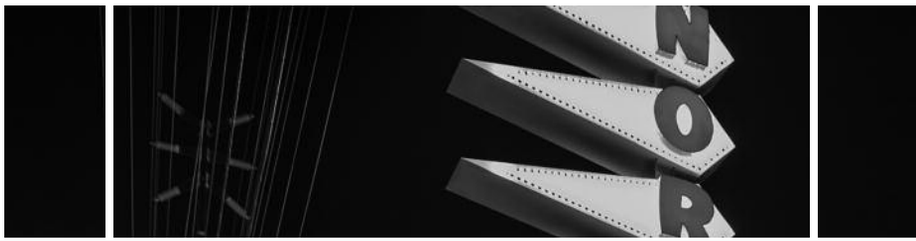
studia



FRANCISCA RAMÓN FERNÁNDEZ

Secretos empresariales en documentos y ficheros electrónicos y la protección de datos personales y garantía de los derechos digitales

Business secrets in electronic records and files and the personal data protection and guarantee of digital rights

Francisca Ramón Fernández
frarafer@urb.upv.es
Universitat Politècnica de València

Citación: Ramón Fernández, Francisca (2019). "Secretos empresariales en documentos y ficheros electrónicos y la protección de datos personales y garantía de los derechos digitales". *Tábula,* n. 22, pp. 73-92

Recibido: 1-4-2019. Aceptado: 9-9-2019

Resumen analítico / Analitic summary

Se analiza la relación existente entre los documentos y ficheros electrónicos que contienen secretos empresariales y la protección de datos de carácter personal, a través del análisis de la principal legislación aplicable como es la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Se atenderá a la casuística referente a la prestación del consentimiento, confidencialidad y derecho a la información. Los resultados nos determinarán si la legislación resulta adecuada y las lagunas e incertidumbres que la normativa no resuelve.

DOCUMENTOS | FICHEROS ELECTRÓNICOS | SECRETOS EMPRESARIALES | PROTECCIÓN DE DATOS | DERECHO A LA INFORMACIÓN

The relationship between electronic documents and files containing business secrets and the protection of personal data is analyzed, through the analysis of the main applicable legislation such as Law 1/2019, of February 20, on Business Secrets, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, and Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights. The casuistry regarding the provision of consent, confidentiality and right to information will be addressed. The results will determine if the legislation is adequate and the gaps and uncertainties that the regulation does not resolve.

DOCUMENTS | ELECTRONIC FILES | BUSINESS SECRETS | DATA PROTECTION | RIGHT TO INFORMATION

En el ámbito de la transferencia de conocimiento y la innovación, la protección de ésta última se enmarca tanto a través de la propiedad intelectual e industrial respecto de cada uno de los derechos que se aplican (Ramón, 2015, p. 41; Flores, 2017, p. 57). La relación con la competitividad y la protección de la información es innegable y los conocimientos abarcan no sólo el área tecnológica y científica (Rabasa, 2018, p. 5), sino también los datos en relación con listas de clientes, proveedores, etc. (Fernández, 2013, p. 413; Fernández, 2016, p. 260).

En el presente trabajo se analizará la repercusión que ha tenido la Ley 1/2019, de 20 de febrero, de Secretos Empresariales (BOE núm. 45, de 21 de febrero de 2019) al referirse a documentos y ficheros electrónicos como soporte de los mismos y su encaje con el derecho a la información y la protección de datos tras el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Diario Oficial de la Unión Europea L119/1, de 4 de mayo de 2016), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre de 2018).

Los secretos empresariales: concepto y características

Con anterioridad a la Ley 1/2019, no se disponía de una legislación en la que se definiera lo que se entendía como secreto empresarial. El propio Tribunal Supremo, en sentencia 285/2008, de 12 de mayo (TOL1.335.978) manifestó que ello

era debido por "tratarse de un concepto lábil, dinámico, no constreñible en un «numerus clausus»". La sentencia se inclinaba, pues, por "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".

Posteriormente, la sentencia núm. 679/2018, de 20 de diciembre (TOL6.988.673), reiteró que ante la falta de un concepto legal de secreto empresarial, para determinar si existía o no el mismo, se debía acudir al art. 39 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (Anexo 1C del Convenio por el que se crea la Organización Mundial del Comercio, Ronda de Uruguay de 1994, conocido con el nombre de ADPIC, que fue ratificado por España el 30 de diciembre de 1994 (BOE núm. 20, de 24 de enero de 1995).

En esta última sentencia del Alto Tribunal se precisaba que la información tenía que contener una serie de caracteres para que se pudiera considerar como secreto:

a) Que sea secreta, en cuanto no sea conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza este tipo de información.

b) Que tenga un valor comercial o competitivo por ser secreta.

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

Por lo que se refiere a sus características, se encuentran las siguientes, siguiendo lo indicado en el Acuerdo sobre los aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, Ronda, Uruguay, 1994, conocidos como Acuerdo ADPIC, en su art. 39:

a) confidencialidad;

b) exclusividad;

c) valor económico, y

d) licitud.

El fundamento reside en la lealtad de quienes deben guardar el secreto, e incluye los secretos de naturaleza técnico industrial (objeto empresarial), comercial (clientela o marketing) y organizacional (laboral, funcionamiento y planes empresariales).

