# ASPECTOS JURIDICOS DE LA SEGURIDAD INFORMATICA Y LA PRIVACIDAD DE LOS DATOS PERSONALES

JAIME VALCARCEL RUBIO
Comandante

## INTRODUCCION

El desarrollo de las nuevas tecnologías de la información ha supuesto una transformación sustancial de las relaciones humanas, de la cultura, de la economía y de la política en nuestra sociedad, tal revolución técnica está produciendo un importante cambio social e institucional, por la rapidez y por la gran magnitud de sus consecuencias. El ritmo con el que crecen en los países más avanzados los instrumentos de la denominada "sociedad de la información" evolucionan en progresión geométrica y de su buen desarrollo desde un punto de vista armónico depende en gran medida nuestro futuro en el nuevo mundo que se vislumbra. La revolución tecnológica está sobrepasando los planteamientos actuales, la velocidad de crecimiento y la dependencia cada vez mayor del progreso tecnológico supera la del desarrollo social y acrecienta las desigualdades.

Todos los cambios tecnológicos traen consigo nuevas inquietudes, suponen reestructuraciones sociales y animan a nuevas perspectivas de progreso y bienestar social. Sin embargo, también traen consigo nuevas preocupaciones y problemas no planteados en el presente. Las nuevas tecnologías pueden propiciar un salto cualitativo hacia adelante siempre que se favorezca la generación y el acceso a la información al conjunto de la población para transformarlo en conocimiento compartido y fuente de progreso y riqueza colectiva.

Esta aceleración y globalización sobrepasa los mecanismos sociales de ajuste legislativo, no sólo en el ámbito temporal y territorial, sino también en el conceptual y el dogmático, donde, por ejemplo, el negocio jurídico efec-

tuado por medios electrónicos violenta en bastantes casos las concepciones tradicionales del Derecho.

Una de las grandes preocupaciones en muchos sectores de la sociedad a finales del año 1999 es qué ocurriría el 1 de enero del año 2000. No eran temores ancestrales ni milenaristas consecuencia del fin de siglo y milenio, sino la ignorancia de las consecuencias que se podían producir, en una sociedad tan industrializada en la que vivimos, por el denominado *efecto 2000*.

Actualmente la informática penetra en todos los campos, sistemas de control de pagos, de control del tráfico urbano, del tráfico aéreo o marítimo, hospitales, suministros eléctricos y de agua, sistemas de defensa y seguridad nacional, etc. Todo ello hace que la informática alcance una importancia inusitada en la ya sociedad del siglo XXI, sociedad que realmente merecerá el calificativo de "sociedad de la información".

Existen, pues, importantes riesgos que hay que prevenir y evitar antes de que ocurran, por ello las Administraciones Públicas tienen la obligación inmediata de tomar las medidas necesarias. Para ello es necesario que la Administración garantice la seguridad informática.

## INTERNET: UN NUEVO AMBITO

No podemos seguir hablando del fenómeno de Internet como una cuestión de futuro más o menos lejano, se está comenzando el camino de lo que será una sociedad hiperconectada que ve en Internet un sistema de abaratamiento de costes y de proceso de tratamiento de la información. Servicios básicos están en la actualidad ya prestándose a través de la red. Pensemos en nuestra propia Administración tributaria que premia a los contribuyentes que presenten sus declaraciones del IRPF por Internet con una devolución más rápida, o en la banca electrónica a través de Internet para ir haciendo desaparecer las sucursales físicas. El loable impulso de la Administración en el empleo y aplicación de los procedimientos electrónicos, informáticos y telemáticos en el desarrollo de su actividad es notorio y se ha hecho patente en la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas, LO 15/1999, RD 14/99 de firma electrónica, Ley Orgánica del Poder Judicial, Ley de Enjuiciamiento Civil, etc.

Efectivamente, la Ley 30/1992, modificada por la Ley 4/1999, establece en sus artículos 38 y 45 un mandato legal, con la finalidad de que la Administración impulse el empleo y aplicación de dichas técnicas en el desarrollo de su actividad y en el ejercicio de sus competencias, con las limitaciones que en la utilización de estos medios señalan la Constitución y las leyes. Se reconoce a los ciudadanos la facultad de relacionarse con las Administraciones Públicas a través de estos medios.

