TÍTULO: ALGUNAS CONSIDERACIONES SOBRE LA PROTECCIÓN DE DATOS PERSONALES EN LA LEGISLACIÓN CUBANA.

Resumen:
En las últimas décadas se ha producido un intenso desarrollo de las tecnologías de la información. Los modernos sistemas de información y comunicación generan incertidumbre y riesgo ya que la informática proporciona ilimitadas posibilidades para que los datos personales sean recolectados, tratados, conservados y transmitidos. La tecnología es capaz de mover un gran volumen de información que puede limitar nuestra libertad o condicionar nuestro modo de actuar.
La presente investigación tiene el propósito de delimitar los aspectos esenciales que conforman el tratamiento jurídico a la protección de datos personales en el ordenamiento jurídico cubano, partiendo de la sistematización de las regulaciones existentes en esta materia.
Nuestro país como parte de los procesos de informatización de la sociedad debe implementar mecanismos jurídicos eficientes que respalden la conservación y confidencialidad de los datos personales, por lo que se plantean nuevos retos jurídicos para el legislador cubano en la esfera de la industria informática nacional.
Por: MSc. Mayda Gallardo Villavicencio

"A quien dices el secreto, das tu libertad"
Fernando de Rojas, La Celestina

SUMARIO:

1. CONSIDERACIONES GENERALES. 2. LOS DATOS PERSONALES. PRECISIONES CONCEPTUALES. 3. TRATAMIENTO JURÍDICOS DE LOS DATOS PERSONALES EN CUBA. 4. CONCLUSIONES.

1. CONSIDERACIONES GENERALES.

En las sociedades contemporáneas nadie puede sustraerse al incesante flujo de los datos; cuando uno compra un electrodoméstico o cuando abre una cuenta corriente en un banco, cuando va a un hospital o es atendido por un médico, cuando paga sus impuestos, debe cumplimentar y rellenar formularios donde se fijan necesariamente datos personales del comprador, del paciente, del cliente, del ciudadano. La gestión de las relaciones sociales, jurídicas y económicas exige el intercambio y flujo constante de datos personales. Esta gestión se realiza hoy en día con el auxilio de las nuevas tecnologías, particularmente de la informática.
Junto a la informática, el auge de las telecomunicaciones ha llevado a modificar en nuestros días los sistemas de comunicación y el flujo de los datos. Dos elementos caracterizan la expansión de estas tecnologías;

- ✓ El aumento progresivo de información relativa a las personas que se utiliza por terceros, muchas veces con desconocimiento de los propios titulares;
- ✓ La facilidad y rapidez en la comunicación de dicha información desde cualquier punto de cualquier continente.

Consecuentemente, se aprecia un riesgo importante en el tratamiento automático de los datos personales derivado de la interconexión de los ordenadores a través de las redes de telecomunicaciones y de la posibilidad de que los datos sean transferidos a otros lugares, o países, donde no exista una suficiente protección.

Determinar los medios de protección de la información personal que se acumula en registros públicos, muchas veces accesibles, con trasgresión de derechos fundamentales, plantea nuevos retos a nuestro ordenamiento jurídico en aras de propiciar tutela a los titulares de la información, sobre todo en el campo de la informática que posee un incipiente desarrollo y por ello constituye uno de los entornos más vulnerables para la circulación de datos.

Por lo que el propósito fundamental de esta investigación lo constituye delimitar los aspectos que conforman el tratamiento jurídico al derecho a la protección de datos personales y algunas de las alternativas de tutela existentes en el ordenamiento jurídico cubano.

2. LOS DATOS PERSONALES. PRECISIONES CONCEPTUALES.

Los datos personales son definidos legalmente como aquella información relativa a los individuos ya sea numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. Esta información le da identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional.

Se restringe a las personas físicas, por lo que no constituye dato personal la denominación social, dirección, teléfono o fax de una empresa, aunque la información sobre los trabajadores de la misma si se considera información personal.

La dirección de correo electrónico se considera como dato personal, aunque ésta no muestre directamente datos relacionados con el titular de la cuenta, sino una denominación abstracta o un conjunto de caracteres alfanuméricos sin significado alguno.

Los datos personales también describen los aspectos más sensibles o delicados sobre el individuo, como es el caso de su origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, forma de pensar, estado de salud o vida sexual, estos son los denominados datos sensibles.

