ENSAYO JURÍDICO DE DERECHO INFORMATICO

DERECHOS FUNDAMENTALES, INFORMATICA Y NORMAS PENALES

LA VISION IUSINFORMATICA DE LA INTIMIDAD Y LOS DELITOS RELATIVOS A LOS DATOS PERSONALES INFORMATIZATIDOS.

Por:

Libardo Orlando Riascos Gómez
Doctor en Derecho
lriascos@alumni.unav.es
2008

ABSTRACT

El objeto principal de la presente investigación bibliográfica es analizar, estudiar y cuestionar de la visión ius informática del derecho fundamental a la intimidad, conocido como derecho de "habeas Data" o derecho de autodeterminación informativa en el derecho español y alemán. Una de las instituciones jurídicas relacionadas con esta visión ius informática del derecho es el llamado "*delito informático*". El Delito informático se analiza en el derecho comparado norteamericano, europeo, australiano y colombiano. En el ámbito penal se estudia: El bien jurídico tutelado, los diferentes tipos penales y los medios comisivos del delito o medios electrónicos, telemáticos o informáticos.

Palabras Claves: Derechos, Intimidad, visión ius informática, delito, medios electrónicos o telemáticos, Constitución, legislación.

ABSTRACT

The main object of the present bibliographical investigation is to analyze, to study and to question of the vision computer ius from the fundamental right to the intimacy, well-known as right of "habeas Data" or right of informative self-determination in the Spanish and German right. One of the juridical institutions related with this vision ius informatic of the right is the call "*computer crime*." The computer Crime is analyzed in the North American, European, Australian and Colombian compared right. In the penal environment it is studied: The property juridical protégé, the different penal types and the commisive means of the crime or electronic, telematic or computer means.

Key words: Rights, Intimacy, vision ius computer, crime, electronic or telematic means, Constitution, legislation.

CONTENIDO

5.2.2.2. Parte In fine del tipo: La interceptación o la intervención..
5.2.3. Los "Datos Sensibles" de la persona humana.
5.2.3.1. Información personal del concernido.
5.2.3.2. Diferentes grados de protección de los datos o informaciones personales del concernido. El consentimiento.
5.2.3.3. Protección penal de los datos sensibles, en el artículo 197 del C.P. Español.

DESARROLLO:

5.1. Estructura General del delito.

5.1.1. Notas preliminares básicas.

En este apartado no pretendemos diseccionar finamente los pormenores de los delitos contra *la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio,* previsto en el Título X, artículos. 197 a 201, del Código Penal Español de 1995, sino sólo aquellos delitos denominados contra *los datos personales registrados en forma automatizada (informática y/o telemáticamente) contra la intimidad*, que aún estando subsumidos en el título mencionado, constituyen una vertiente plenamente identificable dentro del contexto, entre otras razones, por las siguientes:

a) Porque como lo ha determinado el Tribunal Constitucional Español, al analizar la influencia actual de la informática con relación al derecho a la intimidad prevista en el artículo 18.4 CE, concluyó que se ha *incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama "la informática"* [66] .

b) El bien jurídico objeto de tutela estatal en el título X del Código Penal Español de 1995, es sin lugar a dudas la *Intimidad*, como derecho fundamental, autónomo y limitado de la persona, o como genuinamente se concibió en el ensayo de Warren y Brandeis: un derecho a la "*inviolabilidad de la persona",* que incorpora; por un lado, las facultades de no hacer, de abstención o de exclusión (en términos de Cooley, *Right to be let alone)* de cualquier atentado contra de " *la dignidad y la convivencia de un individuo en la sociedad o en sus relaciones sociales y familiares "* [67]; y de otro, el derecho precisado años más tarde por *Westin* y consistente en el derecho al control a la información referente a uno mismo (*A Right to control information about oneselft).* Este última faceta de la intimidad se potenciaría con el advenimiento de las nuevas tecnologías de la información y comunicación (TIC) y la informática , a partir de la segunda mitad del s. xx., como hemos anotado en esta investigación; y sobre todo cuando la *información* potencia su esencia conceptual de ser todo aquello que *nos proporciona conocimiento* [69] y por ende, protegible y/o vulnerable.

c) Recientes decisiones del Tribunal Constitucional Español (SSTC 254/1993 , Mayo 9 de 1994, Enero 13 de 1998 y Marzo 16 de 1998), enfatizan que "el artículo 18.4 de la CE incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona: derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos". Así como que la *libertad informática* "*es un derecho a controlar el uso de los mismos datos insertos en un programa informático* (*habeas data*)" .

.

d) Porque los denominados delitos de los datos de carácter personal contra la intimidad son conductas típicas surgidas como producto indefectible y concomitantemente con las nuevas tecnologías de la información y la comunicación (TIC), en las modernas *sociedades de la información* [70] , y en los que los sujetos emplean medios comisivos o de ejecución del *iter criminis* de naturaleza electromagnética o computacional y dispositivos o aparatos informáticos y/o telemáticos.

e) *Los términos iusinformáticos: datos de carácter personal*, fichero automatizado o bancos de datos, tratamiento de datos, responsable del fichero, *afectado* (por titular o interesado) y procedimiento de disociación se interpretan en el Código Penal Español, con base en la normativa extrapenal, básicamente en el Convenio del Consejo de Europa de 1981 y la Directiva del Parlamento Europeo y del Consejo de la Unión Europea de 24 de octubre de 1995, relativas 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 como no, en las definiciones que la LORTAD, trae en el artículo 31, pues se ha hecho una práctica inveterada que el legislador acuda a definiciones técnico-jurídicas, que aunque en no pocas veces producen colisiones o dificultades en su comprensibilidad diáfana al operador jurídico, resulta a la vista de la visión ius-informática de los derechos y libertades fundamentales --como hemos comentado en nuestros escritos electrónicos referidos a la Visión Ius-informática del Derecho a la intimidad en ésta página de WEB-- el glosario mínimo necesario que aquél debe observar para la interiorización de la norma jurídica, la técnica TIC y la informática, y sobre todo para discernir el espíritu de la norma jurídica y aplicarla en cada caso *sub judice* en un momento histórico determinado.

Como se ha analizado en el escrito electrónico sobre la Visión Ius-informática del derecho a la intimidad, La Directiva 95/46/CE y la Directiva 97/66/CE, amplían el glosario de definiciones aplicables al procedimiento de ingreso, tratamiento, divulgación y tele-transmisión y protección de datos de carácter personal, ya que el fenómeno TIC y la informática, día a día evoluciona y las ciencias jurídicas deben asimilar esa evolución reflejándola en los términos jurídico-técnicos: interesado, tratamiento (por almacenamiento, registro, transmisión, difusión, interconexión, bloqueo, supresión o destrucción, etc), fichero, responsable del tratamiento (más amplio que el del fichero), encargado del tratamiento, tercero, destinatario y consentimiento del interesado (como toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan) [71] . Por tanto, el operador jurídico en las áreas del derecho civil, administrativo y penal deberá acudir a ellas cuando se trate de aplicar una interpretación mínima o gramatical para escrutar el espíritu de las normas jurídicas referentes a la visión ius-informática de los derechos.

f) En la visión ius-informática de los derechos se parte del concepto tradicional de *documento impreso, escrito* o *similares* para definir y precisar el concepto de docu*mento informático* contenidos en *soportes o aplicaciones informáticas y electrónicas (v.gr."Los mensajes de correo electrónico") o telemáticas* (no sin alguna resistencia teórica v.gr. El Internet y la problemática de los derechos fundamentales en el *ciberespacio:"Netlaw"* [72] , Los documentos EDI: Electronic Data Interchange o IED: Intercambio electrónico de datos) [73] , como objetos materiales sobre los que recae la actividad ilícita de *apoderamiento (por acceso), utilización, modificación* de datos reservados con carácter personal, o a los cuales se *accede* para *alterar o utilizarlos* en perjuicio del titular de los datos o de un tercero.

Tanto la jurisprudencia como la legislación han reconocido la existencia de los llamados documentos informáticos, electrónicos y telemáticos. En efecto, el Tribunal Supremo de España, Sala 20 en sus múltiples decisiones ha reconocido la existencia de los *documentos informáticos*, a partir del concepto de documento impreso, escrito, similar o tradicional (STSS 19/04/91. FJ.4. M.P. Soto Nieto; 14/11/93.FJ.3. M.P. Puerta Luis; y, 3/06/94. FJ.1. M.P. Martín Canivell; entre otras.), o bien aplicando el artículo 26 del nuevo Código Penal Español de 1995 (STSS: 10/07/96. FJ.6.M.P: Soto Nieto; 121/1997, y 3/2/97.FJ.2, M.P: Joaquín Delgado García); pero al fin y al cabo, *documento informático* desde el punto de vista del hardware y software [74] , como precisaremos al final de éste ensayo jurídico en documento electrónico.

Por su parte, la Ley 30 de 1992, Ley de Régimen jurídico de las administraciones públicas y del procedimiento administrativo común (LPRJPA, antes LPA), al regular las relaciones de los ciudadanos con la Administración General del Estado, destaca la incorporación de las nuevas tecnologías TIC en vida ius-administrativa y, particularmente denota, la "*validez y eficacia de documento original* " a los obtenidos con "*medios electrónicos, informáticos o telemáticos*". Si bien la existencia de éstas modalidades de documento informático se hallan curiosamente desintonizadas con la LORTAD, a pesar creemos que en la realidad y práctica normativa deben no sólo sintonizarse sino de expedirse por el mismo año y fecha [75] y regular el fenómeno TIC en el derecho, interpretarse hermenéuticamente como norma extrapenal que ayuda a entender los términos técnicos que el Código Penal Español emplea en el Título X, aparentemente divorciado de éstos.

g) Por referirse al descubrimiento y revelación de *secretos documentales informáticos,* sin consentimiento del titular, como una gama de las variopintas previstas en el tipo penal muy amplio que las protege: artículo 197 del Código Penal Español [76] ;

h) Por referirse al control auditivo o audiovisual clandestino de datos de carácter personal [77] a través de la interceptación con medios electromagnéticos que unen las telecomunicaciones y la informática (v.gr. TIC-Interactivo: Imagen, sonidos y datos: La multimedia); y,

i) En cuanto a los sujetos activo y pasivo; los verbos rectores (apropiar, usar, utilizar, interceptar, acceder, revelar, descubrir, divulgar); la base normativa penal y extrapenal (LORTAD, L.O 5/1992, de Oct. 29; Directiva 46/95/CE; Convenio Europeo de 1981); las modalidades de las conductas agravadas del tipo penal básico (v.gr. Si se realizan por personas responsables o encargados de ficheros, personas menores o incapaces, por cometerse en los *datos sensibles* [78] , --por regla general, exentos de tratamiento automatizado, según las normas comunitarias--, o con fines lucrativos), y la penalidad, son similares a los aplicados para los delitos contra la intimidad y demás derechos de la persona humana, estipulados en el Título X, del Código Penal Español Igualmente, y sobre éste último aspecto, particularmente en cuanto a la gravedad de las penas que se establecen para casi todos los supuestos pueden llevar en algún caso a violar el *principio de culpabilidad*, pues a la infracción cometida se le fija una pena desproporcionada [79] , como puntualizaremos más adelante.

5.1.2. Tipos delictivos.

El delito de los datos o las informaciones de carácter personal que atenta la visión ius-informática del derecho fundamental a la intimidad de las personas en la estructura actual del Título X, Cap. I del Código Penal Español de 1995, es un planteamiento doctrinal que pretende mostrar el cúmulo de figuras delictivas (previstas o no en la legislación penal [80]) saturadas o condicionadas por las nuevas tecnologías de la información y la comunicación (TIC) y los medios automatizados electromagnéticamente. Es decir, aquellos tipos delictivos denominados de *Descubrimiento y Revelación de Secretos*, a través de medios informáticos y/o telemáticos que *" el legislador regula... de una forma realmente complicada, con algún artículo interminable y de difícil concreción, lo que lleva a la inseguridad jurídica"* [81] . Súmese a ello, que en el artículo 197.1 del Código Penal Español, contiene objetos materiales del hecho punible, como los llamados "*mensajes de correo electrónico"*, que técnica, jurídica, sistemática e ius-informáticamente mejor ubicados quedarían en el numeral 2 del artículo 197. Igualmente el artículo 197.2 id., contiene acciones punitivas sinónimas al tipificar doblemente la *"utilización de datos"*, tanto en el apartado primero como en el segundo. Estos y otros aspectos que son aparentemente son fruto del "*desconcierto y la precipitación (lo que) han presidido la creación de este precepto"* [82] , tal como precisaremos y ampliaremos

Pese a ello, y a la vista de la actual redacción que el Código Penal Español se erigen los Delitos de "Descubrimiento y Revelación de Secretos" contra la intimidad y el derecho a la propia imagen (Tit. X). Las tipos delictivos básicos de los delitos que llamamos de los datos o informaciones de carácter personal contra la intimidad, previa la transcripción de la norma penal vigente, son:

> **Artículo 197-1**. *El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere 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 doce a veinticuatro meses*.

a) Delito de Acceso a los documentos informáticos ("mensajes de correo electrónico") en soportes electrónicos, previsto en el artículo 197.1, *ab initio* del Código Penal Español más adelante.

b) Delito de interceptación de documentos informáticos en soportes electrónicos o telemáticos, previsto en el artículo 197.1, *in fine* del Código Penal Español

> **Artículo 197-2.** *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.*

c) Delito de acceso, utilización y alteración de datos o informaciones de carácter particular o familiar registrados en documentos informáticos, electrónicos o telemáticos, previstos en el artículo 197.2 Id.

Los tipos delictivos agravados, son:

> **Artículo197- 3.** *Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.*

a) Por la difusión, revelación o cesión a terceros de datos informáticos y/o telemáticos (artículo 197.3. *ab initio*).

> **Artículo197-4.** *Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.*

b) Son dos tipos agravados fundidos en un inciso, con diferente pena: El primero, por la condición calificada del sujeto activo del delito al actuar como encargado o responsable del fichero o banco de datos informatizados o telemáticos (artículo 197. 4. *ab initio*). El segundo, por la conducta subsiguiente realizada por el sujeto activo, es decir, por la difusión, cesión o revelación de los datos (artículo197.4 *in fine).*En este última caso la pena es super agravada.