Concretamente, en el ámbito judicial, el artículo 230 LOPJ da validez al documento electrónico con las garantías necesarias de autenticidad e integridad, permitiendo el documento judicial electrónico y los actos de comunicación con la Administración de Justicia.

El comercio electrónico es un gran desconocido que va teniendo múltiples adeptos y entusiastas donde se manejan cifras dispares y hasta alarmantes, y aunque la realidad social no está aún suficientemente arraigado, sin embargo su implantación en el mercado creo que es irreversible.

La posibilidad de ofrecer productos y servicios a través de las denominadas *redes abiertas* ha modificado en gran medida la mentalidad del profesional y consecuentemente del mercado, ofreciéndose tal abanico de posibilidades que hasta hace poco hubiera parecido de ciencia ficción.

Estas redes adolecen de una falta de normativa que permita superar tiempos y espacios actuando en distintos lugares, con diferentes Ordenamientos Jurídicos, e incluso distintas actitudes y comportamientos. Por ello es necesario definir un marco jurídico adecuado y armonioso que permita su utilización superando fronteras e incluso soberanías estatales.

La internacionalización de las comunicaciones y la creación de lo que ha venido a denominarse la *aldea global* pone de manifiesto dos hechos sumamente importantes: por un lado, que mediante la utilización de Internet pueden cometerse una serie de delitos (estafas electrónicas, daños informáticos, revelación de secretos, publicidad engañosa, etc.),

por otro, la posibilidad de comisión de delitos transfronterizos cuya persecución escape a lo que hasta ahora se ha denominado el principio de territorialidad de las leyes y suponga, por tanto, la creación de paraísos informáticos, o lugares donde se pueda llevar a cabo con absoluta impunidad la comisión de determinados hechos delictivos.

La naturaleza humana en la red no difiere mucho de lo que se exhibe fuera de ella, sin embargo el hecho que permite a cualquiera ubicarse en cualquier punto del planeta en cuestión de segundos crea nuevas formas relación. La tecnología crea una sociedad *sin roce*, lo que nos permite huir de nuestro presente y pasado, pero en la que la violación de la intimidad, descubrir secretos sobre propios y extraños o encontrar víctimas potenciales de un fraude, abuso o delito es moneda corriente. Si en la red se vulnera la intimidad de una persona una sola vez, ésta ha quedado violada en el mundo entero y para siempre.

Esta evolución vivida en los últimos meses no viene acompañada, como debiera, con la aparición de nuevos derechos, sino más bien con el debilitamiento de los derechos constitucionales ya existentes como el de la intimidad.

## INFORMATICA E INTIMIDAD PERSONAL

Uno de los aspectos destacados de interacción entre tecnologías de la información y el derecho lo constituye la protección de los datos personales. Ello ha originado una intensa preocupación por lograr proteger la información personal, contenida en sistemas automatizados de datos, del empleo para fines distintos de aquellos para los que dicha información se suministró. La protección de datos personales es hoy en día una de las puntas de lanza de la colonización por el Derecho de la nueva sociedad de la información. Muestra de ello lo constituye la labor realizada por las organizaciones internacionales, como el Consejo de Europa, la Organización para la Cooperación y el Desarrollo Económico (OCDE) o la propia Unión Europea que han elaborado numerosas directrices en tal sentido.

La defensa de la intimidad personal en el ámbito de las telecomunicaciones se ha ido desarrollando paralela a los avances tecnológicos que se iban produciendo.

En un primer término se trató de cubrir mediante el correspondiente tratamiento penal y procesal la defensa de la intimidad frente a comunicaciones postales y telegráficas, para posteriormente amparar la intimidad frente a las comunicaciones telefónicas.

Los modernos y rápidos avances en materia de telecomunicaciones hacen necesario un planteamiento efectivo de defensa de la intimidad personal, esencialmente consecuencia de los riesgos derivados del almacenamiento y tratamiento informático de datos relativos a abonado y usuarios.

Los datos relativos a los abonados para el establecimiento de llamadas contienen información sobre la vida privada de las personas físicas y atañen a su derecho de que se respete su correspondencia, por lo que los datos sólo se podrán almacenar en la medida en que resulten necesarios para la prestación del servicio (para fines de facturación) siempre por un período limitado. Cualquier tratamiento posterior de dichos datos sólo se podrá realizar si el abonado ha prestado conformidad en base a una información clara y veraz que le debe ser facilitada sobre el tratamiento que se pretende llevar a cabo por el proveedor de servicios de telecomunicaciones.