Estos datos pueden proceder de dos fuentes: del propio interesado, y de las denominadas fuentes accesibles al público.

3. TRATAMIENTO JURÍDICOS DE LOS DATOS PERSONALES EN CUBA.

La implantación de las nuevas tecnologías en Cuba constituye prioridad gubernamental, ya que esto incide directamente en el progreso social y el desarrollo de la economía. La política de Ciencia y Tecnología se centra fundamentalmente en el acceso a las Tecnologías de la Informática y las Comunicaciones como eslabón fundamental que posibilita el conocimiento, la información y la comunicación fundamentales para el progreso y el bienestar.

En virtud del Decreto-Ley No. 204 de fecha 11 de enero del 2000 se encarga al Ministerio de la Informática y las Comunicaciones, las tareas y funciones encaminadas a rectorar y desarrollar los procesos informáticos y tecnológicos. De igual manera se otorgó a la Empresa de Telecomunicaciones de Cuba S.A, (ETECSA), exclusividad para prestar los servicios públicos de transmisión de datos y conducción de señales, nacional e internacional en virtud del Decreto 190 de fecha 17 de agosto de 1994 adoptado por el Comité Ejecutivo del Consejo de Ministros (CECM). Funciones que desde el 1976 se venían desarrollando en el país por diferentes organismos.

La protección de la información, específicamente en materia del tratamiento de datos o información personal, no se encuentra definida en una ley o norma que reúna o trate de analizar en forma sistemática el tema.
Existen instituciones en nuestro país que poseen y gestionan datos personales, por ello, la protección de estos debe plasmarse en una norma específica cuidadosamente elaborada y puesta en práctica, si tenemos en cuenta que los ciudadanos ceden su privacidad al Estado cuando le proporcionan información de diversa índole de la cual son titulares y que no necesariamente proporcionarían a terceros, si no es para el cumplimiento de la ley.
Por tanto, existirá seguridad jurídica para el titular de los datos, en todos aquellos casos en que el Estado los recaba cuando ello resulta indispensable para el ejercicio de sus atribuciones.
Derivado de esto se han generado una serie de disposiciones legales que establecen, por un lado la confidencialidad de cierta información relativa a las personas y, por el otro la subordinación de la privacidad frente a otros bienes jurídicamente protegidos. En este sentido, se propone analizar algunas de estas disposiciones partiendo en primer lugar del análisis del texto constitucional.

3.1 REGULACIÓN CONSTITUCIONAL.

El derecho a la protección de datos personales se traduce como el reconocimiento y establecimiento de prerrogativas, principios y procedimientos para el tratamiento por parte del Estado o de terceros, de la información concerniente a personas físicas.(1) Sin embargo, este derecho instituido en Europa y en varios países de América no adquiere la misma peculiaridad en Cuba ya que esta prerrogativa no ha sido incluida en la Constitución de la República de Cuba de 24 de febrero de 1976. Reformada el 12 de julio de 1992 y el 10 de junio de 2002.
En el referido texto no existen pronunciamientos explícitos a conceptos tan modernos como la autodeterminación informativa sobre los propios datos personales (como denomina a este derecho fundamental la jurisprudencia alemana, o a la libertad informática, como es llamado por la jurisprudencia española,(2) ni que posibiliten el derecho de acceso a la información (recurso de habeas data), por lo que al no existir regulación sustantiva sobre protección de datos, la doctrina internacional plantea que la tutela judicial de la libertad informática pueda diseñarse sobre la base de la tutela de la intimidad.(3)

La constitución cubana tampoco regula de manera expresa el derecho a la intimidad,(4) no obstante se infiere su regulación de lo preceptuado en el artículo 9 a) que expone: “El Estado garantiza la libertad y la dignidad plena del hombre, el disfrute de sus derechos, el ejercicio y cumplimiento de sus deberes y el desarrollo integral de su personalidad”, en su artículo 58 cuando garantiza la inviolabilidad de la persona, “La libertad e inviolabilidad de la persona están garantizados a todos los que residen en el territorio nacional”, en el artículo 57 que se refiere expresamente a la inviolabilidad de la correspondencia, al plantearse: La correspondencia es inviolable. Solo puede ser ocupada, abierta y examinada en los casos previstos por la ley. Se guardará el secreto de los asuntos ajenos al hecho que motivare al examen. El mismo principio se observará respecto a las comunicaciones cablegráficas, telegráficas y telefónicas y en su artículo 56 que regula la inviolabilidad del domicilio regulado de la siguiente manera: “El domicilio es inviolable. Nadie puede penetrar en el ajeno contra la voluntad del