> **Artículo 197-5.** *Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.*

c) Son dos tipos agravados fundidos en un mismo inciso, con igual pena aumentada, por la afectación y calidad de los datos y la *capitis diminutio* de la víctima: El primero, por la afectación a los datos de carácter personal, considerados "*sensibles*" o constitutivos del *"núcleo duro*" de la intimidad (artículo 197.5, *ab initio* del Código Penal Español). El segundo, es por la condición cualificada de la víctima del delito (ser menor o incapaz), según el artículo 197.5, *in fine* del Código Penal Español

> **Artículo 197-6.** *Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 a 4 de este artículo en su*

mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

d) Nuevamente son dos tipos agravados en un mismo inciso, con diferente pena impuesta, pero en la parte *in fine* se establece un tipo agravado potenciado de ultraprotección, se entiende, a los datos sensibles y no a la condición de *capitis diminutio* de la víctima. El primero, será por la realización con fines lucrativos de los tipos básicos a), b), c) y/o los tipos agravados previstos en el literal a), b), c) --artículo 197.6 *ab initio*--. El segundo, se entiende un tipo ultragravado --si nos permiten el término--, si se realiza además del fin lucrativo sobre los datos sensibles, es decir, contra la ideología, religión, creencias, salud, origen racial o vida sexual (artículo 197.6. *in fine).*

> **Artículo 198.** *La autoridad o funcionario público que, fuera de los casos permitidos por la ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualesquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.*

e) Por la condición calificada del sujeto activo, al actuar como autoridad o funcionario público, en circunstancias especiales y prevaliéndose de su cargo y con imposición de penas principales (prisión) y accesorias (inhabilitación absoluta del cargo) --artículo 198 Código Penal Español--

Como tipo atenuado del tipo agravado previsto en el artículo 197.3. Código Penal Español

> ***Artículo 197. 3. Parte In fine****. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que con conocimiento de su origen ilícito y sin haber tomado parte de su descubrimiento, realizare la conducta descrita en el párrafo anterior.*

f) Es el tipo atenuado por la difusión, revelación o cesión a terceros de datos informáticos y/o telemáticos, que requiere para su configuración, lo siguiente: a) Conocimiento del origen ilícito de los datos, b) No tomar parte en el descubrimiento o revelación de los mismos, c) Realizar las conductas previstas en la parte *ab initio* del artículo 197.3, es decir, la difusión, revelación o cesión a terceros de los datos (Artículo 197.3. *ab initio*) y d) La pena impuesta es menor que la impuesta al tipo agravado del artículo 197.3 *ab initio,* pues se disminuye de dos a cinco, a uno a tres años de prisión.

5.2. Delito de acceso, utilización y alteración de datos o informaciones de carácter personal o familiar registrados en documentos informáticos o de interceptación de documentos electrónicos o telemáticos.

Este delito se encuentra previsto en el artículo 197.2 del Código Penal Español, y tipifica conductas tendientes a descubrir los secretos o vulnerar la intimidad del titular de los datos o de un tercero, por quien, sin estar autorizado, accede (o "*apodere*", según la redacción gramatical, pero impropia a la utilizada por la LORTAD [83]), utilice, modifique o altere datos o informaciones de carácter personal o familiar que se hallen registrados en ficheros o bancos de datos o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

En la redacción actual del artículo 197.1, *ab initio* Código Penal Español se tipifica el delito de "*apoderamiento de papeles, cartas, mensaje de correo electrónico o cualesquiera otros documentos o efectos personales".* Sin embargo, los mensajes de correo electrónico, como se ha sostenido en la parte tercera de éste trabajo, son una modalidad de documentos informáticos, y más concretamente electrónicos o telemáticos. En tal virtud, desde el punto de vista técnico, jurídico e ius-informático, dichos documentos muestran ajenidad sistemática al incluirlos en la parte inicial del artículo 197.1, cuando mejor ubicados quedarían en el numeral 2 del artículo 197, dentro del género de documentos informáticos y/o telemáticos que el legislador del 1995, bien acoge sin entrar a enlistar o enumerarlos taxativamente o con el sistema *numerus clausus,* como muestra palmaria de que el fenómeno tecnológico de la información y la comunicación (TIC), en esta sociedad

informatizada está en constante crecimiento y evolución que no permite cláusulas y términos cerrados para describirlos fidedignamente.

Sin embargo, se diría que el término *o cualesquiera otros documentos*, previsto en el artículo197.1., incluiría a los todos los documentos (escritos o por sistemas tradicionales de impresión, como los informáticos y/o telemáticos) y que de nada valdría eliminar el término *mensajes de correo electrónico (E-mail)*, del numeral primero, pues seguirían estando incluidos por el término genérico de "documentos", lo cual no es correcto, ya que los *documentos informáticos y/o telemáticos,* si tienen expresa referencia en el artículo197.2 Código Penal Español lo cual los descarta de la previsión general del numeral 11. Por lo más, el término empleado en el numeral 11, se refiere a todos aquellas formas de documentos escritos o impresos, conocidos o conocibles en el futuro; por lo menos, a los diferentes de papeles o cartas.

Este es otro argumento interpretativo gramatical de la ajenidad de los mensajes de correo electrónico en el numeral 1 del artículo197 Código Penal Español pues de lo contrario se daría la paradoja jurídica de estar ubicado doblemente un mismo objeto material del delito [84] ("mensajes de *correo electrónico*" en el numeral 1 y 2), con diferente tratamiento jurídico aunque con igual sanción punitiva.

En efecto, sin desconocer la autonomía de tipificación ni la redacción gramatical empleada por el actual Código Penal Español tanto para el delito de apoderamiento de papeles, cartas, mensajes de correo electrónico o documentos y que la doctrina califica de *delitos sobre secretos documentales* [85] , para diferenciarlo del delito de *apoderamiento (por acceso), utilización y alteración de datos registrados en documentos informáticos y/o telemáticos,* que la doctrina ius-penalista llama de *"Abusos informáticos"* [86] , creemos a la vista de las razones antes dadas, que para tratar el fenómeno TIC y los delitos contra la intimidad, podemos plantear el *Delito de acceso, utilización y alteración de datos o informaciones de carácter particular o familiar registrados en documentos informáticos (artículo197.2),* en una primera parte y el *de interceptación de documentos electrónicos o telemáticos (artículo197.1 in fine),* en una segunda parte, en atención a una mejor sistematización de los documentos informáticos y/o telemáticos, con la aclaración de que una y otra figuras punitivas, están referidas a la visión ius-informática del derecho a la intimidad personal y familiar, pues de lo contrario, nos estaríamos refiriendo: o, a los delitos *contra los datos informáticos* previstos en el Código Penal Español para otros bienes jurídicos como el Patrimonio y el orden socioeconómico (Tit.XIII), v.gr. delitos de destrucción, alteración, inutilización de datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos ("Delito de Daños", artículo 264.2), o a cualquier otro tipo o bien jurídico penalmente tutelado.

Ahora bien, por regla general, la tele-transmisión de datos o informaciones se realiza entre máquinas automatizadas a través de medios o equipos electromagnéticos o computacionales con el auxilio de soportes (hardware y/o software) informáticos y/o telemáticos y su producto en consecuencia es de idéntica naturaleza tecnológica (El documento telemático), y por tanto, la transmisión, emisión y la recepción de los datos o informaciones, se presenta en la memoria de los discos electromagnéticos conocidos (fijos o removibles de diferente formato: *disquettes,* CD´s, CD-ROM, CD-RAM, CD-I, DVD) o conocibles en el futuro (p.e. evolución del DVD); en las unidades periféricas computacionales (como impresoras, grabadoras de sonido o audio-visuales, altoparlantes y aparatos audio-visuales, etc) o asimilables. La multimedia (que une telecomunicaciones e informática: datos, imagen y sonido), hace acopio de estas técnicas TIC en la actualidad y una de las formas de transmitir y recepcionar datos, imagen y sonido es a través del llamado documento electrónico de intercambio de datos "*EDI*" [87] .

Ahora bien, la interceptación de las telecomunicaciones [88] utilizando "*artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o cualquier otra señal de comunicación*", se ha tipificado en la parte *in fine* del artículo 197.1 del Código Penal Español como un

delito mutilado o imperfecto de actos, que no requiere para la consumación el efectivo descubrimiento de la intimidad; basta así para colmar la perfección típica con la interceptación de telecomunicaciones o con la utilización de aparatos de escucha, grabación o reproducción del sonido o de la imagen o cualquier otra señal de comunicación, siempre que alguno de estos sea llevado a cabo con la finalidad de descubrir la intimidad de otro (elemento subjetivo del injusto)... [89] .

En nuestro caso y sin desconocer la amplitud del tipo penal, nos remitimos sólo a la interceptación de los datos o informaciones de carácter personal contenidas en un soporte o documento telemático y con la finalidad de descubrir la intimidad de una persona, tras la denominación de *delito de interceptación de los datos o informaciones de carácter personal o familiar contenidos en documentos electrónicos o telemáticos (artículo 197.1 in fine Código Penal Español),* es decir, a aquellos documentos de intercambio de información o (EDI) o "actos satélites" en los cuales "*no se produce papel sino en registros informáticos de los mensajes que se emiten o recepcionan*" [90].

5.2.1. Bien Jurídico Constitucional Protegido: La intimidad.

El derecho fundamental a la intimidad personal y familiar es el bien jurídico tutelado en el Título X del Código Penal Español a partir de 1995. Esta prerrogativa, *sine qua nom* del bien jurídico y la condición de protección sólo de la persona humana, como sujeto físico (personal o grupo familiar, no extensible a otros grupos o entes sin personalidad v.gr. una comunidad de bienes) abre la puerta a la discusión hermenéutica de sí aquí también se incluye la intimidad de las personas jurídicas o morales, para las cuales la ley finge tienen similares atribuciones que la persona física, cuando en el artículo 200 del Código Penal Español extiende la tutela de la intimidad a las personas jurídicas. Algunos estiman que la nueva protección que brinda el CP a la intimidad, se extiende a las personas jurídicas "*al socaire, que no mandato del TC...*(por lo cual) *merece aplauso* [91] ; otros, entendemos que la extensión a la protección penal de la intimidad de las personas jurídicas, al menos en el Tít. X., quebranta la estructura sistémica del Código Penal Español, y desconoce la legislación comparada sobre el tema (EE.UU., Alemania, Francia), el concepto genuino de la intimidad como derecho derivado exclusivamente de la persona humana y prevista en el artículo 18 C.E. y reglamentado en la LORTAD, especialmente en el artículo3,a) LORTAD, como un derecho de la personalidad exclusivo de los seres humanos y no atribuible a las personas morales o jurídicas, aunque no se desconoce que éstas tengan otros derechos de naturaleza no fundamental o de la personalidad, fundados en la dignidad, prestigio o autoridad moral, según el Tribunal Constitucional (STCS, 06/8/1988, 11/11/91) y otros mecanismos de protección civil (artículo1002 C.c.), según el Tribunal Supremo [92] , o derechos que por ficción legal se han atribuido a las personas jurídicas, como si fueran físicas de los cuales en todo caso, se excluyen los de potestad y carácter de personalísimos, como la intimidad. El Convenio de Europa de 1981 y la Directiva 95/46/CE, sobre el tema es concordante al deferir éste derecho a la intimidad como un derecho exclusivo de las personas físicas.

A pesar de todo, con la protección a la intimidad de las personas jurídicas --se dice--, se brinda una interpretación delimitada para éstas, pero también discutible: primero, porque se hace acopio de una "cláusula de extensión de la tutela penal", al aclarar que si bien las personas jurídicas no tienen intimidad, sí la poseen las personas físicas que la representan, pero siendo así, el régimen jurídico no es el de las personas jurídicas sino el de las personas físicas, ubicado en diferente parte y bajo diversos bienes jurídicos tutelados por el Código Penal. Y, segundo, porque la interpretación. del artículo 200 del Código Penal Español con relación al artículo 278, basado en la frase *in fine* que aquel contiene: "*salvo lo dispuesto en otros preceptos*", debe llevarnos a reconocer que el legislador ha generado "*una grave laguna*", al no preveer "*atentados a la información empresarial reservada mediante abusos informáticos, puesto que no alude a medios comisivos del artículo 197.2 Código Penal Español ", y* por tanto , el artículo 200 "*no cumple una función subsidiaria, de recogida de conducta no abarcadas en el artículo 278 CP. Así, el artículo 200 CP, acogería conductas ilícitas de descubrimiento y de revelación o cesión de datos automatizados de personas jurídicas* (en relación a los núms. 2 y 3 del artículo

197 CP) *pero al precio de desconocer su ubicación sistemática entre los delitos contra la intimidad de las personas*" [93] .

En consecuencia, al estimar que el bien jurídico protegido en el Tít. X, es la intimidad de las personas, se pone fin a las interpretaciones doctrinales derivadas de los delitos contra la libertad de las personas (*Delitos contra la libertad y seguridad*), a las que se recurría en el anterior código penal para conceptualizar la intimidad como bien jurídico tutelable (artículo 497ss) y en las que, por un lado, se hacía énfasis sobre la concreción necesaria que debía dársele a dicho bien jurídico en su funcionalidad y para evitar que todo delito se convierta en un hecho contra la intimidad [94] ; y por otro, se posibilitaba la protección penal *inespecífica* de la intimidad, en forma limitada, fragmentaria [95] y no plena [96] y que quedáse

> anacrónico la protección a la intimidad frente al salto cualitativo de la tecnología, tanto en relación a los nuevos *procedimientos técnicos generales* para entrar en el ámbito físico y espiritual personal de otro, como los *procesos de informatización,* que permiten establecer una red que absorbe toda la experiencia personal del sujeto y la ajeniza [97] .

Hoy por hoy, el derecho a la intimidad como reiteradamente lo ha sostenido el Tribunal Constitucional Español, no es un derecho absoluto, como no lo es ninguno de los derechos fundamentales, es un derecho limitado por la Constitución, la leyes y los demás derechos y valores constitucionales (artículo 10.1-2 y 55.1CE) y como derivación de la dignidad de la persona, implica "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" (STC 209/1988, FJ 3, STC, y Mayo 9 de 1994, FJ.6), pero además es un derecho en latente amenaza por las nuevas tecnologías de la información y la comunicación (TIC), lo cual lo ha hecho un derecho altamente vulnerable a la par que potencialmente protegible por las normas civiles, administrativas y penales.

Por ello, y con mucha mayor razón, la famosa Sentencia de Julio 20 de 1993 y más recientemente la Sentencia de Mayo 9 de 1994 del TC., al desestimar un recurso de amparo sobre el régimen de obligatoriedad del NIF (Número de Identificación Fiscal Español) y de obtención de información con base en el mismo, contenido en el Real Decreto 338/1990, el cual, se decía, atentaba contra el derecho a la intimidad previsto en el artículo18 CE (y en relación directa con el artículo 18.4 id), reconoce el Tribunal Constitucional, la vulnerabilidad de derechos subjetivos e intereses legítimos como el grado de protección que debe garantizar el Estado en base a la Constitución, el Ordenamiento Jurídico interno y la interpretación hermenéutica de las normas, principios y tratados ratificados por España (artículo10.2 CE), en cuanto se refieran al tratamiento automatizado de datos de carácter particular y los derechos fundamentales, y en especial, al derecho de la intimidad (Convenio Europeo de Dic. 27 de 1981. Hoy también, la Directiva 95/46/CE, del Parlamento y Consejo de Europa, que amplia y precisa aspectos del tratamiento de datos del Convenio y los demás instrumentos normativos comunitarios de desarrollo sobre el tema [98]) .

