



UNIVERSIDAD CENTRAL DE VENEZUELA  
FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS  
CENTRO DE ESTUDIOS DE POSTGRADO  
ESPECIALIZACIÓN EN DERECHO PROCESAL LABORAL

LA CERTIFICACIÓN TÉCNICA DE LAS ACTUACIONES JUDICIALES  
COMO GARANTIA DEL DEBIDO PROCESO EN LA ADMINISTRACIÓN DE  
JUSTICIA. CASO JURIS 2000

Trabajo Especial presentado para optar al Título de Especialista en Derecho  
Procesal Laboral

Autora: Abg. Mayra González

Tutor: Dr. Aníbal Rueda

Caracas, julio de 2014

## **DEDICATORIA**

A Dios por haberme permitido transitar por el camino de mis objetivos y por darme la oportunidad de vivir para verlos materializados.

A mis padres por ser el pilar fundamental en todo lo que soy, por su ejemplo de perseverancia y motivación en mi educación, tanto académica, como de la vida y por su incondicional apoyo, perfectamente mantenido a través del tiempo.

A todos aquellos colegas cuyo ejercicio profesional los somete a los embates de un proceso judicial que experimenta con el uso de los sistemas automatizados de gestión.

## **AGRADECIMIENTO**

Al Dr. Aníbal Rueda, por su confianza, su colaboración y por haber sido parte de mi desarrollo profesional.

A colegas y amigos que han apostado por mi crecimiento profesional a lo largo de los años y de quienes he recibido su apoyo incondicional.

## INDICE

<b>RESUMEN.....</b>	<b>VI</b>
<b>INTRODUCCION.....</b>	<b>VII</b>
<b>CAPITULO I. LA SISTEMATIZACIÓN JUDICIAL DE LOS TRIBUNALES VENEZOLANOS</b>	
1.1 ANTECEDENTES DE LA REFORMA Y MODERNIZACIÓN JUDICIAL EN VENEZUELA..	1
1.2 PROCESO DE IMPLANTACIÓN JURIS 2000.....	6
1.3 NATURALEZA FUNCIONAL DEL SISTEMA JURIS 2000 .....	9
1.3.1 <i>Sistema de Seguimiento Procesal</i> .....	11
1.3.2 <i>Sistemas de Gestión o de Control de Gestión</i> .....	15
<b>CAPITULO II. BASE NORMATIVA DE LA IMPLEMENTACIÓN DEL JURIS 2000 EN LA ADMINISTRACIÓN JUDICIAL VENEZOLANA</b>	
2.1 REGULACIÓN NORMATIVA DEL MODELO ORGANIZACIONAL .....	18
2.2 REGULACIÓN LEGAL DEL SISTEMA INTEGRAL DE GESTIÓN, DECISIÓN Y DOCUMENTACIÓN JURIS 2000 .....	25
<b>CAPITULO III. LA CERTIFICACIÓN TÉCNICA DE LAS ACTUACIONES Y EL DEBIDO PROCESO EN UN SISTEMA AUTOMATIZADO DE JUSTICIA.</b>	
3.1. CONSIDERACIONES PRELIMINARES.....	28
3.2 LA CERTIFICACIÓN TÉCNICA O ELECTRÓNICA .....	30
3.2.1 <i>Definición</i> .....	30
3.2.2 <i>Beneficios del Certificado Electrónico</i> .....	37
3.2.3 <i>Regulación Legal de la Certificación Electrónica en Venezuela</i> .....	40
3.3 ELEMENTOS DE UN PROCESO ELECTRÓNICO .....	51
3.3.1 <i>La Firma Digital</i> .....	52

3.3.2 <i>El Documento Electrónico</i> .....	57
3.3.3 <i>El expediente judicial electrónico</i> .....	63
3.3.4 <i>Las Notificaciones Electrónicas</i> .....	69
3.4 CONNOTACIÓN DEL DEBIDO PROCESO EN UN SERVICIO JUDICIAL DE GESTIÓN AUTOMATIZADA (EL JURIS 2000).-.....	75
3.5 FORMAS DE QUEBRANTAMIENTO DEL DEBIDO PROCESO A TRAVÉS DE UN SERVICIO JUDICIAL AUTOMATIZADO.- .....	88
3.6 EL CERTIFICADO ELECTRÓNICO COMO NECESIDAD DE UN PROCESO JUDICIAL DEBIDO.-.....	95
3.7 IMPULSOS DEL ESTADO PARA IMPLEMENTACIÓN DE LA FIRMA ELECTRÓNICA Y LA CERTIFICACIÓN TÉCNICA EN LA ADMINISTRACIÓN DE JUSTICIA VENEZOLANA.....	105
<b>CAPITULO IV. PRAXIS DE LA SISTEMATIZACIÓN JUDICIAL</b>	
4.1 LA SEGURIDAD EN EL USO DE LAS TIC´S IMPLEMENTADAS EN LA ADMINISTRACIÓN DE JUSTICIA DE LATINOAMÉRICA .....	110
4.1.1 <i>Brasil</i> .....	116
4.1.2 <i>Perú</i> .....	119
4.1.3 <i>Costa Rica</i> .....	120
4.1.4 <i>Argentina</i> .....	122
4.2 MECANISMOS DE VALIDACIÓN, SEGURIDAD Y REGISTRO DE ACTUACIONES DEL JURIS 2000 .....	124
4.3 SEÑALAMIENTOS JUDICIALES EN EL SISTEMA DE GESTIÓN INFORMÁTICA JURIS 2000.....	131
4.3.1 <i>Caso de la mudanza de los Tribunales Civiles, Mercantiles, de Tránsito y Bancarios del Área Metropolitana de Caracas</i> .....	131

<i>4.3.2 Sentencia Controversial. A pesar de que no se tenga en físico el expediente respectivo aún se puede decir que las partes se encuentran a derecho y se da la notificación presunta.....</i>	140
<b>CONCLUSIONES .....</b>	143
<b>RECOMENDACIONES.....</b>	149
<b>FUENTES DOCUMENTALES .....</b>	152
<b>BIBLIOGRAFÍA.-.....</b>	152
<b>REFERENCIAS DE DOCUMENTOS ELECTRÓNICOS.-.....</b>	154
<b>LEGISLACIÓN CONSULTADA.-.....</b>	162
<b>GLOSARIO.....</b>	164



## **La Certificación Técnica de las Actuaciones Judiciales como Garantía del Debido Proceso en la Administración de Justicia. Caso Juris 2000**

Autora: Mayra González M.

Tutor: Dr. Aníbal Rueda.

Fecha: Julio 2014.

### **RESUMEN**

El propósito de la investigación es analizar los efectos de la certificación técnica de las actuaciones judiciales del sistema automatizado Juris 2000 para garantizar el debido proceso, a partir de registros documentados de la modernización judicial venezolana que permitan generar consideraciones críticas y recomendaciones conducentes a mejorar la sistematización de la administración de justicia. Para ello se establecieron los siguientes objetivos específicos: a) Describir el proceso de sistematización judicial en Venezuela y los avances jurisprudenciales sobre la materia en casos emblemáticos; b) Examinar el ordenamiento jurídico que sustenta la implementación del Juris 2000 en los circuitos judiciales del país; c) Destacar la importancia de la certificación electrónica en los procesos de sistematización judicial y su connotación en el debido proceso; y d) Comparar las perspectivas de uso e impactos de las tecnologías de información y comunicaciones (TIC) en la administración de justicia de América Latina, con los mecanismos de validación, seguridad y registro de actuaciones del sistema automatizado Juris 2000. Partiendo de los objetivos planteados, se empleó una metodología descriptiva-documental, donde se examinaron casos emblemáticos, como el de la mudanza de los tribunales civiles de Caracas, en los que se compromete el cumplimiento de garantías como el debido proceso, ocasionados por la restringida fiabilidad los registros electrónicos, una revisión histórica del proceso de modernización judicial en Venezuela, con apoyo del método deductivo-inductivo y analítico de la documentación contenida en la página Web del CEJA para estudios internacionales sobre la materia, examen de sentencias del Tribunal Supremo de Justicia y de los tribunales, para examinar los criterios adoptados frente a las irregularidades del sistema el Juris 2000 en el proceso, referencias doctrinarias sobre la garantía procesal del debido proceso, y reportes anuales de la Dirección Ejecutiva de la Magistratura. Finalmente, como resultado de la investigación se generaron las siguientes conclusiones: 1) La Certificación Técnica es un elemento de seguridad indispensable para materializar la naturaleza funcional del sistema automatizado frente al físico del expediente y la fiabilidad en la publicidad electrónica de las actuaciones procesales, y 2) El Juris 2000 no tiene asociado firmas digitales ni certificados electrónicos que le ofrezcan fiabilidad, integridad y no repudio a sus registros electrónicos.

Términos Descriptores: Modernización Judicial, Certificación técnica, Debido Proceso, Sistematización.

## INTRODUCCION

La informática utilizada en los procesos judiciales de Venezuela se limitaba a que todos los juzgados y tribunales contaran con el uso de computadoras que funcionaban como procesadoras de documentos, sin embargo, el manejo de los recursos de información adquirieron una importancia central, que le impuso al Estado asumir avances en la modernización de la Administración de Justicia, por ser un sector altamente sensible en cuanto a la expectativa de idoneidad, celeridad y eficiencia.

A este respecto, en el año 1993 a través de un convenio firmado entre la República de Venezuela, actualmente, República Bolivariana de Venezuela y el Banco Mundial<sup>1</sup> se desarrollaron varios componentes de Asistencia Técnico-Financiera, relativos a la modernización de la administración de trabajo de los tribunales y a la infraestructura física del Sistema Judicial, que abrió paso a la implementación del sistema Juris 2000 como un nuevo modelo Organizacional y sistema de gestión que permite agilizar el trabajo administrativo judicial (elaboración automatizada del libro diario, distribución aleatoria automatizada de causas, registro automatizado del trabajo administrativo judicial, configuración prediseñada de actas, boletas u oficios y otras actuaciones); así como, lograr la desagregación de funciones administrativas judiciales, de las propiamente jurisdiccionales a cargo de los jueces para alcanzar mayor celeridad, transparencia, homogeneidad y eficacia en la administración de justicia.

---

<sup>1</sup> Seintex. *Diseño e Implementación del Modelo Organizacional y un Sistema Integral de Gestión, Decisión y Documentación para los Tribunales Pilotos*. Manual del Técnico Jurídico. Caracas. 2000, p.4

De acuerdo con los informes de la Dirección Ejecutiva de la Magistratura<sup>2</sup> este sistema proporciona al ciudadano, una mayor seguridad de los procesos judiciales que se encuentran tramitando en cada sede implantada, toda vez que evita la posible violación del Libro Diario, listado donde se asientan las actuaciones diarias realizadas por el juez en su gestión jurisdiccional, a través de su cierre automático; así como, permite transparencia en la distribución de los asuntos que ingresan a las sedes judiciales, debido a que las mismas son llevadas de manera aleatoria, equitativa, imparcial y expedita, cumpliendo con lo establecido en el artículo 26 de la Constitución de la República Bolivariana de Venezuela.

No obstante, en el ejercicio, la prestación del servicio automatizado Juris 2000 no puede equipararse con el acceso físico de las actas del expediente y así lo ha confirmado la Sala Constitucional del Tribunal supremo de Justicia al establecer que:

*“...El expediente da fe de lo ocurrido en una causa particular, pero no puede afirmarse lo mismo respecto del sistema informático a que se ha hecho referencia, pues, en primer lugar, sus registros no cumplen con los requisitos que establecen los artículos 6, único aparte, y 8 de la Ley sobre Mensajes de Datos y Firmas Electrónicas...”<sup>3</sup>.*

Desde el punto de vista funcional, la sistematización judicial que ha sufrido el proceso venezolano no cuenta con la validez legal que ofrecen las tecnologías de firmas digitales, que hoy día son reguladas en nuestro país por la Ley de Mensajes de Datos y Firmas electrónicas. Deficiencia técnica que ha sido declarada recientemente en Amparo Constitucional al señalar

---

<sup>2</sup> Dirección Ejecutiva de la Magistratura. *Juris 2000. El Modelo Organizacional*. [Documento en línea]. Disponible en: <http://www.dem.gob.ve>. (fecha de consulta: 25/07/2010)

<sup>3</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 04-3055 de fecha 21 de marzo de 2006. (Alida Teresa Pernaleté Gásperi vs. Coordinadora del Circuito de Protección del Niño y del Adolescente del Estado Lara, abogada Erlinda Oropeza) Disponible en: <http://www.tsj.gov.ve>. (fecha de consulta: 15/05/2010)

que “...el Sistema Juris 2000 implantado,...no posee firmas digitales que certifiquen las actuaciones realizadas”<sup>4</sup>.

Sin embargo, la Sala Constitucional, recientemente se aparta del criterio sostenido respecto a la validez de los datos extraídos del Sistema Juris 2000, y establece con carácter vinculante que “las decisiones judiciales obtenidas a través del aludido sistema informático del Poder Judicial serán consideradas copias simples conforme al artículo 429 del Código de Procedimiento Civil”<sup>5</sup>, afirmación que podría comprometer garantías procesales de carácter constitucional, como el debido proceso, por las irregularidades que puedan surgir de la confrontación de los datos electrónicos con el físico. Tal y como se evidenció en el caso emblemático de la mudanza de los tribunales de primera instancia civiles de Caracas, en los que se obligaba a revisar en sistema los expedientes de los tribunales que se habían trasladado, ya que no contaban con el resguardo del físico. Posteriormente, con el acceso a las actas, muchas causas aparecieron sentenciadas, con vencimiento de lapsos para actuaciones, y sin registro sistemático, violando el derecho que tiene todo ciudadano de ejercer sus defensas.

De manera que, la información registrada por los despachos judiciales en las bases de datos de consulta a las que tienen acceso los usuarios del sistema judicial, deben tener equivalencia funcional o igual valor probatorio a la información escrita en los expedientes, en especial en lo referido a los actos de comunicación procesal de actuaciones, debiendo garantizar la veracidad en la información registrada en pro de la conservación del derecho

---

<sup>4</sup> Juzgado Superior Décimo en lo Civil, Mercantil y Tránsito de la Circunscripción Judicial del Área Metropolitana de Caracas, en sede Constitucional. Sentencia N° 5.878. (Mary Luz del Carmen Lugo Betancourt vs. Sentencia dictada el 13/04/2009 Juzgado Tercero de Primera Instancia en lo Civil, Mercantil, Tránsito y Bancario de la Circunscripción Judicial del Área Metropolitana de Caracas). Disponible en: <http://www.tecnoiuris.com>. (fecha de consulta: 15/05/2010)

<sup>5</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 224 de fecha 09 de julio de 2010. (Edson Alejandro Rojas Rivas) Disponible en: <http://www.tsj.gov.ve>. (fecha de consulta: 18/12/2010)

al debido proceso. Teniendo en cuenta que para los casos en los que sea necesaria una consulta directa de los expedientes para verificar aspectos sustanciales de contenido de las decisiones judiciales los usuarios deberán proceder de tal manera.

Ahora, la autenticidad y la confiabilidad de la información aportada por una herramienta como el Juris 2000, debe estar determinada por la seguridad de que esté dotado en cuanto a la forma como se hubiese generado y conservado la integridad de la información y, por supuesto, en la forma en que se identifique a su iniciador y la asociación de éste a su contenido. Como todo documento, la eficacia probatoria del mensaje electrónico dependerá, también, de su autenticidad, contándose con mecanismos tecnológicos que permiten identificar el autor del mismo y asociarlo con su contenido. Seguridad jurídica y técnica que se logra con la certificación y firma electrónica y que de acuerdo con el Ing. Luis Enrique Hellin *“garantiza la protección de los derechos del justiciable, las garantías procesales y genera confianza en el sistema judicial”*<sup>6</sup>.

Por otra parte, el sistema Juris 2000 constituye un resguardo de la información relevante del expediente, cuyos registros pudieran reconstruir la conformación física del mismo, en caso de existir extravío. Pues, el proceso judicial continúa girando en torno a la agregación de documentos a un expediente físico y de papel y el principal rol de los sistemas informáticos es registrar información lo más fidedigna posible acerca de los documentos contenidos en el expediente. Pero, previamente sería necesario resolver el problema de la autenticación de los documentos, a través de mecanismos

---

<sup>6</sup> Hellin, Luis Enrique. *La Certificación y Firma Electrónica en el ámbito de la Informática Forense*. Primer Congreso Internacional de Seguridad de la Información. Caracas. 2010 Disponible en: <http://www.SUSCERTE.gob.ve/>. (fecha de consulta: 26/02/2011)

de validación. A este respecto, el Centro de Estudios de Justicia de las Américas, CEJA, señala que:

*“La escrituración, la forma “normal” en la cual se han procesado los casos judiciales es mediante la formación de un expediente escrito, que contiene toda la información relevante para su solución... Es posible decir que en la región, la tecnología predominante de producción de sentencias judiciales es la tramitación de expedientes, lo que tiene numerosas consecuencias sobre una serie de otros aspectos, entre los que está: el resguardo de la información relevante...En esta situación, el sistema informático podría contener un expediente electrónico que sea espejo del expediente físico”.*<sup>7</sup>

En razón de lo anterior, se deben analizar los quebrantamientos procesales de la seguridad jurídica, con ocasión a la aplicación de un sistema automatizado de gestión, limitado para otorgar fe pública a sus registros, partiendo de la siguiente interrogante: *¿Cómo afecta la implantación de un sistema automatizado judicial (Juris 2000) sin certificación electrónica, la garantía procedimental del debido proceso?*

---

<sup>7</sup> Hernández, C. y Adelardi, R. “Perspectivas de uso e impactos de las TIC en la administración de justicia en América Latina” (2008). [Documento en línea]. Disponible en: <http://www.cejamericas.org>. (fecha de consulta: 26/08/2010)

## CAPITULO I. LA SISTEMATIZACIÓN JUDICIAL DE LOS TRIBUNALES VENEZOLANOS

### 1.1 Antecedentes de la Reforma y Modernización Judicial en Venezuela<sup>8</sup>.-

El primer crédito del Banco Mundial exclusivamente para la reforma judicial en Venezuela, fue aprobado en 1993 y se denominó Convenio 3.514-VE de Modernización del Consejo de la Judicatura, actualmente Dirección Ejecutiva de la Magistratura (DEM) y los Tribunales. El convenio tuvo serias dificultades de ejecución ya que el Consejo de la Judicatura no estaba preparado para manejarlo ni había una idea consensuada del significado de la reforma judicial. Los conflictos internos y externos, generaron retardos e ineficiencias. Los primeros desembolsos no se hicieron sino en 1995 y sucesivos retardos llevaron la ejecución del mismo hasta el 2002<sup>9</sup>.

El propósito de modernización judicial ascendió a una inversión de 60 millones de dólares, distribuidos en 30 millones aportados por el Banco Mundial y 30 millones aportados por la República de Venezuela (ahora República Bolivariana de Venezuela). El Consejo de la Judicatura fue el órgano que actuó como representante de la República en el convenio. El

---

<sup>8</sup> Lawyers Committee for Human Rights (U.S.), Programa Venezolano de Educación-Acción en Derechos Humanos. *El Banco Mundial y la reforma judicial en Venezuela. Estudio de caso: documento de trabajo preparado para la Conferencia de ONG sobre el Banco Mundial y la reforma judicial en Latinoamérica*. Serie: Aportes N° 5. Provea. Caracas, 1996. . [Documento en línea]. Disponible en: <http://190.41.250.173/RIJ/BASES/PDFS/CAP4.pdf>. (fecha de consulta: 12/08/2010).

<sup>9</sup> La información fue tomada del Draft Implementation Completion Report de diciembre de 2002 y en las Propuestas de Prórroga del Convenio, respectivamente, enero de 2001 y mayo de 2002. Citado por Pérez, R. *Reforma judicial, Estado de Derecho y revolución en Venezuela*. (2003). [Documento en línea]. Disponible en: <http://www.accesoalajusticia.org/documentos/detalle.php?mrdstartid=10&catid=6>, (fecha de consulta: 10/07/2010).

proyecto que debía ser ejecutado en 5 años, se dividió originalmente en dos fases:

a) La primera fase del proyecto estaba dirigida al diseño e implementación de los nuevos procedimientos administrativos, cambio en la infraestructura de los tribunales e instalación de equipos informáticos, capacitación de personal administrativo, mejoras en el mobiliario de las oficinas, desarrollo del programa de capacitación de la Escuela de la Judicatura (hoy Escuela Nacional de la Magistratura) y análisis de los principales aspectos en la problemática del Poder Judicial. En esta primera fase resultaba esencial determinar los modelos a ser aplicados en la siguiente etapa, a fin de lograr transformar los tribunales.

b) La segunda fase estaba dirigida a la implementación y puesta en funcionamiento de los nuevos modelos en los tribunales, se continuaría con la capacitación del personal y se pondría en funcionamiento la Escuela de la Judicatura.

Estas fases, se encontraban estructuradas en cuatro componentes de Asistencia Técnico-Financiera relacionados con:

1. Componente "A" (*organización interna del Consejo de la Judicatura*): este componente estaba destinado a fortalecer el Consejo de la Judicatura en sus tareas de administración del Poder Judicial. Se buscaba mejorar la capacidad institucional del Consejo a fin de lograr su efectividad en el diseño y ejecución de las políticas hacia el Poder Judicial. Como forma de alcanzar estos objetivos, se debía informatizar este órgano y capacitar a sus funcionarios de distintos niveles en temas técnicos y gerenciales.

2. El componente "B" (*forma de operar los tribunales*): tenía por objeto modernizar los procedimientos internos de los tribunales. El objetivo era desarrollar un modelo de organización y un sistema integral de gestión de los tribunales para optimizar la actividad administrativa y los procesos jurisdiccionales. Este nuevo modelo organizacional y el sistema integrado de gestión, decisión y documentación, denominado *Juris 2000*, opera mediante las redes de computadoras, para lo cual se propone diseñar software y cursos de inducción y formación al personal administrativo de los tribunales.

3. El componente "C" (*formación y capacitación de jueces*): buscaba desarrollar la Escuela de la Judicatura. El objetivo era establecer una Escuela de la Judicatura que fuese eficiente en la formación y capacitación de los magistrados y jueces, debiendo desarrollar un adecuado programa de cursos de capacitación, metodología a ser empleada y evaluación.

4. El componente "D" (*infraestructura física del Sistema Judicial*): estaba destinado a la implantación de una adecuada infraestructura física para el funcionamiento del Poder Judicial. El objetivo era superar el grave problema de carencia de locales adecuados para el funcionamiento del Poder Judicial, en edificios arrendados, con poco espacio y que no se adecuan para la realización de los procesos orales que demanda el nuevo sistema legal.

En referencia a este convenio es necesario señalar que tras una la licitación internacional se adjudicó la realización del proyecto a la Consultora Multinacional especializada en Organización, Tecnologías de la Información y Comunicaciones, Seintex Consultores, S.A, la cual es una empresa de origen español que también estuvo encargada de los procesos de reforma judicial de Costa Rica y República Dominicana.

El segundo convenio (4.270-VE), suscrito con el Banco Mundial en diciembre de 1997, llevó adelante un proyecto para modernizar la Corte Suprema, hoy Tribunal Supremo de Justicia. Fue a comienzos del año 1996, cuando el representante del Banco Mundial visitara por primera vez a la Corte Suprema de Justicia, con la finalidad de realizar todos los preparativos para la ejecución del Proyecto de modernización de este tribunal.

Como consecuencia de las reuniones realizadas por los entonces Magistrados con el representante del Banco Mundial, en julio de 1996, la Corte Suprema de Justicia acordó la creación del Comité Técnico de Modernización y de la Unidad de Apoyo al Proyecto de Modernización. Esta Unidad de Apoyo se financió con una donación, efectuada por el Gobierno de Japón.

Los integrantes del Comité Técnico de Modernización comenzaron por realizar un diagnóstico de los principales problemas del tribunal, con la finalidad de elaborar propuestas para solucionarlos. Entre los objetivos que se buscaron esta: el fortalecimiento de la independencia del Magistrado, mejorar la eficiencia del órgano jurisdiccional y garantizar el acceso efectivo del ciudadano a la justicia. Para ello se establecieron varios componentes:

1. El componente "A" constituido por la Política Institucional, tuvo como objetivo el desarrollo de disposiciones que permitieran a la Corte Suprema de Justicia, la coordinación de una política judicial nacional. Ello incluyó la investigación, evaluación de la calidad y desempeño del sistema judicial, asumir la iniciativa legislativa, en las áreas relacionadas al Poder Judicial y la comunicación e información con la sociedad civil.

2. El componente "B" referido a la Actividad Judicial comprendió el nuevo modelo organizacional, la reorganización y redistribución de los procedimientos internos mediante los cuales se tramitan los asuntos en cada Sala, para alcanzar una economía de escala y una mayor eficiencia en la resolución de las causas.

3. El componente "C" representado por la divulgación de las sentencias, trazó como objetivo la publicación y divulgación de las decisiones, brindando a la ciudadanía un mayor conocimiento de la aplicación e interpretación del derecho que ejecutaba la Corte Suprema de Justicia.

4. El componente "D" referido al Apoyo Administrativo y Gerencial. Fijó como objetivo lograr la eficiencia de los servicios internos administrativos, que brindan apoyo a los Magistrados.

En tales términos, el Banco Mundial dio su aprobación al Proyecto de Modernización de la Corte Suprema de Justicia, en julio de 1997. El crédito aprobado era de 1 millón de dólares, mientras se terminaban de realizar los trámites para la aprobación definitiva del Proyecto.

Concretando lo anterior, el convenio signado con el núm. 3514-VE dio a conocer como uno de los productos más importantes el Juris 2000, considerado como una verdadera revolución judicial que adoptó cambios relevantes en la estructura y funcionalidad de la Administración de Justicia.

Por su parte, El convenio con el Banco Mundial para la modernización de la Corte Suprema de Justicia (4270-VE), dio a conocer sus primeros avances

de modernización con el uso intensivo de la tecnología de la comunicación e información (TIC) y de un sistema de gestión judicial denominado Tepuy XXI.<sup>10</sup>, considerado como un enorme éxito.<sup>11</sup>. La innovación permitió dejar atrás las obras impresas de las sentencias, las cuales no eran llevadas al día y sus consultas resultaban complejas, por lo poco manejable de los compendios, avanzando a publicaciones de resoluciones que se registraban en internet desde el mismo momento en que el magistrado las suscribía.

De lo reseñado, es importante señalar que dentro de las políticas asumidas en el proceso de modernización judicial no se formuló el desarrollo, instalación y perfeccionamiento de herramientas informáticas de seguridad, posiblemente por el poco conocimiento que se tenía para aquellos años de la instauración del proyecto, de la firma digital y de certificación electrónica en los sistemas de gestión, mecanismos que fueron regulados años más tarde por el Decreto-Ley sobre Mensajes de Datos y Firmas electrónicas del 2001.

## **1.2 Proceso de Implantación Juris 2000.-**

El Juris 2000 nace como uno de los productos del “Proyecto de infraestructura de apoyo al Poder Judicial”, que tenía como uno de sus objetivos la modernización de los tribunales de dos ciudades pilotos en una

---

<sup>10</sup> El “Tepuy XXI”, es un sistema desarrollado en el lenguaje de programación “*VISUAL BASIC2 6*”, y posee como manejador de base de datos “*ORACLE*” 10G; el objeto principal de esta aplicación es la automatización y manejo de los casos jurídicos de las diferentes Salas del Tsj desde el momento en que ingresan hasta su decisión final, facilitar apoyo a los usuarios internos en la realización de sus labores, suministrar información eficiente y oportuna a los usuarios externos, garantizando así, el acceso a la data del sistema judicial de todos los ciudadanos, en igualdad de condiciones. Disponible en: [www.cgr.gob.ve/pdf/.../ecotribunalsupremodejusticiasistema086](http://www.cgr.gob.ve/pdf/.../ecotribunalsupremodejusticiasistema086). (fecha de consulta: 18/08/2012)

<sup>11</sup> Estas afirmaciones se encuentran en el Implementation Completion Report del 28-06-02. El público tiene igualmente la percepción de un funcionamiento más eficiente, ordenado y abierto del Tribunal. Lamentablemente no conoce estudios de opinión realizados después de concluido el convenio con el Banco Mundial.

primera etapa, específicamente los tribunales penales de los palacios de Justicia de Barquisimeto, estado Lara, y Barcelona, estado Anzoátegui, y en una segunda etapa la modernización de otras seis ciudades adicionales, a través de la implantación de un nuevo modelo organizacional, Sistema de Gestión, Decisión y Documentación, denominado Juris 2000.

Ante la implantación del Modelo Organizacional y Sistema Juris 2000 en las sedes antes mencionadas se evaluó su impacto en cuanto al servicio de prestación de justicia, los cuales arrojaron resultados tan beneficiosos para el sistema judicial<sup>12</sup>, que se consideró conveniente continuar con la implantación de los mismos en las sedes de otras ciudades a nivel nacional.

Ahora bien, es importante señalar que como modelo organizacional la principal innovación del Juris 2000 radica en la creación de oficinas centralizadas de apoyo judicial, las cuales se encuentran divididas en dos grandes grupos: Las Oficinas de Apoyo Directo a la Actividad Jurisdiccional y Las Oficinas de Servicios Comunes Procesales, ubicadas éstas dentro de una misma sede judicial, creando así los Circuitos Judiciales establecidos en el artículo 269 de la Constitución de la República Bolivariana de Venezuela.

Las Oficinas de Apoyo Directo a la Actividad Jurisdiccional tienen a su cargo el archivo, el mantenimiento del orden dentro de la sede judicial, la atención al público, la recepción y distribución de los diferentes tipos de documento dirigidos a los tribunales ubicados en esa sede, y la práctica de notificaciones y citaciones.

---

<sup>12</sup> “El estudio de opinión mostró que el 62 por ciento de las personas que usaron los tribunales consideraron excelentes sus servicios y el 22 por ciento los consideraron buenos; el resto, según el caso, los considero regular o deficiente”. Scognamiglio, Laura L. *La Revolución Judicial en Venezuela*. Funeda, Caracas, 2011, p.36

Por su parte, las Oficinas de Servicios Comunes Procesales se encargan de la elaboración de actos de mero trámite, el control de los libros que se deben generar en los Juzgados, el control de los lapsos procesales, el control en la fijación de audiencias, entre otros.

Estas Oficinas de Apoyo al Poder Judicial tienen como finalidad que el juez pueda dedicarse el cien por ciento (100%) de su tiempo a estudiar el problema sometido a su conocimiento y emitir pronunciamientos que cada caso requiera, con una mayor celeridad, en virtud de la separación del juez de todas aquellas actividades administrativas que se encontraba ejecutando, lo cual permite, a su vez, importantes economías de escala, al existir un único personal asignado a todos los jueces ubicados en una misma sede, para que realicen estas tareas, a diferencia de las sedes en las cuales no se ha implantado el Modelo Organizacional y el Sistema Juris 2000, en las que cada juez dispone de un personal específico que ejecuta estas labores.

Es importante indicar que el Juris 2000 se apoya en un modelo arquitectónico, que establece un criterio de distribución de los espacios, de manera de que el usuario obtenga información sobre sus casos de forma expedita, pero siempre protegiendo la seguridad del archivo y del personal judicial. De esta manera, el diseño de los edificios tribunales con el Juris 2000 representa un reto importante, ya que debe lograr, por una parte, garantizar al ciudadano tanto el acceso rápido a la información, como la transparencia de las operaciones judiciales; y por la otra, proteger la confidencialidad de esa información y crear los mecanismos para asegurar la imparcialidad del juez, todo ello, sin sacrificar el funcionamiento eficiente del servicio de justicia.

Igualmente, de la mano de este Modelo Organizacional se encuentra el Sistema de Gestión, Decisión y Documentación Juris 2000, que como sistema de computación, permite la automatización del expediente procesal y la jurisprudencia de los tribunales, lo que genera celeridad a la función jurisdiccional y llevar un efectivo control, por lo que el usuario puede obtener una información precisa sobre sus casos y un mejor servicio de administración de justicia.

Este sistema aporta al ciudadano una mayor seguridad de los procesos judiciales que se encuentran tramitando en cada sede implantada, toda vez que el mismo evita la posible violación del Libro Diario, libro éste donde se asientan las actuaciones diarias realizadas por el juez en su gestión jurisdiccional, a través de su cierre automático; así como permite una mayor transparencia en la distribución de los asuntos que ingresan a las sedes judiciales, debido a que las mismas son llevadas de manera aleatoria, equitativa, imparcial y expedita, cumpliendo así con lo establecido en el artículo 26 de la Constitución de la República Bolivariana de Venezuela.

### **1.3 Naturaleza Funcional del Sistema Juris 2000.-**

Existen sistemas informáticos de diversos niveles de complejidad. De esta manera, habrá algunos para el manejo y seguimiento de causas, de tramitación electrónica, e incluso algunos que permiten la litigación en un ambiente Web sin necesidad de intervención humana. Desde sistemas que permiten la pura gestión documental, facilitando el registro, archivo y digitalización de documentos y contribuyendo a la existencia de procesos electrónicos, que identifican con facilidad todos los datos de una causa y monitorean el desempeño de la oficina judicial, el manejo de audiencias y del

valioso tiempo de jueces; hasta otros que combinan estas características con otras más complejas, como permitir la relación entre diversos actores del sistema judicial.

Considerando lo anterior, la Dirección Ejecutiva de la Magistratura ha señalado en sus diversos informes que *“El Juris 2000 es un modelo organizacional y sistema de gestión...”*<sup>13</sup>. Sin embargo, vale la pena hacer una comparación de las cualidades que ofrece este sistema automatizado, con los modelos procesales que señala el Centro de Estudios de Justicia de las Américas (CEJA)<sup>14</sup>, en el informe de las *“Perspectivas de uso e Impactos de las TIC en la Administración de Justicia en América Latina”*<sup>15</sup>, a los fines de determinar la funcionalidad, confiabilidad y seguridad de sus registros. Cabe destacar que el término “modelos procesales”, se usará no en un sentido jurídico, sino estrictamente en el sentido de distinguir el tipo de sistemas informáticos de seguimiento de causas, de acuerdo a su funcionamiento.

En el mencionado estudio se hace referencia a dos tipos de modelos procesales. El primero son los sistemas informáticos de seguimiento procesal; y lo segundos los sistemas de gestión o de control de gestión, los cuales se detallaran por separado en el siguiente punto.

---

<sup>13</sup> Dirección Ejecutiva de la Magistratura. *Juris 2000. El Modelo Organizacional*. [Documento en línea]. Disponible en: <http://www.dem.gob.ve>. (fecha de consulta: 25/07/2010)

<sup>14</sup> El Centro de Estudios de Justicia de las Américas (CEJA) es un organismo internacional, cuya misión es apoyar a los Estados de la región en sus procesos de reforma a la justicia, para lo cual desarrolla actividades de capacitación, estudios e investigaciones empíricas, entre otras acciones. Disponible en: <http://www.cejamericas.org>.

<sup>15</sup> Hernández, C. y Adelardi, R. *“Perspectivas de uso e impactos de las TIC en la administración de justicia en América Latina”* (2008). [Documento en línea]. Disponible en: <http://www.cejamericas.org>. (fecha de consulta: 26/08/2010)

### *1.3.1 Sistema de Seguimiento Procesal.-*

Los sistemas informáticos de seguimiento procesal o de tramitación de casos son los que permiten registrar los datos y movimientos relacionados con el ingreso, actuaciones y término de casos que recibe o inicia un tribunal, aunque el concepto es aplicable totalmente al seguimiento que requiere un despacho fiscal o uno de defensores, con algunas particularidades.

Su objetivo o resultado esperado es mejorar el control del avance del proceso judicial, consiguiendo reducciones en los tiempos procesales, mayor seguridad en el resguardo de información, y mayor acceso de las partes al caso. Constituyen la base para el desarrollo de otro tipo de aplicaciones, como los sistemas de estadísticas judiciales, los sistemas de control de gestión o los sistemas administrativos, entre otros, ya que permiten registrar los datos que posteriormente serán empleados, total o parcialmente por esos otros sistemas. Las funcionalidades mínimas para este tipo de sistemas son:

a) Que proporcione al menos información acerca de los intervinientes del caso, de los movimientos y el estado de tramitación de la causa.

A este respecto, el Sistema Juris 2000 ofrece los datos de quienes forman parte del litigio (nombre, sexo, estado civil, dirección, teléfono, nacionalidad, fecha de nacimiento, entre otros) y del rol de cada uno en el caso (demandante, demandado, abogado, representante, entre otros), registro que permite posteriormente obtener cruces valiosos de datos entre causas para saber si un interviniente tiene otras causas en trámite.

En cuanto a los movimientos del caso, señala qué acciones (acontecimientos) han tomado las partes, que puede variar desde identificar

todos los documentos que han entregado éstas en un proceso basado en expedientes, hasta las peticiones realizadas durante las audiencias orales. En relación al estado de la causa, muestra el avance procesal de ésta, lo que le permite a las partes saber la etapa en que se encuentra el caso.

b) Que sea capaz de soportar el registro de todos los datos relevantes desde el punto de vista de la información estadística que se elabora a partir del movimiento de casos. Esto no implica necesariamente que el sistema de tramitación deba ser en sí mismo un sistema estadístico, pero al menos debe proporcionar parte de la materia prima útil para los sistemas especializados en estadísticas judiciales.

