

DERECHO Y TECNOLOGÍA

UNIVERSIDAD CATOLICA
DEL TACHIRA

2015

Vicerrectorado Académico
Decanato de Investigación y Postgrado

Número 1/2015 Edición Digital
Depósito Legal en línea: ppi201602TA4734
ISSN en Línea: (en trámite)

16/2015 Edición Ordinaria
Enero - Diciembre 2015
Depósito Legal: p.p 200202TA1209
ISSN: 1317-9306



Universidad Católica del Táchira
San Cristóbal - Venezuela

Derecho y Tecnología

Revista arbitrada de Derecho y Nuevas Tecnologías
Editada por el Vicerrectorado Académico
Decanato de Investigación y Postgrado
Universidad Católica del Táchira

Editor-Director

Mariliana Rico Carrillo

Consejo de Redacción

Rafael ILLESCAS ORTÍZ (Universidad Carlos III de Madrid); Isabel RAMOS HERRANZ (Universidad Carlos III de Madrid); Apolonia MARTÍNEZ NADAL (Universidad de las Islas Baleares); Leopoldo BRANDT GRATEROL (Universidad Católica Andrés Bello); Antonio SÁNCHEZ RODRÍGUEZ (Universidad Carlos III de Madrid); José Ovidio SALGUEIRO (Universidad Católica Andrés Bello); Miguel ARRIETA ZINGUER (Universidad Católica del Táchira); David LÓPEZ JIMÉNEZ (Universidad Autónoma de Chile); María PÉREZ PEREIRA (Universidad Carlos III de Madrid); Emilio SUÑÉ (Universidad Complutense de Madrid); José Luis BARZALLO (Universidad Andina Simón Bolívar de Ecuador).

Diseño Gráfico

Nina Gabriela Vásquez

Montaje

Edy Marleni Lozano

Identificación Legal

Depósito Legal: p.p. 200202TA1209
ISSN: 1317-9306
Deposito Legal en Línea: ppi 201602TA4734
ISSN: Está en trámite
Periodicidad: Anual

Publicación registrada en el *Catálogo Latindex*
www.latindex.org

Revista indizada en REVENCYT: Índice y Biblioteca Electrónica de Revistas Venezolanas de Ciencia y Tecnología. Código RVD012

Revista Derecho y Tecnología

Número 1/2015 Edición Digital - 16/2015 Edición Ordinaria

La edición impresa de la Revista Derecho y Tecnología llega hasta la N° 15 año 2014, por falta de papel. La edición correspondiente al 2015 será en digital y por disposiciones de la Biblioteca Nacional y su departamento de Depósito Legal se inicia la numeración en la versión digital desde N° 1, para efectos de la continuidad de la Edición Ordinaria es la N° 16.

Dirección:
Carrera 14 con calle 14
Apartado 366
San Cristóbal
Estado Táchira
Venezuela

Teléfonos:
(58) (0276) 344.75.72 -90.83
Fax:
(058) (0276) 344.61.83
E-mail:
derechoytecnologia@ucacat.edu.ve
mrco@ucacat.edu.ve

Distribución:
Universidad Católica
del Táchira
Apartado 366
San Cristóbal
Estado Táchira
Venezuela

Derecho y Tecnología

Revista arbitrada de Derecho y Nuevas Tecnologías
Editada por el Vicerrectorado Académico
Decanato de Investigación y Postgrado
Universidad Católica del Táchira

Misión

Derecho y Tecnología es una revista científica con periodicidad anual que tiene como misión difundir los trabajos de expertos nacionales e internacionales dedicados al estudio de los avances tecnológicos y jurídicos en general, con especial énfasis en las modificaciones que produce la aplicación de las Tecnologías de la Información y la Comunicación (TIC) en el campo del Derecho, fenómeno que ha dado origen al nacimiento de una nueva área de investigación jurídica.

En cada número se ofrece una publicación que contiene artículos doctrinales, recopilación de legislación nacional e internacional y la jurisprudencia nacional más destacada en la materia. La revista está dirigida a abogados, ingenieros, académicos, estudiantes y otros profesionales interesados en el estudio del impacto de las TIC en el ámbito jurídico.

A través de esta iniciativa editorial, la Universidad Católica del Táchira abre una vez más sus puertas a la investigación, con la finalidad de proporcionar un medio adecuado de difusión en esta área.



ÍNDICE

Artículos

Laura NAHABETIÁN BRUNET: Responsabilidad civil en el marco del Gobierno de la Información	9
Horacio FERNÁNDEZ DELPECH: La <i>Cloud Computing</i> . Una visión Argentina	47
Apolònia MARTÍNEZ NADAL: Las polémicas cláusulas de paridad en la contratación turística electrónica: ¿Prohibición absoluta o aceptación de cláusulas de paridad relativa?	65
Sulmer Paola RAMÍREZ: El contrato electrónico laboral	81
Nayibe CHACÓN GÓMEZ: La transferencia tecnológica: ¿Desarrollo de una política pública en Venezuela?	105
Gustavo Adolfo AMONI REVERÓN: Posibles soluciones a problemas de la audiencia de casación penal telemática	117
Erika Yamel MUNIVE CORTÉS: 2000 - 2015: 15 aniversario del Sistema Nacional e-México	143
Miguel ARRIETA ZINGÜER: Comercio electrónico y redes sociales: nuevo paradigma negocial	177

Conferencias

XIX Congreso Iberoamericano de Derecho e Informática. Federación Iberoamericana de Asociaciones de Derecho e Informática. Medellín, agosto 2015	
Lorenzo COTINO HUESO: Protección de datos y servicios públicos y privados de <i>Cloud Computing</i> en España y Europa	195
Jacqueline GUERRERO CARRERA: Democracia deliberativa y participación ciudadana electrónica	217

Olivia Andrea MENDOZA ENRÍQUEZ: Plataformas ciudadanas de participación como herramientas del ejercicio de la libertad de expresión en Internet	225
Marcelo BAUZÁ: Datos abiertos, ¿derecho humano?, ¿política pública? o ambas cosas	237
Natalia Soledad NOVAS; Jorge Alberto NOVAS; Humberto Félix RUANI y Humberto Martín RUANI: Historia clínica electrónica	253

Legislación

Unión Europea

Reglamento (UE) N° 524/2013 del Parlamento Europeo y del Consejo de 21 de mayo 2013 sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) n° 2006/2004 y la Directiva 2009/22/CE	265
--	-----

Jurisprudencia

Mariliana RICO CARRILLO: La posición del Tribunal Supremo de Justicia venezolano respecto a las pruebas documentales electrónicas	293
---	-----

Recensión

Selección y comentarios sobre bibliografía jurídica especializada.	
Horacio RANGEL GÓMEZ	303
<ul style="list-style-type: none"> • LASTIRI SANTIAGO, Mónica. <i>La comercialización del nombre de dominio</i>. Los bienes jurídicos digitales, el derecho de control y los nombres de dominio. Ed. Marcial Pons, España (2014), 352 pp. 	303
Mariliana RICO CARRILLO	311
<ul style="list-style-type: none"> • MARTÍNEZ NADAL, Apol.lonia. <i>El pago capitativo en la prestación de servicios médicos</i>. Civitas Thomson Reuters Aranzadi, España 2015. • KOZOLCHYK, Boris, Ph. D. <i>Comparative Commercial Contracts: Law, Culture and Economic Development</i>. West Academic Publishing, United States of America, 2014. 	311 315
Índice acumulado	333

DOCTRINA

Responsabilidad civil en el marco del Gobierno de la Información

Laura Nahabetián Brunet*

SUMARIO: 1. Introducción. 2. Responsabilidad civil. 3. El daño a la persona como lesión a derechos fundamentales. 3.1. La esfera íntima. 3.2. Enfoque integral de la persona. 4. Responsabilidad del gestor de una base de datos informatizada. 5. Responsabilidad civil del transmisor de información digitalizada. 6. Responsabilidad civil derivada del tratamiento de datos personales. 6.1. Responsabilidad civil contractual. 6.1.1. Responsabilidad del encargado de tratamiento de los datos frente al responsable de los mismos. 6.1.2. Responsabilidad del responsable de la base de datos respecto el titular de los mismos. 6.2. Responsabilidad civil extracontractual. 6.2.1. Tesis objetivista. 6.2.2. Tesis subjetivista. 6.2.3. Tesis mixta. 6.3. Extensión de la responsabilidad civil extracontractual. 7. Responsabilidad civil del principal por el hecho del dependiente. 8. Responsabilidad civil del funcionario público. 9. Actores en Internet. 9.1. Proveedores de acceso. 9.2. Proveedores de alojamiento. 9.3. Proveedores de contenidos. 9.4. Buscadores. 9.5. Usuarios. 10. Responsabilidad por contenidos publicados en la web. 10.1. El proveedor de servicios de Internet (ISP) como intermediario. 10.1.1. Proveedores de acceso. 10.1.2. Proveedores de alojamiento. 10.2. El ISP como organizador u editor. 11. Responsabilidad de los buscadores.