En el FJ.7, la STC 05/09/94, sostuvo al respecto:

> *Como ya se ha anticipado, cuestiona la demanda la legitimidad constitucional de una norma que, a través de un instrumento de recopilación de información, puede propiciar un uso desviado de ésta y, en consecuencia, la efectiva invasión de la esfera privada de los ciudadanos afectados. Desde luego, es un hecho también admitido en la jurisprudencia de este Tribunal que el incremento de medios técnicos de tratamiento de la información puede ocasionar este efecto y, correlativamente, se hace precisa la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aun indirecto, que produzca este efecto, y a incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho (STC 254/1993). En este sentido se ha afirmado que, ya que "los datos personales que almacena la Administración son*

utilizados por sus autoridades y servicios", no es posible "aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión" (STC 254/1993, FJ7). En consecuencia con ello, habría que convenir en que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta.

5.2.2. Acceso, utilización. alteración e interceptación de datos contenidos en documentos informáticos.

5.2.2.1. Parte A*b initio* del tipo.

Para el *Delito de acceso, utilización y alteración de datos o informaciones de carácter particular o familiar* [99] *registrados en documentos informáticos* (artículo197.2). La acción consiste en el acceso, la utilización y alteración de documentos informáticos, electrónicos o telemáticos, siempre que se hagan con la finalidad de descubrir secretos, sin posterior divulgación, que atenta contra la intimidad del titular de los datos de carácter personal o familiar o de un tercero y se hallen registrados.

En el titulo VI del Código Penal Canadiense destinado a los Delitos contra la Intimidad ("*Invasion Privacy*"), en los artículos. 183 a 196, se estructura la figura penal básica de la interceptación (que subsume el acceso, utilización y alteración) de datos o informaciones ("*Interception of communications*") de carácter particular, sin consentimiento del titular, o sin consentimiento de una de las partes cuando existe una comunicación hablada o escrito y por cualquier medio mecánico o eletromagnético. Así mismo se establece las excepciones a encasillarse en el tipo penal básico, por disposición legal o judicial, la interceptación de secretos o informaciones confidenciales y la interceptación de las telecomunicaciones por medios subrepticios mecánicos, acústicos o electromagnéticos, tal como vimos en el apartado 2.2. de éste trabajo. Sin embargo, la figura que más se aproxima a los tipo penal aquí analizado es la prevista en el artículo 193.1, sobre el delito de "*Disclosure of information*", que tipifica el delito de descubrimiento, revelación y utilización de datos o informaciones de carácter personal, sin el consentimiento expreso o tácito del titular, contra la intimidad y sea cual fuere el soporte en el que se hallen (documentos impresos, escritos o informáticos y/o telemáticos, al decir: "...*by means of an electro-magnetic, acustic, mechanical or other device...*"). En el mismo artículo expone las causales de excepción a los que no se aplica la norma, tales como, por ejemplo, cuando media un procedimiento civil, penal o de cualquier otra índole en los que se requiera alguna prueba contra la persona concernida con los datos (Subdivisión 2).

5.2.2.1.1. Acceso.

El tradicional *delito de apoderamiento* de papeles, cartas o *documentos en general* que contienen secretos y son objeto de descubrimiento, existe una clara, matizada y evolucionada jurisprudencia y doctrina, antes y después del C .P. de 1995 [100]. Sin embargo, desde antes de la existencia del artículo 197 del actual Código Penal, se planteaba la excepcionalidad referente al significado y significante del término *apoderamiento* aplicado a los documentos elaborados a través de "medios tecnológicos modernos" o informáticos y/o telemáticos que contenían secretos, pues se discutía si éstos eran o no objeto de aprehensibilidad material con igual criterio al aplicado al documento escrito, impreso o similares (v.gr. una fotografía, un plano, etc), o al menos se planteaba el anacronismo y la dificultad de aplicar el concepto de apoderamiento documental previsto en el ordenamiento jurídico a los documentos informáticos [101].

Hoy, la doctrina y jurisprudencia españolas, teniendo en cuenta que los documentos informáticos son una modalidad de documento, según las previsiones del artículo 26 del Código Penal (STSS, Sala Penal: 9/05/94, 3/2/97), interpretan el concepto de apoderamiento utilizado en el artículo 197, en un sentido amplio, que no solamente incluye

al referente físico, sino al sentido lógico de conocimiento, es decir, que se puede aprehender no sólo lo material (aprehensión física u objetiva) sino lo que puede ser captado por el sistema sensorial humano, tal como las imágenes, datos y sonidos (aprehensión sensorial).

Si bien esto es cierto, no podemos desconocer que la conducta comportamental exigida por el artículo 197.1 y 2., sobre el apoderamiento no sólo se aplica a los documentos escritos, sino a los no escritos e informáticos y por éstos últimos se impone que el término apoderamiento se ajuste a las nuevas tecnologías TIC que destaca la informática jurídica, el ciclo o fases de tratamiento automatizado de la información y la normas jurídicas penales y extrapenales (LORTAD, Directiva 95/46/CE, Convenio de 1981) sobre el tema. En efecto, "*la acción de apoderamiento de datos... tiene como traducción técnica más ajustada la acción de acceso a los mismos, que es la tipificada en el inciso segundo*" [102] parte *in fine* del artículo 197.

Ahora bien, para entender la punibilidad del acceso a los datos contenidos en documentos informáticos, veamos cuál es el ámbito normativo legal del derecho de acceso. Para ello recurrimos a las normas extrapenales (LORTAD, D.R..1332/1994, Directiva 95/46/CE). En efecto, mediante el derecho de acceso, se garantiza que:

> *1. El afectado (por el titular del derecho o interesado, según la Directiva 95/46/CE) tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados (o bancos de datos).*
> *2. La información podrá consistir en la mera consulta de los ficheros por medio de su visualización, o en la comunicación de los datos pertinentes mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos convencionales que requieran el uso de dispositivos mecánicos específicos.*
> *3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes (artículo 14, LORTAD). --paréntesis nuestros--*

Este derecho personalísimo de acceso a los datos o informaciones (legibles o inteligibles) automatizadas, que le conciernen al titular o interesado, es parte integrante del derecho de *habeas data* junto al de actualización, rectificación y cancelación de datos y desde el punto de vista formal se configura siempre que la solicitud o petición reúna los requisitos legales de forma y de fondo, se ejercite *in témpore* o se demuestre un interés legítimo (artículos. 14 a 16, LORTAD). Este derecho ha sido objeto de puntuales reglamentaciones, sobre todo de *tipo procedimental*, tal como lo confirma la exposición de motivos del Real Decreto 20/6/94, Núm. 1332/94, a efectos de completar el ámbito, esencia y grado de protegibilidad del derecho, y por ende, para que el interesado solicite la consulta de los ficheros o bancos de datos, por medio de la visualización en pantalla, la comunicación escrita, impresa, copiada, tele-copiada, certificada por correo, *o cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo* (artículo 12 Id.).

El derecho de acceso a los datos de carácter particular registrados, bajo las anteriores condiciones y requisitos, sólo puede ser negado, cuando los ficheros siendo de titularidad pública se dé alguno de los siguientes supuestos: a) Por el factor temporal o de legitimidad previsto en el artículo14.3, b) Por el factor de acentuada protección de los *ficheros de las fuerzas y cuerpos de seguridad* en la recogida y tratamiento automatizado y del que pudieren derivarse riesgos para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizado (artículo20 y 21.1); c) Por el factor de protección de las funciones administrativas tributarias en los ficheros de la Hacienda pública (artículo 21.2); y, d) Por el factor de ponderación de los intereses público o de terceros más dignos de protección, previstos en el artículo 22.2 de la Ley Orgánica 5/1992; o, finalmente y siendo los ficheros de titularidad privada, cuando la solicitud sea formulada por persona distinta del *afectado* o interesado (artículo 14 D.R.1332/1994).

En la ley 30/1992, *Ley de Régimen jurídico de las administraciones públicas y el procedimiento administrativo común* (LRJPA), hermana pero desconectada en la esencia y objeto material de regulación con la LORTAD, como antes indicábamos al tratar los documentos informáticos, regula el derecho de acceso de los ciudadanos ante las administraciones generales del Estado (artículo105 b), CE) y por tanto, debe servir de norma extrapenal, para entender la licitud e ilicitud del mentado derecho, y en particular cuando se acceda a documentos informáticos o telemáticos que se encuentren en *archivos o registros públicos* (artículo197.2 *ab initio* Código Penal Español).

En efecto, el artículo 37 y 45 de la LRJPA, se regula expresamente el derecho de *habeas data* que incluye el de acceso a los archivos, registros y documentos públicos, "*cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren...",*y en especial "*el acceso a los documentos que contengan datos referentes a la intimidad de las personas estará reservado a éstas, que, en el supuesto de observar que tales datos figuran incompletos o inexactos, podrán exigir que sean rectificados o completados..."* (artículo37.1 y 2). Por su parte el artículo 45, al hacer mención a la *incorporación de medios técnicos* (TIC) al derecho, *"con las limitaciones que a utilización de estos medios establecen la Constitución y las leyes"* (artículo 45.1), hace énfasis en la compatibilidad de esta utilización con el ejercicio de los derechos del titular (artículo 45.2), terminando con una denominación de documento electrónico, informático y telemático (artículo 45.5). Como se puede apreciar, sobre estos tópicos resulta más precisa la LRJPA que la LORTAD, cara la interpretación del Código Penal, no sólo en el título X, sino en otras partes donde repetidamente se utiliza la conceptualización técnica TIC, para proteger derechos e intereses legítimos de las personas. Por ello no han dudado los ius-administrativistas al plantear la conexidad y la observancia de *la unidad de materia* reguladas entre la LRJPA y la LORTAD [103] , cuando está presente la informática y el derecho (la ius-informática), aunque el legislador actúa a espaldas de esa realidad temática y prefirió dejar a la doctrina que desentrañara esa sintonía.

Finalmente, la Directiva 95/46/CE, --que precisa y amplia el Convenio de Europa de 1981, sobre la materia--, en su artículo 12, extiende el derecho de *habeas data* inicialmente al derecho de acceso que ostentan ***todos*** los interesados para obtener del responsable del tratamiento automatizado de los datos o de la información de ciertas acciones, conductas y mecanismos de control, protección y obtención de información o consulta que le concierne, a la vez que impone unas excepciones o limitaciones a éste derecho devenidas principalmente de la seguridad del Estado, la defensa, la seguridad pública, por ser objeto de investigación penal o de infracciones deontológicas en las profesiones, por un interés económico y financiero estatal, por la protección del interesado o de los derechos y libertades de otras personas (artículo13.1 Id). Los derechos del concernido; entre otros, son: a) los de confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen; la comunicación de los mismos y de su origen, así como el conocimiento de algunos tratamientos automatizados de datos, cuando se tiendan a evaluar determinados aspectos de la personalidad, como p.e., el aspecto laboral, la fiabilidad, la conducta, etc. (artículo 15.1.id); b) la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, por ser incompletos o inexactos; c) Notificación a terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con el anterior literal y siempre que no resulte imposible o suponga un esfuerzo desproporcionado.

5.2.2.1.2. Utilización y Alteración.

La acción de utilizar, en perjuicio de tercero o mejor del titular [104] de los datos o informaciones de carácter particular o familiar que se hallen registrados en documentos informáticos, electrónicos y telemáticos en archivos o registros públicos o privados, ha sido objeto de tipificación doble en un mismo apartado (artículo 197.2 *ab initio* Código Penal Español), como dijimos, conduce a multitud de problemas interpretativos por no observar el ciclo operativo completo de los banco de datos en su creación (se entiende desde la recolección de los datos, con excepción de la recogida manual de que es pre-informática), almacenamiento, registro y transmisión (p.e., para consulta) y sólo reducirlo al registro de

los datos para encuadrar los tipos en sede penal, como sostiene el profesor *Morales Prats* [105] , pero además crea una incertidumbre jurídica al tipificar *in fine* del artículo197.2., nuevamente la utilización de datos sin mencionar que éstos estén o no registrados, lo cual nos llevaría a pensar que en éste aparte sí esta previsto ese ciclo o fases del ingreso o acceso, tratamiento o procesamiento y consulta automatizada de datos o informaciones de carácter particular. Y, aquí el desconcierto es mayor, pues las conductas de recogida ilícita de datos personales con fines informáticos y la creación clandestina de ficheros o bancos de datos personales con fines de automatización y manejo de datos personales, encuentran respuesta sancionadora *extra-muros* del Derecho Penal, como infracciones administrativas en la LORTAD (artículo 43.4 a) y artículo 43.3. a), b), y c) [106] .

Una aproximación hermenéutica a la solución del problema debería comenzar sintonizando la regulación de un mismo nuevo fenómeno tecnológico, como el TIC, su regulación por parte del derecho, la visión ius-formática prevista en la LORTAD, con la reglamentación del derecho de habeas data contenido en la LRJPA y su Real Decreto No. 263/1996, de 2 Febrero, al menos para comprender holísticamente los derechos de acceso, utilización y alteración de los datos o informaciones.

En la exposición de motivos de la LORTAD, se sostiene que el artículo 18-4, de CE, emplaza al legislador a limitar el uso de la informática para garantizar la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos, con lo cual se fija directrices y mecanismos de control y de protección que tienden "expresamente a la articulación de garantías *contra la posible utilización torticera de ese fenómeno* de la contemporaneidad que es la informática" [107] en las fases del recolección, almacenamiento y acceso al tratamiento automatizado de datos o informaciones. Sin embargo, en el texto de la ley la utilización lícita del fenómeno informático sólo es posible gracias a la interpretación por exclusión de lo ilícito, pues el legislador precisó varias formas de infracciones administrativas (muy graves, graves y leves) de "utilización y cesión ilícita de datos de carácter particular (artículo 48, LORTAD), pero no la forma de utilizar lícitamente la informática como sí lo hicieron normas posteriores sin conexión sistemática alguna. Por ello, cabe el enclave interpretativo siguiente.

En efecto, la LRJPA, al reglamentar el derecho de acceso de los ciudadanos ante la administración general del Estado, prevé la incorporación de medios técnicos informáticos y/o telemáticos, la forma de acceso y utilización de los mismos, "*con las limitaciones que a la utilización de estos medios* (se refiere a los informáticos, electrónicos y telemáticos) *establecen la constitución y las leyes" (artículo45.1)*. Los límites constitucionales a observar serán los que imponen todos los derechos fundamentales (artículo 10 y 55.1 CE) y los legales, los previstos en la LORTAD y la propia LRJPA. La utilización de medios informáticas y/o telemáticos, como derecho de los ciudadanos no es absoluta, pues está limitado a la Constitución y el Ordenamiento Jurídico vigente.

La ilícita utilización de los medios técnicos en estas relaciones jurídicas del ciudadano y el Estado, será sancionada por el Código Penal, y en particular, cuando el bien jurídico sea el de la intimidad y previamente se acceda a archivos, registros o documentos informáticos y/o telemáticos públicos y privados, según el artículo 197.2.

