Transparencia vs. privacidad en el acceso y transferencia de información

Nayibe Chacón Gómez*

SUMARIO: I. Presentación y delimitación del tema. II. Contenido y alcance del Decreto No. 9.051, mediante el cual se dicta el Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado. III. La protección de la privacidad de los datos, información y documentos de los particulares que se encuentran en los órganos y entes del Estado. IV. Conclusiones.

Resumen

El término "transparencia" es utilizado especialmente para referirse a la necesidad que tienen los ciudadanos de conocer la gestión de la Administración Pública, principalmente en cuanto al uso que se hace de los recursos del Estado. La privacidad de la información es un derecho que tienen los ciudadanos frente a los demás ciudadanos y frente a los órganos y entes del Estado. En este trabajo, se analizan estos dos términos a la luz del Decreto venezolano con rango, valor y fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado.

Palabras clave: Privacidad de la información. Transparencia. *Open Data*. Interoperabilidad.

Abstract

The term "transparency" is used especially to refer to the citizen's need of knowing the management of the Public Administration, principally for the use that is done of the resources of the State. Information privacy is a right that the citizens have, with regards to other citizens and to the entities of the State. These two terms are analyzed in this paper under Venezuelan "Decreto con rango, valor y fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado".

Keywords: Privacy of the information. Transparency. Open Data. Interoperability.

Recibido: 4/11/2013 • Aceptado: 16/1/2014

* Profesor Asociado de la Facultad de Ciencias Jurídicas y Políticas. Universidad Central de Venezuela. nayibe.chacon@ucv.ve

I. Presentación y delimitación del tema

En Venezuela, las Tecnologías de Información y Comunicación (TIC) han revestido no solamente el carácter de hecho social[1] sino también se han agregado al catálogo de derechos de los ciudadanos. En la Constitución de la República Bolivariana de Venezuela del año 1999, se incorporaron normas sobre el empleo de las TIC como herramientas para el desarrollo del país.

Desde la promulgación de estas normas constitucionales y su proyección en la legislación nacional, el actual Ministerio del Poder Popular para la Ciencia y Tecnología ha sido el encargado de delinear la implementación de las TIC en todos los ámbitos nacionales, aunque no se encuentra solo en esta tarea de creación e implementación del *gobierno electrónico*[2] venezolano.

El 15 de junio de 2012 apareció publicado en la Gaceta Oficial de la República Bolivariana de Venezuela No. 39.945 el Decreto No. 9.051 el Decreto con

1 El empleo en todos los ámbitos de nuestra vida de los medios electrónicos, han dado lugar a que nuestra sociedad sea conocida como una "Sociedad de la Información y del Conocimiento", la cual conjuga por una parte, el concepto de Sociedad, y por otra parte, el concepto y alcance de las Tecnologías de Información y Comunicación. Por "sociedad", puede entenderse en el concepto tradicional citando a Rafael Gamboa, como la integración de "una serie de individuos, quienes reunidos en mismo espacio, acuerdan someterse a una serie de normas y, a cambio, obtendrán una serie de derechos. En este concepto de sociedad tradicional, unos son los que gobiernan, y otros son los gobernados". Y el autor Anthony Giddens, escribe en su obra *Sociología*, que sociedad «es un sistema de interrelaciones que conecta a los individuos entre sí". Por otro lado, las Tecnologías de Información y Comunicación se han definido "como sistemas tecnológicos mediante los que se recibe, manipula y procesa información, y que facilitan la comunicación entre dos o más interlocutores…las Tecnologías de Información y Comunicación son algo más que informática y computadoras, puesto que no funcionan como sistemas aislados, sino en conexión con otras mediante una red". GAMBOA BERNATE, Rafael Hernando: "Soberanía estatal en Internet; análisis desde la perspectiva de conflictos de jurisdicción y competencia en el plano nacional e internacional" en *Comercio Electrónico*, Legis Editores, S.A, Bogotá, 2005, p. 635. GIDDENS, Anthony. *Sociología*, Alianza Editorial, Tercera Reimpresión de la Segunda Edición, Madrid, 1997. Naciones Unidas, Comisión Económica Para América Latina y El Caribe – CEPAL. *Los Caminos hacia una Sociedad de la Información en América Latina y el Caribe*, Conferencia Ministerial Regional Preparatoria de América Latina y el Caribe para la Cumbre Mundial de la Sociedad de la Información. Bávaro, Punta Cana, República Dominicana, 29 al 31 de enero de 2003, p. 3.

2 A lo largo de esta investigación se citan otras definiciones de gobierno electrónico, no obstante, resulta oportuno anotar en esta presentación el concepto esclarecedor y descriptivo de la Prof. Mariliana Rico Carrillo, "*Cuando hablamos de gobierno electrónico, (e-goverment en terminología anglosajona) nos referimos a la utilización de las TIC, en particular de Internet, en los diferentes sectores del ámbito gubernamental como elemento de modernización de la gestión administrativa, que permite mejorar la prestación de servicios y facilita el contacto directo con los ciudadanos, a través de canales de comunicación que potencian su participación en el sector público*". RICO CARRILLO, Mariliana: "Las Tecnologías de las Información y Comunicación en la actividad gubernamental: gobierno electrónico y participación ciudadana", en: *Ciudadanas 2020 El Gobierno de la Información*, Instituto Chileno de Derecho y Tecnologías. Federación Iberoamericana de Derecho Informático (FIADI), Chile, 2011, pp. 208-209.

Rango, Valor y Fuerza de *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado,* el cual entró en vigencia el 15 de junio de 2014, fecha en que se venció el plazo de dos años contado a partir de dicha publicación en la Gaceta Oficial[3].

El objeto de este Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado* se encuentra consagrado en el artículo 1° en los siguientes términos: "*establecer las bases y principios que regirá el acceso e intercambio electrónico de datos, información y documentos entre los órganos y entes del Estado*[4]*, con el fin de garantizar la implementación de un estándar de interoperabilidad*", misión que intenta cubrir en 65 artículos, 4 disposiciones finales y 3 disposiciones transitorias.

En vista de que la presente investigación no podrá abarcar el conjunto de artículos, disposiciones finales y transitorias con que cuenta el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado,* nos dedicaremos al estudio de la relación existente entre "la obligación que tienen los *órganos y entes del Estado a permitir el acceso e intercambio electrónico de datos, información y documentos*" y "*el derecho que tienen los ciudadanos a la protección de la privacidad*", específicamente en atención a la información personal de los particulares que se encuentra en posesión de estos órganos y entes del Estado en calidad de autores de la misma; es decir, datos que han sido generados por órganos y entes del Estados sobre la base de la información aportada por los ciudadanos.