Bajo este planteamiento el Juris 2000, de forma simultánea, optimiza el procesamiento de casos, produce estadísticas cuantitativas y valorativas del desempeño de un tribunal específico o de un conjunto de estos. A su vez, proporciona reportes de seguimiento procesal de causas en trámite. Sin embargo, es necesario aclarar, que aun cuando el sistema proporciona una herramienta automatizada de estadísticas cuantitativas en formato Excel, es inoperante en la mayoría de las sedes en las que se halla implementado este software de gestión. La data de las estadísticas mensuales que se reportan son obtenidas de manera manual de los listados que registra el Juris respecto a los asuntos en trámite, asuntos ingresados, egresados, asuntos paralizados, asuntos terminados, audiencias iniciales, diferidas, realizadas, entre otras. La fiabilidad de la estadística dependerá del llenado y registros del sistema.

c) Se requiere que estos sistemas apoyen a los jueces con información legal actualizada y con jurisprudencia relevante, de forma ágil y confiable, de

manera de facilitar el estudio de algún caso en particular, o de criterios jurídicos, en general, para poder elaborar sus sentencias y otras resoluciones.

Para el sistema automatizado Juris 2000, esta herramienta la constituye el denominado “*Sistema Documental*”, el cual da a conocer a las decisiones judiciales, permite la publicación de aquellas que constituyen jurisprudencia, esto es, que contengan una interpretación novedosa de la ley y que tenga eficacia orientadora en la resolución de los casos sometidos al conocimiento jurisdiccional, además, mantiene un registro de la información legal necesaria. No obstante, esta es una herramienta en que no es operativa en la mayoría de las sedes judiciales por no mantenerse actualizada.

A los efectos de determinar que decisiones tienen el carácter de jurisprudencia, se requiere la creación de un comité de juristas que estudie y evalúe los fallos que los jueces de primera instancia y de la Corte de Apelaciones o Superiores, estimen remitir a dicho comité por considerarlas jurisprudencia.

d) Desde el punto de vista del control de la tramitación, los sistemas deben ser trazables, esto es, proporcionar información acerca de quiénes y cuándo ha ingresado información relacionada con la tramitación de una causa. Sin embargo cuando se trata de agregación de documentos a un expediente físico, se pueden presentar dos modalidades:

- Aquella en la cual las actuaciones y resoluciones que emite el tribunal en el marco de un caso, se realizan por parte del personal del tribunal en el sistema informático, y desde aquí se imprime la resolución y se agrega al

expediente. Respecto a los documentos provenientes de terceros, en algunos casos estos se escanean, o incluso se puede pedir en forma electrónica, para luego agregarse al expediente físico. En esta situación, el sistema informático podría contener un expediente electrónico que sea espejo del expediente físico.

- Aquella en la cual en el sistema informático solamente se registra que ha ingresado un documento desde el exterior del tribunal, o que el tribunal ha emitido un documento, pero solo se consignan datos resumidos de tales documentos. En ese caso, el sistema informático, si es que estuviera bien diseñado, permite saber el estado del caso y algunos datos de los movimientos acaecidos y antecedentes de las partes, pero si se desea saber el contenido de las resoluciones del tribunal, se debe revisar físicamente el expediente.

En estas dos modalidades que señala el estudio del CEJA, existen variaciones respecto de cuanta similitud tenga el registro electrónico con el físico.

El Sistema Juris 2000, por señalamientos de la jurisprudencia, presenta limitaciones en la información de sus registros, ya que los mismos *“aportan un resumen de las actuaciones pero no las transcriben y, en ese sentido, el acceso al expediente a través del sistema es limitado”*<sup>16</sup>. No obstante, esa limitación es presentada cuando corresponde a documentos que vienen de las partes como por ejemplo, la presentación de la demanda, la contestación,

---

<sup>16</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia Nº 04-3055 de fecha 21 de marzo de 2006. (Alida Teresa Pernalette Gásperi vs. Coordinadora del Circuito de Protección del Niño y del Adolescente del Estado Lara, abogada Erlinda Oropeza) Disponible en: <http://www.tsj.gov.ve>. (fecha de consulta: 15/05/2010).

solicitudes, donde la data consiste en una transcripción parcial de lo presentado por las partes. Pero cuando son actuaciones del tribunal, la información debe ser dispuesta en el sistema automatizado a través del asociado de un documento con el mismo formato de un documento Word.

### *1.3.2 Sistemas de Gestión o de Control de Gestión.-<sup>17</sup>*

El sistema de gestión procesal permite la automatización de la tramitación de los procedimientos y los procesos judiciales en sus diferentes fases: registro, reparto, tramitación, agenda, resoluciones, ejecución, entre otras. Para ello aporta soluciones en tres áreas de actuación:

1. *Gestión de expedientes judiciales*: basada en el modelo de tramitación judicial definido, da soporte automatizado a todas las fases de la gestión de los expedientes y a las necesidades de comunicación entre las Oficinas Judiciales, las Fiscalías y los Servicios Comunes.

2. *Servicios comunes*: en la organización judicial hay tareas como el apoyo a jueces y magistrados, la ordenación del procedimiento, notificaciones, la gestión de efectos y piezas de convicción, las ejecuciones o el archivo, que albergan funciones específicas que requieren un tratamiento especializado para poder realizar esa tarea de forma común para los órganos judiciales correspondientes.

Por su parte Julio Téllez Valdés<sup>18</sup> señala que este tipo de aplicación ha dado lugar a la llamada informática Jurídica con un enorme desarrollo en la

---

<sup>17</sup> Administración de Justicia Electrónica. Ibermatica. [Documento en línea]. Disponible en: [www.ibermatica.com/a.landa](http://www.ibermatica.com/a.landa). (fecha de consulta: 05/08/2011)

actualidad, considerando numerosos ejemplos de actividades automatizadas a nivel judicial como la formulación agenda de jueces, hasta la redacción automática de textos jurídicos a manera de sentencias. En el medio hay una enorme cantidad de acciones desarrolladas en juzgados, siendo uno de los casos más representativos la aceptación, registro e indicación de competencia y seguimiento de los expedientes. Una causa nueva que debe ser radicada ante un tribunal, pasa previamente por la inscripción automática, la cual le asigna un número, juzgado y verifica si hay o no conexidad de la causa.

De las dos modalidades de sistemas referidas, se puede concretar que el Juris 2000 ofrece características tanto de un sistema de seguimiento procesal como se observó de la comparación realizada, en cada una de las características que este tipo ofrece; y de un sistema de gestión como lo ha señalado los diversos informes de la Dirección Ejecutiva de la Magistratura ya que las diferentes fases del proceso pueden ser conocidas en cualquier momento, permitiendo verificar el estado del juicio, así como el lugar donde se encuentra el expediente (secretario, asistente, alguacil, entre otros).

---

<sup>18</sup> Téllez Valdés, Julio. *Informática Jurídica: Documentaria, Control y Gestión*. [Documento en línea]. Disponible en: <http://biblio.juridicas.unam.mx/libros/1/313/4.pdf>. (fecha de consulta: 21/11/2011)

## CAPITULO II. BASE NORMATIVA DE LA IMPLEMENTACIÓN DEL JURIS 2000 EN LA ADMINISTRACIÓN JUDICIAL VENEZOLANA

Del apoyo del Banco Mundial para la reforma, fueron consideradas varias iniciativas normativas de importancia. Pérez Perdomo<sup>19</sup> señala que distintos trabajos legislativos concluyeron en 1998, siendo uno de los más relevantes, la aprobación del Código Orgánico Procesal Penal (COPP). Este incluyó el establecimiento de los circuitos o tribunales corporativos, en los cuales se consolidó la estructura administrativa que se conoce hoy día en las sedes judiciales, de manera que los funcionarios prestaran servicio a un conjunto de jueces y las tareas de gestión recayeran en un solo juzgador. Este juez presidente, tiene a su cargo la organización y también la supervisión de los demás jueces. Es un cambio substancial, que no sólo modificó la infraestructura funcional de la oficina judicial, manejada con reglas definidas por la tradición, completamente arcaicas y donde la última innovación tecnológica aceptada, era la máquina de escribir, sino que, además, se instauraron nuevos principios para el juzgamiento en Venezuela.

Posteriormente, el artículo 269 de la Constitución de la República Bolivariana de Venezuela consagró el nuevo modelo organizacional de la función jurisdiccional, de los Circuitos Judiciales, señalando que *“La ley regulará la organización de circuitos judiciales, así como la creación y competencias de tribunales y cortes regionales a fin de promover la descentralización administrativa y jurisdiccional del Poder Judicial”*.

---

<sup>19</sup> Pérez P, Rogelio. Reforma Judicial, Estado de Derecho y Revolución en Venezuela. [Documento en línea]. Disponible en: <http://accesoalajusticia.org/documentos/detalle.php?mrdstartid=10&catid=33>. (fecha de consulta: 16/02/2011).

En función de los Convenios suscritos por Venezuela con el Banco Mundial, para el mejoramiento y modernización del Poder Judicial se logró como producto final para los Tribunales, tanto el diseño de un Modelo Organizacional, como de un Sistema Integral de Gestión, Decisión y Documentación JURIS 2000, los cuales requirieron que se dictaran normas reguladoras para el desarrollo de las funciones a desempeñar. Disposiciones que se detallaran a continuación, en atención de la infraestructura (modelo organizacional) y del elemento tecnológico (sistema automatizado).

### **2.1 Regulación Normativa del Modelo Organizacional.-**

La base normativa de la implantación tanto del modelo organizacional como del sistema automatizado, descansa en la Resolución N° 70 de fecha 27 de agosto de 2004, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.015 de fecha 3 de septiembre de ese mismo año. En sus disposiciones generales, contenidas en el artículo 1º, se ordena la creación progresiva de la estructura organizativa y funcional necesaria para implantar y desarrollar en todos los Tribunales del país el sistema de Gestión, Decisión y Documentación Juris 2000, el cual deberá ser obligatoriamente utilizado en el desarrollo de sus actividades y ejercicio de sus funciones.

Es importante resaltar, que cada materia en las que por especialidad se haya implantado el Juris 2000, está regulada por una resolución aparte, como se detalla en el cuadro a continuación:

MATERIA	N° DE RESOLUCIÓN	N° DE GACETA
Circuitos Judiciales Penales	Resolución N° 1.484 de fecha 30 de octubre de 2003 publicada en la Noviembre de 2003.	Gaceta Oficial N° 37.810 de fecha 4 de noviembre de 2004.
Corte Primera y Segunda de lo Contencioso Administrativo	Resolución N° 68 de fecha 27 de agosto de 2004.	Gaceta Oficial N° 38.011 de fecha 30 de agosto de 2004.
Circuitos Judiciales de Protección	Resolución N° 69 de fecha 08 de octubre de 2004.	Gaceta Oficial N° 38.011 de fecha 30 de agosto de 2004.
Circuitos Judiciales del Trabajo	-Resolución N° 1.475 de fecha N° 03 de octubre de 2003. -Resolución N° 2003-00017 de la Sala Plena del Tribunal Supremo de Justicia.	-Gaceta Oficial N° 37.806 de fecha 29 de octubre de 2003. -Gaceta Oficial N° 37.756 de fecha 19 de agosto de 2003.

Cuadro 1: Elaboración de la Autora.

El artículo 33 de la Resolución 70 ha señalado que sus normas son subsidiarias a las presentadas en otras resoluciones que regulen materias especiales, las cuales deben aplicarse con preferencia. Sin embargo, las consideraciones que a continuación se exponen, serán realizadas en base a la Resolución 70 que sienta las bases legales previas a la implantación del modelo organizacional y del sistema automatizado. Así se tiene que:

En primer lugar, la Resolución se detiene en su artículo 2, en hacer una definición de lo que se conoce como circuitos judiciales, señalando que se trata de la *“integración de tribunales ubicados en una misma sede, a los efectos de dotarlos de una estructura común que soporte la realización*

*eficaz de la actividad jurisdiccional*”. Proposición regulatoria ya prevista en el Código Orgánico Procesal Penal del año 1998, que disponía en su artículo 530 que en toda circunscripción judicial se creará “...una organización jurisdiccional y administrativa... que se denominará Circuito Judicial Penal...”.

Por su parte, el funcionamiento de los Circuitos Judiciales, está enmarcado dentro de los postulados previstos en el artículo 5 de la Resolución:

1. Jueces dedicados exclusivamente a la actividad jurisdiccional. Es decir, los jueces no tienen ahora otra función que cumplir la estrictamente jurisdiccional, razón por la cual podrán dedicarse al estudio de la doctrina, de la jurisprudencia, del derecho comparado y de los casos subjudice, elevando indudablemente la calidad de la justicia.

2. Limitación del contacto entre el público en general y los jueces. Postulado que guarda absoluta correspondencia con el artículo 26 constitucional que establece que el Estado debe garantizar una justicia imparcial, transparente e independiente.

Para el cumplimiento de estos postulados, el artículo 4 de la Resolución ha señalado que los Circuitos Judiciales deberán estar apoyados por las Oficinas de Apoyo Directo a la Actividad Jurisdiccional y las Oficinas de Servicios Comunes Procesales, cuya regulación será resumida en el siguiente cuadro:

**OFICINAS DE APOYO DIRECTO A LA ACTIVIDAD JURISDICCIONAL**

Artículo 11 (conformación): representado por un Coordinador Judicial que se encargará de supervisar, dirigir y controlar Oficinas de Apoyo Directo a la Actividad Jurisdiccional.

<b>Oficinas</b>	<b>Regulación</b>
<i>Unidad de Recepción y Distribución de Documentos (U.R.D.D.)</i>	Artículo 13: Encargada de recibir y distribuir internamente, de forma física (por intermedio de la Unidad de Correo Interno) y automatizada, cualquier documento (asuntos nuevos, correspondencia dirigida a los tribunales, solicitudes, recursos y otras actuaciones) que este dirigido a los Tribunales.
<i>Oficina de Atención al Público (OAP)</i>	Artículo 18: Esta oficina estará integrada por un número de auxiliares administrativos, y será la encargada de atender al público en general y de aportar la información a los interesados legitimados sobre el estado de la causa en la cual intervienen.
<i>1. La Unidad de Seguridad y Orden (USO)</i>  <i>2. Unidad de Correo Interno (UCI)</i>  <i>3. Unidad de Actos de Comunicación (UAC)</i>	1. Artículo 21: Encargada de preservar la seguridad interna y externa de la sede del circuito judicial penal; custodiar y trasladar procesados al interior de la misma y resguardar el orden tanto en las salas de audiencias como en el resto del circuito. Está integrada por un número suficiente alguaciles según sea necesario.  2. Artículo 22: Encarga de proporcionar el servicio de transporte de documentos, expedientes, oficios, etc., en el interior de la sede judicial y estará integrada por un número suficiente de alguaciles suficientes, quienes realizaran tres recorridos diarios por los diferentes despachos ubicados en las sedes.  3. Artículo 23: Unidad se encarga de practicar las citaciones, notificaciones, solicitudes de las partes, enviar oficios, expedientes, comisiones u otro tipo de comunicación hacia entes externos de la sede judicial.
<i>Archivo de Sede (AS)</i>	Artículo 25: Tiene a su cargo conjuntamente con el personal adscrito a esa dependencia mantener el archivo de los asuntos, libros, copiadores, y demás instrumentos ordenados por ley, que se encuentran en curso y, que por lo tanto, necesitan una gestión centralizada que garantice el control de su ubicación en cada momento, tanto si están bajo la custodia de la oficina de tramitación como si es el propio archivo el que tiene el asunto en su poder.

<b><u>OFICINAS DE SERVICIOS COMUNES PROCESALES</u></b>	
Artículo 27: Encargadas de dar apoyo al Juez en cuanto a la tramitación y sustanciación de los expedientes.	
<b>Oficinas</b>	<b>Regulación</b>
<i>Oficina de Secretarios Judiciales (OSJ)</i>	<p>Artículo 28: Esta dependencia administrativa-judicial, está conformada por todos los Secretarios de una misma sede judicial quienes estarán dirigidos por un Coordinador de Secretaría y cuyas atribuciones principales según el artículo 28 son:</p> <ul style="list-style-type: none"> <li>• Dirigir, supervisar y controlar las actividades que realicen los secretarios organizados en pool.</li> <li>• Supervisar el correcto manejo y mantenimiento de los Libros Diarios, Libros de Acuerdos y Decretos y demás Libros registrados.</li> <li>• Prestar apoyo a los jueces en el ejercicio de la función jurisdiccional.</li> <li>• Llevar el control de la agenda de audiencias a celebrarse.</li> <li>• Según el artículo 29 los secretarios ejercerán las funciones que les asignen las leyes vigentes.</li> </ul>
<i>Oficina de Tramitación de Asuntos Procesales (OTAPRO)</i>	Artículo 30: Conformada por asistentes que tendrán a su cargo la sustanciación de los asuntos. La supervisión de esta oficina será realizada por un Coordinador de Asistentes, cuando se requiera por el volumen del personal y asuntos en trámite.

Cuadro 2: Elaboración de la Autora.

Estas regulaciones normativas han sido complementadas con un conjunto de manuales dispuestos para definir la estructura organizativa y funcional de las oficinas y unidades que integran las dependencias de la Dirección Ejecutiva de la Magistratura y del Poder Judicial, los cuales se exponen a continuación:

1. *Manual de Organización de las Oficinas de Servicios Comunes Procesales*: se constituye como una herramienta de consulta, tanto para el

nivel supervisorio como para el nivel operativo, en cuanto a definición de objetivos y funciones que deben ejecutar, lo cual contribuirá al alcance de los mismos y al mejoramiento continuo de la calidad del servicio prestado por estas Oficinas.

2. *Manual de Normas y Procedimientos para el Archivo de la Sede (As)*: suministra al Archivo de la Sede de los Tribunales una herramienta metodológica que le permita agilizar los procesos de recepción, archivo físico, control y traslado, préstamo y devolución de Asuntos, dentro de la sede judicial.

3. *Manual de Normas y Procedimientos para la Unidad de Apoyo Audiovisual (UAA)*: suministra una herramienta administrativa que permita establecer la metodología para la solicitud de los equipos audiovisuales y del personal técnico encargado de su operación, esto con la finalidad de desarrollar grabación y filmación de las audiencias y los actos de informes orales.

4. *Manual de Normas y Procedimientos para la Unidad de Actos de Comunicación (UAC)*: suministra a la Unidad de Actos de Comunicación de los Tribunales del Trabajo, una herramienta administrativa que agilice el conjunto de acciones orientadas al manejo de notificaciones, citaciones, oficios y otros documentos de comunicación externa.

5. *Manual de Normas y Procedimientos para la Oficina de Atención al Público (OAP)*: suministra a la Oficina de Atención al Público (OAP), una herramienta metodológica que le permita agilizar los procesos de suministro de información, entrega de documentos y videos.

6. *Manual de Normas y Procedimiento para la Unidad de Correo Interno (UCI)*: suministra a la Unidad de Correo Interno (UCI) en los Circuitos Judiciales, una herramienta metodológica que le permita agilizar los procesos de traslado y entrega de documentos, correspondencia y expedientes dentro de la sede judicial de los tribunales.

7. *Manual de Normas y Procedimientos para la Unidad de Seguridad y Orden (USO)*: suministra a la Unidad de Seguridad y Orden un instrumento administrativo que permita normalizar el proceso de seguridad y orden dentro de la sede judicial, garantizando así la protección de los bienes y personas en los despachos de los tribunales del trabajo y/o mantenimiento del orden en las salas de audiencia.

8. *Manual de Normas y Procedimiento para la Oficina de Control de Consignaciones (OCC)*: suministra a la Oficina de Control de Consignaciones de Tribunales, una herramienta metodológica que le permita agilizar los procesos de recepción de consignaciones por oferta real de pago, de solicitud de calificación de despido, de entrega de libretas de ahorros y custodia y entrega de valores mercantiles y/o instrumentos bancarios.

9. *Manual de Normas y Procedimiento para la Unidad de Recepción y Distribución de Documentos (URDD)*: suministra a la Unidad de Recepción y Distribución de Documentos (URDD) en los Circuitos Judiciales de una herramienta metodológica que permita agilizar los procesos de recepción y distribución de asuntos.

## **2.2 Regulación Legal del Sistema Integral de Gestión, Decisión y Documentación JURIS 2000.-**

En la Regulación N° 70 son escasas las disposiciones referidas a la implantación del elemento tecnológico del Sistema automatizado Juris 2000, sin embargo, en sus disposiciones se pueden abordar algunas consideraciones relevantes:

*1. De los Registros Automatizados de los Libros Diarios:* El artículo 8 de la Resolución ha dispuesto que los Libros Diarios que deben llevar los Jueces de los Circuitos Judiciales y donde deben asentarse todas las actuaciones procesales realizadas diariamente, se obtendrán *“de la impresión de los archivos digitalizados, contenidos en el Juris 2000, que deberá compilarse por Tomos, bajo serie numérica, con la debida firma del Juez y del secretario...”*. Esto último es una formalidad que debe cumplirse a los efectos de dar fe pública a los reportes que suministra el Sistema, ya que estos por si solos no otorgan la formalidad legal de un documento público. Esto último a no ser que se dé cumplimiento a las herramientas tecnológicas que ofrece el Decreto-Ley de Mensaje de Datos y Firmas Electrónicas del año 2001, del firma digital o electrónica y certificado electrónico.

Cuando la eficacia y valor jurídico de la firma electrónica se incorpore al desempeño de los Jueces y con ello el servicio de las autoridades de certificación electrónica, se estará en presencia de un verdadero documento público, tal y como lo dispone, por ejemplo, el Decreto Presidencial de Ley de Registro Público y del Notariado, de fecha 13 de noviembre del año 2000, el cual establece en su artículo 5, que *“La firma electrónica de los*

*Registradores y Notarios tendrá la misma validez y eficacia probatoria que la ley otorga a la Firma autógrafa”.*

2. Por su parte, el literal b del artículo 9, señala que “...*Los Tribunales ubicados en un mismo circuito, tendrán conjuntamente, un registro de Entradas y Salidas de Causas, un Libro Índice y de Registro de Expedientes, éstos últimos podrán ser compilaciones de actas derivadas del sistema...*”.

3. El artículo 17 ha referido que a los fines de regularizar la fecha y la hora de registro en el sistema Juris 2000 de cualquier escrito, libelo de demanda, solicitud, diligencia u otro tipo de documento, se entiende la fecha y hora de ingreso de dichos documentos en la URDD. Sin embargo, nada más se regulo respecto a la certeza del tiempo que deben contener los servidores en el registro de los documentos electrónicos del sistema. Existen certificados que permiten determinar el día y la hora en que un documento fue digitalmente firmado, llamados también Digital time-stamp certificates.

Peñaranda ha referido que las autoridades de fechado digital (Tsa O Time Stamping Authorities) “*vinculan un instante de tiempo a un documento electrónico avalando con su firma la existencia del documento en el instante de tiempo referenciado, así es como se podrían resolver los problemas de la exactitud en el tiempo de los documentos electrónicos*”.<sup>20</sup> Es decir, determinan fechados fraudulentos antes o después de la fecha consignada, e impiden alterar el contenido del documento luego de la firma. Pero para ello, es necesario que se materialice la implementación de la firma digital y la certificación técnica de las actuaciones judiciales.

---

<sup>20</sup> Peñaranda Q, Héctor R. *El Documento Electrónico como Medio de Prueba en el Proceso Civil Venezolano*. Trabajo Especial de Grado. Universidad del Zulia. Maracaibo. 2005, p.p. 79-80

4. Finalmente, el artículo 35 ha abierto la posibilidad de avanzar la sistematización judicial al cumplimiento de herramientas tecnológicas que permitan materializar un proceso judicial más efectivo. En consecuencia, esta disposición ha señalado que:

*“A los efectos de realizar las notificaciones y demás actos de comunicación, las oficinas mencionadas en la presente Resolución, podrán utilizar, una vez que estos estén debidamente implementados, los mecanismos que señala el Decreto con Rango y Fuerza de Ley N° 1204 de fecha 10 de febrero de 2001, de Mensaje de Datos y Firmas Electrónicas publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148 del 28 de febrero de 2001”.*

## CAPITULO III. LA CERTIFICACIÓN TÉCNICA DE LAS ACTUACIONES Y EL DEBIDO PROCESO EN UN SISTEMA AUTOMATIZADO DE JUSTICIA.-

### 3.1. Consideraciones Preliminares.-

Este capítulo define las ventajas y cualidades que ofrece la certificación electrónica en los sistemas automatizados de gestión judicial, así como, la incorporación de ésta en el mundo de las relaciones jurídicas, sustentada como una garantía que permita a los ciudadanos ejercitar su defensa, en el marco de una sucesión de actuaciones judiciales, dando fiel cumplimiento al debido proceso.

Ahora bien, la noción de la certificación electrónica, ofrece un conjunto de precisiones técnicas a considerar, siendo el primero de ellos, el referido a la seguridad de la información, por constituirse la base de cualquier sistema automatizado que mantenga tráfico de documento electrónico.

Granados Paredes<sup>21</sup> refiere la seguridad de la información como el conjunto de reglas, planes y acciones que permiten asegurar la información, manteniendo las propiedades de confidencialidad, integridad y disponibilidad de la misma.

*a.- La confidencialidad* es que la información sea accesible sólo para aquéllos que están autorizados.

*b.- La integridad* es que la información sólo puede ser creada y modificada por quien esté autorizado a hacerlo.

---

<sup>21</sup> Granados P, Gibran. Introducción a la Criptografía. Revista Digital Universitaria. Volumen N° 7, JULIO 2006. [Documento en línea]. Disponible en: [http://www.revista.unam.mx/vol.7/num7/art55/jul\\_art55.pdf](http://www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf). (fecha de consulta: 01/09/2012)

c.- La *disponibilidad* es que la información debe ser accesible para su consulta o modificación cuando se requiera.

Además, este autor también hace la distinción con el término *seguridad informática* que está constituido por el conjunto de políticas y mecanismos que permiten garantizar la confidencialidad, la integridad y la disponibilidad de los recursos de un sistema (entiéndase recursos de un sistema como memoria de procesamiento, espacio de almacenamiento en algún medio físico, tiempo de procesamiento, ancho de banda y por supuesto la información contenida en el sistema).

La Ingeniera Clara Boanza<sup>22</sup>, define la seguridad de la información como la habilidad para proteger la información y los recursos respecto a la confidencialidad y la integridad. En este sentido, es preciso garantizar la autenticación, confidencialidad, integridad y disponibilidad.

De acuerdo, a las definiciones anteriores, la seguridad de la información es la garantía que permite que un proceso automatizado sea confiable, ofrezca autenticidad y credibilidad a los usuarios y sobre todo a un sistema de justicia que cuente con estas herramientas, a través de una serie de mecanismos y políticas de procesamiento tecnológico. En consecuencia, la certificación digital o electrónica es una de las acciones más novedosas para asegurar el patrimonio informático de las instituciones públicas, que manejan como sistema de apoyo las Tecnologías de la Información y Comunicación (TIC).

---

<sup>22</sup> Boanza, Clara. *Integridad y Confiabilidad de la Información*. [Documento en línea]. Disponible en: <http://www.cypsela.es/especiales/pdf206/confidencialidad.pdf>. (fecha de consulta: 21/11/2011).

## 3.2 La Certificación Técnica o Electrónica.

### 3.2.1 Definición.-

SUSCERTE<sup>23</sup> señala que la certificación electrónica es un área que involucra políticas, procedimientos, infraestructura, estándares y equipamiento, que hacen posible el ciclo de vida de un certificado y su uso, con las garantías que dictan los estándares de seguridad electrónica. Esto permite al usuario confiar en operaciones como la firma electrónica, correo electrónico seguro, fecha y hora certificada, entre otras.

Por otra parte, define al certificado electrónico como un documento electrónico emitido por un Proveedor de Servicios de Certificación<sup>24</sup>, que vinculado a un usuario (signatario) con su firma electrónica, el mismo está compuesto por dos elementos (clave pública y clave privada), con el cual se identifica al propietario del mismo y permite la generación de firmas electrónicas. La clave pública es un conjunto de datos de carácter público que vinculan al remitente con el mensaje y que permiten cifrarlo. La clave privada, por su parte, es aquella combinación secreta que se utiliza para descifrar el mensaje y sólo la posee el receptor.

---

<sup>23</sup> Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) es el organismo encargado de coordinar e implementar el modelo jerárquico de la infraestructura Nacional de Certificación Electrónica, también acredita, supervisa y controla a los Proveedores de Servicios de Certificación (PSC) y es el ente responsable de la Autoridad de Certificación Raíz del Estado Venezolano. Así mismo tiene como alcance proveer estándares y herramientas para implementar una tecnología de información óptima en las empresas del sector público, a fin de obtener un mejor funcionamiento y proporcionar niveles de seguridad confiables. [Documento en línea]. Disponible en: <http://www.SUSCERTE.gob.ve>. (fecha de consulta: 21/11/2011).

<sup>24</sup> Persona dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en este Decreto-Ley de Mensajes de Datos y Firmas Electrónicas. [Documento en línea]. Disponible en: <http://www.SUSCERTE.gob.ve>. (fecha de consulta: 21/11/2011).

Esto último implica que el certificado electrónico requiere de la implementación previa de la firma digital para materializar su finalidad, que no es otra que la de otorgarles validez lo cual resulta indispensable en los sistemas automatizados de justicia para configurar fe pública, autenticidad y no repudio en los documentos electrónicos (actuaciones judiciales) que se registran.

Díaz, en su estudio sobre la “*Desnaturalización del Documento Electrónico Judicial con la Apelación de la Sentencia*”, define el certificado electrónico como:

*“El documento digital de identidad emitido a una persona (natural o jurídica). La emisión está bajo la responsabilidad de una entidad de certificación debidamente autorizada. Esta entidad garantiza la veracidad de los datos relativos a una persona y contenidos en el citado documento. El Certificado Digital es una herramienta clave para la identificación de las partes contratantes en el comercio electrónico. Este documento digital podría equipararse conceptualmente aun Documento de Identidad, Licencia, pasaporte o carné de empresa...”<sup>25</sup>*

Un certificado digital básicamente es un documento digital expedido por una autoridad de confianza que contiene los datos que identifican al dueño del certificado, su llave pública, fecha de expedición, fecha de caducidad, los datos de la autoridad de confianza y finalmente todo esto está firmado por la misma autoridad. Sirven para establecer lazos de confianza entre sistemas o personas, ya que si se confía en la autoridad de certificación, entonces se puede confiar en la llave pública del dueño del certificado, tratando así de resolver el problema de relacionar las identidades con las llaves públicas.

---

<sup>25</sup> Díaz G, Alexander. *Desnaturalización del Documento Electrónico Judicial con la Apelación de la Sentencia*. El Juicio Oral en el Nuevo Sistema Penal Acusatorio Colombiano. [Documento en línea]. Disponible en: <http://www.alfa-redi.org/sites/default/files/articles/files/Diaz.pdf>. (fecha de consulta: 21/11/2011).

De lo anterior se observa, que las definiciones realzan el término *identidad* de los usuarios involucrados en un proceso automatizado de emisión de datos, que es lo que se conoce como la *entidad electrónica*. De acuerdo, con SUSCERTE, la identidad electrónica es:

*“Un conjunto de rasgos que caracterizan a un individuo o colectivo en un medio de transmisión electrónico. En efecto, cuando se habla de Identidad Electrónica no es más que la asociación entre un ente físico y un ente electrónico, es decir, es un conjunto de datos electrónicos asociados a cada persona: nombre, apellido, dirección de correo, contraseñas, etc., que hace diferente a un individuo de otro que usa el mismo tipo de identidad”<sup>26</sup>.*

Generalmente, se trata de una "personalidad" electrónica que permite ser reconocido e identificado tras la introducción de un nombre de usuario y una contraseña. Y es en este punto, donde vale la pena preguntarse, si el Sistema Juris 2000 ofrece las bondades de una verdadera identidad electrónica, siendo importante evaluar la validación y autenticación de su data.

En los Criterios generales de seguridad de los sistemas de información al servicio de la Administración de Justicia se ha señalado que:

*“Los sistemas de información (y software de base) dispondrán de mecanismos de identificación y autenticación que prevengan los accesos no autorizados basados en la existencia de un identificador unívoco de usuario y contraseña, o mediante la utilización de certificado digital o algún otro mecanismo de protección suficientemente probado, dado el estado de la tecnología en cada*

---

<sup>26</sup> Hernández, R; Berrios, Kranya y González, Víctor. *Identidad Electrónica*. SUSCERTE. [Documento en línea]. Disponible en: [www.SUSCERTE.gob.ve](http://www.SUSCERTE.gob.ve). (fecha de consulta: 21/11/2010)

*momento y las características de la información a proteger*".<sup>27</sup>

Basado en lo citado, el Juris 2000 es un sistema de identificación, con usuario y contraseña (login o password), donde la creación del usuario se realiza atendiendo al procedimiento establecido y con previa autorización del responsable competente, que en este caso es la Oficina de Desarrollo Informático (ODI) adscrita a la Dirección Ejecutiva de la Magistratura (DEM). La asignación de contraseña inicial será provisional pudiendo ser personalizada en cualquier momento por los funcionarios. Este sistema no permite asociar períodos de validez a los identificadores de usuario de forma que fuera de ese rango de fechas, el sistema prevenga la autenticación a través de dicho identificador, sino que dependerá del usuario la modificación de su clave de acceso. Además hay que agregar que no existe un histórico de contraseñas que prevenga la re-utilización de la contraseña anterior.

En consecuencia, si existe un control de acceso a los servicios del sistema Juris 2000, cuyo tráfico es recogido por un sistema log file<sup>28</sup> que regula el comportamiento de los usuarios conectados a la red, pero que no puede verse como una verdadera identidad electrónica por las limitaciones que presta en cuanto al tema de la seguridad.

Una de las principales vulnerabilidades que tienen los análisis logfile es que el único modo de determinar la autoría de la navegación es mediante la

---

<sup>27</sup> Criterios generales de seguridad en los sistemas de información al servicio de la Administración de Justicia. Acuerdo del Pleno, de 13 de septiembre de 2007. [Documento en línea]. Disponible en: [www.juntadeandalucia.es](http://www.juntadeandalucia.es). (fecha de consulta: 13/03/2011)

<sup>28</sup> El Log file: registra cambios a la base de datos como resultado de transacciones o acciones internas del servidor. [http://es.wikipedia.org/wiki/Redo\\_Log\\_File](http://es.wikipedia.org/wiki/Redo_Log_File). (fecha de consulta: 15/07/2010).

dirección IP del ordenador desde el cual se está haciendo la navegación<sup>29</sup>, esto supone una importante limitación debido a que desde un mismo ordenador se pueden conectar diferentes usuarios, incluso, también hay que remarcar que un usuario no tiene porque navegar o interactuar en espacios virtuales, desde un mismo ordenador, lo puede hacer desde varios dependiendo del momento del día, por ejemplo.

Por otro lado, la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE)<sup>30</sup> señala que existe una serie de desventajas al momento de utilizar un login o password como identidad electrónica, ya que es mucho más vulnerable para ser descubierto por otras personas. Es por ello que existe el Certificado Electrónico, el cual al momento de utilizarlo asegura que la persona es quien dice ser, documento electrónico con el que no cuenta el Sistema Automatizado Juris 2000. La Dirección Ejecutiva de la Magistratura a través de la Unidad Coordinadora de Proyectos en oficio N° 057-2010 de fecha 29 enero de 2010 ha dejado establecido que: *“El Sistema de Gestión, Decisión y Documentación Juris 2000 implantado en este Circuito Judicial, no posee firmas digitales que certifiquen las actuaciones realizadas”*<sup>31</sup>.

En este sentido, la noción del certificado electrónico, como se ha visto, involucra, algunos otros elementos, además de la firma digital, que lo hacen posible para su ejecución, como el de la identidad electrónica. A este se le

---

<sup>29</sup> Martínez, Rodolfo; Mateo, Miguel y Albert, María. *El uso de técnicas de investigación en línea: desde el análisis de logs hasta la encuesta electrónica*. [Documento en línea]. Disponible en: [http://www.ua.es/personal/rmg/publicaciones/ponencia\\_Martinez\\_Mateo\\_Albert\\_Granada.pdf](http://www.ua.es/personal/rmg/publicaciones/ponencia_Martinez_Mateo_Albert_Granada.pdf). (fecha de consulta: 13/03/2011)

<sup>30</sup> Hernández, R; Berrios, Kranya y González, Víctor. *Identidad Electrónica...ob. cit.*

<sup>31</sup> Dirección Ejecutiva de la Magistratura. Unidad Coordinadora de Proyectos. Oficio N° 057-2010 de fecha 29 de enero de 2010. Caso Amparo Constitucional (Mary Luz del Carmen Betancourt vs. Decisión dictada en fecha 13 de abril de 2009, por el Juzgado Tercero de Primera Instancia en lo Civil, Mercantil, Tránsito y Bancario del Circunscripción Judicial del Área Metropolitana de Caracas)

adiciona la criptografía, cuyo principio básico es mantener la privacidad de la comunicación entre dos personas, entes gubernamentales o empresas privadas, entre otros, alterando el mensaje original de modo que sea incomprensible a toda persona distinta del destinatario; a ello se le puede atribuir de cierta forma la autenticación de quien manda el mensaje, de modo que un tercero no pueda hacerse pasar por el emisor.