morador, salvo en los casos previstos por la ley". Estos preceptos reflejan que el tratamiento que se le concede al derecho a la intimidad es ambiguo y abstracto, lo que propicia una mayor vulnerabilidad a la regulación de la libertad informática que podría provocar el tratamiento abusivo de la información personal ya que no existe un marco adecuado de garantías.

Las pautas para la definición del derecho a la protección de datos personales deben centrarse en la finalidad de lograr visualizarlo en su carácter autónomo, de lo contrario existe el riesgo de confundirlo con el concepto del derecho que protege la privacidad de las personas.

Por lo que se propone valorar la posibilidad de establecer un marco de garantías que se asienten sobre dos principios jurídicos de gran importancia:

Legitimidad del tratamiento de los datos, por lo que solo podrán realizarse aquellos tratamientos que sean legítimos conforme los criterios que fijen las leyes.

Un sistema de control de los datos personales que configure la libertad informática como un derecho subjetivo que permita controlar los datos que están siendo tratados, dentro de los límites establecidos por la ley.

En tal sentido, solo existirá libertad informática cuando, a través de la ley, solo se consientan aquellos tratamientos que sean legítimos en su origen y en su ejercicio.

3.2 REGULACIÓN ADMINISTRATIVA.

En el ámbito administrativo es donde, por los respectivos Ministerios, se han creado regulaciones que en alguna medida se refieren a la protección de los datos personales, aunque ciertamente el objetivo fundamental de dichas disposiciones no ha sido la protección de este derecho.

Tratamiento de datos personales por el Ministerio de la Informática y las Comunicaciones.

El 18 de julio de 2000 el Comité Ejecutivo del Consejo de Ministros adopta el Acuerdo No. 3736 en el que se determinan los objetivos y funciones específicas del Ministerio de la Informática y las Comunicaciones, quien debe elaborar y controlar las disposiciones relativas a la integridad y privacidad de la información; la seguridad e invulnerabilidad de las redes de infocomunicaciones; el diseño y documentación de los sistemas informáticos, así como la inviolabilidad de la correspondencia postal y telegráfica.

En el ejercicio de estas atribuciones y cumpliendo con lo dispuesto en el Acuerdo No. 6058 del Comité Ejecutivo del Consejo de Ministros, de fecha 9 de julio del 2007 en cuanto a la necesidad de implementar un Reglamento de Seguridad Informática, se dicta la Resolución No. 127 del 2007 a partir de la cual se aprueba y pone en vigor el Reglamento de Seguridad para las Tecnologías de la Información. Como su propia denominación lo indica su objetivo fundamental es garantizar la seguridad de las tecnologías de la información(5) mediante la instauración de un conjunto de preceptivas que determinan aspectos generales de la seguridad informática en el marco de actuación de algunas instituciones, las que en el caso del Ministerio del Interior y de la Ministerio de las Fuerzas Armadas Revolucionarias se adecuarán por los propios ministerios a sus condiciones de trabajo debido a la relevancia de la información procesada que incide en la seguridad del Estado cubano.(6) Para garantizar la seguridad de la información, las entidades están obligadas a diseñar y mantener un Sistema de Seguridad Informática(7) que se acompaña de un Plan de Seguridad