Resumen

En la actividad informática y telemática se verifican multiplicidad de posibilidades de existencia de daños que deberían originar su reparación; sin embargo, en la realidad

Recibido: 15/3/20150 • Aceptado: 18/4/2015

* Doctora en Derecho y Ciencias Sociales por la Facultad de Derecho de la Universidad Mayor de la República Oriental del Uruguay. Magister en Ciencias de la Legislación y Gobernanza Política por la Universidad de Pisa, República Italiana. Magister © en Derecho con énfasis en Derecho Constitucional por la Universidad Católica del Uruguay. Doctora © en Ciencias Jurídicas por la Universidad Católica Argentina. Docente universitario integrante del Instituto de Derecho Informático de la Facultad de Derecho de la Universidad Mayor de la República y del Departamento de Derecho Constitucional y Derechos Humanos de la Facultad de Derecho de la Universidad Católica del Uruguay. Inahabetian@gmail.com

las disposiciones normativas vigentes no siempre han considerado las posibilidades de existencia de daño y consecuentemente su resarcimiento adecuado.

Se efectúa en consecuencia un análisis integral de la responsabilidad civil emergente en una variedad de casos vinculados con la información personal, a partir de la consideración de los datos personales en tanto derecho fundamental, eventualmente vulnerado, la actuación de los diferentes sujetos que intervienen en Internet, en sus diferentes calidades.

La pretensión es analizar en clave de responsabilidad civil en distintas variantes, las situaciones que la realidad de la sociedad de la información plantea en el marco del emergente gobierno de la información.

Palabras clave: Responsabilidad civil. Daño. Información personal. Internet. Actividad informática.

Abstract

In computer and telematics there are lots of possibilities for damage that should cause liability. However, the regulatory provisions in force have not always considered the possibility of injury and consequently its adequate compensation.

A comprehensive analysis of liability arising in a variety of cases relating to personal information since the consideration of personal data as a fundamental right, eventually violated, and the rol of different people involved in Internet in its different qualities.

The aim is to analyze the liability in its different variants, considering the situations that the reality of the information society has in the context of emerging information governance.

Key words: Liability. Damage. Personal Information. Internet. Informatics Activity

1. Introducción

Las personas en tanto seres de relación, en el desenvolvimiento de su actividad intersubjetiva, permanentemente están en la posibilidad de incurrir en responsabilidad, ya que ésta es inherente a la vida social.

Una vez verificada, genera la obligación de indemnización del daño causado por la conducta y así el daño en su significado más simple, es un factor determinante y por tanto fundamento primario de la responsabilidad civil.

El daño es el presupuesto más importante del deber de reparar. Es el eje en torno al cual gira todo el fenómeno resarcitorio

... sin daño no hay responsabilidad. La teoría de la reparación de daños dirige su mirada precisamente al daño, por lo cual éste se constituye no solo en

el presupuesto básico sino que también fija la medida de la reparación. El perjuicio marcado marca el límite de la obligación indemnizatoria¹.

En la actividad informática y telemática se verifican multiplicidad de posibilidades de existencia de daños que deberían originar su reparación; sin embargo, en la realidad las disposiciones normativas vigentes no siempre han considerado las posibilidades de existencia de daño y consecuentemente su resarcimiento adecuado.

La información digitalizada como elemento base de la intercomunicación personal, atendiendo a los aspectos del flujo de información relacionada con la forma de transmitir iniciativas, realizar transacciones comerciales, formalizar ofertas y demandas, realizar campañas publicitarias comerciales, llegar a acuerdos, acercar posiciones, fomentar colaboraciones, incluso ratificar de manera formal acuerdos vía telemática, constituyen solamente algunos de los supuestos en los que la materia de responsabilidad de daños podría tener un tratamiento diferencial.

2. Responsabilidad civil

Los estudios acerca de la responsabilidad civil, generalmente parten de una consideración de tipo histórico, en tanto fenómeno jurídico, cuyas primeras manifestaciones se vinculan por tanto con la actividad humana.

Así desde la venganza privada como primera manifestación de la solución del daño de que fuera objeto la víctima, se pasa a la reparación del mismo, conjuntamente con la aparición del Estado y la configuración delictual en el Estado Romano².

Sin embargo, el término responsabilidad civil no se utilizó en Roma sino que su origen y significado responden al correspondiente a la etimología de la palabra responsabilidad cuya raíz latina *spondere* tiene como acepción prometer, comprometerse, ligarse como deudor. De esta forma, en Roma el compromiso incumplido, *spondere* derivaba en *respondere*, de donde –a su vez– se derivaba *responsus*, *responsum*, lo que conduce. Esta última, etimológicamente, se vincula con la idea de la responsabilidad relacionada con una relación jurídica preexistente³.

Así, la responsabilidad civil inició su perfilamiento desde que la autoridad calificó el hecho que causaba daños para los fines de su reparación, pero sin tratar de determinar si éste amenazaba o no el orden social, aunque siempre de

¹ Roberto VÁSQUEZ FERREYRA: *Responsabilidad por daños*, Editorial Depalma, Primera Edición, Buenos Aires, 1993.

² Hugo BUSTAMANTE: *Teoría General de la Responsabilidad*, Abeledo Perrot, Buenos Aires, 1986.

³ José DE AGUIAR: *Tratado de la Responsabilidad Civil*, Tomo 1, Editorial José M. Cajica, J.R.m.S.A., Puebla, 1957.

alguna forma implicara afectación. A partir de ahí es que en la evolución de la responsabilidad en tanto fenómeno jurídico en el Derecho Romano se inicia el camino de la diferenciación entre la responsabilidad patrimonial de la responsabilidad personal, sentándose de esta forma, las bases para la distinción de la responsabilidad civil de la responsabilidad penal.

La evolución de la responsabilidad jurídicamente imputable se fue perfilando de forma tal de dejar de ser una responsabilidad personal y ser una responsabilidad patrimonial, resultando consecuentemente de la responsabilidad civil pero no de la responsabilidad penal, que siguió siendo una responsabilidad personal.

Por lo tanto, mientras la responsabilidad civil fue siendo consecuencia de un daño causado, sin necesidad de la tipificación del evento dañoso que la generaba, la responsabilidad penal requirió del postulado, *nullum crimen sine lege, nulla poena sine lege*.

Se regularon asimismo, las obligaciones que nacían de aquéllas contraídas con anterioridad y de cuyo incumplimiento se irrogaba un daño, por lo que el sujeto constituido en deudor que no solventaba, asumía frente al acreedor la obligación de reparación del daño, mas siempre que la causa de la inexecución fueran el dolo o la culpa.

Aun cuando la distinción de la responsabilidad contractual y extracontractual no se delimitó con claridad en el Derecho Romano, es posible atribuir a la Ley de las XII Tablas el origen de la responsabilidad contractual y, a la Lex Aquilia, el de la responsabilidad extracontractual.

El Código Civil francés, desde 1804 planteó el tratamiento de la responsabilidad separando la responsabilidad por daños originados por el incumplimiento de una obligación, determinándola como responsabilidad contractual, y la responsabilidad por daños causados por delitos y cuasidelitos, en tanto responsabilidad extracontractual.

Para los dos tipos de responsabilidad determina el principio de la culpa para la imputación de responsabilidad, aunque ésta sola no es suficiente ya que si no se verifica el daño no es posible la admisión de la imputabilidad.

Hacia fines del mismo siglo, la jurisprudencia francesa, en materia de responsabilidad extracontractual, da un giro importante cuando introduce como variante de la responsabilidad cuyo fundamento es la culpa, la responsabilidad fundada en el riesgo de la utilización de artefactos peligrosos, determinando bajo este criterio, la obligación indemnizatoria basada en el hecho objetivo del daño causado⁴.

El tratamiento de la responsabilidad civil del Código francés fue seguida por la codificación civil del siglo XIX, tanto en Europa como América con un proyecto integral de reforma en el que la problemática de la responsabilidad

4 César ABELENDA: *Derecho Civil*, Parte General, Tomo 2, Astrea, Buenos Aires, 1980.

civil, contractual y extracontractual, es desarrollada de manera unitaria y con el criterio uniformador basado en el daño.

