficheros informáticos a los que tenía acceso en el ejercicio de su funciones propias, con objeto de servirse de ellos a través de la empresa que constituyeran, y que aprovecharía aquella información para instalarse con fuerza en el mercado, en clara competencia con "Técnica"".

II. ACCIONES CIVILES DE REPARACIÓN DEL DAÑO. SU VALORACIÓN, DELIMITACIÓN Y ALCANCE

Sin perjuicio de lo anterior, y sin ánimo de exhaustividad en cuanto al desarrollo de las acciones civiles previstas en la normativa mercantil en esta materia que no son objeto de este trabajo, debe tenerse en cuenta que junto con la acción penal podrán ejercitarse en el mismo proceso penal –o reservarse para ulterior proceso civil– las acciones civiles previstas en la *LSE*, sin que las acciones ejercitadas pierdan su naturaleza civil al ejercitarse en el marco del proceso penal. De igual modo podrán

solicitarse en el proceso penal de acuerdo con el *art. 13 de la Ley de Enjuiciamiento Criminal* las medidas cautelares previstas en la *Ley de Patentes y Marcas* a la que se remite la *LSE* tendentes a limitar los efectos del daño y garantizar la eficacia de las acciones civiles.

Acciones civiles en defensa de la leal competencia y de resarcimiento del daño derivado de la divulgación o cesión de secretos de empresa que vienen recogidas en el *artículo 9 de la LSE* que establece las siguientes: a) La declaración de la violación del secreto empresarial. b) La cesación o, en su caso, la prohibición de los actos de violación del secreto empresarial. c) La prohibición de fabricar, ofrecer, comercializar o utilizar mercancías infractoras o de su importación, exportación o almacenamiento con dichos fines. d) La aprehensión de las mercancías infractoras, incluida la recuperación de las que se encuentren en el mercado, y de los medios destinados únicamente a su producción, siempre que tal recuperación no menoscabe la protección del secreto comercial en cuestión, con una de las siguientes finalidades: su modificación para eliminar las características que determinen que las mercancías sean infractoras, o que los medios estén destinados únicamente a su producción, su destrucción o su entrega a entidades benéficas. e) La remoción, que comprende la entrega al demandante de la totalidad o parte de los documentos, objetos, materiales, sustancias, ficheros electrónicos y cualesquiera otros soportes que contengan el secreto empresarial, y en su caso su destrucción total o parcial. f) La atribución en propiedad de las mercancías infractoras al demandante, en cuyo caso el valor de las mercancías entregadas podrá imputarse al importe de la indemnización de daños y perjuicios debida, sin perjuicio de la subsistencia de la responsabilidad del infractor en lo que se refiere a la cuantía indemnizatoria que exceda del referido valor. Si el valor de las mercancías excede del importe de la indemnización, el demandante deberá compensarlo a la otra parte. g) La indemnización de los daños y perjuicios, si ha intervenido dolo o culpa del infractor, que será adecuada respecto de la lesión realmente sufrida como consecuencia de la violación del secreto empresarial. h) La publicación o difusión completa o parcial de la sentencia, que deberá preservar en todo caso la confidencialidad del secreto empresarial en los términos previstos en el *artículo 15 de la LSE*.

Respecto de la acción de indemnización de los daños y perjuicios, éstos deberán ser probados y concretados por la acusación, perjudicada por la revelación de secretos empresariales. En este sentido, sirve de ejemplo la Sentencia de la Audiencia Provincial de Barcelona, de 13 de enero de 2009 (nº 13/2009, rec 129/2008) que fija con claridad la necesidad de probar el daño derivado del acto desleal y su la traducción económica. En este caso, la mercantil no probó el daño y, pese a que se condenó a la publicación en dos revistas del sector tales acciones desleales, no se obtuvo una condena por daños y perjuicios. (En igual sentido Sentencia Tribunal Supremo, Sala Primera, de lo Civil, del 14 de julio de 2003, (nº. 714/2003, Rec. 3589/1997)].