La licitud en la utilización de los medios informáticos y/o telemáticos, está prevista en el R.D.263, de 2 de febrero de 1996 que reglamenta el artículo 45 de la LRJPA, *con la pretensión de delimitar, en el ámbito de la Administración General del Estado, las garantías, requisitos y supuestos de utilización de las técnicas electrónicas, informáticas y telemáticas*, como se sostiene en la exposición de motivos del referido Real Decreto. Destaca que la utilización de las técnicas señaladas tendrán las limitaciones establecidas en la Constitución, la Ley 30/92, el "*resto*" del ordenamiento Jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos. En especial, se garantizará el honor y la intimidad personal y familiar de los ciudadanos, ajustándose, a tal efecto, a lo dispuesto en la Ley Orgánica 5/1992", (LORTAD) y en las demás leyes específicas que regulan el tratamiento de la información así como sus correspondientes normas de desarrollo. La utilización de tales técnicas en ningún caso podrá implicar la existencia de restricciones o discriminaciones de cualquier naturaleza en el acceso de los

ciudadanos a la prestación de servicios públicos o a cualquier actuación o procedimiento administrativo (artículo 2).

Igualmente se establecen las garantías generales de la utilización de los soportes, medios y aplicaciones electrónicas, informáticas y telemáticas (artículo 4) y dentro de las medidas de seguridad que deben garantizar la administración del Estado y sus entidades de derecho público; entre otras, las siguientes: a) Cuando se utilice medios técnicos, se adoptarán medidas sinónimas y de organización necesarias que aseguren la autenticidad, la confidencialidad, integridad, disponibilidad y conservación de la información. Estas medidas deben tener en cuenta el estado de la tecnología y ser proporcionadas a la naturaleza de los datos y de los tratamientos y a los riesgos a los que estén expuestos, y b) Se aplicará medidas que garanticen, la prevención de alteraciones o pérdidas de los datos e informaciones y la protección de los procesos informáticos frente a manipulaciones no autorizadas.

Esto último nos sirve para hacer énfasis sobre la *alteración de datos* y como acertadamente se sostiene por la doctrina ius-penalista, la acción de modificación es sinónima a la de alteración utilizada por el legislador en el artículo 197.2 [108] . Esta es otra más de las inconsistencias gramaticales del mentado artículo, que conllevan a tipificar doblemente una misma acción, sin necesidad ni rigor jurídico. Por ello, a nuestros fines preferimos manejar la conducta comportamental humana de alteración por ser más explicativa en el proceso de tratamiento automatizado de datos o informaciones personales.

5.2.2.2. Parte *in fine* del tipo: La Interceptación o la intervención..

La acción del *delito de interceptación de los datos o informaciones de carácter personal o familiar contenidos en documentos electrónicos o telemáticos* (artículo 197.1 in fine Código Penal Español) consiste en interceptar datos con medios informáticos para descubrir la intimidad. Hay que entender por interceptar la intervención para conocer el contenido de la misma, de ahí que sólo sea punible la comisión dolosa [109]. La interceptación de los datos o informaciones de carácter particular se hacen interceptando las telecomunicaciones o teletransmisiones de datos que contengan voces (naturales y digitalizadas), sonidos, imágenes (estáticas y en movimiento) y datos alfanuméricos: textos o figuras (gráficos o digitalizados), componentes de un documentos electrónicos o telemáticos y emitidos y recepcionados por medios tecnológicos, TIC e informática. v.gr. por vía internet, por correo electrónico, La multimedia y la red alámbrica e inalámbricas de teletransmisión que une datos, imagen y texto. Obviamente se debe entender que esta interceptación delictuosa de las telecomunicaciones debe tender a descubrir la intimidad y la imagen como expresión o visión de éste (elemento subjetivo del injusto) y que excluye las infracciones administrativas de interceptación de telecomunicaciones no destinadas al uso público o a cualquier otro uso, previstas en el artículo 33 de la Ley de Ordenación de las Telecomunicaciones (LOT: 31/1987, de 18 de diciembre) [110].

Debemos partir de una premisa constitucional básica para tratar el tema, y es el de que "*se garantiza el secreto de las comunicaciones y, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial"* (artículo18.3), entendiendo que en el género de las comunicaciones se halla el fenómeno tecnológico TIC y las denominadas telecomunicaciones. Por ello, "*sea cual sea el ámbito objetivo del concepto de comunicación, el artículo18.3... se dirige inequívocamente a garantizar su impenetrabilidad por terceros ajenos a la comunicación; no hay secretos para aquel a quien se dirige la comunicación"* (STC 114/1984, Nov. 29). En concordancia, el artículo22 LOT, expresa que se garantizará "*el secreto de las comunicaciones*".

El bien constitucionalmente protegido, en el artículo18.3 CE, con el secreto de las comunicaciones, es en términos del Tribunal constitucional la "*Libertad de las comunicaciones*, *siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto (*que suponga aprehensión física del soporte del mensaje, con consecuencia o no del mismo o captación de otra forma del proceso de comunicación*) como por el simple conocimiento antijurídico de lo comunicado* (apertura de

correspondencia ajena guardada por su destinatario, por ejemplo)". (FJ.7 STC 114/1984). Esta libertad es otra más de las facetas del derecho a la intimidad.

Por telecomunicaciones, se entiende acudiendo a la LOT (anexo núm.3), "*toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos*". A su vez, siguiendo el sistema de terminología técnica, que es la regla en el legislador de finales del siglo XX, podemos distinguir entre telecomunicaciones por ondas hertzianas o electromagnéticas o radioeléctricas (la radiocomunicación y la radiodifusión v. gr. radio y televisión , destinada al servicio del público en general), por cable y por satélite.

Las telecomunicaciones por cable, hace referencia al "*suministro o intercambio de información en forma de imágenes, sonidos, textos, gráficos o combinaciones de ellos, que se prestan al público en sus domicilios o dependencias de forma integrada mediante redes de cable*" (Ley 42/1995, de 22 de diciembre). Entre sus múltiples servicios se incluye la radio y la televisión a domicilio o dependencia del interesado y previo contrato con las empresas que lo suministran [111] .

Las telecomunicaciones por satélite, son "*los servicios de telecomunicaciones para cuya prestación se utilizan de forma principal redes de satélite de comunicaciones*" (v.gr. La televisión digital por satélite, D.L.1/1997 y Ley 17/1997).

Sin embargo, la legislación de telecomunicaciones no descansa exclusivamente en estas tres categorías, sino que a estos conceptos se superponen otras nociones que no atienden a la técnica empleada (ondas, cable o satélite), sino al tipo de actividad que se realiza. Reciben el nombre de "servicios", tales como: los finales (telefonía básica, telex, telegrama); los portadores (telefonía, radio, televisión); los de difusión (radio y televisión); y los de valor añadido [112] . En estos últimos están (telefonía móvil, teletex, telefax, burofax y el datafax) y consisten en

> "*los servicios de telecomunicación que, no siendo servicios de difusión, y utilizando como soportes servicios portadores o servicios finales de telecomunicación, añaden otras facilidades al servicio de soporte o satisfacen nuevas necesidades específicas de telecomunicación como, entre otras, acceder a información almacenada, enviar información o realizar el tratamiento, depósito o recuperación de información"* (artículo 20.1 LOT)

Las telecomunicaciones unidas a la informática forman esa compleja amalgama que bien podríamos llamar la teleinformática y la telemática como especie de ésta. Quizá por ello, la Directiva 95/46/CE, hace énfasis sobre los objetivos y finalidades de la *Transferencia de datos personales a países terceros* (artículo 25), los mecanismos de protección de los derechos y libertades que deben observarse, así como los medios tecnológicos TIC, unidos a la informática, por los cuales se transmiten, emiten y recepcionan. En efecto, cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico, y tenga éste único fin, será responsable del tratamiento de los datos personales contenidos en el mensaje, el emisor y no quien ofrezca el servicio de transmisión; *que no obstante, las personas que ofrezcan estos servicios normalmente serán considerados responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio* (C. 47).

Ahora bien, el delito que comentamos ahora, sólo requiere para su consumación el efectivo descubrimiento de la intimidad, bastando así para la perfección típica con la interceptación de las telecomunicaciones o con la utilización de aparatos de escucha, grabación o reproducción del sonido o de la imagen o "*cualquier otra señal de comunicación*" (p.e. la correspondencia informática que posibilita la conexión de la red telefónica al ordenador, como el correo electrónico *--E-Mail--* y las variadas formas de comunicación electrónica de hoy en día, tales como*: list servs, newgroups, chat rooms, y World Wide Web --WWW--;* entre otros). Estos aparatos utilizados para el control auditivo o visual, dado el carácter penetrante y permanente que estos medios facilitan en la intimidad de las personas, comportará normalmente ya el efectivo descubrimiento de aquella, según

lo sostiene el profesor *Morales Prats*, al ubicar esta modalidad típica de interceptación de datos informáticos y/o telemáticos, como de *control auditivo y visual clandestino y de control ilícito de señales de comunicación de carácter informático* [113] , y con esto último, se establece una cláusula abierta que permite ofrecer una cobertura típica amplia a cualquier modalidad, tipo o servicio de comunicaciones [114] , tanto tradicional como actual (p.e. la telemática: multimedia y la hipermedia).

Un aspecto importante a destacar en esta figura típica de la interceptación de datos o informaciones de carácter personal, es que para su configuración se requiere que no haya consentimiento del sujeto pasivo del delito, o de todos, si son varios los que intervienen en una comunicación, pues de lo contrario la tipicidad se excluye, como lo han expuesto *Serrano Gómez, Muñoz Conde* y desde antes del C.P de 1995, *Bustos Ramírez* [115] o se cae en otro tipo penal, pero no en éste. Sin embargo, se ha estimado que la alusión de la norma penal (artículo197.1) a "*sin su consentimiento*" (del titular se entiende), en términos de la LORTAD, debe referirse a una "*ausencia de consentimiento del titular de los datos*", y por tanto, el Código Penal Español de 1995 debería haber indicado que esas conductas deben realizarse *ilegalmente* [116] y así evitar la alusión que hoy trae en forma expresa, pues tácitamente puede entenderse que no ha habido consentimiento por parte del titular y que las conductas que se realizan no han tomado en cuenta su consentimiento. Aunque es pleonástico decir que la conducta se realiza ilegalmente, pues ello va inmerso en el concepto delito, referido en el artículo 197 *in fine*, que resulta más apropiado que el de la frase de cajón: sin su consentimiento, entendido sólo en forma expresa.

Quizá por esto, el Código Penal Canadiense, en el artículo 193.1(1) a), tipifica en forma autónoma el delito de *Disclosure of information received from interception of radio-based telephone comunications* y cuando estas comunicaciones sean interceptadas por medios electromagnéticos, acústicos o mecánicos o cualesquiera otros, sin el consentimiento expreso o tácito del titular o de las personas involucradas en la comunicación, para evitar la interpretación sobre el consentimiento tácito, antes mencionado.

Ahora bien, con igual criterio al observado en el aparte anterior (b), utilización y alteración), como enclave de interpretación normativa de LORTAD y LRJPA, respecto al entendimiento del fenómeno ilícito de la interceptación de datos informáticos previsto en el artículo 197.1. *in fine*, debemos recurrir a la lícita reglamentación de la utilización de técnicas electrónicas, informáticas y telemáticas por la administración General del Estado, estipulada en el R.D. 263/1996, de 16 de Febrero, artículo 7.

> *Comunicaciones en soportes o a través de medios o aplicaciones informáticos, electrónicos o telemáticos. **1**. La transmisión o recepción de comunicaciones entre órganos o entidades del ámbito de la Administración General del Estado o entre éstos y cualquier persona física o jurídica podrá realizarse a través de soportes, medios y aplicaciones informáticos, electrónicos y telemáticos, siempre que cumplan los siguientes requisitos: **a)** La garantía de su disponibilidad y acceso en las condiciones que en cada caso se establezcan. **b)** La existencia de compatibilidad entre los utilizados por el emisor y el destinatario que permita técnicamente las comunicaciones entre ambos, incluyendo la utilización de códigos y formatos o diseños de registro establecidos por la Administración General del Estado. **c)** La existencia de medidas de seguridad tendentes a evitar la interceptación y alteración de las comunicaciones, así como los accesos no autorizados. **2.** Las comunicaciones y notificaciones efectuadas en los soportes o a través de los medios y aplicaciones referidos en el apartado anterior serán válidas siempre que: **a)** Exista constancia de la transmisión y recepción, de sus fechas y del contenido íntegro de las comunicaciones. **b)** Se identifique fidedignamente al remitente y al destinatario de la comunicación. **c)** En los supuestos de comunicaciones y notificaciones dirigidas a particulares, que éstos hayan señalado el soporte, medio o aplicación como preferente para sus comunicaciones con la Administración General del Estado en cualquier momento de la iniciación o tramitación del procedimiento o del desarrollo de la actuación administrativa. **3.** En las actuaciones o procedimientos que se desarrollen íntegramente en soportes electrónicos, informáticos y telemáticos, en los que se produzcan comunicaciones caracterizadas por su regularidad, número y volumen entre órganos y entidades*

del ámbito de la Administración General del Estado y determinadas personas físicas o jurídicas, éstas comunicarán la forma y código de accesos a sus sistemas de comunicación. Dichos sistemas se entenderán señalados con carácter general como preferentes para la recepción y transmisión de comunicaciones y notificaciones en las actuaciones a que se refiere este apartado. ***4.*** *(...)*"

Una reciente sentencia del Tribunal Constitucional, como lo destaca *Queralt Jiménez* [117] , con motivo de la reforma operada por la LO 18/1984, tenía por objeto proteger la interceptación, no sólo de las conversaciones telefónicas strictu sensu o conversacionales, sino cualquier tipo de telecomunicación. Así se terminó con la duda que asaltaba a algunos al entender si estaban o no previstas otras formas de comunicación como el fax o la telefonía celular, y creemos nosotros, que cualquiera otro medio de comunicación que una telecomunicaciones e informática (telemática, vía internet, correo electrónico, etc.), como antes indicábamos. En consecuencia, cualquier "*captación y divulgación de las conversaciones telefónicas, sea cual sea el sistema que utilicen los interlocutores es ilícita*", entendiendo que interceptar en los términos de la sentencia, consiste en *apoderarse del mensaje antes de que llegue a su destino o interrumpir una vía de comunicación.* (STC 34/1996, de 11 de marzo. Aunque como se sabe ésta se refiere a la interceptación de comunicaciones por funcionarios o agentes públicos --artículo 536 Código Penal Español--, pero en todo caso contra la intimidad de las personas).