3 *Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes,* Disposición Final Cuarta. "*El presente Decreto entrará en vigencia vencido el plazo de dos años contado a partir de la publicación del presente Decreto con Rango, Valor y Fuerza de Ley en la Gaceta Oficial de la República Bolivariana de Venezuela*".

4 Según el artículo 2° del *Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes,* estos "*órganos y entes del Estado*", son: 1. Los órganos del Poder Público Nacional, Estadal y Municipal. 2. Los institutos públicos nacionales, estadales, distritales y municipales. 3. El Banco Central de Venezuela. 4. Las Universidades públicas nacionales autónomas y experimentales, así como cualquier otra institución del sector universitario de naturaleza pública. 5. Las demás personas de derecho público nacionales, estadales, distritales y municipales. 6. Las sociedades de cualquier naturaleza en las cuales las personas a que se refieren los numerales anteriores tengan una participación en su capital social superior al cincuenta por ciento (50%), las que se constituyan con la participación de aquellas, o que a través de otro mecanismo jurídico, tengan el control de sus decisiones. 7. Las fundaciones y asociaciones civiles y demás instituciones creadas con fondos públicos, o que sean dirigidas por las personas a que se refieren los numerales anteriores, o en las cuales tales personas designen sus autoridades, o cuando los aportes presupuestarios o contribuciones efectuados en un ejercicio, por una o varias de las personas a que se refieren los numerales anteriores, representen el cincuenta por ciento (50%) o más de su presupuesto. 8. Los demás entes de carácter público.

II. Contenido y alcance del Decreto No. 9.051, mediante el cual se dicta el Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado

Resulta necesario considerar el núcleo del Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, el cual se encuentra en la "*implementación de un estándar de interoperabilidad*"; es decir, la creación y puesta en marcha de especificaciones técnicas, aceptadas por la industria, que permitirá a los órganos y entes del Estado el intercambio por medios electrónicos de datos, información y documentos de acceso público.

Cuando se habla de *interoperabilidad*, se hace referencia a la necesidad que tiene la Administración Pública de compartir e intercambiar información de los procedimientos que son realizados o llevados en cada una de sus dependencias, de conformidad con su propia naturaleza.

En opinión de la autora Yarina Amoroso Fernández:

> La interoperabilidad dentro del Estado es hoy en día un nudo operacional si se quiere mejorar su eficiencia. Existen factores que impulsan o aletargan implementar un sistema de interoperabilidad, con capacidad para usar datos u orquestar funcionalidades con otro sistema o proceso adhiriendo estándares comunes[5].

Continua la citada autora destacando que la planificación de la *interoperabilidad* forma parte de las políticas públicas y que debe emanar de la confianza a las instituciones públicas a modo de poder gestionar adecuadamente los procesos del Estado.

Así la *interoperabilidad* entre los distintos órganos y entes del Estado que permita el acceso o la transmisión de datos, información y documentos se presenta como el elemento imprescindible del llamado *Open Data*; es decir, del

> …compromiso del Estado de exponer los datos públicos que obran en su poder de forma reutilizable, con el fin de optimizar el uso de la información pública en función de un mejor servicio a la ciudadanía y una mejor gestión de gobierno así como que terceros puedan crear servicios derivados de los mismos datos[6].

5 AMOROSO FERNANDEZ, Yarina. "Open Data: una contribución necesaria al gobierno electrónico y la sociedad del conocimiento", en: *Ciudadanas 2020 El Gobierno de la Información.* Instituto Chileno de Derecho y Tecnologías. Federación Iberoamericana de Derecho Informático (FIADI), Chile, 2011, p. 15.

6 AMOROSO FERNANDEZ, Yarina. "Open Data:…", *ob. cit*., p. 11.

En el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado* se estructura la *Plataforma Nacional de Servicios de Información Interoperables*; es decir, una plataforma tecnológica que busca el cumplimiento de la obligación que tienen los órganos y entes del Estado de implementar servicios de información interoperables, a fin de permitir el acceso e intercambio electrónico de datos, información y documentos, a cualquier órgano y ente del Estado que lo requiera.

El desarrollo, operación, mantenimiento y administración de dicha plataforma se encuentra a cargo del *Operador de la Interoperabilidad*, ente cuya finalidad es la de estandarizar, formalizar, integrar, reutilizar y compartir, por medios electrónicos, entre los órganos y entes del Estado, los datos, información y documentos que éstos poseen conforme a sus atribuciones, de acuerdo al principio de unidad orgánica y demás principios aplicables a la interoperabilidad[7].

El *Operador de la Interoperabilidad* forma parte del "*Comité Nacional de Interoperabilidad*"[8], el cual es dependiente administrativamente de la Vicepresidencia Ejecutiva, y es el encargado de "*establecer y coordinar la aplicación de los principios y políticas para el acceso e intercambio electrónico de datos, información y documentos entre los distintos órganos y entes del Estado*"[9].

A tenor del contenido del Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, la *interoperabilidad* es una herramienta que garantiza el desarrollo de los servicios públicos integrados y transparentes, así como, la simplificación de los trámites administrativos que sus órganos y entes ejecutan en atención a los requerimientos de los ciudadanos, en pro de la satisfacción de sus necesidades y mejora de las relaciones de éstos con el Estado, en tal sentido la *interoperabilidad* se presenta como de "interés público", y como uno de los elementos necesarios para el desarrollo de los cometidos del *gobierno electrónico*[10] en Venezuela.

7 Artículos 18 y ss., del Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado.

8 El Comité Nacional de Interoperabilidad se encuentra conformado por: 1. La Vicepresidencia Ejecutiva de la República, quien lo preside. 2. El Consejo Federal de Gobierno. 3. El Ministerio del Poder Popular con competencia en planificación. 4. El Ministerio del Poder Popular con competencia en tecnologías e información. 5. La Procuraduría General de la República. 6. La Asamblea Nacional. 7. El Tribunal Supremo de Justicia. 8. El Consejo Nacional Electoral. 9. El Consejo Moral Republicano. 10. El Banco Central de Venezuela. 11. El Operador de la Interoperabilidad.

