"Libertad Informática y Criptología"

JOSÉ MARIA MOLINA MATEOS

Abogado, Criptólogo, miembro de la Junta Directiva y socio fundador de la ASOCIACION ESPAÑOLA DE CRIPTOLOGIA, y Consultor de OMNISEC

SUMARIO:

I.- LIBERTAD INFORMATICA.

La terminología es uno de los elementos que posibilitan la comunicación y, consiguientemente, la coherencia en un ámbito de relaciones.

Los términos lingüisticos son medios cuyo sentido está en el nivel de conciencia del ámbito en que se desenvuelven, si no tienen un significado unívoco pierden su capacidad de comunicar[1].

De ahí la conveniencia de una previa delimitación conceptual que fije el significado y alcance del concepto que subyace bajo la expresión "libertad informática", que va a ser el concepto que constituirá el soporte y justificación de

■ 1 Fernando de Elzaburu Márquez y Jesús Martitegui Susunaga en "La crisis Mundial: De la incertidumbre a la esperanza".- Espasa Calpe, 1.988

cuanto desarrollaremos en el presente trabajo, aplicado al entorno a que nos referimos.

La libertad informática tiene sus orígenes en el "derecho de autodeterminación informativa" surgido de la Sentencia de 13 de abril de 1.983, del Tribunal Constitucional Alemán, sobre la Ley del Censo de Población, cuya evolución ha configurado el concepto de "libertad informática" como hoy lo entendemos:

- En su formulación positiva de libertad de controlar el uso de los propios datos personales insertos en un programa informático.

- Como control para que los datos se usen adecuadamente y no se atente contra los derechos y liberetades, entendido como un "habeas data" del respeto debido a la integridad y libertad de la persona.

- Como derecho de acceso a los bancos de datos, derecho de control de su exactitud, derecho de puesta al día y de rectificación, derecho de secreto para los datos 'sensibles', derecho de autorización para su difusión: todo este conjunto de derechos es lo que hoy constituye el 'right of privacy'".

La propia sentencia del Tribunal Constitucional alemán señalaba las limitaciones del derecho de autodeterminación informática, sólo admisible en el marco de un interés general superior con fundamento en la Constitución. Lo que obliga al legislador a dictar reglas que protejan estos nuevos valores en un marco de garantía que preserve los intereses generales, observando el principio de proporcionalidad, y tomando las precauciones necesarias para neutralizar el peligro derivado de la vulneración del derecho.

En el sistema constitucional español, la libertad informática encuentra un reconocimiento inmediato en los artículos 18.4[2] y 105 b)[3] de la Constitución Española de 1.978, y tiene, asimismo, soporte en la propia definición de nuestra forma política como "Estado social y democrático de Derecho, que propugna como valores superiores del ordenamiento jurídico la libertad, la justicia, la igualdad y el pluralismo político" (art. 1.1. C.E.), todo ello en equilibrada relación con otros principios constitucionales y, fundamentalmente, con las libertades de expresión y derecho a la información del artículo 20 , o el secreto de las comunicaciones del artículo 18.3, ambos de nuestra Carta Magna.

- 2 "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."
- 3 "El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas".

Se trata de encontrar el punto de equilibrio entre la libertad de expresión -en su acepción más amplia, comprensiva, tanto de expresar y difundir libremente los pensamientos, ideas y opiniones, como el derecho a comunicar y recibir libremente información veraz por cualquier medio- y la protección de la esfera privada del individuo.

II.- LA CONFIDENCIALIDAD.-

La protección de la información almacenada, tratada o transmitida electrónicamente exige infraestructura de telecomunicaciones seguras, terminales seguras, procesadores y bases de datos seguros y una utilización segura de todo ello.

De las diferentes definiciones doctrinales, así como de las normas relativas a la seguridad de la información se desprenden tres propiedades fundamentales: la confidencialidad, la integridad y la accesibilidad.