Se puede materializar el secreto en cualquier tipo de soporte, tanto en papel como electrónico, y en original como copia, incluso en el caso de comunicación

verbal, y se extiende a cifras, listados, partidas contables, organigramas, planos, memorándums, entre otros. La duración de la obligación de no revelación se atenderá a la fuente del deber de reserva que se establezca por norma o contractualmente.

La jurisprudencia también se ha pronunciado respecto a un supuesto relativo a revelación de secretos empresariales mediante la utilización del correo electrónico (Cfr. Trujillo, 2014, p. 292). Así, la sentencia del Tribunal Constitucional 170/2013, de 7 de octubre de 2013 (BOE núm. 267, de 07 de noviembre de 2013) consideró que:

> "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 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 contexto descrito, debemos concluir que la conducta empresarial denunciada, realizada además cuando el proceso de comunicación podía entenderse ya finalizado, no ha supuesto una interceptación o conocimiento antijurídico de comunicaciones ajenas realizadas en canal cerrado, en definitiva, debe descartarse la invocada lesión del derecho al secreto de las comunicaciones".

La futura regulación contemplaba una definición, así como la incorporación de la Directiva comunitaria. De esta forma, el informe del Anteproyecto de la actual Ley 1/2019, de 20 de febrero, de Secretos Empresariales (BOE núm. 45, de 21 de febrero de 2019) (en adelante, Ley 1/2019), que emitió el Consejo General del Poder Judicial, mediante acuerdo del 22 de marzo de 2018, señaló:

> "La norma europea trata de paliar la falta de armonización existente en los ordenamientos de los Estados miembros de la Unión Europea en la definición y protección de los secretos empresariales, identificados con los conocimientos técnicos (*know how*) y la información empresarial, articulando las medidas, remedios y procedimientos a través de los que se ha de dispensar tal protección. (…)
>
> Se concibe, por tanto, como una norma de contenido netamente tuitivo de tal derecho y de aquellos intereses legítimos que tiene como finalidad establecer un marco procesal de tutela que comprende no sólo la delimitación de las acciones y subsiguientes pretensiones de que dispone el titular del secreto para obtener la protección del capital intelectual y de la información empresarial que constituyen su objeto (…)".

El texto actual, Ley 1/2019, recoge las anteriores precisiones del Tribunal Supremo, y formula el concepto de secreto empresarial como cualquier información o conocimiento, entre los que se incluye el tecnológico, científico, industrial, comercial, organizativo o financiero, pero que debe reunir unas condiciones específicas que determina el art. 1 de la Ley 1/2019. En este sentido, debe ser secreto, entendido como no conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento, ni sea fácilmente accesible; debe tener un valor empresarial, que puede ser real o potencial; y debe hacer sido objeto de medidas razonables por parte de su titular para que no sea conocido (más ampliamente, véase, Sainz de Aja y Peinado, 2018, p. 32; Saldarriaga, 2018, p. 9).

Queda, por tanto, excluida la información de escasa importancia, así como la experiencia y competencias adquiridas por el personal durante el transcurso de su trayectoria, así como la información que sea de conocimiento general o considerada como fácilmente accesible en los círculos en los que se utilice (Cfr. Félix y Díaz, 2018; Lissén y Guillén, 2019; Massaguer, 2018a, p. 7 y 2018b, p. 3; Fernández de Córdova, 2019, p. 16).

Por último, se encuentra tipificado el secreto de empresa dentro de los delitos relativos al mercado y a los consumidores, recogidos en los arts. 278 y 279 del Código Penal.

El art. 278 se entiende tanto por parte de personas que trabajan dentro de la empresa, como también por parte de terceros (Fernández, 2017; Domingo, 2018). Los instrumentos que señala el art. 197.1 del Código penal son los siguientes: papeles, cartas, mensajes de correo electrónico o cualquiera otros documentos o efectos personales, interceptación de telecomunicaciones, o utilización de artificios técnicos de escucha, transmisión, grabación o reproducción de sonido e imagen, o cualquier otra señal de comunicación.

Esta nueva norma se incluye, de conformidad con lo indicado en la Ley 50/1997, de 27 de noviembre, del Gobierno (BOE núm. 285, de 28 de noviembre de 1997), en su art. 25, dentro del Plan Anual Normativo de 2018, con la finalidad, como hemos indicado, de transposición de la Directiva, mejora la eficacia de la protección jurídica de los secretos empresariales contra la apropiación indebida y como complemento de lo indicado en la Ley 3/1991, de 10 de enero, de Competencia Desleal (BOE núm. 10, de 11 de enero de 1991), (véase, Suñol, 2009), en su art. 13, que se modifica por la disposición final segunda de la Ley 1/2019, quedando con la siguiente redacción que establece:

> "1. Se considera desleal la violación de secretos empresariales, que se regirá por lo dispuesto en la legislación de secretos empresariales".

Documento, ficheros electrónicos y secreto empresarial: la Ley 1/2019, de 20 de febrero, de secretos empresariales

Se entiende por documento como establece el art. 49.1 de la Ley 16/1985, de 25 de junio, de Patrimonio Histórico Español (BOE núm. 155, de 29 de junio de 1985), "toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos".