Por último, en cuanto a la cuantificación y valoración de los daños y perjuicios derivados de la revelación de secretos, el *artículo 10 de la LSE* establece las partidas indemnizatorias: los perjuicios económicos, incluido el lucro cesante que haya sufrido

el titular del secreto empresarial, el enriquecimiento injusto obtenido por el infractor y, cuando proceda, otros elementos que no sean de orden económico, como el perjuicio moral causado al titular del secreto empresarial por su obtención, utilización o revelación ilícitas. También podrán incluirse, en su caso, los gastos de investigación en los que se haya incurrido para obtener pruebas razonables de la comisión de la infracción objeto del procedimiento judicial.

Daños y perjuicios que, para su concreción y cuantificación, precisará de un informe pericial como prueba adecuada en juicio en el análisis del alcance y determinación.

III. LA PRUEBA EN JUICIO: LA VALIDEZ DE LA PRUEBA OBTENIDA MEDIANTE EL ACCESO A LOS DISPOSITIVOS ELECTRÓNICOS DE EMPRESA ASIGNADOS AL TRABAJADOR PARA EL DESARROLLO DE SUS FUNCIONES LABORALES

En la práctica es frecuente que, la comisión del delito de revelación de secretos empresariales se lleve a cabo por parte de un socio o trabajador de una empresa que filtra información susceptible de considerarse secreto empresarial por su valor económico y competitivo, utilizando para ello el ordenador, el correo electrónico, el teléfono móvil u otros medios informáticos de empresa, cuya utilización es asignada al trabajador para el desarrollo de sus funciones laborales.

Se plantea la posibilidad de acceso por el empresario a los dispositivos tecnológicos de empresa asignados al trabajador en el ejercicio de su función fiscalizadora y de control, con el objeto de obtener la prueba del hecho delictivo: la divulgación y revelación de información, sin que dicho acceso suponga una vulneración del derecho fundamental a la intimidad del trabajador invalidante de la prueba.

La cuestión sobre la nulidad de la prueba obtenida por el empresario tras un examen y análisis del ordenador o correo electrónico del trabajador ha sido resuelta en la jurisprudencia social, penal y constitucional.

En este sentido, el Tribunal Constitucional en Sentencia 170/2013, de 7 de octubre [nº 170/2013, Rec. 2907/2011 (BOE núm. 267, de 07 de noviembre de 2013)] realiza un análisis de la licitud del medio de prueba, admitiendo como medio lícito de prueba en un proceso de despido la aportación de la empresa del contenido de determinados correos electrónicos del trabajador cuya obtención tuvo lugar mediante el acceso a un ordenador portátil de la empresa en cuyos correos electrónicos éste había remitido información susceptible de considerarse secreto. Considera el Alto Tribunal que esta actuación fue adecuada por cuanto el propio Convenio aplicable preveía la exclusiva utilización del ordenador a fines laborales, lo que ex *art. 20. 3 ET* posibilitaba el acceso, en el ejercicio de la función fiscalizadora y de control por parte de la empresa al no existir una expectativa fundada y razonable de confidencialidad en base al régimen de la empresa. Asimismo, concluye que la medida fue justificada por existir sospechas, fue idónea y proporcional para la finalidad pretendida, necesaria y

equilibrada, lo que conlleva la legitimidad en el acceso y la licitud de la prueba obtenida.

En este supuesto, el demandante venía prestando servicios laborales para la empresa con categoría profesional de jefe de primera administrativo. Con fecha 17 de octubre de 2008, la empresa notificó al recurrente carta de despido disciplinario por transgresión de la buena fe, en la que, entre otros hechos, le imputaba haber mantenido durante mucho tiempo una conducta de máxima deslealtad por haber proporcionado indebidamente información confidencial de la empresa a personal de otra entidad mercantil, sin haber pedido nunca autorización para ello y utilizando en dicha transmisión medios que eran propiedad de la empresa —en concreto, teléfono móvil y correo electrónico—. De manera específica, desde el correo electrónico de la empresa, el demandante había transmitido todos los datos relativos a la previsión de la cosecha de 2007 y 2008 a esa otra entidad, incluyendo extremos especialmente sensibles de cuya importancia era conocedor, por lo que no debían transmitirse en ningún caso a nadie de fuera de la empresa.