9 Artículos 14 y ss., del Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado.

10 Las expresiones "Gobierno electrónico" y "Administración Electrónica" son definidas en la Carta Iberoamericana como sinónimas, ambas consideradas como el uso de las TIC en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos,

Así, la *interoperabilidad* busca apoyar la función y gestión pública que desarrollan los órganos y entes del Estado, garantizando la cooperación y colaboración requerida para proporcionar servicios y procesos públicos integrados complementarios y transparentes, con el empleo de licencias tecnologías de propiedad abierta, que haría posible la reutilización de los datos, información y documentos generados, sobre la base del principio de la unidad orgánica de las instituciones que conforman la Administración Pública; es decir, la integración de éstas, que permitan alcanzar el máximo provecho de la función pública, en beneficio de los ciudadanos.

Debemos tener presente que en Venezuela desde la entrada en vigencia del Decreto No. 3.390 de fecha 23 de diciembre de 2004, publicado en la Gaceta Oficial No. 38.095 de fecha 28 de diciembre del mismo año, conocido como el "*Decreto del Software Libre*", se estableció como una obligación de la Administración Pública venezolana la utilización de programas de computación cuya licencia garantiza al usuario acceso al código fuente del programa y lo autoriza a ejecutarlo con cualquier propósito, modificarlo y redistribuir tanto el programa original como sus modificaciones en las mismas condiciones de licenciamiento acordadas al programa original, sin tener que pagar regalías a los desarrolladores previos.

En el artículo 1° de este *Decreto del Software Libre* se establece*: "La Administración Pública Nacional empleará prioritariamente Software Libre desarrollado con Estándares Abiertos, en sus sistemas, proyectos y servicios informáticos. A tales fines, todos los órganos y entes de la Administración Pública Nacional iniciarán los procesos de migración gradual y progresiva de éstos hacia el Software Libre desarrollado con Estándares Abiertos*". La justificación del empleo prioritario del Software Libre en la Administración Pública venezolana, ha sido descrita en los siguientes términos: "Dada la alta demanda y calidad de las habilidades en TI, el software que adquiere el Gobierno debe: a) ser predecible en su comportamiento y *performance*; b) tener un costo razonable de mantenimiento; c) ser de razonable esfuerzo para Integrarlo, evolucionarlo, adaptarlo; y, d) ser seguro"[11].

De igual manera, resulta meridianamente claro que actualmente los órganos y entes del Estado venezolano se encuentran inmersos en un proceso de digitalización y automatización de sus procedimientos, cuestión de la que se

orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos. Todo ello, sin perjuicio de las denominaciones establecidas en las legislaciones nacionales.

11 BERRIZBEITIA, Jorge. Políticas de uso de Software Libre en el Sector Público Venezolano. Centro Nacional de Tecnologías de Información (CNTI), [En línea]. [Citado: 27. Enero. 2005, Disponible en: http://www.cnti.gob.ve/cnti_docmgr/sharedfiles/Politicas_Uso_Software_Libre_Sector_Publico_Vzla.pdf

derivan consecuencias de diversa índole, tanto desde la perspectiva del ciudadano como de la perspectiva de la misma Administración[12].

Por otra parte, resulta oportuno anotar que, no obstante, la consagración en el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, del derecho que tienen todos los ciudadanos de estar informados de manera oportuna, adecuada y efectiva sobre los servicios desarrollados por el Estado para la eficaz y eficiente prestación de los mismos[13], y que en el texto del mencionado Decreto-ley se utilice la palabra "*transparencia*", no se refiere al derecho constitucional que tienen los ciudadanos al acceso a los archivos y registros administrativos, que se traduce en la obligación del Estado de poner a la disposición de los ciudadanos dicha información, conservando los límites aceptables dentro de una sociedad democrática en materias relativas a seguridad interior y exterior, a investigación criminal y a la intimidad de la vida privada, de conformidad con la ley que regule la materia de clasificación de documentos de contenido confidencial o secreto, de conformidad con lo establecido en el artículo 143[14] de la Constitución de la República Bolivariana de Venezuela[15].

12 "La utilización de las nuevas tecnologías en la actividad administrativa supone un cambio de paradigma de gran trascendencia, en primer lugar, para el ciudadano. La implantación de la Administración electrónica ofrece la posibilidad de ejercer vía *online*, durante las 24 horas del día, todos los días del año y sin limitaciones geográficas, el catálogo de derechos del que tradicionalmente ha sido titular, según la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante LRJAP-PAC). Sin ánimo de ser exhaustivos: el derecho al conocimiento sobre el estado de la tramitación de los procedimientos en los que ostente la calidad de interesado, el derecho a la obtención de copias electrónicas de los documentos que obren en el expediente, el derecho a formular alegaciones y a aportar documentos en cualquier fase del procedimiento, son algunos de los mencionados derechos". ALAMILLO, Ignacio y Erika Henao Hoyos. "La gestión electrónica de la identidad y de la firma electrónica en el intercambio electrónico de datos entre Administraciones Públicas", [En línea]. AR: *Revista de Derecho Informático* No. 121 - Agosto del 2008. Disponible en: http://www.buscalegis.ufsc.br/revistas/files/anexos/29615-29631-1-PB.pdf

13 Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado, artículo 8°.- "*Las Oficinas de Atención al Ciudadano de los órganos y entes del Estado, deberán suministrar y ofrecer a los ciudadanos, de forma oportuna, adecuada y efectiva; información sobre los servicios desarrollados por el Estado para la eficaz y eficiente prestación de sus servicios*". **Y artículo 9**°.- "*Los ciudadanos, en forma individual o colectiva, directa, por medios de sus representantes o a través de la comunidad organizada; podrán presentar física o electrónicamente ante las Oficinas de Atención al Ciudadano de los organismos y entes del Estado; peticiones, sugerencias, reclamos, quejas o denuncias en la prestación de servicios públicos o por la irregularidad de la actuación de los servidores públicos en los términos de ésta y otras leyes aplicables*".