La propiedad que tiene una directa relación con "el derecho de secreto para los datos sensibles" como una manifestación concreta de uno de los aspectos de la libertad informática es la confidencialidad, mediante la cual, un sistema de información sólo permite el conocimiento de la misma a quienes estén autorizados.

Para algunos autores la seguridad aplicada a la información se asocia, generalmente, con aspectos parciales de la misma, tales como la disponibilidad o la seguridad física o, incluso, la integridad, olvidando otros enfoques fundamentales, relacionados con la confidencialidad, produciendose una quiebra, no solo por la omisión de un factor determinante, sino por la falta de una concepción integral de la seguridad que demanda un equilibrio de la proporción en que interviene cada una de las dimensiones de la misma, en función del uso a que esté destinada.

En esta ponencia trataremos de la confidencialidad como propiedad de la seguridad, en cuya protección interviene, de forma determinante, los procedimientos criptológicos.

Secreto de las comunicaciones privadas.

El artículo 18 de la Constitución Española, dedicado de forma general a regular la intimidad de las personas como derecho fundamental, en su apartado

3, se ocupa de garantizar el secreto de las comunicaciones: "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".

El bién jurídico protegido es el secreto de las comunicaciones privadas, el cual presupone la libertad de comunicación. Las comunicaciones públicas vienen tuteladas por el artículo 20 de la C.E. referido a la libertad de expresión e información.

El derecho fundamental del secreto de las comunicaciones recogido en el artículo 18.3 de la C.E. se configura como un derecho que garantiza a los particulares una esfera de libertad que ha de ser respetada y es, esencialmente, una garantía frente al Estado, aunque, en menor medida, también, frente a los particulares.

Sus titulares son tanto las personas físicas como las personas jurídicas y, aunque el derecho a la intimidad sólo es atribuible a las personas físicas (Tribunal Constitucional, Auto de 17 de abril de 1.985), el derecho al secreto de las comunicaciones, al igual que otros derechos de la personalidad puede ser atribuido a las personas morales.

El secreto de las comunicaciones privadas no depende del contenido de estas, ni de que el contenido de lo comunicado esté o no dentro del ámbito de la intimidad. El concepto de secreto del artículo 18.3 tiene un carácter formal, en el sentido que se predica de lo comunicado, sea cual fuere su contenido y pertenezca o no el objeto de lo comunicado, al ámbito de la persona, lo íntimo y lo reservado (S.T.C. 114/1.984 de 29 de noviembre). Esta misma sentencia afirma que el derecho fundamental del secreto de las comunicaciones consagra la "libertad de comunicaciones" implícitamente y, de modo expreso, su secreto.

Este derecho ampara a todo tipo de comunicaciones[4] con independencia del medio o forma en que tenga lugar la transmisión y representa para los datos informáticos un plus de confidencialidad.

■ 4 La Ley 31/1.987, de 18 de diciembre, de "Ordenación de las Telecomunicaciones", en su artículo 2.2. dice:"Los servicios de telecomunicaciones se organizarán de manera que pueda garantizarse eficazmente el secreto de las comunicaciones, de conformidad con lo previsto en el artículo 18.3 de la Constitución". y, el art. 16 dice "1.-La prestaciones de los servicios portadores y de los servicios finales de telecomunicación deberá ajustarse, con carácrter general a los siguientes principios: ...e) Posibilidad de intercambio y envío de comunicaciones, por los servicios que permiten tales usos, sin otras limitaciones que las impuestas por las leyes, por resolución judicial o que sean consecuencia del incumplimiento contractual grave o reiterado por el usuario o abonado. f) Garantía del secreto de las comunicaciones, de conformidad con lo previsto en el artículo 18.3 de la Constitución.

El secreto de las comunicaciones tiene un carácter omnicomprensivo y es aplicable a cualquier medio o servicio que sirva para la transmisión de las mismas.