A fines también del siglo XIX con la finalización de la elaboración del Código Civil alemán, cuya vigencia parte en 1900, se produce una atenuación al criterio de la culpa y otorga preponderancia al daño, adoptando, para el efecto, un conjunto de disposiciones generales para su resarcimiento, motivando que sus doctrinos desarrollaran el criterio objetivo de la responsabilidad basado en el daño y sólo en la necesidad de un nexo causal⁵.

Su significativa influencia en la adopción del criterio objetivo, cuyo fundamento es el daño de la responsabilidad civil, el que se vincula con la teoría derivada del riesgo creado, ha determinado que la codificación civil pretendiera abandonar la teoría tradicional de la culpa, al menos en materia de responsabilidad extracontractual. Esta influencia determinó la inclusión de la delimitación de un principio rector cuya base se fundamente en el daño y su reparación.

Esto ha conducido al rebasamiento de los tradicionales lineamientos y la formulación de un Derecho de daños que, desplazando a la culpa como centralidad de la responsabilidad civil, de relevancia al daño como su presupuesto fundamental.

Sin embargo, la responsabilidad civil no puede resumirse únicamente en el daño, pese a que éste sea el factor determinante que obliga a su reparación. El daño causado por el incumplimiento de obligaciones, si bien es también el factor determinante de la obligación de repararlo, en ésta, se configura asimismo una responsabilidad civil, donde no se produce un desligue de los factores subjetivos del dolo y de la culpa.

En definitiva, la responsabilidad civil tiene dos regímenes diferenciados, el que regula el resarcimiento del daño causado por la inexecución de las obligaciones contractuales que vinculan al autor y la víctima y el que regula la indemnización por el evento dañoso que se constituye en la causa generadora de la relación jurídica que surge entre el autor y la víctima.

La etimología de la palabra responsabilidad determina que pueda indicarse que la referencia es al incumplimiento de lo prometido o a la violación de un deber jurídico.

En el Derecho Romano no se plantearon diferencias entre la responsabilidad objetiva y aquella subjetiva, en la medida que ésta se calificaba de manera objetiva tanto en la Ley de las XII Tablas cuanto en la Lex Aquilia, y solo se avanzó con la incorporación del carácter subjetivo al momento de la consideración de las especificaciones en el tratamiento de la inexecución de las obligaciones convencionales al introducirse la culpa.

⁵ Ennecerus KIPP Y WOLF: *Tratado de Derecho Civil. Derecho de las Obligaciones*, Tomo 2, Bosch, Barcelona, 1991.

El concurso de ambos órdenes de responsabilidad es el que fundamenta la necesidad de mantener el carácter unitario de la responsabilidad civil⁶.

En efecto, su fundamento puede ubicarse precisamente en que constituyen una fuente única de generación de la obligación de reparación del daño, siendo su origen la inejecución de un contrato o la existencia de un hecho imprudente que la determina, generando la violación del deber jurídico de no causar daño, que no es otra cosa que “el deber fundamental y síntesis de los demás deberes”⁷.

Lefebvre⁸ sostiene el carácter unívoco de la responsabilidad civil estableciendo que la obligación de reparación del daño, al igual que en la responsabilidad extracontractual nace de la ley y no de un acuerdo de partes.

La reparación del daño tiene su fuente –en ambos casos– en la existencia de un señalamiento legislativo en mérito a que en el caso de la responsabilidad contractual la obligación de tipo convencional incumplida es la que la disposición normativa de índole legal ordena reparar.

De esta forma, las dos responsabilidades tienen un origen común, que no es otro que una disposición legal, e igual fundamento, que no es otro que el daño.

Los Mazeaud, por su parte, han señalado que ésta surge en razón de la existencia de una violación a una obligación cuyo origen es o bien contractual o bien legal, siendo su conocimiento previo de carácter sustancial para la determinación del carácter de la obligación que origina la responsabilidad, esto es, si la referencia es a una obligación de tipo determinado o a una obligación general de prudencia y diligencia⁹.

En cualquiera de los dos casos, el que señala la necesidad de abstenerse del comportamiento lesivo para un tercero, es el deber jurídico del *neminem laedere*.

La unidad de la responsabilidad civil tiene asimismo fundamento en los planteos doctrinarios que remiten a la formulación de una teoría general del resarcimiento¹⁰ que es factible de aplicación de una forma uniforme, tanto en lo que refiere a la responsabilidad contractual como a aquella extracontractual y es alentada también con la formulación de un Derecho de daños, abarcativo de los problemas de los dos órdenes de responsabilidad.

La unidad de la responsabilidad civil, aglutina no solamente a aquellos hechos que la pueden generar, sino también, además de la antijuridicidad y la ilicitud, a aquellos hechos lícitos que pueden generarla.

6 Luis DIEZ PICAZO y Antonio GULLÓN: *Instituciones de Derecho Civil*, Vol. 1, Tecnos, Madrid, 1995.

7 L. DIEZ PICAZO y A. GULLÓN: *Instituciones de Derecho Civil ... op. cit.*

8 Según indicación de Fernando DE TRANZEGNIES: *La Responsabilidad Extracontractual*, Fondo Editorial de la Pontificia Universidad Católica del Perú, Lima, 1988.

9 Henri MAZEAUD y León MAZEAUD: *Lecciones de Derecho Civil*, Parte Segunda, Vol. 2, Ediciones Jurídicas Europa-América, Buenos Aires, 1959.

10 Eduardo BONASI: *La Responsabilidad Civil*, Bosch, Barcelona, 1958.

De ahí que se ubique en el daño su factor coadyuvante, pues lo importante para la responsabilidad civil, en tanto teoría y en tanto sistema, es la reparación del daño, con prevalencia de la víctima respecto del autor.

La conceptualización del daño como factor determinante de la responsabilidad civil ha determinado una ampliación del espectro de consideración de éste, incluyendo el daño a los derechos de la persona en cuanto tal, como la violación de su derecho a la intimidad o a la imagen, así como el denominado daño a la persona en sus diversas facetas.

Así es que la responsabilidad civil, sea de tipo contractual o de tipo extracontractual, tiene su fundamento en acciones u omisiones, dado que ambas son el resultado de la violación de obligaciones de hacer o de dar, o de obligaciones de no hacer. No hay que olvidar que éstas son el resultado de la violación del deber jurídico del *neminem laedere*.

Asimismo, debe considerarse el daño como factor determinante de la responsabilidad, el nexo causal, es decir, la relación de causalidad respecto del *eventus damni* y el sujeto al que se imputa la responsabilidad y por tanto obligado a la indemnización.

El daño se constituye en el centro alrededor del cual gravita la responsabilidad, no solo la lesión del patrimonio, sino también la de la persona en su integridad sicofísica. Ya no es necesaria la lesión de un derecho subjetivo, siendo resarcible la afectación de un interés simple o de hecho no reprobado por la ley. La compensación no consiste en algo ontológicamente equivalente, ya que se la busca a través de intermediarios como el dinero y se articula sobre la previsibilidad ordinaria de las consecuencias. No se da lo mismo perdido, sino que se lo calcula, se lo regula en función de una orden razonable, que no es de ningún modo el exacto reverso de lo perdido.

La antijuridicidad deja de ser formal y subjetiva, es material en cuanto es ilícito el comportamiento que menosprecia al ordenamiento jurídico en su conjunto, y no sólo a la ley. Es objetiva porque surge de la observación previa y primaria del acto, ajena a toda consideración de la subjetividad del agente.

La antijuridicidad se desprende también de la tipicidad, siendo innecesaria la descripción previa del ilícito. Surgen los actos ilícitos atípicos derivados de la violación del deber genérico de no dañar. Surgen también hipótesis de responsabilidad por actividad lícita.

El principio de que no hay responsabilidad sin culpa fue superado por la explosión de numerosos factores objetivos de atribución: el riesgo creado, la garantía, el abuso de derecho, la equidad o la culpa objetiva¹¹.

¹¹ Ricardo LORENZETTI: “Las nuevas fronteras de la responsabilidad por daños”, en *Responsabilidad civil derecho de daños Teoría General de la Responsabilidad Civil*, Editora Jurídica Grilley, Lima, 2006.

3. El daño a la persona como lesión a derechos fundamentales

La persona en tanto bien jurídico, es factible de protección desde los diferentes ángulos.

Así, la tutela resarcitoria es uno de los mecanismos provistos por el legislador, que a pesar que funciona frente a la existencia de un perjuicio que ya se ha producido, concede una indemnización.