De manera que la criptografía, se afianza como herramienta de seguridad de la información en las Tecnologías de Información y Comunicación (TIC), constituyéndose como elemento indispensable para garantizar la debida protección en el manejo de la información. Rico citado por Urdaneta Benítez, explica que *“la criptografía se compone de dos grandes ciencias: la criptología, encargada de estudiar los procedimientos para cifrar y descifrar la información y el criptoanálisis, que estudia la forma de esclarecer la escritura oculta”*<sup>32</sup>.

El procedimiento se realiza a través un cifrado del mensaje, para brindar un mínimo de seguridad a la información que se desea transmitir. Es importante resaltar, que el proceso de cifrar es llevado a cabo por el emisor o dueño de la información y el proceso de descifrar, en la mayoría de los casos es realizado por el receptor o destinatario.

Existen diferentes métodos criptográficos entre los cuales se destacan los siguientes:

---

<sup>32</sup> Urdaneta. B, José V. *Los Mensajes de Datos y la Firma Electrónica (Seguridad Jurídica que ofrecen y Valor Probatorio)*. Serie Tesis 5. Académica de Ciencias Sociales y Políticas de la Universidad Metropolitana. Caracas. 2010, 21.

a. *Cifrado Simétrico*: consiste en la utilización de la misma clave para cifrar y descifrar una información. Este tipo de fuentes posee como ventaja la sencillez para su aplicación, ya que se utiliza la misma clave para cifrar y descifrar la información. El principal problema de éste tipo de técnica reside en que se debe disponer de un medio seguro para el intercambio de la clave entre el emisor y el receptor.

b. *Cifrado Asimétrico*: consiste en que las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla para que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.

c. *Función Hash o Función de Control*: es un proceso matemático para verificar una firma digital, que permite reducir la longitud del texto y cifrar rápidamente la información mediante el uso de un algoritmo que crea una representación comprimida del mensaje, denominada “huella digital” y es única para cada mensaje.<sup>33</sup>

La importancia de este elemento en cuanto a la certificación electrónica, es que se requiere de la existencia de una clave pública y una privada para que la entidad certificadora asegure el vínculo entre ellas, es decir, garantice que tanto una como la otra corresponden a la persona que reclama su titularidad.

---

<sup>33</sup> Urdaneta. B, José V. *Los Mensajes de Datos y la Firma Electrónica (Seguridad Jurídica que ofrecen y Valor Probatorio)*... ob. cit, p.22

### 3.2.2 Beneficios del Certificado Electrónico.-

SUSCERTE ha desarrollado los beneficios de la Certificación Electrónica tanto para el Estado como para la ciudadanía, beneficios que serán adaptados y complementados con su aplicación al ámbito de la Administración Judicial. Así se tiene que:

#### a. Para el Estado.-

- *La simplificación de trámites administrativos:* Con el uso de los certificados electrónicos, el usuario podrá autenticarse (es decir, identificándose según quien dice ser) en los portales del gobierno y la empresa privada. De ésta manera podrá realizar las transacciones en línea de forma segura y eficiente, eliminando el flagelo de procesos largos y engorrosos de los trámites administrativos.
- *Habilitador para el Gobierno electrónico protagónico:* La masificación de los certificados electrónicos en los ciudadanos venezolanos, impulsará el desarrollo y la independencia tecnológica del país, promoviendo a su vez la política de Estado de fortalecer el Gobierno electrónico en los procesos y actividades de la Administración Pública Nacional.
- *Descentralización:* El Estado venezolano se perfila como estado pionero en la descentralización de trámites administrativos mediante el impulso regional de la implementación de certificados electrónicos para realizar transacciones electrónicas en los portales del gobierno sin necesidad de trasladarse los ciudadanos del interior hacia la capital.

Este aspecto orienta a que la administración de justicia cuente con la infraestructura técnica y la logística informática, necesaria para el recto cumplimiento de las atribuciones y responsabilidades que la Constitución le asigna. Naturalmente, el uso de los medios tecnológicos que se encuentran a disposición de sedes judiciales exige una utilización adecuada del proceso automatizado a través de un ofrecimiento pleno de confiabilidad, autenticidad y credibilidad.

- *Ahorro:* El uso de la plataforma tecnológica acarrea un ahorro evidente en uso de papel y otros insumos para el Estado Venezolano respondiendo a políticas de protección ambiental y a las iniciativas de Gobierno sin papel. De este elemento se consuma el nacimiento del expediente electrónico en las sedes judiciales. Se logra que la información que se genera en el desarrollo del proceso, tanto la emitida desde la propia oficina judicial como la aportada por las partes, sea automatizada en su totalidad

**b. Para la Ciudadanía:**

- *Autenticación:* Su uso genera esquemas de confianza entre la identidad del usuario que accede al sistema y el portal del gobierno o empresas.

La adjudicación de autenticación de los documentos electrónicos (mensaje de datos), ofrecería las medidas necesarias para que los organismos públicos, en este caso jurisdiccionales, puedan desarrollar sus funciones conforme los mecanismos de la Ley. Es decir, el Tribunal mediante el uso de los servicios electrónicos, crea una firma electrónica y ésta asociada al mensaje de datos, que en este caso sería la notificación, permitiría a la persona que recibe ese mensaje de datos atribuirle la autoría al Tribunal.

- *Disminución de tiempos de respuestas:* El usuario podrá gestionar un mayor número de trámites a través de internet. Esto en el ámbito jurisdiccional lograría celeridad en actividades como: envío de oficios, notificaciones, citaciones, entre otras cosas, por parte de los órganos jurisdiccionales. Es decir, las comunicaciones que realizan los tribunales hacia otros tribunales que se encuentran fuera de la circunscripción judicial, o hacia aquellos organismos públicos ubicados en otros estados, podrían ser agilizadas mediante el uso de la informática, específicamente de la certificación técnica de las actuaciones.

A tal efecto, en el tratamiento de la información, no se puede olvidar la posibilidad de su intercambio entre los operadores jurídicos (dentro de un órgano judicial, entre órganos judiciales, entre éstos y las administraciones públicas o también con abogados y procuradores). El intercambio telemático de información o datos entre operadores jurídicos agiliza la gestión de los procedimientos y la hace más eficiente. Sin embargo, debe hacer frente a barreras técnicas, puesto que requieren establecerse medidas de seguridad para garantizar el acceso a la información, únicamente por parte de aquellos que tengan autorización para hacerlo.

- *Acceso Gobierno - Ciudadano:* Permitirá al ciudadano común mantener esa condición de portabilidad y movilidad permanente de sus operaciones en línea con los portales del Estado en cualquier parte del país.

Este elemento es interesante desde el punto de vista de la constitución del llamado expediente electrónico, el cual será detallado en el punto 4.3.3 de este capítulo. La implementación del Certificado Electrónico en los sistemas automatizados de las sedes judiciales, sugiere la prevención de mecanismos eficaces para el examen del expediente integralmente

considerado, no sólo a través de terminales de consulta dispuestos en los sedes judiciales del país sino también la conveniencia de permitir un acceso remoto mediante mecanismos de seguridad, así como opciones para que los interesados puedan consultar sus expedientes en el despacho judicial más cercano a sus intereses.

- *Disponibilidad:* Organizar información para tenerla “a la mano”. Conocer el estado de un trámite.

- *Fortalecimiento del Desarrollo Endógeno:* Busca la implementación de estrategias autóctonas para la consolidación de las instituciones públicas y el fomento de la participación ciudadana orientada en las necesidades del colectivo en materia de certificación electrónica, seguridad de la información, automatización de trámites, entre otras.

### *3.2.3 Regulación Legal de la Certificación Electrónica en Venezuela.-*

Como cimiento del ordenamiento jurídico legal, la transmisión de mensajes de datos ha estado sometida a disposiciones de carácter constitucional desde la promulgación de la Constitución de la República Bolivariana de Venezuela del año 1999, en la que se ha visto una marcada integración del Estado con los avances tecnológicos. De su texto se puede apreciar la influencia de la tecnología en el ámbito jurídico, al consagrarse el acceso a la tecnología como un derecho fundamental de los ciudadanos, reconociéndose dentro de los derechos culturales, el carácter de interés público de la ciencia, la tecnología, el conocimiento y la innovación, tal como lo establece el artículo 110. En el artículo 108, La Constitución impone al Estado la obligación de garantizar los servicios de radio, televisión, redes de

biblioteca y de informática, con el fin de permitir el acceso universal a la información, estableciendo como deber de los centros educativos, la necesidad de incorporar el conocimiento y la aplicación de las Nuevas Tecnologías en los procesos de enseñanza.

El reconocimiento constitucional de los avances tecnológicos, como de interés público, ha motivado en el ámbito legislativo, el desarrollo de un conjunto Leyes, conducentes a proporcionar las normas legales, que deben ser consideradas en materia de tecnologías de información, democratización del conocimiento y apropiación social de estas tecnologías. De estos esfuerzos legales, surge el Decreto con Fuerza de Ley N° 1.204 de fecha 10 de febrero de 2001 de Mensajes de Datos y Firmas Electrónicas y el Reglamento Parcial del Decreto Ley Sobre Mensaje de Datos y Firmas Electrónicas N° 3.335 de fecha 14 de diciembre de 2004.

De cada una de estos instrumentos normativos, será analizada las previsiones legales propuestas para el tema de la certificación electrónica.

*1. Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas.-*

Los redactores de esta Ley, se basaron en legislaciones internacionales, como la Ley Modelo de Comercio Electrónico de Uncitral (United Nations Commission on International Trade Law). También se usaron como referencia la Ley de Firmas Digitales promulgada en el estado de Utah, EE.UU., así como disposiciones regulatorias promulgadas por la Unión

Europea y la legislación sobre Comercio Electrónico y Firmas Digitales de España, Francia y Singapur<sup>34</sup>.

El objeto principal de este Decreto-Ley, es adoptar un marco normativo que avale los desarrollos tecnológicos sobre seguridad, en materia de comunicación y negocios electrónicos, para dar pleno valor jurídico a los mensajes de datos que hagan uso de estas tecnologías. A tales efectos, otorga y reconoce eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico (video, música, fotografía, entre otros), independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular lo relativo a los Proveedores de Servicios de Certificación Electrónica y los Certificados Electrónicos.

En cuanto al tratamiento legal de la Certificación Electrónica, los comentarios que a continuación se exponen, han sido recogidos de Rondón García<sup>35</sup>, en su estudio sobre el Decreto-Ley de Mensaje de Datos y Firmas Electrónicas de la República Bolivariana de Venezuela, en el punto de la regulación sobre los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El Decreto-Ley al definir en su artículo 2 al proveedor de certificación como *“la persona dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en este Decreto-Ley”*, deja un vacío jurídico al no especificar, el tipo de persona de que se trata, por lo que está abierta la

---

<sup>34</sup> VENECONOMIA. Llegan las Firmas Electrónicas. Veneconomía Hemeroteca. [Documento en línea]. Disponible en: [www.veneconomia.com](http://www.veneconomia.com). (fecha de consulta: 03/07/2010).

<sup>35</sup> Rondón G, Andrea I. *Comentarios generales al Decreto-Ley de Mensaje de Datos y Firmas Electrónicas de la República Bolivariana de Venezuela*. [Documento en línea]. Disponible en: [http://www.ulpiano.org.ve/revistas/bases/artic/texto/RDUCV/123/rucv\\_2002\\_123\\_151-182.pdf](http://www.ulpiano.org.ve/revistas/bases/artic/texto/RDUCV/123/rucv_2002_123_151-182.pdf). (fecha de consulta: 03/05/2011).

posibilidad de que el proveedor de servicios pueda ser tanto una persona física como jurídica. Es así que, ni esta norma, ni la dispuesta en la tercera disposición final, la cual establece que *“sin limitación de otros que se constituyan, el Estado creará un Proveedor de servicios de Certificación de carácter público”*, se contempla si el proveedor debe ser privado o público.

En referencia al tema de la acreditación, el artículo 48 dispone que serán sancionadas *“las personas que presten los servicios de Proveedores de Servicios de Certificación previstos en este Decreto-Ley, sin la acreditación de la Superintendencia de Servicios de Certificación Electrónica, alegando tenerla”*. En este caso, la técnica legislativa utilizada, no especifica si la acreditación debe ser obligatoria o no para el proveedor de servicios, ya que únicamente sanciona a quienes aleguen tener la acreditación cuando no es cierto, por lo que parecería que la misma no es de obligatorio cumplimiento.

Sin embargo, la Exposición de Motivos del Decreto-Ley, orienta en este sentido, al señalar que estos Proveedores de Servicios de Certificación una vez acreditados, tendrán entre sus funciones, emitir un documento contentivo de información cerciorada, que vincule a una persona natural o jurídica y confirme su identidad, con la finalidad que el receptor pueda asociar inequívocamente la firma electrónica del mensaje emisor. A este respecto, las intenciones del legislador no deberían observarse de la exposición de motivos sino de la propia letra de la norma, de una manera clara e inequívoca, a los fines de establecer un sistema de acreditación obligatoria.

No obstante, el tema de la acreditación no se agota con la regulación establecida en el Decreto-Ley, sino que SUSCERTE se ha encargado de contemplar un proceso de acreditación en su norma N° 27-08/08, disponible

en su sitio web [www.SUSCERTE.gob.ve](http://www.SUSCERTE.gob.ve). Dicha norma tiene por objeto y campo de aplicación, la descripción de todos los recaudos que deben presentarse por parte de los solicitantes a Proveedores de Servicios de Certificación, así como el recorrido del proceso de acreditación con respecto a dicha solicitud. Es importante mencionar que los recaudos exigidos por SUSCERTE para la acreditación de los Proveedores de Servicios de Certificación son de tipo técnico, económico-financiero, legal y de auditoría, los cuales deben cumplirse a cabalidad para lograr la aprobación de la solicitud de acreditación.

Por otro lado, los interesados en convertirse en Proveedores de Servicios de Certificación acreditados, la Norma SUSCERTE N° 40 *“Guía de estándares tecnológicos y lineamientos de seguridad para la Acreditación como Proveedor de Servicios de Certificación”*, contiene la descripción y aspectos a evaluar de todos los recaudos técnicos exigidos para la acreditación e incluso presenta una serie de anexos donde se especifica la documentación solicitada y se ejemplifica a estructura de muchos de los recaudos exigidos.

Ahora bien, continuando con los comentarios del Decreto-Ley, el artículo 2, ha definido el certificado electrónico como *“Mensaje de Datos otorgado por el Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica”*. Es decir, entre sus funciones esta vincular la firma electrónica con una persona determinada. Función ésta, que además de ser confirmada por el contenido del artículo 38, adiciona el elemento referente a la integridad del mensaje de datos, cuando afirma que el *“Certificado Electrónico garantiza la autoría de la Firma Electrónica que certifica, así como la integridad del Mensaje de Datos”*, lo cual proporciona certeza de que el mensaje no ha sufrido alteración alguna.

Otra de las funciones otorgadas a los proveedores de servicios ha sido la de garantizar que los certificados electrónicos extranjeros cumplan con los requisitos de seguridad, validez y vigencia exigidos por el Decreto-Ley. Este certificado extranjero garantizado por un proveedor de servicios, debidamente acreditado, le proporcionará a la firma electrónica la misma validez y eficacia probatoria que se le otorga a la firma autógrafa. No obstante, si este certificado extranjero no está garantizado por un proveedor de servicios, no le brindará estos mismos efectos a la firma electrónica, sino que la misma constituirá un elemento de convicción valorable según las reglas de la sana crítica.

En cuanto al contenido de los certificados, la ley ha previsto en su artículo 43 que estos deben prever:

*a) Identificación del Proveedor de Servicios de Certificación que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica.* Como ya se refirió, el legislador dejó abierta la posibilidad de que el proveedor de servicios fuese una persona física o jurídica. De tratarse de una persona jurídica, deberá adicionar la razón social y datos de registro.

*b) El Código de Identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica.* Para cumplir con este requisito se ha contemplado en artículo 22, numeral 3, que una de las competencias de la Superintendencia sea la de “mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores de Servicios de Certificación públicos o privados”.

*c) Identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica.* Al respecto, el Decreto-Ley define al

signatario en el artículo 2, como “la persona titular de una Firma Electrónica o Certificado Electrónico”. Tal y como ocurre con los proveedores de servicios de certificación, el legislador deja abierta la posibilidad de que el signatario sea una persona física o jurídica.

*d) Las fechas de inicio y vencimiento del período de vigencia del Certificado Electrónico.* En este caso, el proveedor y el signatario deberán acordar el periodo durante el cual el certificado tendrá vigencia. No obstante, la vigencia que puedan acordar el proveedor y signatario, este último podrá solicitar la cancelación o suspensión temporal del certificado.

Adicionalmente, según el artículo 42 del Decreto-Ley, se podrá suspender o revocar el certificado, cuando sea solicitado por una autoridad competente, se compruebe que los datos del certificado o alguno de ellos son falsos, se compruebe el incumplimiento de alguna de las obligaciones derivadas del contrato celebrado entre el proveedor de servicios y el signatario, se produzca la quiebra técnica del sistema de seguridad del proveedor de servicios que afecte la integridad y confiabilidad del certificado o por incapacidad absoluta del signatario.

*e) La firma electrónica del signatario.* El signatario puede ser como ya se señaló anteriormente, una persona natural o jurídica. Cuando se trate de una persona Jurídica, la firma será de un persona física con poder de representación, circunstancia que puede hacerse constar en el mismo documento que se firma.

*f) Un serial único de identificación del Certificado Electrónico.* Este serial único le facilita a los proveedores de servicios el cumplimiento conforme al

artículo 35 numeral 9 del Decreto-Ley de la obligación de “efectuar las notificaciones y publicaciones necesarias para informar a los signatarios y personas interesadas acerca del vencimiento, revocación, suspensión o cancelación de los certificados electrónicos que proporcione, así como cualquier otro aspecto de relevancia para el público en general, en relación con dichos certificados electrónicos”.

*g) Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico.* El legislador ha previsto la posibilidad de que los prestadores de servicios puedan limitar su responsabilidad, es decir, no se hará responsable por los certificados que han sido utilizados de forma distinta a la prevista en el certificado y dicho límite debe estar claramente formulado.

En referencia a este punto de la responsabilidad de los proveedores de servicios, el legislador al explicar los principios que se adoptan en el Decreto-Ley, amplía, que se excluirá la responsabilidad siempre que el sujeto pueda demostrar que ha tomado las diligencias necesarias según las circunstancias. Los Proveedores de Servicios de Certificación Electrónica pueden limitar su responsabilidad, incluyendo en los certificados que emitan las restricciones, condiciones y límites establecidos para su utilización.

Ahora bien, en el desarrollo de las diferentes normas que regulan el servicio de los Proveedores de Certificación Electrónica, se ha observado que ha sido la Exposición de Motivos el instrumento que llena los espacios vacíos dejados por el legislador en la redacción de muchas de las normas de este Decreto-Ley. Pero a juicio de la Sala Constitucional respecto a la naturaleza jurídica que tiene la Exposición de Motivos, ha referido que:

*“...Se consulta sólo a título referencial e ilustrativo para el análisis de la norma constitucional, pues la misma constituye un documento independiente al Texto Constitucional propiamente dicho y, no siendo parte integrante de la Constitución, no posee carácter normativo... No puede entonces fundamentarse en la Exposición de Motivos la justificación jurídica para interpretar una modificación, ampliación o corrección de lo expresado en el Texto Fundamental. No puede igualmente otorgarse un carácter interpretativo de la Constitución a la Exposición de Motivos cuando la misma Constitución le otorga dicho carácter expresamente a esta Sala. La Exposición de Motivos constituye simplemente una expresión de la intención subjetiva del Constituyente, y tiene el único fin de complementar al lector de la norma constitucional en la comprensión de la misma.”<sup>36</sup>*

En este sentido, lo referente al tema de la responsabilidad de los proveedores de servicios, debe ser complementado con las disposiciones del Código Civil y de la Ley de Protección al Consumidor.

Finalmente, en atención a los daños y perjuicios que pueda ocasionar el cese de actividades por parte del proveedor de servicios, el legislador le ha impuesto a éste un conjunto de obligaciones. Entre ellas, el proveedor deberá notificar a la Superintendencia con al menos treinta (30) días de anticipación de su decisión y, en caso de inhabilitación técnica, la notificación deberá ser inmediata.

Una vez cumplido el requisito de las notificaciones, la Superintendencia a través de un acto administrativo declarará públicamente la cesación de actividades del proveedor. La Superintendencia, en virtud de las atribuciones que ejerce, como las de supervisar las actividades de los proveedores,

---

<sup>36</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia Nº 93 de fecha 06 de febrero de 2001. (Caso: Acción de Amparo. Corpoturismo). Disponible en: <http://www.tsj.gov.ve/decisiones/consulta>. (fecha de consulta:08/09/2012)

inspeccionar y fiscalizar las instalaciones, operaciones y prestación de servicio de los proveedores, pudiendo solicitarle a éstos últimos cualquier información que considere necesaria, está facultada para investigar los motivos que dieron lugar a la cesación de actividades y adoptar las medidas necesarias que tienda a proteger a los usuarios.

## *2. Reglamento Parcial del Decreto Ley Sobre Mensaje de Datos y Firmas Electrónicas.-*

Este Reglamento dedica su contenido a regular fundamentalmente el procedimiento de acreditación de los Proveedores de servicios, detallando para ello una serie de requisitos técnicos, legales y financieros. Su objeto de regulación esta resumido en los siguientes puntos:

a. Las obligaciones de los Proveedores de Servicios de Certificación Electrónica, acreditados.

b. Las formalidades que deberá cumplir el Proveedor de Servicio de Certificación Electrónica en caso de suspensión del servicio, ya sea por motivo de mantenimiento y mejoras en sus sistemas, o bien sea por caso fortuito o fuerza mayor.

c. Reconoce a su vez la validez de los certificados electrónicos extranjeros, siempre y cuando sean garantizados por un Proveedor de Servicio de Certificación debidamente acreditado por SUSCERTE.

d. Establecer las inspecciones ordinarias y extraordinarias como mecanismo de control y supervisión de los Proveedores de Servicios de Certificación Electrónica acreditados por SUSCERTE.

e. Ordena la creación del Registro de Auditores y dispone el procedimiento de inscripción.

g. Finalmente establece estándares, planes procedimientos de seguridad y requisitos técnicos que deberán llevar a cabo los Proveedores de Servicios de Certificación Electrónica.

Finalmente, hay que hacer referencia a la regulación de lo que se ha denominado Infraestructura Nacional de Certificación Electrónica, prevista en la Norma SUSCERTE N° 032-01/11.

La Infraestructura Nacional de Certificación Electrónica es el conjunto de servidores, programas (software), dispositivos criptográficos, políticas, normas y procedimientos, dispuestos y utilizados de manera exclusiva por la Autoridad de Certificación Raíz y los PSC acreditados para la generación, almacenamiento y publicación de los certificados electrónicos, así como también, para la publicación de información y consulta del estado de vigencia y validez de dichos certificados. Esta Infraestructura se basa en dos pilares fundamentales, tales como la confianza y la tecnología<sup>37</sup>.

La Infraestructura Nacional de Certificación Electrónica, fue concebida según Providencia emitida el 2 de marzo de 2007; en la cual se establecen las Normas Técnicas bajo las cuales SUSCERTE, coordinará e implementará el modelo jerárquico de dicha infraestructura, para que los Proveedores de Servicios de Certificación acreditados (PSC) emitan los certificados electrónicos en el Marco del Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas y su Reglamento. Al respecto, los elementos de la Infraestructura Nacional de Certificación Electrónica, están previstos de la siguiente forma:

---

<sup>37</sup> Hernández, R; Berríos, Kranya y González, Víctor. *Identidad Electrónica*. ..op. cit.

1. La Autoridad de Certificación Raíz del Estado Venezolano, operada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), ente rector que dicta las normas y estándares de uso, acreditación, supervisión y control de los Proveedores de Servicios de Certificados.

2. El PSC es la entidad encargada de emitir los Certificados Electrónicos a los usuarios.

3. El Certificado Electrónico, documento electrónico emitido por un PSC que vincula a un signatario con su clave pública.

4. La Firma Electrónica, es un conjunto de datos que vincula de manera única el documento al signatario y garantiza la integridad del documento electrónico. Es importante resaltar dos aspectos vinculantes: La integridad, que su contenido no ha variado desde el momento en que se firmó y la autoría, quien firmó el documento.

5. El documento electrónico, representación de actos o hechos en formato electrónico.

### **3.3 Elementos de un Proceso Electrónico.-**

Ricardo Madrigal<sup>38</sup> ha señalado que dentro del proceso electrónico judicial se ubican al menos cuatro componentes, a saber: la firma digital, el documento electrónico, el expediente electrónico y lo atinente a las

---

<sup>38</sup> Madrigal J, Ricardo. *El Procedimiento Judicial Electrónico*. Revista de Derecho y Tecnología de la Información N° 3-2005. UNED. Costa Rica. [Documento en línea]. Disponible en: <http://www.uned.ac.cr/redti/tercera/documentos/>. (fecha de consulta: 21/11/2011)

notificaciones. En el desarrollo de cada uno de estos elementos lo relevante esta en contrastar el tratamiento implementado en Venezuela.

### 3.3.1 La Firma Digital.-

La Ley de Mensaje de Datos y Firmas Electrónicas ofrece en el artículo 2 una definición de la firma electrónica al señalar que:

*“A los efectos del presente Decreto-Ley, se entenderá por:*

*...Firma Electrónica: información creada o usada por el signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado...”*

El artículo 3º de la Ley de Firmas y Certificados Digitales de Perú (Ley No. 27269) publicada en el Diario Oficial El Peruano el día 28 de mayo de 2000, citada por Peñaranda, establece que:

*“La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada”<sup>39</sup>.*

De las definiciones aportadas, existe un elemento que las hace diferentes y es el calificativo que cada una le otorga a la firma, electrónica y digital. Al respecto, Ricardo Lorenzetti ha advertido que la firma electrónica es el género y la firma digital la especie, pues, en ésta última, se agregan elementos de seguridad que la firma electrónica no posee. Este autor también ha señalado que *“las legislaciones reconocen el género de firma*

---

<sup>39</sup> Peñaranda Q, Héctor R. La Firma Electrónica Digital en Venezuela. *Nómadas*. Revista Crítica de Ciencias Sociales y Jurídicas | 29 (2011.1). Universidad del Zulia. Venezuela. 2011. [Documento en línea]. Disponible en: <http://www.ucm.es/info/nomadas/29/hectorpenaranda.pdf>. (fecha de consulta: 01/03/2012)

*electrónica y luego eligen una especie dentro de él, que denominan firma electrónica avanzada, o firma electrónica digital que es la que utiliza un sistema, generalmente criptográfico<sup>40</sup>, que da seguridad<sup>41</sup>*

Esta distinción ha sido recogida por la Directiva 1999/93/Ce del Parlamento Europeo y del Consejo, que establece un marco comunitario para la firma electrónica, y que en su artículo 2, define por firma electrónica “*los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación;*”. Pero además, señala que:

*“La firma electrónica avanzada es la firma electrónica que cumple los requisitos siguientes:*

- a) estar vinculada al firmante de manera única;*
- b) permitir la identificación del firmante;*
- c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control;*
- d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable<sup>42</sup>*

Sin embargo, para Peñaranda ésta precisión terminológica que señala lo electrónico como el género y lo digital como la especie, resulta errónea, ya que se tratan de conceptos que se contraponen dependiendo del método tecnológico en que se base. Así, este autor señala lo siguiente:

*“...Lo digital es la forma en que se representa la información...Mientras que lo electrónico se refiere a*

---

<sup>40</sup> La palabra criptografía proviene en un sentido etimológico del griego *Kriptos=ocultar*, *Grapho s=escritura*, lo que significaría ocultar la escritura, o en un sentido más amplio sería aplicar alguna técnica para hacer ininteligible un mensaje. Granados P, Gibran. Introducción a la Criptografía. Revista Digital Universitaria...op.cit

<sup>41</sup> Lorenzetti, Ricardo. Comercio Electrónico. Abeledo Perrot. Argentina. 2000, p. 78

<sup>42</sup> Diario Oficial de las Comunidades Europeas. Directiva 1999/93/Ce del Parlamento Europeo y del Consejo por la que se establece el marco comunitario para la firma electrónica de fecha 13 de diciembre de 1999. [Documento en línea]. Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:ES:PDF>. (fecha de consulta: 01/09/2012)

*una tecnología específica, que se utiliza en informática, mas no es la única, porque participa junto a otras como la mecánica, eléctrica, magnética, óptica e inclusive otras menos conocidas como las memorias moleculares...la expresión digital no se limita con ninguna tecnología específica, sino que es la manera convencional que se ha adoptado para tratar la información, independientemente de la tecnología de turno...*<sup>43</sup>

Considerando este último planteamiento, la Ley de Mensaje y Firmas Electrónicas vigente, revela una contrariedad entre la calificación que le otorga a la firma “electrónica” y la progresividad normativa que plantea el artículo 1, al señalar que el Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. Sin embargo, hay quienes prefieren mantenerse con el planteamiento de la generalidad que representa la calificación firma electrónica y argumentan que bajo esta ley no se adopta como única modalidad la firma digital, pues, se establecen definiciones generales que no solo hacen admisible el sistema de la firma digital, dejando libertad para emplear otros.

No obstante, a pesar de los distintos debates que se generen en torno a la calificación de la firma (digital o electrónica), lo relevante es reconocer, que la Ley de Mensajes de Datos y Firmas Electrónicas en su artículo 16 ha previsto requisitos de validez y eficacia muy similares a los que le otorgan legislaciones extranjeras a la firma digital o firma electrónica avanzada:

*“Artículo 16. La Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y atribuir la*

---

<sup>43</sup> Peñaranda Q, Héctor R. La Firma Electrónica Digital en Venezuela. *Nómadas*. Revista Crítica de Ciencias Sociales y Jurídicas | 29 (2011.1). Universidad del Zulia. Venezuela. 2011. [Documento en línea]. Disponible en: <http://www.ucm.es/info/nomadas/29/hectorpenaranda.pdf>. (fecha de consulta: 01/03/2012)

*autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la Firma Electrónica deberá llenar los siguientes aspectos:*

- 1. Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.*
- 2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.*
- 3. No alterar la integridad del Mensaje de Datos”.*

De la norma citada y de los planteamientos referidos, se puede concretar que aun cuando el Decreto-Ley haga referencia a la firma como electrónica, esta debe revestir un conjunto de formalidades que confieran seguridad jurídica, en tanto garantice la autoría, mantenga la confidencialidad del mensaje, posibilite el control de acceso limitado, mantenga la integridad de la información y asegure la validez probatoria y los plenos efectos de la firma escrita.

La seguridad que ofrece la firma digital está basado en un sistema de criptografía asimétrico, es decir, la persona que emite el mensaje tiene dos claves, una publica la cual debe ser accesible para todos, y una privada, la cual solo es conocida por el titular o incluso ni siquiera conocida por este y puede acceder a ella a través de un número de identificación personal o, en el mejor de los casos, con el reconocimiento de una huella digital, con esta ultima clave el emisor cifra su mensaje digitalmente y con la clave publica el receptor lo descifra.

En virtud de este procedimiento, la firma digital ofrece al receptor:

- a) Autenticidad:* vincula de forma única el documento a su autor.

b) *Integridad*: La utilización de la tecnología de la firma digital con la criptografía asimétrica asegura que la información no ha sido modificada, de manera que el mensaje se puede obtener completo, lo cual constituye un requisito sine qua non para otorgarle plena validez jurídica al documento y firma. La firma digital detecta la integridad del mensaje firmado, independientemente del medio de su almacenamiento.

c) *No repudio*: garantiza que el emisor no pueda negar o repudiar su autoría o existencia, ser susceptible de verificación ante terceros.

d) *Imposibilidad de Suplantación*: la firma electrónica, debidamente otorgada por los proveedores de certificación electrónica al emisor o usuario final, a través de una tarjeta criptográfica o de un dispositivo electrónico de almacenamiento que contenga la información y clave privada respectiva, la cual además es guardada y utilizada por el signatario bajo su propio y exclusivo control, asegura la imposibilidad de suplantación por parte de otro individuo.

e) *Auditabilidad*: este aspecto de seguridad de la firma electrónica, según señala Abad citado por Urdaneta Benítez, “*permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático, cuyo acceso se realiza mediante la presentación de un certificado electrónico*”<sup>44</sup>, en el cual queda registrado, de manera totalmente fiable la fecha y la hora de las acciones realizadas, a través del estampillado de tiempo.

---

<sup>44</sup> Urdaneta. B, José V. (2010). *Los Mensajes de Datos y la Firma Electrónica (Seguridad Jurídica que ofrecen y Valor Probatorio)*...ob. cit, p. 12.

Ahora bien, la firma electrónica esta fielmente ligada a un componente de seguridad tecnológica, como el de la entidad certificadora, es decir, un intermediario que asegure el vinculo que existe entre la clave pública y el titular de la clave privada, un ente que garantice que las claves corresponden a esa persona. Esta persona encargada de proveer servicios de certificación podrá ser una persona física o jurídica y de naturaleza privada o pública. En consecuencia, la firma digital generará responsabilidad legal a partir de la fe de las autoridades certificadoras, pues de lo contrario no tendría lógica jurídica alguna.

### 3.3.2 El Documento Electrónico.-

Soto Caldera define el documento Electrónico como *“toda aquella representación del pensamiento y de la voluntad del hombre materializado en soportes magnéticos de acceso inmediato, capaz de trasladarse de un lugar a otro por medio de redes telemáticas”*<sup>45</sup>

Para Peñaranda el documento electrónico es:

*“Aquel instrumento que contiene escrito un mensaje, destinado a durar en el tiempo, en lenguaje convencional (bits), sobre soporte, que podría ser cinta o disco. En otras palabras, es el documento proveniente de cualquier medio de informática o que haya sido formado o realizado por éste”*<sup>46</sup>

La Sala de Casación Civil del Tribunal Supremo de Justicia ha expuesto que *“...el documento electrónico o mensaje de datos es un medio de prueba*

---

<sup>45</sup> Soto C, Milagros M. *“Consideraciones sobre la prueba documental electrónica en el proceso civil venezolano”*. Estudios de Derecho Civil. Vol III. Libro homenaje a José Luis Aguilar Gorrondona. Tribunal Supremo de Justicia. Colección Libros homenaje No. 5. Caracas. 2001, p. 658.

<sup>46</sup> Peñaranda. Q, Héctor. *Iuscibemetica: Interrelación entre el Derecho y la Informática*. Fondo Editorial para el Desarrollo de la Educación Superior (FIDES). Maracaibo. 2001, p. 121.

*atípico, cuyo soporte original está contenido en la base de datos de un PC o en el servidor de la empresa y es sobre esto que debe recaer la prueba...”<sup>47</sup>*

Por su parte, La Ley de Mensaje de Datos y Firmas Electrónicas, en su artículo 2 señala que:

*“A los efectos del presente Decreto-Ley, se entenderá por:  
Mensajes de Datos: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio”.*

Una de las características más resaltantes de esta normativa y del criterio del Tribunal Supremo de Justicia, es que se equiparan los términos, mensaje de datos y documento electrónico, aunque, hay quienes han advertido que la equiparación de los términos es errónea. Así, el abogado Odreman Ordozgoitty ha referido que:

*“A manera de determinar una correcta definición del Mensaje de Datos y de hacer la necesaria diferenciación con el Documento Electrónico, podemos afirmar: que el mensaje de datos es toda información generada o recibida por medios electrónicos, pero para que este mensaje de datos se convierta y sea tratado como documento electrónico con consecuencias jurídicas, es necesario que el mismo contenga derechos y obligaciones exigibles entre las partes intervinientes en la relación electrónica, por lo que todo documento es y será un mensaje de datos, pero no todo mensaje de datos podrá ser considerado como documento electrónico...”<sup>48</sup>*

---

<sup>47</sup> Tribunal Supremo de Justicia. Sala de Casación Civil. Sentencia N° 769 en fecha 24 de octubre de 2007. (Caso: Distribuidora Industrial de Materiales, C.A., contra Rockwell Automation de Venezuela, C.A.). Documento disponible en: <http://www.tsj.gov.ve/decisiones/>. (fecha de consulta: 13/04/2011)

<sup>48</sup> Odreman O, Gregory. Eficacia Probatoria del Mensaje de Datos y de la Firma Electrónica según la nueva Ley de Mensaje de Datos y Firmas Electrónicas. Universidad Católica Andrés Bello. Caracas 2003, pp.11-12

En este sentido el autor refiere al Documento Electrónico como especie del Mensaje de Datos y no admite una equivalencia de ambos términos.

