INFORME DE INVESTIGACIÓN CIJUL

TEMA: PROTECCIÓN DATOS PERSONALES Y BASES DE DATOS

RESUMEN: La presente recopilación de doctrina extranjera tiene como eje principal el desarrollo del tema de la protección de los datos en diferentes aspectos, como lo son el manejo de información de carácter público, la protección de información personal, y la responsabilidad de proveedores de servicios de internet entre otros temas relacionados.

Índice de contenido

1 DOCTRINA

a) Protección de Datos Personales contenidos en las Bases de Datos Informatizadas y no Informatizadas obrantes en el Poder Judicial Uruguayo

[BORTOLOTTO][1]

“No nos resulta posible comenzar el estudio del tema propuesto, sin recordar las enseñanzas de nuestro Maestro Prof. Dr. Horacio Cassinelli Muñoz acerca del principio de publicidad de la gestión administrativa imperante en el derecho positivo uruguayo. Y para ello, nada mejor que hacerlo con sus propias palabras.

En efecto, “el buen funcionamiento de la forma republicana de gobierno exige, entre otras cosas, la información del pueblo acerca de la gestión de los gobernantes. Ello es así porque el rasgo esencial de la república consiste en la calidad derivada del poder de los gobernantes: la opinión pública debe tener las vías de acceso a la gestión del gobierno, para que el control popular sobre los gobernantes sea una realidad efectiva”.

“Puede afirmarse, por ende, que el principio de la publicidad de la gestión administrativa deriva de la forma republicana de gobierno, lo que trae como consecuencia, en el orden jurídico uruguayo, que los derechos, deberes y garantías implícitos en aquel principio, resultan indirectamente consagrados por el Artículo 72 de la Constitución”.

Ante todo, dice, no debe olvidarse que la solución de principio es la publicidad, y que la reserva o secreto o cualquier restricción a ese principio requiere de un acto expreso de la autoridad competente, debiendo examinarse, en segundo lugar, la legitimidad de las restricciones a esa solución de principio, porque las restricciones a la publicidad deben atender a dos criterios: por un lado deben ser más débiles cuánto mayor sea el interés individual del que pide la información; y por el otro, deben ser más débiles cuánto mayor sea la responsabilidad del solicitante por el buen funcionamiento del ente administrativo requerido. Y en ambos casos, la restricción debe ser motivada en una razón que sea suficientemente importante como para compensar la razón genérica que aconseja la publicidad como resorte esencial del sistema republicano, sin olvidar que la restricción debe tener siempre un motivo legítimo, y derivar de un acto inspirado en alguna razón atendible.

Y refiriéndose al tema específico del interés requerido para obtener testimonio de las actuaciones administrativas, el insigne jurista enfoca dicha situación desde dos perspectivas: por un lado, haciendo hincapié en que de la forma republicana de gobierno deriva el principio de publicidad de la gestión administrativa, el cuál, dice, en el Derecho uruguayo, deriva de la disposición contenida en el Artículo 72 de la Constitución nacional, tal cual viene de expresarse. Y por el otro, advirtiendo que como no se trata sólo de la exhibición de una actuación administrativa sino de la expedición de un testimonio de la misma, lo cual implica una prestación de la Administración que insume energía, ha de hallarse cuál es la solución constitucional sobre los efectos de las peticiones presentadas ante la Administración.

En tal sentido, el Artículo 30 de la Constitución nacional, nos acuerda el derecho de petición a todos los habitantes de la República; ninguna Ley, pues, puede impedir que cualquier habitante formule una solicitud ante cualesquiera autoridad

nacional. Pero a su vez, si ese peticionante es titular de un interés legítimo en que se le expida el testimonio solicitado, la autoridad administrativa requerida se encuentra obligada a decidir sobre su petición, dentro de los términos establecidos en el Artículo 318 de la Constitución, que en lo que nos interesa dispone: “Toda autoridad administrativa está obligada a decidir sobre cualquier petición que le formule el titular de un interés legítimo en la ejecución de un determinado acto, y a resolver los recursos administrativos que se interpongan contra sus decisiones...”. Al ser la expedición de un testimonio de una actuación administrativa la ejecución de un determinado acto administrativo, precisamente, el de decidir sobre la expidición del testimonio solicitado, la solución constitucional resulta perfectamente aplicable a la situación que estamos analizando.

“Quien solicita testimonio manifiesta un interés prospectivo, esto es, que se satisfaría mediante un hecho futuro: la obtención del testimonio. Al hacer la solicitud, tiene la esperanza o la perspectiva de obtenerlo. Este interés puede estar protegido bajo la forma del derecho subjetivo, lo que significa que la Administración tendrá la correlativa obligación de expedirle el testimonio; o bajo la forma del interés condicionalmente protegido por el Derecho, en cuyo caso la Administración deberá expedírselo si no lo encuentra inconveniente; o bajo la forma del interés ocasionalmente protegido, hipótesis en la cual la Administración sólo expedirá el testimonio si conviene al interés público, pero nunca en atención al interés del peticionario. En el caso del derecho subjetivo, podría hacerse valer inclusive mediante acción judicial; en los otros dos casos, que son variantes del interés legítimo, la pretensión del peticionario a que se satisfaga su interés sólo puede hacerse valer a través de los Artículos 318 y 309 de la Constitución”.

En una línea de pensamiento que podríamos calificar de más moderna se ubica el Prof. Dr. Carlos E. Delpiazzo, para quien “cuando se habla de transparencia de la gestión administrativa, se quiere dar un paso más respecto a la publicidad ... como que la publicidad implica mostrar, pero la transparencia implica algo más que mostrar, implica dejar ver; simplemente que el actuar de la Administración se deje ver como a través de un cristal”.

Más allá de la publicidad, dice, “la transparencia refiere a la diafanidad del obrar público, permitiendo ver con claridad el actuar de la Administración en la disposición y uso de los fondos

públicos y en el obrar de sus funcionarios; constituye una consecuencia de la muy elemental presunción de que el gobierno pertenece al pueblo, quien tiene derecho a saber qué hacen los servidores públicos, por qué y cómo lo hacen".

"Se trata de subrayar cómo la sociedad quiere que sea la Administración de principios del siglo XXI: no sólo debe servir, sino que debe mostrar cómo sirve, lo cual exige que sea abierta a la información, a la participación y al control democrático, con un funcionamiento transparente que la transforme en una verdadera casa de cristal".

Citando a Jaime Rodríguez Arana, el Prof. Dr. Delpiazzo estima que la transparencia se asocia a lo que es visible y accesible, a lo que puede ser conocido y comprendido, por oposición a lo cerrado, misterioso, inaccesible o inexplicable. Igualmente, dice, la transparencia se asocia a una carga afectiva ligada a la tranquilidad y serenidad provocada por todo aquello que se domina y racionaliza, por oposición a la angustia y perturbación que provoca en el ser humano lo misterioso y desconocido. Además, prosigue, del contraste entre las sombras y la luz, entre opacidad y transparencia, nacen nuevos métodos que tratan de referir el principio de legalidad, como límite y fundamento de la acción administrativa, al principio de consecución del interés público y respeto por los derechos de los ciudadanos en el marco del bien común, métodos que tratan de promover los principios de colaboración ciudadana y de promoción de una nueva y diferente forma de concebir el poder administrativo más próximo a los ciudadanos.

Aunque a su juicio la operatividad de los principios generales del derecho no se encuentra condicionada a su explicitación por normas positivas dado que participan de la idea básica de principalidad en sentido ontológico, el Prof. Dr. Delpiazzo explica que el Derecho positivo uruguayo reciente exhibe una marcada tendencia a su enunciación a través de normas legales y reglamentarias, destacándose, en lo que refiere al principio de transparencia en el obrar público, su reconocimiento en el marco del ordenamiento positivo, para prevenir y reprimir la corrupción. Es así que el Artículo 7º de la Ley 17.060 de 23 de Diciembre de 1998 establece que "Los actos, documentos y demás elementos relativos a la función pública pueden ser divulgados libremente, salvo que por su naturaleza deban permanecer reservados o secretos o hayan sido declarados tales por Ley o resolución fundada. En todo caso, bajo

la responsabilidad a que hubiere lugar por Derecho".

A la luz de lo antes expresado, en el presente trabajo analizaremos la Acordada dictada por la Suprema Corte de Justicia de la República Oriental del Uruguay Nº 7564 de 21 de Febrero de 2006, mediante la cuál se dictan normas tendientes a la protección de los datos personales, asentados en los bancos o bases de datos de carácter documental o jurisprudencial en todos los ámbitos del Poder Judicial y cualquiera sea el soporte que los contenga - papel o magnético.

Analizaremos asimismo si ella se ajusta a las prescripciones del Artículo 7º de la Ley 17.060 transcripto, y si la "normativa en vigencia" a que refiere el numeral I) de su VISTOS Y CONSIDERANDOS es la Ley 17.838 de 29 de Setiembre de 2004 de protección de datos personales para ser utilizados en informes comerciales y acción de habeas data

2.- Ámbito de aplicación de la ley 17.838.

La Ley 17.838 se originó en el proyecto presentado por los Senadores Luis A. Heber y Alberto Brause el 6 de Mayo de 2003 [xxi]. Dicho proyecto se componía de seis Capítulos (Disposiciones Generales, Principios Generales, De los derechos de los titulares de datos, Del tratamiento de datos personales relativos a obligaciones de carácter comercial, Acción de protección de los datos personales o Hábeas Data, Órgano de Control y Disposiciones finales y transitorias respectivamente) y veinticuatro artículos.

En la Exposición de Motivos que acompañó al Proyecto, sus impulsores destacaron, en lo que nos interesa para determinar el ámbito de aplicación de la Ley, que "El Capítulo I que lleva como título "Disposiciones Generales" establece el objetivo preciso que pretende regular el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración y, en general, el tratamiento de datos personales asentados en archivos, registros, bases de datos u otros medios sean estos públicos o privados, destinados a brindar informes de carácter general. Se consagra, además, las excepciones no comprendidas en la Ley por carecer de carácter de información comercial".

Con fecha 9 de Setiembre de 2003, la Comisión de Constitución y Legislación de la Cámara de Senadores recibió al Director del Instituto de Derecho Informático de la Facultad de Derecho de la Universidad de la República, Prof. Dr. Carlos E. Delpiazzo quien, en lo que nos interesa expresó en la oportunidad que respecto del "proyecto de Ley, el Instituto ha señalado la importancia y la necesidad de que se legisle en este tema. No obstante, en las conclusiones de este informe, se señala el alcance limitado que tiene esta iniciativa, porque el mismo no refiere a todos los datos de carácter personal sino específicamente a los datos personales de carácter comercial". "Quizás la Ley, que tiene una estructura en capítulos, podría dividirse en dos grandes partes o en dos grandes títulos, y que se disciplinara lo que a la sensibilidad parlamentaria en este momento atiende, que es procurar un régimen para los datos personales de carácter comercial. En cambio, en el segundo título, la normativa que se ha redactado en materia de "hábeas data", quizás podría ser generalizada, no como referida específicamente a los datos de carácter comercial, sino como provisión de una acción específica, que sirva para la tutela de cualquier situación vinculada a los datos personales". "Por consiguiente, un primer aspecto que señalaría es la importancia y necesidad de regular y en todo caso, al hacerlo – aunque el objeto específico de la Ley a dictarse sea la protección de los datos personales de carácter comercial – determinar que la acción de "hábeas data" eventualmente pueda tener el más amplio alcance tuitivo y no referido o acotado exclusivamente a estos datos". "Un último aspecto a señalar, objeto de discusión en el Derecho Comparado, es el relativo al hecho de que no se dice nada sobre la posibilidad de los entrecruzamientos de información, aun cuando podría inferirse del texto del proyecto un sano criterio limitativo, en función de los principios que se consagran en el Capítulo II. Pero este es un tema sobre el cuál los convido a la reflexión, porque es de gran sensibilidad".

El Presidente de la Comisión de Constitución y Legislación de la Cámara de Senadores solicitó al Prof. Dr. Delpiazzo, en nombre de la misma y contando con la conformidad de todos sus integrantes, que contribuyera con el mejoramiento de la redacción del proyecto haciéndoles llegar las correcciones pertinentes, habiéndose comprometido éste a hacerlo, sobre todo en lo referente a la universalización del "hábeas data" como elemento tuitivo de todos los datos personales, así como una propuesta de rearmado del articulado del proyecto.

Las correcciones al proyecto versaron esencialmente [xxvii], y en lo que nos interesa, en dos puntos: (a) desde el punto de vista estructural, dividir el proyecto en 3 Títulos (lo cuál fue recogido por el texto legal, por lo que no merece ser desarrollado); y (b) desde el punto de vista del contenido del articulado, modificar los siguientes textos: el Artículo 1º comenzaría diciendo: "El presente Título tiene por objeto ...." (lo cuál fue recogido por el texto aprobado); el Artículo 2º diría: "Se exceptúan de este Título ...." (lo cuál no fue recogido por el texto aprobado); el Artículo 16 (que corresponde al Artículo 17 del texto aprobado) podría comenzar así: "El titular de todo dato personal, cualquiera fuera su objeto, podrá entablar ..." (lo cuál no fue recogido en el texto aprobado); en los numerales 1º y 2º del Artículo 16 (que corresponde al Artículo 17 del texto aprobado, como ya se expresó) deberían eliminarse las referencias a los Artículos 9º y 10º respectivamente (la remisión al Artículo 9º se mantuvo en el texto aprobado aunque debe advertirse que ella es errónea, pues la remisión debió haber sido hecha al Artículo 14, que es el Artículo que corresponde al Artículo 9º del proyecto; la remisión al Artículo 10 se eliminó del texto aprobado).

De lo antes expresado puede arribarse sin mayores hesitaciones, y sin forzar la interpretación conforme a derecho del texto legal, a la conclusión de que la Ley 17.838 solamente se aplica a los datos personales para ser utilizados en informes comerciales, y que la acción de hábeas data se encuentra referida solamente a dichos datos, ya que las sugerencias formuladas por el Instituto de Derecho Informático relativas a ampliar el alcance de dicha acción no fue tomada en cuenta por el legislador, tal cuál se acaba de exponer.

En efecto, el Artículo 2º de la citada norma establece claramente que "Se exceptúan de esta ley, el tratamiento de datos que no sean de carácter comercial", lo cuál, a nuestro juicio, exime de mayores comentarios y quita fundamento a las novedosas e ingeniosas argumentaciones que se han ensayado por una parte de la doctrina especializada de nuestro país, en el intento de incluir dentro de la protección de esta Ley a todo tipo de dato personal. Ello sin mencionar que la redacción del Artículo 16 del proyecto (hoy 17 de la Ley) se mantuvo incambiado, cuando el Instituto de Derecho Informático sugirió que para ampliar el alcance de la acción de "hábeas data" debía sustituirse la expresión utilizada

en el proyecto por la de “El titular de todo dato personal, cualquiera fuera su objeto, podrá entablar ...”, hecho que en definitiva no ocurrió.

En esta línea de pensamiento encontramos, por ejemplo, al Prof. Dr. Lorenzo Sánchez Carnelli, para quien la disposición del Artículo 2º de la Ley se refiere a toda la Ley y no al Título primero, quedando en consecuencia fuera de su protección los datos personales que no sean de carácter comercial; a la Dra. Anabella Aldaz, para quien “por expresa disposición de la Ley han quedado excluidos los datos personales no comerciales, cuando seguramente la norma pudo tener un alcance tuitivo más amplio y no restringido exclusivamente a datos de carácter comercial. De todas maneras la protección de los datos personales y la acción de “Hábeas Data” continuaría recibiendo amparo en el marco de los Artículos 72 y 332 de la Constitución”; al Prof. Dr. Walter Guerra Pérez, para quien “esta Ley que resultó definitivamente aprobada, como puede apreciarse, no alcanza a la protección de todos los datos personales por el uso que de ellos pueda realizarse en cualquier circunstancia, sino que está limitada a la protección de datos personales cuyo tratamiento tenga un destino comercial, tanto de personas físicas como jurídicas (Artículos 1º y 2º de la Ley)”; o a la Prof. Dra. María Balsa Cadenas, para quien la “legislación reciente reconoce el derecho de las personas a una acción sumaria para informarse, pedir rectificación, actualización y/o eliminación de sus datos personales tratados por las entidades financieras”.