Por razones de facturación el usuario de servicios de telecomunicación autoriza contractualmente al operador a registrar y a conservar aquellos datos (número de llamadas efectuadas en cada período de facturación, número de los abonados con los que se ha puesto en conexión, duración de la llamada, fecha y hora, etc.) que resultan indispensables para determinar el precio justo del servicio prestado y, por ello, para fundar una posible reclamación en caso de discrepancia o abuso.

La normativa sectorial de telecomunicaciones autoriza y regula el registro de los datos de tráfico de acuerdo con los principios de confidencialidad y anonimato establecidos en la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre que ordena con carácter general su destrucción inmediata tan pronto cese la comunicación y autoriza con carácter excepcional y restrictivo su conserva-

ción para fines de facturación por el tiempo absolutamente imprescindible.

El único uso autorizado de esos datos desviado de su fin primordial de facturación, el referente a la promoción comercial de los propios servicios del operador, exige inexcusablemente el consentimiento previo del abonado (art. 65.3, RD 1736/98).

La toma de datos a través de Internet generará la creación de grandes ficheros automatizados, pero se plantea qué ley es la aplicable al tratamiento automatizado de datos. Tengamos en cuenta que los datos se pueden tomar de una compañía situada en cualquier país no perteneciente a la Unión Europea a usuarios españoles, pero el peligro es que el nivel de protección de dichos datos no sea el mismo que el de la Unión Europea.

Por ello, la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, referente a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, dispone que los Estados miembros deben prever que la transferencia a un tercer país de datos personales sólo pueda efectuarse cuando el tercer país del que se trate garantice un nivel de protección adecuado, y cuando con anterioridad a la transferencia se respeten las disposiciones legales de los Estados miembros, adoptadas con arreglo a las demás disposiciones de dicha Directiva. Si bien, este nivel de protección de los datos debe evaluarse atendiendo a las circunstancias y condiciones que concurran en una transferencia de datos, por ello debe hacerse de una forma que no resulte una discriminación arbitraria entre terceros países y no constituya una restricción comercial.

La defensa de la intimidad personal frente al tratamiento automatizado de datos personales en el ámbito de los servicios de telecomunicación tiene su origen constitucional en el artículo 18.4 que dispone que *"...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..."*, y una regulación específica en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que derogó la LORTAD (Ley Orgánica Reguladora del Tratamiento Automatizado de Datos).

Como han señalado algunos autores, el mundo de la cibernética ha evidenciado un potencial lesivo para la intimidad cuya intensidad y eficacia resultaban inimaginables en contraste con las formas tradicionales o históricas de erosión o menoscabo del derecho fundamental a la intimidad.

Ya desde hace años en diferentes trabajos científicos y en posteriores desarrollos legislativos se viene solicitando una regulación restrictiva del uso de la informática que haga realidad el mandato contenido en la Constitución de 1978.

Paralelamente a esta petición de regulación, algunos autores tratan de introducir un nuevo concepto, más amplio de intimidad, en la medida que pueda suponer una mejor defensa de lo que constituye su núcleo esencial. Romeo Casabona (1) la define como *"aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento o desarrollo quedan reservados a su titular o sobre los que ejerce alguna forma de control cuando se ven implicados terceros"*. Morales Prats (2) sostiene que se ha asumido en nuestro derecho el de la cultura anglosajona, derecho a la *privacy*, lo que ha supuesto la tradicional concepción de la esfera privada, configurada en torno a un anacrónico concepto de libertad negativa. Para Lucas Murillo se hace necesario la inclusión en el catálogo de derechos un nuevo derecho fundamental que configure una nueva categoría con sustantividad propia.

La Exposición de Motivos de la LORTAD distinguía entre privacidad e intimidad, afirmando que *"...mientras la intimidad protege a esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona, el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de consideración intrínseca pero que, coherentemente enlazadas entre sí, arrojan un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado..."*.

No se trata de que la intimidad haya sido sustituida por la privacidad, sino que se ha producido una mutación de aquélla, de forma que lo que ahora llamamos privacidad no es más que la intimidad del presente siglo.

La LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, si bien no contiene una Exposición de Motivos, no ha desvirtuado las consideraciones que efectuaba la hoy derogada.