La doctrina indica que esta definición de documento no se aplica para la generalidad de documentos de archivo producidos por organizaciones o personas (Giménez, 2017, p. 65).

La Ley 1/2019 traspone la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas (DOUE núm. 157, de 15 de junio de 2016). La citada norma nacional contempla, en su art. 3, el documento en relación con la obtención de secretos empresariales y su violación

cuando, sin consentimiento de su titular, y de manera no autorizada, se accede, copia o apropia de documentos, objetos, materiales, sustancias, ficheros electrónicos u otros soportes que contengan el secreto empresarial o a partir de los cuales se pueda deducir el mismo.

Se indica que en el caso de violación de secretos empresariales se podrá solicitar, como precisa el art. 9, la remoción que comprenderá la entrega al demandante de todos o parte de los documentos y ficheros electrónicos, y en su caso su destrucción total o parcial.

Hay que tener en cuenta la relación entre documento y secreto empresarial, ya que los primeros pueden ser el soporte del secreto, y por ello hay que realizar una adecuada gestión de los documentos con la finalidad de garantizar un tratamiento lícito de los mismos. Esta adecuada gestión documental se traduciría en una serie de medidas: clasificación de los documentos y archivo correspondiente; determinar la forma de acceso al documento (establecimiento de claves, restricciones a determinadas personas); indicar cuáles serán los criterios para la gestión del soporte (copias de seguridad, cifrado, medidas informáticas ante posibles ataques); acuerdos de confidencialidad con cláusulas referentes a la revelación de los secretos; establecimiento de los procedimientos de transmisión de la información contenida en los documentos (físicos o electrónicos), y la utilización de correo electrónico y firma electrónica.

Respecto a la gestión de los documentos se debe tener en cuenta lo indicado en el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso (BOE núm. 284, de 25 de noviembre de 2011), por lo que se tendrá que tener en cuenta el establecimiento de repositorios de estos documentos, estableciendo los metadatos, y con la clasificación adecuada para la reutilización y el intercambio, teniendo en cuenta de adoptar las medidas adecuadas en los casos de contener un secreto empresarial. También se adoptarán las medidas adecuadas para proteger la información con el fin de asegurar su acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos.

Respecto a la información que se contiene en un documento o fichero electrónico en relación con el secreto empresarial, es contemplado por la Ley 1/2019, en su art. 15, con la adopción de una serie de medidas específicas:

a) Los operadores jurídicos, partes y peritos que intervienen en un procedimiento que resuelva una controversia sobre violación de secreto empresarial, o bien tengan acceso a documentos obrantes en el procedimiento, no pueden hacer uso ni revelar la información constitutiva de secreto empresarial, y que los órganos judiciales (de oficio o a instancia de parte) hayan declarado confidencial y que hayan tenido conocimiento por intervenir en el procedimiento o acceder a la documentación.

La prohibición se extenderá no sólo durante el proceso, sino también después, salvo que por sentencia firme se indique que la información no es constitutiva de secreto empresarial, o bien con el paso del tiempo pase a ser de conocimiento general o fácilmente accesible en los círculos en los que se utilice.

b) Los órganos judiciales (de oficio o a instancia de parte) podrán adoptar medidas para la preservación de la confidencialidad de la información.

Estas medidas pueden ser las siguientes, no excluyéndose otras que se consideren adecuadas y proporcionadas:

1. Restricción a un número limitado de personas el acceso a los documentos o ficheros electrónicos que contengan información que pueda constituir total o parcialmente secreto empresarial.
2. Restricción a un número limitado de personas el acceso a las vistas, grabaciones o transcripciones de ellas cuando se pueda revelar información total o parcial que pueda constituir secreto empresarial.

La prestación del consentimiento y confidencialidad en relación con los secretos empresariales

Como hemos indicado, el art. 3 de la Ley 1/2019 se refiere al consentimiento y la obtención de secretos sin él como ilícita. Así como el incumplimiento del acuerdo de confidencialidad.

Respecto al consentimiento la norma no indica qué tipo de consentimiento debe de prestarse para que sea lícita la obtención de secretos, si debe ser expreso o por escrito o tácito. Junto a ello, el consentimiento no deberá adolecer de ningún vicio (error, violencia, intimidación o dolo) (Ramón, 2014, p. 21). Es por ello, que debemos acudir a la normativa de protección de datos para documentar el consentimiento de un tratamiento de datos personales por parte de la persona interesada o afectada. Así, respecto a la prestación del consentimiento y la confidencialidad, debemos mencionar el Reglamento (UE) 2016/679, y la Ley Orgánica 3/2018 que se erige en complemento de la normativa comunitaria, al que se remite de forma constante, sin que, en ningún caso sustituya al citado Reglamento (UE) 2016/679, sino que lo desarrolla en los aspectos que se dejan a la interpretación discrecional de los Estados miembros.

El Reglamento (UE) 2016/679 indica que el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado. Consideramos que su aplicación en relación con los secretos empresariales excluiría un consentimiento de tipo tácito, y que debería ser prestado por escrito, ya que como dice el mencionado Reglamento (UE) 2016/679, puede ser marcar una casilla de un sitio web

en internet, utilizar parámetros técnicos para la utilización de servicios de la sociedad de la información, u cualquier otra declaración o conducta que se considere que el interesado acepta. No debe constituir consentimiento el silencio, las casillas ya marcadas o la inacción. Debe ser el consentimiento claro y conciso, y no perturbar de forma innecesaria el uso del servicio para el que se presta.