En síntesis: nosotros adherimos a la posición de quienes sostienen que la Ley 17.838 protege solamente a los datos personales, tanto de personas físicas como de personas jurídicas, cuyo tratamiento tenga un destino comercial, por lo que entendemos que las bases de datos que resultan alcanzadas por sus disposiciones, y a la cuál deberán ajustar su funcionamiento, son aquellas que se dedican a brindar informes objetivos de carácter comercial, en la inteligencia de que la Ley 17.838 permite arribar solamente a tales conclusiones, si se la interpreta conforme a Derecho.

3.- Protección de los datos personales contenidos en bases de datos informatizadas.

Previo a abordar el estudio del tema propuesto vale precisar

algunos conceptos, a efectos de advertir al lector de la posición doctrinaria a la que adhiere la autora.

En primer lugar, aclarar por qué y para qué se instituyó el Hábeas Data. Su origen se explica en virtud del desarrollo del denominado "poder informático". Quienes "hacen" informática (el productor, el gestor y el distribuidor de datos), cuentan generalmente de protección constitucional (o legal) de su actividad en las normas que protegen la libertad de comerciar, de trabajar, propiedad, inviolabilidad de los papeles privados, entre otros. La situación no es la misma para los "registrados" en los archivos o bancos de datos, ya que éstos pueden contener información equivocada, antigua, falsa o con potenciales fines discriminatorios, o lesiva del derecho a la intimidad de las personas.

El "Hábeas Data" pretende dar una respuesta transaccional a los derechos constitucionales de "registrantes" y "registrados", y atiende tanto a las cuestiones de fondo (es decir, a los derechos de cada uno de ellos) como a las de forma (es decir, el tipo de procedimiento para asegurar tales derechos). Con relación la primera de las cuestiones, el Hábeas Data tiene cinco finalidades principales: (a) acceder al registro de datos; (b) añadir datos omitidos o actualizar los datos atrasados (por ejemplo, si una persona aparece como procesada y en realidad fue sobreseida); (c) corregir información inexacta; (d) asegurar la confidencialidad de cierta información legalmente recogida, pero que no debería ser proporcionada a terceros (como por ejemplo, los balances presentados por una corporación ante un organismo fiscal, pero que no deberían suministrarse a empresas rivales); (e) cancelar aquellos datos calificados como "sensibles" (ideas religiosas, políticas o gremiales, comportamiento sexual, etc) potencialmente discriminatoria o que "perfora" la privacidad del registrado. En cuánto a la segunda de las cuestiones, las diferentes Constituciones latinoamericanas, como por ejemplo la argentina, lo concibe como una variable de la acción de amparo.

Es decir, entonces, que el Hábeas Data no procede ante cualquier situación de acopio de datos ni tampoco para conocer, actualizar, rectificar o eliminar cualquier tipo de dato. Como bien lo expresa Badeni el propósito del Hábeas Data es evitar que mediante el uso de la informática se pueda lesionar el honor, la intimidad de las personas y sus restantes derechos como consecuencia de una información errónea o incompleta obrante en una base de datos (resaltado nuestro).

En la misma línea de pensamiento encontramos a Colautti, para quien el Hábeas Data es un instituto relativamente reciente, vinculado con el auge de la informática y es consecuencia de la multiplicación de los archivos de datos acerca de las personas. Se trata de una garantía que tiende a que todos los habitantes puedan acceder a las constancias de los archivos y a controlar su veracidad y difusión.

En síntesis, y aunque pequemos de reiterativos, el Hábeas Data no procede si la información contenida en un banco de datos no es ni errónea ni incompleta, por lo que, si la información es correcta y es completa, y fue acopiada en forma legítima, aún causando discriminación, esta garantía constitucional no resulta procedente. Es lo que sucede con los bancos de datos destinados a brindar informes de carácter comercial, respecto de los cuales el legislador ha reconocido como de rango superior al derecho a la privacidad de las personas, el derecho de la colectividad a conocer los antecedentes comerciales de los individuos en sus relaciones comerciales y patrimoniales con los restantes miembros de la sociedad.

En segundo lugar que, a nuestro jucio, el Hábeas Data procede para proteger los datos personales incluidos en bases de datos informatizadas, es decir aquellas que se encuentran en soporte electrónico o digital, por oposición a las documentales, que son las que se encuentran en soporte papel, en la inteligencia de que los datos por sí mismos no reflejan gran utilidad sino que es a a partir de su procesamiento (al adicionarlos, combinarlos, excluirlos y compararlos con otros datos) lo que nos proporciona un resultado, que es la “información”.

Como lo ha destacado en forma inmejorable el insigne Eduardo Cifuentes Muñoz, “los seres reales se disuelven en múltiples datos y así se observan sujetos que operan desde la penunbra con un instrumento formidable que torna visibles a los demás. La ausencia de regulación y de control a los usos de las técnicas informáticas, podría expandir ilimitadamente el dominio del Estado o de los sujetos que disponen de poder informático. La respuesta del Derecho, sin embargo, no se endereza a suprimir este nuevo factor de control social. El Hábeas Data representa apenas un intento incipiente y tímido, dirigido a corregir distorsiones extremas del proceso comunicativo informático. De un lado, reduce

en cierto grado la invisibilidad de los gestores o titulares de bancos de datos – lo que se logra exigiendo un registro de bancos, una declaración de sus objetivos y de sus procedimientos, etc.; del otro lado, permite a las personas, en cierta medida, adquirir consciencia de su transparencia externa y de las condiciones de la misma, pudiendo incidir en la elaboración y transmisión de formatos singulares o unidimensionales de su personalidad y de sus acciones. La diferencia entre información sensible y no sensible, resulta esencial para determinar la extensión y los límites de los poderes informáticos".

En el fondo, prosigue, el derecho legitima el poder informático. Si bien las regulaciones cumplen la función de "domesticar" este elemento de la modernidad, al mismo tiempo, implícitamente, no deja de reconocerle a la técnica el "despiece" del sujeto en una multiplicidad de datos. Así se recaba para la persona humana una victoria importante: la facultad de ser consciente de su sombra informática.

El Derecho no sale indemne de su confrontación con la técnica, dice. La regulación del Hábeas Data, positiva, en términos generales e indispensables, como forma de sujetar la técnica al Derecho, ha tenido de todas formas un precio para éste que ha consentido – o se ha visto compelido a hacerlo – y justificado el tipo particular de la antropología que asume la tecnología informática, para la cuál la persona humana se convierte en un mero dato o conjunto de datos esparcibles y transmisibles a través de sus canales y al tenor de sus pulsaciones. Al final, la regulación ha resultado funcional a la tecnología informática.

Por cierto que nada impide que el legislador, o el constituyente en su caso, extienda la garantía del Hábeas Data a la protección de los datos personales obrantes en bancos de datos no informatizados, aunque en realidad no alcanzamos a advertir la necesidad de hacerlo, pues resulta sumamente dificultoso ordenar sistemáticamente así como transmitir en tiempo real los datos obrantes en este tipo de bases de datos. Y ni qué decir de siquiera pensar en intentar interconectarlas, pues ello resulta materialmente imposible (sin pasarlas a formato electrónico, claro está). Son los bancos de datos informatizados los que amenazan los derechos de privacidad, intimidad, honor, etc., de las personas. Salvando las diferencias del caso, nos viene a la mente la comparación que hace Phil Zimmermann del correo convencional con el electrónico,: "en el pasado, si el Gobierno quería violar la

privacidad de los ciudadanos tenía que dedicar una cierta cantidad de esfuerzo para interceptar, abrir al vapor y leer el correo de papel. Esto es similar a pescar con una caña, un pez cada vez. Afortunadamente para la libertad, esta vigilancia que requiere tanto esfuerzo no es práctica a gran escala. Hoy en día, el e-mail está reemplazando al correo convencional y, a diferencia de éste, los mensajes electrónicos son facilísimos de interceptar y escudriñar buscando palabras clave. Esto se puede llevar a cabo de manera rutinaria, automática, indetectable y a gran escala. Es similar a la pesca con red de arrastre, lo que constituye una diferencia orwelliana para la salud de la democracia".

En ese mismo sentido encontramos a Francisco Cumplido Cereceda, para quien el problema fundamental surge en Chile como consecuencia del desarrollo tecnológico, porque cuando había solamente registros manuales, era muy difícil cruzar la información. Hoy día el desarrollo tecnológico es de tal magnitud, que se facilita cada vez más la relación de datos, y en consecuencia, los afectados se ven cada vez más expuestos al público en lo que es propiamente su vida privada.

En una posición distinta se ubica Miguel Heredero, para quien el tema central es el llamado derecho de acceso, que consiste en el derecho de toda persona a conocer los datos que hay registrados con relación a ella en un fichero dado. A su juicio, el nombre de derecho de acceso debe entenderse en el sentido de derecho a conocer los datos, pero no mediante el acceso automatizado a un soporte de datos, porque de lo contrario, este derecho se limitaría a los ficheros automatizados, e implicaría la exclusión de los ficheros de consulta manual o convencional.

Por los motivos precedentemente expuestos, nosotros no tenemos el honor de compartir tan autorizada opinión.

En tercer y último lugar, la evolución que se ha operado desde el antiguo "derecho a ser dejado solo" a la libertad informática y la diferencia entre vida privada e intimidad.

Respecto del primero de los aspectos antes señalados, Francisco Fernández Segado citando a Vittorio Frosini, entiende que al poder social informático se ha contrapuesto la "libertad informática". Esta ya no es el antiguo "right to privacy" como derecho a la

intimidad entendido como separación y defensa de la persona frente a la sociedad; es un nuevo derecho social de libertad; no es únicamente el derecho a negar la información sobre sí mismo, sino también el derecho a pretenderla. La libertad informática se perfila así como el derecho de disponer de la información, de preservar la propia identidad informática, es decir, de consentir, controlar y, en su caso, rectificar los datos informativos concernientes a la propia personalidad.

Concluye Fernández Segado que el “right to privacy” ha pasado a tener un contenido positivo, por medio del cuál se reconoce a cada persona el ejercicio de un control sobre el uso que pueda hacerse de sus propios datos personales recogidos en un archivo electrónico de un centro de proceso de datos. La libertad informática encierra así un derecho de autotutela de la propia identidad informática, cuya primera exigencia es la protección de los datos informáticos personales frente a aquellas personas no autorizadas para conocerlos, procesarlos modificarlos o difundirlos, razón por la que, el primero de los contenidos cuya normación viene exigida por la efectividad de la nueva libertad es el del acceso al banco de datos, con el fin de, por un lado poder disponer de toda la información almacenada en un archivo electrónico sobre la propia personalidad, y por otro, poder rectificar ciertos datos concernientes a la misma. Nace así, finaliza, la garantía conocida con el nombre de Hábeas Data

En cuánto al segundo de los aspectos señalados, nosotros adherimos a la posición de aquellos que sostienen que vida privada e intimidad no son sinónimos, sin dejar de reconocer que destacados especialistas en la materia los conciben como tal, negando toda diferencia jurídica y lingüística entre ellos.

Siguiendo a Carlos S. Nino, entonces, la privacidad comprende el ámbito de las acciones de los individuos que no afectan a terceros: pertenecen a una esfera personal y autorreferente. Son privadas aún cuando no haya limitaciones para el acceso público a su conocimiento. Por el contrario la intimidad es una esfera de la persona que está protegida del conocimiento del público y abarca la protección contra la violación de la correspondencia privada, la interceptación de las comunicaciones telefónicas, el allanamiento ilegal de domicilios, entre otros, derechos éstos protegidos por la Constitución uruguaya.

En esta misma línea de pensamiento se sitúa Alexy, quien concluye afirmando la existencia de un derecho fundamental abierto, conectado a la teoría de las esferas y de los derechos de libertad tácitos. El distingo de las esferas íntima, privada, amplia y social es problemática, señala. La esfera más interna o íntima tiene un mayor grado de protección, dado que los comportamientos del individuo no afectarían a la comunidad, resultado de una ponderación a favor de la libertad negativa y de la dignidad de la persona. En la esfera más amplia, la jurisprudencia subraya al respecto la regla de la proporcionalidad, que obliga a fundar las restricciones o intrusiones en la esfera privada.

Es por ello que coincidimos con Jaime Guerrero, en el sentido de que dentro de los derechos de la vida privada (que es el género) de las personas, toda normativa que se implante debe distinguir claramente dos aspectos: (a) un primer aspecto que dice relación con la esfera íntima de las personas, con su patrimonio moral y el campo de sus afectos, dentro de los cuáles se situarían los antecedentes relacionados con los principios religiosos o filosóficos; los referidos con ancestros étnicos o de familia (porque lo que para unos es motivo de orgullo, para otros lo es de sufrimiento); los referidos a la filiación natural o ilegítima; los que se refieran a enfermedades u operaciones quirúrgicas que una persona tenga o haya tenido; y, en general, todos aquellos antecedentes cuya divulgación causen dolor, aflicción o vergüenza; y (b) un segundo aspecto que dice relación con la privacidad de las personas, y es el referido a los antecedentes de carácter comercial que terceros pudieran estar interesados en conocer para mejor relacionarse social y económicamente. Esta es una información no íntima de la persona, en la que tiene un rol destacado la actividad económica, pues aún cuando la persona deseare mantener en absoluta reserva sus antecedentes económicos negativos, tiene un rango superior en la sociedad el derecho de los terceros a conocer esos antecedentes en sus relaciones comerciales o patrimoniales.

Así lo ha reconocido el legislador uruguayo en la Ley 17.838 antes mencionada.

4.- Protección de los datos personales contenidos en bases de datos informatizadas y no informatizadas obrantes en el poder judicial.

a.- Ubicación del tema.

Debemos comenzar por precisar que en el ordenamiento jurídico uruguayo, el proceso civil es público. Así lo edicta el Artículo 7º del Código General del Proceso, que establece "Publicidad del proceso.- Todo proceso será de conocimiento público, salvo que expresamente la ley disponga lo contrario o el tribunal así lo decida por razones de seguridad, de moral o en protección de la personalidad de alguna de las partes.

No serán de conocimiento público los procesos en que se traten las situaciones previstas en los Artículos 148 §, 187 © y 285 ª del Código Civil y en el Artículo 1º de la Ley Nº 10.674 de 20/11/1945 ·, modificado por el Artículo 1º de la Ley 12.486 ·· de 26/12/957, y por el Artículo 1º del Decreto Ley 14.759 ··· de 5/1/978. No obstante, el Tribunal podrá decidir la publicidad del proceso siempre que las partes consintieren en ello. (resaltado nuestro)." *

En el derecho español, por ejemplo, encontramos Artículo 232 de la Ley Orgánica 6/1985, de 1 de Julio, del Poder Judicial (B.O.E. núm. 157, de 2 de julio de 1985), actualizada por la Ley Orgánica 19/2003, vigente desde 30-12-2003, que establece que:

1. Las actuaciones judiciales serán públicas, con las excepciones que prevean las Leyes de procedimiento.

2. Excepcionalmente, por razones de orden público y de protección de los derechos y libertades, los jueces y tribunales, mediante resolución motivada, podrán limitar el ámbito de la publicidad y acordar el carácter secreto de todas o parte de las actuaciones. (resaltado nuestro).

En nuestro derecho pacíficamente se admite que toda norma que limite los derechos de los ciudadanos que se encuentran consagrados en la Constitución de la República debe ser

establecida por Ley, en el entendido de que es sólo el soberano, representado en el Parlamento, quien puede imponer ese tipo de acotamientos.

Por tal motivo entendemos que por ejemplo, el Artículo 7º de la Ley 17.060 ya citado, que establece que los actos, documentos y demás elementos relativos a la función pública pueden ser divulgados libremente, salvo que por su naturaleza deban permanecer reservados o secretos o hayan sido declarados tales por ley o resolución fundada (resaltado nuestro), sería de dudosa constitucionalidad, pues el derecho de todo ciudadano a acceder a los documentos en poder del Estado es un derecho que deriva de la forma republicana de gobierno, derecho que se encuentra reconocido implícitamente por nuestra Constitución (en el Artículo 72), y que es limitable (pues en nuestro ordenamiento jurídico ningún derecho o libertad es ilimitada, salvo el derecho a la vida) por Ley dictada por razones de interés general (Artículo 7º de la Constitución).