Existe un gran reto en la actualidad como es el de dar las mayores garantías en las relaciones comerciales a través de Internet, incluso simplemente de cualquier relación jurídica aunque sólo sea de comunicación o transmisión de datos o de información realizadas a través de este medio.

Pero hay una desconfianza al medio basada en la falta de seguridad física (ubicación de los centros de procesos, control físico de accesos, vigilantes, etc.), seguridad lógica (control de accesos a la información, cifrado de soportes magnéticos intercambiados entre entidades, etcétera) y seguridad jurídica.

La sola utilización del correo electrónico, sin entrar en mayores profundidades sobre la validez y eficacia jurídica de los contratos realizados por este medio, que modifica las concepciones tradicionales del Derecho, implica el análisis de tres grandes aspectos que es necesario abordar, la confidencialidad, la intimidad y la seguridad; aspectos que están íntimamente unidos y que no se pueden tratar por separado, sino que deben ser analizados en conjunto debido a las interrelaciones existentes entre ellos.

## PRIVACIDAD Y SEGURIDAD

Para Davara Rodríguez, con intimidad o esfera de la intimidad se hace referencia a aquellas cuestiones que se mueven o entran a formar parte o afectan al ámbito íntimo de la persona, la cual protege en el grado que considera adecuado.

La intimidad está protegida por el artículo 18, en sus cuatro apartados, de la Constitución, Título I, Sección que lleva por título "*De los derechos fundamentales y libertades públicas*".

Por confidencialidad se entiende el mayor o menor grado de secreto al que una persona quiere someter un dato o una información de carácter netamente personal.

Por privacidad, término que no se encuentra en nuestro Diccionario de la Lengua, se hace referencia, como he mencionado anteriormente, a los datos pertenecientes a una persona que analizados individualmente no tienen mayor trascendencia, pero al unirlos con otros pueden configurar un perfil claro sobre determinadas características de esa persona, por lo que ésta tiene derecho a exigir que permanezcan en su *ámbito de privacidad*.

Pues bien, para garantizar la intimidad, la privacidad, o incluso el grado de confidencialidad al que queremos someter una información es necesaria la existencia de medidas de seguridad, mediante una normativa técnica y jurídica que asegure en la medida de lo posible las relaciones jurídicas a través de los nuevos medios tecnológicos.

Con ese fin, por RD 994/1999, de 11 de junio, se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, que determina las medidas básicas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Este Reglamento establece tres niveles de seguridad (básico, medio y alto) atendiendo a la naturaleza de la información tratada en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico. Los que contengan datos referentes a la comisión de infracciones administrativas, penales, con Hacienda, etc., deberán reunir además de las medidas de nivel básico, las de nivel medio. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, y los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas, deberán reunir además de las medidas de nivel básico y medio las medidas de nivel alto.

El incumplimiento de las medidas de seguridad descritas en este Reglamento será sancionado, por ello los responsables de los ficheros deberán adoptar las medidas necesarias, de índole técnica y organizativas, que garanti-

cen la seguridad de los datos de carácter personal.

## EL DERECHO A LA PROTECCION DE DATOS DE CARACTER PERSONAL

El derecho a la protección de datos de carácter personal, o derecho de autodeterminación informativa (como fue denominado por el Tribunal Federal Alemán en su trascendental sentencia de 15/12/1983), consiste en un conjunto de facultades mediante las que se pretende que el individuo controle el flujo de datos derivados de sus relaciones personales y sociales en el seno de la comunidad.

El contenido de estos derechos se recogió en el Título III de la LO 5/1992 (LORTAD), ampliado por la Directiva 95/46/CE en su artículo 14, que añade el derecho a la oposición al tratamiento automatizado de datos por causa legítima. En la actualidad se encuentran en el Título III de la LO 15/1999, artículos 13 a 19.