El demandante impugnó en amparo la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Madrid de 27 de abril de 2010, por considerar que la interpretación realizada por esta resolución respecto a la admisibilidad de las pruebas en que la empresa fundaba su despido resultaba contraria a sus derechos a la intimidad personal (art. 18.1 CE) y al secreto de las comunicaciones (art. 18.3 CE). El recurrente denunció la lesión de estos derechos por entender que la empresa se extralimitó en sus facultades de fiscalización cuando, no habiendo informado previamente sobre las reglas de uso y control de las herramientas informáticas de la entidad, procedió a interceptar de forma ilícita el contenido de sus correos electrónicos registrados en el ordenador facilitado por la empresa. A su juicio, resultaba a tal efecto insuficiente que el convenio colectivo aplicable previera como infracción leve de los trabajadores la utilización de los medios informáticos propiedad de la empresa para fines distintos de los relacionados con la prestación laboral.

El caso fue resuelto previamente por el Tribunal Superior de Justicia de Madrid que desestimó la nulidad de la prueba, razonando que: *"El art. 59.11 del Convenio colectivo de la industria química aplicable a las partes tipificaba como falta leve sancionable la utilización de los medios informáticos propiedad de la empresa para fines distintos de los relacionados con la prestación laboral. Dado que esta prohibición del Convenio no hacía referencia a los teléfonos móviles, la Sentencia entendió que, al no haber establecido previamente la empresa las reglas sobre su uso y control, las pruebas obtenidas de los mensajes de texto del teléfono móvil proporcionado al trabajador debían ser rechazadas por resultar contrarias a su derecho a la intimidad. Por el contrario, la citada prohibición convencional sí alcanzaba al uso del correo electrónico, y puesto que el trabajador debía conocer el Convenio y no constaba que esa limitación hubiera sido levantada por la empresa, la Sentencia concluyó que no era preciso que la empresa estableciera previamente las reglas de uso de los medios informáticos; estaba pues legitimada para comprobar su utilización y las comunicaciones realizadas a través de ellos, sin vulnerar el derecho a la intimidad del trabajador. En consecuencia, probado que el trabajador había remitido a terceros —en particular, a la cuenta de otra empresa— información detallada sobre la previsión de la cosecha de 2007 y 2008 desde el correo electrónico de*

la empresa demandada, sin contar con autorización para ello, la Sentencia concluyó que, tratándose de datos confidenciales y de obligada reserva, la conducta constituía un supuesto de transgresión de la buena fe contractual, razón por la que declaró la procedencia del despido".

La Sentencia del Tribunal Constitucional que resolvió sobre el recurso de amparo concluye que*: "Conforme al presupuesto admitido en la Sentencia impugnada, este contenido del Convenio colectivo —en concreto, se refiere al indicado art. 59.11— resultaba aplicable a la empresa Alcaliber, S.A., y al trabajador demandante; de ahí que, en virtud de lo establecido en el art. 82.3 del texto refundido de la Ley del estatuto de los trabajadores (LET), haya de entenderse que ambas partes quedaban obligadas a lo allí dispuesto. En atención al carácter vinculante de esta regulación colectivamente pactada, cabe concluir que, en su relación laboral, sólo estaba permitido al trabajador el uso profesional del correo electrónico de titularidad empresarial; en tanto su utilización para fines ajenos al contenido de la prestación laboral se encontraba tipificada como infracción sancionable por el empresario, regía pues en la empresa una prohibición expresa de uso extralaboral, no constando que dicha prohibición hubiera sido atenuada por la entidad. Siendo este el régimen aplicable, el poder de control de la empresa sobre las herramientas informáticas de titularidad empresarial puestas a disposición de los trabajadores podía legítimamente ejercerse, ex art. 20.3 LET, tanto a efectos de vigilar el cumplimiento de la prestación laboral realizada a través del uso profesional de estos instrumentos, como para fiscalizar que su utilización no se destinaba a fines personales o ajenos al contenido propio de su prestación de trabajo.*

En tales circunstancias, de acuerdo con la doctrina constitucional expuesta, cabe entender también en el presente supuesto que no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa y que habían quedado registradas en el ordenador de propiedad empresarial. La expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, incluida la adecuación de su prestación a las exigencias de la buena fe [arts. 5 a) y 20.2 y 3 LET]. En el supuesto analizado la remisión de mensajes enjuiciada se llevó pues a cabo a través de un canal de comunicación que, conforme a las previsiones legales y convencionales indicadas, se hallaba abierto al ejercicio del poder de inspección reconocido al empresario; sometido en consecuencia a su posible fiscalización, con lo que, de acuerdo con nuestra doctrina, quedaba fuera de la protección constitucional del art. 18.3 CE"

En el orden jurisdiccional penal –que es el aquí nos interesa-, es de obligada cita por su claridad expositiva la Sentencia del Tribunal Supremo de 23 de octubre de 2018 [(nº 489/2018, Rec. 1674/2017) Ponente: Excmo. Sr. D. Antonio del Moral) que sintetiza el desarrollo e interpretación jurisprudencial sobre la licitud de la prueba derivada de un acceso al ordenador de empresa.