De modo tal que del otro extremo de la relación jurídica que tiene de un lado a una persona titular de un derecho subjetivo al acceso irrestricto de los documentos obrantes en poder del Estado, se encuentra otra persona (el Estado) sobre quien pesa la obligación de permitir ese acceso. Y que si no cumple con dicha obligación que la Constitución le impone, el titular de ese derecho subjetivo podrá, o mejor dicho puede, exigir judicialmente su cumplimiento, como por otra parte sucedió en nuestro medio con el sonado caso Alsina.

Coincidimos plenamente con Badeni quien, en conceptos trasladables a nuestro derecho, señala que “si bien resulta aceptable la tramitación reservada asignada a un expediente judicial, consideramos que no se puede vedar o mutilar la publicación de las sentencias sin ocasionarle lesión al principio de la publicidad de los actos gubernamentales, que es de esencia en un sistema republicano” de gobierno. “En nuestro sistema constitucional, el Poder Judicial integra el gobierno” nacional, “y todos sus actos – sentencias, acordadas, etc. – son actos gubernamentales sujetos a la regla de la publicidad que impone la forma republicana de gobierno. Cuando a través del ejercicio de la libertad de prensa se dan a publicidad los actos de gobierno, aquélla se proyecta a una dimensión institucional frente a la cual ceden las libertades individuales. Hay en el caso un interés público comprometido: el derecho del titular del poder político – el pueblo – por conocer

los actos oficiales de sus representantes en el ejercicio de ese poder", así como de controlarlos.

"Si la publicidad de los actos gubernamentales es una de las características esenciales del sistema republicano de gobierno, mal se puede prohibir o cercenar la publicación de las sentencias judiciales emanadas de los jueces, a quienes el soberano encomendó el ejercicio de la función de administrar justicia. Toda la legitimidad del sistema democrático está basada sobre la participación del pueblo en el proceso del poder, en su derecho a conocer los actos gubernamentales" y a efectuar el control sobre los mismos. "Ese derecho de acceso a las fuentes de información se expresa en todos los ámbitos gubernamentales, tanto frente a los actos de los órganos legislativo y ejecutivo, como los emanados del órgano judicial".

Concluye Badeni diciendo que la publicación de un fallo judicial, en las hipótesis en que pudiera generar un conflicto con el derecho a la intimidad, no opera un conflicto entre dos derechos individuales, sino entre uno de carácter individual y otro de raíz institucional: entre el derecho a la intimidad y el derecho de la sociedad a ser informada sobre el contenido de los actos gubernamentales que hace a la esencia misma del sistema político en el cual se desarrollan la totalidad de las libertades individuales.

En cuánto a nuestro derecho, corresponde precisar que el Código General del Proceso establece claramente quiénes son los únicos habilitados para conocer el estado de un procedimiento judicial en trámite, así como de las facultades que el Derecho les acuerda a las partes para autorizar a las personas que ellos deseen para interesarse del procedimiento en sus respectivos nombres, notificarse, recibir oficios, obtener testimonios y certificados, consultar y retirar los expedientes judiciales para su estudio.

Cabe precisar, además, que amparado en lo dispuesto por el Artículo 490 de la Ley 16.736, el Poder Judicial ha liberado, a los autorizados en expedientes judiciales que tramitan en Juzgados con gestión computarizada, la impresión del historial del expediente (hojas de trámite computarizadas), previo pago de un timbre especial por cada hoja. La información con que cuenta dicho historial incluye: subidas al despacho, decretos y su texto, notificaciones y demás movimientos del giro del expediente en la

Oficina del Juzgado.

Además, por Resolución 769/96/29 de la Suprema Corte de Justicia (comunicada a los Tribunales por Circular 82/96 de 28/10/996) se reiteró que la consulta de expedientes archivados no reviste ningún requisito formal, siendo suficiente el pedido verbal, no pudiendo el Juzgado exigir la presentación de escrito alguno, salvo que se desee reanudar el trámite.

b.- Análisis de la Acordada 7564.-

1.- En el numeral I) de sus Vistos y Considerandos la Corporación fundamenta el dictado de la Acordada en “la necesidad de adecuar la reglamentación referente al tratamiento de datos en el ámbito del Poder Judicial a la normativa vigente, a los avances tecnológicos y al estadio actual de la materia”.

De acuerdo a lo antes expuesto, surge evidente que la normativa vigente no puede ser la Ley 17.838, conforme al análisis efectuado en el punto 2 de este trabajo, por lo que estimamos que se estaría refiriendo a la protección que los Artículos 72 y 332 de la Constitución nacional acuerda a los datos personales, por ser inherentes a la persona humana.

2.- En el numeral II) de sus Vistos y Considerandos la Corporación entiende necesario buscar un equilibrio en la protección en el goce de los diversos derechos fundamentales reconocidos por la Constitución Nacional que resultan involucrados con motivo de la creación de bases de datos, en particular, el derecho a la información y la tutela del derecho a la intimidad.

En tal sentido, estimamos que los derechos en pugna no se limitarían a los señalados en la Acordada en estudio, pues en realidad colidirían el derecho que se le reconoce a todo habitante de la República de acceder a los documentos en poder del Estado, el derecho a la información (que, en principio, no es limitable, aunque por imperio del Artículo 29º de la Constitución al hacer referencia a la responsabilidad en que puede incurrirse por abuso de esa libertad, implica que hay limitaciones a esa libertad) y el derecho a la protección en el goce de la intimidad de las personas (que es limitable por razones de interés general, por

imperio del Artículo 7º de la Constitución).

3.- El Numeral 1º de la parte dispositiva dispone que la presente Acordada "tiene por objeto la protección integral de los datos personales –incluidos los sensibles- asentados en bancos o bases de datos de carácter documental o jurisprudencial en todos los ámbitos del Poder Judicial y cualquiera sea el soporte que los contenga – papel o magnético".

En primer lugar, corresponde destacar que la Acordada utiliza como sinónimos los bancos de datos "documental" y "jurisprudencial", porque de haber entendido que se trataba de bases de datos diferentes, debió haberlas definido. Ello obliga al intérprete a desentrañar el significado de los términos "documental" y "jurisprudencial", para averiguar si en realidad se tratan de la misma cosa.

Así, "documental" es un adjetivo cuyo significado es "que se funda en documentos, o se refiere a ellos". Y el término "jurisprudencial" es un término inexistente en la lengua española, siendo el más parecido que hemos encontrado el término "jurisprudencia", que tiene tres significados posibles: (a) Ciencia del derecho; (b) Conjunto de las sentencias de los tribunales, y doctrina que contienen; (c) Criterio sobre un problema jurídico establecido por una pluralidad de sentencias concordes. De estos tres significados, creemos que el que mejor se adecua al objeto de la Acordada en estudio es el contenido en el literal (b), o sea, "conjunto de las sentencias de los tribunales, y doctrina que contienen".

De todo lo cuál concluimos que al ser las sentencias de los Tribunales verdaderos "documentos", en el entendido de que se trata de escritos en los que constan datos fidedignos susceptibles de ser empleados como tales para probar algo, estimamos que la Acordada en cuestión se aplica a las bases de datos comprensivas de las sentencias de los Tribunales, cualquiera sea el soporte que las contenga – papel o magnético - .

4.- El Numeral 2º de la parte dispositiva dispone que "los datos que deberán ser protegidos mediante su ocultación son: (a) nombres y apellidos; (b) documento de identidad; (c) registro único de contribuyentes; (d) nacionalidad; (e) estado civil; (f) nombre del

o de la cónyuge; (g) régimen patrimonial del matrimonio; (h) fecha de nacimiento; (i) domicilio y teléfono; (j) profesión y ocupación y domicilio respectivo; (k) datos identificatorios de bienes inmuebles o muebles; (l) datos de partidas de nacimiento, matrimonio o defunción.

Corresponde destacar que si bien la Ley 17.838 no se aplica a la protección de los datos personales contenidos en este tipo de bases de datos, el Artículo 4º de la misma establece expresamente que "No requiere previo consentimiento el registro y posterior tratamiento de datos personales cuando: C) Se trate de listados cuyos datos se limiten a nombres y apellidos, documento de identidad o registro único de contribuyente, nacionalidad, estado civil, nombre del cónyuge, régimen patrimonial del matrimonio, fecha de nacimiento, domicilio y teléfono, ocupación o profesión y domicilio".

5.- El Numeral 3º de la parte dispositiva dispone que también serán suprimidos "salvo en aquellos casos en que se vinculen esencialmente a la cuestión litigiosa, los elementos que refieren a datos sensibles, a saber: (a) origen racial o étnico; (b) preferencias políticas; (c) convicciones religiosas, filosóficas o morales; (d) afiliación sindical, y (e) información referente a la salud o sexualidad.

Ahora bien. La Ley 17.838 sí resulta aplicable para el tratamiento de este tipo de datos, pues su Artículo 2º dispone que "Se exceptúan de esta ley, el tratamiento de datos que no sean de carácter comercial como por ejemplo: b) datos sensibles sobre la privacidad de las personas, entendiéndose por éstos, aquellos datos referentes al origen racial y étnico de las personas, así como sus preferencias políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o información referente a su salud física o a su sexualidad y toda otra zona reservada a la libertad individual. Para la obtención y tratamiento de datos que no sean de carácter comercial se requerirá expresa y previa conformidad de los titulares, luego de informados del fin y alcance del registro en cuestión".

Esta disposición de la Ley 17.838 entra en directa contradicción con las previsiones de la Acordada, pues ésta ordena suprimir datos que en realidad en sí mismos son inocuos (adquirirán relevancia si las bases de datos informatizadas se interconectan,

posibilidad respecto de la cual la Acordada guarda silencio), y en cambio permite mantener en sus bases de datos “datos sensibles”, siempre y cuando se “vinculen esencialmente” a la cuestión litigiosa, sin mencionar a cargo de quién estará dicha calificación, es decir, quién será la persona encargada de decidir que los datos sensibles se mantengan en la base de datos por vincularse esencialmente al proceso. Lo decidirá ¿el Juez competente?, ¿el operador de la base de datos? ¿la Directora de Jurisprudencia de la Suprema Corte de Justicia?, ¿la Directora de Jurisprudencia de los Tribunales de Apelaciones?, ¿el funcionario administrativo que ingresa los datos a la computadora?.

6.- El Numeral 4º de la parte dispositiva carece de importancia académica, por lo que iremos directamente al 5º, el cual dispone que la “protección resultante de esta Acordada comprende los datos referentes a las partes del proceso, terceros, testigos y toda otra persona que actúe en éste en calidad de auxiliar de la justicia”.

Resulta curioso que no se haya dispuesto la eliminación de aquellos datos que permitan identificar el Juzgado interviniente, los autos, el número de ficha así como el propio número de la sentencia, pues con esos simples datos cualquier persona podrá dirigirse al Juzgado y acceder a todo el expediente judicial (que se supone que ya está archivado), y obtener del mismo todos los datos personales que la Acordada busca proteger.

7.- El Numeral 6º de la parte dispositiva establece de qué modo se sustituirán los datos personales que deberán omitirse, mientras que el 7º establece que en “las dependencias del Poder Judicial en que existan bases o bancos de datos deberá guardarse un respaldo con el texto de la sentencia o documento original en soporte magnético, para uso interno”.

No surge de la Acordada a qué efectos se debe guardar un respaldo del texto de la sentencia original en soporte magnético para uso interno, ya que resulta más importante respaldar el expediente judicial que la sentencia, la cuál se releva por parte de los operadores jurídicos con fines generalmente académicos, de investigación, para su simple estudio o, inclusive para su publicación en Anuarios o manuales de estudio.

En todo caso nos parece una previsión discriminatoria, pues todos los habitantes de la República tenemos el derecho de acceder a la sentencia o documento original, ya sea en formato digital o en soporte papel.

8.- Es recién en el Numeral 8º de la parte dispositiva donde se hace referencia a otro tipo de bases de datos diferentes de aquellas que contienen sentencias. En efecto, el numeral en cuestión luego de disponer que a partir de la fecha de entrada en vigor de la presente Acordada la protección de los datos personales se aplicará a todas las materias, establece que los datos personales ya existentes en las bases o bancos de datos jurisprudenciales o administrativos deberán ajustarse a ésta dentro de determinado plazo.

En primer término, debemos señalar que la Acordada no define ni establece qué entiende por bancos de datos administrativos. ¿Se trata de los bancos de datos donde constan los datos personales de los funcionarios del Poder Judicial? ¿O en los que constan los gastos del Poder Judicial? ¿O en los que constan las compras del Poder Judicial? ¿O en los que constan los llamados a licitación del Poder Judicial? ¿O en los que constan las sanciones impuestas a cada funcionario del Poder Judicial? ¿O en los que constan los días de licencia que cada funcionario del Poder Judicial ha gozado a lo largo de su vida funcional?

La referencia a los bancos de datos administrativos nos parece sumamente excesiva, ya que si bien entendemos que la Corporación carece de facultades para limitar el acceso de los ciudadanos a los documentos que nos ilustran acerca de cómo funciona el servicio de justicia, es decir, de cómo el Estado imparte justicia, como sin duda lo son las sentencias que los Magistrados han dictado en los pleitos en los que les ha tocado intervenir, en el caso de los archivos pertenecientes a la Administración su ausencia de facultades nos parece indubitable.

Por otra parte, no logramos advertir cuál es el fundamento para adoptar este tipo de medidas que tienden a la protección a ultranza de los datos personales, sin advertir que por el camino quedan derechos fundamentales que tienen su fuente en la existencia misma de nuestra sociedad como Nación.

5.- CONCLUSIONES.-

1.- El ámbito de aplicación de la Acordada 7564 se circunscribe a las bases de datos comprensivas de las sentencias judiciales de los Tribunales, cualquiera sea el soporte que las contenga – papel o magnético.

2.- La misma contraría el derecho subjetivo que la Constitución acuerda a todo habitante de la República, de acceder a la documentación obrante en poder del Estado en su versión original, sin mutilaciones, como una forma de ejercer el control ciudadano que emerge naturalmente de la forma republicana de gobierno.

3.- El derecho a la protección de los datos personales y a la autodeterminación informativa en nuestro derecho, encuentra protección en el marco los Artículos 72 y 332 de la Constitución de la República, ya que el objeto de la Ley 17.838 es regular el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración, y en general, el tratamiento de datos personales asentados en archivos, registros, bases de datos, u otros medios similares autorizados, sean éstos públicos o privados, destinados a brindar informes objetivos de carácter comercial.

4.- Las bases de datos que contienen sentencias judiciales, por lo general, no contienen información errónea o inexacta, ni son susceptibles de causar discriminación en el sentido definido por Sagués, ya que imperan en ellas los valores de verdad y de justicia, fin último del Derecho.

5.- El derecho a la privacidad (o intimidad, según otros autores) de las personas es un derecho limitable.

6.- A nuestro juicio, el derecho a la autodeterminación informativa no puede ejercerse respecto de cualquier tipo de datos ni de cualquier clase de base de datos. En el caso de las de sentencias judiciales, mantener los datos personales de los justiciables resulta de especial importancia para los ciudadanos, pues solamente así se podrá saber si tanto la persona públicamente conocida como la desconocida reciben el mismo tratamiento por parte de la justicia. Es, por otra parte, lo que hoy sucede con el

Tribunal Constitucional Español, el cual publica las sentencias que dicta en su página web, sin suprimir los datos personales de los justiciables ni los Abogados que los patrocinan.

7.- La publicidad y la transparencia en la gestión pública son un postulado básico del Estado del siglo XXI. Ningún derecho individual puede cercenar el derecho de la sociedad a conocer lo que el Estado hace (publicidad) mientras lo está haciendo (transparencia).

8.- Por último y por una simple razón de honestidad, nos resulta ineludible precisar que los actos administrativos, en la casi totalidad de los casos, no son redactados por quienes los suscriben, sino que son elaborados por quienes se desempeñan como Asesores en sus respectivas especialidades.

Muchas veces, la excesiva especialización de éstos lejos de permitirles "mirar" o "percibir" al Derecho como una unidad, los hace verlo como una disciplina científica compartimentada.