Sobre este particular y bajo un enfoque de lo que es un Documento Electrónico, es necesario advertir que estos tienen la misma garantía legal que los documentos en papel, tal como lo establece la Ley Sobre Mensajes de Datos y Firma Electrónica en su Artículo 4:

*“Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este decreto ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil. La información contenida en un Mensaje de Datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas”.*

Es decir, para la valoración del documento se deben observar, las siguientes distinciones:

1. El documento electrónico que esté asociado a una firma electrónica debidamente certificada por un Proveedor de Servicios de Certificación conforme a lo establecido en la Ley sobre Mensajes de Datos y Firmas Electrónicas (2001), tendrá la misma validez y eficacia probatoria que la Ley otorgue al documento que contiene una firma autógrafa, es decir, hace plena prueba entre las partes.

2. El documento electrónico al cual esté asociado una firma electrónica, validada por un certificado electrónico de firma, emitida por un Proveedor de Servicios de Certificación no acreditado ante la Superintendencia de Servicios de Certificación Electrónica o al cual esté asociado simplemente

una firma electrónica no certificada, constituirá un elemento de convicción valorable conforme a la regla de la sana crítica.

3. El documento electrónico no asociado a una firma electrónica, solo tendrá el valor de un indicio, por lo que debe ser acompañado de otros medios de prueba que sustenten los hechos contenidos en el mensaje de datos.

En argumento a esta última consideración, se cita el criterio de la Sala Constitucional del Tribunal Supremo de Justicia en sentencia N° 721, respecto a los ejemplares de sentencias extraídos del Juris 2000:

*“Se aparta del criterio sostenido respecto a la validez de los datos extraídos del Sistema Juris 2000, y a partir del presente fallo establece con carácter vinculante que las decisiones judiciales obtenidas a través del aludido sistema -actual sistema informático del Poder Judicial- serán consideradas copias simples conforme al artículo 429 del Código de Procedimiento Civil, a los efectos de la interposición de acciones de amparos constitucionales contra sentencias, caso en el cual, tal como se estableció en la sentencia N° 7/2000, la parte accionante tendrá la carga de presentar hasta la oportunidad de la audiencia oral, la copia certificada de la decisión impugnada. Si ello no ocurriera la Sala declarará inadmisibles el amparo interpuesto en el acto de celebración de la audiencia oral. Asimismo, se declarará inadmisibles la acción antes o en la audiencia oral si se constata, de oficio o a instancia de parte, que el ejemplar de la sentencia accionada en amparo extraído del Sistema Juris 2000 no es conforme con la copia certificada de la sentencia o su original que reposa en el expediente”.*<sup>49</sup>

---

<sup>49</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 721 de fecha 09 de julio de 2010 (Saco: Acción de Amparo. Parte accionante: Grecia Figueroa). Documento disponible en: <http://www.tsj.gov.ve/decisiones/>. (fecha de consulta: 13/04/2011)

Aunque los registros electrónicos (mensaje de datos) del Sistema Juris 2000 no tengan asociado una firma electrónica, pudiera concretarse que en este caso, la Sala ha considerado que el documento privado puede prescindir de la firma, en la medida en la cual, por otros medios se pueda cumplir con las finalidades perseguidas con su utilización, es decir, la determinación de la autoría y autenticidad de la declaración. Tratándose de un Mensaje de Datos el sentenciador vio satisfechos los parámetros del artículo 429 del Código de Procedimiento Civil venezolano a través de lo regulado en la Ley de Mensaje de Datos y Firmas Electrónicas sobre la constancia por escrito del documento electrónico. Esto es que, la información que éste contiene sea accesible para su ulterior consulta, permitiendo que los órganos jurisdiccionales tengan la oportunidad de constatar, de oficio o a instancia de parte, la veracidad del documento consignado, a los efectos de la admisión, y ver cumplido el requerimiento de cotejo a que alude el artículo mencionado. No obstante, la parte accionante tendrá la carga de presentar hasta la oportunidad de la audiencia oral, la copia certificada de la decisión impugnada, ya que la misma es un indicio que debe ser acompañado de otros medios de prueba que sustenten los hechos contenidos en el mensaje de dato.

Con motivo de ahondar, en la naturaleza jurídica del documento electrónico es necesario advertir, que la misma surgirá por analogía de la distinción prevista en el Código Civil venezolano, respecto de los documentos públicos y los documentos privados, distinguiéndose los unos de los otros, en la intervención del funcionario público en su formación. Y a los fines de asentar las características de cada uno de ellos, se refieren los artículos del Código Civil vigente, que definen estas dos especies documentales:

*Artículo 1.357: "Instrumento público o autentico es el que ha sido autorizado con las solemnidades legales*

*por un Registrador, por un Juez u otro funcionario o empleado público que tenga facultad para darle fe pública, en el lugar donde el instrumento se haya autorizado”.*

*Artículo 1.363: “El instrumento privado reconocido o tenido legalmente por reconocido, tiene entre las partes y respecto de terceros, la misma fuerza probatoria que el instrumento publico en lo que se refiere al hecho material de las declaraciones; hace fe, hasta prueba en contrario, de la verdad de esas declaraciones”.*

Detallando los elementos y características que rodean ambas regulaciones es indudable asimilar al documento electrónico como ya lo ha referido la Jurisprudencia, con el documento privado simple, cuando no se hacen presentes los requisitos de autenticidad, fecha cierta y buena fe que le otorga el funcionario público ampliamente facultado por la ley. Sin embargo, cuando la eficacia y valor jurídico de la firma electrónica es incorporada al desempeño de los Notarios, Registradores y/o Jueces y se suma el servicio de las autoridades de certificación electrónica, se está en presencia de un verdadero documento público. Un ejemplo de ello, lo constituye el Decreto con Fuerza de Ley de Registro Público y del Notariado, de fecha 13 de noviembre del año 2001, el cual dispuso en su artículo 5, que *“La firma electrónica de los Registradores y Notarios tendrá la misma validez y eficacia probatoria que la ley otorga a la Firma autógrafa”* y que bajo la vigencia de su reforma del año 2006 mantiene en su artículo 24 que *“La firma electrónica de los Registradores y Notarios tendrá la misma validez y eficacia probatoria que la ley otorga”*.

De estas últimas consideraciones, resulta importante señalar, que los certificados electrónicos cuya finalidad es acreditar y certificar la autoría e integridad del mensaje electrónico, no se bastan por sí solos para dar

autenticidad legal a un documento y revestirlo con carácter público, a no ser que se cumplan con los extremos de ley, referentes a la fe pública de los funcionarios facultados.

### 3.3.3 *El expediente judicial electrónico.-*

Indiferentemente del tipo de procedimiento al que se refiera, es posible asegurar según Hess, que *“un expediente es siempre una colección, secuencialmente ordenada, de las actuaciones de los intervinientes en el proceso”*<sup>50</sup>.

El expediente avanza en razón del proceso que refleja y las piezas constituyen exposición del estado de este, así como de los elementos de prueba que se considerarán para la determinación final. Cumple la importante labor de permitir fundamentar el proceso mental que conduce al juzgador a la decisión y al mismo tiempo es un elemento de control sobre la correcta adopción de la decisión. Lo difícil ha sido asumir que el documento cuyo soporte ha sido el papel por más de cinco siglos, sea sustituido por la modalidad de registros tecnológicos. De allí, que la administración judicial con la praxis de las nuevas Tecnologías de información y Comunicaciones ha dado un espacio al llamado expediente judicial para el resguardo de todas las tramitaciones que surgen en el paso de un proceso jurisdiccional.

---

<sup>50</sup> Hess A. Cristian. Hacia el Procedimiento Electrónico, Administrativo y Judicial. Ponencia al VII Congreso Iberoamericano de Derecho e Informática. [Documento en línea]. Disponible en: <http://www.hess-cr.com/secciones/dere-info/proced.html>. (fecha de consulta: 01/02/2010).

El expediente judicial electrónico es un *conjunto de documentos electrónicos correspondientes a un procedimiento judicial, cualquiera que sea el tipo de información que contenga*.<sup>51</sup>

Por otra parte, el Expediente Judicial Electrónico, en el ámbito de la Administración de Justicia, se define como el conjunto de información que se genera durante la tramitación de un expediente judicial, tanto la emitida desde la propia oficina judicial como la aportada por las partes durante el desarrollo del proceso o la que se deriva de los informes o aportaciones de peritos y profesionales<sup>52</sup>.

Hess también afirma que son varias las ventajas del expediente a través del medio electrónico, las cuales conviene evidenciar:

- a. Presenta menor efecto de deterioro por el transcurso del tiempo.
- b. Su transferencia electrónica evita el extravío, así como la pérdida de tiempo y de dinero.
- c. Requieren menos espacio físico, lo que disminuye el costo y los riesgos por este concepto.
- d. Se reduce o elimina el tiempo de recuperación de un determinado documento o expediente almacenado.
- e. La duplicación del expediente se torna más cómoda y menos costosa.
- f. Se elimina el costo social y económico que tiene la utilización del papel, debido a su impacto sobre la conservación de los recursos naturales.

---

<sup>51</sup> Informes de Modernización Judicial en España. Expediente Electrónico Judicial. Ministerio de Justicia. [Documento en línea]. Disponible en: <http://www.oficinajudicial.justicia.es>. (fecha de consulta: 21/03/2012).

<sup>52</sup> Ibermatica. Expediente Judicial Electrónico. La Justicia se Moderniza. [Documento en línea]. Disponible en: <http://www.ibermatica.com>. (fecha de consulta: 19/04/2011).

El empleo del expediente electrónico como un modelo del expediente tradicional exige adaptar sus diversas cualidades al medio tecnológico. Por ejemplo, el citado autor sostiene, que debería variarse el término de folios por el de "asientos" o "registros", pues dentro del último concepto no existen folios en el sentido técnico. Sin embargo, este es un cambio poco importante ya que se pueden establecer parámetros a los cuales se podría denominar "folios" para evitar el cambio de nomenclatura históricamente acuñada, tal y como lo mantiene inserto el Sistema Juris 2000.

Un aspecto vital es prever mecanismos eficaces para el examen del expediente integralmente considerado, no sólo a través de terminales de consulta dispuestos en los sedes judiciales del país, sino también la conveniencia de permitir un acceso remoto mediante mecanismos de seguridad, así como opciones para que los interesados puedan consultar sus expedientes en el despacho judicial más cercano a sus intereses.

En Venezuela el proceso judicial desde sus inicios ha girado en torno a la agregación de documentos a un expediente físico y de papel, por tanto, con la implementación del Sistema Automatizado Juris 2000 la pretensión ha sido lograr que el sistema de gestión, procure registros los mas fidedigno posible acerca de los documentos contenidos en el expediente. Al respecto, el artículo 25 de la Resolución N° 70 que ordena la creación progresiva de la estructura organizativa y funcional del Juris 2000 en los Circuitos Judiciales del país, establece el Archivo de la Sede (AS) como encargado del manejo físico de los expedientes (asuntos), de la custodia de los mismos y del control sobre su ubicación dentro de la Sede.

Laura Louza Scognamiglio, quien fue en el año 2002 Gerente de la Unidad Coordinadora del Proyecto de Infraestructura de Apoyo al Poder Judicial, ha señalado en su estudio sobre “La Revolución Judicial en Venezuela” *que el sistema (Juris 2000) permite crear un expediente electrónico que garantiza que se reconozca el contenido del expediente y el estado de la causa electrónicamente*<sup>53</sup>. Sin embargo, aunque este tipo de sistemas brinda la posibilidad de hacer seguimiento de documentos, de manera de saber el estado y ubicación, tanto lógica como física, de los documentos componentes de un expediente judicial, no cuenta con la autenticación del mensaje de dato, que ofrece la firma digital como mecanismo de validación.

En defensa de este argumento, la Sala Constitucional ha realizado un llamado de atención sobre sus limitaciones en este aspecto, al reseñar que el acceso directo a las actas procesales es indispensable para la obtención de certeza de lo que ocurre en el juicio y para que, en consecuencia, se defiendan con conocimiento de causa, es decir, no puede equipararse el acceso físico de las actas con la consulta de actuaciones en el Juris 2000.

Ahora bien, si se reflexiona este criterio frente a un caso de extravío y reconstrucción del físico de un expediente, sería necesario citar la Sala de Casación Civil del Tribunal supremo de Justicia, en sentencia N° RC.00294, la cual ha indicado al respecto lo siguiente:

*“...Se estima oportuno realizar algunas consideraciones en cuanto a ciertos lineamientos que deberán seguir los jueces cuando en lo sucesivo les ocurran este tipo de situaciones irregulares en las cuales se extravíe un expediente.*”

---

<sup>53</sup> Louza S, Laura. La revolución Judicial en Venezuela. FUNEDA. Caracas, 2011, p.36

*En este orden de ideas, una vez verificada por parte del tribunal la pérdida del expediente, el juez debe ordenar con apremio la reconstrucción del mismo, a tales fines **el secretario expedirá certificación de los asientos del libro Diario llevado al respecto por el tribunal**, por esto es indispensable que tales asientos a pesar de ser breves, deben abarcar lo más detallado posible el contenido de la actuación que se trate, pues de ello depende que posteriormente se puedan verificar con exactitud cómputos, lapsos procesales y demás actuaciones”.*<sup>54</sup> (Resaltado en negritas de la autora)

Por su parte, el artículo 8 de la Resolución N° 70, que ordena la implantación progresiva del Sistema Integral de Gestión, Decisión y Documentación JURIS 2000, señala que:

*“Artículo 8. Los Jueces que integran los Circuitos Judiciales en cada Circunscripción Judicial individualmente llevarán un Libro Diario y un Copiador de Sentencia... **los asientos de las actuaciones del Libro Diario se realizarán a través de la actuación de la impresión de los archivos digitalizados, contenidos en JURIS 2000...**”* (Resaltado en negritas de la autora)

De lo citado, vale la pena resaltar que si los registros en el sistema Juris tienen entre sus limitaciones la inexistencia de fiabilidad y certeza, tal y como lo ha ido demostrando en la praxis, no es viable que se reconstruya el expediente extraviado con las actuaciones de los archivos electrónicos (Libro Diario de Actuaciones) aún cuando estos se hallen refrendados con la firma del Juez o del secretario según los requerimientos de Ley. Pues, existen casos en los que se omite el registro informático de algunas actuaciones, y siendo así, el registro en el Libro Diario resultaría inexistente. Esta situación que ha sido evidenciada por los señalamientos del Juzgado Superior Noveno

---

<sup>54</sup> Tribunal Supremo de Justicia. Sala de Casación Civil. Sentencia N° RC.00294 de fecha 31 de mayo de 2005. (caso: Roland Fetit Pifano contra Beatriz Coromoto Hernández de Fuentes) [Documento en línea]. Disponible en: [www.tsj.gov.ve](http://www.tsj.gov.ve). (fecha de consulta: 21/11/2010)

en lo Civil, Mercantil y de Tránsito del Área Metropolitana de Caracas al referir:

*“...Las partes no pueden pretender sustituir la revisión del expediente con la consulta del sistema Juris 2000, pues los registros informáticos aportan un resumen cronológico automatizado de las fases preclusivas y de las actuaciones pero no transcriben la totalidad de su contenido y, en ese sentido, el acceso al expediente a través del sistema es limitado; **aunado al hecho de que pueden darse casos donde no coincide o aún no está cargado o actualizado en el sistema la información por cualquier circunstancia...**”<sup>65</sup> (Resaltado en negritas de la autora).*

Finalmente, hay que señalar, que siendo el Libro Diario un instrumento de carácter público, que se genera del registro digital efectivo de una actuación judicial, debe hacerse la salvedad que si no se encuentra registrada una actuación por la omisión negligente de un funcionario, ésta se tendrá como no válida.

La Sala Constitucional del Tribunal Supremo de Justicia ha dejado sentado, que la información errada en la consulta de la Oficina de Atención al Público, no implica una consecuencia jurídica gravosa del derecho de defensa de la parte, pues, para que se configure la denuncia se hace necesario y obligatorio el acceso al expediente, es decir, el no aparecer una actuación en el Juris 2000, no tiene la misma consecuencia que el físico del expediente. En este sentido, exculpar los registros de un sistema, sería válido cuando carece de los sistemas de seguridad que certifiquen su

---

<sup>55</sup> Juzgado Superior Noveno en lo Civil, Mercantil y del Tránsito de la Circunscripción Judicial del Área Metropolitana de Caracas. Exp. N° 8490. (Caso: Vicente Rios Castillo vs. Hippocampus Vacation Club, C.A) [Documento en línea]. Disponible en: [www.tsj.gov.ve](http://www.tsj.gov.ve). (fecha de consulta: 21/11/2010)

fiabilidad, pero qué sucede cuando es el único medio de reproducción cuando el expediente se ha extraviado.

#### 3.3.4 Las Notificaciones Electrónicas.-

De acuerdo con Pérez Sarmiento<sup>56</sup>, la notificación y citación son formas diferentes, pero sutilmente emparentadas, de comunicación de los actos procesales, sin las cuales sería imposible hacer avanzar un proceso y al mismo tiempo garantizar los derechos de las partes de defensa y accesos a la justicia.

Según este mismo autor, en la estricta pureza de doctrina, la notificación “*es el acto procesal por medio del cual se impone a una parte del contenido de una decisión judicial, copia de la cual se le entrega o se le impone de manifiesto*”. Por su parte, la citación “*se concibe como el acto procesal por medio del cual se informa a una parte o a un tercero (testigo, perito, tercero citado en saneamiento) que debe concurrir al proceso para intervenir en un acto concreto*”. Tratándose de una u otra, ambas son convocatorias que permiten la incorporación de la parte al proceso como cumplimiento de las formalidades legales necesarias para garantizar el derecho constitucional a la defensa. Es por ello, que a los efectos de este estudio no revierte mayor importancia su distinción, sino detallar su tratamiento bajo medios tecnológicos de gestión procesal.

Siendo la notificación y la citación una formalidad del proceso de suma importancia, es delicado su tratamiento a través de medios tecnológicos, sobre todo si surgen como una alternativa inmediata para lograr que los

---

<sup>56</sup> Pérez S, Erick L. *Comentarios a la Ley Orgánica Procesal del Trabajo*. Segunda Edición. Editores Hermanos Vadell. Valencia. 2004, p.152

procesos judiciales se desarrollen con una mayor celeridad, economía y seguridad procesal. Al respecto, Peñaranda Quintero ha definido la notificación electrónica como:

*“Actos comunicacionales emanados por la administración pública y privada utilizando medios electrónicos y telemáticos, haciendo posible a las partes de un proceso poder enterarse del contenido de las resoluciones de su interés, desde su hogar, oficina o de cualquier lugar donde cuente con acceso a internet, sin necesidad de desplazarse al órgano emisor de la comunicación”.*<sup>57</sup>

Antes de la entrada en vigencia de la Ley de Mensaje de Datos y Firmas Electrónicas del año 2001, ya se había ventilado en el ámbito jurídico venezolano, el uso de la notificación electrónica. La Sala Constitucional del Tribunal Supremo de Justicia, el 1 de febrero de 2000, modificó el procedimiento de amparo y una de las novedades incluidas fue la forma de realizar la citación del presunto agraviante y la notificación del Ministerio Público, pues, la misma puede hacerse a través de boleta, comunicación telefónica, fax, telegrama, correo electrónico, o cualquier otro medio de comunicación interpersonal. La sentencia referida señala textualmente:

*“Los Tribunales o la Sala Constitucional que conozcan de la solicitud de amparo, por aplicación de los artículos de la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales, admitirán o no el amparo, ordenarán que se amplíen los hechos y las pruebas, o se corrijan los defectos u omisiones de la solicitud, para lo cual se señalará un lapso, también preclusivo. Todo ello conforme a los artículos 17 y 19 de la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales.”*

*“Admitida la acción, se ordenará la citación del presunto agraviante y la notificación del Ministerio Público, para que concurran al tribunal a conocer el día en que se celebrará la audiencia oral, la cual*

---

<sup>57</sup> Peñaranda Q, Héctor R. *Propuesta para lograr la Notificación Electrónica en La República Bolivariana de Venezuela mediante un Sistema de Información Automatizado*. Dirección Ejecutiva de la Magistratura. Disponible en: [http://www.ucol.mx/investigacionesjuridicas/archivos/2012/06/mar\\_283\\_notificacion\\_electronica.pdf](http://www.ucol.mx/investigacionesjuridicas/archivos/2012/06/mar_283_notificacion_electronica.pdf). (fecha de consulta: 27/08/2012)

*tendrá lugar, tanto en su fijación como para su práctica, dentro de las noventa y seis (96) horas a partir de la última notificación efectuada. Para dar cumplimiento a la brevedad y falta de formalidad, la notificación podrá ser practicada mediante boleta, o comunicación telefónica, fax, telegrama, correo electrónico, o cualquier medio de comunicación interpersonal, bien por el órgano jurisdiccional o bien por el Alguacil del mismo, indicándose en la notificación la fecha de comparecencia del presunto agraviante y dejando el Secretario del órgano jurisdiccional, en autos, constancia de haberse efectuado la citación o notificación y de sus consecuencias”.*<sup>58</sup>

Parafraseando a Peñaranda<sup>59</sup>, se trata de una sentencia en la no se prevén los sistemas de seguridad que acrediten la fiabilidad de la información contenida en la notificación electrónica, y lo que en consecuencia crea inseguridad jurídica y podría llegar a violar el derecho de defensa de las personas. Además, en virtud de lo establecido en el artículo 335 de la Constitución de la República Bolivariana de Venezuela, la referida sentencia es vinculante “para otras Salas del Tribunal Supremo de Justicia y demás tribunales de la República”.

Ahora bien, considerando requerimientos necesarios para materializar y otorgarle validez a la notificación electrónica, Madrigal Jiménez cita la legislación peruana (Ley N° 27419), la cual ha previsto los siguientes:

*“-Confirmación de recepción, es decir, el correo electrónico debería presentar una confirmación de recepción del documento;*

*-Sólo se notificará por correo electrónico a la parte que lo hubiere solicitado;*

---

<sup>58</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 07 de fecha 01 de febrero de 2000. (Caso: José Amado Mejía Betancourt y otros contra "los actos lesivos contenidos en: Primero: El acto dictado por el Fiscal Trigésimo Séptimo del 3/12/99. Segundo: el acto dictado por el titular del Juzgado de Control Vigésimo Sexto de Primera Instancia del Circuito Judicial Penal del Área Metropolitana de Caracas el 12/01/00). Disponible en: <http://www.tsi.gov.ve>. (fecha de consulta: 27/08/2012)

<sup>59</sup> Peñaranda Q, Héctor R. *Propuesta para lograr la Notificación Electrónica en La República Bolivariana de Venezuela mediante un Sistema de Información Automatizado...ob. cit.*

*-Los gastos directos (no así los indirectos) por el servicio quedan incluidos en la condena de costas;*

*-Se dejará constancia en el expediente del ejemplar de la notificación entregado para su envío y se anexará al expediente el reporte técnico;*

*-La Notificación por correo electrónico debería contener los mismos datos que la cédula de notificación judicial (notificación tradicional)»<sup>60</sup>*

Por su parte, en Venezuela la Ley de Mensaje de Datos y Firmas Electrónicas (LMDFE) prevé lo siguiente en su artículo 9:

*“Las partes podrán acordar un procedimiento para establecer cuándo el mensaje de datos proviene efectivamente del emisor. A falta de acuerdo entre las partes, se entenderá que un mensaje de datos proviene del emisor, cuando éste ha sido enviado por: el propio emisor.*

*Persona autorizada para actuar en nombre del emisor respecto de ese mensaje. Por un sistema de información programado por el emisor, o bajo su autorización, para que opere automáticamente”.*

Es decir, establece con precisión el origen y destino del mensaje de datos. La constancia del origen del mensaje de datos, esto es, del emisor del mismo, operará de conformidad con lo pactado entre las partes o, en su defecto, cuando fuere posible evidenciar que el mismo fue, efectivamente, enviado por el propio emisor o por una persona autorizada para actuar en nombre del emisor a través de un sistema de información programado por el emisor, o bajo su autorización.

Además, el artículo 11 de la Ley de Mensaje de Datos y Firmas Electrónicas (LMDFE) dispone que el momento de recepción de un mensaje de datos se producirá cuando éste hubiere ingresado al sistema de información que el destinatario hubiere designado al efecto o, en caso de que

---

<sup>60</sup> Madrigal J, Ricardo. *El Procedimiento Judicial Electrónico...*ob. cit.

ningún sistema se hubiere designado, cuando, salvo prueba en contrario, ingrese en un “sistema de información utilizado regularmente por el destinatario”

De regulaciones y consideraciones previas, se puede concretar que todas estas garantías, sólo las ofrece los Certificados Electrónicos llamados Fedatarios Judiciales en otros países, o las mismas llamadas entidades certificadoras de firma digital, que garantizarán la integridad, inalterabilidad y confidencialidad de un mensaje de datos judicial, que se le debe imprimir a una notificación judicial y más si se trata de una que se le quiere dar carácter de personal. Sin en cumplimiento de tales técnicas, los mensajes de datos no ofrecerán ninguna garantía de confiabilidad procesal a sus interlocutores.

La sentencia de la Sala Constitucional ya citada al inicio de este punto, hace referencia a la notificación por medio de correo electrónico, la cual es pertinente indicar que no ofrece garantía de la lectura efectiva del mensaje y así lo confirma Peñaranda al señalar:

*“Por ejemplo, si el usuario posee una cuenta de correo electrónico gratuita, tipo Hotmail, Yahoo o Gmail, por citar los proveedores más utilizados, los cuales no proporcionan en sus interfaces la opción de confirmación de lectura requerida para blindar el proceso, no se puede garantizar la lectura de la notificación por parte del usuario”.<sup>61</sup>*

Aparte del criterio que asumió la Sala Constitucional de la notificación por medios electrónicos, los legisladores han sumado al cuerpo normativo de ciertas leyes, la posibilidad de practicar las notificaciones bajo la modalidad

---

<sup>61</sup> Peñaranda Q, Héctor R. Propuesta para lograr la Notificación Electrónica en La República Bolivariana de Venezuela mediante un Sistema de Información Automatizado... op. cit

de las nuevas tecnologías. Por ejemplo, La Ley Orgánica Procesal del Trabajo vigente regula en su artículo 126 lo siguiente:

*“...El Tribunal, a solicitud de parte o de oficio, podrá practicar la notificación del demandado por los medios electrónicos de los cuales disponga, siempre y cuando éstos le pertenezcan. A efectos de la certificación de la notificación, se procederá de conformidad con lo establecido en la Ley Sobre Mensajes de Datos y Firmas Electrónicas en todo cuanto le sea aplicable, atendiendo siempre a los principios de inmediatez, brevedad y celeridad de la presente Ley. A todo evento, el Juez dejará constancia en el expediente, que efectivamente se materializó la notificación del demandado. Al día siguiente a la certificación anteriormente referida, comenzará a correr el lapso para la comparecencia de las partes a la audiencia preliminar...”*

Por otro lado, la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes prevé la notificación electrónica en su artículo 459 al señalar:

*“El Tribunal también puede practicar la notificación de la parte demandada por los medios electrónicos de los cuales disponga, siempre y cuando estén adscritos al Tribunal o al Poder Judicial. A efectos de la certificación de la notificación, se debe proceder de conformidad con lo dispuesto en la*

*Ley sobre Mensajes de Datos y Firmas Electrónicas y su Reglamento en todo cuanto le sea aplicable, atendiendo siempre a los principio procesales de esta Ley. De no ser posible la plena certificación electrónica de estos mensajes de datos, por no existir en el país los medios necesarios para ello, el Tribunal utilizará todos los medios a su disposición para asegurar que los mensajes enviados contengan medios de seguridad suficientes para asimilar, en el mayor grado posible, los mensajes enviados a los requisitos previstos en dicha Ley.*

*En todo caso, el secretario o secretaria debe dejar constancia en el expediente, que efectivamente se materializó la notificación del demandado o demandada. Se presume cierta la certificación que haga el secretario o secretaria de la efectiva concreción de esta notificación, salvo prueba en contrario por quien alegue no haber sido efectivamente notificado o notificada”.*

De ambas normas se desprende un elemento importante y es que el secretario debe dejar constancia de la práctica efectiva de la notificación por medio electrónico. Esto no significa que, solamente, deje constancia del envío del correo electrónico, sino además, de que se materializó la notificación electrónica; es decir, que el receptor recibió la notificación electrónica y que tuvo acceso a la lectura de la misma. No obstante, puede sostenerse que en Venezuela la modalidad de la notificación electrónica no resulta en la actualidad operativa, ya que carece de los medios tecnológicos adecuados para certificar la recepción y el origen de la información, así como la integridad del documento. A los efectos de la certificación del accionado que contemplan las normas citadas, se debe advertir de un servicio de certificación que pertenezca al Tribunal Supremo de Justicia o a la Dirección Ejecutiva de la Magistratura. SUSCERTE debe acreditar al Tribunal Supremo de Justicia como un Proveedor de Servicios de Certificación, tal y como se acordó en el Convenio de Cooperación Interinstitucional entre el Poder Judicial y el Ministerio de Ciencia y Tecnología en el año 2004, a los fines de que asuma el reto de convertirse en un certificador de firmas y datos electrónicos.

### **3.4 Connotación del Debido Proceso en un servicio judicial de gestión automatizada (el Juris 2000).-**

El constituyente venezolano en el año 1999, reconoció un conjunto de derechos y garantías previstas en el artículo 49 constitucional, que conforman el llamado principio de legalidad de las formas procesales, el cual es pilar fundamental en el ejercicio de las funciones por parte de las autoridades judiciales y administrativas, razón por la cual están obligadas a respetar las formas propias de cada juicio y a asegurar la efectividad de todas aquellas normas que permitan al justiciable el ejercicio de la defensa de los derechos u obligaciones que están bajo consideración judicial.

De esta manera, el debido proceso se configura como la regulación jurídica que de manera previa limita los poderes del Estado y establece las garantías de protección a los derechos de las partes en un proceso, de modo que ninguna de las actuaciones de las autoridades judiciales dependa de su propio arbitrio, sino que se encuentren sujetas a los procedimientos señalados en la ley.

En apoyo a este argumento, la Sala Constitucional del Tribunal Supremo de Justicia señaló que:

*“Dentro del conjunto de garantías que conforman la compleja noción del debido proceso, entendido en su sentido formal, se encuentra el derecho de toda persona a ser juzgada de acuerdo con el procedimiento judicial establecido con anterioridad en la ley, ello en virtud del principio de legalidad de las formas procesales que rige en ordenamientos jurídicos como el venezolano, donde está excluido el principio de libertad de las formas procesales. Tal garantía, atiende al mismo tiempo al principio de seguridad jurídica que ha de regir las relaciones jurídicas existentes entre los particulares y entre éstos y el Estado, específicamente, en cuanto a la determinación previa de las vías judiciales que deberán seguirse en aquellos casos en los que surjan conflictos con motivo de dichas relaciones, que deban ser dirimidos en definitiva por los órganos jurisdiccionales competentes”.*<sup>62</sup>

Ahora bien, el artículo 49 de la Constitución de la República Bolivariana de Venezuela ha sido taxativo al señalar que un proceso será debido cuando en la actividad judicial concurren los siguientes presupuestos:

1. El derecho a la defensa, es decir, a ser notificado de los cargos de investigación, en todo estado y grado, de contar con asistencia jurídica, tener acceso a las pruebas y el permitir su correspondiente defensa frente a ellas,

---

<sup>62</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 2403 de fecha 09 de octubre de 2002. (Caso: Amparo José Diógenes Romero). [Documento en Línea]. Disponible en: <http://www.tsj.gov.ve/decisiones/scon/Octubre/2403-091002-01-2813%20.htm>. (Fecha de consulta: 19/05/2011)

así como, el derecho a recurrir del fallo..."con las excepciones establecidas en la Constitución y la ley";

2. Presunción de inocencia, en la que establece en forma explícita el principio de que "toda persona se presume inocente mientras no se pruebe lo contrario";

3. El Derecho a audiencia, es decir, a ser oído;

4. Derecho al juez natural, competente e imparcial;

5. La garantía de la confesión no coactiva;

6. El Principio de legalidad (Nullum crimen nulla poena sine lege).Nadie puede ser sancionado por actos u omisiones que no fueren previstos como infracciones en leyes preexistentes;

7. La Cosa juzgada: "Non bis in idem". Nadie puede ser sometido a juicio por los mismos hechos en virtud de los cuales hubiese sido juzgada anteriormente;

8. La garantía de la responsabilidad estatal por errores o retardos judiciales, por lo que toda persona puede solicitar del Estado, el restablecimiento o reparación de la situación jurídica lesionada por error judicial, retardo u omisión injustificada. Queda a salvo el derecho del particular de exigir la responsabilidad personal del magistrado o del juez del Estado.

Entre las garantías que constituyen el debido proceso, el derecho a la defensa contenido en el numeral 1º del artículo 49, tiene especial significación, por cuanto comporta entre otros derechos, el derecho a ser oído, a acceder al expediente, a ser notificado, a solicitar y participar en la práctica de las pruebas y a impugnar decisiones judiciales, los cuales obligan a los órganos jurisdiccionales a brindar las más amplias posibilidades al

justiciable; antes y después de la adopción de cualquier decisión, garantizando la protección de los derechos fundamentales dentro de la relación procesal, en procura de decisiones verdaderamente justas y materiales. De esta forma, no podría el órgano judicial sorprender a las partes con una decisión que lesione su esfera jurídica, sin que previamente haya tenido oportunidad de defenderse contra ella, en virtud de que esa situación iría en contra de los fundamentales principios de defensa.

Uno de los medios de satisfacción del debido proceso se verifica cuando el trámite garantiza a las partes la defensa efectiva y adecuada de sus derechos de conformidad con lo consagrado en la Ley, otorgándoseles el tiempo y los medios apropiados para anteponer sus posturas y elementos probatorios en la tutela de sus intereses. Bajo este planteamiento, más allá de la conformación legal del proceso en la actualidad, la transformación de los órganos jurisdiccionales sometidos a un sistema de gestión automatizado como el Juris 2000 debe apostar a herramientas tecnológicas que permitan una efectiva protección del derecho de defensa y en consecuencia del debido proceso.

De una manera explícita, la Sala Política Administrativa del Tribunal Supremo de Justicia ha señalado el contenido y el alcance del derecho a la defensa, al pronunciar que:

*"Entre otras manifestaciones, ha sido concebido como el derecho a ser oído, puesto que no podría hablarse de defensa alguna, si el administrado no cuenta con esta posibilidad; el derecho a ser notificado de la decisión administrativa a los efectos de que le sea posible al particular, presentar los alegatos que en su defensa pueda aportar al procedimiento, más aun si se trata de un procedimiento que ha sido iniciado de oficio; el derecho a tener acceso al expediente, justamente con el propósito de examinar en cualquier estado del procedimiento, las actas que lo componen,*

*de tal manera que con ello pueda el particular obtener un real seguimiento de lo que acontece en su expediente administrativo. Asimismo, se ha sostenido doctrinariamente que la defensa tiene lugar cuando el administrado puede presentar pruebas, las cuales permitan desvirtuar los alegatos ofrecidos en su contra por la Administración y finalmente, con una gran connotación, el derecho que tiene toda persona a ser informado de los recursos y medios de defensa, a objeto de ejercer esta última frente a los actos dictados por la Administración.<sup>63</sup>*

A tal efecto, un proceso debido se ofrece como una garantía que permite a los ciudadanos ejercitar su defensa en el marco de una sucesión de actuaciones judiciales y disfrutar de la oportunidad efectiva de interponer los recursos que las mismas normas autoricen. La notificación de una decisión judicial es un requisito básico para el posterior ejercicio del derecho a responder o controvertir, y si, el medio electrónico no es accesible o confiable, el ciudadano puede perder la oportunidad de respuesta y con ello su derecho de defensa.

Al respecto, Flores Zuloaga ha referido que:

*“El artículo 14 del Pacto Internacional de Derechos Civiles y Políticos en su numeral primero establece la igualdad de todas las personas ante los tribunales y cortes de justicia. En el contexto venezolano esta exigencia debe interpretarse como la posibilidad material o real de acceder en igualdad de condiciones a las herramientas tecnológicas, si estas llegasen a considerarse por los funcionarios como obligatorias, o como opciones que reemplacen los medios tradicionales de comunicación de las decisiones públicas (los medios físicos)<sup>64</sup> .*

---

<sup>63</sup> Tribunal Supremo de Justicia. Sala Político Administrativa. Sentencia N° 01459 de fecha 12 de julio de 2001. (Caso: Alejandro Ramón Guedez E. vs. Ministro De Justicia). [Documento en Línea]. Disponible en: <http://www.tsj.gov.ve/decisiones/spa/Julio/01459-120701-01-0326.htm>. (fecha de consulta: 19/06/2010)

<sup>64</sup> Flores. Z, Felipe. *Uso de las Tecnologías de la Información y la Comunicación. ¿El Debido Proceso en Peligro?* Grupo de Acciones Públicas ICESI. [Documento en línea]. Disponible en: [http://www.icesi.edu.co/grupo\\_acciones\\_publicas\\_icesi/images/pdfs/articulo\\_injusticias.pdf](http://www.icesi.edu.co/grupo_acciones_publicas_icesi/images/pdfs/articulo_injusticias.pdf). (fecha de consulta: 26/02/2011)

Ahora bien, con la implantación del sistema Juris 2000, en las sedes judiciales del país, diversos criterios reiterados del Tribunal Supremo de Justicia han considerado, que la certeza jurídica de lo que acontece en un proceso judicial, se encuentra contenida en los expedientes que reposan en los archivos de los Tribunales, por lo que las informaciones a través de un medio auxiliar, como es el Sistema Integral de Gestión y Documentación, Juris 2000, es simplemente informativo. En él se procura divulgar las distintas actividades y decisiones que se producen en el ámbito judicial, sin sustituir las actas de un expediente.