En caso de considerarse que el daño es una lesión a un interés, es pertinente sostener que no hay un daño a la persona sino a la relación de disfrute que se motiva a partir del bien jurídico protegido. Mientras que si se entiende que el daño es el resultado del carácter antieconómico y antiespiritual, no habrá una identificación con la persona sino con las repercusiones que la lesión ha producido.

De esta forma, la determinación normativa de persona en tanto centro de imputación de derechos fundamentales, con diferente extensión y contenido, se entiende tiene recepción desde las propias constituciones nacionales.

Así, en la afectación de derechos puede verse que algunos de ellos gozan de una protección inhibitoria y resarcitoria, otros verifican una tutela resarcitoria y otros pueden ceder frente a la consideración de lo público.

3.1. La esfera íntima

El derecho a la intimidad, en tanto derecho diferenciado aparece como el más reciente de los derechos individuales relativos a la libertad, ya que en las primeras declaraciones de derechos (al igual que en sus precedentes medievales, como la Carta Magna inglesa), el derecho a lo que hoy llamamos protección de la vida privada estaba subsumido en algunos de los derechos de la libertad. El dicho “mi hogar es mi castillo”, refleja el estado de espíritu correspondiente; pero después se hacía sentir la necesidad de una defensa más refinada a la vida privada, pues por encima de los muros del “castillo hogareño” se produjeron amenazas, antes desconocidas, para el último reducto de la vida privada, y a ello contribuyó decisivamente el progreso de las ciencias y las técnicas que con acciones, generalmente clandestinas, permiten intromisiones en los rincones más recónditos de la personalidad. Desde los teleobjetivos a los aparatos de escuchas telefónicas, nos llevan a la mente el escándalo del “Watergate” y al más reciente, llamado “la guerra de las escuchas telefónicas”¹².

En el ámbito de la intimidad, el sujeto se encuentra en el ejercicio pleno de su autonomía personal, mientras que si hablamos de privacidad es allí donde imperan en exclusividad los deseos y preferencias individuales, implica una condición indispensable para el ejercicio de la libertad individual.

¹² Valentín CARRASCOSA: “Derecho a la intimidad e informática”, en *Informática y Derecho* N° 1, UNED, Mérida, 1992.

Hay muchos... que desean saber quién soy yo... los cuales, aunque hanme oído algo o han oído a otros de mí, no pueden aplicar su oído a mi corazón, donde soy lo que soy. Quieren, sin duda, saber por confesión mía lo que soy interiormente, allí donde ellos no pueden penetrar con la vista, ni el oído, ni la mente¹³.

Desde el punto de vista jurídico, correspondería efectuar tres determinaciones:

- **Conceptualización objetiva del derecho a la intimidad:** se atiende a la esencia de la etimología de la palabra intimidad y coincide con lo que el Diccionario de la Real Academia indica por tal al establecer: “zona espiritual reservada o íntima de una persona o de un grupo, especialmente de una familia”. Este concepto tiene su origen en la doctrina alemana –teoría de las esferas o de los círculos concéntricos– en función de la cual el centro principal, lo más interior está constituido por lo íntimo, luego en una segunda capa se encontraría lo familiar, luego lo secreto o confidencial para al final llegar a una última esfera que constituiría lo público. No se tratará de esferas repartidas con exactitud sino que son variables y cada persona las configura en función de sus propias intenciones y en forma absolutamente libre. En el mismo sentido se pronuncia el Tribunal Constitucional español, al señalar que se trata de “...*la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener la calidad mínima de la vida humana*”¹⁴.

- **Conceptualización subjetiva del derecho a la intimidad:** será identificado con el denominado “derecho a la autodeterminación informativa”. Esto implicará: “*la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a su propia vida*”¹⁵. Así es que este concepto es identificable con una esfera de disponibilidad plena del individuo, siendo que será él mismo quien determine lo que debe o no estar reservado al conocimiento externo. El Tribunal Constitucional español, por su parte, establece que existe un ámbito propio de la vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás salvo que el interesado lo consienta.

¹³ SAN AGUSTÍN: *Confesiones*, Libro X, Obras de San Agustín, Madrid, 1956.

¹⁴ Tribunal Constitucional español.- Sentencia STC 231/1988, de fecha 2 de diciembre de 1988.

¹⁵ Tribunal Constitucional alemán: Sentencia relativa a la Ley de Censo y de Población. 1983. “*el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo, se sabe algo sobre él ... la libre eclosión de la personalidad presupone en condiciones modernas de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la trasmisión ilimitada de los datos concernientes a su persona*”.

Estos dos conceptos tienen plena incardinación con la evolución tanto de la idea, como del derecho a la intimidad. El concepto objetivo se identifica con la protección de un ámbito concreto del individuo, de su dignidad como persona y en esencia con la concepción de la intimidad como un derecho de defensa. El concepto subjetivo atiende al elemento de libertad como trasfondo de la intimidad. Es una extensión de la idea y del derecho de intimidad que alcanza no sólo a la defensa de un ámbito, sino a la posibilidad del individuo de intervenir en lo que es externo a él, pero que le afecta. Cada persona tiene derecho a controlar lo que de ella se conoce, los datos a ella relativos, y el ordenamiento jurídico debe establecer los mecanismos necesarios para que este derecho sea efectivo¹⁶.

- **Teoría del mosaico:** se trata de una construcción doctrinal de aparición relativamente reciente y que se debe a la necesidad de explicación de la protección de la intimidad individual frente a las amenazas producidas por las Tecnologías de la Información. En efecto, Fulgencio Madrid determina que

la teoría de las esferas no es válida, dado que hoy los conceptos de lo público y lo privado son relativos, pues existen datos que a priori son irrelevantes desde el punto de vista del derecho a la intimidad, pero que unidos unos con otros, pueden servir para configurar una idea prácticamente completa de cualquier individuo, al igual que ocurre con las pequeñas piedras que forman un mosaico, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado¹⁷.

Ahora bien, así como es correcto afirmar que el derecho a la intimidad refiere en una primera instancia a un espacio restringido de absoluta libre disposición de las personas, también lo es que su desarrollo efectivo se produce en relación con los demás tanto para su valor cuanto para compartirlo, en la medida que este derecho siempre reviste un carácter aperturista y abierto, ya que en él interviene un importante componente subjetivo que inexorablemente dependerá y, se verá a su vez modificado, de cada persona grupo o sociedad.

Por su parte, la privacidad constituye un conjunto más amplio de significación intrínseca pero que coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

Implica el conjunto de datos, hechos o situaciones reales que la sociedad no conoce y que se encuentran reservados al conocimiento y decisión del propio sujeto o de un pequeño grupo de personas, siendo que de ser divulgados o puestos a conocimiento de otros podría llegar a ocasionar perjuicios en el patrimonio o la moral de una persona o familia.

¹⁶ Lucrecio REBOLLO: *Introducción a la protección de datos*, SL DIKINSON, Madrid, 2008.

¹⁷ Fulgencio MADRID CONESA: *Derecho a la intimidad, informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984.

Es de resaltar el control que sobre los aspectos de su vida privada tienen el individuo y su núcleo familiar y que la autorización o consentimiento de la víctima no quita al dato el carácter de integrante de la vida privada, sino que elimina el carácter antijurídico de la intromisión cambiando las bases de una posible reparación del daño sufrido con la revelación, si se tiene que fue consentida¹⁸.

En definitiva es posible afirmar que la vida privada constituye un valor de tipo moral.

La protección de datos personales es un derecho fundamental de las personas, un derecho de nueva generación que forma parte de lo que la doctrina ha denominado cuarta generación de derechos humanos. Se encuentra especialmente vinculada con las nuevas tecnologías y con la globalización, con la libertad de expresión en la red y la libre circulación de información, con el acopio vertiginoso de información, con el manejo o manipulación de la información y también con la democratización en el acceso a la información¹⁹.

En definitiva se trata de una determinación que refiere a un derecho humano que es inherente a la persona en la medida que éstos no pertenecen a la persona, sino que son la persona, permiten identificarla o la identifican.

En efecto, es de sustancia la consideración de que este derecho es de configuración jurisprudencial ya que existieron una serie de sentencias que serán las que lo determinen como un nuevo derecho fundamental y con autonomía respecto del derecho a la intimidad.

En ese sentido, el fundamento quinto de la Sentencia del Tribunal Constitucional Español N° 292/000 determina:

La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada “libertad informática” es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

¹⁸ Henry TORRES: *Derecho Informático*, Ediciones Jurídicas Gustavo Ibañez Ltda., Bogotá, 2002.