Estos derechos básicamente son los siguientes:

- Derecho a ser informado sobre el tratamiento a que van a ser sometidos sus datos personales, finalidad del mismo y responsable de éstos.
- Acceder a sus datos, rectificarlos y cancelarlos cuando no sean precisos a los fines que motivaron su recogida.
- A la impugnación de valoraciones basadas únicamente en un tratamiento de datos destinado a evaluar determinados aspectos de su personalidad.
- A reclamar ante la Agencia de Protección de Datos (que tiene un plazo máximo para resolver de 6 meses); contra las resoluciones de la citada Agencia podrá interponer recurso contencioso-administrativo.
- A ser indemnizado en caso de originarse daños en sus bienes o derechos por dicho tratamiento. Si los ficheros son de titularidad pública, la responsabilidad se regirá conforme al régimen de responsabilidad patrimonial o extracontractual de las Administraciones Públicas. Si los ficheros son de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

Su naturaleza de derecho fundamental, amparada en los apartados 1º a 3º del artículo 18 de la Constitución, fue reconocida por la sentencia del Tribunal Constitucional número 254 de 20 de julio de 1993, y reiterada en sentencias posteriores (3).

Las normas sobre protección de datos desde el Convenio 108 hasta la Directiva 95/46/CE contemplan una serie de definiciones y principios que diseñan, junto a los derechos antes mencionados y los mecanismos institucionales de protección, la denominada autodeterminación informativa.

Estas definiciones se encuentran en el artículo 3 de la LO 15/1999, que derogó la LORTAD, y el RD 1332/1994, de 20 de junio.

Según la Ley, se entenderá por datos de carácter personal cualquier información concerniente a personas físicas identificadas o identificables.

Se entiende por fichero todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización o acceso.

Por cesión o comunicación de datos toda revelación de datos realizada a una persona distinta del interesado.

Respecto a la cesión, recientemente el Pleno del Tribunal Constitucional ha estimado el recurso de inconstitucionalidad presentado por el Defensor del Pueblo contra los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD).

El artículo 21.1 establece la posibilidad de que se puedan ceder datos, de carácter personal, de una Administración a otra cuando dicha comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso.

El artículo 24.1 regula que lo dispuesto en los apartados 1 y 2 del artículo 5 (derecho a la información a los interesados en la recogida de datos) no será aplicable cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas... o administrativas.

El artículo 24.2 hace referencia a que los derechos recogidos en el artículo 15 (acceso a sus datos por los propios interesados) y en el 16 (rectificación y cancelación de datos) no se podrán ejercer por los interesados si ponderados los intereses en presencia estos derechos hubiesen de ceder ante razones de interés público o ante intereses de terceros más dignos de protección.

El Defensor del Pueblo argumenta que el inciso del artículo 21 de la LOPD impugnado vulneraría la Constitución al permitir la cesión de datos para fines diferentes a aquellos para los que han sido recabados, sin consentimiento ni conocimiento del interesado y con cobertura en una norma de rango inferior a la Ley. Con ello el artículo 21.1 contiene una excepción a la regla del artículo 11 LOPD según la cual la cesión de datos sólo es posible previo consentimiento del interesado. La LOPD posibilitaría la cesión de datos entre Administraciones Públicas para fines distintos a los que motivaron su recogida, y el titular de los mismos no estaría informado de la posibilidad de dicha cesión, ni la propia cesión se realizaría con consentimiento del afectado.

Como decimos, el Defensor del Pueblo también impugna en su recurso el artículo 24.1 de la LOPD, que exime a la Administración de cumplir con sus obligaciones de información y advertencia del artículo 5.1 y 2 (facultades de acceso a los datos, de rectificación y cancelación de los mismos y de oponerse a su tratamiento automatizado). Estas excepciones a los derechos de los titulares de los datos lesionan el contenido esencial del derecho fundamental a la intimidad frente al uso de la informática (artículos 18.1 y 4, y 53.1 de la Constitución).

Por último se impugna, por el Defensor del Pueblo, el artículo 24.2 al no respetar el contenido fundamental de los derechos fundamentales al honor y a la intimidad personal y familiar. La referencia al interés público es una cláusula en blanco bajo la que puede tener cobijo toda la actividad administrativa, ya que toda la actividad administrativa sirve a ese interés. La mención a intereses de terceros dignos de protección tampoco la considera aceptable.

## LA PROTECCION DE LOS DATOS PERSONALES: INFRACCIONES Y SANCIONES ADMINISTRATIVAS

Se regulan en el Título VII de la LO 15/1999, artículos 43 a 48.

### SUJETOS SOBRE LOS QUE RECAE

Están sujetos al régimen sancionador establecido en la Ley los responsables de los ficheros y los encargados de los tratamientos.