14 Constitución de la República Bolivariana de Venezuela, artículo 143.- "*Los ciudadanos y ciudadanas tienen derecho a ser informados e informadas oportuna y verazmente por la Administración Pública, sobre el estado de las actuaciones en que estén directamente interesados e interesadas, y a conocer las resoluciones definitivas que se adopten sobre el particular. Asimismo,* ***tienen acceso a los archivos y registros administrativos, sin perjuicio de los límites aceptables dentro de una sociedad democrática en materias relativas a seguridad interior y exterior, a***

En el contexto de la citada norma constitucional y como función del gobierno electrónico y del *Open Data*, la *transparencia* debe ser entendida como

> …el ejercicio de solicitar y entregar la información. Formar una cultura de transparencia es que las autoridades rindan cuentas a los gobernados de las decisiones que realizan en la función pública y crear una cultura ciudadana de participación, respeto y ejercicio del derecho de acceso a la información pública[16].

Dicha actuación de la Administración Pública, a tenor de lo establecido en la *Carta Iberoamericana de Gobierno Electrónico*, se encuentra fundamentada en el "*Principio de transparencia y accesibilidad*", según el cual se garantiza que la información de las Administraciones Públicas y el conocimiento de los servicios por medios electrónicos se haga en un lenguaje comprensible según el perfil del destinatario.

Por el contrario, como se ha mencionado, este novedoso Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, sólo atiende a la necesidad de crear la *Plataforma Nacional de Servicios de Información Interoperables*; es decir, el acceso y transmisión de datos, información y documentos entre los órganos y entes del Estado.

investigación criminal y a la intimidad de la vida privada, de conformidad con la ley que regule la materia de clasificación de documentos de contenido confidencial o secreto. *No se permitirá censura alguna a los funcionarios públicos o funcionarias públicas que informen sobre asuntos bajo su responsabilidad*". (Destacados nuestros).

15 La situación de la *transparencia* de las actividades de las dependencias de la Administración Pública en Venezuela ha sido descrito por Mercedes De Freitas en su trabajo titulado: "El acceso a la información pública en Venezuela. Transparencia vs. Opacidad", donde se destacan las siguientes percepciones: "*Identificamos un problema grave de acceso, veracidad, oportunidad e inexistencia de la información en poder de una gran parte de las instancias del Estado venezolano. Y nos referimos no sólo a información militar o de seguridad del Estado. Carecemos de información de uso común en cualquier Estado democrático, por ejemplo, sobre el presupuesto, la inversión en programas sociales, sus responsables y objetivos, entre otros puntos. Carecemos de la información sobre muchos datos e indicadores y existe desconfianza de otros, como los indicadores de mortalidad infantil y mortalidad materna, pues la data no concuerda con otros registros. La información sobre los sueldos de los funcionarios públicos se considera confidencial en Venezuela… El bloqueo a la información pública toma formas diversas en Venezuela. Una de ellas es negar el acceso a las fuentes*". La autora reconoce que en las Oficinas de Atención al Ciudadano, particularmente de la Contraloría General de la República, existía desde antes de la publicación del Decreto Ley bajo análisis, la posibilidad de realizar denuncias contra funcionarios o procesos, pero en ningún caso se contemplaba el acceso para los ciudadanos a la información actualizada de los asuntos llevados por ese órgano, menos aun "*sobre la utilización de los bienes y el gasto de los recursos que integran el patrimonio público, y cuya administración le corresponde*". DE FREITAS, Mercedes. *El acceso a la información pública en Venezuela. Transparencia vs. Opacidad,* Editorial CEC, S.A., primera edición, Caracas, 2010, pp. 29-31.

16 GARCÍA BARRERA, Mirna. "La información pública es de todos", en: *Ciudadanas 2020 El Gobierno de la Información*, Instituto Chileno de Derecho y Tecnologías, Federación Iberoamericana de Derecho Informático (FIADI), Chile, 2011, p. 79.

En materia de acceso a la información pública y transparencia, la autora Mercedes De Freitas se refiere, de manera muy precisa, al hecho que en fecha 26 de octubre de 2008, la Coalición ProAcceso intentó, sin éxito, entregar una propuesta de Ley de Acceso a la Información Pública a la Comisión de Ciencias, Tecnología y Medios de Comunicación de la Asamblea Nacional venezolana[17].

Con la publicación del Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado* no podemos decir que se haya cumplido con la tarea de crear un marco normativo que permita el acceso a la información pública y como consecuencia la *transparencia* de la gestión de la Administración Pública; sin embargo, su implementación se presenta como un paso para la articulación entre los órganos y entes del Estado, que permita dar cumplimiento a los mandatos constitucionales.

III. La protección de la privacidad de los datos, información y documentos de los particulares que se encuentran en los órganos y entes del Estado

Hechas las anteriores precisiones sobre el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, lo siguiente en que puedo pensar es en algo que leí de un artículo escrito en el año 2004 por un autor español:

> …las Nuevas Tecnologías pueden facilitar muchos trámites administrativos y mejorar la gestión de los servicios públicos, pero también deben tenerse en cuenta las consecuencias que conlleva que cualquier Administración tenga acceso a datos que, en principio, no les corresponde conocer[18].

El autor de la noticia jurídico-informática continuaba en los siguientes términos:

> Puede parecer algo alarmista, pero lo cierto es que muchas veces no somos conscientes del control y la vigilancia a la que estamos o podemos estar sometidos, ni de la importancia que tiene el derecho a la *autodeterminación informativa*, que puede ser definido como la facultad de ejercer el control sobre los datos referentes a nuestra persona contenidos en ficheros o registros públicos o privados, normalmente procesados por medio de dispositivos informáticos. A parte de los conocidos derechos que confiere en relación con dichos ficheros (acceso, rectificación o cancelación) y el de oposición al tratamiento de los datos, la Ley Orgánica de Protección de Datos establece el derecho a la impugnación de valoraciones o decisiones "*cuyo único fundamento*

17 DE FREITAS, Mercedes. *El acceso a la información…, ob. cit*., p. 31.

18 PRENAFETA RODRÍGUEZ, Javier. "La privacidad en el gobierno electrónico y el DNI digital", [En línea], Noticias Jurídicas, Marzo, 2004. Disponible en: http://noticias.juridicas.com/articulos/20-Derecho%20Informatico/200403-305591621042750.html

> *sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad*". Este derecho, que tan poco se ejerce –el requerimiento de *único* es difícil de apreciar en la práctica–, permite realizar la autodeterminación informativa en su plenitud, ya que, tan importante como conocer quién tiene nuestros datos, qué datos de gestionan o lo que se ha hecho con ellos, es poder intervenir en las decisiones que se tomen basándose en dicho tratamiento[19].