¹⁹ Ana, BRIAN NOUGRÉRES: “De la protección de datos personales y la cooperación internacional”, en *Anuario de Derecho Informático* N° VI, Fundación de Cultura Universitaria, Montevideo, 2006.

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran²⁰.

Según el propio Tribunal Constitucional el objeto del derecho a la protección de datos alcanza:

...a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquéllos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo²¹.

En función de lo establecido, es importante entonces tener presente que el derecho a la protección de datos personales como derecho fundamental tiene su fundamento en el poder de disposición de los datos personales por parte de su titular y en que esos datos sean sometidos a tratamiento. Esto implica, en consecuencia, que quien trata los datos personales, lo está haciendo sobre datos de terceros ajenos, por lo que deberán utilizarse con control específico del respeto a los derechos del interesado. Esto determina, que sea necesario considerar que en el centro del tema se encuentra el respeto a la dignidad de la persona que es, en definitiva, el fundamento de la protección de datos personales. Asimismo, es un requisito fundamental para el ejercicio de otras libertades y

²⁰ Tribunal Constitucional del Reino de España, *Sentencia STC 292/2000*, de 30 de noviembre de 2000.

²¹ Tribunal Constitucional del Reino de España, *Sentencia STC 292/2000*, de 30 de noviembre de 2000.

para que su respeto sea garantizado. De esta forma, hay que considerar que la información que pudiera estar disponible sobre las personas podrá ser utilizada como una forma de restricción ilegítima de derechos como la libertad de religión, la libertad de asociación, el derecho al trabajo, entre otros.

Estos enfoques del derecho a la intimidad, a la privacidad y a la protección de los datos personales determinan que la regla de principio sea aquélla del principio de la autodeterminación, lo que provoca en forma inmediata la aplicación de una serie de reglas conexas tal el caso de “*in dubio pro libertatis*”.

Originalmente, la progresiva disponibilidad que se le fue reconociendo a la persona en este sentido, y su oponibilidad frente a terceros, fue determinando su consideración tal si se tratara del derecho de propiedad, motivo por el cual se le otorgó una protección similar. De ahí que surgiera una tutela de tipo inhibitorio –a pesar que hoy no se los considera como una propiedad sino como ínsitos en la condición de la propia persona–.

Asimismo, es necesario señalar que en relación con los derechos de las demás personas, en el ámbito de la privacidad y la protección de datos, rige el criterio del respeto recíproco. Kant afirmaba que es necesario tratar al hombre como un fin en sí mismo, reconocer la dignidad ajena y actuar de modo que lo que uno haga pueda ser elevado a la categoría universal del obrar²².

De esta forma se conceden indemnizaciones resarcitorias e incluso punitivas, al punto que es factible establecer que en este ámbito rigen:

- La regla de la autodeterminación y su oponibilidad frente a terceros.
- Toda invasión en estas esferas es ilegítima.
- Se conceden tutelas inhibitorias y resarcitorias.

3.2. Enfoque integral de la persona

En la pretensión de obtener una protección mejor para la persona, se destacan facetas que pueden ser pasibles de daño, tal el caso –y particularmente en este tema –de los denominados daño estético, daño biológico, daño a la vida de relación, daño a la intimidad personal, daño psíquico, entre otros.

Existen al respecto algunas teorías denominadas unificadoras que hacen el intento de incluir todos estos rubros dentro del concepto de daño moral, tal el caso de los Dres. Venturini y Gamarra quienes establecen que “*el daño moral absorbe la categoría de daño biológico porque éste se traduce en una alteración psíquica o violación de derechos inherentes a la personalidad que incluyen la integridad física como la salud psíquica o el honor*”²³.

22 Emmanuel KANT: *Fundamentos de la metafísica de las costumbres*, Editorial Porrúa, México D.F., 1990.

23 Beatriz VENTURINI: *El daño moral*, Fundación de Cultura Universitaria, Montevideo, 1992; GAMARRA, Jorge, *Tratado de Derecho Civil Uruguayo*, Tomo XXV, Fundación de Cultura Universitaria, Montevideo, 1994.

El Prof. Ordoqui por su parte, no comparte esta postura y afirma que generan un riesgo ante la ausencia de individualización específica que imposibilita una verdadera evaluación de los perjuicios que se ocasionaren.

Por su parte, Mosset Iturraspe ha indicado que los debates deberían plantearse en relación con la verdadera diferenciación entre los ítems a considerar en relación con los daños a la persona y no en vínculo con lo que denomina “*guerra de etiquetas*”²⁴.

De esta forma, no todo daño a la persona supone la existencia de un daño moral, o un daño a la vida de relación, sino que será necesario analizar los diferentes rubros a los efectos de determinar el monto que responda a la realidad del perjuicio causado.

Por su parte Viney ha destacado que la realización del avalúo de los perjuicios no puede ser global en tanto no permitiría el contralor de qué es lo que se ha considerado por parte del juez para arribar a determinado monto en la reparación.

Avaluar es efectuar una cuantificación económica de las consecuencias perjudiciales que un cierto hecho dañoso causó en la persona y éste debe presentarse con individualización de los ítems correspondientes a los efectos de evitar arbitrariedades en la resolución de los fallos judiciales.

De todas formas no debe perderse de vista que el principio general es que la reparación debe ser íntegra, que debe existir equivalencia entre el daño y la reparación. Y esto es así en mérito a que debe tenderse a restituir el equilibrio pre existente y no enriquecer injustamente al afectado.

4. Responsabilidad del gestor de una base de datos informatizada

Lo primero a determinar es qué debe entenderse por base de datos para luego avanzar en las responsabilidades emergentes del vínculo de personas e información con las mismas. En este sentido, puede establecerse que:

una base de datos es un depósito común de documentación, útil para diferentes usuarios y distintas aplicaciones, que permite la recuperación de la información adecuada, para la resolución de un problema planteado en una consulta ... La base de datos está formada por un conjunto de documentos. Estos documentos pueden ser objeto de propiedad de un tercero y éste tener derechos sobre ellos²⁵.

A partir de lo señalado, la primera cuestión es el derecho de los titulares de los documentos almacenados en la base de datos y la necesidad o no de su

²⁴ Mosset ITURRASPE, “El daño fundado en la dimensión del hombre en su concreta realidad” en *Revista de Derecho Privado y Comunitario* N° 1, Rubinzal – Culzoni Editores, Buenos Aires, 1992.

²⁵ Miguel Ángel DAVARA: *Derecho Informático*, Editorial Aranzadi, Primera Edición, Navarra, 1993.

autorización para que formen parte de la misma, teniendo en consideración que la información contenida en los documentos puede ser transmitida una vez archivada a diferentes usuarios mediante diferentes mecanismos de transmisión telemática de datos.

La divulgación de información no autorizada por parte del gestor de la base de datos puede originar daños al titular de la misma. Dependiendo de su naturaleza el perjuicio puede variar ya sea que se trate de información económica, financiera, de empresas o datos personales.

Una segunda cuestión a considerar refiere a las obligaciones que asumen los gestores de las bases de datos al suministrar información correcta en forma oportuna. En ciertos tipos de bases de datos como los de carácter legal es central que la información esté vigente y sea obtenible en forma oportuna, ya que una información derogada o modificada puede ocasionar daños a los usuarios.

Una tercera cuestión a tener en cuenta hace relación con las medidas que deben tomarse por parte del gestor de la base de datos en relación con la seguridad de los sistemas informáticos con la finalidad de evitar el uso indebido de ellos o el conocimiento no autorizado de la información contenida, lo que puede ocasionar perjuicios a los titulares de la información o los documentos almacenados en la misma.

A partir de lo señalado, es pertinente avanzar en la consideración de qué tipo de responsabilidad civil asumen los gestores de la base de datos.

En el ámbito de la responsabilidad contractual debe señalarse que quien opera una base de datos y ofrece sus servicios a terceros contrae obligaciones cuyo incumplimiento puede generar un daño resarcible.

En este sentido, se compromete básicamente a suministrar información correcta, lo cual implica un compromiso de actualización, de suministro oportuno y continuado, de manera que la información precisa se encuentre en poder del usuario cuando necesite utilizarla.

Salvador Bergel opina que

se trata de un supuesto de responsabilidad contractual objetiva, ya que el gestor del banco de datos asume una obligación de seguridad en cuanto al contenido, exactitud y periodicidad de la información que suministre. Esta obligación de seguridad es una obligación de resultados y por ende quien presta el servicio, solo se eximirá de responsabilidad en cuanto pruebe la culpa de un tercero por quien no debe responder o bien el caso fortuito extraño a riesgo propio del sistema computarizado²⁶.