### TIPOS DE INFRACCIONES

Las infracciones se clasifican en leves, graves y muy graves.

*Infracciones leves:* Son entre otras las siguientes, no atender por motivos formales la solicitud del interesado a la rectificación o cancelación de datos personales cuando proceda, no proporcionar la información que solicite la Agencia de Protección de Datos, no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, incumplir el deber de secreto salvo que constituya infracción más grave.

*Infracciones graves:* Entre otras, crear ficheros de titularidad pública o recoger datos personales para los mismos sin autorización de disposición general publicada en el BOE o Diario Oficial correspondiente, crear ficheros de titularidad privada con finalidades distintas de lo que constituye el objeto de la empresa o entidad, tratar o usar los datos de carácter personal con conculcación de los principios y garantías de la ley, impedir el derecho de acceso y negativa a facilitar información solicitada, vulneración del deber de guardar secreto de datos referentes a infracciones administrativas o penales o de la Hacienda Pública, obstruir la función inspectora, etc.

*Infracciones muy graves:* Entre otras, recoger datos de forma engañosa y fraudulenta, la comunicación o cesión de los datos de carácter personal fuera de los casos en que esté permitida, tratar los datos de forma ilegítima o con menos precio de las garantías que les sean de aplicación cuando atente a los derechos fundamentales, la vulneración del deber

de guardar secreto de los datos especialmente protegidos así como de los recabados para fines policiales, etc.

SANCIONES

Las infracciones leves se sancionan con multa de 100.000 a 10.000.000 de pesetas, y prescriben dichas infracciones al año de haberse cometido la misma.

Las graves se sancionan con multa de 10.000.000 a 50.000.000 de pesetas, y prescriben a los dos años.

Las muy graves se sancionan con multa de 50.000.000 a 100.000.000 de pesetas, y prescriben a los tres años.

La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a los interesados y terceras personas, y a cualquier otra circunstancia que sea determinante para fijar el grado de antijuricidad y de culpabilidad presentes en la acción infractora.

El procedimiento sancionador se ajustará a lo dispuesto en el Capítulo V (arts. 18 y 19) del RD 1332/94, de 20 de junio, que continúa en vigor en virtud de lo dispuesto en la disposición transitoria tercera de la LO 15/1999.

Si las infracciones se cometiesen en ficheros de los que sean responsables las Administraciones Públicas, el Director de la Agencia de Protección de Datos podrá proponer el inicio de actuaciones disciplinarias, si procedieran, conforme a la legislación sobre régimen disciplinario de las Administraciones Públicas.

## LA PROTECCION PENAL DE LOS DATOS PERSONALES

El Código Penal de 1995 incorporó el derecho a la intimidad y a la propia imagen entre aquellos bienes jurídicos que deben ser objeto de protección.

Según Martín-Casallo, la nueva regulación de lo que se denomina delito informático puede configurarse como un agotamiento del mandato constitucional del artículo 18.4, en cuanto ha permitido el desarrollo de una legislación específica sancionadora en materia de protección de datos que se hallaba constituida antes de su aparición fundamentalmente por la LO 5/1992, de 29 de octubre (LORTAD), por la Directiva 95/46/CE, de 24 de octubre de 1995, y por el Convenio 108 del Consejo de Europa de 28 de enero de 1981.

La protección penal de la información no se agota en la regulación contenida en los artículos 197 y siguientes del CP, sino que se proyecta sobre otros tipos penales como el de receptación de la información secreta de las empresas (art. 280), y los delitos de información privilegiada (art. 284) o relevante (art. 285).

La doctrina no considera adecuada la denominación de delito informático a la figura tipificada en el artículo 197.2 del CP. Concretamente, a Bueno Arús (4) le parece discutible la expresión delito informático por ser un concepto ambiguo con el que se puede aludir bien a los delitos que recaen sobre objetos pertenecientes al mundo de la informática: destrucción o sustracción de programas o de material, alteración, destrucción o reproducción de datos almacenados, utilización indebida de los ordenadores, o bien a la comisión de los delitos más variados y tradicionales: delitos contra la intimidad, delitos contra la fe pública, delitos contra el patrimonio, delitos contra la Administración Pública, delitos contra la seguridad nacional.

Falta, pues, una definición de lo que debe entenderse por delito informático, con perfiles concretos y límites precisos que lo diferencien de otras figuras.