Aunque el precepto constitucional subraya especialmente "las postales, telegráficas y telefónicas", la cobertura no se otorga sólo y exclusiva a este tipo de comunicaciones.

Podriamos decir que el secreto de las comunicaciones aplicado a la información almacenada, tratada o transmitida electrónicamente viene a complementar y reforzar la "libertad informática" en su faceta de derecho de secreto para los datos "sensibles".

La condición formal del secreto de las comunicaciones implica para el Tribunal Constitucional una presunión de que lo comunicado es secreto, que no admite prueba en contrario.

Este derecho se puede conculcar tanto mediante la interceptación que suponga la aprehensión del soporte del mensaje -con conocimiento o no del mismo- , como por el conocimiento antijurídico de lo comunicado.

El artículo 18.3 de la C.E., al reconocer el derecho fundamental del secreto de las comunicaciones, determina su caracter relativo, en el sentido de permitir su limitación por una resolución judicial que autorice la injerencia en su objeto.

La limitación de este derecho fundamental depende sólo de la oportuna resolución judicial motivada. Monopolio jurisdiccional que resulta imprescindible para establecer la posibilidad de limitación de un derecho fundamental integrado en el "status libertatis" de la persona.

III.- PROTECCION CRIPTOLOGICA.-

La protección que brinda el ordenamiento jurídico es una protección "a posteriori" que, por las características de la información, y la propia naturaleza de la tecnología informática, en muchos casos resulta insuficiente para el logro efectivo de la protección del derecho de secreto para los datos sensibles, por lo que, además de la protección jurídica, se requieren medidas de prevención que, "a priori", impidan materialmente el éxito de las amenazas contra la información almacenada, tratada o transmitida electrónicamete. Medidas que pueden ser de naturaleza diversa tales como medidas físicas, lógicas, criptológicas, organizativa etc.

La criptología -ó criptografía- como mero instrumento técnico para la realización efectiva de una protección, se incorpora al sistema de información una vez determinado qué ha de protegerse y con qué niveles.

La Criptología, como ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones, ha sido utilizada tradicionalmente en los ámbitos militar, diplomático y comercial. Actualmente, se ha ampliado a otros usos mucho más próximos aunque con niveles de exigencias diferentes y, entre los que son cada vez más frecuentes, las aplicaciones destinadas a la protección de los derechos y libertades.

La forma tradicional de preservar la confidencialidad de una red de comunicaciones ha sido la protección criptológica.

La protección criptológica implica la utilización de técnicas que permiten llevar a cabo, de forma efectiva, el ocultamiento de la información protegida a personas no autorizadas. El carácter instrumental de la criptología la convierte en mera herramienta para el cumplimiento de una decisión previa que comporta la sustracción de información al conocimiento público.

Corresponde a la criptología únicamente la misión de ser eficaz en el cumplimiento de sus fines, perteneciento a la norma la determinación de los ámbitos y niveles de aplicación. Lo que en definitiva es una forma concreta de configurar y hacer realidad unos límites que pudieran incidir en las libertades públicas o en la garantía de determinados derechos fundamentales, y viene a suscitar un tema de indudable relevancia ética, jurídica y política.

Ante los avances tecnológicos que permiten el acceso a las bases de datos y la interceptación de las transmisiones efectuadas por cualquier medio, la necesidad de protección criptológica, como medio para que la "libertad informática" sea real y efectiva, se torna en una exigencia imprescindible.

Pero la protección de la información no es un valor absoluto, sino que se justifica en función del interés que protege.

La protección criptológica de la información se encuentra sometida a una doble tensión, con tendencia ascendente hacia los máximos niveles de impenetrabilidad, cuando se refiere a los altos intereses y, orientada hacia niveles de impenetrabilidad relativa, en otros casos, dentro de toda una gama de opciones en función del ámbito a que se refiere y que vienen a responder a los dos grandes bloques en que, básicamente, podriamos encontrar agrupada la protección

de la información: el destinado a garantizar el secreto de las comunicaciones privadas y el constituido por la protección de información pública.