En esta última línea y fin, y con motivo de la noticia de la intervención, acordada por un juez norteamericano, respecto de las comunicaciones que circulan por las redes informáticas, vía internet y con el propósito de la investigación de unos hechos presuntamente delictivos, *Maza Martín* [118] , sostiene que dicha intervención debe ser asimilada en el derecho español, en sus efectos procesales, a la telefónica, así como los requisitos para su eficacia probatoria. Estos serán: a) la autorización de su realización por autoridad judicial en resolución motivada; b) el carácter excepcional y por tiempo determinado; c) el que se dirijan a la obtención de pruebas sobre un hecho delictivo concreto de que consten los indicios de su comisión; d) practicada sólo sobre teléfonos de personas sospechosas de participar en los delitos investigados y llevadas a cabo bajo riguroso control del juez autorizante; y e) con la obligación de entrega a la autoridad judicial de los soportes originales en que se haya recogido el contenido de las intervenciones (STS, de 24 de Junio de 1995). El Tribunal Supremo Español, Sala 20, tiene una amplia como fecunda jurisprudencia sobre las "intervenciones telefónicas" (o "*escuchas telefónicas clandestinas*" como vulgarmente se les conoce) v.gr. un resumen fructíferamente sobre el tema: Marzo 2 de 1996 (M.P. Montero Fernández Zapater), Octubre 26 de 1996 (M.P. Bacigalupo Zapater) y la de Diciembre 17 de 1996 (M.P.Martínez-Pereda Rodríguez).

Pero, hay más: la compleja amalgama que conforma la tecnología TIC, las telecomunicaciones y la informática; por un lado, avanza día por día, en ese también complejo como ambiguo marco de mejoras potenciales de las nuevas tecnologías en la sociedad de la informática; y por otro, los constantes, penetrantes y porosos riesgos que éstos avances representan frente a los derechos fundamentales de la persona, principalmente del derecho a la información, expresión, la intimidad y el honor. Así mismo, son constantes las dificultades de todo tipo y cada vez mayores las garantías reales y medios de protección, por parte del Estado para prevenir, evitar, o más aún, reprimirlos civil, administrativa o penalmente.

Una reciente Sentencia de la Corte de Apelaciones de los Estados Unidos de América, de Octubre 31 de 1994, conocido como el caso *Steve Jackson Games, Inc. et al. v. US Secret Service* [119] , se hizo referencia, entre otros aspectos, a los que llamamos medios comisivos informáticos (de hardware y software) de conductas ilícitas y de los que nos ocuparemos más adelante; y sobre todo, el diferente tratamiento jurídico devenido de la tecnología aplicada a una y otra forma de comunicación (la llamada en la sentencia Comunicación por " Cable"--*Wire*-- y la comunicación "electrónica"), el tiempo en el que se realiza la intervención o interceptación (factor temporal), la variada forma de almacenamiento de la información o datos (en forma electrónica solo para la comunicación ídem, mediante software o hardware: discos fijos y removibles) y en fin, el trámite distinto seguido por parte de las autoridades judiciales y/o administrativas, para la interceptación de comunicaciones

electrónicas (*electronic communication*) y la intervención de comunicaciones por cable (*Wire communications*). Aunque, queda claro que tanto una y otra forma de comunicación son objeto de interceptación, pues la *intercepte*, se define como *"adquisición auditiva o similar de cierto volumen de información o comunicación por cable, electrónica, o en forma oral, a través del uso de cualquier dispositivo electrónico, mecánico u otros",* según el artículo 2510 del Act Wiretap, 18 U.S.C. La interceptación, requiere un elemento temporal fundamental para que ésta se cumpla . En efecto, *"...la adquisición* (debe ser) *contemporánea a la comunicación* (es decir, a la transmisión: emisión y recepción del mensaje), *a través del uso del dispositivo"* idóneo (instrumentos y/o aparatos TIC e informática) según se trate de comunicación por cable o electrónica y que en éste último caso, la información no esté almacenada o guardada en memoria o discos de computador

En efecto, se dijo que la *comunicación electrónica,* se define como*: cualquier transferencia de señales, signos, escritura, imágenes, sonido, datos o informaciones de cualquier naturaleza transmitidas en todo o en parte por cable, radio o en forma electromagnética, foto-eléctrica o por sistema foto-óptico y afectan al comercio entre estados o con el extranjero.*(F.N.4 de la Sent. C.F.US. Oct.31/94).

No queda cubierta en esta definición las comunicaciones siguientes: a) La realizada mediante radio-teléfonos o los teléfonos inalámbricos, ni la comunicación entre éstos con unidades de teléfono fijas; b) Cualquier comunicación por cable en forma oral; c) Cualquier comunicación realizada, a través de sólo tonos con dispositivo de paginación; y, d) Cualquier comunicación realizada con un dispositivo de rastreo, definidos en el artículo 3117 de la Ley Federal de Comunicaciones por Cable (*The Federal Wiretap Act, 18 U.S.C*) (FN.4 *In fine*). Enmendada por la Ley de Protección a la intimidad en las comunicaciones electrónicas de 1986 (*The Electronic Communication Privacy Act of 1986.*

Los mensajes de correo electrónico (*E-Mail*) [120] , fueron el objeto de la supuesta intervención o interceptación de las comunicaciones electrónicas, en el caso norteamericano, por cuanto los Servicios Secretos de los Estados Unidos (*Secret Service US*), incautaron un ordenador, con sus programas, unidades de almacenamiento (*storage*) de la información o datos, tanto principal (Disco Fijo o Duro), como de copias de seguridad (*Backup*) --formas exclusivas de la comunicación electrónica--, con motivo de una investigación preliminar, por supuesta comisión de un ilícito por parte de uno de los colaboradores y/o trabajadores de una empresa particular que laboraba con el Sistema Electrónico del Tablón de Anuncios (BBS), en el cual se almacenaba la información enviada por los destinatarios mediante los *E-Mail privados,* no leídos por el destinatario *Steve Jackson Games Inc*., antes de la incautación.

La Corte de Apelaciones, estimó que siendo distinto los sistemas de comunicación por cable (*Wire*), y los de comunicación electrónica, como la realizada por mensajes de correo electrónico, se deberá diferenciar en ésta última, sí: a) las comunicaciones electrónicas han estado en almacenamiento electrónico (en discos fijos y removibles o unidades de copia de seguridad) durante 180 días o menos, el gobierno puede acceder a su contenido, sí dispone de una *garantía federal o estatal* (*Federal or state warrant*), a términos del artículo 2703 de la Act Wiretap , 18 U.S.C.; y, b) si las comunicaciones que son almacenadas por un servicio remoto de informática (*remote computing service*) y ésta ha permanecido por más de 180 días, el gobierno puede acceder a su contenido, siempre que disponga una garantía por vía administrativa del Gran Jurado o haya obtenido una orden judicial de la Corte, a tenor del artículo 2703 Ibídem.

5.2.3. Los "datos sensibles" de la persona humana.

5.2.3.1. Información personal del concernido.

Los datos de carácter personal se han considerado como "*cualquier información concerniente a personas físicas, identificadas o identificables*" (artículo 3, a, LORTAD). A su vez persona identificable es aquella a quien puede determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos de su identidad física, fisiológica, psíquica, cultural o social (artículo2,a), Directiva 95/46/CE).

La persona identificable también se le denomina "*interesado*" o impropiamente "*afectado*", según la LORTAD, pues destaca el aspecto negativo del derecho que tiene una persona humana (v.gr. la vulnerabilidad) y no el positivo de ser titular de los mismos o tener interés legítimo para ejercitarlos en las condiciones previstas en la Constitución y el ordenamiento jurídico vigente.

En términos ius-informáticos, las expresiones "*cualquier información*", deben interpretarse como una unidad de datos (textual, imagen o sonido) representada en forma binaria (0/1) en el tratamiento computarizado y relacionado con una persona natural o física. La información recogida, procesada, almacenada y recuperada por consulta o transferencia total o parcialmente por medios "automáticos" y electro-computacionales. Esta información se caracteriza por ser relevante, clara, oportuna y confiable. Relevante significa que el contenido transmitido es por sí solo suficiente para ser comprendido por el receptor de una información. Clara e inteligible significa que sea transparente, de fácil entendimiento y que el mensaje transmitido por el emisor sea través de canales aceptables y entendibles para el receptor. La oportunidad hace relación a la temporalidad en la que es transmitida y recepcionada; y finalmente confiable, significa que reúne todos los elementos y calidades anteriores [121] . Sin embargo, se ha creído que el término *cualquier información* utilizado por la LORTAD constituye un error de definición consistente en no haber excluido de su ámbito objetivo a un núcleo mínimo de datos, para así evitar que toda información relativa a una persona física, por nimia que parezca, constituya un dato de carácter personal a los efectos legales [122] .

Pero lo que no se repara es que la información de carácter personal a la que hace referencia la LORTAD, es la referida al concernido dentro de un marco constitucional de derechos y libertades inherentes a la persona humana (artículos. 14,15,16 y 55.1 CE), valores y principios como la dignidad de la persona, el desarrollo de la personalidad, el interés público, la paz social y democrática (artículo 10 CE); y los límites constitucionales a los derechos de los demás previstos en la propia CE (artículo 18.4., 20.1.d) y la ley (LORTAD y normas de desarrollo).

Por contra, para quienes reclaman más excepciones y limitaciones al concepto "*cualquier información*"; además y, por si fuera poco, se sostiene que la LORTAD, paralelo al cúmulo de derechos (principalmente integrantes del *habeas data),* se plantea una escalonada y categórica relación de excepciones y limitaciones establecidas para los titulares de los datos, los ficheros de titularidad pública y privada (aunque sean más acusadas para los de carácter público), que no está lejos de desvirtuar los derechos constitucionales, principalmente la intimidad y el habeas data que pretende protegérselos, y quizá por ello, no se duda en calificar la actividad legislativa de los creadores de la LORTAD como una página de protección de derechos fundamentales frente a un catálogo que contiene un "*máximo de euforia de excepciones y limitaciones"*, según *Davara* y que "afectan el contenido esencial de la garantía reconocida en el artículo18.4" CE, a tal punto que ha sido objeto de recursos de inconstitucionalidad ante el Tribunal Español, [123] y con fundadas razones jurídicas, como se observó en la parte primera de éste trabajo.

Este régimen de excepciones y limitaciones a los derechos, tanto en el Convenio Europeo de 1981, como en la Directiva 95/46/CE, es igualmente amplio y enfático cuando se refiere a los asuntos de seguridad y salubridad públicas, la defensa, los intereses económicos o financiero y de investigación del Estado; entre otros (artículo13 y 26), y muy puntual cuando se relaciona con el régimen de protección de derechos y libertades de la persona (*intimidad* o *vida privada* y habeas data, artículo 13 *in fine* y 26.2 y 3), todos los cuales se justifican y legitiman *por razones de seguridad del Estado o de la defensa* (C. 43).

En otras latitudes, como la canadiense, por ejemplo, han preferido no utilizar el concepto genérico de datos o informaciones personales, sino una relación de los que se consideran como tales, y aunque es una relación *numerus clausus,* la interpretación hermenéutica posibilita la actualización del listado. La *Act Privacy* canadiense [124] , previamente entiende como *personal information,* la concerniente a una persona, cualquiera sean los mecanismos o tecnologías de las que se obtengan o graben, para luego relatar los siguientes supuestos de información personal:

a) La información relacionada con la raza, origen nacional o étnico, color, religión, edad o estado civil de la persona. b) la información relacionada con la educación, el historial médico, delictivo, laboral de la persona, o la información relacionada a las transacciones financieras en las que el individuo ha estado involucrado. c) cualquier número o símbolo que identifique o se le asigne a una persona. d) la dirección, las huellas digitales o el tipo sanguíneo de la persona. e) las opiniones o ideas personales, excepto aquellas vertidas sobre otra persona, o sobre una propuesta de subvención, recompensa o un premio otorgado por una institución gubernamental, sección, departamento o Ministerio, según lo estipulen sus reglamentos. f) la correspondencia enviada a una institución gubernamental por una persona que es implícita o explícitamente de naturaleza privada o confidencial, así como las contestaciones a la misma en la medida que revelen un contenido que corresponda a la envida originalmente. g) las ideas u opiniones de otra persona sobre él. h) las ideas u opiniones de otra persona sobre una propuesta de subvención, recompensa o premio otorgado por una institución gubernamental, sección, departamento o Ministerio, según lo estipulen sus reglamentos y referida en el parágrafo (e), pero excluyendo el nombre de la otra persona sobre la cual dedicó sus ideas u opiniones. i) el nombre de la persona que aparece relacionada con otra información personal y que el sólo descubrimiento del verdadero nombre revelaría información sobre aquél; pero para los propósitos de artículos 7, 8 y 26 de ésta ley y el artículo 19 de la LAIC (Ley de acceso a la información canadiense. *Access to information Act* [125]), la información personal queda excluida. J) la información de una persona que es o fue funcionario o empleado de una institución gubernamental y relacionada con la posición o funciones del mismo. Esta información incluye: 1. el hecho de que el individuo es o era funcionario o empleado de la institución gubernamental; 2. el título, dirección comercial y número del teléfono de la persona; 3. la clasificación, rango y monto del sueldo y atribuciones según su cargo; 4. el nombre de la persona que figura en un documento preparado por éste en el ejercicio de su empleo; y, 5. las ideas u opiniones personales expresadas en el curso de su empleo. k) la información sobre una persona que desempeña o desempeñó los servicios bajo contrato con una institución gubernamental. Esta información incluye: los términos del contrato, el nombre del individuo y las opiniones o ideas expresadas en el transcurso del mismo. l) información relacionada con cualquier beneficio discrecional de naturaleza financiera, incluida la concesión de una licencia o permiso, así como nominación del mismo, el nombre de quien la confirió y la naturaleza precisa de la misma.; y, m) la información sobre una persona muerta y hasta por veinte (20) años.

La regla general para la protección de *toda información personal* en el derecho canadiense es el no descubrimiento o divulgación de los datos o las informaciones de carácter personal cuando no haya consentimiento de una persona a quien concierne una información catalogada de personal (artículo3,b),) y siempre que ésta se halle bajo el control o responsabilidad de una institución gubernamental. La excepción, es que se podrá descubrir la información previo un procedimiento administrativo breve y sumario en las trece situaciones previstas en el artículo8.2. de la *Act Privacy*.[126] [Mackenzie vs. Canadá (Ministerio de Salud Nacional y Bienestar Social). 1994.Primera Instancia. Corte Federal Canadiense .F.C.TD.] .Estas que se pueden catalogar de excepciones al descubrimiento o divulgación de la información por parte de un organismo del Estado, tienen como fundamento la realización de algunos de los fines de un Estado de derecho, tales como la seguridad, la defensa, la salubridad y la economía públicas, o bien los intereses generales, públicos, de relaciones internacionales, investigativos (judiciales o administrativos), científicos o archivísticos o, en últimas, los del concernido o interesado con la información.

5.2.3.2. Diferentes grados de protección de los datos o informaciones personales del concernido. Especial referencia al consentimiento.