Martín-Casallo entiende que es más conveniente cuando se hable de las conductas tipificadas en el artículo 197.2 del CP referirse a atentados contra la intimidad personal cometidos sobre datos que se hallan registrados en soportes informáticos, electrónicos o telemáticos.

EL DELITO CONTRA LA LIBERTAD INFORMATICA DEL ARTICULO 197.2 DEL CODIGO PENAL

Según Morales Prats (5), el artículo 197.1 contiene el tipo básico de apoderamiento de documentos (papeles, cartas, mensajes de

correo electrónico) y abarca la interceptación de comunicaciones, en el se establece que *"El que para descubrir los secretos o vulnerar la intimidad de otro sin su consentimiento se apodera de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de 12 a 24 meses".*

Por otro lado, el artículo 197.2 dispone que *"Las mismas penas se impondrán al que sin estar autorizado se apodere, utilice o modifique en perjuicio de tercero datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero".*

El ámbito que regula el artículo 197.2 hace referencia más propiamente a los datos de carácter personal, a la protección de los datos personales con independencia de que hayan sido objeto o no de tratamiento automatizado. No tiene cabida en este apartado, en cuanto a su protección, los datos personales que integren el contenido de un mensaje de correo electrónico, por hallarse previsto expresamente en el apartado 1º de este artículo 197.

Por otro lado, los datos personales que figuren en Internet sí tienen cabida dentro de este número 2º, ya que es posible la realización de las conductas en él descritas sin que necesariamente supongan la interceptación de comunicaciones, figura comprendida en el apartado 1º.

Este artículo 197.2 en opinión de la sentencia del Tribunal Supremo (Sala 2ª) de 18 de febrero de 1999 describe el tipo básico de los llamados por la doctrina delitos contra la libertad informática, es un nuevo derecho de autotutela de la propia identidad informática, que no es otro que el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en un programa electrónico.

Esta sentencia continúa diciendo que *"...parece razonable que no todos los datos reservados de carácter personal o familiar puedan ser objeto del delito contra la libertad informática, debe entenderse que la norma requiere la existencia de un perjuicio añadido, que puede afectar al titular de los datos o a un tercero, que se produce siempre que se trata de un dato que el hombre medio de nuestra cultura considera sensible por ser inherente al ámbito de su intimidad más estricta...".*

De lo anterior se pueden extraer dos conclusiones:

1. No todo dato personal o familiar es capaz de producir un perjuicio, por lo que no daría lugar a la existencia del delito previsto en el artículo 197.2.
2. Se establece la presunción *iuris tantum* de que toda acción efectuada contra los denominados datos sensibles siempre ocasionan el requisito del perjuicio y por tanto es de aplicación el tipo penal del artículo 197.2.

Por ello cabe hacer las siguientes consideraciones:

1. Todo dato personal es por sí mismo un dato reservado, y no existen datos personales que, en principio, queden fuera del campo de aplicación del artículo 197.2.
2. La aplicación del citado tipo penal dependerá exclusivamente del ánimo de causar perjuicio (dolo), siendo éste el elemento diferenciador en la aplicación del tipo penal o de las faltas administrativas (del Título VII de la LO 15/1999).
3. Acreditada la existencia de dicho elemento subjetivo del injusto, las conductas efectuadas sobre la categoría de los datos sensibles (ideología, religión, creencias, salud, origen racial o vida sexual), objeto de una especial protección, darían lugar a la agravación de la pena prevista conforme al apartado 5º del artículo 197.

## LOS TIPOS AGRAVADOS

Se recogen en los artículos 197 y 198 del Código Penal.

El artículo 197 contempla cuatro figuras o supuestos de agravación perfectamente diferenciados:

1. El artículo 197.3, que alude a comportamientos consistentes en la difusión, revelación o cesión a terceros de datos o hechos descubiertos o imágenes captadas a que se refieren los números anteriores.

Refiriéndonos en concreto a los datos personales, las conductas agravatorias del tipo básico suponen una actividad posterior, así tras el acceso, apoderamiento, utilización o modificación, lo que se castiga con mayor rigor es la conducta de difusión, revelación o cesión a terceros. Esta participación de tercero o terceros junto al que hasta ahora había sido el único sujeto activo de la infracción es la causa justificativa de la agravación en cuanto a que la intimidad, bien jurídico protegido, sufre un deterioro añadido por la participación de ese tercero o multitud de terceros en el conocimiento de lo que constituye la intimidad del hecho transferido al conocimiento de aquéllos.