El acuerdo de confidencialidad debemos tener en cuenta que se precisará el valor de la tecnología, marcas, así como los extremos a los que se atendrá el citado acuerdo (Acea, 2016, p. 145).

Ello también lo aplicamos, desde luego, al tratamiento de datos personales en relación con los secretos empresariales por referencia a dicha legislación del art. 15 de la Ley 1/2019.

El Reglamento (UE) 2016/679 indica que se deberá de proporcionar un modelo de declaración de consentimiento elaborado de forma previa por el responsable del tratamiento con un lenguaje inteligible, accesible, claro y sencillo, sin cláusulas abusivas. Debe informarse de la identidad del responsable del tratamiento y los fines a los que se van a destinar los datos.

El art. 4 del Reglamento (UE) 2016/679 precisa que por consentimiento del interesado se entiende: "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

El art. 6 de la Ley Orgánica 3/2018, referente al tratamiento basado en el consentimiento del afectado, se remite al art. 4 del Reglamento (UE) 2016/679 referido anteriormente, y excluye, consideramos el consentimiento tácito, ya que indica que se entenderá como consentimiento "toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". Es por ello que el consentimiento debe proceder de una declaración o de una acción clara afirmativa del afectado, excluyendo el consentimiento tácito, que no se admite. Importante insistir en que el Reglamento (UE) 2016/679 prohíbe de forma tajante el consentimiento tácito como presupuesto para el tratamiento de datos.

También señala el art. 6 de la Ley Orgánica 3/2018, que cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para distintas finalidades, deberá constar de forma específica e inequívoca que el consentimiento se presta para todas ellas.

No se puede supeditar la ejecución contractual a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

No obstante, es preciso indicar que el consentimiento no es la única base legitimadora para poder realizar el tratamiento de datos personales. Así, el

Reglamento (UE) 2016/679, en su art. 6.4, establece que en los casos en que el tratamiento para otro fin diferente de aquel para el que se recogieron los datos no esté basado en el consentimiento, el responsable del tratamiento para poder determinar si el tratamiento con otro fin es compatible con el inicial, tendrá en cuenta las siguientes circunstancias:

a) Cualquier relación entre los fines para los que se han recogido los datos y los fines del tratamiento posterior previsto.

b) El contexto en que se hayan recogido los datos personales.

c) La naturaleza de los datos personales, particularmente si son categorías especiales de datos.

d) Las posibles consecuencias para los interesados del tratamiento ulterior.

e) La existencia de garantías adecuadas, que podrá ser cifrar los datos o bien la seudonimización

En cuanto al deber de confidencialidad, el art. 5 de la Ley Orgánica 3/2018, precisa que se sujetarán los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase al deber de responsabilidad que establece el art. 5.1.f) del Reglamento (UE9 2016/679, que determina lo siguiente, que los mismos serán tratados "de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)".

Derecho a la información en el caso de documentos y ficheros electrónicos que contienen secretos empresariales: análisis de la casuística

El art. 2 de la Ley 1/2019 trata de la obtención, utilización y revelación lícita de secretos empresariales. De tal forma, que la información obtenida que sea constitutiva de secreto empresarial será lícita cuando sea realizada por alguno de los medios que señala. Se indica que no proceden las acciones y medidas de la Ley 1/2019 en los casos de obtención, utilización y revelación que se haya producido en ejercicio del derecho a la libertad de expresión e información que se contempla en el art. 11 de la Carta de los Derechos Fundamentales de la Unión Europea (2016/C 202/02) (DOUE C 202/389, de 7 de junio de 2016) que comprende la libertad de opinión y la libertad de recibir o comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.

Hay que tener en cuenta que en relación con los secretos empresariales se encuentra la transmisión de conocimiento dentro de la empresa y que se conecta con la innovación y la creación (Canós, Ramón y Mauri, 2008, p. 57). Es por ello, que la transmisión de dicho activo deberá atender a estándares de seguridad y privacidad (Ramón, 2011, p. 102) en relación con los datos que se puedan contener (Canós, Ramón y Mauri, 2007, p. 3).

Otra cuestión a tener en cuenta es la distinción que se debe establecer, como ha indicado la doctrina (Martín, 2019) con lo que se refiere a las bases de datos de clientes como datos protegidos en relación con el secreto empresarial. Para ello, hay que tener en cuenta varias premisas: su consideración como secreto según lo indicado en la Ley 1/2019; que tenga valor comercial y las medidas de protección aplicables.