Informática; ambos documentos deben elaborarse en correspondencia con las metodologías establecidas por la Oficina de Seguridad para las Redes Informáticas.(8)
También se delimitan un conjunto de deberes para los diferentes sujetos que intervienen en las actividades relacionadas con la utilización de las tecnologías, destacándose entre ellas la obligación de los jefes de organismos de imponer o proponer sanciones ante violaciones del Sistema de Seguridad,(9) así como la responsabilidad de los usuarios con respecto a la protección de la tecnología que se le ha asignado evitando que sea robada, dañada o usada la información que contiene.(10) Además de estas medidas, se estipulan otras tareas de carácter técnico que están encaminadas igualmente a la seguridad de los ordenadores, abarcando la protección a todas las tecnologías o a su información frente a cualquier sustracción o alteración, independientemente del valor que posean,(11) lo que indica el alcance de las regulaciones que contiene este Reglamento. Por otra parte se aclara que en el cumplimiento de las acciones de seguridad se debe controlar que el acceso a los sistemas se realice únicamente por el personal autorizado y no por otras personas,(12) ya que la restricción del conocimiento permite el mantenimiento de la confidencialidad de la información; y por otro lado aquellos que si la conozcan deben abstenerse de utilizarla para beneficio propio(13) en virtud de la prohibición plasmada al respecto en este Reglamento.
Los preceptos tratados, de una forma u otra, se encargan de proteger la información en sentido general, es decir, que en ellos no se especifica qué tipo de datos se procesan, sólo están destinados a la preservación de la confidencialidad, integridad y disponibilidad de la información, aspectos que han sido analizados como parte de la seguridad de los datos. Otras regulaciones de este Reglamento si influyen en la protección de los datos personales, ya que se prohíbe el desarrollo de fenómenos informáticos como el conocido spam(14) que invade la esfera privada de las personas ante la ausencia de consentimiento. También se prohíbe la difusión de datos que puedan afectar la moral, las buenas costumbres, la integridad de las personas o la Seguridad Nacional,(15) disposición que considero defiende en gran medida los intereses más cercanos a los ciudadanos, evitando la vulneración de sus derechos. De igual forma se defiende el derecho de acceso de los usuarios autorizados a acceder a sistemas de información(16) y se prohíbe tanto a personas naturales como jurídicas la búsqueda en las redes públicas de trasmisión de datos, de información perteneciente a los usuarios legales.(17) Para evitar el incumplimiento de alguna de estas disposiciones se aplican medidas de carácter administrativo y cautelar.
Una de las instituciones adscriptas a este Ministerio es la Empresa de Telecomunicaciones de Cuba (ETECSA), que fue creada en virtud del Decreto No.190 del 17 de Agosto de 1994 dictado por el Comité Ejecutivo del Consejo de Ministros (CECM), planteándose como Objeto Social la prestación de servicios públicos de telecomunicaciones(18) mediante la operación, instalación, explotación, comercialización y mantenimiento de redes públicas de telecomunicaciones en todo el territorio de la República de Cuba. Además dentro de sus principales propósitos se encuentra el logro de la calidad como Filosofía de Gestión, por lo que para sus trabajadores resulta imprescindible alcanzar la excelencia en los servicios. Para lograrlo, en primer lugar, debe otorgarse a los clientes suficiente seguridad mediante las garantías de inviolabilidad, confidencialidad, integridad, disponibilidad de los

sistemas de información y comunicación sobre todo de los datos y la información transmitida por cada uno de los servicios prestados.
Por ello la Concesión Administrativa se refiere al Secreto de las Telecomunicaciones(19) estableciendo que debe protegerse la información proporcionada por los usuarios en la concertación del contrato de prestación de servicios, requiriéndose del consentimiento de estos para su divulgación. Igualmente existe un Reglamento Disciplinario Interno de ETECSA en el que se establecen un conjunto de obligaciones y prohibiciones que deben ser cumplidos por todos los trabajadores. Entre ellas se presentan algunas relacionadas con la información que se procesa, estableciéndose específicamente dentro de las obligaciones(20) que el trabajador debe mantener discreción con respecto a la labor que desempeña y a los documentos que posee, por lo que no debe divulgarlos sin la correspondiente autorización, cumpliendo además las normas de inviolabilidad de las comunicaciones, no escuchando ni divulgando su contenido dentro o fuera del puesto de trabajo. De igual forma constituye una prohibición(21) para el trabajador revelar a personas no autorizadas, cualquier información que reciba o conozca en razón de su cargo. El incumplimiento de alguno de estos preceptos entraña violaciones graves, que son consideradas infracciones de la disciplina laboral por las que el trabajador puede ser objeto de aplicación de medida disciplinaria a partir de este reglamento en correspondencia con el Decreto Ley 176 Sobre Justicia Laboral.(22) Sin embargo no se tipifica como conducta violatoria de la disciplina las que bien pudiera cometer un trabajador de ETECSA que acceda a determinado segmento de red y desvíe tráfico telefónico o cualquier otra información que se genere o trasmita por nuestra red, cuando no está en el ejercicio de sus funciones.
Por otra parte en el Contrato de Servicio Telefónico Básico, puesto en vigor por la Resolución No 15/98 del entonces Ministerio de Comunicaciones, a partir del cual se elaboraron las demás proformas de los servicios que abarcan la Concesión y que forman parte del Manual de Operaciones Comerciales, dispone entre las Obligaciones de ETECSA (que a su vez constituye un derecho del Cliente), la identificación del Cliente que lo desee en el Directorio Telefónico, acorde a los datos registrados en el Contrato, con el fin de respetar su privacidad y si se produce cualquier error humano en la manipulación de esta gran base de datos se subsana a instancia del propio Cliente. Entre las Obligaciones del Cliente se expresa que no se deben causar molestias a terceros, lo cual no es posible ni legal comprobar, atendiendo a que su investigación y comprobación resulta una flagrante violación, no sólo de la intimidad de la persona que lo solicita sino más aún de aquella tercera persona que no ha dado su consentimiento en el sentido de que sea escuchada su conversación. En este sentido las solicitudes que realizan los Clientes no deben resultar satisfechas, los cambios tecnológicos en las centrales digitalizadas brindan una solución a través del servicio agregado de identificador de llamadas.
El avance de las nuevas tecnologías abre nuevas posibilidades de comunicación que deben contar con garantías suficientes para los Clientes a partir de los contratos a suscribir con ellos de modo que estos sientan que pueden acceder a estos servicios libremente con confianza en la red, sin temor de que sus datos vayan a parar a ficheros no autorizados que pudieran utilizarse por personas inescrupulosas con variados fines