Nada más alejado de la realidad."

b) Privacidad de la Información Personal y su Protección Legal en Estados Unidos

[PUENTE DE LA MORA][2]

I. Introducción

"Vivimos en un mundo caracterizado por la tecnología y la información. Avances tecnológicos como el teléfono, video, audio, computadoras y por supuesto, el Internet han revolucionado nuestra capacidad de percibir información del mundo y también la manera de comunicarnos con los demás. La información entonces se ha convertido en la "parte vital de nuestra sociedad". Día con día aumentan nuestras actividades que involucran la transferencia y grabación de la información; por una parte, el gobierno recolecta

una gran cantidad de información personal relacionada con el nacimiento, matrimonio, divorcio, propiedad, procedimientos judiciales, actividades políticas, licencias profesionales, entre otros asuntos que involucran la acción de alguna autoridad gubernamental; y por el otro, el sector privado posee gigantescas bases de datos personales para propósitos de mercadeo o de la elaboración de registros relacionados con el historial crediticio. A donde quiera que vamos o lo que sea que hagamos vamos dejando una estela de datos que pueden ser recolectados y grabados para una utilización diferente al fin con el que fueron proporcionados, a veces de manera voluntaria o involuntaria.

La privacidad de la información se refiere a la recolección, uso y revelación de la información personal, Daniel J. Solove se pronuncia por una diferenciación entre lo que denomina "«decisión personal» relativa a la libertad de tomar decisiones sobre el físico propio y la familia. Las «decisiones privadas» las cuales se vinculan a la libre decisión sobre procreación, contracepción, y cuidado infantil", como podemos observar no son muy claras las fronteras entre estos tipos de decisiones, es aquí donde la Corte Suprema ha jugado un papel muy importante porque ha ayudado a aclarar a través de sus resoluciones. Sin embargo, la privacidad de la información ha incrementado la incorporación de elementos de las denominadas "decisiones privadas" tales como el uso de los datos que expanden los límites de la autonomía individual.

A diferencia de las tendencias europeas que se observa respecto a la intimidad informática o protección de datos personales, en Estados Unidos se ha seguido un camino diferente a través del desarrollo del concepto de "privacy" en cual se aplica a varias vertientes del derecho: privacidad genética, privacidad en las conversaciones de un psicoterapeuta y su paciente, privacidad en la información médica, privacidad en las asociaciones, privacidad en el hogar, en la escuela, en el trabajo, etc. siendo la protección de datos personales un concepto que se protege a través de la privacidad aplicada a los registros y bases de datos electrónicas.

El derecho a la privacidad (Information privacy law) es un tejido interrelacionado de ilícitos civiles (tort law), derecho constitucional federal, derecho constitucional estatal, derecho codificado federal y estatal, información privilegiada, derecho de la propiedad, derecho contractual y derecho penal (criminal law), a pesar que es un derecho relativamente nuevo, sus raíces se

remontan a la antigüedad. La importancia del estudio del derecho a la privacidad radica en que es de vital importancia para la libertad y democracia en un Estado.

II. Orígenes del derecho a la privacidad. raíces del derecho anglosajón (common law)

Al terminar el siglo XIX preocupaciones considerables a cerca de la privacidad capturaron la atención pública, dando como resultado la publicación de Samuel Warren y Louis Brandeis con el artículo titulado The Right to Privacy el cual revolucionó el sentido de privacidad que se tenía en aquella época y que ha sido retomado en numerosas decisiones de la Corte Suprema en Estados Unidos.

Debemos recordar que a finales del s. XIX se produjo un cambio radical en la circulación de información, lo que originó un incremento en la producción de algunos medios impresos, además de que se fue creando en la población la necesidad de poseer información actualizada. Como ejemplo podemos mencionar que “entre 1850 y 1890 la circulación de periódicos se había incrementado casi 1,000% –de 100 ejemplares con 800,000 lectores a 900 ejemplares con más de 900,000 millones de lectores–“, además de que en ciertas ocasiones el periodismo sensacionalista se convertía en el paradigma del periodismo amarillista. El incremento de la prensa escrita y los avances tecnológicos de la época causaron gran alarma acerca de la invasión a la privacidad, la cual refleja el artículo de Warren y Brandeis al mencionar la invención de la “fotografía instantánea” como nuevo reto para preservar precisamente este reducto privado de las personas.

Warren y Brandeis se vieron fuertemente influenciados por un artículo escrito también en 1890 por E. L. Godkin un famoso comentarista social de la época, el cual mencionaba: “la privacidad es un producto moderno, un de los lujos de la civilización, el cual no solo pasaba desapercibido, sino que era desconocido en las sociedades primitivas... el principal enemigo de la privacidad en la vida moderna es el interés de la gente de conocer los asuntos personales que en días después los periódicos divulgaran como chisme...”, agrega Godkin además que “mientras que la comunicación fue solamente oral se divulgaban los hechos únicamente de persona a persona, sobre un área pequeña y eran divulgados solamente en el círculo inmediato de conocidos...

mientras que ahora la comunicación a cerca de la privacidad es impresa, y fabrica una víctima con todos los defectos, mismos que son conocidos cientos de miles de millas de su lugar de origen, llevando la información con todos los detalles de una persona".

Resulta interesante pues advertir que este artículo que data de 1890 advierte el cambio de pautas de información, pero también de necesidad y cierta curiosidad de la gente por conocer cada vez más detalles de la vida privada de las personas, esta divulgación facilitada también por el acelerado incremento de la producción de instrumentos de comunicación como el periódico.

En la elaboración del célebre artículo titulado The Right to Privacy, publicado en The Harvard Law Review también en 1890, Warren y Brandeis citan el artículo de Godkin, presentando además gran similitud en sus razonamientos. No obstante esta semejanza en algunos aspectos, defieren en un punto importante; mientras Godkin se pronuncia porque la solución al problema que presenta la protección de la privacidad de los individuos solamente en la esperanza de que cambie la actitud de la gente al respecto, Warren y Brandeis fieles a su formación como abogados, tienen una concepción diferente, puesto que ellos afirmaron que se podía proteger la privacidad mediante la ley.

Este artículo con el tema central del derecho a la privacidad, se centraba en afirmar que cada individuo debe tener una protección completa en su persona y en su propiedad como un viejo principio del derecho común, pero este derecho tiene que estar en continua redefinición para fijar los límites de su protección, puesto que por ejemplo al principio el derecho de propiedad de un individuo aseguraba sus tierras y su ganado, pero más tarde vino un reconocimiento de la naturaleza individual de la persona, a sus sentimientos y a su intelecto, "gradualmente el ámbito de esos derechos legales se fue extendiendo y ahora el derecho a la vida significa el derecho a disfrutar de la misma, el derecho a ser dejado solo, el derecho a asegurar la libertad individual incluyendo los privilegios civiles, haciendo que el derecho a la propiedad como tal, se extienda para abarcar todas las formas de posesión tanto tangibles como intangibles...". Es decir, Warren y Brandeis se pronuncian por asegurar como parte del derecho mismo de la personalidad el derecho "a ser dejado solo", esta es una de las principales contribuciones de este artículo.

En este artículo en mención, se afirma que los derechos se deben de proteger atendiendo a su naturaleza, no solamente los derivados de un contrato o de un acuerdo especial, sino que existen ciertos derechos que no pueden ser englobados dentro del principio de la propiedad privada. El principio que se debe de aplicar las aspiraciones individuales, las emociones y otros productos del intelecto humano es el derecho a la privacidad. Warren y Brandeis reconocen también que la línea que separa la dignidad personal y la conveniencia de la protección de los derechos personales, no es fácil de definir puesto que tiene que beneficiar al mismo tiempo las demandas del estado de bienestar y al mismo tiempo aspirar a alcanzar la justicia.

Estos autores norteamericanos tuvieron la precaución de describir a la privacidad no como un derecho absoluto, mencionando seis limitaciones:

1.El derecho a la privacidad no prohíbe las publicaciones de aspectos que son de interés público o general.

2.El derecho a la privacidad no prohíbe la comunicación de algún tema, basada en su naturaleza privada, cuando la publicación se realice bajo circunstancias que pudieran representar un privilegio.

3.El derecho probablemente no garantice algún tipo de reparación por la invasión a la privacidad por publicaciones orales en ausencia de un daño especial (puesto que los daños causados por las comunicaciones orales se consideran insignificantes para el derecho).

4.El derecho a la privacidad se suspende en caso de que la publicación de los hechos se realice por el propio individuo o con su consentimiento.

5.La verdad sobre el contenido de lo publicado no significa una defensa (puesto que lo que se protege es el hecho de la divulgación, más no la verdad o falsedad de los hechos).

6.La ausencia de “malicia”en la publicación no representa una defensa.

Finalmente, Warren y Brandeis señalan que el remedio por la invasión a la privacidad se encuentran en la acción de ilícito civil (action of tort) para todos los casos, incluso en la ausencia de daños especiales; y las medidas precautorias

(injunctions) para un número limitado de casos.

III. El desarrollo de la protección de la privacidad en el derecho común (common law)

El ámbito del derecho a la privacidad en el Common Law es muy amplio, se basa en distintas clases de figuras jurídicas las cuales tienden a proteger alguna parte relacionada con este derecho. A continuación mencionaremos algunos aspectos de éstas a fin de esquematizar el amplio alcance que puede tener el derecho a la privacidad:

Ilícitos civiles. Como antecedente histórico, el artículo de Warren y Brandeis dejó una profunda influencia en el desarrollo del derecho a la privacidad. En el comienzo de 1900s, las cortes y legislaturas reaccionaron a la publicación de este artículo mediante el reconocimiento del derecho a la privacidad en la resolución de casos y en el derecho codificado. En 1960 William Prosser catalogó cientos de casos judiciales decididos desde la publicación señalada, y concluyó que había cuatro clases de ilícitos civiles:

1.La divulgación de hechos privados. Este ilícito civil crea una causal de acción para quien hace público un hecho privado el cual es “altamente ofensivo para una persona razonable y no es legítimamente concerniente al público”.

2.Intrusión al ámbito de intimidad individual. Este ilícito proviene el remedio cuando existe una intrusión a la voluntad del individuo de permanecer aislado respecto a sus asuntos o relaciones personales.

3.Falsas revelaciones. Este ilícito crea la causa de la acción cuando la publicidad hace una falsa revelación respecto a un hecho que le sucede a una persona, mismo que sea altamente ofensivo.

4.Apropiación. Este ilícito civil protege a la persona en contra de la cual se apropia como suyo del nombre o imagen del demandante.

Difamación. La figura de la difamación existe mucho antes del artículo de Warren y Brandeis, la cual consiste en un ilícito civil con la característica de crear responsabilidad cuando alguien hace una declaración falsa sobre una persona, la cual afecta su reputación.

Para crear responsabilidad por difamación deberán de cumplirse los siguientes requisitos: “a. una declaración falsa e injuriosa respecto a otro; b. La publicación de información no privilegiada a un tercero (es decir, la publicación de la información que no se tenga que guardar en secreto como la del abogado con su cliente, el psicoanalista con su paciente por mencionar algunos casos); c. conducta culposa en grado de negligencia por parte del editor; d. La existencia ya sea de la acción derivada de la declaración irrespetuosa que cauce daño especial; o la existencia de un daño especial causado por la publicación”.

Una declaración difamatoria “tiende a dañar la reputación de otro, aminorar la valoración que le tenga la comunidad, o impedir que terceros se asocien o traten con él”.

Imposición de un peligro emocional. Este ilícito sobre la imposición intencional de un peligro emocional puede también servir de remedio para los casos en los cuales se comente una conducta extrema y excesiva que de manera intencional o imprudente, causa una afectación emocional a otro. Desde que las invasiones a la privacidad pueden resultar en ocasiones causantes de un peligro emocional, este ilícito provee un remedio, pero es necesario que exista una “conducta extrema y excesiva”.

Información privilegiada. En el derecho común, ciertas comunicaciones son privilegiadas, por lo tanto no podrán ser requeridas durante los procesos legales. Este derecho reconoce la importancia de proteger la privacidad de ciertas comunicaciones tales como las sostenidas entre el abogado y el cliente, entre el sacerdote y el penitente, el esposo y la esposa, el psicólogo y su paciente, etc.

La información privilegiada “confiere al individuo el derecho a rehusar a testificar o revelar información a cerca de ciertos

temas o prevenir que esto le suceda a otro". Este tipo de protección se aplica a casi todos los procedimientos gubernamentales, especialmente los procesos judiciales. Podemos mencionar como ejemplo de esta información privilegiada cuando un cliente le comenta a su abogado información confidencial inculpatoria y como el privilegio protege la confidencialidad de la información abogado-cliente, el abogado no puede ser forzado a testificar revelando esta información.

En el caso Upjonh Co. v. United States la Corte Suprema reconoce que "el privilegio abogado-cliente es el más antiguo respecto a la comunicación confidencial. Su propósito es por lo tanto, alentar la comunicación completa y franca entre el abogado y sus clientes, y la ampliación de los intereses públicos y la observancia de la ley y la administración de justicia... es decir, alentar a los clientes a hacer una declaración completa a sus abogados...".

Derechos de propiedad. Aunque existen algunos derechos de propiedad que específicamente regulan la privacidad, estos derechos frecuentemente implican privacidad. Es decir, el derecho de apropiación es parecido al derecho de propiedad, y algunas posiciones sugieren que el derecho a la privacidad informática debe ser visto como una forma de propiedad. Debemos señalar que Warren y Brandeis señalaron en su artículo que el derecho a la propiedad no era una forma adecuada para proteger la privacidad.

Derecho contractual. Las especificaciones contractuales en ocasiones protegen contra la recolección, uso o divulgación de la información personal. En ocasiones las cortes conocen de acciones por incumplimiento de contrato, las cuales han sido establecidas como análogas de las relaciones fiduciarias. Resulta importante señalar que las políticas de privacidad así como los términos de la prestación de un servicio contienen provisiones de privacidad que pueden ser análogas con disposiciones contractuales.

Algunos tratadistas establecen la protección contractual de la privacidad, como Jerry Kang que sugiere "la estipulación de una regla contractual que limite la forma en la que pueda ser usada la información personal, siempre y cuando las partes estén de acuerdo es los términos de la misma".

Derecho penal. La privacidad es protegida también mediante el

derecho penal (criminal law), el cual establece principios generales de responsabilidad penal protege invasiones corporales tales como el asalto y el robo. La privacidad de un hogar está protegida también mediante el derecho criminal para quién la transgreda. La figura del chantaje por ejemplo, protege la coacción de un individuo a otro que pretenda revelar sus secretos personales. Muchos de los estatutos para proteger la privacidad contienen penalidades dentro del derecho penal, como los estatutos pertenecientes a los dispositivos para interceptar e identificar la información, tal como la Federal Communicatios Act promulgada por el Congreso de los Estados Unidos en 1934, cuya sección 605 establece que “ninguna persona podrá ser autorizada a interceptar información de cualquier tipo y divulgarla o publicar su existencia, contenido, sustancia, propósito, efecto o significado de esta información interceptada a otra persona”.

Sin embargo, la mencionada sección 605 de esta Ley Federal de Comunicaciones no prevé expresamente una regla exclusiva, la Corte Suprema se pronunció al respecto en el caso Nardone v. United States en donde sostuvo que “los funcionarios federales no podrán introducir evidencia obtenida por la interceptación ilegal en una corte federal”.

IV. Orígenes de la privacidad en el derecho constitucional

Debemos de iniciar este apartado sobre el derecho constitucional estadounidense mencionando que se trata de la interpretación del modo en que se debe aplicar la Constitución de Estados Unidos de América, la cual fue redactada en 1787. Este instrumento normativo “contiene menos de 4,400 palabras, divididas en siete partes llamadas artículos. En 1791 se le añadió la Carta de Derechos (Bill of Rights) las 10 primeras enmiendas, fecha desde la cual, hace más de dos siglos, sólo se han agregado 17 más”.