Asumir estas consideraciones acarrea inseguridad jurídica para las partes de un proceso, toda vez que la Dirección Ejecutiva de la Magistratura ha referido al sistema Juris 2000 como:

*“...Un sistema de computación que permite la automatización del expediente procesal y la jurisprudencia de los tribunales, lo que genera celeridad a la función jurisdiccional y llevar un efectivo control, por lo que **el usuario puede obtener una información precisa sobre sus casos** y un mejor servicio de administración de justicia<sup>65</sup>”.*(Resaltado en Negritas de la autora).

En consecuencia, se trata de un diseño apropiado que logra garantizar al ciudadano transparencia en las operaciones judiciales, mecanismos que aseguren la imparcialidad del Juez, así como, solventar las necesidades de acceso a la información sobre las acciones que se ventilan en cada despacho judicial por parte del ciudadano.

---

<sup>65</sup> Dirección Ejecutiva de la Magistratura. *Juris 2000. El Modelo Organizacional*. Justicia en un click. [Documento en Línea]. Disponible en: <http://dem.tsj.gov.ve/unclick.htm>. (fecha de consulta: 25/07/2010)

Con ocasión a estos señalamientos, se hace mención al cumplimiento de dos elementos, como la publicidad de las actuaciones judiciales y la equivalencia funcional del mensaje de datos, que informa sobre el historial del proceso y la información escrita en el expediente. Es decir, la información sobre el historial de los procesos que aparece registrada en los computadores de los juzgados tiene el carácter de un “mensaje de datos”, por cuanto se trata de información comunicada a través de un medio electrónico, en este caso, la pantalla de un computador que opera como dispositivo de salida. Así mismo, la emisión de este tipo de mensajes de datos puede considerarse un acto de publicidad procesal, por cuanto a través de ella se pone en conocimiento de las partes, de terceros o de otras autoridades judiciales o administrativas, las resoluciones y órdenes de jueces, en relación con los procesos sometidos a su conocimiento.

De lo anterior, se enfatiza que, la materialización del derecho a la defensa y del debido proceso, regulada en el numeral 1 del artículo 49 de la Constitución de la República Bolivariana de Venezuela, ese ve resuelta a través de la publicidad de las actuaciones judiciales y del tratamiento que se le dé.

La Sala Electoral del Tribunal Supremo de Justicia en sentencia N° 26 de fecha 15 de Abril del 2008, resolvió al respecto que:

*“...El derecho a un debido proceso consiste en la exigencia de ver cumplidos, tanto en la fase cognoscitiva como en la de carácter ejecutiva, un conjunto de derechos y garantías mínimas establecidas por ley, aplicable a cualquier asunto incidental o principal, en sede administrativa y jurisdiccional...Dentro de este grupo, se encuentran el derecho a la defensa: integrado por el derecho de acceso a la prueba, **la publicidad de los actos**, entre otros...Concretamente, en cuanto a la publicidad de los actos procesales, la misma debe entenderse como*

*un presupuesto de validez del proceso, por cuanto ella se integra a una fase esencial de aquél, cuyo fin último es mantener el equilibrio procesal al permitir a una de las partes conocer su situación jurídica procesal y hacer valer todos los alegatos y pruebas, de allí que sea parte fundamental del derecho a la defensa<sup>66</sup>.”(Resaltado en negritas de la autora).*

En este sentido, los sistemas informáticos utilizados por los despachos judiciales, para generar, enviar, archivar o procesar tales mensajes de datos, configuran un sistema de información que facilita a la administración de justicia, el cumplimiento eficiente de sus cometidos, en particular, de su deber de dar publicidad a las actuaciones judiciales, a la vez que facilita a los ciudadanos el acceso a la administración de justicia. Propósitos que sólo se satisfacen si los datos registrados en dichos sistemas computarizados tienen carácter de información oficial, de modo tal que puedan generar confianza legítima en los usuarios de la administración de justicia. De lo contrario, la implementación de tales sistemas, además, de no contribuir a lograr mayores niveles de eficiencia, publicidad y acceso a la administración de justicia, resultan incluso contraproducente para alcanzar tales fines.

Es necesario que los sistemas automatizados dispuestos al servicio de las sedes judiciales, mantengan el elemento de la equivalencia funcional entre los registros electrónicos y el expediente. Es decir, que no exista una discriminación del mensaje de dato frente a la cultura del físico del expediente, lo cual será posible cuando se dispongan en los softwares de gestión judicial, mecanismos de seguridad en el tráfico de la información.

---

<sup>66</sup> Tribunal Supremo de Justicia. Sala Electoral. Sentencia N° 26 de fecha 15 de abril de 2008. (Caso: Wolfgang Hernández, Pedro Figueredo y Julián Mendoza miembros de la junta directiva del Sindicato de Obreros y Empleados de la Industria de La Construcción y Conservación de Parques y Jardines y sus similares del Municipio Heres del Estado Bolívar. Recurso Contencioso Electoral conjuntamente con solicitud de Amparo Cautelar Expediente N° AA70-X-2008-000004). [Documento en Línea]. Disponible en: [http://www.tsj.gov.ve/decisiones/consulta\\_sala.asp?sala=006&dia=15/4/2008&nombre=Sala Electoral](http://www.tsj.gov.ve/decisiones/consulta_sala.asp?sala=006&dia=15/4/2008&nombre=Sala%20Electoral). (Fecha de Consulta: 18/10/12).

Ese mecanismo de seguridad necesario para que la publicidad de los actos procesales de un sistema automatizado, es la certificación técnica de las actuaciones judiciales, es decir, la implementación de certificados electrónicos que aseguren la integridad de la información, el no repudio, la emisión y recepción de datos, así como, la fiabilidad del momento exacto (tiempo) en que se registran efectivamente los actos procesales.

En apoyo al argumento anterior, en el año 2004 la entonces Ministra de Ciencia y Tecnología, Marlene Córdova señaló lo siguiente:

*“El convenio firmado, a través de la Superintendencia de Certificación de Firmas Electrónicas (SUSCERTE), órgano adscrito a su despacho, convierte a la DEM en el primer órgano del Estado venezolano que asume lo que significaría ser un proyecto piloto para convertirse en certificador de firmas electrónicas\*. **Esto tiene repercusiones importantísimas porque va a permitir al ciudadano común el poder tener comunicación certificada sobre el avance de sus procesos que se están llevando a través de los tribunales y que le brinda la seguridad de que lo que les es comunicado a través de la Dirección Ejecutiva de la Magistratura tiene detrás una certificación legal<sup>67</sup>”.** (Resaltado en negritas de la autora)*

Por otro lado, resulta pertinente citar la Sentencia N° 2821 proferida por la Sala Constitucional del Tribunal Supremo de Justicia, que señala:

*“En sentido estricto el desorden procesal, consiste en la subversión de los actos procesales, lo que produce la nulidad de las actuaciones, al desestabilizar el proceso, y que en sentido amplio es un tipo de*

---

\* Los acuerdos de este convenio no han sido implementados hasta ahora en los servicios que presta los sistemas automatizados en las sedes judiciales, por lo tanto, la Dirección Ejecutiva de la Magistratura, no logró convertirse en el primer órgano certificador de firmas digitales. Actualmente existen dos Proveedores de Servicios de Certificación Electrónica (PSC) como la [Fundación Instituto de Ingeniería para Investigación y Desarrollo Tecnológico \(FIID\)](#) y PROCERT.

<sup>67</sup> Córdova, Marlene. *Suscritos Convenios para modernizar y dignificar la justicia en el país*. Sede del Tribunal Supremo de Justicia. 27 de abril de 2004. [Documento en línea]. Disponible en: <http://www.tsj.gov.ve/decisiones/scon/Octubre/2821-281003-03-1152%20.htm>. (fecha de consulta: 15/05/2010)

*anarquía procesal, que se subsume en la teoría de las nulidades procesales.*

*Stricto sensu, uno de los tipos de desorden procesal no se refiere a una subversión de actos procesales, sino a la forma como ellos se documenten. Los actos no son nulos, cumplen todas las exigencias de ley, pero su documentación en el expediente o su interconexión con la infraestructura del proceso, es contradictoria, ambigua, inexacta cronológicamente, lo que atenta contra la transparencia que debe regir la administración de justicia, y perjudica el derecho de defensa de las partes, al permitir que al menos a uno de ellos se le sorprenda (artículos 26 y 49 constitucionales). En otras palabras, la confianza legítima que genere la documentación del proceso y la publicidad que ofrece la organización tribunalicia, queda menoscabada en detrimento del Estado social de derecho y de justicia<sup>68</sup> (Resaltado en negritas de la autora).*

De acuerdo a este último señalamiento, es necesario insistir, que la función jurídica que cumple la instrumentación escrita y autógrafa respecto de todo acto jurídico, debe cumplirla igualmente la instrumentación electrónica, en la medida que se cumplan los parámetros de confianza. Al efecto, siendo el sistema Juris 2000 una herramienta de información y de participación directa en la publicidad de las actuaciones, no debería ser considerado de restricta fiabilidad en el tratamiento del mensaje de datos (documento judicial electrónico), sino que debería disponer de los mecanismos necesarios de seguridad (firma electrónica y certificación técnica).

Adicionalmente, la certificación técnica de las actuaciones, haría operativa la notificación electrónica prevista en algunas leyes especiales de nuestro país, y cuya práctica ha sido retardada en algunos casos, o no se ha

---

<sup>68</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 2821 de fecha 28 de octubre de 2003. (Caso: José Gregorio Rivero Bastardo. Acción de Amparo) [Documento en Línea]. Disponible en: <http://www.tsi.gov.ve/decisiones/scon/Octubre/2821>. (Fecha de Consulta: 18/07/2011).

aplicado debidamente en otros. Para utilizar el correo electrónico como mecanismo de citación o notificación en la función jurisdiccional, son necesarios sistemas de seguridad que acrediten fiabilidad de la información contenida en la citación o notificación electrónica como la implementación de la firma digital y del certificado electrónico.

Esto último, ampliaría las posibilidades de las partes de ser notificadas de manera más expedita de los procesos que se siguen en su contra y otorgarle validez a la notificación electrónica. Ello a los fines, de no incurrir en decisiones lesivas del derecho a la defensa, como la de la Sala Constitucional del Tribunal Supremo de Justicia, del 1 de febrero de 2000, que modificó el procedimiento de amparo e incluyó la novedad de realizar la citación del presunto agravante y la notificación del Ministerio Público, a través de boleta, comunicación telefónica, fax, telegrama, correo electrónico, o cualquier otro medio de comunicación interpersonal, sin preverse los mecanismos de seguridad.

En relación al derecho de defensa de las partes, es fundamental que en los juicios se utilice la tecnología de punta para lograr una impartición de justicia más rápida y eficaz, sin embargo, ante la falta en nuestro país de un sistema dotado de las seguridades técnicas necesarias (lo que ha denotado una evolución lenta), las partes se limitan a ofrecer como pruebas las que son enumeradas en la ley procesal, pese a que en la mayoría de ordenamientos legales se deja abierta la posibilidad de presentar como prueba los elementos aportados por la tecnología. Se trata del problema de la prueba electrónica que podrían utilizar las partes en un proceso como medio de defensa y el que revierte mayor importancia, cuando la fuente es un sistema automatizado de gestión judicial.

En Jurisprudencia vinculante, la Sala Constitucional del Tribunal Supremo de Justicia ha señalado que las sentencias obtenidas del Juris 2000, deben ser consideradas copias simples, al sostener lo siguiente:

*“...Se aparta del criterio sostenido respecto a la validez de los datos extraídos del Sistema Juris 2000, y a partir del presente fallo establece con carácter vinculante que las decisiones judiciales obtenidas a través del aludido sistema actual sistema informático del Poder Judicial serán consideradas copias simples conforme al artículo 429 del Código de Procedimiento Civil, a los efectos de la interposición de acciones de amparos constitucionales contra sentencias, caso en el cual, tal como se estableció en la sentencia N° 7/2000, la parte accionante tendrá la carga de presentar hasta la oportunidad de la audiencia oral, la copia certificada de la decisión impugnada. Si ello no ocurriera la Sala declarará inadmisibles el amparo interpuesto en el acto de celebración de la audiencia oral (vid. Sent. Núms. 2362/2007 caso: Banco del Caroní, C.A. ó 208/2005 caso: Aracelis Rosa). Asimismo, se declarará inadmisibles la acción antes o en la audiencia oral si se constata, de oficio o a instancia de parte, que el ejemplar de la sentencia accionada en amparo extraído del Sistema Juris 2000 no es conforme con la copia certificada de la sentencia o su original que reposa en el expediente<sup>69</sup>...”*

De lo referido, se concreta, que el documento electrónico no asociado a una firma electrónica, solo tendrá el valor de un indicio, por lo que debe ser acompañado de otros medios de prueba que sustenten los hechos contenidos en el mensaje de datos. En el caso del sistema automatizado Juris 2000 este carácter dado por la sala a sus mensajes de datos (documento), desaparecería, sí las actuaciones judiciales pudieran estar debidamente certificadas por un proveedor de servicios que le otorgara a través de la firma digital, fe pública a sus registros, considerando que este carácter le es otorgado, cuando la impresión de los archivos digitalizados es

---

<sup>69</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 721 de fecha 09 de julio de 2010 (Saco: Acción de Amparo. Parte accionante: Grecia Figueroa). Documento disponible en: <http://www.tsj.gov.ve/decisiones/>. (fecha de consulta: 13/04/2011)

previamente firmado por la autoridades judiciales (juez y secretario) según las formalidades del artículo 1357 del Código Civil venezolano vigente, referidas al documento público.

Finalmente, el Sistema Juris 2000, citando señalamientos de la Sala Constitucional, presenta limitaciones en la información de sus registros, ya que los mismos *“aportan un resumen de las actuaciones pero no las transcriben y, en ese sentido, el acceso al expediente a través del sistema es limitado”*<sup>70</sup>. En este caso, no es posible hablar de equivalencia funcional, ya que la publicidad de las actuaciones, consiste en un reporte de datos que obliga a consultar la totalidad del documento, directamente del expediente. Así, en el historial de un expediente que aparece en el computador del juzgado puede registrarse que en una fecha determinada se profirió sentencia, o se expidió un auto que ordena la práctica de pruebas. Para enterarse del sentido de la decisión adoptada en la sentencia, o de las pruebas ordenadas en el auto, es claro que se debe acudir directamente al expediente, puesto que el historial que aparece en los computadores del juzgado sólo serviría como equivalente funcional de tales providencias si registrara su contenido completo.

Si el adelanto en la implementación de medios tecnológicos en la administración de justicia lleva en el futuro a una completa sistematización de la información contenida en los expedientes, no existirá razón para dejar de considerar tales mensajes de datos, como equivalentes funcionales que reemplacen por completo la revisión directa de los expedientes o de los órganos tradicionales de publicidad oficial de dicha información, siempre que

---

<sup>70</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia Nº 04-3055 de fecha 21 de marzo de 2006. (Alida Teresa Pernaleté Gásperi vs. Coordinadora del Circuito de Protección del Niño y del Adolescente del Estado Lara, abogada Erlinda Oropeza). [Documento en Línea]. Disponible en: <http://www.tsj.gov.ve>. (fecha de consulta: 15/05/2010).

se adopten las debidas medidas de seguridad, de manera similar a como ocurre en la actualidad con las bases de datos de jurisprudencia de países como España.

### **3.5 Formas de quebrantamiento del Debido Proceso a través de un servicio judicial automatizado.-**

La violación del debido proceso y la consecuente indefensión operan en principio dentro de un proceso instaurado, cuando alguna de las partes en el proceso se le priva o se le coarta su derecho a efectuar un acto de petición hasta el punto de quedar menguado. La Sala Constitucional del Tribunal Supremo de Justicia, en la Sentencia N° 80, ha concretado que la violación al debido proceso podrá manifestarse en los siguientes términos:

*“...El derecho al debido proceso - y dentro de éste el derecho a la defensa -, tiene un carácter optativo e instrumental que nos permite poner en práctica los denominados derechos de goce (p. Ej. Derecho a la vida a la libertad, al trabajo), es decir, su función última es garantizar el ejercicio de otros derechos materiales mediante la tutela judicial efectiva, por ello, su ejercicio implica la concesión para ambas partes en conflicto, de la misma oportunidad de formular pedimentos ante el órgano jurisdiccional a) Cuando se prive o coarte a alguna de las partes la facultad procesal para efectuar un acto de petición que a ella privativamente le corresponda por su posición en el proceso; b) cuando esa facultad resulte afectada de forma tal que se vea reducida, teniendo por resultado la indebida restricción a la partes de participar efectivamente en plano de igualdad, en cualquier juicio en el que se ventilen cuestiones que les afecte. Bajo esta óptica la violación al debido proceso y la consecuente indefensión, operará, en principio, dentro de un proceso ya instaurado, y su existencia será imputable al Juez que con su conducta impida a alguna de las partes la utilización efectiva de los*

*medios o recursos que la ley pone a su alcance para la defensa de sus derechos*<sup>71</sup>.

No obstante, en Venezuela, cuando se adoptaron los mecanismos necesarios para implementar la tecnología al servicio de la administración de justicia, para realizar las consultas de los procesos por medios electrónicos, no pareció preverse la relevancia funcional del sistema automatizado Juris 2000 para resguardar la garantía de un proceso debido, a través de la información que revela de las actuaciones judiciales.

La vulneración de garantías constitucionales como el debido proceso, en materia de tecnologías se presenta, cuando se niega toda relevancia a los errores o limitaciones del sistema automatizado de gestión judicial, declarando, por ejemplo, fuera del término las actuaciones realizadas por las partes que confiaron en la información suministrada por la administración de justicia a través de su sistema de gestión.

La Sala Constitucional del Tribunal Supremo de Justicia cuando señaló que *“no puede equipararse el acceso físico a las actas con la consulta de actuaciones en el JURIS 2000, porque el expediente da fe de lo ocurrido en una causa particular, pero no puede afirmarse lo mismo respecto del sistema informático”*<sup>72</sup> ha permitido inferir que la información errada en la consulta de la Oficina de Atención al Público, no, implica una consecuencia jurídica gravosa del derecho de defensa de la parte. Pues, para que se configure la

---

<sup>71</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 80 de fecha 01 de febrero de 2001. (Caso: José Pedro Barnola y otros). [Documento en Línea]. Disponible en: <http://www.tsj.gov.ve/decisiones/scon/Febrero/80-010201-00-1435%20.htm>. (fecha de consulta: 15/05/2010).

<sup>72</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 04-3055 de fecha 21 de marzo de 2006. (Alida Teresa Pernalette Gásperi vs. Erlinda Oropeza). Disponible en: <http://www.tsj.gov.ve>, (fecha de consulta: 15/05/2010).

denuncia se hace necesario y obligatorio el acceso al expediente, es decir, el no aparecer una actuación el Juris 2000 no tiene la misma consecuencia que el físico del expediente. El efecto importante y fundamental es el acceso al físico expediente, y solo en caso que no se permita el acceso al físico del expediente puede la parte proponer ese impedimento de manera real y fehaciente demostrando ante el Juez, violación al derecho a la defensa o a la garantía de la parte.

Al respecto, es necesario observar dos posibles casos de violación que se originan de inconsistencias en los registros del sistema automatizado Juris 2000 y que han mantenido activo, el criterio citado de la Sala Constitucional.

*1. La actuación está inserta en las actas del físico del expediente, pero no se encuentra registrada en el sistema automatizado y en consecuencia en el Libro Diario de Actuaciones.-*

En decisiones reiteradas del Tribunal Supremo de Justicia se ha señalado que el acceso directo a las actas procesales es indispensable para la obtención de certeza de lo que ocurre en el juicio y para que, en consecuencia, las partes se defiendan con conocimiento de causa. Y, adicionalmente, la Dirección Ejecutiva de la Magistratura de nuestro máximo Tribunal, no otorga fe pública a los registros del sistema JURIS 2000.

Sin embargo, en escasas decisiones regionales, se ha considerado, que cuando la actuación no se encuentra asentada en el sistema y menos diarizada, en el libro Diario del Tribunal, debe tenerse como inexistente y nula, es decir, no puede producir efecto jurídico alguno, por cuanto se produjo una omisión en el proceso que solo puede ser subsanada por los

Jueces, quienes deben corregir las faltas que pudieran anular cualquier acto procesal y siendo necesaria la corrección de la actuación irregular efectuada.

Así se tiene, por ejemplo, que el Tribunal Primero de Sustanciación, Mediación y Ejecución de la Coordinación Laboral del Estado Aragua, en un caso como el referido, señaló que:

*“En el caso de autos se observa que el funcionario Judicial no procedió conforme lo prevé el sistema Juris pero lo consigno en el físico del expediente por lo que indujo en error al Tribunal, no existiendo en el sistema Juris la referida consignación aun cuando existía en el físico del expediente mas no en el sistema Juris y por ende no se encuentra asentada dicha actuación y mucho menos diarizada, en el libro Diario del Tribunal de manera que al no ser diarizado en consecuencia, dicha actuación, el cartel consignado debe tenerse como inexistente y nulo”<sup>73</sup>.*

Esta decisión fue revocada por el Tribunal Superior Tercero del Trabajo, quién señaló:

*“Así, en el caso concreto se refiere supuestamente la ocurrencia de una situación irregular en la tramitación de la información automatizada que no la relevaba de cumplir con su carga de constatar en el físico del expediente el estado en el cual se encontraba su causa; expediente que contiene materialmente todas las actuaciones cumplidas en ella que garantizan la transparencia, el principio de publicidad de los actos y el debido proceso”<sup>74</sup>.*

*2. La actuación está inserta en el sistema automatizado y en consecuencia en el Libro Diario de Actuaciones pero no en el físico del expediente.-*

---

<sup>73</sup> Tribunal Primero de Sustanciación, Mediación y Ejecución de la Coordinación Laboral del Estado Aragua. ASUNTO: DP11-L-2008-000913. (Caso: Ángel Luis González vs. Sociedad Mercantil DISTRIBUIDORA LA NUEVA DRAGO I C.A ).

<sup>74</sup> Tribunal Superior Tercero del Trabajo de la Circunscripción Judicial del Estado Aragua. Asunto. No. DP11-R-2009-000038 (Caso: Ángel Luis González vs. Sociedad Mercantil DISTRIBUIDORA LA NUEVA DRAGO I C.A )

En referencia al planteamiento, se ha señalado que la utilización del Juris 2000 permite que las partes consignen actuaciones sin tener a la vista el expediente de la causa ya que no se requiere que las diligencias se extiendan directamente en el expediente sino su presentación ante la Unidad de Recepción y Distribución de Documentos; pero ello, no significa que las partes no tengan derecho a la revisión de las actas procesales cuando así lo requieran, pues, tal como declaró esta Sala, el acceso directo a las actas procesales es indispensable para la obtención de certeza de lo que ocurre en el juicio y para que, en consecuencia, se defiendan con conocimiento de causa. Es decir, se ha continuado con el criterio de la Sala Constitucional ya citado.

Un pronunciamiento de la Sala Constitucional de mayo de este año, ha contrariado las consideraciones que se venían asumiendo respecto a la fiabilidad del registro electrónico del Juris 2000, señalando lo siguiente:

*“...Se debe tener en cuenta que el libro de diario refleja todo lo que aparece en el Sistema Juris 2000, el cual a su vez puede ser consultado por las partes a través de las computadoras disponibles de lo que se ha denominado “Autoconsulta” y que se refiere a que las partes y los abogados (quienes generan su propia clave) pueden ver y consultar el expediente, una vez que se encuentran diarizadas y cargadas en el sistema de manera inmediata, pudiendo observar todas las actuaciones y la hora de realización aunque no tenga en físico el expediente respectivo, viendo todos los expedientes en los que aparecen. Además del mecanismo indicado anteriormente, también el Secretario de guardia puede dar la información a las partes y sus apoderados de manera inmediata y actualizada y finalmente la Oficina de Atención al Público también puede suministrar información sobre el contenido del expediente cuando no se puede observar el físico. Con esto se observa que a pesar de la instalación tecnológica moderna y que no se tenga en físico el expediente respectivo aún se puede decir*

*que las partes se encuentran a derecho y se da la notificación presunta*<sup>75</sup>.

Bajo esta apreciación de la Sala, es necesario advertir que la frase prevista en disposiciones legales, *“una vez que constara en autos la notificación de las partes”*, se ha extendido mas allá de las actas del físico del expediente hasta alcanzar, el registro electrónico del Sistema Juris 2000, sin estimar un posible quebrantamiento material del debido proceso al dejar de un lado las inconsistencias en los registros por errores materiales involuntarios y la inexistencia de equivalencia funcional.

Frente a un caso extremo, de un sistema de gestión judicial que no posee certificación técnica de actuaciones, y en consecuencia, no ofrece fiabilidad en sus registros, cuáles son las garantías que se le otorgan a las partes, cuando por extravío del acta o de alguna causa, la minuta del asiento del libro diario (automatizado) es el que reconstruye las actuaciones del expediente. Sobre todo, cuando de la praxis se observan inexactitudes y contradicciones entre actas del físico y el diario llevado en el sistema informático de un tribunal.

Ahora bien, considerando el derecho que tiene toda persona de ejercer dentro de los lapsos legales establecidos, las acciones y excepciones que consideren beneficiosas, según su condición jurídica dentro del proceso, materializados a través de garantías y derechos como: la asistencia jurídica, notificación de los cargos, derecho a la pruebas, nulidad de las pruebas ilícitas y la doble instancia, cuando estos se limitan, se coartan o disminuyen se activa o patentiza la indefensión. Quebrantamiento de forma que se

---

<sup>75</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 624 de fecha 15 de mayo de 2012. (Caso: Instituto Fondo de Protección Social de los Depósitos Bancarios. Acción de Amparo). [Documento en Línea]. Disponible en: <http://www.tsj.gov.ve/decisiones/scon/Mayo/624-15512-2012-11-0638.html>. (Fecha de Consulta: 02/06/2012)

caracteriza, según el Dr. Aníbal Rueda y la profesora Peretti de Parada<sup>76</sup>, en los siguientes elementos:

a. Que sea imputable al operador de justicia, pues siendo éste el árbitro y director judicial, debe garantizar y no limitar el derecho, de manera que aun cuando alguna de las partes del proceso, pueda inducir o perpetrar cualquier acto que menoscabe el derecho a la defensa, es el operador de justicia quien debe tomar las medidas pertinentes para que el acto no llegue a consumarse, siendo él quien debe producir la decisión judicial pertinente que al final es la que pueda generar o producir la indefensión.

b. Que el operador de Justicia impida a las partes la utilización efectiva de los medios o recursos que la ley impone a su alcance para la defensa de sus derechos.

Al respecto, vale la pena asumir que la publicidad de las actuaciones judiciales como resultado de lo tramitado en el proceso, es una garantía importante, en el sentido de que pone a conocimiento de las partes los juicios que se siguen en su contra y las determinaciones de carácter procesal que se han tomado en el transcurso del litigio. No obstante, cuando en los servicios de justicia participa la implementación de un sistema de gestión automatizado, esa garantía debe extenderse a los registros electrónicos que permiten informar a las partes del historial del proceso, siempre que se cumpla con el elemento de la equivalencia funcional de lo que se maneja en registros automáticos y el físico de las actas. En consecuencia, cuando la equivalencia funcional no opera en el sistema de gestión judicial, y es de notoriedad judicial que los registros de éste, presentan irregularidades o inconsistencias, será imputable al juzgador las indefensiones que se causen

---

<sup>76</sup> Rueda, Aníbal y Peretti de Parada Magali. *La indefensión*. Vadell Hermanos Editores. Caracas. 1998, p.12

al justiciable como resultado de la desinformación de un registro que no guarda fiabilidad en el mensaje de datos o que muchas veces causa inseguridad jurídica en las partes porque los ingresos de las actuaciones son realizadas a destiempo.

### **3.6 El Certificado Electrónico como necesidad de un proceso judicial debido.-**

El Ingeniero Luis Hellin<sup>77</sup> señala que es necesario el certificado digital en la Administración de Justicia para la protección de los derechos del justiciable, por garantías procesales y para generar confianza en el sistema judicial.

Lo anterior, es posible lograrlo a partir de lo que se ha denominado *Equivalencia Funcional*, el cual según Soto Caldera, citado por Jurado consiste en:

*“Aplicar a los mensajes de datos un principio de no discriminación respecto a las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas; en este sentido los efectos jurídicos deseados por el emisor de la declaración deben producirse con independencia del soporte en papel o electrónico donde conste la declaración”.*<sup>78</sup>

---

<sup>77</sup> Hellin, Luis. *La Certificación y Firma Electrónica en el ámbito de la informática Forense*. I Congreso Internacional de Seguridad de la Información. Caracas, 2010. [Documento en línea]. Disponible en: [www.SUSCERTE.gob.ve](http://www.SUSCERTE.gob.ve). (fecha de consulta: 21/11/2010).

<sup>78</sup> Soto C, Milagros M. “*Consideraciones sobre la prueba documental electrónica en el proceso civil venezolano*”. Estudios de Derecho Civil. Vol III. Libro homenaje a José Luis Aguilar Gorronzona. Tribunal Supremo de Justicia. Colección Libros homenaje No. 5. Caracas, 2001, p.663

Existe un derecho de las partes de consultar las actuaciones surtidas en el proceso, derecho que se cumple cuando se consulta personalmente el medio físico del expediente, o cuando se consulta por medios electrónicos, siempre que estas anotaciones tengan equivalencia funcional. Así, es claro que una de las obligaciones propias de los abogados que actúan como apoderados en un proceso, es estar al tanto de las actuaciones judiciales que se generen en el mismo, para así poder intervenir de manera oportuna en defensa de los intereses de sus representados.

En el caso venezolano, la Sala Constitucional del Tribunal Supremo de Justicia, en el año 2006, partió del criterio de que el acceso directo a las actas procesales es indispensable para la obtención de certeza de lo que ocurre en juicio y para que, en consecuencia, la defensa sea con conocimiento de causa. A este respecto, no puede equipararse el acceso físico de las actas con la consulta de actuaciones en el Juris 2000, porque el expediente da fe de lo ocurrido en una causa particular, sin poder afirmarse lo mismo del sistema informático<sup>79</sup>.

Este pronunciamiento dejó de un lado la equivalencia funcional de la consulta electrónica de actuaciones judiciales del Juris 2000 respecto al físico del expediente, ya que por opinión de la Sala, no cumplen con los requisitos formales establecidos en la Ley de Mensajes de Datos y Firmas Electrónicas, como el de la firma electrónica asociada al mensaje de datos y la constancia por escrito de este.

---

<sup>79</sup> Tribunal Supremo Justicia. Sala Constitucional. Exp N° 04-3055 de fecha 21 de marzo de 2006. (Caso: Alida Teresa Pernaleté Gásperi vs. Coordinadora del Circuito de Protección del Niño y del Adolescente del Estado Lara) Disponible en: <http://www.tsj.gov.ve>. (fecha de consulta: 15/05/2010)

Ahora bien, el artículo 2 de la Ley de Mensajes de Datos y Firmas Electrónicas define el mensaje de datos como “*la información inteligible en formato electrónico o similar que puede ser almacenada o intercambiada por cualquier medio*”.

Tal consideración legal, permite inferir que el historial de los procesos registrados en los hardwares dispuestos para el efecto en las Sedes Judiciales de Venezuela, tiene el carácter de un “mensaje de datos” y así lo ha dejado sentado en el año 2010 la misma Sala Constitucional cuando señala:

*“Se aparta del criterio sostenido respecto a la validez de los datos extraídos del Sistema Juris 2000, y a partir del presente fallo establece con carácter vinculante que las decisiones judiciales obtenidas a través del aludido sistema -actual sistema informático del Poder Judicial- serán consideradas copias simples conforme al artículo 429 del Código de Procedimiento Civil, a los efectos de la interposición de acciones de amparos constitucionales contra sentencias”<sup>80</sup>*

Esta premisa la hace, refiriendo que es evidente que los órganos jurisdiccionales tendrán la oportunidad de constatar, de oficio o a instancia de parte, la veracidad del documento consignado a los efectos de la admisión, con lo cual se cumple el requerimiento de cotejo que alude el artículo 8 la Ley de Mensajes de Datos y Firmas Electrónicas, es decir, se asume que la data almacenada en el Juris 2000 es, ciertamente, un mensaje de dato.

Sin embargo, aún cuando no cabe duda que la información que aparece registrada en los computadores de los juzgados tiene la cualidad de un

---

<sup>80</sup> Tribunal Supremo de Justicia. Sala Constitucional. Exp. 10-0224 de fecha 09 de julio de 2010. (Caso: acción de amparo constitucional interpuesta por el ciudadano Edson Alejandro Rojas Rivas). Disponible en: <http://www.tsj.gov.ve>. (fecha de consulta: 23/08/2010)

mensaje de datos, se debe evaluar, el carácter oficial de los datos registrados, la equivalencia del mensaje de datos con los documentos escritos, su finalidad y la responsabilidad de los servidores encargados de alimentar el sistema.

La equivalencia funcional del registro electrónico y del físico del expediente se verá satisfecha cuando se cumplan las condiciones de tratamiento del mensaje de dato. Al respecto, la exposición de motivos de la Ley de Mensaje de Datos y Firmas Electrónicas ha referido que en esta nueva modalidad de relación (transmisión y recepción de información) hace falta establecer dos elementos principales: la identificación de las partes y la integridad del documento, elementos de los cuales se derivan responsabilidades (civil, penal, patrimonial, disciplinaria, administrativa, fiscal, entre otras).<sup>81</sup>

Estos elementos serán materializados con la emisión de los certificados electrónicos, pudiéndose identificar a las personas y/u organizaciones, lo que se convertirá en documentos de identidad que contienen información importante con respecto a su portador, por ejemplo: nombre, fecha de nacimiento o constitución y dirección. Además, contienen el dato más importante para la identificación de la persona natural o jurídica: La clave pública de su signatario. La función de esta clave es establecer un parámetro técnico que permita darle seguridad a una información y el acceso a ella cuando sea necesario o deseado, y así lo ha dejado establecido SUSCERTE en su estudio sobre La Identidad Electrónica.<sup>82</sup>

---

<sup>81</sup> Salcedo C, Juvenal. *La prueba Documental*. Departamento de Publicaciones de la Facultad De Ciencias Jurídicas y Políticas de la Universidad Central de Venezuela. Caracas, 2006, p.450

<sup>82</sup> Hernández, R; Berrios, Kranya y González, Víctor. *Identidad Electrónica...ob. cit.*

La materialización del certificado electrónico en la Administración Judicial, generará esquemas de confianza en los procesos de registro del sistema, tal cual como si se tratara del físico del expediente.

La segunda necesidad que surge del certificado electrónico en el ámbito judicial, parte de las notificaciones electrónicas previstas en algunas leyes especiales de nuestro país, y cuya práctica ha sido retardada en algunos casos, o no se ha aplicado debidamente en otros. Para utilizar el correo electrónico como mecanismo de citación o notificación en la función jurisdiccional, son necesarios sistemas de seguridad que acrediten fiabilidad de la información contenida en la citación o notificación electrónica. Bajo esta consideración, Díaz, prevé que:

*“...El uso del correo electrónico en comunicaciones oficiales, en donde están en juego derechos fundamentales, como son las judiciales, éstas deberían estar sometidas a unas condiciones especiales de seguridad, como las que ofrece las entidades certificadoras de firmas digitales: los llamados **FEDATARIOS JUDICIALES**. El afán de estar a tono con el uso de las TIC's en los procedimientos judiciales no puede ser excusa para legitimar el uso, de métodos no confiables, sin considerarlas consecuencias que generan sistemas que no garantizan seguridad en la transferencia de datos...”*<sup>83</sup>

De lo citado, se deduce que para la seguridad procesal, se requiere la implementación de la certificación electrónica. Usando este mecanismo técnico de seguridad, se podrá garantizar que las comunicaciones sean conocidas sólo por las partes interesadas (Confidencialidad); que exista la seguridad de confirmar la identidad del emisor (Autenticidad); que las comunicaciones no sean alteradas en el camino (Integridad) y la forma en la

---

<sup>83</sup> Díaz G, Alexander. *Las Notificaciones Electrónicas Judiciales en Colombia. El notario Electrónico (firmado electrónicamente)*, Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento N° 2. Mayo-Agosto 2008, p.132

que se haya generado, archivado o comunicado el mensaje y la forma en que se haya conservado la integridad de la información (confiabilidad).