Bloques que responden a principios distintos. Mientras en las comunicaciones privadas (art. 18.3 de la C.E.), la regla general es el secreto y la excepción la transparencia, en las comunicaciones públicas (art. 20 de la C.E.), la regla general es la transparencia y la excepción el secreto. Este postulado, aplicado a su correlativo de protección criptológica, nos llevaría a una necesidad de protección sistemática de las comunicaciones privadas y, excepcionalmente, de las públicas.

Preservar el secreto de los datos sensibles es una aplicación concreta al ámbito de la "libertad informática".

La Ley 30/1.992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común contribuye a la definición de perfiles de algunos ámbitos necesitados de protección, al preceptuar en el apartado 6 de su artículo 37, que se regirán por disposiciones específicas, el acceso a los archivos de materias clasificadas, datos sanitarios de los pacientes, datos electorales, etc, y, en todo caso, los datos relativos a la intimidad (art. 37.2).

En los ámbitos indicados, referidos a los archivos y registros,la regulación de acceso rebasa el carácrter estático y ha de extenderse también a su regulación desde una perspectiva dinámica, durante la transmisión de esos datos, sobre todo, teniendo en cuenta los principios de cooperación, coordinación y colaboración entre Administraciones Públicas que requiere la intercomunicación y transmisión telemática de asientos de registros coordinados, y la agilización, mediante el empleo de nuevas técnicas de transmisión de información, recogidas en la ley indicada, que en su artículo 45.1 establece que "Las Administraciones Públicas impulsarán el empleo y aploicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias...".

La Ley Orgánica 5/1.992 de 29 de octubre sobre Regulación del tratamiento Automatizado de los Datos de carácter personal,se pueden encontrar algunas referencias indirectas a determinados ámbitos susceptibles de protección criptológica.[5]

■ 5 Art. 9."1.-El responsable del fichero deberá adoptar las medidas necesarias para garantizar la seguridad de los datos de carácer personal.- 2.- No se registrarán datos de carácter personal en ficheros automatizados que no reunan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a la de los centros de tratamiento, locales, equipos, sistemas y programas".
Art. 20.2 "in fine" dice que "La recogida y tratamiento automatizado para fines policiales de datos de carácter personal..." deberán "ser almacenados en ficheros específicos establecidos al efecto, que deberán claisifcarse por categorias, en función de su grado de fiabilidad".

En el ámbito comunitario hay referencias a la protección criptológica en la Decisión del Consejo de 31 de marzo de 1.992, relativa a la seguridad de los sistemas de información, Recomendación del Consejo de la OCDE de 26 de noviembre de 1.992, que contiene las líneas directrices para la Seguridad de los Sistemas de Información, el Convenio de 28 de enero de 1.981 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal y Propuesta de Directiva del Consejo relativa a la protección de los datos personales y de la intimidad, en relación con las redes públicas digitales de telecomunicación, y, en particular, la Red Digital de Servicios Integrados (RDSI) y las Redes Móviles Digitales Públicas.

IV.- CONFLICTOS EN TORNO A LA PROTECCION CRIPTOLOGICA DE LOS DATOS INFORMATICOS.

La Sentencia del Tribunal Constitucional Alemán de 13 de abril de 1.983, sobre la Ley del Censo de Población , en la que está el origen del concepto de "libertad informática", señalaba como limitaciones admisibles las derivadas del marco de un interés superior con fundamento en la constitución, cuyas normas, además de tomar las precauciones necesarias para neutralizar el peligro derivado de la vulneración del derecho, apliquen el principio de proporcionalidad, y preserven los intereses generales.

La protección criptológica de los datos "sensibles", -manifestación concreta de la "libertad informática"- se sitúa en un contexto de mayor amplitud, donde se relaciona con otras realidades. Constexto constituido por la aplicación de las nuevas tecnologías de la información en el entorno social, jurídico y político de una sociedad democrática, donde la protección de datos "sensibles" encuentra su reforzamiento, e, incluso, su legitimación, pero, también, sus límites.