La LORTAD, reconoce ciertos grados de protección a los datos o informaciones de carácter personal, de conformidad con los criterios observados en el tratamiento automatizado de la información y, sobre todo, del consentimiento de la persona concernida, que bien puede

sostener y representarse en una tipología de los datos de ultra-protección, datos de protección calificada y los datos de protección general, como en seguida veremos.

Sea lo primero decir que, tratamiento automatizado, es el conjunto de operaciones y procedimientos técnicos de carácter automatizado que permiten la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como la cesión de datos que resulten de comunicaciones, consultas, interconexiones y transferencias (artículo 3,c), LORTAD). Definición que en esencia es igual a la observada por la Ley núm. 78-17, de 6 de enero de 1978, *relativa a la informática, los ficheros y las libertades.*, el Convenio de Europa de 28/1/81, artículo 2., c), ratificado por España el 27 de Enero de 1984 y la Directiva 95/46/CE, artículo2, b),relativa a la protección de las personas físicas en lo respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Esta definición como las fases del tratamiento automatizado de los datos de carácter personal previstas en ésta, por la ubicación, el contenido y los criterios orientadores y hermenéuticos que tiene en la LORTAD, se aplica a toda clase de datos en ésta previstos y sin perjuicio de que se haga énfasis para una cualquiera de las fases o del ciclo de tratamiento informático y su correspondiente régimen de protección reforzado. v.gr. el artículo 7.3. LORTAD .

La regla general es que el consentimiento de la persona concernida se requerirá siempre para el tratamiento automatizado de los datos personales, salvo que la ley disponga lo contrario o que pueda ser revocado por causa justificada y sin efectos retroactivos o *ex nunc* (artículo6.1 y 3).

Las excepciones a la regla se presentan en los siguientes eventos: a) cuando los datos se recojan de fuentes accesibles al público, b) cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, c) cuando se refieran a personas vinculadas por una relación negocial, laboral o administrativa, o un contrato y sean necesarias para el mantenimiento de las relaciones o para el complimiento del contrato.

Con éstas premisas, los datos de carácter personal a tenor de la LORTAD, serán de ultra-protección, sí se requiere el consentimiento expreso y escrito de la persona concernida para el tratamiento de automatizado de los datos que revelen la ideología, religión y creencias (artículo7.2 LORTAD y 16.2 CE).

De protección calificada, si se requiere el consentimiento expreso de la persona concernida para el "tratamiento automatizado y cesión" de datos de carácter personal que hacen referencia al origen racial, a la salud y a la vida sexual, siempre que sea por razones de interés general previstos en la ley, es decir, por *habilitación legal expresa*, según la exposición de motivos de la propia LORTAD. (artículo 7.3 LORTAD).

Algunos de los mecanismos de protección para los anteriores datos se refleja en la prohibición a la creación de ficheros con finalidad exclusiva de almacenar datos de carácter personal que revelen ideología, religión, creencias, origen racial o vida sexual (7.4. LORTAD). En cuanto a los datos de carácter personal relativos a la salud de las personas, sólo podrán procederse al tratamiento automatizado o la cesión de datos prevista en el artículo 11 LORTAD (para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario), por parte de las instituciones y centros sanitarios públicos o privados y los profesionales correspondientes, de conformidad con las normas especiales (Ley 14/1986, de 25 de abril, General de Sanidad; Ley 25 de 1990, de 20 de diciembre, del Medicamento; Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública, y demás leyes sanitarias), previo el consentimiento del concernido.

En cuanto a los datos de carácter particular relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros automatizados de las administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Estas prohibiciones, restricciones y limitantes al tratamiento automatizado de los datos relativos al origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad, previstas en la Directiva 95/46/CE, artículo8.1. "Categorías especiales de tratamientos", desde el Convenio Europeo de 1981, en su artículo 6, ya habían sido detectadas bajo el epígrafe de "Categorías particulares de datos", en las cuales se incluye los datos de carácter personal referentes a condenas penales y no se incluye los datos referentes a la pertenencia a sindicatos relacionada en la Directiva. (por las claras razones no sólo temporales de la norma sino por el impacto social, gremial, político y de poder de la información actual sobre el tema, aunque la Ley francesa sobre la informática ya la preveía). A pesar de las prohibiciones al tratamiento automática estipuladas en el Convenio, se deja abierta la posibilidad para que puedan hacerlo los Estados en su "derecho interno", siempre que se "prevea garantías apropiadas". La Directiva aparentemente fue más tajante al prohibir cualquier tratamiento de datos personales, sin cláusulas abiertas. Sin embargo, bajo el amplio pero puntual régimen de excepciones y las desnaturalizaciones o derogaciones de la regla general de prohibición previstas en la Directiva, no sólo es posible regular sobre la temática prohibida sino que se tienen parámetros en cascada para hacerlo en el artículo 8.2 [a), a e),], 8.3. a 8.7., aparte claro está ,de las no aplicaciones de la regla general en cada etapa o fase del ciclo de tratamiento automatizado que también es amplio. v.gr. artículo 13 de la Directiva.

Por exclusión de los "*datos especialmente protegidos*" en el artículo 7 de la LORTAD, se presentan los datos de carácter general con régimen de protección y tratamiento automatizado general, es decir, se aplicará la regla general del consentimiento y las excepciones, sin más.

Con base en el criterio o principio del consentimiento o de "*autodeterminación*" como lo denomina la exposición de motivos de la LORTAD, la doctrina española [127] , ha clasificado a los datos de carácter personal, así: a) datos de carácter general, y b) datos "sensibles"(término también utilizado por la exposición de motivos de la LORTAD, para destacar el nivel reforzado de protección) o "hipersensibles", contraponiendo un tratamiento y régimen de protección, que sólo se funda en el consentimiento del afectado, salvo que la ley disponga otra cosa, para los primeros; al de los datos sensibles o "hipersensibles", cuyo consentimiento debe ser por escrito y expreso, del afectado al cual deberá advertirse de su derecho a no prestarlo. Por su parte, *López Díaz* [128] , además de destacar los datos de carácter personal de tipo general y hace énfasis en los llamados *sensibles*, asignándole una triple tipología a éstos: a) Datos relativos a la ideología, religión y creencias; b) Datos relativos al origen racial, la salud y la vida sexual de los interesados; c) Los datos referentes a la comisión de infracciones penales o administrativas. Además *Orti Vallejo* [129] , al plantear la anterior tipología de datos sensibles, destaca que los datos relativos a la vida familiar, relaciones personales y patrimoniales entre cónyuges (no las sexuales), relaciones con los hijos, pensiones o costumbres familiares o personales no han quedado incluidas en estos grupos de datos a pesar de merecer especial protección por parte de la LORTAD, quizá, interpreta el autor citado, que es por la tendencia mayoritaria de las leyes de todos los países que afirman que los datos relativos a la vida privada resultan secundarios frente a aquellos que se refieren a las opiniones o ideologías. Sin embargo, conviene re-estudiar la posibilidad de que algunos datos íntimos gocen de protección legal, pues tras datos aparentemente inocuos se esconden datos verdaderamente sensibles y viceversa.

Herbert M., establece una tipología de los datos de carácter particular obrantes en bancos automatizados, agrupándolos en muy sensibles, sensibles y neutros, y para cada uno un sistema de garantías diferenciado. La jurisprudencia alemana ha rechazado la diferenciación entre los distintos datos, y apoyándose en la *sensibilidad, no por relación al dato mismo, sino a la vista del contexto y de las finalidades perseguidas* [130] .

La "*teoría del mosaico*" de *Simitis,* plantea que datos *ab initio* irrelevantes o "anodinos" pueden esconder datos "sensibles", con el simple cambio de la finalidad que dichos datos perseguía y dado su multi-funcionalidad como tales, la interconexión de los ficheros y la libre utilización de los mismos. Datos *sensibles*, se reputaban los relativos a la salud, la vida sexual o las convicciones políticas y, en tal virtud, los sistemas de protección eran máximos, contrapuesto a los datos *libres* que escondían una inocuidad en el espacio proteccionista. Por ello, el autor citado, era partidario que el legislador al regular los sistemas de tratamientos de datos, tome en cuenta la finalidad y el contexto de los mismos, *hasta el punto de conseguir que el éxito de la protección de los datos dependerá, no de una calificación abstracta de los mismos, sino mediante una reglamentación flexible, adaptada a las condiciones particulares de los diferentes tratamientos* [131] .

Como antes se observó, en la Ley de Protección de la Intimidad del Canadá, (LPDPC), *Act Privacy* 1983, se incluyen los denominados "datos sensibles" dentro de un extenso listado en el artículo 3, en trece literales, como datos personales o informaciones de carácter personal, sin calificarlos de tal o de diferenciar el grado de protección que a éstos debe darse. En consecuencia, la sensibilidad de los datos personales o su limitado o prohibido descubrimiento, se determina por la condición de ser datos a los que les falta el consentimiento del titular, se hallan bajo el control del Estado y constituyen una causal de excepción (numerus clausus) según el artículo 8.2. LPDPC [132] .

5.2.3.3. Protección penal de los datos *sensibles,* en el artículo197 del Código Penal Español

Sí en el ambiente extrapenal (civil y administrativo principalmente), amplia y fructíferamente han teorizado; entre otros temas, la determinación de los grados de protección, la clasificación de los datos denominados "sensibles" y la naturaleza misma de estos datos, a través de la *teoría del mosaico de Simitis,* la cual resulta todavía aún discutible, como hemos visto, en el órbita penal que todavía no ha conformado su propia teoría sobre la sensibilidad de los datos y el grado de protección punitiva gradado que debe suministrarles, a la vista de la clasificación que la propia

Constitución (artículo16.2), la LORTAD (artículo7) y la propia doctrina ibérica han realizado, resulta cuando menos, imprecisa la protección deparada a los denominados datos *sensibles*, por las siguientes razones:

a) Los legisladores del Código Penal Español de 1995, por "*nítido fundamento y legitimidad político-criminal*" [133] , se limitaron a aplicar la técnica de los tipos agravados y ultra-gravados, cuando un delito contra la intimidad se realice con medios informáticos y/o telemáticos y recaiga sobre datos de carácter particular que revelen la *ideología, religión, creencias, salud, origen racial o vida sexual* (artículo197.5 y 6 *in fine*), sin distinción alguna de los datos y el grado de protección deparada por la Constitución y el ordenamiento jurídico.

b) La enunciación *numerus clausus* de los datos considerados *sensibles*, por el Código Penal Español resulta imprecisa, pues no son todos los que están, ni están todos los que son, como suele decirse. En efecto, como vimos el Convenio Europeo, al prohibir inicialmente el tratamiento automatizado de los datos de carácter personal relacionados con el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, la salud o la vida sexual, así como los datos de carácter personal referente a condenas penales (artículo6), establece paralelamente una relación de los datos que considera sensibles, y por tanto, con mayor incidencia en protección legal asignada. Igual cosa sucede con la Directiva 95/46/CE, artículo 8. Una simple comparación gramatical del listado de los datos considerados sensibles por el Código Penal Español (Artículo197.5), de una parte; y los estimados tales por las normas comunitarias, de otra parte, es indicativo de que el listado *numerus clausus* del Código Penal Español peca por defecto. Algunas de las implicaciones por este proceder son las de quedar por fuera de la protección penal datos de carácter personal que las normas consideran sensibles y que los doctrinantes las han ratificado.

c) Bien es cierto que al Código Penal Español, no le corresponde resolver el problema surgido por la rebaja en el mínimo de garantías previstas en el Convenio de Europa de 1981 (y diríamos nosotros del mínimo también establecido en la Directiva 95/46/CE), con relación a la LORTAD, tolerante y laxa [134] , al permitir lo que inicialmente está prohibido, es decir, el tratamiento informatizado de datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual. Aspecto que incluso es objeto de recurso de inconstitucionalidad ante el Tribunal Constitucional. No es menos cierto, que el legislador de 1995, hizo caso omiso a esa expectativa de inconstitucionalidad sobrevenida y conocida a la fecha de expedición del Código Penal Español, al enlistar algunos de los datos considerados sensibles, los cuales al prohibirse su tratamiento informatizado por disposición legal e incluso constitucional (artículo16.2.CE), cuando menos resulta sorprendente, pues su uso legítimo estaría proscrito civilmente previamente antes que recurrir al ámbito penal como *ultima ratio.*

A pesar de ello, parece existir solución al problema desde el punto vista penal dirigida al ámbito extra-penal, como lo denota el profesor MORALES. En efecto, aconseja que se pudiera tratar automáticamente datos sobre el origen racial o vida sexual de las personas, si previamente estos han sido sometidos al procedimiento de disociación, es decir, que el tratamiento de la información personal, previo procedimiento, no asocie a una persona determinada o determinable (artículo3, f),), o se *anule la posibilidad de identificar o determinar al titular de los datos*. De esta forma sólo podría tratarse automáticamente datos personales sin identificar a la persona y con fines estadísticos y sociológicos.

d) No parece acertada la política legislativa adoptada en el numeral 6, del artículo 197 del Código Penal Español, por la cual, se ultra-gravó con fines de ultra-protección penal, la comisión de un delito contra la intimidad realizado con medios informáticos y/o telemáticos cuando *afectan a datos de los mencionados en el apartado 5*, es decir, a los denominados "sensibles" sólo enlistados: "*ideología, religión, creencias, salud, origen racial o vida sexual*". Y no nos parece, por el exceso de punibilidad aplicado a la ultra-gravación, con penas que habiendo sido aumentadas por la agravación del tipo previsto en el apartado 5 del artículo 197, con penas impuestas al tipo básico (uno a cuatro años y multa de doce a veinticuatro meses) y aumentadas en su mitad superior, para

luego con esta ultra-gravación, imponérsele además la “pena de prisión de cuatro a siete años”, según el artículo 197.6 *in fine*, lo cual a la vista del principio de culpabilidad, como antes se dijo, resulta quebrantado por exceso de punibilidad, máxime si tenemos en cuenta la clase del tipo penal, sus implicaciones sociales y culturales; y sobre todo, la incertidumbre que pone de en evidencia la llamada teoría del mosaico sobre los datos inicuos o irrelevantes considerados sensibles o viceversa, como nosotros estimamos.

_____ .

CITAS:

(66) Cfr. Sentencia de Julio 20 de 1993, Tribunal Constitucional Español. M.P.: García Mon., Fundamento Jurídico (FJ 6). AA.VV. *Colección de discos de Aranzadi.* Ed. Aranzadi, Pamplona (Esp.), 1997. Planteamientos que aceptamos con la excepción de considerar a la “libertad informática” como derecho nuevo, por los argumentos vertidos en nuestro documento electrónico denominado ***LA VISION IUS-INFORMATICA DE LA INTIMIDAD, NO ES UN NUEVO DERECHO FUNDAMENTAL*** En: http://akane.udenar.edu.co/derechopublico . regresar.