En el Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas se establece el reconocimiento jurídico de los mensajes de datos, siempre y cuando se cumplan los parámetros que establece este mismo Decreto Ley. Pero el obstáculo es que en el Decreto se prevé la firma digital, cuyo certificado es suministrado por un proveedor de certificados electrónicos adscrito a la Superintendencia, que es el ente rector en esta materia; no obstante, los servidores de las Sedes Judiciales no están provistos de estos certificados electrónicos. Pero si existiese el sistema de firma digital desarrollado y aplicado como lo establece el Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas, la situación sería diferente, porque la tecnología de firma electrónica digital, garantiza los sistemas de seguridad necesarios, así como el seguimiento de la transmisión del mensaje de datos hasta su lectura.

Pero además, de lo referido, las actuaciones judiciales pudieran estar debidamente certificadas por un proveedor de servicios y otorgar a través de la firma digital, fe pública a los registros del Sistema Juris 2000, considerando que este carácter le es otorgado, cuando la impresión de los archivos digitalizados es previamente firmado por la autoridades judiciales (juez y secretario). El artículo 8 de la Resolución N° 70 mediante la cual se ordena crear progresivamente la estructura organizativa y funcional del Sistema Integral de Gestión, Decisión y Documentación JURIS 2000 establece:

*“Artículo 8. Los Jueces que integran los Circuitos Judiciales en cada Circunscripción Judicial individualmente llevarán un Libro Diario y un Copiador de Sentencia. En el Libro Diario se asentarán todas las actuaciones procesales, administrativas y de cualquier otra índole, realizadas diariamente por el*

*Juez en dicha materia, durante el horario de labores. Del mismo modo, los asientos de las actuaciones del Libro Diario se realizarán a través de la actuación de la impresión de los archivos digitalizados, contenidos en JURIS 2000, que deberán compilarse en Tomos, bajo serie numérica, con la debida firma del Juez y del Secretario con el respectivo sello del Tribunal, el cual además deberá contener nota de apertura y cierre.*

***Parágrafo único: Los reportes de los registros que suministra el Sistema JURIS 2000 no darán fe pública si no están refrendados con la firma del Juez, del secretario o de ambos, según los requerimientos de Ley.*** (Negritas Propias)

Si se considera que La información electrónica contenida en medios informáticos pertenece al género de los documentos, tal y como lo establece la Ley de Mensaje de Datos y Firmas Electrónicas en su artículo 2, entonces vale la pena determinar que para que se evalúe con carácter de instrumento público, debe cumplir con las formalidades del artículo 1357 del Código Civil venezolano vigente que señala: *“El instrumento público o autentico es el que ha sido autorizado con las solemnidades legales por un Registrador, por un Juez u otro funcionario o empleado público que tenga facultad para darle fe pública, en el lugar donde el instrumento se haya autorizado”*<sup>84</sup>

Considerando tal aseveración, Oxana y Betancourt, en estudio realizado sobre la validez de los contratos electrónicos del año 2008, han revelado que:

*“Se ha aceptado que los documentos electrónicos tendrán valor de “instrumentos públicos y privados”, con lo cual, entendemos, se estaría admitiendo que, según el autor del documento electrónico, éste podría ser un instrumento público o privado...En atención al necesario contenido formal del instrumento público, la doctrina se ha inclinado por señalar que tales documentos constituyen prueba documental privada...**Como única excepción, se admite que a***

---

<sup>84</sup> Código Civil de Venezuela. Gaceta Oficial N° 2.990 de fecha 26 de julio de 1982.

***través de una autoridad pública de certificación (federatario electrónico) podría otorgársele fe pública a los documentos electrónicos***.<sup>85</sup>  
(Resaltado en negritas de la autora)

A los efectos de precisar lo anterior, es necesario distinguir los términos autenticidad y fe pública, ya que todo documento público es autentico, pero no todo documento autentico tiene fe pública y ello dependerá de las facultades que revista el funcionario que lo conforme. Así lo ha afirmado el profesor Hernández al señalar:

*“El desarrollo del concepto de fe pública nos ha servido para distinguirla de la autenticidad, al observar que el ordenamiento jurídico determina tal facultad, la de imprimir fe pública a ciertos y determinados funcionarios públicos por disposición del artículo 1.357 del Código Civil, tales como el Registrador y los Jueces...se les da la facultad única y exclusivamente de insuflar autenticidad a sus actos cuando se les permite documentarlos...”*<sup>86</sup>

Por su parte, la Ley de Mensaje de Datos y Firmas Electrónicas cuando define la firma electrónica, lo hace atendiendo a 3 elementos de relevancia como: a) es una información creada o utilizada por el creador o emisor del mensaje de datos; b) debe estar asociada al mensaje de datos y por lo tanto debe formar parte de su contenido y c) determina la autoría del mensaje de datos. De manera que, al funcionario judicial (juez) ampliamente facultado para dar fe a una actuación judicial según la normativa legal del 1.357 del Código Civil, al refrendar un documento electrónico mediante la firma digital, además de ser partícipe de la formación del mensaje de datos, este será

---

<sup>85</sup> Oxana. Lidia y Betancourt, Ricardo. Contrato Solemne. ¿Electrónicos? AR: Revista de Derecho Informático, ISSN 1681-5726, N°. 117, 2008. [Documento en línea]. Disponible en: <http://www.alfa-redi.org>.(fecha de consulta: 21/11/2010)

<sup>86</sup> Hernández, M, Luis A. *La Autenticidad Proveniente de los Particulares sin Intervención de Funcionario Público* Revista de Derecho Probatorio N° 5, cuyo director es el Dr. Jesús Eduardo Cabrea Romero, Editorial Jurídica Alva, S.R.L., Caracas. 1995, P. 307.

avalado por la autoridad de certificación electrónica, quien es la responsable de autenticar la fidelidad de dicha firma. Elementos que logran satisfacer las exigencias de contenido del documento público.

De hacerse posible la certificación electrónica en los registros del Sistema automatizado Juris 2000, podría equipararse el acceso físico de las actas con la consulta de actuaciones electrónicas, ya que las actuaciones estarán refrendadas por el sistema de la firma digital, la cual le otorgará fe pública a través de un Proveedor de Servicios de Certificación (PSC) como la Fundación Instituto de Ingeniería para Investigación y Desarrollo Tecnológico (FII) y PROCERT<sup>87</sup>.

La violación de derechos fundamentales como el debido proceso se constituye, cuando se niega toda relevancia de los errores registrados en la información suministrada por la administración de justicia en su sistema automatizado de gestión. Errores, limitaciones o deficiencias de un sistema que de agotarse los recursos tecnológicos de la certificación electrónica pudiera incluso ahorrar costos al Estado en papel si se avanza a un expediente electrónico.

Otras necesidades de la implementación de la certificación electrónica que se pueden sumar a los ya aportados, son los expuestos por Peñaranda en su trabajo sobre *“La Firma Digital en Venezuela”*<sup>88</sup>, destacando los siguientes:

---

<sup>87</sup> Únicos Proveedores de Servicios de Certificación Electrónica (PSC) acreditados por la Autoridad Certificadora Raíz del Estado Venezolano con capacidad para emitir certificados a la Administración Pública y al Sector Privado. Disponible en: [www.SUSCERTE.gob.ve](http://www.SUSCERTE.gob.ve)

<sup>88</sup> Peñaranda Q, Héctor R. *La Firma Electrónica Digital en Venezuela*. Nómadas. Revista Crítica de Ciencias Sociales y Jurídicas | 29 (2011.1). Universidad del Zulia.

1. Las comunicaciones que realizan los tribunales hacia otros tribunales que se encuentran fuera de la circunscripción judicial, o hacia aquellos organismos públicos ubicados en otros Estados, podrían ser agilizadas mediante el uso de la informática.

Por ejemplo si en Venezuela un juez ordena una prohibición de enajenar y gravar un inmueble ubicado en otro Estado. Previo el cumplimiento de los requisitos de las medidas cautelares, dicho juez podría oficiar directamente al Registro de la propiedad del inmueble enviando la orden de la mencionada prohibición mediante correo electrónico, con el sistema de la firma digital. Lo que traería consecuencias positivas respecto a la celeridad en el tiempo, costos y gastos del proceso.

2. Notificar medidas a organismos de otros Estados, como un registro de la propiedad inmobiliaria, de automotor o de registro público de comercio, donde las comunicaciones tienen una gran importancia en lo que se refiere a la eficacia de medidas cautelares. Estas medidas en muchos casos deben ser efectuadas con celeridad para evitar que se tornen ilusorios los derechos de los peticionantes.

En este sentido el Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas de Venezuela determina en su artículo 3 que “El Estado adoptará las medidas que fueren necesarias para que los organismos públicos puedan desarrollar sus funciones, utilizando los mecanismos descritos en este Decreto-Ley”.

### **3.7 Impulsos del Estado para implementación de la Firma Electrónica y La Certificación Técnica en la Administración de Justicia venezolana.-**

La Información que será expuesta en este punto, ha sido recabada principalmente de documentos y sitios Web oficiales del Estado como el portal electrónico del Tribunal Supremo de Justicia, SUSCERTE y la Memoria y cuenta 2004 del entonces Ministerio de Ciencia y Tecnología, ahora Ministerio del Poder Popular para Ciencia, Tecnología e Innovación.

La exposición de Motivos de la Ley de Mensajes y Firmas Electrónicas ha señalado que:

*“...El Decreto-Ley hace especial mención al Estado para que utilice los mecanismos pertinentes previstos en él...Esto incidirá determinadamente en la automatización de los procesos, la calidad de los servicios públicos, en el ahorro de recursos informáticos y presupuestarios y una mayor transparencia de la gestión de los organismos del Estado...”<sup>89</sup>*

El artículo 35 de la Resolución N° 70 que ordena la implantación progresiva del Sistema de Gestión Decisión y Documentación Juris 2000, ha referido también que:

*“A los efectos d realizar las notificaciones y demás actos de comunicación, las oficinas mencionadas en la presente Resolución, podrán utilizar, una vez que estos estén debidamente implementados, los mecanismos que señala el Decreto con Rango y Fuerza de Ley N° 1204 de fecha 10 de febrero de 2001, de Mensaje de Datos y Firmas Electrónicas publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148 del 28 de febrero de 2001”.*

---

<sup>89</sup> Salcedo C, Juvenal. *La prueba Documental...* ob. cit, p.453

Ahora bien, aún cuando la implantación del Sistema automatizado Juris 2000 se hizo posible a partir del año 2002, se trata de un proyecto desarrollado desde 1993, anterior al año de promulgación de la Ley de Mensaje de Datos y Firma Electrónicas del 2001. Sin embargo, El 26 de abril de 2004 fue firmado un Convenio de Cooperación Interinstitucional entre el Poder Judicial y el Ministerio de Ciencia y Tecnología. La SUSCERTE y la Dirección Ejecutiva de la Magistratura, órgano auxiliar del Tribunal Supremo de Justicia, encargado de la administración del Poder Judicial, eran los responsables de ejecutar el convenio, el cual tenía como objeto la implantación de servicios de certificación electrónica en el proceso de modernización del Estado y agilización de trámites por medios electrónicos en el Poder Judicial.

Dr. Ricardo Jiménez Dan, Gerente de Informática y Telecomunicaciones del Tribunal Supremo de Justicia declaró en el año 2004 que:

*“...Para que los ciudadanos entiendan lo que significa la firma del convenio al corto plazo, es que los tribunales pudieran estar usando certificados de firmas electrónicas para notificar y realizar diferentes actuaciones, lo cual pudiera abrir las puertas para lo que se llame la diligencia judicial electrónica, para los trámites judiciales el línea, se pudieran estar abriendo las puertas para lo que pudiera ser el litigio electrónico, lo cual no es más que una plataforma legal y tecnológica que permita a los abogados y a las partes interactuar con los órganos jurisdiccionales mediante el empleo de tecnologías de la información y la comunicación que permitan hacer mucho más simples, cómodos y seguros, por qué no, de cierta forma, los trámites entre las partes y los diferentes actores del sistema de justicia... Estamos hablando de un proceso pionero de aplicación de tecnologías de seguridad en trámites judiciales, haciendo en cierta forma, letra viva y vigente todo un ordenamiento jurídico que el Estado venezolano desde el año dos mil con la Ley de Telecomunicaciones, la Ley de Servicios de Certificación de Mensajes de Datos y*

*Certificados Electrónicos y la Ley de Delitos Informáticos*<sup>90</sup>

Por su parte la entonces ministra de Ciencia y Tecnología, Marlene Yadira Córdova dio a conocer lo siguiente:

*“...Esto tiene repercusiones importantísimas porque va a permitir al ciudadano común el poder tener comunicación certificada sobre el avance de sus procesos que se están llevando a través de los tribunales y que le brinda la seguridad de que lo que les es comunicado a través de la Dirección Ejecutiva de la Magistratura tiene detrás una certificación legal...”*<sup>91</sup>

Del portal electrónico del Tribunal Supremo de Justicia se pudo conocer que los antecedentes del Convenio Interinstitucional eran:

*“...Ahorrar espacio en lo referente al Archivo Judicial y reducir el gasto de mantenimiento de un archivo físico, eliminando así las necesidades existentes y futuras de espacios tipo galpón...estudiar la posibilidad de digitalizar expedientes físicos, firmar electrónicamente los mismos, para otorgarle la validez (Ley sobre mensajes de datos y firmas electrónicas) y crear un Proveedor de Servicios de Certificación Electrónica (Propiedad del Poder Judicial)”*.<sup>92</sup>

Sumado a lo anterior, es necesario señalar que de las fuentes examinadas, no fue posible ubicar el número del convenio de Cooperación Interinstitucional celebrado en el año 2004 que colocaría a disposición del servicio de justicia venezolano el certificado electrónico. No obstante, de la

---

<sup>90</sup> Jiménez Dan, Ricardo. *Suscritos Convenios para modernizar y dignificar la justicia en el país*. Sede del Tribunal Supremo de Justicia. 27 de abril de 2004. [Documento en línea]. Disponible en: <http://www.tsj.gov.ve> .(fecha de consulta: 15/05/2010)

<sup>91</sup> Córdova, M. *Suscritos Convenios para modernizar y dignificar la justicia en el país*...op. cit.

<sup>92</sup> Tribunal Supremo de Justicia. *Convenio de Cooperación Interinstitucional entre El Poder Judicial y el Ministerio De Ciencia Y Tecnología*. [Documento en línea]. Disponible en: <http://www.tsj.gov.ve> .(fecha de consulta: 17/06/2010).

Memoria y Cuenta del Ministerio de Ciencia y Tecnología, presentado a la Asamblea Nacional de ese mismo año, se puede observar las intenciones de implantación de la certificación electrónica en la Administración Judicial. Así se tiene que, a través de SUSCERTE:

*“...Se realizaron las asesorías para la implantación de tecnologías de Firma Electrónica y el establecimiento como Proveedores de Servicios de Certificación en importantes organismos del Estado como son el Servicio Nacional Integrado de la Administración Tributaria (SENIAT), **El Tribunal Supremo de Justicia (TSJ), la Dirección Ejecutiva de la Magistratura (DEM), Comisión de Administración de Divisas (CADIVI), Banco Central de Venezuela (BCV)...**”<sup>93</sup> (Resaltado en negritas de la autora).*

De una consulta realizada a la página oficial de SUSCERTE ([www.SUSCERTE.gob.ve](http://www.SUSCERTE.gob.ve)), se pudo observar que existen proyectos en ejecución en los que no se encuentra el de la certificación electrónica a disposición de los servicios automatizados del poder judicial. Algunos de estos proyectos son:

*a. Ministerio del Poder Popular para las Relaciones Exteriores: Uso de los certificados para Autenticación y firmas electrónicas en documentos y correo electrónico.*

*b. Ministerio del Poder Popular para el Trabajo y la Seguridad Social: Firmas para las Solvencias Laborales.*

*c. CNE: Digitalización y Firmas de Documentos.*

*d. Ministerio del Poder Popular para Relaciones Interiores y Justicia: Firmas electrónicas en los Antecedentes Penales.*

*e. SAIME: Firma electrónica para la cédula del ciudadano.*

---

<sup>93</sup> República Bolivariana de Venezuela. Ministerio de Ciencia y Tecnología. Memoria y Cuenta 2004. Caracas. 2005, p.224.

f. *SAREM*: Firma electrónica de documentos generados para la prestación del servicio).

g. *SUDEBAN*: Incorporación del chip con certificado electrónico a las tarjetas de débito y crédito.

h. *Alcaldías y Gobernaciones a nivel nacional*: Solvencias, Permisos y Autorizaciones Firmadas electrónicamente

De lo referido, se concreta que aún bajo la existencia de un sistema normativo (Decreto-Ley de Mensaje de Datos y Firmas Electrónicas) que impulsa la implementación de la firma y la certificación electrónica, el Tribunal Supremo de Justicia y el Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación, mantienen un esfuerzo detenido en un convenio cuya materialización no se ha visto empleada en los servicios automatizados que se presta en los Tribunales del país a través del Juris 2000.

Cabe destacar, que el Estado venezolano, específicamente, el Poder Judicial, no ha establecido una política de desarrollo del tribunal electrónico en cuanto a la implementación de herramientas necesarias para la seguridad de la información judicial que se maneja en sus sistemas automatizados.

## CAPITULO IV. PRAXIS DE LA SISTEMATIZACIÓN JUDICIAL

### 4.1 La seguridad en el uso de las TIC'S implementadas en la Administración de Justicia de Latinoamérica.-

Desde mediados de los años ochenta la mayoría de los países de América Latina ha emprendido reformas muy significativas, orientadas a transformar sus sistemas de administración de justicia<sup>94</sup>. Parte importante de estos esfuerzos se ha centrado en la sensibilidad de la información jurisdiccional y la creciente importancia de los sistemas de información en la tramitación de los procedimientos judiciales, elementos estos, que inciden en la relevancia de la seguridad de la información. Pero un sistema informático será seguro, según Hernández Orallo, “cuando se pueda confiar en él y se comporte de acuerdo a lo esperado”<sup>95</sup>.

Este mismo autor señala que el término seguridad es muy amplio y comprende distintos aspectos como:

**“Confidencialidad:** la información sólo puede ser accedida por aquel que esté autorizado.

**Integridad:** La información no puede ser eliminada o modificada sin permiso.

**Disponibilidad:** La información tiene que estar disponible siempre que sea necesario, evitando por tanto, ataques externos que puedan reducir esta disponibilidad o incluso una caída del servicio.

**Consistencia:** Hay que asegurar que las operaciones que se realizan sobre la información se comporten de acuerdo a lo esperado. Esto implica que los

---

<sup>94</sup> CEJA, “Reformas Procesales Penales en América Latina: Discusiones Locales”. Disponible en: [http://ceja.cl/portal/index.php/es/biblioteca/biblioteca-virtual/doc\\_details/3320-reformas-procesales-penales-en-america-latina-discusiones-locales](http://ceja.cl/portal/index.php/es/biblioteca/biblioteca-virtual/doc_details/3320-reformas-procesales-penales-en-america-latina-discusiones-locales). (fecha de consulta: 05/03/2011)

<sup>95</sup> Hernández. O, Enrique. *Seguridad y Privacidad en los Sistema Informáticos*. [Documento en línea]. Disponible en: <http://www.disca.upv.es/enheror/pdf/ACTASeguridad.PDF>. (fecha de consulta: 17/08/2010).

*programas realicen correctamente las tareas encomendadas.*

**Control:** *Es importante regular y controlar el acceso a la información de la empresa”.*

De manera que las TIC’S y la seguridad, es un trabajo conjunto que puede ser visto desde dos perspectivas. Por un lado, las condiciones necesarias para aumentar los niveles de seguridad del almacenamiento de datos, dentro de las cuales hay tecnologías (redes de voz y datos con soportes de fibra óptica, por ejemplo) y procedimientos, que son un punto de partida para este fin. Por otro lado, la interrogante acerca de qué tan altos deberían ser los niveles de seguridad requeridos en el almacenamiento de datos relacionados con la administración de justicia.

Al respecto, en el informe de CEJA, sobre *las “Perspectivas de uso e impactos de las TIC en la administración de justicia en América Latina”*<sup>96</sup> se han delineado algunos aspectos relevantes sobre el tema de la seguridad en los sistemas de justicia, destacando los siguientes:

1. *El almacenamiento de datos:* en este punto, las TIC presentan claras y evidentes ventajas que pueden y deben ser aprovechadas. Si se piensa solamente en el deterioro físico que sufre un expediente escrito con el tiempo, y en lo inseguro y costoso que es como medio de almacenamiento de información, ya que su pérdida temporal o permanente supone un grave trastorno del proceso judicial, y su archivo puede significarle a los tribunales de justicia destinar grandes espacios, y su acceso supone que una persona físicamente pueda consultarlo, se entienden las ventajas de contar con

---

<sup>96</sup> Hernández, C. y Adelardi, R. *“Perspectivas de uso e impactos de las TIC en la administración de justicia en América Latina”* (2008). [Documento en línea]. Disponible en: <http://www.cejamericas.org>. (fecha de consulta: 26/08/2010).

sistemas informáticos que, con los debidos niveles de seguridad, respalden la información de los casos judiciales, la almacenen en dispositivos electrónicos y la tenga disponible para quien sea necesario, de acuerdo a las definiciones que se hagan.

Si fuera estrictamente necesario guardar algún tipo de documentación en papel, las TIC también ofrecen posibilidades de tener sistemas de seguimiento documental, los que combinados con la tradicional tecnologías de códigos de barra o moderna tecnología en los documentos deseados, permiten saber en línea en qué lugar exacto está cada documento. Para que esto pueda operar, las dificultades no son técnicas, sino que vienen por el lado de la disciplina de los usuarios para registrar cada movimiento de los documentos.

*2. Disponibilidad de aplicaciones informáticas:* este es un elemento que puede tener una alta incidencia en la confianza que los usuarios tengan en relación a las TIC. Las aplicaciones con las que se cuenta tienen que ser percibidas como que están siempre operativas y disponibles, sin caídas, suspensiones del servicio o altos tiempos de respuesta que hagan inviable en la práctica su uso. Esto tiene por consecuencia la necesidad de fijar objetivos de disponibilidad con las áreas técnicas correspondientes, lo que trae asociado a su vez el establecimiento de políticas de operación, de mantenimiento y de soporte a usuarios.

*3. Búsqueda de datos:* en relación a este elemento, existe un serio problema en la desactualización de datos, en carencias en la alimentación de datos a los sistemas informáticos e, incluso en el falseamiento de datos. Son diversas las causas que pueden explicar estos problemas tales como el no

entendimiento en los usuarios de los sistemas informáticos del daño que su acción genera, o probablemente que el diseño de los sistemas es inadecuado y los usuarios tienen la percepción que el ingresar datos les hace perder tiempo, o bien en carencias en las labores de control de la calidad de los datos. Cualquiera sea el motivo, la situación es un problema, pero su solución probablemente tiene más que ver con la capacitación de los usuarios que con el desarrollo de las TIC.

Adicionalmente los sistemas correctamente desarrollados permiten su propio monitoreo y procesos de auditoría, para de esa manera identificar si alguien ha accedido, borrado o alterado algún dato.

En este sentido, ha resultado imprescindible la modernización del sistema judicial latinoamericano y la incorporación de las nuevas tecnologías de información y comunicación, que posibiliten a los habitantes de estos países de América un acceso rápido, igualitario y eficiente a la justicia. Deberá propenderse que dichos mecanismos y plataforma informática tenga características similares y con la simplificación necesaria para garantizar el uso y transferencia fidedigna de la información que contienen. La organización y gestión del despacho judicial, la digitalización de los procesos, la administración de la oficina judicial, entre otros aspectos, son un instrumento esencial para lograr un servicio judicial moderno, eficiente y oportuno. Los poderes judiciales de estos países habrán de desarrollar los mecanismos y acciones de cooperación que permitan eficazmente esos objetivos de un modo armónico, sostenido, progresivo e integrador, con una amplia discusión e inclusión de todos los operadores e involucrados.

En un panorama más reflexivo, los jueces y magistrados de diecinueve países de América del Sur, Centro América, México y el Caribe, miembros de la Red Latinoamericana de Jueces, reunidos en la ciudad de Fortaleza, Brasil, con motivo del III Congreso Iberoamericano de Cooperación Judicial: *Sociedad del Conocimiento y Derechos Humanos*, realizaron las siguientes consideraciones<sup>97</sup>:

1. Se procurará que los organismos judiciales permitan activamente, por medios digitales y públicos, en sitios electrónicos, que los usuarios y operadores del sistema reciban las informaciones contenidas en actas y procesos jurisdiccionales, así como los datos de los órganos y operadores del sistema que tengan incidencia en ese ámbito; a la vez que se implementen mecanismos de consulta particular por vías idóneas, rápidas y seguras. Deberá resguardarse los principios de la transparencia, máxima divulgación, facilitación de derechos, con responsabilidad y gratuidad.

2. La plataforma informática, digital y comunicacional, así como la transparencia de los procesos judiciales y datos contenidos en ellos, es la base para la creación de un espacio jurisdiccional latinoamericano ético que permita internamente en cada Estado el acceso a la justicia, la igualdad entre los habitantes, su seguridad y la efectividad de los derechos fundamentales y la participación de los ciudadanos. En el plano internacional, la modernización y transparencia procurará existan mecanismos de validación de los actos judiciales que sean eficientes y directos entre los órganos, libres de burocracia y razonablemente accesibles. En esta perspectiva, es necesario reducir los vacíos del espacio jurisdiccional interamericano,

---

<sup>97</sup> Processo Eletrônico. *Cooperação Internacional*. Carta de Fortaleza, Brasil. A Red Latinoamericana de Jueces - Redejal - editou. [Documento en Línea]. Disponible en: <http://www.processoeletronico.com.br/page4.aspx>. (fecha de consulta: 19/05/2012).

extendiendo al ámbito interno los mecanismos informales y electrónicos de cooperación judicial.

3. Consideran que el respeto a los derechos fundamentales supone que las nuevas tecnologías y la difusión judicial resguarden la intimidad, como la privacidad de las personas, y reiteramos que en el ámbito físico o virtual del trabajo, se debe garantizar la dignidad, privacidad y confidencialidad de los datos y comunicaciones que por su naturaleza son de índole estrictamente privado, inclusive al operar los medios tecnológicos dispuestos por aquel a quien se debe subordinación y dependencia, habida cuenta de la necesaria protección del teletrabajo y de los derechos sociales y colectivos.

4. Advierten que todos los avances tecnológicos que permiten la administración de una justicia más eficiente y transparente, pueden resultar ineficaces, si no se tiene un judiciary independiente tanto interna como externamente, con plena libertad y según las garantías que se consagran a nivel constitucional, y que están aceptadas en el ámbito democrático contemporáneo.

6. En conclusión, se trata de generar un espacio moderno y transparente en el ámbito judicial latinoamericano que, respetando los derechos fundamentales del ser humano, permita la existencia de una justicia autónoma, eficiente y eficaz, cercana a sus destinatarios y ampliamente comprensiva de las diferencias culturales de nuestras naciones.

Ahora bien, la fórmula para alcanzar varios de los planteamientos citados, se ha encontrado en los avances tecnológicos de la firma electrónica y los proveedores de servicios de certificación. Herramientas de seguridad

tecnológica adoptadas en el contexto de algunos países Latinoamericanos, en las buenas prácticas de una modernización de justicia electrónica. Al respecto, considerando como fuente principal el “Informe: Buenas Prácticas en el uso de Nuevas Tecnologías en el Poder Judicial”<sup>98</sup> realizado por CEJA en el año 2010 serán señalados algunos países que han adoptados avances tecnológicos de certificación técnica y firma digital en el proceso judicial.

#### 4.1.1 Brasil.-

El 19 de diciembre de 2006 se aprueba en Brasil la Ley N° 11.419 *Informatização do Processo Judicial*, sobre la informatización del proceso judicial (Ley del Proceso Electrónico). En ella también se recogen importantes aspectos sobre los cuales hoy en día Brasil es referencia a nivel mundial en aspectos como lo son, el software libre y la estandarización o la interoperabilidad, pero también elementos tan relevantes en el ámbito judicial como la credencial electrónica, los plazos procesales cuando intervienen sistemas electrónicos, el proceso electrónico, el acceso a las piezas procesales, la digitalización, conservación de los autos por medio electrónico, entre otros<sup>99</sup>.

Sin duda entre las buenas prácticas de esta Ley y de sus siguientes modificaciones (Resolución n 341/2007, Resolución 357/2007, Resolución 344/2007) han introducido una gran cantidad de innovaciones en el sistema

---

<sup>98</sup> Lillo, L., Ricardo. *Informe: Buenas Prácticas en el uso de Nuevas Tecnologías en el Poder Judicial*. Centro de Estudios de Justicia de las Américas. 2010. [Documento e Línea]. Disponible en: [www.cejamericas.org](http://www.cejamericas.org). (fecha de consulta: 02/11/2011).

<sup>99</sup> Jiménez, Carlos .E. *Interoperabilidad en la administración de justicia: Experiencias y buenas prácticas en un ámbito complejo*. Ponencia presentada en el XV Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública. Disponible en: [http://estratic.files.wordpress.com/2010/12/jimenez\\_io\\_justicia.pdf](http://estratic.files.wordpress.com/2010/12/jimenez_io_justicia.pdf). (fecha de consulta: 17/08/2010).

jurisdiccional brasileiro en el uso de las tecnologías entre las que se mencionan<sup>100</sup>:

1. La creación del Diario de Justicia Electrónico (Abril 2007 - Ley 11419/06).

2. El uso de certificación digital, autenticidad integridad e interoperabilidad de los documentos electrónicos asignados con certificados digitales emitidos para la infraestructura de Llaves públicas Brasileñas – ICP.

3. El Recurso Extraordinario Electrónico, conocido como RE electrónico para el traspaso de material probatorio al Supremo Tribunal Federal (objetivo de reducir marcadamente el número de material en papel que llega a los Tribunales). Desde el 2007 está funcionando regularmente el e-Pet, servicio que permite la petición electrónica de todo tipo de documentos en los Tribunales.

4. La citación electrónica prevista por el Código Civil bajo dos condiciones: a) previa registración de los usuarios en el Portal del Poder Judicial ("*credenciamento no Poder Judiciário*"), b) acceso para entrega de los actos por parte de la persona citada.

5. En el Proceso Electrónico todas las Citaciones deben ser hechas por medio electrónico, cuando no sea posible deberá ser realizada según las

---

<sup>100</sup> Jacopo Gamba. *Panorama del derecho informático en América Latina y el Caribe*. Comisión Económica para América Latina y el Caribe (CEPAL). Colección Documentos de proyectos. 2010, pp. 37-38

reglas ordinarias, a través de la digitalización del documento físico que será posteriormente destruido (para ahorro de papel y menor gasto de justicia).

6. Iniciación electrónica (acto con el cual se deja saber a alguien que tiene que dejar de hacer una cosa o que tiene que empezar a hacerla).

Cada tribunal tiene su sitio web para proveer servicios al público. El servicio de “Acompañamiento procesal” corresponde a un sistema online de seguimiento de demandas que permite a cualquier usuario obtener la información actualizada de cualquier caso, requiriendo el uso de alguna de estas tres formas de obtener acceso: el número de registro del abogado asociado al colegio de abogados, el nombre de uno de los litigantes, o buscando el número de la demanda en sí misma. El sistema “Push” permite a los usuarios especificar que casos quieren seguir y registrarse para recibir actualizaciones automáticas vía email.

Los usuarios pueden ingresar en un sistema de manejo de causas donde asuntos administrativos relativos a la presentación y participación en una demanda pueden ser realizados en línea.

Brasil ha realizado un esfuerzo concentrado en construir una base de datos pública que pueda facilitar las referencias cruzadas de información pública obtenida de varias agencias gubernamentales. Aunque un sistema que global no se encuentra actualmente en operación, Brasil ha integrado las bases de datos del Banco Central de Brasil, del Departamento Nacional de Tránsito, y de la Secretaría de Renta Federal con el Poder Judicial, permitiendo la implementación en línea de todo tipo de actuaciones de secuestros.

Los sitios de los poderes judiciales locales también proveen acceso a bases de datos jurisprudenciales. Adicionalmente, boletines de jurisprudencia son periódicamente publicados con las opiniones de la corte en distintas materias.

Además de ello, aunque no es común, algunas cortes envían información actualizada acerca de causas a teléfonos móviles. Una Corte federal permite argumentación oral a través de videoconferencia, y algunas cortes ofrecen un servicio de comunicación a través de *podcast* en el cual informan al público acerca de las tendencias jurisprudenciales e innovaciones legislativas. Finalmente, una Corte en materias laborales transmite sus audiencias a través de internet.

#### 4.1.2 Perú.-

Un caso destacable en América Latina es el Cibertribunal peruano, órgano para la resolución de conflictos originados en el uso de Internet. El Cibertribunal peruano “*es un órgano de resolución de conflictos y controversias ocurridas en y por el uso de Internet que fomenta la Conciliación entre las partes y el Arbitraje como medio de resolución de conflictos y es competente en temas de Derecho Informático*”.<sup>101</sup> Es un Centro de Conciliación acreditado por el Ministerio de Justicia y Centro de Resolución de Controversias entre nombres de dominio y marcas. El procedimiento está previsto como sigue: una vez presentada la solicitud de arbitraje, el Cibertribunal peruano operará como un Centro de Arbitraje entre las partes. La comunicación entre los representantes del Cibertribunal peruano se desarrollará mediante correo electrónico. Las audiencias de

---

<sup>101</sup> [Documento e Línea]. Disponible en: <http://www.cibertribunalperuano.org>.

arbitraje se realizarán utilizando en algunos casos el correo electrónico y en otros se aplicarán sesiones de *chat* y de vídeo conferencia entre las partes en conflicto y el Tribunal, así como entre los Vocales del Tribunal. Se usarán sistemas de encriptación que asegurarán la confidencialidad de las comunicaciones. Si la solicitud de arbitraje es presentada por una sola parte, se publica en la Página Web del Cibertribunal una reseña de la solicitud o demanda para alentar la respuesta de la contraparte. Finalizado el caso, se publica en la Página Web del Cibertribunal peruano un resumen de la resolución únicamente con el fin de crear precedentes.

#### *4.1.3 Costa Rica.-*

En el año 2000 el Poder Judicial de Costa Rica inicia este proyecto de automatización de los despachos judiciales, incluyendo sistemas de apoyo para la tramitación y gestión de los mismos, Sistemas para la Recepción de Documentos y Sistemas Automatizados de Notificaciones.

A la fecha la automatización se ha ido expandiendo a nivel nacional, y se cuenta con 254 despachos a lo largo del país bajo la implementación del proyecto, de esta manera, aproximadamente el 70% del flujo de casos del país se tramita utilizando nuevas tecnologías. Dichas herramientas cubren todas las materias e instancias incluyendo las Salas de Corte Suprema de Justicia.

En el año 2008, el reto fue más allá con la implementación de Tribunales electrónicos o "cero papel" para lo que se estableció un proyecto con los siguientes objetivos:

a. Disminuir el uso de papel y de suministros de oficina utilizados en la producción de sentencias, resoluciones y escritos.

b. Disminuir el tiempo de respuesta al usuario en la tramitación de sus procesos.

c. Incorporar la Tecnología en la gestión de los despachos judiciales, de forma tal que se facilite la tramitación y gestión de causas de forma completamente electrónica.

d. Incorporar la oralidad en los procesos y en el expediente electrónico.

e. Conformar la causa de forma completamente electrónica, permitiendo el acceso a las mismas mediante Internet.

f. Brindar facilidades a los usuarios que permitan el litigio electrónico, iniciando con la presentación de demandas y presentación de otros escritos a través de Internet.

g. Acceso a la justicia 24 horas al día 7 días a la semana.

Actualmente en el seguimiento de los Juzgados de Cobros se están implementando los procesos completamente electrónicos, de esta forma las causas que ingresan por la página web pasan directamente a la tramitación y las causas que presentan en papel se digitalizan y pasan al trámite electrónico.

Desde el punto de vista de Tecnología de la información se aprovecharon al 100% los esfuerzos ya realizados en automatización de despachos judiciales y se desarrollan herramientas complementarias, integradas a las ya existentes que apoyen la tramitación y gestión electrónica por parte de los usuarios externos (por medio del sistema de GESTION EN LINEA) y los usuarios internos (por medio del Escritorio Virtual).

Ahora, el Poder Judicial cuenta con una SUITE de soluciones integradas que permite la implantación de los Tribunales electrónicos "cero papel", la cual incluye:

1. Sistema Costarricense de Gestión de Despachos Judiciales (apoya la tramitación en el despacho judicial).

2. Sistema Automatizado de Notificaciones. (Incluye las notificaciones electrónicas).

3. Sistema de Recepción y Distribución de Documentos (físicos y electrónicos).

4. Escritorio Virtual (incluye la firma electrónica de las resoluciones, sentencias y oficios), así como la gestión del escritorio).

5. Agenda única. (gestión de los recursos compartidos en un acto procesal, defensores, fiscales, salas, Jueces).

6. Sistema de Mensajería Judicial (Permite el envío de mensajes SMS y correo electrónicos a los usuarios).

7. Sistema de Gestión en Línea (Permite la consulta en línea de las causas, presentación de demandas y escritos por internet).