Para muchos la Constitución Norteamericana de 1787 es la obra de iluminados intelectuales, para otros la Constitución es mejor entendida como una serie de compromisos ad hoc diseñados para resolver asuntos muy específicos sobre los cuales la joven nación estaba dividida. Para ello, hay que entender el contexto histórico, la Declaración de Independencia fue firmada en 1776, pero la Revolución Norteamericana formalmente finalizó en 1783, con la firma del tratado de paz con Inglaterra, habiendo cesado

las hostilidades en 1781, año en que las 13 Colonias ratificaron los artículos de la Confederación bajo los cuales reglamentaron su vida soberana por 7 años, posteriormente, la Constitución Norteamericana fue escrita en 1787 y ratificada un año después. Dos años más tarde de su ratificación fue adoptada la Carta de Derechos (Bill of Rights).

Con un sentido pragmático los artículos de la Confederación fueron adoptados con el propósito de buscar la unión de los Estados para resolver algunos problemas, pero cada Estados reteniendo su soberanía, libertad e independencia. En Confederación no fue previsto un poder ejecutivo, ni judicial, tampoco el Congreso tenía el poder para imponer impuestos o regular el comercio, sólo se limitaba al poder para “declarar la guerra, resolver disputas entre Estados, acuñación de moneda, establecer oficinas postales, lidiar con asuntos de las tribus indígenas”.

Por tanto, la Constitución Norteamericana pretendía establecer un poder central fuerte y duradero, pero no tanto en forma tal que diluyera la autonomía de los Estados Federados, por lo que se diseñó un sistema de pesos y contrapesos para ordenar y regular el poder público dividido en tres ramas del gobierno. El poder judicial federal tiene la importante misión de vigilar que todos los actos de autoridad se ajusten a la Constitución, situación que en los primeros años de la Constitución era difícil de realizar, y que sólo adquirió plena vigencia hasta 1803, fecha en que la Suprema Corte decidió el importante caso Marbury v. Madison, donde a propósito de una disputa entre el poder ejecutivo y legislativo la Suprema Corte de los Estados Unidos aprovechó para delinear una serie de principios básicos que establecían en forma indubitable la supremacía de la Constitución sobre cualquier ley general de la Unión.

Como podemos ver, la Constitución estadounidense posee características particulares respecto a otros textos normativos utilizados en otras tradiciones jurídicas, por lo que es importante señalar que en esta área de derecho constitucional de acuerdo con Jay Feinman, en Estados Unidos se distinguen cuatro características principales:

Primera. El primero de estos aspectos es que todas las demás ramas del derecho estadounidense operan en conjunto, puesto que define la estructura y funcionamiento del gobierno y las relaciones entre

éste y los ciudadanos, así mismo se encarga de definir las facultades relativas a los gobiernos federal y estatales, prohibiendo también la realización de ciertas acciones como la prohibición de violar la libertad de culto. La Constitución se proclama a sí misma como la ley suprema de la nación, de esta manera, toda ley estatal o federal de cualquier tema –contratos, sanciones penales, donativos electorales o escuelas públicas– pierde validez si contradice la constitución.

Segunda. El segundo aspecto se refiere a que las demás ramas del derecho se basan tanto en leyes como en fallos judiciales, lo que les aporta una extensa variedad de fuentes, reglas principios y argumentos; sin embargo cuando se trata de decisiones de índole constitucional se remite en definitiva a una sola fuente el texto de la Constitución y sus enmiendas.

Tercera. Otro aspecto que particulariza al derecho constitucional con las demás ramas del derecho es que plantea cuestiones políticas y decisiones de valores fundamentales.

Cuarta. El cuarto aspecto es que los procedimientos para la elaboración y aplicación de las leyes y reglamentos parecen obvios y aptos, puesto que derivan de la Constitución. Las legislaturas y las cortes formulan principios jurídicos mismos que aplican las propias cortes para resolver casos particulares.

Aunque la Constitución de Estados Unidos no menciona específicamente el derecho a la privacidad, existen algunas disposiciones que protegen la privacidad o que han sido interpretadas por la Corte Suprema como protectoras del derecho a la privacidad, entre estas disposiciones se encuentran las siguientes:

La primera enmienda Constitucional. En algunos casos la primera enmienda sirve para salvaguardar algunos aspectos de la privacidad, tales como “hablar en forma anónima”, también protege a los individuos de ser obligados de revelar los grupos a los cuales pertenecen o contribuyan.

La tercera enmienda Constitucional protege la privacidad del hogar mediante la prevención de no requerir que los soldados residan en

casas de particulares al establecer que “ningún soldado puede, en tiempo de paz, ser acuartelado en alguna casa, sin el consentimiento del dueño, no en tiempo de guerra, pero de acuerdo a lo prescrito por la ley”.

La cuarta enmienda Constitucional prevé el derecho de la gente sobre su persona, casa, papeles y pertenencias sobre registros excesivos y embargos. Casi cuarenta años después de escribir The Right to Privacy, Brandeis como Ministro de la Corte Suprema de Justicia, escribió un voto disidente el cual fue una significativa influencia para la interpretación de la cuarta enmienda constitucional. En el caso Olmstead v. United States, en donde la Corte sostuvo que la interceptación no constituía una invasión de la privacidad bajo la cuarta enmienda, porque no era un traspaso físico a una vivienda, el juez Brandeis disintió señalando que el interés central de esta cuarta enmienda no era proteger la propiedad sino el “derecho a ser dejado solo”, al señalar que el ámbito de protección garantizada por esta cuarta enmienda es más amplio, al señalar que los autores de la Constitución (norteamericana) se encargaron de asegurar condiciones favorables para alcanzar la felicidad, al reconocer el significado de la naturaleza espiritual del hombre, sus sentimientos y su intelecto. Brandeis hizo hincapié en señalar que ellos mismos sabían que solo una parte del dolor, placer y satisfacciones de la vida era alcanzadas mediante cosas materiales; sin embargo anhelaban proteger las creencias de los americanos, sus pensamientos y emociones.

En este voto de disentimiento del juez Brandeis, señaló que para proteger este derecho más valorado en la civilización del hombre, el derecho a la privacidad o a ser dejado solo (“right to be let alone”), era injustificable la intrusión del gobierno sobre la privacidad de los individuos, en ninguna clase de empleo, la cual se debe considerar como una violación a la cuarta enmienda constitucional.

Las decisiones actuales de los tribunales basadas en la cuarta enmienda constitucional incorporan mucho de la visión de Brandeis, al señalar que “se protege a las personas, no los lugares”, además de apuntar la obligación de la policía de contar con una autorización cuando la investigación se realiza en lugares públicos tales como una cabina telefónica o una calle pública.

La quinta enmienda garantiza que ninguna persona puede ser obligada a declarar en ningún caso del orden penal contra de sí mismo. Este derecho protege la privacidad puesto que establece que nadie puede ser obligado a responder por un delito salvo mediante una orden de presentación o la consignación ante un gran jurado, excepto en causas derivadas de las fuerzas armadas navales o militares. Tampoco persona alguna será juzgada dos veces por el mismo delito, ni será obligada a declarar en su contra en causas penales, ni privada de su vida, libertad ni propiedades, sino mediante debido proceso establecido por la ley. El debido proceso impone la exigencia de fundamentar justicia en todos los procedimientos de identificación usados como evidencia en juicio, sin importar que la identificación sea previa o posterior a la consignación.

La jurisprudencia norteamericana ha desarrollado la exigencia de debido proceso prevista en la quinta enmienda, a través de teorías que garantizan los derechos fundamentales de los individuos, tales como “la ausencia de inducción”; la necesidad de atender la totalidad de las circunstancias en casos de “incriminación por careos o fotografía”; “confrontación en la escena del crimen”; “la confiabilidad de la identificación”, y la regla de exclusión de evidencia obtenida ilegalmente.

En el caso Whalen v. Roe de 1977, la Corte extendió su protección sustantiva de la privacidad llamándola la “zona de la privacidad” protegida por la Constitución abarca el “interés individual de evitar la divulgación de los asuntos personales”. Cabe señalar que esta vertiente del derecho a la privacidad se ha vuelto conocida como el “derecho constitucional a la privacidad informática” la cual desarrollaremos en nuestro trabajo de investigación. Dentro de esta quinta enmienda se considera también la protección de ciertos derechos fundamentales como el derecho a interrumpir el embarazo (con ciertas particularidades) pero no el derecho de morir, y protege también ciertos aspectos de la vide íntima como la contracepción.

Decimocuarta enmienda. Esta enmienda promulgada en 1868 consigna entre otras las garantías de privilegios e inmunidades, misma protección ante la ley y debido proceso (la cual se complementa con la quinta enmienda antes señalada) y establece que ningún Estado promulgará ni dará validez a ley alguna que restrinja los privilegios e inmunidades de los ciudadanos de los Estados Unidos, ni los Estados privarán a persona alguna de su vida, libertad o

posesiones sino mediante el debido proceso establecido en la ley, ni tampoco negarán a las personas la misma protección ante la ley. Cabe señalar que esta enmienda habla específicamente del debido proceso (due process) en los Estados, al contrario de la quinta enmienda que se refiere al debido proceso en la Federación.

Cabe señalar que respecto al derecho Constitucional de los Estados solo Alaska, California y Florida establecen específicamente disposiciones sobre la Privacidad.

V. Derecho codificado

Desde mediados de los años sesentas hasta mediados de los años setentas, la privacidad emergió como elemento central en los intereses políticos y sociales en Estados Unidos, impulsada por la reflexión filosófica y de abogados y estudiantes de derecho, pudieron impulsar la concientización pública sobre los alcances de la privacidad ante el acelerado crecimiento tecnológico.

A mediados de los años sesenta se produjo una creciente emisión de aparatos electrónicos, incentivados por los numerosos documentales en los noticieros, además de recibir atención significativa en los periódicos. La propuesta de creación del Centro Nacional de Datos en 1965 provocó protestas públicas escuchadas por el congreso. En ese tiempo, la computadora constituía una nueva e inexplorada herramienta tecnológica, que producía algunos riesgos sin precedente, en relación a la recolección de datos individuales, con potenciales efectos devastadores para la conservación de la privacidad. No obstante lo anterior, hacia el final de los años sesenta, la recolección de información personal se convirtió en un problema social dentro de la sociedad norteamericana.

Durante este tiempo la Suprema Corte se pronunció en numerosas ocasiones acerca de la privacidad, como el caso Roe v. Wade en 1973 en relación con los derechos reproductivos y la autonomía de decisión. En este caso el Justice Blakckmun, como Ministro Ponente de la Mayoría en el caso referido, definió el criterio de que el concepto de libertad personal y de restricción a los actos de autoridad comprendidos en la decimocuarta enmienda, así como los derechos contenidos en la novena enmienda, son suficientemente amplios para comprender la protección a la decisión de una mujer

de terminar o no su embarazo, “siempre y cuando esto suceda dentro del primer trimestre de la gestación y la decisión es tomada de acuerdo al criterio médico del doctor que atienda a la paciente en cuestión”.

Fue en este mismo año (1973) que se produjo un importante reporte por parte del Departamento de Salud, Educación y Asistencia Social en Estados Unidos (HEW por sus siglas en inglés). Atendiendo numerosas recomendaciones, este reporte propuso una especie de código que constituyera las Mejores Prácticas de Información, el cual consistía en uno de serie de principios básicos para preservar la privacidad de la información, que asignaba derechos y responsabilidades en la recolección y uso de la información personal entre los cuales podemos mencionar los siguientes:

* No debe existir sistemas de registro de información personal que su misma existencia sea secreta.

* Debe de existir una forma para que el individuo encuentre qué información se tiene sobre él y qué uso se hace de ella.

* Debe de existir una forma para que el individuo prevenga que la información que se obtiene para un determinado objetivo no se use para otro propósito sin su consentimiento.

* Debe de existir una forma para que la persona pueda corregir o agregar información a un registro de su información personal.

* Cualquier organización para crear, mantener, usar o distribuir registros de datos personales debe de asegurar la fiabilidad de los datos para su uso futuro, además de tomar precauciones razonables para prevenir el uso indebido de los datos.

Como puede observarse estos principios anunciados en el comienzo de la década de los años setenta han sido los que han servido de base para la protección de los datos personales derivados de los registros electrónicos y después digitales a pesar del avance de la tecnología.

Como observa Marc Rotenberg, las Mejores Prácticas de Información, “han jugado un rol significativo en la estructura del derecho a la privacidad en los Estados Unidos”.

Desde el inicio de la década de los setentas, el Congreso de los

Estados Unidos ha aprobado una serie de numerosas leyes para proteger la privacidad en varios sectores: Fair Credit Reporting Act, de 1970, Privacy Act de 1974, Family Educational Rights and Privacy Act de 1974, Right to Financial Privacy Act de 1978, Privacy Protection Act de 1980, Cable Communications Privacy Act de 1986, Computer Matching and Privacy Protection Act de 1988, Employee Polygraph Protection Act de 1988, Video Privacy Protection Act de 1988, Telephone Consumer Protection Act de 1991, Driver´s Privacy Protection Act de 1994, Health Insurance Portability and Accountability Act de 1996, Children´s Online Privacy Protection Act de 1998, Gramm-Leach Bliley Act de 1999,

No toda la legislación emitida por el Congreso en los Estados Unidos está formulada para proteger la privacidad de los ciudadanos. Cierto número de leyes o estatutos han estipulado la recolección gubernamental de la llamada información sensible, es decir, aquella que tiene que ver con la raza, el sexo, la filiación sindical, etc., o que facilitan el uso de técnicas de investigación por parte de las autoridades de gobierno, entre estas podemos mencionar las siguientes disposiciones: Bank Secrecy Act de 1970, Communications Assistance for Law Enforcement Act de 1994, Personal Responsability and Work Opportunity Reconciliation Act de 1996, y la Patriot Act o Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act[xliv](USAPA) de 2001.

Esta Ley Patriótica ha modificado en forma sustantiva la legislación vigente en torno a la privacidad en línea, de acuerdo el Centro de Información para la Privacidad Electrónica (EPIC por sus siglas en inglés). La propia ley citada introduce modificaciones importantes a diversos estatutos de la legislación federal de los Estados Unidos, es decir, “impone cambios legislativos con respecto a aspectos tan diversos que van desde el lavado de dinero, prácticas crediticias y servicios bancarios y financieras, comunicaciones por medios electrónicos, educación de la familia, espionaje e inteligencia, migración así como intervención de comunicaciones telefónicas, etc.” Las implicaciones con respecto a la privacidad en línea son considerables, ya que este estatuto incrementa la facultad de los organismos de impartición y administración de justicia para autorizar la instalación de equipos de intervención telefónica y dispositivos de rastreo, así como la instalación de dispositivos que canalicen, envíen y señalen la información de las computadoras. Dicha ley también “aumenta las facultades del

gobierno para obtener información financiera personal, así como estudiantil, sin necesidad de comprobar sospecha o hechos constitutivos de delitos, simplemente con al certificación que posiblemente se obtendrá es relevante para una investigación criminal que actualmente se lleve a cabo".

VI. CONCLUSIONES

En Estados Unidos el derecho a la privacidad de acuerdo con la tradición del Common Law se trata de un derecho cuyo contenido es muy amplio, pues se refiere a diversos ámbitos tales como privacidad genética, privacidad en las conversaciones de un psicoterapeuta y su paciente, privacidad en la información médica, privacidad en las asociaciones, privacidad en el hogar, en la escuela, en el trabajo, etc. siendo la protección de datos personales un concepto que se protege a través de la privacidad aplicada a los registros y bases de datos electrónicas.

Godkin es el primer autor en publicar cuestiones relacionadas con el derecho a la privacidad en 1890; sin embargo, su artículo no proponía soluciones concretas, ni se divulgó de manera generalizada, motivo por el cual en muy pocas ocasiones se menciona como antecedente. A diferencia del célebre artículo de Warren y Brandeis titulado The Right to Privacy, publicado en la revista de derecho de la Universidad de Harvard, el cual aborda la necesidad de proteger un reducto privado del individuo que es precisamente el derecho a la privacidad, calificándolo como "el derecho a ser dejado solo". Este artículo es importante porque desarrolla por primera vez el derecho a la privacidad desde una perspectiva jurídica (pues ambos autores eran abogados), no establece la privacidad como derecho absoluto sino que tiene ciertas limitaciones y propone la necesidad de protegerlo como un derecho diferente al de propiedad.