La Sala Segunda del Tribunal Supremo estimó el recurso de casación, considerando nulo el material probatorio obtenido del acceso al ordenador del trabajador, anulando la Sentencia y acordando retrotraer las actuaciones. De la sentencia se extrae el siguiente contenido relevante: *"Hito reciente y extremadamente relevante de la jurisprudencia recaída en esta materia viene constituido por STEDH de 5 de septiembre de 2017 (Gran Sala):*

asunto Barbulescu. Es invocada por el recurrente. Otras sentencias posteriores del mismo órgano, inciden también en esta temática aunque de forma oblicua (videovigilancias: SSTEDH de 28 de noviembre de 2017 asunto Antori and Murkon de 9 de enero de 2018 asunto López Ribalde; o también examen de un ordenador, asunto Libert, STEDH de 22 de febrero de 2018).

No puede decirse que la sentencia Barbulescu sea totalmente rupturista con los criterios que han ido cristalizando en nuestra jurisprudencia, someramente reseñada. Pero aporta y concreta al establecer con diáfana claridad parámetros de inexcusable respeto empujando a nuevas modulaciones y matizaciones que ya han aparecido en la jurisprudencia laboral (STS -Sala 4ª- 119/2018, de 8 de febrero, que realiza una síntesis clara e íntegramente trasladable al ámbito penal del estado de la cuestión tras Barbulescu). Acudiendo a la clásica técnica, se habla de la insoslayable necesidad de ponderar los bienes en conflicto. De una parte, el interés del empresario en evitar o descubrir conductas desleales o ilícitas del trabajador. Prevalecerá solo si se atiene a ciertos estándares que han venido a conocerse como el test Barbulescu. Se enuncian criterios de ponderación relacionados con la necesidad y utilidad de la medida, la inexistencia de otras vías menos invasivas; la presencia de sospechas fundadas... Algunos se configuran como premisas de inexcusable concurrencia. En particular, no cabe un acceso inconsentido al dispositivo de almacenamiento masivo de datos si el trabajador no ha sido advertido de esa posibilidad y/o, además, no ha sido expresamente limitado el empleo de esa herramienta a las tareas exclusivas de sus funciones dentro de la empresa (los usos sociales admiten en algún grado y según los casos, como se ha dicho, el empleo para fines personales, creándose así un terreno abonado para que germine una expectativa fundada de privacidad que no puede ser laminada o pisoteada).

El resto de factores de ponderación entrarán en juego para inclinar la balanza en uno u otro sentido solo si se cuenta con ese presupuesto. En otro caso, habrá vulneración aunque exista necesidad, se use un método poco invasivo, etc... Esta es la clave que nos permite resolver este asunto. Podrían existir razones fundadas para sospechar y entender que el examen del ordenador era una medida proporcionada para esclarecer la conducta desleal y evaluar los perjuicios. Se buscó, además, una fórmula lo menos invasiva posible. Pero faltaba un prius inexcusable.

Si existiese esa expresa advertencia o instrucción en orden a la necesidad de limitar el uso del ordenador a tareas profesionales, (de la que en podría llegar a derivarse una anuencia tácita al control o, al menos, el conocimiento de esa potestad de supervisión) y/o además alguna cláusula conocida por ambas partes autorizando a la empresa a medidas como la aquí llevada a cabo; o, si se hubiese recabado previamente el consentimiento de quien venía usando de forma exclusiva el ordenador (en caso de negativa, nada impedía recabar la autorización necesaria) pocas dudas podrían albergarse sobre la legitimidad de la actuación indagatoria llevada a cabo por la empresa. Pero en las circunstancias en que se llevó a cabo hay que afirmar que el ordenamiento ni consiente, ni consentía en la fecha de los hechos, tal acción intrusiva por ser lesiva de derechos fundamentales.