En el caso venezolano, la cuestión de los datos o la información personal es más delicada aun, toda vez que nosotros no tenemos una legislación especifica en materia de protección de datos personales que son creados, administrados, almacenados, intercambiados y transmitidos por medios electrónicos.

En el sistema de interoperabilidad contemplado en el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, la legitimación subjetiva para solicitar y obtener el acceso a los datos de una persona que se encuentren en los órganos y entes del Estado sólo le corresponde a dichos órganos y entes del Estado, de forma que el administrado no actúa en el procedimiento de intercambio; según lo consagrado en el marco legal, la actuación se establece entre las instituciones de la Administración Pública, que tratan a la información de los ciudadanos como un objeto sobre el cual versa el intercambio de datos.

> En otras palabras, el ciudadano se encuentra inmerso en la lógica de actuación Administración-Administración, lo que se traduce en su poca capacidad de decisión y de gestión sobre sus propios datos. Pareciera entonces que el modelo hubiera sido creado para responder a las necesidades de acceso de las Administraciones a los datos de los ciudadanos (…) el hecho de que la cesión del dato se base en la presunción de que la Administración requirente efectivamente cuenta con el consentimiento del administrado hace que puedan resultar vulnerados derechos como el derecho fundamental a la protección de datos personales[20].

En opinión de Yarina Amoroso Fernández, el ciudadano se presenta como el "eje central" de todo el proceso de *interoperabilidad*, ya que es a él a quien va dirigida la eficiencia en la ejecución de la función pública.

> Este es el concepto base, cuando se trata de conceptualizar el Gobierno electrónico, los ciudadanos ya no son un elemento más dentro de los procedimientos administrativos o jurídicos. El ciudadano tiene que ser considerado como centro en cualquier solución que se piense[21].

19 PRENAFETA RODRÍGUEZ, Javier. "La privacidad en el Gobierno…", *ob. cit.*
20 ALAMILLO, Ignacio y Erika Henao Hoyos. "La gestión electrónica…", *ob. cit*.
21 AMOROSO FERNANDEZ, Yarina. "Open Data:…", *ob. cit*., p. 14.

Entonces, teniendo claro que el ciudadano es el motor que impulsa mejorar las relaciones y las gestiones de las distintas dependencias de la Administración Pública, resulta evidente que se requieren algún tipo de garantías que permitan disminuir o atenuar los factores de vulnerabilidad a que se encuentran sometidos los datos, la información y los documentos en manos de los órganos y entes del Estado.

En este sentido, se puede anotar que la información personal o los datos de cada individuo han sido objeto de protección desde el reconocimiento del impacto del uso de las TIC en los derechos de las personas. Es en el año 1967 en el seno del Consejo de Europa donde se constituyo una Comisión para estudiar los alcances y consecuencias del mencionado impacto. Posteriormente, y luego de varias transformaciones se alcanza la "*…madurez de la protección de datos (tercera generación, 1980-1998). En este período se contemplan una serie de derechos de los ciudadanos para hacer efectiva la protección de sus datos, así como medidas de seguridad por parte de los responsables de los mismos*"[22].

Actualmente, la protección de datos se tiene como un derecho fundamental, derivando por una parte, en la promulgación de leyes para la protección de los datos; y por otra parte, en la creación de entes de la Administración Pública que velan por el correcto uso de la información personal que se encuentra en posesión de entes públicos o privados.

En la Constitución de la República Bolivariana de Venezuela del año 1999, se consagran dos artículos, que han servido de fundamento para la protección de los derechos de la información personal.

El artículo 28[23] consagra el llamado "*Habeas Data*", entendido como:

> …el derecho de toda persona a interponer la acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad; sea que ellos reposen en registros o bancos de datos público, o los privados destinados a proveer

22 PUENTE de la MORA, Ximena. "Protección de datos personales en posesión de los particulares en México: avances y desafíos", en: *Memorias del XIV Congreso Iberoamericano de Derecho e Informática*. Universidad Autónoma de Nuevo León, Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI), México, 2010, p. 912.

23 Constitución de la República Bolivariana de Venezuela, artículo 28.- "*Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley*".

> informes y, en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos[24].

El artículo 60[25] del texto constitucional corresponde principalmente al derecho a la privacidad, entendido como:

> …derecho de la persona de decidir por sí mismo en qué medida desea compartir con otros sus pensamientos, sus sentimientos y su vida personal, constituye pues una respuesta jurídica a las aspiraciones de cada persona por alcanzar un ámbito de desarrollo interior, ajeno a la intromisión y difícil de delimitar porque lo que para una persona puede ser privado para otra no lo es[26].

Así, los autores nacionales[27] han entendido que la creación y almacenamiento de los datos personales deben seguir unos "*Principios Generales*" para que sean tenidos como lícitos: (1) cuando se encuentren debidamente inscritos, observando en su operación los principios que establezcan las leyes y las reglamentaciones que se dicten en consecuencia; (2) los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública; (3) la información personal que se recoja a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido; (4) la recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley; (5) los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquéllas que motivaron su obtención; (6) los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario; (7) los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate; (8) los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular; y (9) los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

24 ORTIZ ORTIZ, Rafael. *Habeas Data. Derecho Fundamental y Garantía de la Protección de Derechos de la Personalidad. (Derecho a la Información y Libertad de Expresión),* Editorial Frónesis, Caracas, 2001, p. 70.

25 Constitución de la República Bolivariana de Venezuela, artículo 60.- "*Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos*".

26 PUENTE DE LA MORA, Ximena. "Nuevas tendencias del derecho a la privacidad. Caso Naomi Campbell", en: *Revista de Investigación y Análisis DEJURE*, Año 6, Segunda, Número 4, Colima, México, Febrero 2006, p. 58.

27 SALAZAR CANO, Edgar. "El Habeas Data en el Derecho Comparado", en: *Anuario* Nº 29, Facultad de Derecho, Universidad de Carabobo, Valencia, 2006, pp. 125-126.

Estos artículos de la Constitución de la República Bolivariana de Venezuela han sido objeto de atención por parte del Tribunal Supremo de Justicia, especialmente de la Sala Constitucional[28]. De los casos tratados[29] se puede concluir que la protección de datos personales en Venezuela ha estado dirigida principalmente a registros o bases de datos que se encuentran en posesión de órganos y entes del Estado, en archivos de acceso exclusivo o restringido de los funcionarios o del personal que labora en esas instituciones, y no se han tratado, aun, solicitudes de protección a la privacidad de información que se encuentra en posesión de terceros particulares o en las redes abiertas, especialmente en Internet.