(67) WARREN, Samuel y BRANDEIS, Louis. ***El Derecho a la intimidad***. Edición a cargo de Benigno Pendás y Pilar Baselga. Ed. Civitas, S.A. Madrid, 1995. “The Right to Privacy”, 1890. Veáse, Parte I.de este trabajo, en el que comentamos el Ensayo y extractamos las facultades negativas (derecho a no ser molestado) y positivas (derecho a control de la propia información) que más tarde los doctrinantes italianos (v.gr. Frosini y Losano) y españoles (Pérez Luño y Truyol y Serra), llamaran sobre todo, a las segundas, *libertad informática*. Los planteamientos de Frosini, en Vid. FROSINI, V. ***Informática y derecho.*** Ed. Temis, Bogotá, 1988, pág. 64. Regresar.

(69) “El concepto se refiere a los seres humanos, pero puede extenderse también a los ordenadores o, en general, a cualquier sistema con posibilidad de percibirla y en consecuencia variar su estado. El receptor de la información, con su capacidad de asimilación (bien sea incremento de conocimiento, o cambio de estado) es, pues, una parte esencial del concepto. Otra lo es el lenguaje que aporta la información, compuesto de elementos perceptibles a través de los sentidos (o sensores, en el caso de una máquina) del receptor. Y, naturalmente, si hay mensaje habrá también un emisor, a veces otra persona pero, en términos más generales, un sistema que, como el receptor, es dinámico.” Cfr. FERNANDEZ BEOBIDE, César. *Las nuevas tecnologías y las creaciones intelectuales. Aspectos positivos.* En: El Derecho a la propiedad intelectual y las nuevas tecnologías. Mincultura, Madrid, 1996, pág. 51 y ss. Regresar.

(70) “La denominada *sociedad de la información* no es la fantasiosa idealización de un mundo futurista, sino una realidad de nuestros días, aunque todavía se encuentre en un estado embrionario comparado con lo que puede depararnos dentro de pocos años. Muchos de los elementos de esta sociedad de la información son suficientemente conocidos y prestan ya útiles servicios a la sociedad: el teléfono, las emisoras de radio y televisión inalámbricas y por cable, los satélites, las comunicaciones, las bibliotecas, las librerías, las bases de datos accesibles a distancia, y redes informáticas como Internet. Hasta el momento, en términos generales puede afirmarse que estos distintos elementos para vincular la información funcionan aisladamente, sin ningún tipo de interacción entre ellos”. Sin embargo, creemos que, hoy por hoy, existe tal interactividad gracias a la unión de las telecomunicaciones y la informática, con el descubrimiento de la *multimedia* que incorpora imágenes, sonidos y datos, digitalizados o no, con acceso lógico y/o físico a distancia (redes informáticas) o localmente (equipos computacionales personales, institucionales o empresariales). Vid. GOMEZ SEGADE, José. Respuestas de los sistemas de propiedad intelectual al reto tecnológico. El derecho europeo continental y el derecho anglosajón del Copyright. Mincultura, Madrid, 1996, pág. 131 y ss. Regresar

(71) La Directiva 95/46/CE, art. 2 . Cfr. AA.VV. ***Compedio de discos de CELEX, Bruselas*** (B), 1997. Regresar.

(72) Veáse, BARNES VASQUEZ, Javier. *La internet y el derecho. Una nota acerca de la libertad de expre sión e información en el espacio cibernético. En:* Cuaderno de Derecho Judicial. C.G.P.J., Ordenación de las telecomunicaciones No.VI, Madrid, 1997, Pág. 241 y ss. Regresar. Regresar

(73) Veáse, la parte tercera de éste trabajo sobre el tema: Los datos informáticos, electrónicos y/o telemáticos. Los ficheros y/o bases de datos. Jurisprudencia sobre el documento informático. “Podemos definir el IED como el intercambio de datos en un formato normalizado entre los sistemas informáticos de quienes participan en transacciones comerciales o administrativas. Un sistema de este tipo ha de cumplir tres requisitos básicos: a) el intercambio se ha de realizar por medios electrónicos, b) el formato tiene que estar normalizado, y c) la conexión ha de ser de ordenador a ordenador.” Vid. DEL PESO NAVARRO, Emilio. ***Resolución de conflictos en el***

intercambio electrónico de documentos. *En:* Cuaderno de Derecho Judicial. C.G.P.J., Ambito jurídico de las tecnologías de la información. No.XI, Madrid, 1996, Pág.199 y ss. Regresar

(74) El Tribunal reiteradamente ha sostenido: "A) Que exista un documento, lo que equivale: a) Que se trate de un documento en sentido estricto, y ha de entenderse por tal el escrito, en sentido tradicional, o aquella otra cosa que, sin serlo, pueda asimilarse al mismo, por ejemplo, un disquete, un documento de ordenador, un vídeo, una película, etc., con un criterio moderno de interacción de las nuevas realidades tecnológicas, en el sentido en que la palabra documento figura en algunos diccionarios como *cualquier cosa que sirve para ilustrar o comprobar algo+ (obsérvese que se trata de una interpretación ajustada a la realidad sociológica, puesto que, al no haber sido objeto de interpretación contextual y auténtica, puede el operador del derecho tener en cuenta la evolución social), siempre que el llamado *documento+ tenga un soporte material, que es lo que sin duda exige la norma penal (por todas, TS SS 1114/1994 de 3 Jun., 1763/1994 de 11 Oct. y 711/1996 de 19 Oct.)." STS Nov. 23 de 1996. M.P. Montero Fernández. FJ. 6.A. Cfr. AA.VV. Compendio discos Aranzadi. Ob. cit., Madrid, 1997. Regresar

(75) GONZALEZ NAVARRO, Francisco y GONZALEZ PEREZ, Jesús. ***Comentarios a la Ley de Régimen jurídico de las Administraciones públicas y el procedimiento administrativo común***. Ed. Civitas, S.A., 1a, ed., Madrid. 1997, pág. 695. Regresar

(76) SERRANO GOMEZ, Alfonso. ***Delitos contra la intimidad , el derecho a la propia imagen y la inviolabilidad de domicilio***. *En*: Derecho Penal - Parte Especial. Ed. Dykinson, Madrid, 2da. ed., 1997, pág.227. Regresar

(77) MORALES PRATS, F. *Delitos contra la intimidad...* Ob. ut supra cit., pág. 303 y ss. Regresar.

(78) La Directiva 95/46/CE, les concede una categoría especial de tratamiento, a los datos personales que "revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad", prohibiéndolo por parte de los Estados (art.8.1), salvo que se de una cualquiera de las excepciones previstas en los numerales 2 a 7. v.gr. que haya consentimiento explícito del interesado; que sea necesario para salvaguardar el interés vital del interesado o de otra persona, etc. En todo caso, estas excepciones son taxativas o *numerus clausus.* Vid. Compendio CELEX. Ob. cit. Bruselas, 1997. En la Ley de Protección de la Intimidad del Canadá, "Act Privacy" 1983, se incluyen los denominados "datos sensibles" dentro de un extenso listado en el art.3, en trece literales, como datos personales o informaciones de carácter personal v.gr. (a) la información relacionada con la raza, origen nacional o étnico, color, religión, edad o estado civil de la persona. La naturaleza de sensibles o de limitada o prohibido descubrimiento, se determina por la condición de ser datos a los que les falta el consentimiento del titular, se hallan bajo el control del Estado y constituyen una causal de excepción (numerus clausus) según el art. 8.1 y 2. LPDPC**.** Cfr.Caso: Mackenzie v. Canada (Ministerio de Salud Nacional y Bienestar Social). (1994), 88 F.T.R. 52; 59 C.P.R. (3d) 63 (Corte Federal, Primera Instancia). AA. VV. ***Base de Datos de la Univ. de Montreal. Biblioteca Virtual de Derecho Público***. *(C).* Vía Internet en Inglés, Montreal (Canadá), 1998. www.umontreal.edu.ca. Regresar.

(79) Penas. SERRANO GOMEZ, A. Ob. cit. pág. 226. Regresar.

(80) a) La creación ilegal de ficheros automatizados de datos sensibles y no solamente la penalización de los que revelen estos datos (art.197.5.); b) La obtención por medios fraudulentos, desleales o ilícitos o sin menoscabar el consentimiento de la persona afectada, de este tipo de datos (sensibles) para incluirlos en ficheros automatizados. Vid. BAON RAMIREZ, Rogelio. ***Visión general de la informática en el nuevo Código Penal.*** En: Cuadernos de Derecho Judicial. C.S.P.J., Ambito de las tecnologías de la información. No. XI, Madrid, 1996, pág. 95. Regresar.

(81) Cfr. SERRANO GOMEZ, A., Ob. ut supra cit. pág. 226. Regresar.

(82) MORALES PRATS, Fermín. ***La protección penal de la intimidad frente al uso ilícito de la informática en el Código Penal de 1995.*** En: Revista C.G.P.J. Delitos contra la libertad y la seguridad, Madrid, 1996, pág.173 y ss. Regresar.

(83) Siendo la LORTAD (LO. 5/1992), el Convenio Europeo de 1981 y la Directiva 95/46/CE, además de ser normas de protección extrapenal de la intimidad son normas de interpretación de la terminología utilizada por el Código Penal Español en lo referido al Tit. X, debemos en consecuencia atender sus conceptos y estructura normativa y sistemática para entender mejor el fenómeno TIC y su incidencia en los Delitos contra la intimidad. Por ello, se ha sostenido con razón que "...la acción de apoderamiento de datos (expresión impropia la vista de los conceptos informáticos que emplea la LORTAD) tiene como traducción técnica más ajustada la acción de acceso a los mismos, que es la tipificada en el inciso segundo" parte in fine, con igualdad de penas pero con diferente tratamiento jurídico penal a un misma conducta y verbo "utilizar" datos. Cfr. MORALES PRATS, F. Ob.ut supra cit., pág.173. Regresar.

(84) Sin embargo, recurriendo a la una aclaración interpretativa, se ha sostenido que el "primer pasaje del art. 197.1 C.P., debe limitarse a las conductas de apoderamiento por medio de conexión del

ordenador a la red telefónica (correspondencia informática) ya impresos fuera del sistema. Asimismo el tipo puede ser proyectado a la conducta de captación intelectual, sin desplazamiento ilícito, de los referidos mensajes (por ejemplo, cuando se hallan en pantalla de ordenador)". A pesar de ello, la excepción no justifica la separación de la interpretación del objeto material del delito por estar dentro o fuera de un sistema tecnológico. Cfr. MORALES PRATS, F. Ob. ut supra cit., pág. 300. Regresar.

(85) Vid. MUÑOZ CONDE, Francisco. ***Derecho Penal. Parte Especial.*** Undécima ed., Ed. Tirant lo blanch, Valencia, 1996, pág.218. SERRANO GOMEZ, A. Ob. cit., pág. 227. Regresar.

(86) Cfr. MORALES PRATS, F. *Comentarios a la parte Especial del Derecho Penal* ... Ob. cit.pág. 229. Igual En: ***La protección penal de la intimidad...,*** "La protección penal de la "privacy" informática: "habeas Data" y represión penal de los abusos informáticos. El CP de 1995 en el art. 197.2. contempla la tutela penal de la "privacy" informática por primera vez en nuestro país..." Ob. cit., pág. 165. *Regresar*

(87) Véase, apartado 5.5.1., d), sobre el EDI o IDE . Además: AA.VV. *El EDI (Electronic Data Interchange).* En: Actualidad Informática Aranzadi. A.I.A. Núm. 10 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1994.pág.1. Regresar.

(88) El art 2.2 de la Ley 31 de 1987, estipula que "los servicios de telecomunicación se organizarán de manera que pueda garantizarse eficazmente el secreto de las telecomunicaciones de conformidad con lo dispuesto en el art. 18.3 de la Constitución". El art 3, de la ley sostiene que se entiende "por telecomunicaciones: Toda transmisión, emisión, o recepción de signos, señales, escritos imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos". Citado por SERRANO GOMEZ, A. Ob. cit. pág.226. Regresar

(89) Cfr. MORALES PRATS, F. *Comentarios a la parte Especial del Derecho Penal* ... Ob. cit.pág. 305. Regresar.

(90) Vid. AA.VV. *El EDI...* Ob. cit., pág 1 y ss. *Regresar.*

(91) Cfr. QUERALT JIMENEZ, J.J. ***Derecho Penal Español.*** Parte Especial. 3 ed., Ed. J.M. Bosch, Barcelona, 1996, págs. 183 y 184. Regresar.

(92) Citando a PEREZ CANOVAS, apoya la posición de que "las personas jurídicas y el derecho al honor (o prestigio como lo denomina el Tribunal Constitucional): Comentario a la S.T.S. de 5 de octubre de 1989". ORTI VALLEJO, Antonio. ***Derecho a la intimidad e informática.*** Ed. Comares, Granada (Esp.), 1994. págs.74 y ss. Regresar

(93) Cfr. MORALES PRATS, F. Ob. ut supra cit. pág. 338 y ss. Regresar

(94) Vid. BUSTOS RAMIREZ, Juan. *Manual de Derecho Penal. Parte Especial. 2da, ed.* Ed. Ariel S.A., Barcelona, 1991, pág.87. Regresar.

(95) QUERALT JIMENEZ, J.J. ***Derecho Penal Español... Ob. cit., pág. 183. Regresar.***

(96) Vid. GIL HERNANDEZ, Angel. ***Protección de la intimidad corporal: Aspectos penales y procesales.*** En: Revista General del Derecho. Año, LII Núm. 622-623, Jul-Ago., Valencia, 1996, pág. 7950 y ss. Regresar.

(97) Véase, BUSTOS RAMIREZ, J. *Manual de Derecho Penal... Ob. cit., pág. 88. Regresar*

(98) Véase, el documento electrónico: ***LOS DATOS PERSONALES INFORMATIZADOS EN LA LEGISLACIÓN FORÁNEA Y COLOMBIANA***. En: http://akane.udenar.edu.co/derechopublico. Además se debe destacar como lo sostiene el considerando 7 y 10, a saber: "7) las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros;" y "10. que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales". Regresar.

(99) MORALES PRATS, F., *Protección a la ...* Ob. cit., pág. 174 Critica el término ***familiar,*** porque considera una "muletilla" que trae el art.18 CE y que no ha podido desprenderse el legislador penal de 1995, a pesar de que la LORTAD, no menciona a los "datos familiares" sino únicamente los personales en las cuales obviamente están aquellos (art.3, a)). Sin embargo, esto no suma ni resta a la recta interpretación del derecho fundamental de la intimidad que abarca " aquella parcela de la personalidad que su titular puede mantener legítimamente al margen del conocimiento público, el denominado *ius solitudinis", pues la intimidad es un bastión que se erige contra las intromisiones*

de los demás en la esfera privada de un sujeto, intromisión que puede sobrevenir tanto de los particulares como de los poderes públicos". Cfr. QUERALT JIMENEZ, J.J. Ob. cit., pág. 183. Regresar.