Por ello, a la hora de aproximarnos al análisis de los conflictos jurídicos que se suscitan con la protección criptológica de datos informáticos no podemos quedarnos en el "dato sensible", aisladamente considerado, como tipo, clase o especie de un dato informático, sino que, tenemos que ver sus relaciones jurídicas y funcionales con las protección critplógica de otros datos, también informáticos, pero de naturaleza distinta, manifestaciones en "soporte magnético" de otras realidades subyacentes y otros derechos, cuya naturaleza, en modo alguno resulta indiferente al objeto de este trabajo, puesto que la protección de la información no es un valor absoluto, sino que se justifica en función del interés que protege. Interés que puede ser referido a la intimidad, pero también a intereses

del Estado, industriales o comerciales..., cuyas interrelaciones suscitan interesantes problemas jurídicos.

Todo derecho tiene sus límites en relación a los derechos fundamentales que establece la Constitución, en unos casos y, en otros, estos límites se derivan de una manera indirecta del tal norma, en cuanto han de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino, también, otros bienes constitucionalmente protegidos.

El derecho al honor, a la intimidad y a la propia imagen, es un elemento limitativo que, inadecuadamente utilizado puede reducir el propio contenido esencial de las libertades de expresión e información y, por ello, constituir un claro exponente de incompatibilidad entre preceptos constitucionales.

De otra parte, las libertades de expresión y de información ofrecen amplias posibilidades para un aplastamiento de otros derechos y libertades no menos fundamentales y, es por ello, por lo que se advierte sobre unos límites especialmente susceptibles de provocar colisiones con derechos y libertades que gozan también de una protección específica en los textos del ordenamiento internacional.

No es que cuando afecta al honor, la intimidad y la propia imagen disminuya la garantía institucional del ejercicio de las libertades de expresión e información, sino que la realización práctica es polémica.

Estas garantías están incluidas por los límites que, según consolidada doctrina, cabe concebir desde la interpretación de condiciones permitidas en textos internacionales (art. 29.2[6] de la Declaración Universal de Derechos Humanos, art. 19.2[7] y 19.3[8] del Pacto Internacional de Derechos Civiles y Políticos y el art. 10 del convenio Europeo para la Protección de Derechos Humanos y Libertades fundamentales), permiten establecer ciertas regulaciones restrictivas "Que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la

- 6 "En el ejercicio de sus derechos y en el disfrute de sus libertades toda persona estará solamente sujeta a las limitaciones establecidas por la Ley, con el único fín de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática".
- 7 "Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección".
- 8 "El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la Ley y ser necesarias para: a) Asegurar el respeto a los derechos o a la reputación de los demás; b) La protección de la seguridad nacional, el orden público, la salud o la moral públicas".

moral, la protección de la reputación de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad judicial" (art. 10.2 del Convenio Europeo de 1.950).

Semejantes colisiones pueden darse con otros derechos y, de estos entre sí.

Se da la circunstancia que, la seguridad del Estado, la realización efectiva de determinados derechos fundamentales, la averiguación y prevención del delito exigen, en algunas ocasiones, medidas restrictivas del derecho fundamental del secreto y libertad de comunicaciones, y de la libertad de información, que también, y desde otra perspectiva, pueden incidir en la libertad e intimidad de la personas.

La seguridad del Estado, la intimidad del individuo, el secreto de las comunicaciones y la averiguación y prevención del delito, tienen una serie de elementos comunes pero, responde a principios distintos, que operan bajo parámetros diferentes y defienden intereses que, en algunos casos, pueden llegar a ser contrapuestos.