Ahora bien, en lo que respeta al Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, debemos advertir que la protección de los datos personales se puede identificar en dos elementos, claramente diferenciados. Por una parte, el elemento adjetivo, contenido en el concepto de *seguridad de la información* como herramienta de protección; y por otra parte, el elemento sustantivo, que se encuentra referido a la naturaleza de los datos, la información o los documentos que permitirá la *denegación al acceso y transferencia de los datos, información y documentos*.

El primer elemento, la *seguridad de la información* o *seguridad de los servicios*[30], se refiere al otorgamiento de condiciones y medidas de protección, que garanticen un estado de inviolabilidad de influencias o de actos hostiles

28 Es importante anotar que este trabajo no pretende hacer un análisis de las fundamentaciones del Derecho Constitucional, sino presentar de manera integral la problemática de la protección de las personas (naturales y jurídicas) que generan información al alcance de terceros a través del empleo de los medios informáticos en la Sociedad de la Información.

Para el análisis de Derecho Constitucional de la figura del Habeas Data y del derecho a la privacidad, invitamos al estudio del siguiente trabajo: BREWER-CARÍAS, Allan R. *El proceso constitucional de las acciones de Habeas Data en Venezuela: las sentencias de la Sala Constitucional como fuente del Derecho Procesal Constitucional.* [En línea], Disponible en: *www.allanbrewercarias.com.*

29 Sentencias del Tribunal Supremo de Justicia, Sala Constitucional: 1) Sentencia No. 1050/ 2000, Fecha: 23/08/2000, Caso: Ruth Capriles Méndez y otros, Solicitud de Habeas Data. En: http://www.tsj.gov.ve/decisiones/scon/Agosto/1050-230800-00-2378%20.htm; 2) Sentencia No. 332/2000, Fecha: 14/03/2000, Caso: ISACA Compañía Anónima, Solicitud de Habeas Data. En: http://www.tsj.gov.ve/decisiones/scon/Marzo/332-140301-00-1797%20.htm; 3) Sentencia No. 2828/2004, Fecha: 07/12/2004, Caso: Pedro José Cabello Bonillo, Acción de Amparo En: http:/ /www.tsj.gov.ve/decisiones/scon/Diciembre/2829-071204-04-0733%20.htm; 4) Sentencia No. 1281/2006, Fecha: 26/06/2006, Caso: Pedro Reinaldo Carbone Martínez, Acción de Amparo. En: http://www.tsj.gov.ve/decisiones/scon/Junio/1281-260606-05-1964.htm; 5) Sentencia No. 1511/ 2009, Fecha: 09/11/2009, Caso: Mercedes Josefina Ramírez, Acción de Habeas Data. En: http:/ /www.tsj.gov.ve/decisiones/scon/Noviembre/1511-91109-2009-09-0369.html.

30 *Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, artículo 34.- "*Los servicios de información interoperables deberán ser seguros, garantizando la privacidad, confidencialidad e integridad de los datos, información y documentos de acceso público*".

específicos que puedan proporcionar el acceso a la data de personas no autorizadas, o que afecten la operatividad de las funciones de un sistema de computación, bajo los principios de confidencialidad, integridad y disponibilidad de la información.

Los autores Ignacio Alamillo y Erika Henao Hoyos, sobre este punto, destacan que la *Ley española 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*, reconoce la importancia de la seguridad, dedicando varios de sus artículos al desarrollo del tema de la identificación, la autenticación y la firma electrónica, tanto por parte de los ciudadanos como por parte de las propias Administraciones Públicas (personal al servicio de las Administraciones Públicas, sede electrónica, sello de órgano).

> Los principios de proporcionalidad y de seguridad se encuentran consagrados en la *Ley española 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*. El primero hace referencia a que la exigencia de un determinado nivel de acreditación debe circunscribirse a la naturaleza y circunstancias de los distintos trámites y procedimiento. Este principio actúa como límite superior, no pudiendo exigirse un nivel de seguridad más alto que el que resulta adecuado y necesario en el procedimiento tradicional basado en soporte papel. El segundo, establece que en el escenario telemático se exigirán al menos el mismo nivel de garantías exigidas en los trámites y procedimientos llevados a cabo por los conductos tradicionales. Este principio actúa como límite inferior, garantizando un tratamiento equivalente en términos de seguridad a los diferentes canales de tramitación (en soporte papel y en soporte electrónico)[31].

Así, para el caso particular del intercambio de datos entre Administraciones Públicas, se establece el uso de mecanismos que ofrezcan los máximos grados de seguridad; que según la legislación de ese país, puede ser alcanzado combinando la ley general de firma electrónica y la ley especial de identidad y firma electrónica en el sector público, lo cual conduce a un modelo en el que necesariamente han de existir diferentes sistemas y mecanismos de identidad y firma, como son: contraseñas estáticas, contraseñas dinámicas, mecanismos de segundo factor de autenticación, certificados en soporte *software*, certificados en soporte *hardware*, biometría, entre otras posibilidades.

En el análisis de las cuestiones de seguridad, los citados autores van más allá del uso bajo los estándares de interoperabilidad de los datos, información y documentos de las Administraciones Públicas españolas, y anotan los soluciones a las que se han arribado sobre estos temas, dado que se encuentran dentro de las prioridades máximas del programa de Administración Electrónica de la Unión Europea, recogido en la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, "*Plan de*

31 ALAMILLO, Ignacio y Erika Henao Hoyos. "La gestión electrónica…", *ob. cit*.

acción sobre Administración electrónica i2010: Acelerar la Administración electrónica en Europa en beneficio de todos", de fecha 25 de abril de 2006, que recoge y evoluciona el importante Acuerdo Signposts, adoptado a partir de la Declaración de Manchester de 2005[32].

En el caso venezolano, el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, establece la utilización de la firma electrónica[33] en las actuaciones administrativas así como del sistema de certificación electrónica[34], con la finalidad de garantizar la integridad y autenticidad de los datos, información y documentos que se intercambien electrónicamente, ya sea que su original se encuentre en medio impreso o electrónico; conforme a las normas técnicas de seguridad de la información que dicte la autoridad competente en la materia; es decir, la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE)[35].