(100) Es tal, la evolución de la jurisprudencia que se extiende el apoderamiento a la "receptación", por error de correos, de cartas destinadas a otras personas y que luego son abiertas (STS 6/10/67, 25/11/69). "El apoderamiento es tan fundamental, que si se pueden conocer los secretos documentales de otro sin apoderarse de sus papeles no existe este delito o, por lo menos, este tipo delictivo en concreto". Cfr. MUÑOZ CONDE, Francisco. Ob. cit., pág. 218-219. Regresar.

(101) Así se planteaba desde 1983, por MORALES PRATS, F. ***La tutela penal de la intimidad: privacy e informática***. Barcelona, 1983, pág. 191-192. En igual sentido: BUSTOS R., Juan. *Manual...* Ob. cit., pág 88. Regresar

(102) Cfr. MORALES PRATS. *Protección a la ...* Ob. cit., pág 173. Regresar

(103) Véase, GONZALEZ NAVARRO, F y GONZALEZ PEREZ, J. Ob. cit., págs. 686-714 y 808-854. Regresar

(104) Al respecto, se comenta que "sorprende la inclusión de un elemento subjetivo del injusto en este tipo de conducta delictiva; probablemente con esta partícula intencional el legislador ha pretendido reservar la incriminación típica para las conductas de dolo directo, excluyendo las de dolo eventual. La Expresión "tercero" parece, en principio querer referirse al titular de los datos, pues la LORTAD tiene por "afectado a la "persona física titular de los datos que sean objeto de tratamiento electrónico" (art.2.3. e) LORTAD). Sin embargo, en el segundo inciso del art. 197.2 C.P., se alude a conductas verificadas en perjuicio del "titular de los datos o de un tercero". Esta cláusula induce a la perplejidad puesto que la tutela del "habeas data" en la LORTAD se instituye para proteger a la persona física titular de los datos, y a ésta exclusivamente debería referirse el C.P. Por ello, lo más prudente es interpretar que "tercero", en el primer inciso del precepto es la "persona física titular de los datos personales". Cfr. MORALES PRATS, F. Ob. cit. pág. 173. Muy a pesar de ello, la Directiva 95/46/CE, en el art. 2, f), sí distingue entre titular de los datos y el tercero. Sobre este último dice que es "La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento". Regresar

(105) MORALES PRATS, *Protección a la ...* Ob. cit., págs.170-175. Regresar

(106) Ibidem, pág. 171. Regresar

(107) Exposición de Motivos de LORTAD. AA.VV. Base de datos Aranzadi S.A., Pamplona, 1997. Regresar

(108) MORALES PRATS. Ob. ut supra cit., pág.173. Regresar.

(109) Vid. SERRANO GOMEZ, A. Ob. cit. pág. 229. Regresar

(110) Sin embargo, el principio del *non bis in ídem,* entre sanciones penales y administrativas, en éste punto se halla vulnerado, al prever, entendemos, que el art. 197.1 y el art.33 de la Ley de telecomunicaciones hay regulado doblemente un misma conducta. Esto ha sido objeto de recurso de inconstitucionalidad ante el Tribunal Constitucional. SERRANO GOMEZ, A. Ob. cit. pág. 299. Regresar

(111) SERRANO GOMEZ, A. Ob. ut supra cit., pág. 163 y ss. Regresar

(112) Vid. CHINCHILLA MARTIN, Carmen. ***El régimen jurídico de las telecomunicaciones. Introducción***. *En:* Revista de la Escuela Judicial. C.G.P.J., Ordenación de las telecomunicaciones. No. VI, 1997, Madrid, pág. 12. Regresar

(113) Ibídem, pág. 15 y ss. No es sólo son los E-Mail, sino mediante una variada gama como se ejerce ese control. Regresar

(114) MORALES PRATS, F. *Comentarios a la parte...* Ob. cit., pág. 304. Regresar

(115) Vid. Ob. ut supra cits. págs. 229-230; 220-221; y , 94, respectivamente. Regresar

(116) Ibídem., págs. 172. Regresar

(117) QUERALT JIMENEZ, J.J. ***Derecho penal Español. Parte Especial,*** *3 ed.* Ed. J.M. Bosch, Barcelona, 1996, pág. 195. Regresar

(118) Citado por PEREZ VALLEJO, Ana M. ***La informática y el derecho penal***. En: Actualidad Informática Aranzadi. Ed. Aranzadi, Pamplona (Esp.), No. 19, Abril, 1996, pág. 10. Regresar.

(119) En el caso norteamericano que tiene por fundamento la incautación por los Servicios Secretos de los Estados Unidos, de medios informáticos físicos o de hardware (ordenador con su unidad central de procesamiento CPU y unidades periféricas) y lógicos o de software (programas de ordenador), por presunta comisión de actos ilícitos de un colaborador de un sistema electrónicos de tablón de anuncios (*"Electronic Bulletin board system".BBS)* con información y negocios específicos de libros y publicaciones. El sistema BBS, contenían mensajes privados de correo electrónico enviados por personas interesadas en la información y negocios. Estos se almacenaban en la memoria del disco duro del ordenador como copia de seguridad o *(backup)*.

Los mensajes se almacenaban, pero no alcanzaron a ser leídos por el destinatario cuando fueron incautadas por el *Secret Service US* . Steve Jackson Games, Inc et all, como demandante, sostenían que el actuar de la Agencia Especial de EE.UU, constituía una intervención o interceptación ilegal de las comunicaciones electrónicas, en virtud de la Ley Federal de Comunicaciones por Cable. 18 U.S.C., enmendada por la Ley de Protección a la intimidad en las comunicaciones electrónicas de 1986 (*The Electronic Communication Privacy Act of 1986*). La Sentencia, estimó que en el caso presente no existió interceptación de comunicación electrónica, almacenada en disco y backup, pero no leída. El texto completo de la Sentencia de la Corte de Apelaciones de los Estados Unidos de América, 51 Circuito, Octubre 31 de 1994, Caso Steve Jackson v. Secret Service US. En: *WWW.UMONTREAL.CA. (Universidad de Montreal, Canadá).* *Regresar*

(120) *Los mensajes de correo electrónico* (E-Mail), son una de las variadas formas típicas de comunicación electrónica de hoy en día y tiene por objeto, comunicar o transferir datos o informaciones de todo tipo y naturaleza (texto, imagen o sonido), entre dos personas, a través de ordenadores o computadores ubicados en diferentes lugares del planeta. Para ello deben disponer de una línea telefónica, un *MODEM* (Modulador y DEModulador de señales), un operador de comunicaciones (como Telefónica en España, Telecom en Colombia), un proveedor de acceso a la información (como SIEMENS) y un proveedor de contenidos de la información (particulares o instituciones públicas o privadas. p.e. Universidades). En el punto, 5.5.5.2., volveremos sobre el tema y sobre la sentencia de la Corte.. *Sin embargo, adelantemos que hoy en día cualquier persona, puede enviar y recibir un E-Mail, como ayer (siglos atrás), lo hacía, a través de una carta escrita.* Las facilidades de comunicación electrónica a través de E-Mail, como de otros mecanismos de comunicación electrónica (v.gr. Los foros de debate --Newgroups--), han posibilitado un avance significativo y democrático de las comunicaciones a todo nivel y en cualquier sitio del planeta. Paradójicamente esa facilidad en el acceso, consulta y de disposición de equipos y aparatos informático aptos para la comunicación engendra un sinnúmero de formas violatorias de derechos humanos, los cuales plantean nuevos retos y soluciones para los juristas que deben empezar por comprender el fenómeno tecnológico TIC en matrimonio --si nos permiten-- con la informática. Sólo así podremos entender la conducta humana y las actividades de las personas que ya no utilizan una arma física, sino una especie de arma físico-lógica, como el ordenador o computador conectado, vía telefónica a través de un modem, un operador de telecomunicaciones con otro para cometer atentados contra los derechos fundamentales, patrimoniales o no patrimoniales. *El delito de finales del siglo XX y principios del siglo XXI, se caracteriza por la notable sutileza, muchas veces anónima, con que se utilizan los medios físico-lógicos (hardware y software) en la comisión de una conducta ilícita.* *Regresar*

(121) Vid.Nuestro trabajo, *La Constitución...* Ob. cit. pág. 7 y ss. En: http://akane.udenar.edu.co/derechopublico. Regresar

(122) Esto nos conduce a pensar que una "simple agenda informática de teléfonos es un fichero de datos de carácter personal, que debe ser notificado a la APD (se refiere a la "Agencia de Protección de Datos Española") antes de su uso, a cuyo fichero hay que dotar de sistemas de seguridad adecuados, con la obligación de informar al afectado de que integramos su teléfono a un fichero automatizado, etc " En otro lugar, con igual intención alude: "Debemos recabar un consentimiento escrito de nuestros clientes si precisamos tener datos sobre su ideología o creencias, salud o cuestiones relativas a la vida sexual, lo cual no es inusitado en nuestra profesión, en particular por parte de los abogados matrimonialistas o penalistas (art.7, núm. 2 y 3)". Cfr. JIMENEZ ESCOBAR, Raúl. ***Sobre la aplicación de la Ley orgánica 5 de 1992 a los ficheros automatizados de datos de carácter personal mantenidos por los abogados.*** En: Revista Jurídica de Cataluña No. 1, Barcelona, 1995, pág. 37 y 43. Regresar

(123) Vid. CASTELLS ARTECHE, José Manuel. ***Derecho a la privacidad y procesos informáticos: Análisis de la ley orgánica 5/1992, de 29 de octubre (LORTAD).*** En: Revista Vasca de administración pública. R.V.A.P. No. 39, Bilbao, 1994, pág. 268. Regresar

(124) Cfr. AA.VV. ***Banco de Datos. Biblioteca Virtual de la Univ. de Montreal Canadá*** *(versión en inglés y en francés).* WWW.UMONTREAL.EDU.CA. Ob. cit., 1998. Regresar

(125) Cfr. SECTION 6. Request for access to record. 6. A request for access to a record under this Act shall be made in writing to the government institution that has control of the record and shall provide sufficient detail to enable an experienced employee of the institution with a reasonable effort to identify the record. SECTION 7. Notice where access requested. 7. Where access to a record is requested under this Act, the head of the government institution to which the request is made shall, subject to sections 8, 9 and 11, within thirty days after the request is received, (a)_give written notice to the person who made the request as to whether or not access to the record or a part thereof will be given; and (b)_if access is to be given, give the person who made the request access to the record or part thereof. SECTION 19. Personal information. 19.1._Subject to

subsection (2), the head of a government institution shall refuse to disclose any record requested under this Act that contains personal information as defined in section 3 of the Privacy Act.- 19.2. Where disclosure authorized._The head of a government institution may disclose any record requested under this Act that contains personal information if (a)_the individual to whom it relates consents to the disclosure; (b)_the information is publicly available; or (c)_the disclosure is in accordance with section 8 of the Privacy Act. Ob.cit., 1998. Texto completo en WWW.UMONTREAL.EDU.CA. Regresar

(126) **Artículo 8. LPDIC.** *Descubrimiento (o divulgación) de la información personal*.8. (1) Una institución gubernamental bajo la cual está el control de una información personal no podrá descubrirla sin el consentimiento del concernido, salvo que se realice de conformidad con el presente artículo.(2) Cuándo se puede descubrir una información personal. (2) Sin perjuicio de lo estipulado en otras leyes, podrá descubrirse la información personal bajo el control de una institución gubernamental en los siguientes casos: a) cuando el propósito de la obtención o la compilación de la información lo determinó la institución; b) cuando se autoricen de conforme a las leyes federales o reglamentos vigentes; c) cuando sea exigido por una *citación*, orden o mandato de la corte, o cuando sea exigido por una persona u organismo con jurisdicción para compeler la producción de información , o con el propósito de cumplir un procedimiento sobre la producción de información personal ordenada por la Corte; d) cuando la información sea utilizada en procedimientos judiciales por parte del Abogado General del Canadá, en los que se vean involucrada en derecho, la Corona o el Gobierno del Canadá; e) cuando la información sea requerida por un organismo investigador del Estado y en la demanda escrita se ha precisado los propósitos del descubrimiento de la información y los fines de la investigación de conformidad con la leyes federales y provinciales; f) con el propósito de adelantar una investigación legal y en cumplimiento de un Acuerdo o Convenio entre el Gobierno y sus diversos organismos, una provincia, o entre éstos y un Estado Extranjero, o entre un organismo internacional del Estado y el Gobierno o sus organismos; g) por comunicación de un miembro del Parlamento con el propósito de ayudar a una persona a quien concierne la información a resolver un problema; h) por comunicación de la Oficina del Contralor General enviada a una persona o un organismo del Estado con el propósito de realizar una verificación del personal o auditoria contable interna; i) con propósito archivístico a los Archivos Nacionales de Canadá; j) por comunicación a cualquier persona o organismo, con los propósitos de investigación o fines estadísticos , siempre que se realicen cumpliendo estas dos condiciones: 1. que el responsable de la institución este convencido de los fines para los cuales se solicita la información y al proceder de esta forma permitirá que no se identifique al individuo concernido, y 2. obtener de la persona u organismo una constancia escrita de que no se hará ningún descubrimiento subsecuente de la información de forma tal que podría esperarse razonablemente se identifique a la persona concernida; k) por comunicación a una asociación de aborígenes, Banda indiana, institución gubernamental, parte de éstas, o su representante, con el propósito de investigar una solicitud, disputa o agravio contra las gentes aborígenes de Canadá; l) por comunicación a una institución gubernamental con el propósito de localizar a un deudor o acreedor de la Corona del Canadá para hacer efectivo el cobro o su pago; m) por comunicación del responsable de una institución gubernamental para cualquier otro propósito en cual se involucre: 1. el interés público sobre el particular que eventualmente justifique la invasión de la intimidad con el descubrimiento de una información personal, o 2. que el descubrimiento beneficie al concernido. Texto Completo en francés e inglés en : WWW.UMONTREAL.EDU.CA. Regresar

(127) SOUVIRON, José M. ***En torno a la jurisdicción del poder informativo del Estado y del control de datos por la administración***. En Revista Vasca de Administración Pública. R.V.A.P. No.40, Bilbao, 1994.pág. 152-154. Regresar

(128) LOPEZ DIAZ, Elvira. ***EL Derecho al honor y el derecho a la intimidad***. Ed. Dykinson, Madrid, 1996, pág. 243. Regresar

(129) ORTI VALLEJO, A. ***Derecho a la intimidad e informática.*** Ed. Comares, Granada, 1994, págs. 79 y ss. Regresar

(130) CASTELLS ARTECHE, José M**.** ***La limitación informática***. En: Estudios sobre la Constitución Española. Homenaje al profesor Eduardo García de Enterria. Ed. Civitas, Tomo II, Madrid, Tomo II, 1991.pág. 924. Regresar

(131) Ibídem..pág. 924. Regresar

(132) Véase, Artículo 8 de la Ley de protección a la intimidad Canadiense, antes transcrito. Regresar.

(133) MORALES PRATS. ***Comentarios...*** Ob.cit., pág.320. Regresar

(134) Ibídem., pág. 321. Regresar

INICIO