ya sean comerciales, suplantación de la personalidad del usuario con mensajes ofensivos que se remiten en su nombre o virus informáticos.
Es en la Resolución 65 de 2003 del Ministerio de Informática y Comunicaciones donde se regula el funcionamiento de la red privada de datos,(23) debiendo estas inscribirse en el registro existente a esos efectos en la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, quien establecerá los principios que regirán el funcionamiento de las mismas.
En el caso del correo electrónico o correspondencia punto a punto, que identifica a los emisores o remitentes frente a los destinatarios de los e-mail y frente al proveedor del servicio, se le puede aplicar siempre la garantía constitucional del artículo 57 respecto a la inviolabilidad de la correspondencia que regula el secreto de las comunicaciones cablegráficas, telegráficas y telefónicas. Estas operaciones hoy cotidianas involucran el procesamiento de datos personales o nominativos que pueden ser recopilados, almacenados y cruzados indebidamente o sin autorización de su titular.
Las conductas atentatorias contra esta garantía son constitutivas de delito y castigadas según lo establecido en nuestro Código Penal en su artículo 289.1 que plantea: “El que sin estar autorizado, abra carta, telegrama, despacho o cualquier correspondencia perteneciente a otro...”, apreciamos un amplio marco regulador ya que no especifica el tipo de correspondencia lo que permite la posibilidad de violación de la correspondencia punto a punto (correo electrónico).
El uso cada vez más masivo de los denominados “e-mails” o correos electrónicos propicia que estos sean cada vez más interactivos, personales e intrusivos. A través de la Resolución No. 85 de 2004 del Ministerio de la Informática y las Comunicaciones se regula el funcionamiento de las entidades cubanas que brinden los Servicios de Navegación por Internet y/o Correo Electrónico Nacional e Internacional las que deberán estar debidamente registrada a esos efectos en la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones órgano que podrá en cualquier momento y sin previo aviso controlar y supervisar el cumplimiento de lo preceptuado en dicha resolución.
Cada administración estará facultada para controlar el uso del correo electrónico en dependencia de la política que ella misma determine para su uso, según las prerrogativas que el Reglamento de Seguridad Informática le brinda de crear su propia política de seguridad.
Por medio de la Resolución 64 de 2002 se crea la Oficina de Seguridad para las Redes Informáticas subordinada al Ministerio de la Informática y las Comunicaciones.
No obstante, la legislación informática vigente, las condiciones de desarrollo informático en nuestro país aconsejan centrar nuestros esfuerzos en la revisión legislativa de nuestro ordenamiento jurídico vigente para adecuar siempre que sea posible y establecer las disposiciones jurídicas que reconozcan y tutelen el derecho a la protección de la información personal.