8. Sistema para la generación de la estadística Judicial (data warehouse).

#### *4.1.4 Argentina.-*

El concepto de firma digital, y el desarrollo de su infraestructura han sido cuestiones de constante interés por parte del Consejo de la Magistratura de la Nación de la República Argentina. Es así que ya en el año 2001 y a través



los tribunales inferiores de la Nación, y de ellos entre sí. Se inicia con una masa de mil usuarios, para extenderse gradualmente.

*Etapas 2:* La utilización de la Firma Digital en las comunicaciones realizadas entre todos los operadores judiciales.

*Etapas 3:* Apertura en el uso de la firma digital al ámbito jurisdiccional correspondiente, utilizando las “cadenas de confianza” que la propia firma digital otorga.

Para la primera etapa de implementación, que comprende exclusivamente áreas internas del Poder Judicial, se propone la asignación de las funciones propias de la infraestructura de firma digital, a distintas oficinas del Consejo, lo cual permitirá adquirir experiencia en la materia, y controlar todas las instancias del proceso.

#### **4.2 Mecanismos de validación, seguridad y registro de actuaciones del Juris 2000.-**

Los detalles de seguridad relativos a la información judicial del sistema automatizado Juris 2000, son tomados de la tesis de grado del Licenciado Luis Eduardo Torres Zamora, el cual tiene como título “*Análisis de Riesgos y Medidas de Seguridad para el Sistema de Jurisprudencia del Poder Judicial Venezolano (Juris 2000)*”<sup>103</sup>, considerando el estudio práctico que enfoca a la seguridad implementada en el sistema de gestión judicial.

---

<sup>103</sup> Torres Z, Luis E. “*Análisis de Riesgos y Medidas de Seguridad para el Sistema de Jurisprudencia del Poder Judicial Venezolano (Juris 2000)*”. Trabajo de Grado. Universidad Central de Venezuela. Junio 2002

Cada uno de los departamentos de las Sedes Judiciales cuenta con un área de trabajo en los servidores, la cual tiene como finalidad almacenar la información que se considere importante proteger. A estas áreas solo tienen acceso funcionarios de la Oficina de Apoyo Informático, con previa autenticación y control por el servidor. El proceso de backup de estas áreas es planificado por el administrador de redes, realizándose una vez a la semana un respaldo completo y el resto de la semana un backup incremental. En las estaciones de trabajo no se realiza un proceso planificado de respaldo y sólo personas específicas establecidas por la organización cuentan con este servicio.

Es importante destacar que las prácticas de seguridad establecidas actualmente en la Oficina de Apoyo Informático (actualmente Oficina de Desarrollo Informático) no se encuentran documentadas, ni existen manuales que describan los procesos principales de éstas. A su vez, no se ha desarrollado una política de seguridad a seguir por el organismo, que sirva como base para la implementación y configuración de la red local. Las medidas existentes, en cuanto a estos aspectos, son resultado de iniciativas independientes previamente autorizadas.

En la estructura de la informática no existe ningún área orientada específicamente a desarrollar y mantener programas y políticas de seguridad de la información. Las responsabilidades en cuanto a la seguridad de la información se comparten entre dos áreas organizacionales: Oficina de Apoyo Informático y la Oficina de Distribución de Expedientes, situación que origina divergencias en la canalización y conducción de las decisiones a seguir en materia de seguridad.

Los estudios realizados en materia de seguridad de la información, se han enfocado principalmente a la protección y seguridad física de los bienes en los que se procesa, almacena o transporta la información manejada por el organismo. Estos se han basado en la implementación de herramientas tecnológicas implantadas a nivel de la red, sin contar con un establecimiento claro y conciso de las políticas de seguridad necesarias para el organismo.

Anteriormente existía el esfuerzo en el organismo por diversas parte de áreas encargadas de la seguridad de la información, pero no se logró establecer y documentar las directrices de protección necesarias para el mismo. Esta área encargada de salvaguardar la integridad, confiabilidad y disponibilidad de la información, estableció y desarrolló algunas normas, que intentaban regular en ciertos aspectos la conducta de los usuarios de la red corporativa, vinculados con el manejo de la información, pero sin llegar a profundizar ampliamente en los aspectos necesarios que harían efectivo un plan de seguridad. Es importante resaltar que desde el momento que se definieron tales normas, hasta la fecha, no han sido difundidas de forma tal que los funcionarios tengan conocimiento al respecto. Los únicos documentos en los cuales se hace referencia a la seguridad de la información manejada por el organismo, son normas emitidas por la Contraloría General de la República (donde el funcionario se responsabiliza por mantener una conducta ética y un trabajo de calidad) y el Acuerdo de Confidencialidad (donde se resume la normativa que sobre confidencialidad regirá entre la organización y el funcionario).

En la investigación se logró detectar un conjunto de debilidades que se mencionan a continuación:

- a. Ausencia de un plan estratégico de seguridad de información

- b. Ausencia de un departamento o personal específicamente encargado de la seguridad de la información.
- c. Deficiencia del plan de contingencia.
- d. Obsolescencia y ausencia de documentación de Sistemas de Seguridad.
- e. Deficiencia en reportes de fallas.

Ahora bien, una vez resumido el panorama de seguridad que enmarca la automatización judicial venezolana, específicamente el Juris 2000, es necesario agregar a las debilidades, la ausencia de *certificación electrónica o técnica en sus actuaciones* y así lo ha dejado establecido la Comisión de Funcionamiento y Reestructuración del Sistema Judicial, al citar el criterio establecido por la Sala Constitucional del Tribunal Supremo de Justicia, en sentencia N° 600 del 20 de marzo de 2006:

*“...No puede equipararse el acceso físico a las actas con la consulta de actuaciones en el JURIS 2000, porque el expediente da fe de lo ocurrido en una causa particular, pero no puede afirmarse lo mismo respecto del sistema informático a que se ha hecho referencia, pues, en primer lugar, sus registros **no cumplen con los requisitos que establecen los artículos 6, único aparte, y 8 de la Ley sobre Mensajes de Datos y Firmas Electrónicas...** Lo anterior no debe entenderse como una descalificación al JURIS 2000, sistema artífice de la modernización de nuestros Tribunales de Justicia, sino como un llamado de atención sobre sus limitaciones”<sup>104</sup> (Resaltado en negritas de la autora).*

---

<sup>104</sup> Tribunal Supremo de Justicia. Sala Plenaria de la Comisión de Funcionamiento y Reestructuración del Sistema Judicial. Exp. N° 1773-PE-2009 de fecha 15 de diciembre del año 2009 (Amonestación a Herman Vásquez Flores, Titular del Juzgado Tercero Superior del Trabajo de la Circunscripción Judicial del Área Metropolitana de Caracas). Disponible en: <http://www.tsj.gov.ve>. (fecha de consulta: 15/05/2010)

Del contenido de la sentencia se desprende que las actuaciones emitidas por el sistema Juris 2000 no contienen la formalidad y solemnidad de la firma electrónica y en consecuencia del certificado electrónico.

Por otra parte, la Dirección Ejecutiva de la Magistratura a través de la Unidad Coordinadora de Proyectos en oficio N° 057-2010 de fecha 29 enero de 2010 ha dejado establecido que: *“El Sistema de Gestión, Decisión y Documentación Juris 2000 implantado en este Circuito Judicial, no posee firmas digitales que certifiquen las actuaciones realizadas”*<sup>105</sup>. De manera que, no se precisa en qué condiciones el mensaje de datos puede ser auténtico, en lo que corresponde a la prueba de su autoría, a la fecha de la ocurrencia de la carga de las actuaciones y, menos está revestido de la presunción legal que establece el artículo 1 de la Ley de Mensaje de Datos y Firmas Electrónicas:

*“El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos”*.<sup>106</sup>

No obstante, del oficio 057-2012 ya citado, también se señala que el Sistema de Gestión, Decisión y Documentación Juris 2000, almacena todos

---

<sup>105</sup> Dirección Ejecutiva de la Magistratura. Unidad Coordinadora de Proyectos. Oficio N° 057-2010 de fecha 29 de enero de 2010. Caso Amparo Constitucional (Mary Luz del Carmen Betancourt vs. Decisión dictada en fecha 13 de abril de 2009, por el Juzgado Tercero de Primera Instancia en lo Civil, Mercantil, Tránsito y Bancario del Circunscripción Judicial del Área Metropolitana de Caracas)

<sup>106</sup> Decreto con Fuerza de Ley de Mensajes de Datos y Firmas Electrónicas N° 1204 de fecha 10 de febrero de 2001.

los registros en el listado log file<sup>107</sup>, que es el respaldo informático de las actuaciones realizadas en un asunto, en el cual se verifica fecha, hora de actuación, acción, el usuario que la realizó máquina en que se efectuó el trabajo y el cargo del funcionario responsable. Este tipo de análisis log presentan como principal vulnerabilidad, que el único modo de determinar la autoría de la navegación es mediante la dirección IP del ordenador desde el cual se está haciendo la conexión, lo que supone una importante limitación, debido a que desde un mismo ordenador se pueden conectar diferentes usuarios, incluso, también hay que remarcar que un usuario no tiene porque navegar o interactuar en espacios virtuales, desde un mismo ordenador, lo puede hacer desde varios dependiendo del momento del día, por ejemplo.

Desde el punto de vista del acceso, el Juris 2000 es un sistema de identificación, con usuario y contraseña (login o password), donde la creación del usuario se realiza atendiendo al procedimiento establecido y con previa autorización del responsable competente, que en este caso es la Oficina de Desarrollo Informático (ODI) adscrita a la Dirección Ejecutiva de la Magistratura (DEM). La asignación de contraseña inicial será provisional pudiendo ser personalizada en cualquier momento por los funcionarios. Este sistema no permite asociar períodos de validez a los identificadores de usuario de forma que fuera de ese rango de fechas, el sistema prevenga la autenticación a través de dicho identificador, sino que dependerá del usuario la modificación de su clave de acceso. Además hay que agregar que no existe un histórico de contraseñas que prevenga la re-utilización de la contraseña anterior.

---

<sup>107</sup> El Log file: registra cambios a la base de datos como resultado de transacciones o acciones internas del servidor. [http://es.wikipedia.org/wiki/Redo\\_Log\\_File](http://es.wikipedia.org/wiki/Redo_Log_File). (fecha de consulta: 15/07/2010)

No hay regularización de la fecha y la hora de los registros de actuaciones (escrito, libelo de demanda, solicitud, diligencia u otro tipo de documento) en el sistema Juris 2000, descartándose la certeza del tiempo que deben contener los servidores, en el registro de los documentos electrónicos del sistema. No existen certificados como el Digital time-stamp certificates que permita determinar el día y la hora en que un documento fue digitalmente registrado. Es decir, no hay posibilidad de verificar fechados fraudulentos antes o después de la fecha consignada.

Lo anterior, indica que no están cubiertas las necesidades de seguridad, requeridas para un sistema automatizado, que constituye una herramienta para el desempeño de la labor de administración de justicia, con los parámetros con los que han sido implementados otros softwares de gestión judicial en países latinoamericanos. Un ejemplo de ello lo constituye Costa Rica, país cuya modernización Judicial fue desarrollada por la misma empresa española (Seintex Consultores, S.A, licitación internacional N° 1-96<sup>108</sup>), que se encargó de ejecutar el proyecto de modernización judicial venezolano.

En sus avances más recientes, Costa Rica, cuenta con la consumación de Tribunales electrónicos o cero papel, a los fines de incorporar la tecnología en la gestión de los despachos judiciales, de conformar la causa de forma completamente electrónica, permitiendo el acceso a las mismas a través de internet y disminuir el tiempo de respuesta al usuario en la tramitación de los procesos.

---

<sup>108</sup> Poder Judicial de Costa Rica. *Evaluación del Plan Estratégico del Poder Judicial de Costa Rica 2000-2005*. Departamento de Planificación, Sección, Control y Evaluación. San José Costa Rica. Mayo 2005. [Documento en Línea]. Disponible en: [http://www.poder-judicial.go.cr/planificacion/Informes\\_Relevantes/105.pdf](http://www.poder-judicial.go.cr/planificacion/Informes_Relevantes/105.pdf). (Fecha de consulta: 18/06/2011).

### **4.3 Señalamientos Judiciales en el Sistema de Gestión Informática Juris 2000.-**

El Sistema de Gestión, Decisión y Documentación Juris 2000 aún cuando resultó ser una innovación beneficiosa<sup>109</sup> en la actividad administrativa del Poder Judicial, ha originado criterios diversos y muchos de estos contrariados sobre su funcionalidad, seguridad e integridad en la información que registra. A lo largo de la investigación se han detallado casos graves de inconsistencia de los datos guardados en el sistema frente a lo que ha aparecido en los expedientes en diversas partes del país, partiendo de una dualidad del sistema escrito y el electrónico. Adicionalmente se exponen a continuación, dos casos que marcan consideraciones relevantes sobre la importancia de los mecanismos de seguridad en los sistemas de gestión judicial.

#### *4.3.1 Caso de la mudanza de los Tribunales Civiles, Mercantiles, de Tránsito y Bancarios del Área Metropolitana de Caracas.-*

##### *a. Antecedentes<sup>110</sup>.-*

Los Tribunales Civiles, Mercantiles, de Tránsito y Bancarios del Área Metropolitana de Caracas hasta marzo de 2009 estaban ubicados en el edificio José María Vargas en la esquina de Pajaritos (por eso eran llamados los tribunales de Pajaritos), y estaban situados en el centro de Caracas. Este

---

<sup>109</sup> La evaluación que se hizo en mayo de 2003, en que se pretendió medir la duración de los juicios antes y después de la implantación del Juris 2000 mostró un gran éxito en la reducción del tiempo de los juicios. Louza, Laura; Vásquez, María; Tamma, Karol y D'Albano. El Juris 2000. trabajo no publicado. Caracas, 2003.

<sup>110</sup> Datos tomados de Manrique Isabel y Martínez, Alexandra. *El Acceso a La Justicia en los Tribunales Civiles, Mercantiles, de Tránsito y Bancarios del Área Metropolitana de Caracas*. Caracas, 2009. [Documento en línea]. Disponible en: <http://accesoalajusticia.org> (fecha de consulta: 27/08/2012)

edificio fue declarado inhabitable desde hace unos 15 años aproximadamente y ya habían propiciado varios intentos del extinto Consejo de la Judicatura en 1993 y luego de la Dirección Ejecutiva de la Magistratura para adquirir o remodelar nuevas sedes que fueran adecuadas.

Sin embargo, según datos reseñados en El Diario Universal citado por Manrique y Martínez<sup>111</sup>, los problemas de corrupción y burocráticos no dejaron que esto ocurriera. Tales son los casos del Edificio Metrolimpo en Chacao o el proyecto de la ciudad judicial Lebrún en Petare. En el primer caso, para el año 2005, el director ejecutivo de la Dirección Ejecutiva de la Magistratura (DEM), Luis Velásquez Alvaray, ordenó cancelar el proyecto por considerarlo fraudulento. Luego en el 2006, se abre una nueva licitación y se ordena retomar el proyecto, cancelando el 80% de la obra sin lograr ni el 17% de la construcción. En el segundo caso, el proyecto Ciudad Lebrún era de gran envergadura, haciéndose imposible su construcción en un corto período de tiempo como lo planteaba el Director de la DEM.

Ahora bien, la solución a la crisis institucional que atravesaban estos tribunales parecía avizorarse con un su traslado al edificio norte del Centro Simón Bolívar, piso 3, también situado en el centro de Caracas. No obstante, la mudanza duró varios meses (diciembre 2008- marzo 2009) y no hubo mayor información a los usuarios sobre cuándo volverían a entrar en funcionamiento los tribunales.

De lo narrado se suma lo que José Vicente Haro, abogado de una firma privada de Caracas, en una entrevista de Acceso a la Justicia señala:

---

<sup>111</sup> El Universal, 03-05-2008 “Una mudanza con mucha historia” citado por: Manrique, Isabel y Martínez, Alexandra. *El Acceso a La Justicia en los Tribunales Civiles, Mercantiles, de Tránsito y Bancarios del Área Metropolitana de Caracas. Op. cit...*

*“...Que durante el tiempo que los tribunales permanecieron cerrados, “hubo una flagrante violación al derecho de acceso a la justicia, porque no se previó una fecha cierta de duración de la mudanza, nadie informaba de nada, no se designó un tribunal de turno o alguna alternativa. A ninguno de los magistrados del Tribunal Supremo de Justicia, que es el órgano de dirección del Poder Judicial, se le ocurrió establecer un mecanismo transitorio. En esos 3 meses no hubo donde acudir, lo cual es una denegación de justicia”...<sup>112</sup>*

Por su parte, Raymond Orta Martínez especialista en Derecho Procesal, Tecnologías Gerenciales y Pruebas Científicas, ha señalado que:

*“Ya existen varios casos graves de inconsistencia de los datos guardados en el sistema frente a lo que ha aparecido en los expedientes en diversas partes del país. Esta situación se agravó en muchos casos con la mudanza de los tribunales de primera instancia civiles de Caracas, en los que se obligaba a revisar los expedientes de los tribunales que se habían mudado en el sistema, ya que no aparecían muchos expedientes físicos. Aparecieron muchos expedientes sentenciados, sin registro electrónico en el sistema una vez vencidos los lapsos para actuaciones, violando el derecho a la defensa de las partes”<sup>113</sup>.*

La situación citada dio origen a graves casos que violentaron el derecho a la defensa, al debido proceso y el acceso a la justicia, resaltando entre ellos un caso acción de amparo<sup>114</sup> que evidencia la mala gestión de la mudanza y la deficiente implantación del Juris 2000 en los tribunales civiles del Área Metropolitana de Caracas.

---

<sup>112</sup> Haro, José Vicente. Situación de los Tribunales de Primera Instancia, Civiles, Mercantiles y de Tránsito de Caracas. Entrevista. Marzo de 2009. [Documento en línea]. Disponible en: <http://accesoalajusticia.org> (fecha de consulta: 27/08/2012)

<sup>113</sup> Orta M, Raymond. Tecnología a media máquina en el poder Judicial venezolano. Noviembre 2009. [Documento en línea]. Disponible en: [www.tuabogado.com](http://www.tuabogado.com). (fecha de consulta: 12/12/2009)

<sup>114</sup> Juzgado Superior Décimo en lo Civil, Mercantil y Tránsito de la Circunscripción Judicial del Área Metropolitana de Caracas, en sede Constitucional. Sentencia N° 5.878. (Mary Luz del Carmen Lugo Betancourt vs. Sentencia dictada el 13/04/2009 Juzgado Tercero de Primera Instancia en lo Civil, Mercantil, Tránsito y Bancario de la Circunscripción Judicial del Área Metropolitana de Caracas). Disponible en: <http://www.tecnouiuris.com>. (fecha de consulta: 15/05/2010)

*b. Los Hechos.-*

Se inicio con una interposición de apelación, de una sentencia dictada por el Juzgado de Primera Instancia en lo Civil, Mercantil, Tránsito y Bancario, en el momento donde el sistema judicial se encontraba en un proceso de transición, lo cual es de notoriedad judicial, toda vez que los Juzgados de Primera Instancia en lo Civil, Mercantil, Tránsito y Bancario, cesaron sus actividades por la mudanza a la nueva sede ubicada al final de la Avenida Bolívar, Centro Simón Bolívar, Torre Norte, Piso Tres (3), Circuito Judicial de los Juzgados de Primera Instancia de la Circunscripción Judicial del Área Metropolitana de Caracas.

En dichos juzgados se instauró el Sistema Juris 2000, tecnología de información, accesibilidad, efectividad y transparencia. Pero quien interpone la apelación no fue beneficiada de los elementos que identifican al Juris 2000, ya que no tuvo acceso al expediente, siendo la vía más expedita para conocer el estado del juicio, así como tampoco, tuvo acceso a la información a través de la Oficina de Atención al Público (OAP), resultando infructuosos todos los intentos que hiciera para recabar la información acerca del recurso. No estaba cargada a la data la información requerida, siendo imposible obtener respuesta en relación, si el recurso de apelación interpuesto, había sido admitido; si se le había dado entrada al expediente contentivo de dicha apelación; y cuándo vencía el término de los días de despacho para dictar sentencia.

Posteriormente, la información que se logró obtener de la causa, era que el recurso de apelación ejercido fue declarado sin lugar, quedando en estado de indefensión la parte que lo interpone por no haber podido promover las pruebas, las cuales si se hubieran consignado en su oportunidad, la decisión

hubiese sido distinta; violándose el derecho a la defensa, al debido proceso, a la tutela judicial efectiva y el acceso a la justicia. Tales alegatos condujeron a una solicitud de amparo constitucional, a los fines de que se declarará la nulidad de todas las actuaciones procesales realizadas antes de la atacada en amparo, ordenándose la reposición de la causa al estado de la admisión del recurso de apelación.

En la audiencia constitucional expone la representación judicial de la parte agraviada, que fueron violentados los derechos constitucionales de su cliente, tales como el derecho a la defensa, al debido proceso y acceso a la justicia; que se vieron afectados por el sistema Juris, porque no les fue posible tener acceso al expediente. Cada vez que acudían a la sede de los Tribunales, se les informaba que no estaba cargada a la data del sistema dicha información, que trataron de buscar información en el archivo, recibiendo como respuesta que su expediente no tenía número, y que en archivo no sabían cuál era el procedimiento a seguir para los expedientes que venían en apelación y que la secretaria siempre estaba ocupada. Todo ello condujo que la sentencia fuese dictada sin la consignación de pruebas preestablecidas.

La representación del Ministerio Público expuso que revisadas como fueron las actas del expediente, considera que a la parte presuntamente agraviada se le violentó el derecho a la defensa y al acceso a la justicia, en virtud del caos que en principio causó la implementación del sistema Juris. Además, en aras de restituir la situación infringida se le permitió la promoción de las pruebas de experticia, de experimento; de inspección judicial; de testigo experto y de documental, de las cuales el tribunal admite solamente la prueba de informes, en cuanto está dirigida a verificar el dato sobre la certificación de la fecha de la ocurrencia y carga en el sistema de las

actuaciones y consignaciones realizadas por el usuario, en el expediente respectivo.

A los fines de la evacuación de dicha prueba, se ordenó oficiar a la Coordinación del Sistema Juris 2000 de los Juzgados de Primera Instancia en lo Civil, Mercantil, de Tránsito y Bancario de la Circunscripción Judicial del Área Metropolitana de Caracas, a los fines de obtener información sobre la implementación o no de firmas digitales en el Juris 2000. De lo que resulta, que el sistema no cuenta con firmas digitales por lo que no garantiza que dichas actuaciones procesales sean ingresadas en la hora, fecha y día en que ocurrieron, toda vez que se presume que dicho software puede ser alterado por los mismos operarios y en base a tales argumentos, se declara con lugar la acción de amparo, reponiéndose la causa al estado de que el juzgado admita la apelación, a los fines de que las partes puedan ejercer el derecho a la defensa.

*c. Consideraciones.-*

De la jurisprudencia, se ha reiterado el deber de las partes de consultar las actuaciones surtidas en los procesos, a través del medio físico (expediente), ya que la consulta por medios electrónicos no produce certeza en la información suministrada, considerando que sólo constituyen reportes que no muestran la totalidad de las argumentaciones procesales. De manera que, no se logra satisfacer el deber de vigilancia de las actuaciones procesales a través de la información contenida en la base de datos del sistema automatizado del despacho judicial.

Ahora bien, del caso bajo examen, la publicidad de las actuaciones judiciales, se convirtió en la subversión de una garantía procesal, como el

debido proceso. La confianza legítima que genera la documentación del proceso y la publicidad que ofrece la organización tribunalicia, se menoscabó como consecuencia del “*desorden Procesal*”, figura ampliamente interpretada por la jurisprudencia.

Al respecto, la Sala Constitucional del Tribunal Supremo de Justicia, ha referido que:

*“Ejemplos del “desorden”, sin agotar con ello los casos, pueden ser: la mala compaginación en el expediente de la celebración de los actos, trastocando el orden cronológico de los mismos; la falta o errónea identificación de las piezas del expediente o del expediente mismo; la contradicción entre los asientos en el libro diario del Tribunal y lo intercalado en el expediente; la contradicción entre los días laborales del almanaque tribunalicio y los actos efectuados en días que no aparecen como de despacho en dicho almanaque; la dispersión de varias piezas de un proceso, en diferentes tribunales; la ausencia en el archivo del Tribunal de piezas del expediente, en determinados juicios; el cambio de las horas o días de despacho, sin los avisos previos previstos en el Código de Procedimiento Civil (artículo 192); la consignación en el cuaderno separado de actuaciones del cuaderno principal, y viceversa; la actividad en la audiencia que impide su correcto desarrollo (manifestaciones, anarquía, huelga, etc.)”<sup>115</sup>*

En consecuencia, aunque este tipo de situaciones no resulta imputable directamente a un sistema automatizado como el Juris 2000, si es claro, que resulta importante su señalamiento, a los fines de dar mayor relevancia a sus registros y a lo que finalmente constituye el Libro Diario de Actuaciones del Tribunal. La sentencia citada, ha señalado el *Stricto sensu* como uno de los tipos de desorden procesal que no refiere una subversión de actos procesales, sino a la forma como ellos se documenten. Es decir, los actos no

---

<sup>115</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 2821 de fecha 28 de octubre de 2003. (Caso: José Grgorio Rivero Bastardo. Acción de Amparo) [Documento en Línea]. Disponible en: <http://www.tsj.gov.ve/decisiones/scon/Octubre/2821-281003-03-1152%20.htm>. (Fecha de Consulta: 18/07/2011)

son nulos, cumplen todas las exigencias de ley, pero su documentación en el expediente o su interconexión con la infraestructura del proceso, es contradictoria, ambigua, inexacta cronológicamente, lo que atenta contra la transparencia que debe regir la administración de justicia, y perjudica el derecho de defensa de las partes, al permitir que al menos a uno de ellos se le sorprenda, situación ésta que es posible evidenciar del funcionamiento del sistema en algunas sedes judiciales del país.

El caso de la mudanza de los Tribunales Civiles, Mercantiles, de Tránsito y Bancarios del Área Metropolitana de Caracas, fue considerada como la muestra representativa de esta investigación a los fines de fijar las necesidades de ciertos elementos técnicos de seguridad, en situaciones que aún cuando no le sean directamente imputable al funcionamiento electrónico, podrían ayudar a subsanar los quebrantamientos de las irregularidades que se susciten en torno a su documentación. Al respecto, es posible hacer los siguientes señalamientos:

a. La situación funcional de sedes judiciales como la tratada en este caso, donde los expedientes muchas veces no logran ser localizados y en el sistema el registro electrónico resulta escueto, por contener únicamente las partes y las últimas actuaciones, sin constituirse un expediente electrónico completo, conduce a que se hagan mejoras en los sistemas automatizados respecto a la seguridad. Esto de manera directa, no solucionaría el problema del desorden procesal que caracteriza hoy día los registros del Juris 2000, pero permitiría determinar el día y la hora en que un documento fue digitalmente registrado. Es decir, la posibilidad de verificar fechados fraudulentos antes o después de la fecha consignada a los fines de determinar las responsabilidades civiles, administrativas y penales de los funcionarios que participan en la carga del sistema. Situación ésta, que

constituiría una garantía al ciudadano, de que no existe manipulación inescrupulosa de las actas del expediente, que lo sorprendan con decisiones que no visualizó de la última consulta de la causa y que ahora aparecen.

b. En los casos en que la diligencia presentada en el sistema Juris 2000, no aparezca anexada al expediente, como ocurre en los Tribunales que sirven de referencia, se debe abandonar la posición adoptada por la Sala Social del Tribunal Supremo de Justicia, de que la certeza de la información procesal está en el físico y desvirtuar el registro electrónico, para pasar a evaluar, los mecanismos que son necesarios para formar un verdadero proceso electrónico, donde incluso se abandone el papel y se confíe en la autenticidad y veracidad de lo que se registra.

En el estudio realizado por Manrique y Martínez, se evidenció que en los Tribunales Civiles, Mercantiles, de Tránsito y Bancarios del Área Metropolitana de Caracas, ocurren los siguientes hechos:

*“...En 20 minutos luego de la presentación de la diligencia, ésta se encuentra ya en el expediente, pero la experiencia demuestra que no aparece antes de 4 días. Hay casos en que no aparece la diligencia en el expediente. Hubo un caso en el cual se declaró inadmisibles las demandas, supuestamente porque faltaban los documentos originales que debían acompañar el libelo de la demanda. El abogado reclamó a la secretaria del Tribunal porque los había consignado y ésta dijo no haber firmado el auto que declara inadmisibles las demandas”<sup>116</sup>.*

Bajo este tipo de hechos, se genera el desorden procesal determinado por la ambigüedad de los registros que rielan en el físico del expediente y en los registros automatizados, dejando a la expectativa a la parte contra quien

---

<sup>116</sup> Manrique Isabel y Martínez, Alexandra. *El Acceso a La Justicia en los Tribunales Civiles, Mercantiles, de Tránsito y Bancarios del Área Metropolitana de Caracas...op. Cit.*

se produce aquellas actuaciones sujetas a incertidumbre. De considerarse un verdadero proceso electrónico asociado a firmas digitales y certificaciones electrónicas, la constitución de una sola base de resguardo (el expediente electrónico) manejaría de manera más segura los registros electrónicos. No obstante, en Venezuela el proceso judicial desde sus inicios ha girado en torno a la agregación de documentos a un expediente físico y de papel, por tanto, con la implementación del Sistema Automatizado Juris 2000 la pretensión ha sido lograr que el sistema de gestión, procure registros los mas fidedigno posible acerca de los documentos contenidos en el expediente, a los fines de configurar el elemento de la equivalencia funcional, el cual como se ha detallado en capítulos anteriores, se logra partiendo de la fiabilidad, integridad y no repudio que ofrecen la firma electrónica y la certificación técnica.

Finalmente, en casos como este, se ha ido anulando el efecto positivo de las mejoras de gestión, lo que ha sido confirmado por Louza al señalar:

*“La mudanza a finales de 2008, concluida en marzo de 2009, de los tribunales civiles, mercantiles y de tránsito a una nueva sede en que se implantó el Juris 2000, sin responder a los requerimientos de infraestructura física y tecnológica de este sistema de gestión judicial, ni a las reales necesidades de la administración de justicia, ni tampoco respetar los principios básicos del modelo organizacional, demuestra que las mejoras en la gestión judicial dejan también de ser una prioridad para el Tribunal Supremo de Justicia”<sup>117</sup>.*

*4.3.2 Sentencia Controversial. A pesar de que no se tenga en físico el expediente respectivo aún se puede decir que las partes se encuentran a derecho y se da la notificación presunta.-*

En sentencia N° 624, de fecha 15 de mayo de 2012, de la Sala

---

<sup>117</sup> Louza S, Laura. La revolución Judicial en Venezuela. FUNEDA. Caracas, 2011, p.39.

Constitucional del Tribunal Suprema de Justicia ha señalado la posibilidad de que a pesar de que no se tenga en físico el expediente respectivo, aún se puede decir que las partes se encuentran a derecho y se da la notificación presunta.

*“...Se debe tener en cuenta que el libro de diario refleja todo lo que aparece en el Sistema Juris 2000, el cual a su vez puede ser consultado por las partes a través de las computadoras disponibles de lo que se ha denominado “Autoconsulta” y que se refiere a que las partes y los abogados (quienes generan su propia clave) pueden ver y consultar el expediente, una vez que se encuentran diarizadas y cargadas en el sistema de manera inmediata, pudiendo observar todas las actuaciones y la hora de realización aunque no tenga en físico el expediente respectivo, viendo todos los expedientes en los que aparecen. Además del mecanismo indicado anteriormente, también el Secretario de guardia puede dar la información a las partes y sus apoderados de manera inmediata y actualizada y finalmente la Oficina de Atención al Público también puede suministrar información sobre el contenido del expediente cuando no se puede observar el físico. Con esto se observa que a pesar de la instalación tecnológica moderna y que no se tenga en físico el expediente respectivo aún se puede decir que las partes se encuentran a derecho y se da la notificación presunta”<sup>118</sup>.*

Se trata de pronunciamiento que ha contrariado las consideraciones que se venían asumiendo respecto a la fiabilidad del registro electrónico del Juris 2000. Además, advierte sin detenimiento en mayores formalidades de seguridad electrónica, que la frase prevista en disposiciones legales, “*una vez que constara en autos la notificación de las partes*”, se ha extendido mas allá de las actas del físico del expediente hasta alcanzar, el registro electrónico del Sistema Juris 2000, sin estimar un posible quebrantamiento material del debido proceso y del derecho a la defensa, al dejar de un lado

---

<sup>118</sup> Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 624 de fecha 15 de mayo de 2012. (Caso: Instituto Fondo de Protección Social de los Depósitos Bancarios. Acción de Amparo). [Documento en Línea]. Disponible en: <http://www.tsj.gov.ve/decisiones/scon/Mayo/624-15512-2012-11-0638.html>. (Fecha de Consulta: 02/06/2012)

las inconsistencias en los registros por errores materiales involuntarios y la inexistencia de equivalencia funcional.

Las actuaciones compiladas en el respectivo Libro Diario de cada uno de los juzgados, es copia fiel, idéntica, directa e indiscutible de las actuaciones cumplidas por el tribunal correspondiente y no cabe duda de que el texto de una actuación reseñada en él, se corresponde con la insertada en el Modelo Organizacional y Sistema Integral de Gestión, Decisión y Documentación Juris 2000 que es el consultado, en pantalla, por los funcionarios al servicio de la Oficina Atención al Público OAP y por las partes en el servicio de Autoconsulta. Sin embargo, el Sistema Juris 2000 no ofrece herramientas de seguridad que hagan prescindir de la posible manipulación de quienes lo manejan, sus registros no pueden configurarse con los contenidos en el físico del expediente como un documento público, por no estar refrendados de manera electrónica a través de la firma digital, por la autoridad judicial que prevé la ley, ni de un certificado técnico que haga confiable el documento. En definitiva no se cuenta con la existencia de un poder Judicial constituido como autoridad certificadora de las actuaciones judiciales electrónicas que se emiten en el transcurso del proceso.

## CONCLUSIONES

De lo desarrollado en la estructura de la investigación, se exponen las siguientes consideraciones finales:

1. El debido proceso se ofrece como una garantía que permite a los ciudadanos ejercitar su defensa en el marco de una sucesión de actuaciones judiciales y disfrutar de la oportunidad efectiva de interponer los recursos que las mismas normas autoricen, pero cuando ésta garantía se asocia con la implementación de servicios automatizados de gestión, es necesario que concurra el cumplimiento de dos elementos: la publicidad electrónica de las actuaciones judiciales, y la equivalencia funcional del mensaje de datos, contenido en el historial del proceso con lo informado en el expediente. Ello es importante, de acuerdo a la naturaleza funcional que tiene el Sistema Juris 2000, de informar o reportar a las partes de las actuaciones que se generan con ocasión del proceso, es decir, desde el punto de vista de la publicidad de las actuaciones que garantizan a la partes, de ser notificadas de los cargos por los cuales se le investiga; de acceder a las pruebas y de disponer del tiempo y de los medios adecuados para ejercer su defensa.

2. La equivalencia funcional será cumplida en la medida en que los sistemas automatizados de gestión, dispuestos al servicio de la justicia, tengan asociada, la certificación técnica de sus registros, es decir, la implementación de certificados electrónicos que aseguren la integridad de la información, el no repudio, la emisión y recepción de datos, así como, la fiabilidad del momento exacto (tiempo) en que se registran efectivamente los actos procesales.

3. Con la implantación del sistema Juris 2000, en las sedes judiciales del país, diversos criterios reiterados del Tribunal Supremo de Justicia han considerado, que la certeza jurídica de lo que acontece en un proceso judicial, se encuentra contenida en los expedientes que reposan en los archivos de los Tribunales, por lo que las informaciones a través de un medio auxiliar, como es el Sistema Integral de Gestión, Decisión y Documentación, Juris 2000, es simplemente informativo. No existe la referida equivalencia funcional ya que, la publicidad de las actuaciones, consiste en un reporte de datos que obliga a consultar la totalidad del documento, directamente del expediente.

4. Adicionalmente, la certificación técnica de las actuaciones, haría operativa la notificación electrónica prevista en algunas leyes especiales de nuestro país, y cuya práctica ha sido retardada en algunos casos, o no se ha aplicado debidamente en otros. Además, el valor de un indicio que tienen los documentos electrónicos del sistema Juris 2000, desaparecería sí, además, de proveérsele de la firma digital respectiva, fuesen certificadas por un proveedor de servicios que le otorgara la validez y autenticidad para darle fe pública a los registros, y en consecuencia, constituir un documento público electrónico. Considerando que este carácter le es otorgado, cuando la impresión de los archivos digitalizados es previamente firmado por la autoridades judiciales (juez y secretario) según las formalidades del artículo 1357 del Código Civil venezolano.

5. De la consideración que precede, se enfatiza que los certificados electrónicos cuya finalidad es acreditar y certificar la autoría e integridad del mensaje electrónico, no se bastan por sí solos para dar autenticidad legal a un documento y revestirlo con carácter público, a no ser que se cumplan con los extremos de ley, referentes a la fe pública de los funcionarios facultados.