En el ámbito internacional la cuestión no es pacífica (Sosa, 2015, p.251). Así, podemos señalar que el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) de Perú, en la Resolución 1069-2012/SC1, de 7 de mayo de 2012, se remite a la Resolución 006-2012/SC1-INDECOPI del 12 de enero de 2012, la Sala dijo a propósito de las listas de clientes lo siguiente:

> "Si bien las bases de datos poseen un valor comercial efectivo derivado de los costos de búsqueda invertidos para recabar dicha información; ello no resulta suficiente para calificarlos como secreto empresarial y, por tanto, otorgarle la protección que dispone la Ley. Así, en anteriores pronunciamientos, la Sala ha considerado que la relación o listado de clientes de una empresa puede llegar a constituir un secreto comercial o empresarial, en la medida que dicha información se encuentra directamente vinculada a la situación comercial y posición en el mercado de un competidor.
> (…)
>
> De lo anterior se desprende claramente que la relación o lista de clientes no califica por sí misma como secreto comercial, siendo que debe existir una justificación que sustente tal afirmación. (…)
>
> Sobre el particular, de la revisión de la información obrante en el expediente se aprecia que la base de datos a la que hace referencia la denunciante se encuentra limitada a un listado de clientes y proveedores que no contiene mayor detalle (descuentos aplicados, beneficios ofrecidos, flujo de transacciones celebradas, etc.) y que es susceptible de ser conocida por cualquier tercero. En efecto, las referidas bases de datos contienen nombres de empresas y personas de contacto, lo cual se encuentra también en otras fuentes públicas de información (páginas web, guía telefónica, etc.)."

El art. 1 de la Ley 1/2019 hace alusión a medidas razonables para mantenerlo en secreto el secreto empresarial, valga la redundancia. Pero no nos indica qué medidas razonables hay que adoptar, ni cuáles se consideran como medidas razonables. El Preámbulo de la Ley 1/2019 nos indica al respecto solamente que «esta definición de secreto empresarial no abarca la información de escasa importancia, como tampoco la experiencia y las competencias adquiridas por los trabajadores durante el normal transcurso de su carrera profesional ni la información que es de conocimiento general o fácilmente accesible en los círculos en que normalmente se utilice el tipo de información en cuestión», pero no realiza una enumeración de medidas en ningún precepto de la legislación.

El derecho de acceso a la información, el secreto empresarial y el derecho a la protección de datos de carácter personal deben de ser considerados de forma que no constituya éste último un freno al primero, teniendo en cuenta el respeto a los derechos fundamentales. Es por ello, que la normativa de protección de datos que hemos indicado contempla medidas para garantizar los derechos fundamentales, y el acceso a la información contenida en los documentos que contienen secretos empresariales no puede ser ilimitada, sino precisamente limitada por la regulación de los mismos, y con el límite de los derechos de los sujetos intervinientes, principalmente el derecho a la intimidad y al honor de conformidad con lo establecido en la Ley Orgánica 171982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE núm. 115, de 14 de mayo de 1982).

Si acudimos a la normativa aplicable en protección de datos de carácter personal, mencionada anteriormente, podemos entender que no se va a considerar como secreto por el simple hecho de que digamos que lo es. Es más, según la Ley 1/2019, tiene que reunir las condiciones indicadas. Es por ello, que consideramos (siguiendo a Martín, 2019) que habrá que tener en cuenta:

1. Que se tendrá que realizar una clasificación de la información; que no sea accesible, sino restringida en su acceso.
2. La gestión del soporte y transferencia de la información; la utilización de herramientas informáticas y el uso de las mismas; la protección y seguridad de la información, proveedores y acceso por lo que habrá que tenerse en cuenta lo indicado en la Decisión del Consejo, de 31 de marzo de 1992, relativa a la seguridad de los sistemas de información (DOCE núm. 123, de 8 de mayo de 1992), Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (BOE núm. 218, de 8 de septiembre de 2018), que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DOCE L194/1, de 19 de julio de 2016).

No hay que olvidar que el art. 1 del Real Decreto-ley 12/2018 excluye de su ámbito de aplicación a:

«a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.

b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas».

3. Los acuerdos de confidencialidad que se hayan adoptado. Aquí es importante indicar siguiendo a Oliva (2019), que se indique en el mismo que la información, datos, objetivos de futuro, no se hagan públicos. Dicha obligación de confidencialidad resulta esencial en cualquier transferencia de conocimiento que se vaya a realizar. Habrá que atender también a los límites de las cláusulas contractuales para determinar la naturaleza jurídica de la información que se contiene a efectos de protección de los secretos empresariales (Remolina y Tafur, 2017, p. 145).
4. Política referente a las copias de seguridad, transmisión de información, controles y auditorias.
5. Las indicaciones sobre ello contenidas en los esquemas de seguridad de la información. Así, habrá de tenerse en cuenta las siguientes normas, en el caso de que sean aplicables teniendo en cuenta las características de la información, y de conformidad con lo indicado en la Guía de Seguridad de las TIC CCN-STIC 821. Esquema Nacional de Seguridad. Normas de Seguridad (2018):
   a) Ley 40/2015, de 1 de octubre, de Régimen jurídico del Sector Público (BOE núm. 236, de 2 de octubre de 2015).
   b) Reglamento (UE) 2015/703 de la Comisión, de 30 de abril de 2015, por el que se establece un código de red sobre las normas de interoperabilidad y de intercambio de datos (Texto pertinente a efectos del EEE) (DOUE núm. 113, de 1 de mayo de 2015).
   c) Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DOUE núm. 235, de 9 de septiembre de 2015).

   d) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (BOE núm. 25, de 29 de enero de 2010), modificado por Real Decreto 951/2015, de 23 de octubre (BOE núm. 264, de 4 de noviembre de 2015).
   e) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (BOE núm. 25, de 29 de enero de 2010).
   f) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE núm. 150, de 23 de junio de 2007), que ha sido desarrollada parcialmente por Real Decreto 1671/2009, de 6 de noviembre (BOE núm. 278, de 18 de noviembre de 2009), y modificado éste por Real Decreto 668/2015, de 17 de julio (BOE núm. 171, de 18 de julio de 2015).