4. CONCLUSIONES

En Cuba cada día se hacen más visibles los cambios ocasionados por la expansión de las nuevas tecnologías, manifestados en la utilización de computadoras, teléfonos celulares, correos electrónicos y sistemas de navegación. Estas razones indican la importancia de garantizar el equilibrio entre modernización y garantía de los derechos ciudadanos.

El derecho a la protección de datos personales constituye un derecho autónomo que nació como una mera contraposición a la interferencia en la vida privada de las personas facilitada por el avance tecnológico, que consiste en el reconocimiento y establecimiento de prerrogativas, principios y procedimientos para el tratamiento por parte del Estado o de terceros, de la información concerniente a personas físicas.

El ordenamiento jurídico cubano carece de un reconocimiento expreso del derecho a la protección de datos personales, por consiguiente se adolece de mecanismos o vías para su protección, solo a nivel administrativo en este caso fundamentalmente por el Ministerio de la Informática y las Comunicaciones encontramos algunas alternativas de tutela a la información personal.

BIBLIOGRAFÍA

Aparicio Solón, J. (2002). *Estudio sobre la Ley Orgánica de Protección de Datos.* Navarra: Editorial Aranzadi.

Corripio Gil-Delgado, R., Fernández Aller, C. (1998). **"**Protección de datos personales y telecomunicaciones: análisis de los conceptos básicos". *Encuentros Informática y Derecho 1998,* Universidad Pontificia Comillas, Madrid: Editorial Aranzadi.

Freixas Gutiérrez, G. (2001). La *protección de datos de carácter personal en el derecho español.* Barcelona: Editorial Bosch.

García-Berrío Hernández, T. (2003). *Informática y Libertades. La protección de datos personales y su regulación en Francia y España.* Colección Estudios de Derecho, Universidad de Murcia.

Garriga Domínguez, A. (2004). *Tratamiento de datos personales y derechos fundamentales* Madrid: Editorial Dykinson.

Gozaíni, Osvaldo A. (2001). *Hábeas data. Protección de datos personales.* Argentina: Rubinzal-Culzoni Editores.

Gullón Ballesteros y otros. (2001). Protección de datos de carácter personal. Legislación y *Jurisprudencia.* Madrid: Editorial Práctica del Derecho.

Jareño Leal, A. (2008). *Intimidad e imagen: Los límites de la protección penal*. Madrid: Closas-Orcoyen, S.L.

Murillo De La Cueva, P.L. (1993). "La protección de los datos personales ante el uso de la Informática en el Derecho español*"*. *Estudios de jurisprudencia COLEX,* nº4, enero-febrero.

Pérez Luño, A.E. (1996). Manual de Informática y Derecho. Barcelona: Ariel.

Piccimelli, Ó. (1999). El habeas data en Latinoamérica. Santa Fe de Bogotá. Colombia: Temis.

Legislación Utilizada:

Constitución de la República de Cuba, Ministerio de Justicia, La Habana, 2005.

Concesión Administrativa de ETECSA. Decreto 275 del Comité Ejecutivo del Consejo de Ministros.

Manual de Operaciones Comerciales de ETECSA.

Metodología para la elaboración del Plan de Seguridad Informática.

Resolución 127 del 2007 del Ministerio de Informática y las Comunicaciones. Reglamento de Seguridad para las Tecnologías de la Información.

Resolución 139 de 2005, Procedimiento para la autorización de acceso a Internet. Disponible en: http://www.informatica-juridica.com/legislacion/cuba.asp.

Resolución 180 de 2003, Normas que limitan el acceso a Internet. Disponible en: http://www.informatica-juridica.com/legislacion/cuba.asp.
Resolución 23 de 2000, Inscripción de redes privadas. Disponible en: http://www.informatica-juridica.com/legislacion/cuba.asp.
Resolución 3 del 2007. Reglamento Disciplinario Interno de ETECSA.
Resolución 65 de 2003 Red privada de datos. Disponible en: http://www.informaticajuridica.com/legislacion/cuba.asp.