Los gestores de la base de datos tienen frente a los usuarios una obligación de responder si es que han suministrado informaciones falsas, insuficientes, desactualizadas o tardías. Generalmente entre gestores y usuarios preexiste un

²⁶ Salvador BERGEL: "Informática y Responsabilidad civil", en *Informática y Derecho*, Vol. 2, Ediciones Depalma, Primera Edición, Buenos Aires, 1988.

contrato, en el cual se pactan cláusulas limitativas de responsabilidad, sobre todo en mérito a la posibilidad de utilización para un eficaz cumplimiento del contrato de todos los medios a disposición sin perjuicio de lo cual, razones ajenas al gestor, determinan que pueden generarse daños a un tercero.

La responsabilidad extracontractual constituye un tema central en materia de bases de datos. La posibilidad de que por su manejo distorsionado puedan ser conculcados derechos esenciales del hombre y se pueda afectar su privacidad, ha provocado una alerta generalizada que se traduce en la sanción de normas específicas y en la interpretación amplia de normas ya existentes, en función de esta nueva realidad ... en esta materia ... hay criterios que favorecen ... la utilización conjunta de los criterios subjetivos y objetivos delimitando el ámbito operativo de cada uno de ellos²⁷.

1. El criterio subjetivo cuyo fundamento es la culpa, tendría su ámbito de acción en la función preventiva, referida a los daños evitables o típicos. Estos posibles daños son diversos, su delimitación y reconocimiento puede realizarse de diferentes formas que van desde la posibilidad de controles de calidad de la información, la verificación de contratos con la autorización efectiva de los autores de la documentación o que éstos no vulneran la privacidad o hallar errores de ingreso de la información por digitación o utilización de scanners. En todos estos casos se aplica el criterio que establece que en caso de dolo o culpa que causa un daño a otro se está en obligación de indemnización.
2. El criterio objetivo de imputación valdría únicamente para el daño inevitable o imprevisible. Únicamente se podría asegurar una tutela sin fisuras de esta forma. El tema aquí pasa a ser la consideración de la actividad peligrosa o riesgosa a que las diferentes disposiciones normativas de responsabilidad se refieren y la determinación de si la gestión de base de datos puede considerarse tal.

En este sentido, cabe señalar junto a Bergel que:

...el avance de la tecnología informática ha hecho posible compilar información en cantidad antes no imaginable, procesarla en forma mucho más completa y sistemática y difundirla en contados segundos a un ámbito infinito. Ello genera un peligro potencial de daño por la eventualidad de difundir información distorsionada relativa a la persona. El solo hecho de figurar tal información en la base de datos, crea un peligro potencial de daño²⁸.

²⁷ S. BERGEL: "Informática y Responsabilidad civil" ... *op. cit.*

²⁸ S. BERGEL: "Informática y Responsabilidad civil" ... *op. cit.*

De esta forma, se verifica un supuesto en la actividad de compilación y tratamiento sistemático de información que no es peligrosa por su naturaleza sino por la forma de su utilización con tecnología informática.

5. Responsabilidad civil del transmisor de información digitalizada

En muchas empresas se transmiten datos entre computadores, terminales, estaciones de procesamiento de palabras y otros dispositivos, todos situados dentro de un área reducida como puede ser un edificio de oficinas o un campo universitario. En muchos casos las empresas tienen un proveedor que proporciona un procesador multiusuario y el equipo y programas necesarios para conectar estaciones a ese procesador. Pero en otros casos, las organizaciones optan por enlazar sus estaciones mediante el uso de un sistema de comunicaciones que se conoce como red de área local²⁹.

Además de la digitalización de la información puede transmitirse vía satélite, por comprensión digital, fibra óptica, entre otra multiplicidad de medios. La comprensión digital está referida a la posibilidad tecnológica de transmitir altos volúmenes de datos binarios en forma más compacta.

Así es que la seguridad de los datos y la responsabilidad de los daños ocasionados por su utilización indebida o digitalización, pueden recaer en el transmisor de la información.

Esta transmisión puede tener un origen de tipo contractual, y debe tenerse en cuenta que:

...la despersonalización del cumplimiento contractual, conforma una de las particularidades más destacables de la praxis negocial. Al usuario que contrata bienes o servicios le interesa, si el buen nombre, el grado de responsabilidad que ostenta la empresa en la plaza, pero desde ya, sabe que la efectivización de la prestación va a quedar en la mayoría de los casos en manos de dependientes o auxiliares de aquélla, de modo que acepta la superposición fáctica de estos últimos, que quedan insertados así, en la trama de ejecución del contrato de tal modo que sus conductivismos pueden llegar a incidir negativamente en el patrimonio del acreedor de la prestación. Es decir, que la inejecución total o parcial o la deficiente efectivización de las prestaciones que frustra el contrato, tiene sus causas en el comportamiento de quienes no están en realidad unidos por lazo jurídico alguno con el contratante perjudicado³⁰.

Si bien el principal responsable es el titular del servicio, esta responsabilidad también es compartida por el personal que hace posible esta transmisión de

²⁹ Donald SANDERS: *Informática: Presente y Futuro*, Ediciones Mc Graw Hill, México D.F., 1991.

³⁰ Juan VENINI: *Responsabilidad de Daños contractual y extracontractual*, Editorial Juris, Primera Edición, Buenos Aires, 1990.

información, tanto en la esfera misma del contrato como por los hechos propios. En relación con la responsabilidad extracontractual hay que tener presente los criterios indicativos de responsabilidad que determinan que quien tenga a otras personas bajo sus órdenes responde por el daño causado por éstos siempre que éste se hubiere producido en el ejercicio del cargo o en cumplimiento del servicio de que se trate.

Las posibilidades que ofrecen las computadoras a las empresas se pueden ampliar considerablemente si se enlazan varias estaciones de trabajo independientes para formar un sistema más grande. La capacidad de enviar y recibir mensajes y compartir información, programas y datos hace que la interconexión de computadoras sea una sabia decisión para las empresas³¹.

Así es que podrá utilizarse un sistema mixto de criterios de responsabilidad objetiva y subjetiva, con las particularidades propias del transmisor de la información.

6. Responsabilidad civil derivada del tratamiento de datos personales

La compilación sistemática mediante la aplicación de tecnología informática, ha producido, en pocos años, una verdadera revolución en muchas áreas de la actividad humana, llegando a deslumbrar por las posibilidades que se abren en variados campos. Paralelamente ha surgido una alerta sobre la gran aptitud evidenciada para provocar daños de muy diversa caracterización, que van desde los derechos de la personalidad a derechos patrimoniales. Esto señala el creciente interés en estudiar la responsabilidad civil, no solo reparadora sino preventiva³².

El tratamiento de datos personales puede viabilizar el surgimiento de una infinidad de daños y por tanto la consecuente responsabilidad civil que implicará la indemnización de los mismos.

Esto es así, tanto sea respecto de una persona con la que existe un vínculo de índole contractual cuanto respecto de una persona ajena a una relación de este tipo con el responsable o usuario de una base de datos.

La manipulación de datos sensibles o nominativos que pueden tener lugar en las bases de datos, donde éstos se analizan, se combinan y se pueden distorsionar, determina que esta actividad se deba catalogar como riesgosa, dado que todos estos actos son posibilitantes de daños. Es la naturaleza sistemática de la base de datos la que torna peligrosa su actividad y la que a su vez le impone un severo deber de seguridad en el cuidado de la información tratada³³.

31 Donald SANDERS: *Informática: Presente y Futuro*.

32 S. BERGEL: "Informática y Responsabilidad civil" ... *op. cit.*

33 Josefina ORAZABAL: "Base de datos, privacidad y responsabilidad civil", en *Actas del III Congreso Iberoamericano de Informática y Derecho*, Mérida, 1992, pág. 141.

La existencia de bases de datos ha hecho aumentar en forma considerable la amenaza potencial contra el derecho a la intimidad.

Dado que el daño irreparable que puede sufrir un individuo por la utilización y/o publicación indebidas de información sobre su intimidad es necesario que la protección se ejerza preferentemente de un modo preventivo y no solo o principalmente represivo³⁴.

Así, dependiendo del daño de que se trate podrá esgrimirse la existencia de responsabilidad civil contractual o responsabilidad civil extracontractual.