Respecto a las bases de datos de clientes y los requisitos que se deben de cumplir para que su cesión sea lícita, debemos remitirnos a la normativa de protección de casos, que, como ya hemos indicado se encuentra en el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018.

El art. 8 de la Ley Orgánica 372018 contempla el tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos, que sólo se podrá considerar fundado en el cumplimiento de una obligación legal exigible al responsable, remitiéndose a lo indicado en el art. 6. 1. c) del Reglamento (UE) 2016/679, en los casos que lo prevea una norma del Derecho de la UE o una norma que tenga rango de ley, que podrá determinar las condiciones del tratamiento y los tipos de datos, así como las cesiones que puedan realizarse en cumplimiento de la norma legal. Se podrán imponer medidas adicionales de seguridad, de conformidad con el capítulo IV del Reglamento (UE) 2016/679. Un ejemplo de ello, son las bases de datos reguladas por ley y gestionadas por autoridades públicas para control y solvencia.

El tratamiento de los datos, según lo que dispone el Reglamento (UE) 2016/679, en su art. 6.1, sólo será lícito si se cumple alguna de las siguientes condiciones:

a) Que el interesado preste su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

b) Que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte o bien para la aplicación de medidas precontractuales.

c) El tratamiento sea preciso para cumplir una obligación legal aplicable al responsable de aquél.

d) El tratamiento sea necesario para proteger intereses vitales del interesado o de un tercero.

e) El tratamiento se requiera para cumplir una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del mismo.

f) Se precise el tratamiento para satisfacer intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre los intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que precisan la protección de los datos.

Ponderación entre la legislación en materia de secretos empresariales y la nueva regulación de los derechos digitales

El Título X de la Ley Orgánica 3/2018, en los arts. 79 a 97, los denominados derechos digitales y sus garantías, en sintonía con lo indicado en el art. 18.4 de la Constitución Española. Se contiene derechos del entorno digital, en la era internet, como es el caso de la neutralidad en la Red, y el acceso universal a la misma, y también derechos a la seguridad y educación digital, así como el derecho al olvido, a la portabilidad y al testamento digital, y la protección de los menores en internet. Sin embargo, en el ámbito de la empresa y los secretos empresariales nos interesa destacar, aunque sea brevemente, el derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral, así como la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digital.

En el ámbito empresarial, se plantea algún problema en relación con los secretos empresariales y la utilización de dispositivos electrónicos, respecto a su control por parte de la empresa. Se trataría de determinar si la monitorización por parte de la empresa de los dispositivos electrónicos puede interferir con los derechos digitales del trabajador, en concreto, con su intimidad y privacidad (Brands, 2019; Ramón, 2019).

Así, el art. 88 de la Ley Orgánica 3/2018 debe entenderse en sintonía con el articulo 20 bis del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE núm. 255, de 24 de octubre de 2015), introducido por la Ley Orgánica 3/2018, que regula el derecho de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión. De tal forma, que tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, así como a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización según la normativa de protección de datos personales y garantía de los derechos digitales.

La recopilación de datos debe atender a su necesidad, es decir, que sean imprescindibles, y no la utilización de datos masivos. Se deben conocer qué datos se van a tratar, así como la finalidad de los mismos, y la proporcionalidad en su recopilación (Brands, 2019).

Bien, todo ello aplicado a los secretos empresariales se discute cómo establecer su protección en un mundo hiperdigitalizado, en el que el secreto empresarial va mucho más allá de la presencia física en una empresa, ya que puede estar en riesgo al implicarse los dispositivos electrónicos. Se trata de ver cómo evitar y prevenir una fuga de información. Se deben establecer medidas de precaución o cautelares que no vayan en contra de los derechos digitales contemplados en la Ley Orgánica 3/2018, es decir, que permitan el derecho a la desconexión digital, así como el derecho a la intimidad del trabajador.

Esta protección puede realizarse a través de distintas medidas, como por ejemplo de tipo tecnológico, en el que podría implantarse la denominada "cadena de bloques" o blockchain, o bien también de tipo contractual, estableciendo cláusulas para el trabajador y su acceso a los secretos empresariales, como los acuerdos de confidencialidad.

Este argumento lo podemos sostener interpretando el art.3 de la Ley 1/2019, referente a la violación de secretos empresariales, al referirse al incumplimiento de los acuerdos de confidencialidad o el incumplimiento de las obligaciones contractuales.

Conclusiones

La regulación de los secretos empresariales plantea distintos problemas en relación con los documentos y ficheros electrónicos que pueden contener dicha información. No podemos obviar la íntima relación que tiene dicha información protegida con la normativa actual de protección de datos personales, así como con los acuerdos de confidencialidad respecto al tratamiento de los secretos empresariales y los sujetos en las relaciones contractuales.