NOTAS

1. Araujo Carranza, E. 2009. *El derecho a la información y la protección de datos personales en el contexto general y su construcción teórica y jurídica.* Problemática Jurídicas Contemporáneas. Revista del Instituto de Ciencias Jurídicas de Puebla, Editorial Nueva Época, Puebla, México, P. 174
2. STC 254 de 1993: fue la primera en reconocer la existencia de tal derecho fundamental. Sentencia 143 de Mayo 9 de 1998: número de identificación tributaria: es contra la ley y contra el derecho de asociación en sindicatos libres la utilización de la información personal del sindicato para conceder descuentos u otros beneficios. Sentencia de Noviembre 8 de 1999: acerca del diagnóstico médico y del consentimiento del trabajador; Sentencias 290 y 292 del 2000, contra la anterior Ley española de Protección de Datos Ley Orgánica de Tratamiento Automatizado de Datos (LORTAD): existe un derecho fundamental de libertad informática. Disponible en: http://www.tribunalconstitucional.es/STC2000/STC2000-290.html y http://www.tribunalconstitucional.es/STC2000/STC2000-292.html
3. Sánchez Chirino, A. (2002). *El recurso del habeas data como forma de tutela de la persona frente al tratamiento de sus datos personales. El caso de Costa Rica.* IX Congreso Iberoamericano de Derecho e Informática "Justicia e Internet". Disponible en: http://www.hesscr.com/secciones/cursos/uned/dersfund/chirino.doc
4. Delgado Triana, Y. (2007). Protección en el Ordenamiento Jurídico cubano de los Derechos Inherentes a la personalidad en la esfera moral. Tesis en opción al grado de Doctor en Ciencias Jurídicas, La Habana, Cuba.
5. El término Seguridad de las Tecnologías de la Información está relacionado con la confidencialidad, integridad y disponibilidad de la información tratada por los ordenadores y las redes de datos. Regulado en Artículo 2. Reglamento de Seguridad para las Tecnologías de la Información.
6. Artículo 1. Reglamento de Seguridad para las Tecnologías de la Información. El presente Reglamento tiene por objeto establecer los requerimientos que rigen la seguridad de las tecnologías de la información y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país. Este Reglamento no sustituye las medidas específicas que norman el procesamiento de la información clasificada y limitada, que son objeto de normativas emitidas por el Ministerio del Interior.
7. Artículo 4. Reglamento de Seguridad para las Tecnologías de la Información. Cada entidad que haga uso para el desempeño de su actividad de las tecnologías de la información está en la obligación de diseñar, implantar y mantener actualizado, un Sistema de Seguridad Informática a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos, con el fin de alcanzar los siguientes objetivos:

- Minimizar los riesgos sobre los sistemas informáticos.
- Garantizar la continuidad de los procesos informáticos.

8. Artículo 6. Reglamento de Seguridad para las Tecnologías de la Información. El diseño del Sistema de Seguridad Informática y la elaboración del Plan de Seguridad Informática de cada entidad se realizarán en correspondencia con las metodologías establecidas al respecto por la Oficina de Seguridad para las Redes Informáticas, adscripta al Ministerio de la Informática y las Comunicaciones.
9. Artículo 9 inciso f). Reglamento de Seguridad para las Tecnologías de la Información. Los jefes a las diferentes instancias en los órganos, organismos y entidades responden por la protección de los bienes informáticos que le han sido asignados y tienen las siguientes obligaciones: Imponer o proponer sanciones ante violaciones del Sistema de Seguridad, en correspondencia con su naturaleza y con los daños ocasionados.
10. Artículo 12 inciso e). Reglamento de Seguridad para las Tecnologías de la Información. Los usuarios de las tecnologías de información en órganos, organismos y entidades tienen las siguientes obligaciones: Proteger las tecnologías o la terminal de red que le ha sido asignada y colaborar en la protección de cualquier otra, para evitar que sea robada o dañada, usada la información que contiene o utilizado de manera impropia el sistema al que esté conectada.
11. Artículo 36. Reglamento de Seguridad para las Tecnologías de la Información. Todas las tecnologías de información, independientemente de su importancia, se protegerán contra alteraciones o sustracciones, ya sea de éstas o sus componentes, así como de la información que contienen.
12. Artículo 44 inciso a). Reglamento de Seguridad para las Tecnologías de la Información. Las acciones para cubrir las brechas de seguridad y la corrección de los errores del sistema deberán estar minuciosamente controladas en cada entidad. Los procedimientos deberán asegurar que: solo el personal claramente identificado y autorizado tenga acceso a sistemas en funcionamiento y a los datos.
13. Artículo 68 inciso d). Reglamento de Seguridad para las Tecnologías de la Información. Las entidades autorizadas oficialmente para la comprobación de la seguridad de las redes de otras entidades están en la obligación de: Abstenerse de la utilización del conocimiento obtenido sobre la red comprobada en beneficio propio.
14. Artículo 80. Reglamento de Seguridad para las Tecnologías de la Información. Ninguna persona natural o jurídica está autorizada para enviar mensajes de correo electrónico no solicitados a múltiples usuarios de forma indiscriminada (spam), ya sean de carácter informativo, comercial, cultural, social, con intenciones de engaño (hoax) u otros.
15. Artículo 79. Reglamento de Seguridad para las Tecnologías de la Información. Se prohíbe la difusión a través de las redes públicas de transmisión de datos de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas; o que lesione la Seguridad Nacional, por cualquier persona natural o jurídica.
16. Artículo 85. Reglamento de Seguridad para las Tecnologías de la Información. El acceso no autorizado o la agresión a cualquier sistema de cómputo conectado a las redes públicas de transmisión de datos y la usurpación de los derechos de acceso