Asimismo, es importante señalar que las acciones de responsabilidad civil a los efectos de la indemnización de los daños y perjuicios causados, es factible que sean entabladas con absoluta independencia de la posible acción de habeas data que se podría interponer, ya que ésta tiene por finalidad la supresión, confidencialidad o modificación del dato de que se trata, pero no incluye la posibilidad de reclamar en la misma los daños y perjuicios sufridos.

En este sentido, por ejemplo en la República Argentina, la Sala I de la Cámara Contencioso Administrativa ha señalado:

... lo que interesa y basta para la admisión de la pretensión objeto del «sub lite» es que la información sea falsa respecto de los actores, se incurra o no en igual falsedad en relación a otras personas; la hipotética circunstancia de que la falsedad de la información respecto de los actores constituya un eslabón de una cadena de falsedades similares que pueda haber respondido a aquella ilícita finalidad –o a cualquier otro propósito–, podrá resultar relevante a los efectos de determinar el alcance de la eventual responsabilidad del banco en el juicio de daños y perjuicio que los accionantes afirman haberle promovido, cuestión totalmente ajena al marco de cognición permitido en esta vía excepcional y expedita del “habeas data” (G.D., O.D. y otro c. Banco Central de la República Argentina, 2000/08/10, DJ, 2001-1-764).

6.1. Responsabilidad civil contractual

Es posible encontrar dos supuestos de responsabilidad contractual:

- a) Contratación de prestación de servicios informatizados, en la cual el daño tiene su surgimiento entre el encargado del tratamiento de los datos y el responsable de los mismos.
- b) El daño surge en virtud de una relación contractual existente entre el titular de los datos personales y el responsable de un banco de datos en función del cual el primero accede a su inclusión en una base de datos, firmándose un convenio a esos efectos.

34 V. CARRASCOSA: “Derecho a la intimidad e informática” ... *op. cit.*

6.1.1. Responsabilidad del encargado de tratamiento de los datos frente al responsable de los mismos

En este tipo de contrato se verifica la existencia de dos supuestos fundamentalmente:

- a) La base de datos es utilizada para brindar el servicio y será propiedad de la persona que brinda el servicio.
- b) La base de datos que se utiliza es propiedad de la persona que recibe la prestación del servicio, la que habrá entregado la base de datos a su cocontratante para que con éste se le brinde el servicio contratado.

La contratación de estos servicios fundamentalmente se utiliza para el desarrollo de actividades de marketing directo, publicidad, actividades en las que será importante dirigirse a las personas que se encuentran, por sus características personales, cultura, posición económica, hábitos de consumo, sexo, edad, incluidos o etiquetados dentro de un determinado grupo en el que se ubican personas de similares características.

En ambos casos de contratación de la prestación de los servicios informatizados, en principio se está frente a una obligación –en función de la cual se prestará el servicio– que es de medios. Habrá una obligación tácita de seguridad que se ubica en manos del responsable de la prestación del servicio, el que además, en principio es un experto en la prestación de éste en tanto la forma de uso del banco de datos y la información en ella contenida no le son ajenos a su accionar profesional.

La obligación señalada determina la existencia de un deber de confidencialidad en vínculo con los datos ya que el banco de datos es de titularidad de quien brinda el servicio por lo que implica, asimismo, un deber de seguridad en relación con la exactitud y actualidad de los datos.

La responsabilidad por los daños causados a quien recibe el servicio debe considerarse objetiva o subjetiva en dependencia de la obligación que fuera incumplida y atendiendo a que sea ésta de medios o de resultados. La responsabilidad objetiva deriva, en principio, de los daños que ocurrieren en razón de la incorrecta información brindada en razón del servicio, como de la utilización ilícita de la base de datos entregada con la finalidad de la prestación del servicio.

Por otra parte, la responsabilidad subjetiva se verifica cuando la obligación incumplida no tiene relación directa con la utilización en sí misma de la base de datos, sino que consiste en el incumplimiento de alguna obligación de tipo contractual particular, como por ejemplo, el incumplimiento en relación con el envío de una determinada cantidad de publicidad en un determinado lapso de tiempo.

Siendo que el prestador del servicio se ubica dentro del ámbito de la responsabilidad civil contractual, se debe indemnizar, salvo estipulación contractual válida en contrario, tanto los daños verificados como consecuencia inmediata del hecho dañoso, cuanto aquéllos que se deriven en forma mediata prevista o previsible del hecho, en los casos en que la actuación se hubiere producido con malicia.

Hay que considerar también, los casos en que el damnificado pudiere hacer la opción –en los ordenamientos jurídicos en que existe esta posibilidad– entre el régimen de responsabilidad civil contractual y el extracontractual, en los que no es necesario la existencia de malicia para verificarse la obligación del responsable de indemnizar las consecuencias mediatas previstas o previsibles del hecho dañoso, siempre que la víctima opte por el ámbito de responsabilidad extracontractual.

Incluso también es factible la posibilidad de responder por los daños morales causados.

En el caso de la existencia de responsabilidad objetiva, solamente podrá verificarse una eximición total o parcial de la obligación de indemnizar los daños causados, si le fuere factible demostrar la existencia de culpa de la víctima o de un tercero por el que no tiene obligación de responder, o la presencia de caso fortuito o de fuerza mayor que lo eximan.

En cambio, en los supuestos de responsabilidad civil subjetiva también es factible eximirse de la obligación de resarcimiento probando la ausencia de culpabilidad, esto es demostrando un obrar diligente.

Ahora bien, debe incluirse entre los eximentes de responsabilidad, tanto en el caso de la responsabilidad objetiva, como en aquél de la responsabilidad subjetiva el impedimento ajeno a la voluntad del deudor. Éste se aplica siempre que no se verifiquen determinados supuestos o, en el caso de la responsabilidad objetiva, al tratarse de una obligación tácita de seguridad. Habrá eximición total o parcialmente de responsabilidad si se probare haber actuado diligentemente a cuyo fin debería acreditar haber adoptado las medidas de prevención razonablemente adecuadas.

Si el daño fuere consecuencia de una cosa riesgosa o de una actividad especialmente peligrosa, la única causal que podría invocarse y que debería probarse para eximir la obligación de reparación, sería la culpa del damnificado, no pudiendo liberarse de responsabilidad en caso de culpa de un tercero por el cual no deba responder, caso fortuito, fuerza mayor u otra causa ajena.

En los casos de responsabilidad objetiva, si se entiende que el daño cometido es consecuencia de una actividad especialmente peligrosa o de una cosa riesgosa, el resarcimiento del daño imputable podría tener límites que podrían llegar a ser cuestionados por inconstitucionales

6.1.2. Responsabilidad del responsable de la base de datos respecto al titular de los mismos

En caso que un particular consienta que sus datos personales sean incorporados a una base de datos con una determinada finalidad, la responsabilidad que surge para el responsable es de carácter contractual y objetiva, ya que existe una obligación tácita de seguridad en su persona, dada su condición de profesional en la materia, tanto en lo que hace a la seguridad de los datos, como en relación con el destino que se le asigne a éstos, o la utilización o tratamiento que se efectúe de los mismos.

Del tratamiento de estos datos pueden surgir multiplicidad de daños para su titular.

Los perjuicios pueden ser de diferente índole, a saber:

- Utilización con una finalidad diferente a aquélla para la que fueron recolectados.
- Cesión sin consentimiento o en contravención a la normativa vigente.
- Falseamiento de datos.
- Utilización en forma discriminatoria
- Bloqueo o supresión de datos con anterioridad al transcurso del tiempo establecido en la contratación.

Al existir una obligación tácita de seguridad, la responsabilidad del responsable de tratamiento es objetiva, por lo que sólo podrá ser eximido de responsabilidad en caso de demostrar la existencia de culpa de la víctima o de un tercero por el que no debe responder o la presencia de un caso fortuito o fuerza mayor que lo eximan de responder.

Además podrá probar su actuar diligente, esto es, la adopción de todas las medidas adecuadas y razonables para la prevención.

Por otra parte, salvo estipulación en contrario prevista por las partes, el responsable de tratamiento debe reparar los daños que sean consecuencia inmediata del hecho dañoso, así como resarcir también los que fueran consecuencia mediata, prevista o previsible, de dicho hecho.

Es importante tener en cuenta que en general, los contratos en virtud de los cuales los titulares de datos autorizan el tratamiento en bancos de datos, en general se regulan por estipulaciones establecidas unilateralmente por el responsable por lo que la interpretación que se realice debe ser restrictiva de todo tipo de cláusulas que impliquen disminución de los derechos del titular de los datos o de los supuestos que implicarían el surgimiento de responsabilidad civil a cargo del responsable de la base de datos.