La legislación principal, la Ley 1/2019, adolece de algunas carencias que hubiera sido deseable que se hubieran indicando, como, por ejemplo, la falta de precisión de las medidas razonables para el mantenimiento del secreto. Ello en el caso de los documentos y ficheros electrónicos plantea problemas de determinación y operabilidad.

La Ley 1/2019 se remite a la normativa de protección de datos de carácter personal que se regula por el Reglamento (UE) 2016/679 y por la Ley Orgánica 3/2018, siendo ésta última una norma que se remite de forma constante al Reglamento (UE) 2016/679, y que no lo sustituye, sino que lo complementa y desarrolla.

La información referente al secreto empresarial puede estar en un soporte físico o electrónico, y la gestión del documento es de especial relevancia, no sólo para la conservación del mismo, sino también para evitar filtraciones de la información. Es por ello que se deben articular medidas adecuadas de gestión, como la utilización de cifrados y el acceso al correo electrónico por parte de los sujetos titulares del secreto empresarial.

La normativa de protección de datos personales, tanto el Reglamento (UE) 2016/679, como la Ley Orgánica 3/2018, contiene una serie de requisitos para el tratamiento de los datos y su transferencia a terceros, siendo especialmente relevante la necesidad de un consentimiento expreso, no admitiéndose el consentimiento de forma tácita.

Es preciso establecer una ponderación entre la normativa de secretos empresariales y la regulación de los derechos digitales de la Ley Orgánica 3/2018, en el caso de la desconexión digital y también en la utilización de dispositivos electrónicos que contengan secretos empresariales por parte del trabajador y sujetos al control del empresario, para evitar una invasión en el derecho a la intimidad del primero. Se deben articular medidas de control no invasivas, así como fomentar las cláusulas de confianza o la cadenas de bloques, o blockchain.

Bibliografía

ACEA VALDÉS, Yeney (2016). "La transferencia de tecnología en Cuba". *Dereito: Revista xuridica da Universidade de Santiago de Compostela*, vol. 25, n. 2, p. 139-149. <http://www.usc.es/revistas/index.php/dereito/article/view/3474/4122>. [Consulta: 01/03/2019].

BRANDS, E.C. (2019). "Control vs privacidad: ¿qué pueden hacer las empresas con los datos de sus empleados?". *El Confidencial*. <https://www.elconfidencial.com/empresas/2019-06-03/empresas-empleados-datos-secreto-empresarial-bra_1973894/>. [Consulta: 05/10/2019].

CANÓS DARÓS, Lourdes, RAMÓN FERNÁNDEZ, Francisca y MAURI CASTELLÓ, Jordi (2007). "La protección de datos personales y la información para la gestión del conocimiento en las empresas". *Revista General Informática de Derecho*, p. 1-13.

—(2008). "Aspectos jurídicos y económicos de la propiedad industrial de la empresa". *Novática*, n. 193, p. 56-58.

CONSEJO GENERAL DEL PODER JUDICIAL (2018). *Informe sobre el Anteproyecto de Ley de Secretos Empresariales*. <http://www.poderjudicial.es/portal/site/cgpj/menuitem.65d2c4456b6ddb628e635fc1dc432ea0/?vgnextoid=d32caea63c162610VgnVCM1000006f48ac0aRCRD&vgnextchannel=a64e3da6cbe0a210VgnVCM100000cb34e20aRCRD&vgnextfmt=default&vgnextlocale=es_ES>. [Consulta: 31/03/2019].

DOMINGO MONFORTE, José (2018). "El secreto empresarial. Revelación. Tipicidad penal". *Diario La Ley*, n. 9144.

FERNÁNDEZ CARBALLO-CALERO, Pablo (2013). "La configuración del listado de clientes como un secreto empresarial en el derecho contra la competencia desleal". En: Tobío Rivas, Ana María (coord.), Fernández Albor Baltar, Ángel, Tato Plaza, Anxo (ed.), *Estudios de derecho mercantil: Libro homenaje al Prof. Dr. h. c. José Antonio Gómez Segade*. Madrid: Marcial Pons, p. 411-436.

FERNÁNDEZ DE CÓRDOVA, Álvaro (2019). "Ley 1/2019, de 20 de febrero, de Secretos Empresariales: aproximación a los elementos sustantivos de esa «nueva» propiedad intelectual". *Economist & Jurist*, n. 228, p. 16-27.

FERNÁNDEZ DÍAZ, Carmen Rocío (2016). "La lista de clientes como objeto del secreto empresarial". *Revista Aranzadi Doctrinal*, n. 7, p. 251-274.

FÉLIX PARRONDO, Esther DE y DÍAZ BAÑOS, Manuel (2018). "El Anteproyecto de Ley de Secretos Empresariales, a debate". *Diario La Ley*, n. 9201.

FERNÁNDEZ DÍAZ, Carmen Rocío (2017). *La violación de secretos empresariales por persona ajena a la empresa: un estudio del artículo 278 del código penal*, García Pérez, Octavio y Díez Ripollés, José Luis (dir.). Málaga: Universidad de Málaga.