de usuarios debidamente autorizados se consideran violaciones del presente Reglamento, independientemente de otras implicaciones legales que puedan derivarse de estas acciones.

17. Artículo 84. Reglamento de Seguridad para las Tecnologías de la Información. Ninguna persona, natural o jurídica está autorizada para explorar o monitorear las redes públicas de transmisión de datos en busca de vulnerabilidades o información sobre los usuarios legales de las mismas.
18. Entre los servicios que se ofrecen se encuentra el Servicio telefónico básico, nacional e internacional; Servicio de conducción de señales, nacional e internacional; Servicio de transmisión de datos, nacional e internacional; Servicio de telex, nacional e internacional; Servicio de cabinas telefónicas públicas; Servicio de telecomunicaciones de valor agregado; Servicios de radiocomunicación móvil troncalizada.
19. Artículo 31.Secreto de las telecomunicaciones. Concesión Administrativa. Decreto 275. ETECSA debe cuidar del secreto de la información proporcionada por los usuarios o trasmitida o generada por las redes públicas al prestar sus servicios y a no divulgarla si no existe consentimiento previo de estos, tomando todas las medidas conducentes a este fin. El Órgano Regulador vigilará el cumplimiento de esta obligación.
20. Artículo 3 inciso h) y q). Resolución 3 del 2007. Reglamento Disciplinario Interno de ETECSA. Constituyen obligaciones comunes para todos los trabajadores, las siguientes: h) observar la estricta discreción con respecto a las labores que realiza y a los documentos e informaciones que utiliza en el desempeño de su trabajo, no divulgando su contenido sin la autorización correspondiente; q) cumplir estrictamente las normas de inviolabilidad de las comunicaciones, no escuchando o divulgando su contenido, así como no hacer uso de este dentro o fuera de su puesto de trabajo.
21. Artículo 4 inciso e). Resolución 3 del 2007. Reglamento Disciplinario Interno de ETECSA. Constituyen prohibiciones comunes para todos los trabajadores, las siguientes: revelar a personas no autorizadas, cualquier información que reciba o conozca en razón de su cargo.
22. Artículo 5. Resolución 3 del 2007. Reglamento Disciplinario Interno de ETECSA. Se consideran violaciones de la disciplina laboral, además de las establecidas en el Decreto Ley No. 176 de 15 de agosto de 1997 o en su caso en la legislación específica, el incumplimiento de las obligaciones y prohibiciones contenidas en el presente Reglamento Disciplinario Interno; el incumplimiento de las regulaciones contenidas en los Capítulos II, III, VI, VIII y IX, todos del Reglamento Ramal del Ministerio de la Informática y las Comunicaciones, así como el incumplimiento de lo establecido en el Contrato de Trabajo, en el Convenio Colectivo de Trabajo y demás disposiciones que reglamenten las relaciones laborales de la empresa.
23. Red Privada de Datos es aquella red situada en una misma o en distintas localidades geográficas e interconectadas entre sí por enlaces de telecomunicaciones, establecida y operada por una persona jurídica para satisfacer sus necesidades propias de transmisión de datos, no pudiendo prestar estos servicios a terceros, aunque podrá solicitar interconexión con la Red Pública de Transmisión de Datos.