Aunque la Constitución norteamericana no establece una mención literal de la privacidad, se considera que queda dentro de su ámbito de protección pues establece en su primera, tercera, cuarta, quinta y decimocuarta enmienda, disposiciones que se consideran como protectoras de este derecho.

Por su parte la Corte Suprema ha significado un papel fundamental en la configuración de este derecho a la privacidad, porque

gracias a su criterio en la resolución de casos concretos ha ayudado a limitar y definir este derecho tan importante para la vida del individuo en la actualidad, el derecho a la privacidad, específicamente en lo que concierne a su información personal.”

c) Responsabilidad de los Proveedores de Servicios Internet

[FUNDINAGA][3]

1. Introducción:

“La rápida emergencia de un mercado liberalizado de comunicación global, y el uso popular de Internet han traído como consecuencia el cuestionamiento de medios tradicionales de regulación nacional. Martín Bangeman describe la necesidad de una rápida acción en el desarrollo de la sociedad de información: “Si alguien hubiera predecido la atención a las políticas de la sociedad de la información hace algunos años, él o ella hubieran sido considerados como de una imaginación cósmica o cortos de cerebro... el mundo necesita establecer un nuevo juego de reglas adaptadas a las capacidades de las nuevas tecnologías”

En la década de los 60s Marshall McLuhan nos habla de una, hasta entonces, utópica “aldea global”, mientras que, más tarde, Frances Llorens define una nueva cultura mediática, caracterizada por la gran influencia de los mass media. En la actualidad a estos medios de comunicación se suma la información que corre a través de las redes.

La economía digital emerge como plataforma de comercialización de productos en un mundo globalizado que innova toda la actividad humana ya que depende de la implementación correcta del enfoque que se dé a la información.

Así, el derecho debe adecuarse a las nuevas condiciones sociales donde no existen. Se dice que el derecho sufre un desfase frente a las tecnologías, el cual se debe a la falta de importancia que muchas empresas dan a la información. Según un estudio realizado sólo el 40 por 100 de las empresas como un problema grave la seguridad informática. El 72 por 100 cree que existe mayor probabilidad de sufrir ataques externos que internos. El 80 por 100 dice no haber experimentado ataques de intrusión en sus sistemas durante el año anterior, pero sólo el 33 por 100 reconoció su incapacidad para detectar dichos ataques.

En esta nueva sociedad, el sector de las telecomunicaciones es crucial y lo convierte en balaustre del proceso de informatización. La seguridad que se le exige a la red es mucho mayor que la que han ofrecido hasta ahora los medios tradicionales.

Internet implica un medio para muchos atentados contra derechos, bienes e intereses jurídicos. Su potencialidad en la difusión de imágenes e información la hace un medio rápido para atentados contra cuatro tipos de bienes básicos :

1) La intimidad, la imagen, la dignidad y el honor de las personas.

2) La libertad sexual.

3) La propiedad intelectual e industrial, el mercado y los consumidores.

4) La seguridad nacional y el orden público.

5) La seguridad de la información transmitida.

Así, entre estos problemas podemos encontrar:

• Filtración de información confidencial: datos personales, secretos profesionales o información reservada de una empresa.

• Monitoreo de acceso o control de una persona, en la red.

• Protección contra manipulación de datos personales.

• Posibilidades de recoger datos contenidos en la información por medio de programas que se instalan en el cuando se realiza una conexión con un sitio

• Intromisión a la intimidad a través del correo basura y el no deseado

• Protección a menores contra la pornografía y obscenidad, sin violar los derechos de libertad de expresión e información de los adultos.

2. Responsabilidad Civil en la actividad Informática

Las empresas informáticas se enfrentan, en general, a las mismas clases de responsabilidad civil legal que cualquier otra, por las reclamaciones formuladas por sus clientes, empleados, accionistas o terceros.

La responsabilidad civil es el fundamento jurídico del que se hace derivar un derecho indemnizatorio, por las acciones, omisiones o incumplimiento de una obligación, cometidas por una persona, bien sea persona física o jurídica, y que han causado un daño, cualquiera que sea su naturaleza (corporal, material, patrimonial o de índole moral), y en el que haya mediado algún grado de culpa o negligencia . Que aparece como la necesidad jurídica de hacer frente a las consecuencias del obrar culpable – culposo o doloso – que ha ocasionado un daño a otro. Su supuesto, el acto ilícito, concebido como el acto voluntario con cuya ejecución se viola una norma y que, de producir un daño, obliga a su autor a repararlo .

Actualmente, la doctrina defiende la idea de un único concepto de responsabilidad que se identifica con la idea de tener que cumplir una obligación o de compartir las consecuencias de ese deber : “ya no hay que reparar porque existió antes una conducta reprobable, sino que hay que reparar a secas; que no se trata de tanto de moralizar las conductas de los eventuales autores de los daños, como de asegurar las indemnizaciones a las víctimas, la indemnización adquiere el aspecto de un verdadero imperativo social” .

Para que se pueda hablar de responsabilidad es necesaria la concurrencia de cuatro supuestos:

1. Un acto u omisión

2. El daño que supone una pérdida o lesión que sufre un sujeto como consecuencia del acto, consiste en un deterioro que afecta a

bienes personales o patrimoniales del sujeto.

3. El nexo causal: entre el daño y la acción debe haber un vínculo de causalidad, es decir la acción tuvo que provocar el daño.

4. La culpa: mayor o menor conciencia de inobservancia del deber de actuar con la diligencia exigible.

La responsabilidad del profesional que administra una red de datos es contractual o extra contractual según exista vínculo o no entre el ofensor y la víctima. La responsabilidad será contractual siempre que pretensor y obligado estén unidos por un vínculo contractual válido y que el daño derive del incumplimiento o defectuoso incumplimiento de la obligación asumida. Si así no fuera, la responsabilidad será extracontractual .

2.1. La informática como actividad riesgosa

Las telecomunicaciones posibilitan que la información sea obtenida en cantidades casi ilimitadas, y transmitida rápidamente. En la opinión de Parellada , el proveedor informático asume el carácter de obligación de resultado, así el usuario espera de él un resultado funcional de la aplicación del equipo o el programa. Insertar las obligaciones del prestador de los servicios en la categoría de obligación de resultado, implica cargar sobre él la prueba de la causa ajena, cuando el servicio ha sido prestado en forma defectuosa. Ciertamente, esta categorización beneficia al cliente, sin agraviar la justicia que debe consagrar el negocio, pues al proveedor le es mucho más fácil probar cuál es el defecto que provocó el fracaso, que al usuario la prueba de la culpa del prestador.

Así, la obligación de un proveedor de servicios de transmisión de datos debe considerarse como una mezcla de las obligaciones de resultados y de medios. Ya que es responsable tanto de la transmisión perenne de la data, como por velar por su integridad.

En el caso de una obligación de medios se ha cumplido si se desenvuelve con diligencia conforme a los conocimientos y prácticas exigibles según el estado de su profesión o arte y del momento y los medios puestos a su alcance; de manera que le será

atribuible no lograr el resultado cuando medie una conducta limitada o negligente.

El caso de la obligación resultados, se valora que el equipo, programa o transmisión de acuerdo a las necesidades del cliente. Si el equipo, programa o la transmisión no trabajan de acuerdo a lo solicitado existe responsabilidad y la certeza que el cliente lo rechazará.

Ya que se considera que el profesional es un experto en su materia, y que debe tener los medios y conocimientos necesarios para la consecución de su labor. A la hora de establecer su responsabilidad civil hay que observar que tipo de relación tiene con el sujeto que sufrió el daño, sea contractual o extra contractual y sus obligaciones al respecto.

La relación jurídica contractual establecida entre el operador y el usuario ha considerado específicamente la obligación de suministrar un servicio y, como contraprestación, la de pagar un precio por ella.

Sostiene Vázquez Ferreira , que una obligación accesoria de seguridad obliga a que el servicio sea completo, exacto y en tiempo, aún a falta de estipulación expresa por las partes, puesto que tal obligación "...cobra virtualidad por el principio general de la Buena Fe en su función integradora". Los problemas derivados de las relaciones informáticas, pueden encontrar solución en la aplicación del principio de buena fe.

Es éste principio es creador de deberes secundarios de conducta, muchas veces no contemplados por las partes del negocio. Deberes que son exigibles no sólo en la ejecución del contrato, sino también en su formulación, es decir en la etapa pre contractual.

La obligación de seguridad en cuanto al contenido, exactitud y periodicidad del suministro de las informaciones, da lugar a una responsabilidad objetiva contractual, pues tal obligación sería de resultado, y no se admite como excusa la prueba de la falta de culpa, de manera que el que se considera responsable deberá acreditar la ruptura del nexo causal entre su conducta y el incumplimiento.

En los contratos sobre bienes y servicios informáticos el proveedor tiene que cumplir unos deberes que no se agotan con la entrega del bien o la prestación del servicio que se brinda, sino que además tiene el deber de consejo e información. El deber de consejo implica la ayuda al cliente para que exprese sus necesidades y proceder a su estudio si éste no fuera realizado; el proveedor debe informarse de las necesidades de su cliente; también debe informar objetivamente sobre las posibilidades de su sistema. El límite del deber de consejo que asume el proveedor se encuentra en el tiempo de información que el cliente tiene derecho a esperar de él. Por otra parte, una contrapartida obligada de este deber del proveedor es que el cliente brinde al primero información completa y suficiente para que aquél pueda cumplir con su obligación de consejo

2.2. Responsabilidad Extracontractual

En caso de no mediar un contrato destinado a la prestación de un servicio entre el operador del servicio y la víctima, debemos considerar la responsabilidad dentro del ámbito extracontractual. Si hay un acto u omisión ilícito, contra deberes de esa conducta social típica y esperable, un daño infringido injustamente y un vínculo causal entre ambos, se presume que hubo “algún fallo” y surge la obligación de responder, salvo que se pruebe culpa de la víctima o cualquier causa de exoneración. La compensación de los daños producidos extracontractualmente, implica una serie de requisitos:

a) Una conducta injusta en la medida que ocasiona un quebranto injustificado ya sea por culpa, dolo, negligencia o morosidad.

b) La imposibilidad de obtener el cumplimiento forzoso de una manera específica.

c) La ocurrencia efectiva de daños o la pérdida de una ventaja razonablemente segura.

d) Un nexo causal entre la conducta y el daño.

3. Clasificación de las empresas Proveedoras de Servicios Internet

A fin de poder determinar las responsabilidades de los Proveedores, consideramos pertinente el clasificar los diferentes

tipos de proveedores de servicios en:

3.1. Proveedores de Servicios de Redes

Los Proveedores de Red son aquellos que proporcionan infraestructura o capacidad de transmisión de datos. Esto puede ofrecerse en la forma de telefonía tradicional. Además, la infraestructura ofrecida podría ser una red específica para la transmisión de los datos. Los operadores de red serían normados por reglas sobre Internet siempre que sus usuarios se conecten vía módem, y por reglas que involucran a las telecomunicaciones convencionales, siempre que se hagan llamadas telefónicas

La Ley de Telecomunicaciones (Decreto Supremo Nº 013-93-TCC), define a este tipo de Proveedores en su Artículo 10:

“Se considera servicios portadores a aquellos servicios de telecomunicaciones que proporcionan la capacidad necesaria para el transporte de señales que permiten la prestación de servicios finales, de difusión y de valor añadido. Estos servicios pueden ser desarrollados tanto por empresas privadas como por empresas confortantes de la actividad empresarial del Estado y requerirán de concesión expresa para su ejercicio.

El reglamento de la Ley de Telecomunicaciones (Decreto Supremo Nº 027-2004-MTC) en su artículo 30 nos da una mayor definición de los mismos:

“Artículo 30.- Los servicios portadores son aquellos que utilizando la infraestructura del sistema portador, tienen la facultad de proporcionar la capacidad necesaria para el transporte y enrutamiento de las señales de comunicaciones, constituyendo el principal medio de interconexión entre los servicios y redes de telecomunicaciones”.

3.2. Proveedores de Acceso

Los Proveedores de Acceso ofrecen no sólo los medios generales para transferir datos, pero también medios específicos para el

traslado de los mismos. Un Proveedor de acceso a Internet no oferta simplemente conexiones conmutadas, sino los protocolos necesarios para establecer conexiones y frecuentemente la facturación del mismo. Así el servicio ofrecido es específicamente la integración de la computadora del usuario a la red de comunicaciones .

3.3. Proveedores de Contenido

Los Proveedores de Contenidos son aquellos que ofrecen contenido propio en Internet. Éstos son no son un problema en cuando a la determinación de responsabilidad ya que son evidentemente responsables de su propio contenido. Entre ellos podemos encontrar a los denominados “Portales”, tales como: Yupi.com, Terra, etc.

3.4. Proveedores de Servicios Internet y en Línea.

Los Proveedores de Servicios Internet y los Proveedores de Servicios en línea proporcionan acceso a servicios más extensos. En Perú éstos son denominados Proveedores de Servicios de Valor Añadido, los cuales son definidos como:

“… aquellos que utilizando como soporte servicios portadores o finales o de difusión, añaden alguna característica o facilidad al servicio que les sirve de base. Se considera como servicios de valor añadido, entre otros, el facsímile, el videotex, el teletexto, la teleacción, telemando, tele alarma, almacenamiento y retransmisión de datos, teleproceso. El Reglamento de esta Ley señalará los servicios de valor añadido y sus modalidades”.

Entre los servicios de Valor Añadido definidos por el Reglamento encontramos:

Videotex.- Es el servicio interactivo que se presta por la red de telecomunicaciones y que permite la visualización de textos o gráficos por medio de un dispositivo situado en el domicilio del usuario.

Teletex.- Es el servicio que difunde información en forma de texto a diversos usuarios tales como noticias, información de bolsa, entre otros.

Teletexto.- Es el servicio que consiste en insertar información de un texto en la trama de la señal de televisión y es distribuido a través de radiodifusión.

Teleacción.- Es el servicio que emplea mensajes cortos y que requiere velocidades de transmisión muy bajas entre el usuario y la red de telecomunicaciones.

Telemando.- Es el servicio mediante el cual se actúa desde un dispositivo de control distante sobre el sistema supervisado para modificar las condiciones en que se encuentra.

Telealarma.- Es el servicio mediante el cual se genera una señal eléctrica hacia un dispositivo de control distante, cada vez que las condiciones del sistema supervisado se modifican, de forma que se apartan de un margen permitido.

Almacenamiento y retransmisión de datos.- Es el servicio que, a través de la red pública de telecomunicaciones, permite el intercambio de mensajes entre terminales de usuarios empleando medios de almacenamiento y retransmisión. Es decir, permite el intercambio en tiempo diferido de mensajes entre usuarios geográficamente dispersos.

Teleproceso y procesamiento de datos.- Es el servicio interactivo que a través de la red pública de telecomunicaciones permite el procesamiento de datos e intercambio de mensajes a distancia entre terminales de usuarios geográficamente dispersos.

Mensajería interpersonal (correo electrónico en todas sus modalidades).- Es el servicio que permite a los usuarios enviar mensajes a uno o más destinatarios y recibir mensajes a través de redes de telecomunicaciones, empleando una combinación de técnicas de almacenamiento y de retransmisión de datos, para la recuperación del mensaje por el usuario final.

Las modalidades que puede adoptar este servicio son:

Correo electrónico (X.400). Es la mensajería interpersonal que usa

las normas internacionales X.400 del CCITT.

Transmisión electrónica de documentos (EDI). Es la mensajería interpersonal que usa las normas de comunicación EDIFACT.

Transferencia electrónica de fondos.

Correo electrónico de voz. Es la mensajería interpersonal que a través de la digitalización, almacena la voz como archivo digital y la transfiere a otra localidad para su recepción por el destinatario. Otros que determine el Ministerio.

Mensajería de voz.- Es el servicio de transmisión de un mensaje verbal. A petición del solicitante (abonado o no), una operadora transmite un breve mensaje ya sea llamando a uno o a varios números telefónicos a una hora determinada, ya sea respondiendo a la llamada de una persona determinada (abonado o no).

Servicio de consulta.- Es el servicio interactivo que proporciona la capacidad de acceder a la información almacenada en centros de bases de datos. Esta información se enviará al usuario únicamente a petición. La información puede consultarse individualmente en el momento en que debe comenzar la secuencia de información deseada, encontrándose bajo el control del usuario.