6. Dentro de las políticas asumidas en el proceso de modernización judicial no se formuló el desarrollo, instalación y perfeccionamiento de herramientas informáticas de seguridad, posiblemente por el poco conocimiento que se tenía para aquellos años de la instauración del proyecto, de la firma digital y de certificación electrónica en los sistemas de gestión, mecanismos que fueron regulados años más tarde por el Decreto-Ley sobre Mensajes de Datos y Firmas electrónicas del 2001, por tanto el Sistema Juris 2000 es un sistema de gestión automatizada que no cumple con los estándares internacionales de un verdadero sistema automatizado judicial.

7. En la Regulación Nº 70 que ordena la creación progresiva de la estructura organizativa y funcional, necesaria para implantar y desarrollar en todos los Tribunales del país el sistema de Gestión, Decisión y Documentación Juris 2000, son escasas las disposiciones referidas a la implantación del elemento tecnológico del Sistema automatizado Juris 2000 e inexistentes los lineamientos sobre la seguridad de sus registros. Aunque, en el artículo 35 ha dejado abierta la posibilidad de avanzar la sistematización judicial al cumplimiento de herramientas tecnológicas que permitan materializar un proceso judicial más efectivo, a través de la implementación de los mecanismos reglamentados en el Decreto-Ley sobre Mensaje de Datos y Firmas Electrónicas.

8. Considerando el elemento de la identidad electrónica que se vincula a los certificados electrónicos, como aquella que permite ser reconocido e identificado tras la introducción de un nombre de usuario y una contraseña, se concreta que el Juris 2000 es un sistema de identificación, con usuario y contraseña (login o password), donde la creación del usuario se realiza atendiendo al procedimiento establecido y con previa autorización del

responsable competente, que en este caso es la Oficina de Desarrollo Informático (ODI) adscrita a la Dirección Ejecutiva de la Magistratura (DEM). La asignación de contraseña inicial será provisional pudiendo ser personalizada en cualquier momento por los funcionarios. Este sistema no permite asociar períodos de validez a los identificadores de usuario de forma que fuera de ese rango de fechas, el sistema prevenga la autenticación a través de dicho identificador, sino que dependerá del usuario la modificación de su clave de acceso. Además hay que agregar que no existe un histórico de contraseñas que prevenga la re-utilización de la contraseña anterior. Además, el control de acceso a los servicios del sistema es recogido por un fichero (logfile), lo cuales son vulnerables en el modo de determinar la autoría de la navegación en red.

9. Para la valoración del documento electrónico (actuaciones procesales) que genera el sistema automatizado Juris 2000, es necesario precisar tres situaciones: 1. El documento electrónico que esté asociado a una firma electrónica debidamente certificada por un Proveedor de Servicios de Certificación conforme a lo establecido en la Ley sobre Mensajes de Datos y Firmas Electrónicas (2001), tendrá la misma validez y eficacia probatoria que la Ley otorgue al documento que contiene una firma autógrafa, es decir, hace plena prueba entre las partes; 2. El documento electrónico al cual esté asociada una firma electrónica, validada por un certificado electrónico de firma, emitida por un Proveedor de Servicios de Certificación no acreditado ante la Superintendencia de Servicios de Certificación Electrónica o al cual esté asociado simplemente una firma electrónica no certificada, constituirá un elemento de convicción valorable conforme a la regla de la sana crítica. 3. El documento electrónico no asociado a una firma electrónica, solo tendrá el valor de un indicio, por lo que debe ser acompañado de otros medios de prueba que sustenten los hechos contenidos en el mensaje de datos. Bajo

estas precisiones es por lo que los registros electrónicos del Juris 2000 son considerados copias simples.

10. Aún bajo la existencia de un sistema normativo (Decreto-Ley de Mensaje de Datos y Firmas Electrónicas) que impulsa la implementación de la firma y la certificación electrónica, el Tribunal Supremo de Justicia y el Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación, han dejado detenido los esfuerzos de la inclusión de la certificación electrónica en un Convenio de Cooperación Interinstitucional entre el Poder Judicial y el Ministerio de Ciencia y Tecnología, firmado en el año 2004, cuya materialización no se ha visto empleada en los servicios automatizados que se presta en los Tribunales del país a través del Juris 2000. Cabe destacar, que el Estado venezolano, específicamente, el Poder Judicial, no ha establecido una política de desarrollo del tribunal electrónico en cuanto a la implementación de herramientas necesarias para la seguridad de la información judicial que se maneja en sus sistemas automatizados.

11. En la comparación realizada de los sistemas de seguridad implementados en las Tecnologías de Información y Comunicaciones de varios países de Latinoamérica, con los mecanismos de validación, autenticación y seguridad del Juris 2000, despertó la atención, que sistemas automatizados como el de Costa Rica, cuya modernización Judicial fue desarrollada por la misma empresa española que se encargó de ejecutar el proyecto de modernización judicial venezolano, no mantiene similitud en los avances tecnológicos implementados en este último. Costa Rica cuenta con la consumación de Tribunales electrónicos o cero papel, a los fines de incorporar la tecnología en la gestión de los despachos judiciales, de conformar la causa de forma completamente electrónica, permitiendo el acceso a las mismas a través de internet y disminuir el tiempo de respuesta

al usuario en la tramitación de los procesos, todo ello con la participación de mecanismos de seguridad como la firma electrónica y la certificación técnica.

12. Finalmente, del análisis de señalamientos judiciales como el de caso de la mudanza de los Tribunales Civiles, Mercantiles, de Tránsito y Bancarios del Área Metropolitana de Caracas, se conoce por primera vez que los registros del sistema Juris 2000, no poseen firmas digitales que certifiquen las actuaciones realizadas, así como, no existe regularización de la fecha y la hora de los registros de actuaciones (escrito, libelo de demanda, solicitud, diligencia u otro tipo de documento). Esto último, descarta la certeza del tiempo que deben contener los servidores, en el registro de los documentos electrónicos del sistema. El sistema Juris 2000, no posee certificados como el Digital time-stamp certificates que permita determinar el día y la hora en que un documento fue digitalmente registrado. Es decir, no hay posibilidad de verificar fechados fraudulentos antes o después de la fecha consignada.

## RECOMENDACIONES

La inversión tecnológica que se inició en el año 1993, mediante el Convenio 3.514-VE que dio paso a la implantación del Sistema de Gestión, Decisión y Documentación Juris 2000 en las sedes judiciales del país para lograr la efectividad, celeridad y transparencia de las actividades jurisdiccionales, ha generado en la praxis del servicio, irregularidades e inconsistencias, alguna de las cuales se podrían solventar en la posibilidad de materializar los siguientes aportes:

1. Considerando las irregularidades de los registros y la restringida fiabilidad de la información que presta, tal y como se evidenció del desarrollo de esta investigación, es necesario que los criterios de eficacia y eficiencia que deben caracterizar la automatización de un proceso, obedezcan a un nuevo estudio y análisis, acerca de qué prácticas se quieren abandonar y qué resultados se quieren lograr. Bajo este planteamiento, se debe determinar si el Juris 2000, es un software cuya plataforma es adecuada para asumir los retos planteados o si por el contrario debe invertirse en otras iniciativas tecnológicas.

2. La regulación normativa que se le ha ofrecido al sistema de gestión automatizada Juris 2000 no ha sido la más adecuada, desprendiéndose de resoluciones como la N° 70, un desarrollo dispositivo dirigido más hacia la estructura y funcionalidad del modelo organizacional que lo complementa, que a los sistemas de seguridad que deben garantizar la fiabilidad de los registros. Tampoco ha sido posible, implementar aplicación efectiva de las disposiciones normativas que contempla el Decreto-Ley de Mensaje de Datos y Firmas Electrónicas, por ser inexistente en el software judicial, la

asociación de la firma y del certificado electrónico. De estas consideraciones, se sugiere desarrollar una normativa que regule el comportamiento de los registros de un sistema automatizado de gestión procesal, a los fines de prever su alcance, sin que sean los criterios de la Sala Constitucional quienes interpreten su funcionamiento y la fiabilidad de sus mensajes de datos. La regulación normativa debe ordenar y a la vez permitir a los órganos judiciales establecer cuanto antes un verdadero proceso judicial electrónico confiable y seguro en todas sus fases, cimentado sobre los principios de celeridad, eficacia, eficiencia, y transparencia. Además, de ella se deben derivar responsabilidades a los funcionarios que operen el servicio automatizado.

3. Por otro lado, se requiere que el Estado asuma costos de inversión para asociar al Sistema Juris 2000 los mecanismos de la firma digital y del certificado electrónico, para evitar que sigan perdiendo de vista los costos en la adquisición del desarrollo y no exista una discriminación del mensaje de dato frente a la cultura del físico del expediente. Resulta claro que no basta establecer presupuestos para la implementación de tecnologías al servicio de la administración de justicia, sino que muchas veces se pasa por alto (Caso Juris 2000) las inversiones que resultan necesarias para el mantenimiento y actualización de estos. De lo contrario, será difícil detener la obsolescencia tecnológica tanto del software como de los equipos (computadoras) requeridos para su operacionalización.

4. Por otro lado, se recomienda una actividad de monitoreo permanente que permita detectar las dificultades e irregularidades y solucionarlas a la brevedad posible, en lugar de continuar replicando el problema bajo sugerencias jurisprudenciales de la consulta directa de la causa.

5. Finalmente, se aspira que el Sistema Juris 2000 deje de ser una herramienta desconocida para quienes ejercen el derecho y esto en consideración de la documentación que existe respecto al proceso de implantación de este sistema, la funcionalidad, seguridad y naturaleza de los registros. Se debe adoptar una campaña publicitaria que permita conocer a los justiciables de los sistemas automatizados de gestión que se prestan en los tribunales, a los fines de que se conviertan en los auditores más cercanos del servicio y del desempeño funcional.

## FUENTES DOCUMENTALES

### Bibliografía.-

Barrios, Maritza. (1998). Manual de Trabajos de Grado de Especialización, Maestría y Tesis Doctorales. Caracas: Fedupel.

Bello Tabares, H; Jiménez Ramos, D. (2009) *Tutela Judicial Efectiva y otras garantías constitucionales procesales*. Segunda Edición. Ediciones Paredes. Caracas.

Díaz G, Alexander. *Las Notificaciones Electrónicas Judiciales en Colombia. El notario Electrónico (firmado electrónicamente)*, Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento N° 2. Mayo-Agosto 2008, p.132

Dirección Ejecutiva de la Magistratura. Unidad Coordinadora de Proyectos. Oficio N° 057-2010 de fecha 29 de enero de 2010. Caso Amparo Constitucional (Mary Luz del Carmen Betancourt vs. Decisión dictada en fecha 13 de abril de 2009, por el Juzgado Tercero de Primera Instancia en lo Civil, Mercantil, Tránsito y Bancario del Circunscripción Judicial del Área Metropolitana de Caracas)

Garay, Juan. (2001) *La Constitución*. Segunda versión: Gaceta Oficial 5.453. Ediciones Juan Garay. Caracas

Hernández, M, Luis A. (1995). *La Autenticidad Proveniente de los Particulares sin Intervención de Funcionario Público*”Revista de Derecho Probatorio N° 5, cuyo director es el Dr. Jesús Eduardo Cabrea Romero, Editorial Jurídica Alva, S.R.L., Caracas.

Jacopo Gamba. (2010). *Panorama del derecho informático en América Latina y el Caribe*. Comisión Económica para América Latina y el Caribe (CEPAL). Colección Documentos de proyectos.

Lorenzetti, Ricardo. Comercio Electrónico. Abeledo Perrot. Argentina. 2000

Louza Luisa. (2007) *Derecho y Democracia. La sociedad civil y el ciudadano en Venezuela frente al Sistema de Justicia a partir de la nueva constitución*. Cuadernos Unimetanos.

Louza S, Laura. (2011). *La revolución Judicial en Venezuela*. FUNEDA. Caracas.

Louza, Laura; Vázquez, María Alejandra; Tamma, Karol; D´Albano, Mariagrelys (2003); *El Juris 2000*, trabajo no publicado.

Martín T, Miguel A. (2008). *La Fase Previa en el proceso Civil Venezolano*. Trabajo Especial de Grado. Universidad Católica Andrés Bello. Caracas.

Méndez, C. *Metodología*. (1998) *Guía para Elaborar Diseños de Investigación en Ciencias Económicas, Contables y Administrativas*. Editorial Mc GRAW-Hill Interamericana, S. A. Colombia.

Odreman O, Gregory. (2003) *Eficacia Probatoria del Mensaje de Datos y de la Firma Electrónica según la nueva Ley de Mensaje de Datos y Firmas Electrónicas*. Universidad Católica Andrés Bello. Caracas.

Peñaranda. Q, Héctor. (2001). *Iuscibernetica: Interrelación entre el Derecho y la Informática*. Fondo Editorial para el Desarrollo de la Educación Superior (FIDES). Maracaibo.

Peñaranda Quintero, Héctor. (2011) *“La Firma Electrónica Digital en Venezuela”*. Revista Crítica de Ciencias Sociales y Jurídicas N° 29 (2011.1). Universidad del Zulia.

Pérez S, Erick L. (2004). *Comentarios a la Ley Orgánica Procesal del Trabajo*. Segunda Edición. Editores Hermanos Vadell. Valencia.

República Bolivariana de Venezuela. (2005) *Ministerio de Ciencia y Tecnología. Memoria y Cuenta 2004*. Caracas.

Rueda, Aníbal y Peretti de Parada Magali. (1998). *La indefensión*. Vadell Hermanos Editores. Caracas.

Salcedo C, Juvenal. (2006). *La prueba Documental*. Departamento de Publicaciones de la Facultad De Ciencias Jurídicas y Políticas de la Universidad Central de Venezuela. Caracas.

Scognamiglio, Laura L. (2011). *La Revolución Judicial en Venezuela*. Funeda, Caracas.

Seintex. (2000). *Diseño e Implementación del Modelo Organizacional y un Sistema Integral de Gestión, Decisión y Documentación para los Tribunales Pilotos*. Manual del Técnico Jurídico. Caracas.

Soto C, Milagros M. (2001) “*Consideraciones sobre la prueba documental electrónica en el proceso civil venezolano*”. Estudios de Derecho Civil. Vol III. Libro homenaje a José Luis Aguilar Gorrondona. Tribunal Supremo de Justicia. Colección Libros homenaje No. 5. Caracas.

Torres Z, Luís E. (2002). “*Análisis de riesgos y medidas de seguridad para el Sistema de Jurisprudencia del Poder Judicial Venezolano (JURIS 2000)*”. Trabajo de Grado. Universidad Central de Venezuela.

Urdaneta. B, José V. (2010). *Los Mensajes de Datos y la Firma Electrónica (Seguridad Jurídica que ofrecen y Valor Probatorio)*. Serie Tesis 5. Académica de Ciencias Sociales y Políticas de la Universidad Metropolitana. Caracas.

### **Referencias de Documentos Electrónicos.-**

Administración de Justicia Electrónica. Ibermatica. [Documento en línea]. Disponible en: [www.ibermatica.com/a.landa](http://www.ibermatica.com/a.landa). (fecha de consulta: 05/08/2011)

Bencomo Escobar, Tania. (2009). *Tecnología Digital en la Administración de Justicia Laboral venezolana*. Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM. [Documento en línea]. Disponible en: <http://www.juridicas.unam.mx>, (fecha de consulta: 06/09/2010)

Boanza, Clara. *Integridad y Confiabilidad de la Información*. [Documento en línea]. Disponible en: <http://www.cypsela.es>. (fecha de consulta: 21/11/2011).

CEJA. *Reformas Procesales Penales en América Latina: Discusiones Locales*. [Documento en línea]. Disponible en: [http://ceja.cl/portal/index.php/es/biblioteca/biblioteca-virtual/doc\\_details/3320-reformas-procesales-penales-en-america-latina-discusiones-locales](http://ceja.cl/portal/index.php/es/biblioteca/biblioteca-virtual/doc_details/3320-reformas-procesales-penales-en-america-latina-discusiones-locales). (fecha de consulta: 05/03/2011).

Centro de Estudios de Justicia de las Américas (CEJA), [Documento en línea]. Disponible en: <http://www.cejamericas.org>.

Criterios generales de seguridad en los sistemas de información al servicio de la Administración de Justicia. Acuerdo del Pleno, de 13 de septiembre de 2007. [Documento en línea]. Disponible en: [www.juntadeandalucia.es](http://www.juntadeandalucia.es). (fecha de consulta: 13/03/2011).

Diario Oficial de las Comunidades Europeas. Directiva 1999/93/Ce del Parlamento Europeo y Del Consejo por la que se establece el marco comunitario para la firma electrónica de fecha 13 de diciembre de 1999. [Documento en línea]. Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:ES:P DF>. (fecha de consulta: 01/09/2012).

Díaz G, Alexander. *Desnaturalización del Documento Electrónico Judicial con la Apelación de la Sentencia*. El Juicio Oral en el Nuevo Sistema Penal Acusatorio Colombiano. [Documento en línea]. Disponible en: <http://www.alfaredi.org/sites/default/files/articles/files/Diaz.pdf>. (fecha de consulta: 21/11/2011).

Dirección Ejecutiva de la Magistratura. *Juris 2000. El Modelo Organizacional*. [Documento en línea]. Disponible en: <http://dem.tsj.gov.ve/unclick.htm>. (fecha de consulta: 25/07/2010).

Flores. Z, Felipe. *Uso de las Tecnologías de la Información y la Comunicación. ¿El Debido Proceso en Peligro?* Universidad ICESI. [Documento en línea]. Disponible en: <http://www.icesi.edu.co/>; (fecha de consulta: 26/02/2011).

Granados P, Gibran. Introducción a la Criptografía. Revista Digital Universitaria. Volumen N° 7, JULIO 2006. [Documento en línea]. Disponible en: [http://www.revista.unam.mx/vol.7/num7/art55/jul\\_art55.pdf](http://www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf). (fecha de consulta: 01/09/2012).

Haro, José Vicente. Situación de los Tribunales de Primera Instancia, Civiles, Mercantiles y de Tránsito de Caracas. Entrevista. Marzo de 2009. [Documento en línea]. Disponible en: <http://accesoalajusticia.org>. (fecha de consulta: 27/08/2012).

Hellin, Luis Enrique. *La Certificación y Firma Electrónica en el ámbito de la Informática Forense*. Primer Congreso Internacional de Seguridad de la Información. Caracas. 2010 Disponible en: <http://www.suscerte.gob.ve/>. (fecha de consulta: 26/02/2011).

Hernández, C. y Adelardi, R. *Perspectivas de uso e impactos de las TIC en la administración de justicia en América Latina*. [Documento en línea]. Disponible en: <http://www.cejamericas.org/doc/documentos/Libroblancoe-justicia.pdf>, (fecha de consulta: 26/08/2010)

Hernández. O, Enrique. *Seguridad y Privacidad en los Sistema Informáticos*. [Documento en línea]. Disponible en: <http://www.disca.upv.es/enheror/pdf/ACTASeguridad.PDF>. (fecha de consulta: 17/08/2010).

Hernández, R; Berrios, Kranya y González, Víctor. *Identidad Electrónica*. SUSCERTE. [Documento en línea]. Disponible en: [www.SUSCERTE.gob.ve](http://www.SUSCERTE.gob.ve). (fecha de consulta: 21/11/2010)

Hernández, Fernández y Baptista. (2003) Metodología de la Investigación. Tercera Edición. Mc Graw-Hill. México. [Documento en línea]. Disponible en: [http://catarina.udlap.mx/u\\_dl\\_a/tales/documentos/lad/barria\\_k\\_e/capitulo3.pdf](http://catarina.udlap.mx/u_dl_a/tales/documentos/lad/barria_k_e/capitulo3.pdf); (fecha de consulta: 01/10/2010).

Hess A. Cristian. Hacia el Procedimiento Electrónico, Administrativo y Judicial. Ponencia al VII Congreso Iberoamericano de Derecho e Informática. [Documento en línea]. Disponible en: <http://www.hess-cr.com/secciones/dere-info/proced.html>. (fecha de consulta: 01/02/2010).

Ibermatica. Expediente Judicial Electrónico. La Justicia se Moderniza. [Documento en línea]. Disponible en: <http://www.ibermatica.com>. (fecha de consulta: 19/04/2011).

Jiménez, Carlos .E. *Interoperabilidad en la administración de justicia: Experiencias y buenas prácticas en un ámbito complejo*. Ponencia presentada en el XV Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública. Disponible en: [http://estratic.files.wordpress.com/2010/12/jimenez\\_io\\_justicia.pdf](http://estratic.files.wordpress.com/2010/12/jimenez_io_justicia.pdf). (fecha de consulta: 17/08/2010).

Jiménez Dan, Ricardo. *Suscritos Convenios para modernizar y dignificar la justicia en el país*. Sede del Tribunal Supremo de Justicia. 27 de abril de 2004. [Documento en línea]. Disponible en: <http://www.tsj.gov.ve> .(fecha de consulta: 15/05/2010).

Informes de Modernización Judicial en España. Expediente Electrónico Judicial. Ministerio de Justicia. [Documento en línea]. Disponible en: <http://www.oficinajudicial.justicia.es>. (fecha de consulta: 21/03/2012).

Juzgado Superior Décimo en lo Civil, Mercantil y Tránsito de la Circunscripción Judicial del Área Metropolitana de Caracas, en sede Constitucional. Sentencia N° 5.878. (Mary Luz del Carmen Lugo Betancourt vs. Sentencia dictada el 13/04/2009 Juzgado Tercero de Primera Instancia en lo Civil, Mercantil, Tránsito y Bancario de la Circunscripción Judicial del Área Metropolitana de Caracas). Disponible en: <http://www.tecniojuris.com/venezuela/jurisprudencia/constitucional/declarado-con-lugar-amparo-constitucional-por-violacion-del-derecho-a-la-defensa-por-uso-del-sistema-juris-2000-3096.html>; (fecha de consulta: 15/05/2010)

Juzgado Superior Noveno en lo Civil, Mercantil y del Tránsito de la Circunscripción Judicial del Área Metropolitana de Caracas. Exp. N° 8490. (Caso: Vicente Rios Castillo vs. Hippocampus Vacation Club, C.A) [Documento en línea]. Disponible en: [www.tsj.gov.ve](http://www.tsj.gov.ve). (fecha de consulta: 21/11/2010)

Lawyers Committee for Human Rights (U.S.), Programa Venezolano de Educación-Acción en Derechos Humanos. *El Banco Mundial y la reforma judicial en Venezuela. Estudio de caso: documento de trabajo preparado*

para la Conferencia de ONG sobre el Banco Mundial y la reforma judicial en Latinoamérica. Serie: Aportes N° 5. Provea. Caracas, 1996. . [Documento en línea]. Disponible en: <http://190.41.250.173/RIJ/BASES/PDFS/CAP4.pdf>. (fecha de consulta: 12/08/2010).

Lillo, L., Ricardo. *Informe: Buenas Prácticas en el uso de Nuevas Tecnologías en el Poder Judicial*. Centro de Estudios de Justicia de las Américas. 2010. [Documento e Línea]. Disponible en: [www.cejamericas.org](http://www.cejamericas.org). (fecha de consulta: 02/11/2011).

LOG FILE. [http://es.wikipedia.org/wiki/Redo\\_Log\\_File](http://es.wikipedia.org/wiki/Redo_Log_File). (fecha de consulta: 15/07/2010).

Madrigal J, Ricardo. *El Procedimiento Judicial Electrónico*. Revista de Derecho y Tecnología de la Información N° 3-2005. UNED. Costa Rica. [Documento en línea]. Disponible en: <http://www.uned.ac.cr/redti/tercera/documentos/>. (fecha de consulta: 21/11/2011)

Manrique, Isabel y Martínez Alexandra. (2009). *El acceso a la justicia en los Tribunales Civiles, Mercantiles, de Tránsito y Bancarios del área Metropolitana de Caracas* Trabajo de grado. Universidad Metropolitana. [Documento en línea]. Disponible en: <http://accesoalajusticia.org> (fecha de consulta: 27/08/2012)

Martínez, Rodolfo; Mateo, Miguel y Albert, María. *El uso de técnicas de investigación en línea: desde el análisis de logs hasta la encuesta electrónica*. [Documento en línea]. Disponible en: [http://www.ua.es/personal/rmg/publicaciones/ponencia\\_Martinez\\_Mateo\\_Albert\\_Granada.pdf](http://www.ua.es/personal/rmg/publicaciones/ponencia_Martinez_Mateo_Albert_Granada.pdf). (fecha de consulta: 13/03/2011).

Orta M, Raymond. Tecnología a media máquina en el poder Judicial venezolano. Noviembre 2009. [Documento en línea]. Disponible en: [www.tuabogado.com](http://www.tuabogado.com). (fecha de consulta: 12/12/2009)

Oxana. Lidia y Betancourt, Ricardo. Contrato Solemne. ¿Electrónicos? [AR: Revista de Derecho Informático](#), ISSN 1681-5726, [Nº. 117, 2008](#).

[Documento en línea]. Disponible en: <http://www.alfa-redi.org>.(fecha de consulta: 21/11/2010)

Peñaranda Q, Héctor R. La Firma Electrónica Digital en Venezuela. *Nómadas*. Revista Crítica de Ciencias Sociales y Jurídicas | 29 (2011.1). Universidad del Zulia. Venezuela. 2011. [Documento en línea]. Disponible en: <http://www.ucm.es/info/nomadas/29/hectorpenaranda.pdf>. (fecha de consulta: 01/03/2012)

Peñaranda Q, Héctor R. Propuesta para lograr la Notificación Electrónica en La República Bolivariana de Venezuela mediante un Sistema de Información Automatizado. Dirección Ejecutiva de la Magistratura. Disponible en: [http://www.ucol.mx/investigacionesjuridicas/archivos/2012/06/mar\\_283\\_notificacion\\_electronica.pdf](http://www.ucol.mx/investigacionesjuridicas/archivos/2012/06/mar_283_notificacion_electronica.pdf). (fecha de consulta: 27/08/2012)

Pérez, R. *Reforma judicial, Estado de Derecho y revolución en Venezuela*. (2003). [Documento en línea]. Disponible en: <http://www.accesoalajusticia.org/documentos/detalle.php?mrdstartid=10&catid=6>, (fecha de consulta: 10/07/2010)

*Poder Judicial de Costa Rica*. Evaluación del Plan Estratégico del Poder Judicial de Costa Rica 2000-2005. *Departamento de Planificación, Sección, Control y Evaluación*. San José Costa Rica. Mayo 2005. [Documento en Línea]. Disponible en: [http://www.poder-judicial.go.cr/planificacion/Informes\\_Relevantes/105.pdf](http://www.poder-judicial.go.cr/planificacion/Informes_Relevantes/105.pdf). (Fecha de consulta: 18/06/2011).

Processo Eletrônico. *Cooperação Internacional*. Carta de Fortaleza, Brasil. A Red Latinoamericana de Jueces - Redejal - editou. [Documento en Línea]. Disponible en: <http://www.processoeletronico.com.br/page4.aspx>. (fecha de consulta: 19/05/2012).

Rondón G, Andrea I. *Comentarios generales al Decreto-Ley de Mensaje de Datos y Firmas Electrónicas de la República Bolivariana de Venezuela*. [Documento en línea]. Disponible en: [http://www.ulpiano.org.ve/revistas/bases/artic/texto/RDUCV/123/rucv\\_2002\\_123\\_151-182.pdf](http://www.ulpiano.org.ve/revistas/bases/artic/texto/RDUCV/123/rucv_2002_123_151-182.pdf). (fecha de consulta: 03/05/2011).

SUSCERTE. [Documento en línea]. Disponible en: <http://www.SUSCERTE.gob.ve>. (fecha de consulta: 21/11/2011)

Superintendencia de Servicios de Certificación Electrónica "SUSCERTE". (2008, 01 de Julio). Infraestructura Nacional de Certificación Electrónica: Estructura, Certificados y Lista de Certificados Revocados. Recuperado el 11 de mayo de 2009 [Documento en línea]. Disponible en: <http://www.suscerte.gob.ve/images/Norma-032.pdf>. (fecha de consulta: 21/05/2011)

TEPUY XXI. [Documento en línea]: Disponible en: [www.cgr.gob.ve/pdf/.../ecotribunalsupremodejusticiasistema086](http://www.cgr.gob.ve/pdf/.../ecotribunalsupremodejusticiasistema086). (fecha de consulta: 18/08/2012)

Tribunal Supremo de Justicia. *Convenio de Cooperación Interinstitucional entre El Poder Judicial y el Ministerio De Ciencia Y Tecnología*. [Documento en línea]. Disponible en: <http://www.tsj.gov.ve>. (fecha de consulta: 17/06/2010).

Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 04-3055 de fecha 21 de marzo de 2006. (Alida Teresa Pernalette Gásperi vs. Erlinda Oropeza). Disponible en: <http://www.tsj.gov.ve>, (fecha de consulta: 15/05/2010)

Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 80 de fecha 01 de febrero de 2001. (Caso: José Pedro Barnola y otros). [Documento en Línea]. Disponible en: <http://www.tsj.gov.ve/decisiones/scon/Febrero/80-010201-00-1435%20.htm>. (fecha de consulta: 15/05/2010).

Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 2821 de fecha 28 de octubre de 2003. (Caso: José Gregorio Rivero Bastardo. Acción de Amparo) [Documento en Línea]. Disponible en: <http://www.tsj.gov.ve/decisiones/scon/Octubre/2821>. (Fecha de Consulta: 18/07/2011).

Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 721 de fecha 09 de julio de 2010 (Saco: Acción de Amparo. Parte accionante: Grecia

Figueroa). Documento disponible en: <http://www.tsj.gov.ve/decisiones/>. (fecha de consulta: 13/04/2011)

Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 224. (Edson Alejandro Rojas Rivas) Disponible en: <http://www.tsj.gov.ve>. (fecha de consulta: 18/12/2010)

Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 93 de fecha 06 de febrero de 2001. (Caso: Acción de Amparo. Corpoturismo). Disponible en: <http://www.tsj.gov.ve/decisiones/consulta>. (fecha de consulta: 08/09/2012)

Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 2403 de fecha 09 de octubre de 2002. (Caso: Amparo José Diógenes Romero). Disponible en: <http://www.tsj.gov.ve/decisiones/scon/Octubre/2403-091002-01-2813%20.htm>. (Fecha de consulta: 19/05/2011)

Tribunal Supremo de Justicia. Sentencia N° 2807 de fecha 14 de noviembre de 2002. (Caso: Hugo Roldán Martínez Páez. Amparo Constitucional).. Disponible en: <http://www.tsj.gov.ve/decisiones/scon/Noviembre/2807-141102-01-1573.htm>. (fecha de consulta: 18/04/2010)

Tribunal Supremo de Justicia. Sala Constitucional. Exp. 10-0224 de fecha 09 de julio de 2010. (Caso: acción de amparo constitucional interpuesta por el ciudadano Edson Alejandro Rojas Rivas). Disponible en: <http://www.tsj.gov.ve>. (fecha de consulta: 23/08/2010)

Tribunal Supremo de Justicia. Sala de Casación Civil. Sentencia N° 769 en fecha 24 de octubre de 2007. (caso: Distribuidora Industrial de Materiales, C.A., contra Rockwell Automation de Venezuela, C.A.). Documento disponible en: <http://www.tsj.gov.ve/decisiones/>. (fecha de consulta: 13/04/2011)

Tribunal Supremo de Justicia. Sala de Casación Civil. Sentencia N° RC.00294 de fecha 31 de mayo de 2005. (Caso: Roland Fetit Pifano contra Beatriz Coromoto Hernández de Fuentes) [Documento en línea]. Disponible en: [www.tsj.gov.ve](http://www.tsj.gov.ve). (fecha de consulta: 21/11/2010)

Tribunal Supremo de Justicia. Sala Electoral. Sentencia N° 26 de fecha 15 de abril de 2008. (Caso: Wolfgang Hernández, Pedro Figueredo y Julián Mendoza miembros de la junta directiva del Sindicato de Obreros y Empleados de la Industria de la Construcción y Conservación de Parques y Jardines y sus similares del Municipio Heres del Estado Bolívar. Recurso Contencioso Electoral conjuntamente con solicitud de Amparo Cautelar Expediente N° AA70-X-2008-000004). [Documento en Línea]. Disponible en: [http://www.tsj.gov.ve/decisiones/consulta\\_sala.asp?sala=006&dia=15/4/2008 &nombre=Sala Electoral](http://www.tsj.gov.ve/decisiones/consulta_sala.asp?sala=006&dia=15/4/2008&nombre=Sala%20Electoral). (Fecha de Consulta: 18/10/12).

Tribunal Supremo de Justicia. Sala Plenaria de la Comisión de Funcionamiento y Reestructuración del Sistema Judicial. Exp. N° 1773-PE-2009 de fecha 15 de diciembre del año 2009 (Amonestación a Herman Vásquez Flores, Titular del Juzgado Tercero Superior del Trabajo de la Circunscripción Judicial del Área Metropolitana de Caracas). Disponible en: [http:// http://www.tsj.gov.ve](http://www.tsj.gov.ve). (fecha de consulta: 15/05/2010).

Tribunal Supremo de Justicia. Sala Político Administrativa. Sentencia N° 01459 de fecha 12 de julio de 2001. (Caso: Alejandro Ramón Guedez E. vs. Ministro De Justicia). [Documento en Línea]. Disponible en: <http://www.tsj.gov.ve/decisiones/spa/Julio/01459-120701-01-0326.htm>. (fecha de consulta: 19/06/2010).

VENECONOMIA. Llegan las Firmas Electrónicas. Veneconomía Hemeroteca. [Documento en línea]. Disponible en: [www.veneconomia.com](http://www.veneconomia.com). (fecha de consulta: 03/07/2010).

### **Legislación Consultada.-**

Código Civil de Venezuela. Gaceta Oficial N° 2.990 de fecha 26 de julio de 1982.

Decreto Ley sobre Mensaje y Firma Electrónicas N° 1204 de fecha 10 de febrero de 2001, publicada en la Gaceta Oficial. 37.148 de fecha 28 de febrero de 2001.

Reglamento Parcial del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas publicado en la Gaceta Oficial N° 38.086 del 14 de Diciembre de 2004, bajo el Decreto N° 3.335 de Diciembre de 2004

Resolución N° 1475, publicada en Gaceta Oficial N° 37.810 de fecha 3 de octubre de 2003. Creación del Circuito Judicial Laboral.

Resolución N° 1484, publicada en Gaceta Oficial N° 37.810 de fecha 4 de noviembre de 2003. Creación del Circuito Judicial Penal.

Resolución N° 69, publicada en Gaceta Oficial N° 38.011 de fecha 30 de agosto de 2004. Creación de los Circuitos Judiciales de los Tribunales de Protección.

Resolución N° 70, publicada en Gaceta Oficial N° 38.015 de fecha 3 de septiembre de 2004. Creación de los Circuitos Judiciales en los Tribunales no Penales.

## GLOSARIO

**Autenticación:** Validación de la información de inicio de sesión de usuario.

**Autoridad de Certificación:** Entidad de confianza, responsable de emitir y revocar los certificados electrónicos, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública. Jurídicamente es un caso particular de Prestador de Servicios de Certificación.

**Acreditación:** Es el título que otorga la Superintendencia de Servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidos en el Decreto Ley de Mensajes de Datos y Firmas Electrónicas.

**Base de Datos:** Una base de datos o banco de datos (en ocasiones abreviada BB.DD.) es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

**Certificado Electrónico:** Mensaje de datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.

**Cifrar:** es el proceso de conversión de datos en un formato que no puedan leer otros usuarios.

**Clave Pública:** Es un conjunto de datos de carácter público que vinculan al remitente con el mensaje y que permiten cifrarlo.

**Clave Privada:** Es aquella combinación secreta que se utiliza para descifrar el mensaje y sólo la posee el receptor.

**Código Fuente:** Texto escrito en un lenguaje de programación específico y que puede ser leído por un programador.

**Criptografía:** es la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente inteligibles y posteriormente devolverlas a su forma original.

**Descifrar:** Declarar lo que está escrito en cifra o en caracteres desconocidos, sirviéndose de clave dispuesta para ello, o sin clave, por conjeturas y reglas críticas.

**Destinatario:** Persona a quien va dirigido el Mensaje de Datos.

**Dirección IP:** es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del protocolo TCP/IP.

**Emisor:** Persona que origina un Mensaje de Datos por sí mismo, o a través de terceros autorizados.

**Firma Electrónica:** 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.

**Logfile:** Fichero que registra cambios a la base de datos como resultado de transacciones o acciones internas del servidor.

**Login o password:** Propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada. Dicho de una cosa: Que se puede disponer libremente de ella o que está lista para usarse o utilizarse.

**Mensaje de Datos o Documento Electrónico:** Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

**Proveedor de Servicios de Certificación:** Persona dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en el Decreto-Ley de Mensajes y Firmas Electrónicas.

**Podcast:** Consiste en archivos multimedia (normalmente audio o vídeo, que puede incluir texto como subtítulos y notas) mediante un sistema de redifusión (RSS) que permita suscribirse y usar un programa que lo descarga para que el usuario lo escuche en el momento que quiera.

**Signatario:** Es la persona titular de una Firma Electrónica o Certificado Electrónico.

**Software:** Equipamiento lógico o soporte lógico de un computador digital.

**Usuario:** Toda persona que utilice un sistema de información.