FLORES SÁNCHEZ, José Alejandro (2017). "La protección de los derechos de propiedad industrial en el ámbito empresarial. ¿proteger o no proteger?. *Olimpia: Publicación científica de la facultad de cultura física de la Universidad de Granma*, vol. 14, n. 14, p. 55-68.

GIMÉNEZ-CHORNET, Vicent (2017). *Legislación de archivos*. Barcelona: UOC.

Guía de Seguridad de las TIC CCN-STIC 821. Esquema Nacional de Seguridad. Normas de Seguridad (2018). <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/529-ccn-stic-821-normas-de-seguridad-en-el-ens/file.html>. [Consulta: 31/03/2019].

LISSÉN ARBEOLA, José Miguel y GUILLÉN MONJE, Patricia (2019). "Características, alcance de la protección conferida e implicaciones para las empresas en la nueva Ley de Secretos Empresariales". *Diario La Ley*, n. 9363.

MARTÍN, Paz (2019). "La nueva ley de secretos empresariales y la protección de datos ¿algo en común?". *Blog Legal Things Abogados*, 21 de febrero. <https://legalthings.es/la-nueva-ley-de-secretos-empresariales-y-la-proteccion-de-datos-algo-en-comun/>. [Consulta: 31/03/2019].

MASSAGUER FUENTES, José (2018a). "El Anteproyecto de Ley sobre Protección de los Secretos Empresariales". *Actualidad jurídica Aranzadi*, n. 941, p. 7.

—(2018b). "El incumplimiento de los contratos de licencia de patente y de licencia de secretos empresariales: concurrencia entre acciones contractuales y acciones por infracción". *Revista de Derecho mercantil*, n. 309, p. 3.

OLIVA LEÓN, Ricardo (2019). "Acuerdo de confidencialidad y protección de secretos empresariales". *Blog Algoritmo Legal*, 3 de febrero. <https://www.algoritmolegal.com/propiedad-intelectual/acuerdo-de-confidencialidad-y-proteccion-de-secretos-empresariales/>. [Consulta: 31/03/2019].

RABASA MARTÍNEZ, Ignacio (2018). "El anteproyecto de Ley de Secretos Empresariales y la Directiva 2016/943 relativa a los conocimientos técnicos e información empresarial no divulgados". *La Ley mercantil*, n. 47, p. 5.

RAMÓN FERNÁNDEZ, Francisca (2011). "Transmisión del conocimiento en la empresa y la influencia de las redes sociales y TICs". *Revista da micro e pequeña empresa*,

v. 5, n. 3, p. 99-113. <http://revistas.uexternado.edu.co/index.php/propin/article/view/4347/4931>. [Consulta: 02/02/2019].

—(2015). "La ingeniería y la propiedad industrial en el ámbito universitario: marco legal y algunas dudas habituales". *Revista La Propiedad Inmaterial*, n. 20, p. 39-56. <http://www.cc.faccamp.br/ojs-2.4.8-2/index.php/RMPE/article/view/232/174>. [Consulta: 03/02/2019].

—(2014). "La mediación electronica, la confidencialidad y la protección de datos de carácter personal". *InDret. Revista para el análisis del Derecho*, n. 3, p. 1-28. <http://www.indret.com/pdf/1069_es.pdf>. [Consulta: 05/02/2019].

—(2019). "La normativa de protección de datos y derechos digitales en el ámbito de los recursos humanos: un reto para la sociedad y la legislación". En: *¿Se puede crear capital social? Innovación y tecnología: retos para los recursos humanos de las organizaciones*. Valencia: Tirant lo Blanch, p. 202-227.

REMOLINA ANGARITA, Nelson y TAFUR NÁDER, Gabriela (2017). "Limitaciones de las cláusulas contractuales para determinar la naturaleza jurídica de la información y para proteger los secretos empresariales". *Revista La Propiedad Inmaterial*, n. 24, p. 145-165. <https://revistas.uexternado.edu.co/index.php/propin/article/view/5201/6268>. [Consulta: 01/03/2019].

SAINZ DE AJA TIRAPU, Borja y PEINADO IRIBAR, Estíbaliz (2018). "Secretos empresariales. Cuestiones relevantes de la Directiva y del Proyecto de Ley". *Comunicaciones en propiedad industrial y derecho de la competencia*, n. 84, p. 31-45.

SALDARRIAGA, José Ignacio (2018). "La protección del secreto empresarial a la luz de la nueva regulación". *Actualidad jurídica Aranzadi*, n. 945, p. 9.

SOSA HUAPAYA, Alex (2015). "Competencia desleal y resguardo de los secretos empresariales". *THEMIS: Revista de Derecho*, n. 68, p. 245-259. <http://revistas.pucp.edu.pe/index.php/themis/article/view/15597/16046>. [Consulta: 25/02/2019].

SUÑOL LUCEA, Aurea (2009). *La protección jurídica del secreto empresarial en el artículo 13 de la Ley de competencia desleal*. Madrid: Civitas.

TRUJILLO PONS, Francisco (2014). "Revelación de secretos empresariales a terceros por medio del correo electrónico. Posición del Tribunal Constitucional ante una supuesta vulneración a los derechos a la intimidad y al secreto de comunicaciones. Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre de 2013". *Revista General de Derecho del Trabajo y de la Seguridad Social*, n. 36, p. 292-320.