También se contempla, en el apartado 2º del artículo 197.3, el conocimiento ilícito de los datos seguido de su difusión, pero sin haber tomado parte en el descubrimiento. No contempla, sin embargo, el conocimiento lícito de los datos seguido de una posterior difusión de los mismos, lo que daría pie a considerar lícitas, por no punibles, conductas que revelasen, cediesen o difundiesen datos no consentidos de forma expresa por su titular, partiendo de una situación inicial de licitud en cuanto a la recogida del dato y su tratamiento.

2. El artículo 197.4 sanciona con mayor dureza a aquellos sujetos que ocupan una posición dominante en el tratamiento de los datos personales. De esta posición se deriva un deber de secreto vulnerado por su actuación ilícita.

3. El artículo 197.5 contempla otro supuesto de agravación de la pena tipo, la razón de ello es múltiple.

Por un lado se atiende a la naturaleza especialmente sensible de determinados datos personales: ideología, religión o creencias, origen racial, salud y vida sexual.

Por otro se contemplan los supuestos en que la víctima fuese un menor de edad o un incapaz.

4. El artículo 197.6 contempla el supuesto en el que el sujeto activo del delito actúe movido con fines lucrativos, no siendo necesario que este objetivo de lucro sea alcanzado por el autor, bastando simplemente que se realice con la finalidad de obtener una ventaja patrimonial antijurídica.

Por último, el artículo 198 recoge el supuesto en el que es un funcionario público o autoridad el que prevaliéndose de su cargo realiza cualquiera de las conductas descritas en el artículo 197. A este tipo delictivo le corresponden las penas previstas en el artículo 197 en su mitad superior, además de la inhabilitación absoluta de 6 a 12 años.

En todo caso, y en virtud de lo dispuesto en el artículo 201, para proceder por los delitos previstos anteriormente es necesario que exista denuncia de la persona agraviada, o de su representante legal.

## CONCLUSION

El derecho fundamental a la protección de datos de carácter personal pretende garantizar a toda persona un poder de control sobre cualquier tipo de dato personal, sobre su uso y sobre su destino, con el fin de evitar su tráfico ilícito y lesivo para la dignidad y derecho del interesado.

Este derecho alcanza también a los datos personales que podríamos denominar públicos, que por el hecho de serlos, y por ello accesibles al conocimiento de cualquiera, no escapan al poder de disposición del interesado.

Por ello la Administración debe tomar las medidas de seguridad informática necesarias para garantizar la confidencialidad y la integridad de los datos de carácter personal con el fin esencial de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración y tratamiento o acceso no autorizado.

La seguridad informática es un asunto de Estado. Como en la vida real, en Internet no existirá libertad si no hay seguridad.

Por ello es deseable que se pongan en marcha medidas en el marco de la cooperación internacional para luchar contra el fraude en Internet. El éxito de la lucha contra la delincuencia informática será mayor cuanto más se concierte la actuación, en esta materia, de los distintos Estados.

En el fenómeno de la criminalidad informá-

tica se pueden constatar tres aspectos, su complejidad técnica, el carácter fugaz de sus acciones y su condición, en muchos casos, internacional. La ausencia de mecanismos de respuesta rápida en el seno de los poderes coercitivos nacionales ha motivado la necesidad de incrementar la respuesta policial ante los delitos informáticos.

Los mecanismos de cooperación policial existentes en el ámbito de la Unión Europea muestran el futuro de lo que será la respuesta policial de los años venideros, una unidad policial (Europol) potenciada por sistemas informáticos de tratamiento y análisis de la información, con funciones de coordinación de operaciones de inteligencia policial, y a la que se pretende dotar, en un futuro no muy lejano, con funciones operativas.

NOTAS

(1) La reforma penal ante las nuevas tecnologías de la información.

(2) El Código Penal de 1995 y la protección de datos personales.

(3) Sentencias 33, 35 y 95 de 1998 y 123, 124, 125 y 126 de 15 de junio de 1998.

(4) "El delito informático", Actualidad Informática Aranzadi número 11, abril 1994.

(5) Comentarios al Código Penal, parte especial.