Lo que vicia la prueba es el acceso no legítimo. En esto hay que dar la razón al recurrente.

Es indiferente a esos efectos que luego no aparezcan datos vinculados materialmente a la intimidad; o que todo lo que se examinase careciese de calidad para ser protegido por su enlace directo con actividades delictivas; o incluso que se tratase en su totalidad de información que tuviese derecho a conocer la querellante, como titular del negocio. Las comunicaciones y determinados espacios de

privacidad (el domicilio, los aparatos de almacenamiento masivo de datos) se blindan legalmente con murallas que constituyen la materialización de la protección del derecho fundamental, abstracción hecha de que en concreto se identifique una violación material de la intimidad.

(…) La valoración de la legitimidad de la actuación inicial (acceso al ordenador que usaba el querellado) no puede hacerse más que mediante un juicio ex ante. A esos efectos es indiferente que solo se hayan buscado elementos que tuvieran relación con la actividad mercantil de la empresa o que se haya eludido cuidadosamente adentrarse en cualquier archivo o comunicación en la que se percibiese el más mínimo aroma de vinculación con la intimidad o la privacidad. Esto, que solo es posible dilucidar en un juicio ex post, no cambia ni puede cambiar la valoración que se hace ex ante. (…) La jurisprudencia ha situado la clave de la legitimidad de la injerencia empresarial en la ausencia de toda expectativa de confidencialidad por parte del trabajador que sufre la intromisión que puede basarse en una cláusula contractual o en una advertencia del empresario o en la legítima instrucción expresa de limitar el uso del dispositivo a fines laborales. La existencia de un precepto incorporado al convenio del sector donde se prohíbe el uso personal de los instrumentos informáticos, la suscripción de una cláusula que reserva al empresario esa facultad o, en fin, la comunicación, por uno u otro medio, del uso de mecanismos tecnológicos de fiscalización, difuminan el espacio de exclusión del trabajador.

Sin embargo, en el caso presente, a la vista de la jurisprudencia existente y predominante en el momento de la actuación empresarial cuya licitud fiscalizamos ahora, se podía y debía haber extremado la cautela: no existiendo advertencia de que el ordenador había de ser usado exclusivamente para los fines de la empresa y no constando al empleado que la empresa se reservaba la potestad de su examen, por mucho que se utilizasen métodos informáticos especialmente poco invasivos y selectivos, constituía un cierto atrevimiento (una indiligencia), no recabar antes el consentimiento del titular o, en su defecto, la autoridad judicial. Regía ya un cuerpo de doctrina jurisprudencial que alertaba sobradamente sobre la dudosa legalidad de esa actuación. Algo de osadía se aprecia en la iniciativa adoptada por la empresa. La prueba no es rescatable; no puede utilizarse".

El mismo criterio sigue la reciente Sentencia de la Audiencia Provincial de Valencia, sec. 2ª, de 20 de febrero de 2020, (nº 94/2020, rec. 367/2019) que considera la prueba ilícita por haber sido obtenida ante la legítima expectativa de privacidad que tenía el querellado en cuanto al uso de su correo personal, no habiéndose probado por las acusaciones que se hubiera advertido expresamente al trabajador de la posibilidad de revisar: "*No obstante, sí queremos llamar la atención acerca del hecho de que consideramos que la aportación de los correos remitidos a los otros dos acusados por Fulgencio desde su cuenta personal de hotmail sí incurre en un vicio insalvable de nulidad por infracción del derecho al secreto a las comunicaciones del artículo 18.3 de la Constitución. Pues bien, en este caso, no se acredita por las acusaciones que se hubiera advertido expresamente al Sr Fulgencio por parte de GEDESCO de la posibilidad de revisar los correos remitidos desde los ordenadores de la empresa, ni que se suscribiera con el mismo cláusula alguna que permitiera la revisión de su cuenta de correo personal lo que convierte en ilícita la prueba obtenida ante la legítima expectativa de privacidad que tenía el querellado en cuanto al uso de su correo personal".*

En síntesis, de la jurisprudencia penal expuesta se deduce que, el criterio establecido sobre la facultad de acceder al ordenador o datos informáticos del trabajador de

forma lícita y por tanto sin vulneración de derechos fundamentales, se centra en la previa advertencia al trabajador sobre la legítima posibilidad de examen, control y vigilancia que puede establecerse en una cláusula contractual, en una advertencia realizada por el empresario consistente en la instrucción expresa de limitar el uso del dispositivo a fines laborales o en el convenio sectorial aplicable, del que se desprenda que el uso del ordenador o medios informáticos no puede ser utilizado a fines propios, lo que excluye la expectativa de confidencialidad.