Servicio de conmutación de datos por paquetes.- Es el servicio que sin utilizar redes propias, fracciona de acuerdo a una secuencia o trama, las señales de datos en tamaño normalizado denominados paquetes, utilizando las normas X.25 y X.75 de la CCITT.

Este servicio puede incluir modalidades de nuevas tecnologías similares. Queda excluido de este servicio el tráfico de voz en tiempo real.

Suministro de información.- Es el servicio que suministra información obtenida mediante los servicios de radiocomunicaciones.

4. Responsabilidad de Seguridad de los Proveedores de Servicios

Es común la expresión "la información cuesta", lo que refleja su atractivo que en la actualidad representa el manejar datos claves, es la información como elemento de conocimiento, poder y fortuna. Cuando la información se convierte en objeto de apropiación y en blanco lucrativo del delincuente, se ven afectados valiosos bienes jurídicos como la intimidad, el orden socioeconómico, la fe pública y la seguridad del estado, entre otros. Al respecto, Mari luz Gutiérrez Francés nos comenta :

"El computador es un factor criminógeno de primera magnitud que aporta a la conducta criminal, unas veces, un nuevo objeto (la información misma, potenciada y revaluada por los nuevos sistemas de procesamiento de datos y los programas), y otras, un nuevo instrumento: ofreciendo un inmenso abanico de técnicas y estrategias que pueden ponerse al servicio del delito, enriqueciendo el repertorio criminal." Esta acertada distinción permite precisar cuando la tecnología es medio y cuando objeto del delito.

El tema de la informatización y la garantía de las libertades individuales es uno de los que debe enfrentar el derecho y, dentro de éste, por supuesto, el Derecho Penal. El principal aspecto que se discute es el del acceso y utilización de la información privada de las personas. Las normatividades se basan fundamentalmente en acuerdos internacionales sobre telecomunicaciones, comunicaciones vía satélite, protección de software, construcción de equipos y otras .

En un principio, se observaba una reacción a nivel privado frente a las primeras manifestaciones de invasión no autorizada, pero simultáneamente se producía de parte de los transgresores un perfeccionamiento en sus técnicas de intromisión. Posteriormente, ante esta realidad se consideró muy necesaria la participación del Estado y sus organismos, para consolidar la adecuada complementación de los mecanismos de seguridad privados con normativas que establecieran una clara regulación y sanción de estas conductas tipificándolas en los diversos códigos penales como delitos .

El bien jurídico que se pretende tutelar, es precisamente, la Seguridad Informática. La Seguridad Informática es la seguridad de la operación de los sistemas de información, la cual debe proporcionar integridad, disponibilidad y confidencialidad de la información. Integridad: la información debe ser fidedigna y

completa, nadie que no sea el usuario tiene derecho a cambiarla; disponibilidad: el usuario debe tener la información en el momento en que la necesite y confidencialidad: porque sin consentimiento del usuario nadie debe tener acceso ni divulgar su información.

Téllez previene que para intentar una definición de este tipo de delincuencia denominada comúnmente como “delitos informáticos”, es necesario tener en cuenta que ello “no es labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de “delitos” en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión “delitos informáticos” esté consignada en los Códigos Penales” y precisa al respecto que de acuerdo a este análisis se pueden distinguir una definición típica y otra atípica para estas conductas :

“son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin “

“conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin”

Los delitos informáticos se clasifican según

- el perjuicio causado
- el papel que el computador desempeñe en la realización del mismo
- el modo de actuar
- el tipo penal en que se encuadren
- clase de actividad que implique según los datos involucrados.

Quizás la modalidad más conocida de delitos contra la Seguridad Informática, y la más difundida, sea el sabotaje electrónico, el que se presenta en diversas modalidades que van desde la manipulación de los datos antes de su entrada a la máquina, la modificación de un programa para que realice funciones no autorizadas, el redondeo de cuentas, el uso no autorizado de programas, programa de ejecución sujeta a determinadas condiciones, hasta el acceso a líneas de transmisión de datos y el uso de la computadora en la planificación, ejecución o control de la comisión de algún otro delito .

Dentro de este tipo de conductas, comúnmente podemos encontrar:

1.- Phreaking o acceso no autorizado. Es el usual “pinchazo” de redes o teléfonos, donde el individuo se aprovecha ilícitamente del servicio, evitando realizar pago alguno.

2.- Hacking.: Esta conducta se refiere al acceso no autorizado que realiza el sujeto activo a un sistema de información atentando contra el sistema de seguridad que este tenga establecido. Usualmente un hacker realiza estas acciones para satisfacer su curiosidad y aumentar su autoestima.

3.- Cracking: Un cracker, a diferencia de un hacker, usualmente ingresa en redes ajenas con fines ilícitos o para dañar a los mismos.

4.- Atentados contra la propiedad intelectual y de marcas. Son varios los elementos que hacen atractiva la comisión de estos delitos :

- La facilidad con que se pueden perpetra,
- Los montos de las operaciones son elevados,
- Peden perpetrarse a distancia.

4.1. La responsabilidad del prestador de servicios Internet

Este tema tiene dos características principales: la multiplicación de los sujetos pasivos (usuarios, proveedores, fabricantes, etc.) y, en segundo lugar, la complejidad tecnológica de los medios empleados que puede en muchos casos impedir o hacer demasiado costosa la prueba. Así, la pérdida de información por culpa o negligencia del proveedor de acceso será su responsabilidad. En tal sentido, la empresa deberá responder no sólo ante el cliente, sino también ante terceros de los daños y perjuicios que se deriven de la manipulación incorrecta o no autorizada, que puedan provocar averías o deterioros en el servicio o pérdida, modificación o destrucción de la información.

En una prestación de Hosting hablamos de una responsabilidad contractual. Podríamos decir que la relación contractual que une al servidor con sus clientes, es un contrato de arrendamiento o prestación de servicios informáticos, donde el proveedor se

obliga a ejecutar una determinada actividad a cambio de un precio cierto, configurándose una relación de tracto sucesivo que puede ser rescindida en cualquier momento por cualquiera de las partes.

En la responsabilidad por servicios de alojamiento tenemos el riesgo creado y el deber de garantía o de seguridad. El servicio ofrecido por el proveedor de la red se basa en la confianza que sus clientes tienen de la seguridad de sus redes hace que éste tipo de servicio contenga obligaciones tanto de resultado como de seguridad. Los operadores de redes, por ello, no están normalmente expuestos a responsabilidades penales o civiles por el contenido transmitido por sus redes, aunque pueden ser requeridos a dar los pasos adecuados respecto a sus clientes (los proveedores de acceso) si estos últimos usan algunos recursos para transmitir contenidos ilegales o para realizar actos ilícitos.

El principio general de la normativa que regula los requisitos de seguridad que debe cumplir un servicio informático se basa en trasladar a los proveedores la responsabilidad sobre el control de la calidad y seguridad de los servicios que brindan.

En el caso de responsabilidad no imputable al administrador de redes, el responsable será la empresa, o el propietario de la red. Serán responsables de los daños que se causen por la indebida destrucción, apoderamiento, modificación, o utilización de archivos que pertenezcan a los usuarios de modo personal. Sólo serán excluidos de la responsabilidad los Administradores de redes de cómputo, y las empresas o dueñas de la red, si se demuestra que era imposible la prevención del ilícito cometido, a pesar de la debida preparación de los Administradores de la red, así como de que se contaba con los programas actualizados para detección de virus, etc. .

5. Responsabilidad del Proveedor de Servicios Internet frente a contenidos Nocivos e Ilegales

Los contenidos nocivos son aquellos que significan una ofensa a los valores o sentimientos de algunas personas, están íntimamente relacionados con el concepto de honor, pudor, intimidad y moralidad.

Los contenidos ilícitos prohibidos contemplan también apología a algún delito. Así, contempla también a:

a) La difusión de instrucciones sobre preparación de bombas, las actividades terroristas, la producción y tráfico de drogas, y el activismo político, lo que atenta contra la seguridad nacional y mundial;

b) La oferta de servicios sexuales y pornografía relacionada con niños (pedofilia).

c) El envío de mensajes que incitan al odio y la discriminación racial o religiosa.

d) Las conductas de hurto y destrucción de datos que atentan contra la seguridad y confidencialidad de la información;

e) Los delitos de “piratería” de software, que vulneran la propiedad intelectual.

f) Los delitos contra la propiedad industrial: apropiación de logotipos, marcas, diseños originales, etc.

g) El mal uso de tarjetas de crédito ajenas.

h) La recolección, procesamiento y transmisión no autorizada de datos personales.

i) El envío de mensajes difamatorios o injuriantes.

Existen diversas teorías respecto a la responsabilidad de los proveedores de servicios frente a los contenidos transmitidos por sus usuarios a través de la red. Una que sostiene que como medio de comunicación social Internet debe de ser regulada y se debe impedir en ella la transmisión de contenidos nocivos o ilícitos. La otra teoría es la de la autorregulación la cual exime de toda culpa a los proveedores de servicios en cuyas redes o servidores fluya dicho tipo de contenidos, siempre y cuando el proveedor haya advertido a su usuario del carácter de dichos mensajes o publicaciones.

5.1. Posiciones a Favor de la Regulación de Internet

Se sostiene que Internet es un medio de comunicación social, donde se establece una comparación entre los proveedores de acceso a

Internet y los de hospedaje de páginas Web con los editores en el sentido de que ambos proporcionan el soporte material que permite a los autores la divulgación de los contenidos generados. Entonces, las características que definen a un medio de comunicación social son: a) prestar servicios de carácter audible, audiovisuales y/o impresos; y, b) operar en el país.

Para algunos la imputación de responsabilidad a los Proveedores de Servicios es un error como si los proveedores pudieran controlar directamente la totalidad de los contenidos de información que circulan minuto a minuto por sus servidores, datos que son consultados, recopilados, procesados, almacenados o transmitidos por sus usuarios o clientes. .

5.2. Posiciones a favor de la autorregulación de los contenidos

En cambio para algunos autores como Renato Jijena es imposible legislar una sobre una censura y eventual responsabilidad de los proveedores de servicios Internet ya que, bajo la garantía de la "libertad de expresión" universalmente se comprenden la libertad de emitir opinión y el derecho de dar o recibir informaciones o ideas, empero, se trata de un derecho que no es absoluto y que puede estar sujeto a restricciones específicas fundadas en razones de orden público, o pueden originarse responsabilidades derivadas de su mal uso, como cuando con ocasión del ejercicio de la libertad de expresión se atenta contra otros derechos tales como la honra o la intimidad de las personas .

Por ello, los proveedores de servicios Internet no son responsables de las comunicaciones o contenidos que circulan por sus redes o que residen en sus discos duros, salvo en el caso que conociendo la ilegalidad o nocividad de los mismos no hayan sido capaces de detener los actos lesivos o el haber prevenido a sus usuarios del carácter antijurídico de su accionar.

Así, en cuanto al proveedor de acceso y proveedor de alojamiento del sitio cuyo contenido es proporcionado total o parcialmente por terceras personas la publicación y divulgación en un sitio Web de un aviso o mensaje con un contenido ilícito o nocivo también cabe responsabilidad al proveedor de acceso y al proveedor de alojamiento de la página Web respectiva, cuando, a sabiendas de la actividad ilícita que se realiza por los abonados a su servicio,

no ha retirado los datos o no ha hecho que el acceso a ellos sea imposible. Como cuando, sabiendo la actividad ilícita que se realiza, o habiendo podido saberla, no ha retirado los datos, no ha hecho que el acceso a ellos sea imposible o incluso ha promovido ese acceso...” .

El Libro Verde sobre la Protección de los Menores y la Dignidad Humana en los Servicios Audiovisuales y de Información, elaborado por la Comisión Europea, indica que:

“La responsabilidad de un usuario que carga material ilícito en la red y la exención de responsabilidad de los operadores que simplemente lo transmiten parece claramente aceptada. Pero la cuestión de la responsabilidad de los estadios intermedios (especialmente, donde se almacena el material, incluso temporalmente, en formato legible) está lejos de haber quedado establecida. La cuestión consiste en averiguar qué es técnicamente factible y económicamente viable, y conseguir un equilibrio entre la protección de la libertad de expresión y la privacidad, por un lado, y la protección de los menores y la dignidad humana, por otro “ .

5.3. Responsabilidad de los proveedores de servicios

Proveedores de servicios de Red.

El transportar data a cualquier punto dentro o fuera de una red está íntimamente relacionada con las formas tradicionales de telecomunicación más que como una provisión de contenidos, así el Proveedor de Red sólo es responsable de mantener los medios adecuados para la transmisión de datos. El hecho que el servicio de red sirva como medio para la transmisión de contenidos de terceros no hace responsable al administrador del control de los mismos.

Los operadores de redes, por ello, no están normalmente expuestos a responsabilidades penales o civiles por el contenido transmitido por sus redes, Salvo, si conocieron el uso indebido que sus clientes hicieron de sus servicios.

Proveedores de Acceso

En cambio, los proveedores de acceso brindan además “toda la

tecnología electrónica e informática diseñada para la transmisión tanto de caracteres, imágenes o sonidos ” lo cual los hace capaces de transmitir tanto información propia como de terceros.

Los proveedores de acceso que proveen servicios propietarios son siempre responsables, en la medida en que ellos tienen el control del contenido propuesto.

La responsabilidad de los Proveedores de Acceso se puede resumir en:

1. Serán responsables respecto de los contenidos propios que hayan hecho disponibles al público.

2. Los proveedores no serán responsables por el contenido de cualquier tercer parte al menos que hayan tenido conocimiento pleno del mismo, o que técnicamente hayan podido tener conocimiento de ello y bloquear dicha información al público.

3. No serán responsables de la información de terceros que no esté colocada dentro de su red o servidores.

4. La responsabilidad existe cuando el proveedor tenga conocimiento que la información de sus clientes esté enlazada con información nociva esté esta fuera o dentro de la red del proveedor

En los casos en que no existe relación alguna con el usuario de Internet que se considera perjudicado por un contenido determinado es normado a través de las reglas de la responsabilidad extracontractual.”

d) Los Mecanismos de Protección en Colombia del Derecho Fundamental de Intimidad en el manejo de Datos Personales

[BONNET LÓPEZ][4]

“La raza, la religión, la ideología entre otros, han sido siempre factores que han llevado al mundo a sufrir conflictos que

alcanzan dimensiones inimaginables y que violan la dignidad y otros derechos humanos. Vivir en una sociedad dónde, debido a su evolución, la información se ha convertido en la herramienta básica para optimizar la producción de bienes y servicios, aumenta la necesidad de proteger el derecho a la intimidad de las personas. Sin embargo, la creación de mecanismos para lograrlo está estancada y disposiciones de orden internacional como la de Carta de Derechos Fundamentales de la Unión Europea se desconocen en Colombia. Ésta al establecer en el año 2000 en su preámbulo que "….es necesario,….reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y del avance científico y tecnológico", obliga a los gobiernos soberanos a crear mecanismos idóneos para la protección de todos los derechos fundamentales.

En Colombia, datos de identificación personal, comportamiento comercial, comportamiento tributario de las personas entre muchos otros, son considerados necesarios por instituciones públicas o privadas o incluso para particulares para fines controladores o estadísticos de una persona específica. Datos sobre la salud, opinión política e ideología religiosa se manipulan con pocas restricciones.

La tecnología y las innovadoras formas de recopilación y de conservación en esta era de la automatización, los computadores y las nuevas tecnologías en general, han ayudado a lograr gran efectividad en la realización de estas funciones de almacenamiento de información de datos personales. Es decir: a mayor efectividad en los medios de recopilación, procesamiento y almacenamiento de información personal, mayor la posibilidad de vulneración del derecho de intimidad.

En el año 1991 en la Constitución política colombiana, se consagró el derecho a la intimidad en su artículo 15: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar…".

Se tiene un buen punto de partida. Se reconoce que el derecho a la intimidad deber ser garantizado y respetado por el Estado. Sin embargo, el desarrollo legislativo que se requiere para lograr la efectiva protección a este derecho fundamental no ha sido suficiente.

En este artículo se conocerán los mecanismos que en Colombia se han desarrollado para protección del derecho de la intimidad por el manejo de datos personales.