Cuando se da la circunstancia de intereses contrapuestos en ámbitos protegidos criptológicamente, la propia naturaleza de la criptología ,cuya finalidad es proteger del modo más eficaz y mejor, la confidencialidad del ambito a que se aplique, puede introducir un elemento de perturbación en el funcionamiento del sistema, globalmente considerado, si no adecúa sus niveles de protección a la naturaleza de la información protegida, de forma que haga posible el juego de los distintos derechos concernidos.

Los niveles de protección de una red han de ser proporcionales a las amenazas a que está sometida. Pero la variedad de amenazas conlleva la conveniencia de una clasificación y agrupamiento en niveles a los que se les asignaría el correlativo de protección criptológica, de forma que, de modo proporcional, se evite, tanto una exposición del sistema de información a riesgos derivados de una utilización de bajos niveles criptológicos, como un exceso de protección, asignando potentes y sofisticados sistemas, de alto coste, para protegerse de amenazas de escasa entidad, considerado desde una perspectiva global de los intereses del Estado y de la sociedad en su conjunto.

V.- CONCLUSIONES.

De todo lo anteriormente expuesto, se podrían establecer una serie de conclusiones que, a modo de resumen, exponemos a continuación:

1.- El derecho de secreto para los datos "sensibles" es una manifestación concreta de la "libertad informática".

2.- Las limitaciones a la "libertad informática" sólo son admisibles en el marco de un interés general superior con fundamento en los principios básicos de una organización democrática del Estado, reconocidos internacionalmente.

3.- La confidencialidad es una propiedad de la seguridad, en cuya protección interviene, de forma determinante los procedimientos criptológicos.

4.- El derecho al secreto de las comunicaciones es omnicomprensivo y ampara todo tipo de comunicaciones así como a cualquier medio o servicio que sirva para la transmisión de las mismas.

5.- El secreto de las comunicaciones aplicado a la información almacenada, tratada o transmitida electrónicamente viene a complementar y reforzar la "libertad informática", añadiendo un plus de confidencialidad en su faceta de derecho de secreto para los datos "sensibles".

6.- La protección efectiva del secreto de los datos "sensibles", además de la protección jurídica, requiere medidas de prevención que, "a priori", impidan materialmente el éxito de las amenazas contra los mismos, entre las cuales destaca por su importancia las de naturaleza criptológica.

7.- La protección criptológica permite de forma efectiva el ocultamiento de la información protegida, e impide su conocimiento por personas no autorizadas.

8.- La protección criptológica, como medio para que la "libertad informática" sea real y efectiva, se ha convertido en una exigencia imprescindible de cualquier sistema informático.

9.- En las comunicaciones privadas, la regla general es el secreto y, la excepción, la transparencia. En las comunicaciones públicas, la regla general es la transparencia y, la excepción, el secreto, de donde se deriva una exigencia de protección criptológica sistemática del "secreto de los datos sensibles".

10.- La protección criptológica de los datos "sensibles", se sitúa en el contexto de la aplicación de las nuevas tecnologías de la información en el entorno social, jurídico y político de una sociedad democrática, donde encuentra su reforzamiento y legitimación, pero también sus límites.

11.- Globalmente considerada, la protección criptológica de datos referidos a distintos ámbitos con intereses y derechos diferentes, requiere la adecuación de los niveles de protección a la naturaleza de la información protegida, de forma que haga posible el juego de los los distintos derechos concernidos.

12.- Los niveles de protección de una red han de ser proporcionales a las amenazas y demandan una clasificación por niveles criptológicos.

13.- La criptologia como instrumento para la ocultación de la información, no es inócua. Utilizada de forma abusiva o fraudulenta, puede, además de atentar con la libertad de información, puede, incluso, obstaculizar el normal desenvolvimiento de la sociedad y del Estado, a través de la creación de reductos impenetrables.

14.- La proporcionalidad entre lo que se pretende salvaguardar y las medidas de seguridad utilizadas, expresadas a través de la protección criptológica, no es sólo una cuestión de economía, ni, eventualmente, de orden público es, además, una cuestión de salud social.