Esto es, si previamente el trabajador conoce y acepta la posibilidad de que se acceda a su ordenador o se le advierte de que no puede usarlo para otros fines, el acceso con objeto de control y vigilancia estaría justificado.

La clave de la legitimidad de la injerencia empresarial está en la ausencia de toda expectativa de confidencialidad. La ilegitimidad no deriva de la naturaleza del contenido obtenido, ni de la forma más o menos intrusiva, sino del mismo acceso inconsentido y no advertido previamente, que no puede excusarse en la existencia de sospechas.

En definitiva, la falta de previsión impedirá a la empresa el acceso a los medios o dispositivos asignados al trabajador y podrá suponer la vulneración del derecho fundamental a la intimidad o secreto de las comunicaciones que conllevará la expulsión de la prueba obtenida, derivada del acceso inconsentido.

IV. CONCLUSIONES

1. La normativa penal pretende evitar la difusión, revelación y cesión de secretos de empresa, reforzando así la tutela que ofrece la normativa mercantil [*Ley 3/1991, de 10 de enero, de Competencia Desleal y Ley 1/2019 de 20 de febrero de Secretos Empresariales*] en garantía de un correcto funcionamiento del mercado con base en la leal competencia entre empresas y en último término en los intereses de los consumidores.

2. El delito de revelación de secretos empresariales previsto y penado en el *artículo 279 del Código Penal* se configura como un delito especial propio, de peligro concreto y doloso, cuyo bien jurídico protegido es la competencia leal entre las empresas.

3. La adecuada integración de la conducta en el tipo penal analizado exigirá la concurrencia en el sujeto activo –normalmente trabajador o socio de la mercantil- del elemento subjetivo doloso que se colma con el conocimiento del inadecuado proceder en la revelación de secretos, así como su obligación legal o contractual de guardar reserva y en concreto, que la información revelada sea considerada "secreto de empresa" [elemento objetivo, nuclear y esencial del tipo] de acuerdo con las notas definitorias y delimitadoras del concepto que establece la Ley de Secretos

Empresariales que deberán relacionarse con la naturaleza de la información y el mercado en que opera la mercantil titular del secreto revelado.

Extremos que permitirán deducir, mediante un juicio de idoneidad, si el secreto revelado es susceptible de poner en riesgo concreto el bien jurídico protegido: la competencia leal entre empresas, sin necesidad de que la acción típica se concrete en un perjuicio cierto, concreto y evaluable.

4. Junto al ejercicio de la acción penal podrá ejercitarse en el mismo proceso, sin que por ello pierdan su naturaleza civil, las acciones y medidas cautelares previstas en la legislación mercantil.

5. El acceso a los dispositivos electrónicos para la obtención de la prueba sobre el hecho, a título de ejemplo: el ordenador, teléfono móvil y correo electrónico asignado al trabajador para el desarrollo de sus funciones, será legítimo siempre que el trabajador, mediante previa cláusula contractual, instrucción del empresario o previsión en el Convenio Sectorial aplicable, conozca que su utilización es exclusivamente para fines laborales, lo que de suyo conllevará la ausencia de toda expectativa de confidencialidad y exclusividad, y posibilitará el acceso en ejercicio de las facultades fiscalizadoras del empresario, así como la utilización de la prueba en juicio legítimamente obtenida.

6. En mi opinión, y con ello concluyo y cierro mis reflexiones, asistimos a una proliferación y expansión del Derecho Penal, discutible en términos de política legislativa, por cuanto las conductas desleales que prevé y castiga el *artículo 279 del Código Penal* encuentran respuesta en la normativa civil y mercantil.

Estimo que, en defensa de los intereses de la empresa que ha soportado una revelación de secretos con los perjuicios que ello representa, la vía de opción procesal por el menor riesgo y por su eficacia coactiva será generalmente el proceso penal, en el que podrán ejercitarse las acciones civiles de reparación del daño y en su caso las medidas cautelares en evitación de que se perpetúen los efectos del delito.