Existen dos tipos distintos de protección: El primero constitucional que es la acción de tutela y el segundo denominado autorregulación.

Previo al estudio de estos mecanismos se conocerán ejemplos de: Normas generales que dentro de su articulado protegen el derecho a la intimidad y el manejo de datos que por ser tangencial la forma de proteger el derecho no son considerados mecanismos y ejemplos de jurisprudencia colombiana. Se entenderá la gran importancia de los pronunciamientos en el desarrollo de los mecanismos protección de Acción de tutela y de autorregulación.

Normativa general:

Ha sido denominada normativa general, ya que, hace referencia a las normas que dentro de su articulado disponen cierta protección al derecho a la intimidad o al manejo de información pero solo de forma parcial. No son normas específicas sobre protección del derecho de intimidad a través de la regulación de datos personales. Por tal motivo, aunque no se considera un mecanismo efectivo de protección, sus artículos pertinentes al derecho de intimidad y protección de la información son herramienta para ejercer los mecanismos que se estudiarán a continuación.

Como ejemplo tenemos a la ley 527 de 1999 que introduce formas de regulación de acceso y uso de mensaje de datos, comercio electrónico y firmas electrónicas y se establece las funciones de las entidades certificadoras. Esta ley aunque regula la protección de bases de datos no especifica nada sobre la protección del dato personal. Por su parte, en el ordenamiento penal mediante la tipificación de ciertas acciones como las establecidas en el capitulo 7 de "los delitos tos contra la libertad individual…", y el capitulo siguiente referente a delitos sobre "…violación a la intimidad, reserva e interceptación de comunicaciones", el ciudadano podrá resarcir su derecho después de

un largo procedimiento penal.

La Jurisprudencia:

Los pronunciamientos de la Corte Constitucional colombiana son, al contrario de la normativa general, fundamentales parar el desarrollo de la acción de tutela y la autorregulación. Mientras que las normas pueden tangencialmente ayudar a proteger un derecho la jurisprudencia garantiza directa y específicamente el derecho de protección de datos personales y por ende el derecho fundamental de intimidad. Es por lo tanto, la fuente perfecta para llenar los vacíos de la legislación colombiana al respecto.

A continuación veremos unos de los pronunciamientos que esta corporación a tenido recientemente para conocer la forma cómo protege los derechos fundamentales que se ven afectados. La Corte Constitucional creada en el año de 1991 en la Constitución del mismo año, es el tribunal cuyos pronunciamientos resuelven la protección de los derechos fundamentales de los ciudadanos. Así, a partir de ese año se conocen los pronunciamientos para la protección de los mismos.

1. Bases de Datos de carácter privado

1.1 Información financiera y crediticia.

Después de haber podido conocer el proyecto de ley colombiano, se ha podido apreciar que le preocupa al gobierno el manejo de las bases de datos de información financiera y crediticia en el país y por esa razón tal documento enfatiza en la regulación de este aspecto. También como a su vez se conoció que no hay suficientes garantías por parte del Estado en este aspecto, a renglón seguido conoceremos las consideraciones de la Corte Constitucional sobre los datos de carácter crediticio.

La Sentencia de Tutela T – 131 de 1998, fue el resultado del ejercicio del mecanismo para proteger su derecho de Habeas Data por parte de un ciudadano cuyo nombre no trasciende. Sin embargo, de manera sintetizada conoceremos los hechos que lo llevaron al

mismo al incoar el mecanismo. Este individuo solicita la información que tiene una corporación financiera colombiana sobre un crédito hipotecario que este había tomado con tal corporación en dónde constaba la cancelación de un deuda pendiente pero le fue negada por la misma par tener control sobre su situación con tal entidad. Ésta, además de ser negada al no poder ser consultada era de imposible rectificación, lo cual generó que una información morosa según el accionante, no veraz fuera conocida por otras instituciones lo que generó mala reputación financiera para este y la negación de posteriores préstamos de dinero. Debido a lo anterior, la Corte Constitucional se ha pronunciado diciendo que "…el derecho a la información no es absoluto, de donde resulta que no puede ser utilizado para revelar datos íntimos ni para lesionar la honra y el buen nombre de las personas. La información, en los términos del ordenamiento superior, debe corresponder a la verdad, ser veraz e imparcial, pues no existe derecho a divulgar información que no sea cierta y completa. Así, mientras la información sobre un deudor sea veraz, es decir, verdadera y completa, no se puede afirmar que el suministrarla a quienes tienen un interés legítimo en conocerla, vulnera el buen nombre del deudor; si realmente este tiene ese buen nombre, la información no hará sino reafirmarlo; y si no lo tiene, no podrá alegar que se le vulnera su derecho". Y adiciona que "en relación con el derecho a la información y la legitimidad de la conducta de las entidades que solicitan información de sus eventuales clientes, a las centrales de información que para el efecto se han creado, como la Asociación Bancaria, así como la facultad de reportar a quienes incumplan las obligaciones con ellos contraídas, tiene como base fundamental y punto de equilibrio la autorización que el interesado les otorgue para disponer de esa información, pues los datos que se van a suministrar conciernen a él, y por tanto, le asiste el derecho no sólo a autorizar su circulación, sino a rectificarlos o actualizarlos cuando a ello hubiere lugar. Autorización que debe ser expresa y voluntaria por parte del interesado para que sea realmente eficaz". Como conclusión de esta sentencia la Corte Constitucional específicamente afirmó que los derechos a la honra y al buen nombre resultan quebrantados cuando la información que se reporta a los bancos de datos sea falsa, o cuando siendo verdadera sigue apareciendo en el banco de datos a pesar de haber caducado. Por lo anterior, si la información suministrada a dichas entidades es falsa o errónea, afecta los derechos fundamentales a la honra y al buen nombre, e igualmente perjudica su actividad económica.

Adicionalmente, la sentencia La sentencia T – 412 de 1992,

interpuesta por un ciudadano colombiano al que se le estaba violando su derecho a la intimidad y al buen nombre por ejercicio de unas funciones netamente pragmáticas cuyo único objetivo era colaborar con la economía, específicamente la de publicación de datos información financiera negativa y que en el caso concreto se trataba de una no veraz, reconoce con claridad que la dignidad humana es el principio supremo de la Constitución de 1991, y que por tal motivo aclara, que en Colombia "la actividad económica no puede desarrollarse hoy en abierto contraste con los valores fundamentales y las exigencias propias de la libertad humana. Ella prevalece sobre toda pretensión desmesurada de servir por los intereses de la productividad y la eficacia". Y Adiciona que dentro de la perspectiva de crear y definir permanentemente nuevos derechos humanos que respondan a las exigencias de las diversas coyunturas históricas, trayendo a colación la denominada "Proclama de Teherán", aprobada por la Conferencia Internacional de Derechos Humanos el 13 de Mayo de 1968 en donde se declaró que: "Si bien los recientes descubrimientos científicos y adelantos tecnológicos han abierto amplias perspectivas para el progreso económico, social y cultural, esta evaluación puede , sin embargo, comprometer los derechos y las libertades de los individuos y por ello requerirá una atención permanente". Entre tales medidas apropiadas la ONU, a través de sus organismos especializados, ha venido estimulando la adopción de normas para el manejo de bancos de datos y de protección a la intimidad. Es así como la Corte llega a la conclusión que en su función de defender los derechos fundamentales, proteger la intimidad la honra y la libertad contra los abusos de del poder informático vinculado estrechamente con los adelantos tecnológicos, la intimidad, entendida por la corporación como la forma de protección de la vida privada que se hace en sentido amplio y en sentido estricto, designando todas las reglas jurídicas que tienen por objeto proteger la vida personal y familiar y empleando el conjunto de normas que tienen por fin la protección de las personas contra los atentados que afectan particularmente el secreto o la libertad privada, este prevalece sobre el derecho de la información. Y es que es fundamental entender que el derecho no ha sido ajeno a la protección de la vida privada aunque se ha hecho difícil por cuanto en nuestro tiempo los secretos no son simplemente captados por los sentidos sino por el uso de técnicas que limitan su revelación a los nuevos medios de comunicación social. "…Dentro de este complejo contexto, se protege la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad..." "Esta particular naturaleza suya determina que la intimidad sea también un derecho general, absoluto,

extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer "erga omnes", vale decir, tanto frente al Estado como a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada. Su finalidad es la de asegurar la protección de intereses morales; su titular no puede renunciar total o definitivamente a la intimidad pues dicho acto estaría viciado de nulidad absoluta". Gracias a lo anterior, termia la Corte diciendo que en caso insoluble entre el derecho de intimidad con el de información, se reconoce la prevalencia del primero sobre el segundo que es consecuencia necesaria de la consagración de la dignidad humana como principio fundamental y valor esencial, a la vez, del Estado social de derecho que es Colombia.

Habiendo conocido algunos casos de regulación por medio de la jurisprudencia, entraremos a estudiar los mecanismos basados en ella y en las disposiciones constitucionales.

Los mecanismos de protección

1. La Acción de Tutela:

La Acción de Tutela se ha creado como una institución y mecanismo idóneo para la protección de la información del individuo. Creada en la Constitución de 1991 este mecanismo busca que en Colombia sea medianamente posible que los derechos fundamentales de protejan: "Toda persona tendrá acción de tutela para reclamar ante los jueces, en todo momento y lugar, mediante un procedimiento preferente y sumario, por si mismo o por quien actúe a su nombre, la protección inmediata de sus derechos constitucionales fundamentales, cuando quiera que éstos resulten vulnerados o amenazados por la acción o la omisión de cualquier autoridad pública…".

Esta Acción, vale decir tiene las siguientes peculiaridades: Primero que todo, los principios que la gobiernan son los de,

a)Subsidiaridad: Porque solo procede cuando no se dispone de otro medio de defensa judicial.

b)Inmediatez: Porque su propósito es otorgar sin dilaciones la protección solicitada.

c)Informalidad: Porque no ofrece dificultades para su servicio.

d)Especificidad: Porque se contrae a la protección exclusiva de los derechos fundamentales.

e)Eficacia: Porque en toda caso exige del juez un pronunciamiento de fondo para conceder o negar el amparo del derecho.

f)Preferencia: Porque el juez la tramitará con prelación a otros asuntos, salvo la acción de habeas corpus. Los plazos son perentorios e improrrogables.

g)Sumariedad: Porque es breve en sus formas y procedimientos.

Como bien se entiende después de leer estos principios, la tutela se entiende como la principal institución que se creó después de la nueva Constitución para la protección de todos los derechos fundamentales y su función exclusiva es la de proteger esta clase de derechos.

No obstante la intención del constituyente en la creación de este mecanismo de protección y del legislador al regularla fue salvaguardar la mínimas garantías pero no poco importantes del ser humano, en el tema de la protección de datos, esta herramienta no es lo suficientemente eficaz en la práctica. Y es que aunque principios de celeridad gobiernan su funcionamiento, no se da tal en la realidad. Por lo tanto, a pesar de las buenas intenciones en la creación de este recurso todavía hace falta un sistema normativo completo para regular el tema.

2. La autorregulación:

Otra forma desarrollada en Colombia para llenar los vacíos de la

regulación es la autorregulación. Colombia como cualquier otro país en el mundo, cuenta con administradores de información personal, que van desde los que se encargan de los datos de los empleados y directivos de la mediana o gran empresa privada hasta las entidades estatales encargadas del manejo de la información de cada uno de los ciudadanos. Cada uno de ellos, con el fin de mantener una políticas mínimas para el respeto por el derecho de intimidad y buen nombre, frente a las ya mencionadas deficiencias del sistema normativo, los organismos tanto privados como públicos que tienen la capacidad de manejar datos personales, han recurrido a la autorregulación. En otras palabras, han recurrido a la auto creación de normas que determinen las obligaciones y derechos tanto de quienes manejan lo datos personales como de sus titulares.

Esta opción que puede considerarse como temporal dentro de las organizaciones colombianas hasta superar la larga espera del nacimiento de una ley sancionada por el gobierno y que entre a regular el funcionamiento de las mismas en este campo, ha sido la acogida en los últimos tiempos. Para ilustrar la panorámica nacional, se presentará, a manera de ejemplo, la posición que ha adoptado la institución colombiana encargada de manejar la información financiera de todos los ciudadanos. DataCrédito es una Central de Información que recopila información de la forma como las personas y las compañías han cumplido con sus obligaciones con entidades financieras, cooperativas o con almacenes y empresas del sector real, sobre la situación crediticia general e histórica, positiva y negativa de los clientes de cada entidad, previa autorización escrita y voluntaria del ciudadano. Esta entidad, recibe, almacena, procesa y suministra la información sobre la Historia de Crédito de las personas formada por los datos de las personas y las compañías referente al cumplimiento de sus obligaciones con instituciones financieras, cooperativas o con almacenes y empresas que venden crédito.

Recientemente, DataCrédito expidió un código en el que se busca que la forma como se debe funcionar una base da datos protegiendo los derechos de los ciudadanos. Para ese cometido, la entidad parte de los siguientes derechos del titular de la información: consultar la historia de crédito, conocer los usuarios que han consultado su historia de crédito en los últimos seis meses, presentar las reclamaciones necesarias por haberse dado información incorrecta, incluir dentro de su historia de crédito por las razones por las que considera que la información que se

tiene está errado, exigir el cumplimiento del plazo establecido para mantener la información negativa, obtener la actualización de la información proporcionada a DataCrédito de manera rápida, reportar la información solo cuando se solicita respetando la finalidad para la que fue solicitada. Todos estos derechos de los usuarios deben estar regulados para no generar la gran incertidumbre de un vacío legal y en este caso, con la autorregulación de la institución en cuestión, se pretende lograr un equilibrio entre el ejercicio del derecho de información y el habeas data. La misma afirma que lo que se busca es "Un marco regulatorio integral y equilibrado que reconocería explícitamente los bienes jurídicos de interés general (libertad de información, interés público de la actividad de crédito) frente a los de interés particular (habeas data, intimidad)".

Conclusión:

Dentro de los mecanismos legales que se han desarrollado para buscar proteger el derecho a la intimidad el más eficaz es el de la Acción de Tutela. Sin embargo, es absolutamente necesaria la creación de una norma específica que garantice la protección a este derecho. Que cuente con sanciones concretas para aquellos que manipulan información personal de forma desleal e irresponsable. Que incluya dentro de su articulado mecanismos rápidos para que el ciudadano pueda recurrir a la justicia con prontitud, diferentes al de la acción de tutela. La Acción de Tutela establecido desde el año de 1991 es el que ha soportado desde hace más de 13 años todas las reclamaciones por violaciones de derechos fundamentales que han sufrido los colombianos. Esto lo ha convertido en una herramienta sobre utilizada por los mismos y que por tal motivo necesita de la creación de otro tan efectivo y rápido que permita garantizar un protección absoluta del derecho de Habeas Data, privacidad e intimidad por violaciones a datos personales."

FUENTES CITADAS

1 BORLOTTO, Verena. Protección de Datos Personales contenidos en las Bases de Datos Informatizadas y no Informatizadas obrantes en el Poder Judicial Uruguayo. Artículo [en línea]. Publicado en la Página ALFA-REDI en julio del 2006. Visitada el 21/08/08. Disponible en la dirección: http://www.alfa-redi.org/rdi-articulo.shtml?x=6505
2 PUENTE DE LA MORA, Ximena. Privacidad de la Información Personal y su Protección Legal en Estados Unidos. Artículo [en línea]. Publicado en la Página ALFA-REDI en agosto del 2006. Visitada el 21/08/08. Disponible en la dirección: http://www.alfa-redi.org/rdi-articulo.shtml?x=6956
3 FUNDINAGA, Katherine. Responsabilidad de los Proveedores de Servicios Internet. Artículo [en línea]. Publicado en la Página ALFA-REDI en febrero del 2006. Visitada el 21/08/08. Disponible en la dirección: http://www.alfa-redi.org/rdi-articulo.shtml?x=4714
4 BONNET LOPEZ, Andrea. Los Mecanismos de Protección en Colombia del Derecho Fundamnetal de Intimidad en el manejo de Datos Personales. Artículo [en línea]. Publicado en la Página ALFA-REDI en Diciembre del 2006. Visitada el 21/08/08. http://www.alfa-redi.org/rdi-articulo.shtml?x=8082