32 ALAMILLO, Ignacio y Erika Henao Hoyos. "La gestión electrónica…", *ob. cit*.

33 El *Decreto No. 1.204 con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas*, publicado en la Gaceta Oficial No. 37.148 de fecha 28 de febrero de 2001, establece los siguientes aspectos de las firmas electrónicas: i.- Definición Legal: "información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado". ii.- Reconocimiento del valor probatorio: la Firma Electrónica que permita atribuir autoría a los Mensajes de Datos tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. iii.- Requisitos para la validez y eficacia probatoria: la Firma Electrónica deberá: a) garantizar que los datos utilizados para su generación pueden producirse sólo una vez, y asegurar, razonablemente, la confidencialidad; b) ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento, y; c) no alterar la integridad del Mensaje de Datos. iv. Efectos jurídicos: cuando la Firma Electrónica no cuente con los requisitos para su validez y eficacia probatoria, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica. v.- Firma Electrónica Certificada: es aquella que ha sido debidamente certificada por un Proveedor de Servicios de Certificación Electrónica.

34 El Decreto No. 1.204 con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, establece los siguientes aspectos de los certificados electrónicos: i.- Definición legal: "Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica". ii.- Función: garantiza la autoría de la Firma Electrónica que certifica así como la integridad del Mensaje de Datos. iii.- Carácter: no confiere la autenticidad o fe pública que conforme a la ley otorguen los funcionarios públicos a los actos, documentos y certificaciones que con tal carácter suscriban. iv.- Contenido: 1) identificación del Proveedor de Servicios de Certificación que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica; 2) el código de identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica; 3) identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica; 4) las fechas de inicio y vencimiento del periodo de vigencia del Certificado Electrónico; 5) la Firma Electrónica del Signatario; 6) un serial único de identificación del Certificado Electrónico, y; 7) cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico.

35 El *Decreto No. 1.204 con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas*, establece los siguientes aspectos de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE): i.- Características: servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, dependiente del Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación. ii.- Objeto: acreditar, supervisar y controlar a los Proveedores de Servicios de

El segundo elemento, la *denegación al acceso de los datos, información y documentos*[36], es la posibilidad que tiene un órgano o ente del Estado[37] de negarse al acceso o intercambio solicitado a través del *Operador de la*

Certificación Electrónica, públicos o privados. iii.- Competencias: 1) Otorgar la acreditación y renovación a los Proveedores de Servicios de Certificación Electrónica. 2) Revocar o suspender las acreditaciones otorgadas. 3) Mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores de Servicios de Certificación Electrónica. 4) Verificar que los Proveedores de Servicios de Certificación Electrónica cumplan con los requisitos previstos por la ley. 5) Supervisar las actividades de los Proveedores de Servicios de Certificación Electrónica. 6) Liquidar, recaudar y administrar las tasas establecidas en la ley. 7) Liquidar y recaudar las multas establecidas en la Ley. 8) Administrar los recursos que se le asignen y los que obtenga en el desempeño de sus funciones. 9) Coordinar con los organismos nacionales o internacionales cualquier aspecto relacionado con el objeto de la ley. 10) Inspeccionar y fiscalizar la instalación, operación y prestación de servicios realizados por los Proveedores de Servicios de Certificación Electrónica. 11) Abrir, de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativo a las presuntas infracciones de la ley. 12) Requerir a los Proveedores de Servicios de Certificación Electrónica o sus usuarios, cualquier información que considere necesaria y que este relacionada con las materias de su competencia. 13) Actuar como mediador en la solución de conflictos que se susciten entre los Proveedores de Servicios de Certificación Electrónica y sus usuarios, sin perjuicio de las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el usuario, conforme a la ley que rige la materia. 14) Seleccionar los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones. 15) Presentar un informe anual sobre su gestión al Ministerio de adscripción. 16) Tomar las medidas preventivas o correctivas que considere necesarias conforme a lo previsto en la ley. 17) Imponer las sanciones establecidas en la ley. 18) Determinar la forma y el alcance de los requisitos para la acreditación de los Proveedores de Servicios de Certificación Electrónica. 19) Las demás que establezca la ley y sus reglamentos.

36 *Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, artículo 57.- "*La denegación de acceso a los datos, información y documentos que presente un órgano o ente del Estado, deberá estar justificada en alguna disposición legal y sólo se limitará a lo expresamente establecido en la ley. Si el dato, información o documento denegado se encuentra en algún documento que contenga datos o información no confidencial, el órgano o ente del Estado deberá separarlo y permitir el acceso e intercambio electrónico de aquellos que no tengan carácter confidencial*". Artículo 58.- "*La denegación de acceso a los datos, información y documentos deberá ser notificada por el órgano o ente requerido ante el operador de la interoperabilidad, dentro de los diez días hábiles siguientes a su solicitud, acompañada de un informe en el cual se expongan los fundamentos que la sustente. Una vez recibido el informe, el operador de interoperabilidad pondrá en conocimiento del mismo órgano o ente que haya solicitado acceder al dato, información o documentos, para que este manifieste si ratifica o no su solicitud*". Artículo 59.- "*Ratificada la solicitud de acceso e intercambio electrónico de dato, información o documento, el operador de la interoperabilidad convocará a los órganos o entes involucrados a fin de conciliar sus diferencias. Agotada la fase conciliatoria sin llegar a un acuerdo,* el *operador de la interoperabilidad remitirá las actuaciones al Comité Nacional de la Interoperabilidad, para que éste, dentro de un lapso de treinta días hábiles, se pronuncie sobre la procedencia o no de la solicitud de acceso e intercambio electrónico del dato, información o documento requerido. El Comité Nacional de la Interoperabilidad podrá en su decisión establecer todas las medidas necesarias para el adecuado y seguro intercambio electrónico del dato, información y documento, de ser el caso*".

37 La denegación de acceso o intercambio de dato, información o documento también puede ocurrir de oficio, de conformidad con lo establecido en el artículo 60, *eiusdem*.- "*El operador de*

Interoperabilidad por parte de otro órgano o ente del Estado, en virtud de la naturaleza de los datos, la información y los documentos requeridos.

Esta negativa debe ser justificada en alguna disposición legal; no obstante, debemos tener en cuenta que el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, no establece las causales de justificación para la denegación al acceso o intercambio de datos, información y documentos. Por el contrario, establece, con carácter obligatorio, que los órganos o entes del Estado compartirán los datos, información y documentos, dejando claro que las excusas tendrán como finalidad la garantía de la protección al honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de los ciudadanos y ciudadanas. En este mismo orden de ideas, se establece que la solicitud de acceso o intercambio de datos, información y documento no es exigible, si la misma resulta impertinente, inadecuada o excesiva en relación al ámbito y fines del proceso que se desea ejecutar, valoraciones que deberá realizar el Operador de la Interoperabilidad al momento de tramitar la solicitud formulada por un órgano o ente del Estado[38].

Finalmente, en el ámbito de la *Carta Iberoamericana de Gobierno Electrónico*, la protección de datos personales se presenta dentro del derecho de los ciudadanos al gobierno electrónico, en los siguientes términos:

> …se reconoce el derecho de todo ciudadano de solicitar ante los organismos competentes la actualización, la rectificación o la destrucción de aquellos datos contenidos en registros electrónicos oficiales o privados, si fuesen erróneos o afectasen ilegítimamente sus derechos. Para garantizar este derecho, se tiene que asegurar a todo ciudadano el acceso a la información y a los datos que sobre sí mismo o sobre sus bienes consten en registros oficiales o privados, con las excepciones que justificadamente se establezcan, así como se debe facilitar el conocimiento del uso que se haga de dichos datos y su finalidad.

la interoperabilidad, cuando lo estime conveniente, podrá someter a la consideración del Comité Nacional de Interoperabilidad, la denegación de acceso a los datos, información y documentos presentada por un órgano o ente del Estado, aun en aquellos casos en los cuales el solicitante no haya ratificado su solicitud".

38 *Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado,* artículo 43.- "*Los órganos o entes del Estado están obligados a compartir los datos de autoría, y sólo podrán excusarse de compartir los datos, información y documentos que manejan cuando la ley expresamente así lo limite, a fin de garantizar la protección al honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de los ciudadanos. La obligación de compartir datos de autoría, información y documentos de acceso público no será exigible cuando la solicitud de estos sea impertinente, inadecuada o excesiva en relación al ámbito y fines del proceso que se desea ejecutar*".

IV. Conclusiones

Cuando se habla de la Sociedad de la Información no solo se refiere a las personas que son capaces de producir y descodificar información, lo cual les permite participar de relaciones de interconexión con otros actores de esta sociedad, también se alude a las instituciones políticas, económicas y jurídicas, entre otras, que hacen uso de las TIC para el desarrollo de sus actividades.

Esta realidad de interacción social trae consigo requisitos o necesidades para lograr la incorporación de una persona o de un país a la Sociedad de la Información, no son exclusivamente problemas de tipo tecnológico, tales como tener o no computadoras conectadas en red; el elemento fundamental que determina su desarrollo está estrechamente relacionado con condicionantes económicas, sociales, culturales y muy principalmente jurídicas.

La evaluación del régimen jurídico de los servicios relacionados con las TIC, debe perseguir la competencia y la eficiencia, reconociendo los derechos de las personas no solo en las relaciones de uso y consumo que se den a través de la utilización de estas tecnologías, sino también de la garantía de los derechos fundamentales, en todos los aspectos de la Sociedad de la Información, desarrollándose un catálogo de instrumentos jurídicos que permitan hacer efectivos estos derechos.

Es así como la incorporación de las TIC, y el desarrollo de los aspectos económicos, sociales y políticos de la Sociedad de la Información suponen una transformación del concepto y del contenido tradicional de las relaciones de los ciudadanos con los órganos y entes públicos.

En este sentido, debemos tener presente que la llamada “revolución tecnológica”, que comprende los avances científicos que se han venido produciendo a lo largo del tiempo en el campo de la informática requiere la adecuación de los conocimientos científicos a nivel general y particularmente, en la evaluación de los factores de vulnerabilidad de la información de los particulares en poder de los órganos y entes del Estado.

> En definitiva, las Tecnologías de la Información y la Comunicación pueden mejorar la prestación de servicios a los ciudadanos, pero también –al igual que sucede con las empresas privadas– generan un riesgo para la privacidad de los ciudadanos, por lo que deben establecerse las correspondientes garantías, tanto técnicas como jurídicas. La implantación de identificadores únicos, el intercambio de datos entre Administraciones o registros públicos, el desarrollo de intranets, la utilización de Internet para realizar todo tipo de trámites,... y, en general, la implantación de las Tecnologías de la Información tanto para mejorar la organización interna de las Administraciones Públicas como la prestación de los servicios que se ofrecen al ciudadano requiere, previamente a poner en marcha un proyecto de forma global, la definición de los requerimientos técnicos y jurídicos que debe cumplir, y la realización de estudios, análisis, pruebas y validaciones encaminadas a determinar tanto la fiabilidad de la tecnología utilizada

> como el impacto, beneficios y riesgos que conllevan para el ciudadano, así como la conformidad de éstas medidas con la legislación vigente, todo ello de una forma transparente y que permita su discusión política[39].

Para finalizar anotaremos las oportunas conclusiones de los autores Ignacio Alamillo y Erika Henao Hoyos, en el ya citado trabajo: *La gestión electrónica de la identidad y de la firma electrónica en el intercambio electrónico de datos entre Administraciones Públicas:*

> Como consecuencia ineludible de lo anterior, es posible afirmar que para el establecimiento de relaciones electrónicas tanto entre la Administración y el administrado, como entre diferentes Administraciones, e incluso en las relaciones internas de una misma Administración, resulta imperiosa la necesidad de emplear los instrumentos adecuados que garanticen circunstancias como la identidad del actor y la integridad y autenticidad de los datos y documentos. De no ser así, sería imposible la construcción de un entorno de confianza en el cual los actores puedan interactuar, y se frustran los beneficios de la digitalización de los trámites y procedimientos administrativos[40].

Las TIC deben ser utilizadas para el logro de la mayor eficiencia y efectividad organizacional del Estado y el logro de los máximos ahorros; así el modelo de gobierno electrónico debe ser un modelo de servicios, de fácil acceso, ubicación, conocimiento en tecnologías y capacitación de los actores, sin dejar de lado la seguridad y protección de la información de los ciudadanos.

39 PRENAFETA RODRÍGUEZ, Javier. “La privacidad en el Gobierno…”, *ob. cit.*
40 ALAMILLO, Ignacio y Erika Henao Hoyos. “La gestión electrónica…”, *ob. cit*.