También se debe indemnizar el daño moral causado al damnificado.

6.2. Responsabilidad civil extracontractual

En aquellos casos en que no exista relación contractual entre el damnificado y el banco de datos causante del daño, la responsabilidad del responsable de la base de datos será extracontractual.

Salvo excepciones, las disposiciones normativas vinculadas con la consagración del derecho a la protección de datos personales y *habeas data*, no contienen previsiones vinculadas con la responsabilidad civil emergente de la utilización y explotación de los archivos de datos por lo que hay que remitirse a las normas generales de responsabilidad establecidas en los códigos civiles.

En este sentido, se establece que:

...en materia de tratamiento de datos personales la tutela legal pone el acento en la prevención, ya que existe una estrecha relación entre su uso abusivo y la lesión a derechos personalísimos como la intimidad y la identidad, cuya afectación causa una aflicción a las emociones más profundas que las personas tienen sobre su propia estima e incluso puede incidir desfavorablemente en la valoración que sobre aquélla tienen los demás, lo cual difícilmente sea reparado mediante un resarcimiento material³⁵.

Sin embargo, las reglas generales de responsabilidad son en algunos países y en algunos aspectos, insuficientes para contemplar las situaciones difíciles que plantean las tecnologías. Así es que se entiende que estas reglas básicas deben ser adaptadas a las nuevas situaciones; únicamente de esta forma, las disposiciones normativas vigentes en materia de responsabilidad civil podrán aplicarse para la regulación de este fenómeno determinado por las tecnologías.

No es nuevo, en cualquier caso, la adaptación de la teoría general de la responsabilidad civil a fin de atender en forma adecuada los nuevos fenómenos sociales y las nuevas situaciones que se suceden.

Sin embargo, se considera que no es sobre abundante sino por el contrario positivo, el dictado de nuevas disposiciones normativas específicas que clarifiquen la situación, sobre todo, apuntando a la obtención de mayor seguridad jurídica.

Se verifica asimismo, la existencia de tres tesis vinculadas con la responsabilidad civil emergente de los daños ocasionados por el uso de archivos de datos.

6.2.1. Tesis objetivista

Esta tesis sostiene que la responsabilidad civil extracontractual del responsable de la base de datos personales es objetiva, por lo que únicamente se eximirá de su obligación resarcitoria si probara la culpa de la víctima, o de un tercero por el

³⁵ Alejandra GILS: *Régimen legal de las bases de datos y habeas data*, Editorial La Ley, Buenos Aires, 2001.

que no tiene obligación de responder, o la existencia de caso fortuito o fuerza mayor en tanto eximentes.

Algunos autores entienden que los daños derivados de la utilización de bases de datos están comprendidos en el régimen establecido para las cosas riesgosas o vicios e indican que ello se debe a que a la informática deben aplicarse las disposiciones establecidas para las cosas.

La informática, representa una nueva forma de energía. El tratamiento automatizado (computarizado) de la información, comporta la utilización para el almacenamiento, procesamiento y transmisión de los datos, de señales electromagnéticas a través de pulsos eléctricos, magnéticos, electro-ópticos, registros magnéticos, etc.³⁶

Otros autores fundamentan la responsabilidad civil extracontractual objetiva en el hecho de sostener que el procesamiento electrónico de datos constituye una actividad riesgosa debiéndose aplicar la teoría del riesgo creado.

Entonces bien, el tratamiento de datos personales que se realiza mediante la utilización de computadores puede incluirse dentro de las cosas riesgosas como dentro de las actividades riesgosas, ya que es una actividad riesgosa desarrollada a través de cosas riesgosas.

En cualquier caso, cabe señalar que independientemente de cuál sea el fundamento de la aplicación de esta teoría, el resultado final sería el mismo.

6.2.2. Tesis subjetivista

Esta tesis se fundamenta en el criterio establecido que indica que quien ejecuta un hecho siendo que por su culpa o negligencia ocasiona un daño a otro, está obligado a reparar el perjuicio ocasionado.

Esto se sintetiza en la indicación que establece que no hay responsabilidad sin culpa.

Así, el responsable de la base de datos responderá en forma civil si hubiera obrado con culpa o dolo.

En este sentido, Bustamante Alsina afirma que:

...tratándose del ámbito extracontractual, la responsabilidad sería subjetiva o sea que el factor sería la culpa o el dolo de quien opera el sistema automatizado o por cuenta de quien realiza la operación, pues por mucho que los tratamientos automatizados empleen cosas como los ordenadores o computadores y todos los elementos magnéticos que forman el sistema, la recolección de datos, el procesamiento de la información y el tratamiento por medios interconectados así como los programas e instrucciones del software o su resultado o información

³⁶ Gabriel STIGLITZ y Rosana STIGLITZ: *Responsabilidad civil por daños derivados de la informática*, Editorial La Ley, Buenos Aires, 1987.

final son obra de la voluntad y la acción del hombre. Por eso puede afirmarse que la responsabilidad se genera en el sector de la responsabilidad directa por el hecho del hombre con las cosas que le sirven de instrumento³⁷.

Siguiendo la teoría básica subjetivista, se debería concluir que será aplicable el principio básico que establece que quien alega la culpa o el dolo del otro tiene la carga de probarlo, motivo por el cual el damnificado debe acreditar tanto el daño sufrido como el obrar doloso o culposo del responsable de la base de datos para responsabilizar a éste, en forma civil por el daño sufrido.

La aplicación de este principio en materia de prueba ocasiona que la posibilidad de obtener la reparación e incluso a un responsable por el daño sufrido sea prácticamente imposible, ya que, al damnificado en razón de su materia y ámbito en el cual se habría generado el daño le resultaría muy dificultoso por un lado, ubicar al responsable y por otro, en caso de obtenerlo, la posibilidad de atribución y prueba de la culpa o dolo de este responsable de la base de datos.

La transformación de la sociedad tecnológica plantea nuevos retos al régimen tradicional de responsabilidad que fue elaborado en la vista a una trama en la que normalmente había una víctima y un autor del hecho dañoso que eran identificables. El creciente desarrollo de bases de datos que recopilan información sobre las personas y su retroalimentación a través de dispositivos de interconexión que a su vez integran redes de circulación de alcance internacional, crean dificultades peculiares relacionadas con la indeterminación del sujeto responsable y la ineptitud de una reparación posterior que siempre será tardía cuando el daño se ha producido sobre atributos esenciales de la persona humana que hacen a su dignidad³⁸.

Establecido lo anterior, debe indicarse que la forma de sostener esta postura es invirtiendo la carga de la prueba por aplicación del principio de la carga dinámica de las pruebas, de acuerdo con el cual cada prueba debe ser aportada por la parte que se halle en mejores condiciones para hacerlo. Será más fácil al responsable del banco de datos demostrar que actuó sin culpa y sin dolo, antes que al damnificado acreditar la culpa o dolo de éste, ya que el responsable es un profesional en la materia por lo que es más factible que tenga a su alcance las posibilidades que le habiliten a aportar la prueba pertinente y conducente.

Así, esta tesis puede sustentarse siempre que sea útil para establecer el régimen de responsabilidad civil extracontractual en materia de daños causados como consecuencia del uso de bancos de datos personales, si, una vez probado el daño se presume la culpa del responsable.

³⁷ Jorge BUSTAMANTE ALSINA: *La informática y la responsabilidad civil*, Editorial La Ley, Buenos Aires, 1987.

³⁸ A. GIL: *Régimen legal de las bases de datos y habeas data... op. cit.*

Siendo la culpa presumida, el responsable del daño debe probar la inexistencia de culpa de su parte para liberarse de responsabilidad, es decir, debe probar que actuó con la diligencia debida, que existió culpa de la víctima o de un tercero por el que no debe responder o existiere caso fortuito o fuerza mayor que lo eximan.

6.2.3. Tesis mixta

Sus defensores entienden que dependiendo de cada caso la responsabilidad civil extracontractual será objetiva o subjetiva.

La responsabilidad civil extracontractual será objetiva cuando se trate de daños causados por la cosa, actuando ésta en forma activa, debiéndose aplicar en tal caso lo establecido para las actividades peligrosas, mientras que será subjetiva cuando la cosa no intervenga automáticamente en la producción del daño, sino que lo haga respondiendo al actuar del operador.

No parece muy adecuada esta teoría para el supuesto de los daños derivados del tratamiento de datos personales, ya que sería muy difícil distinguir los supuestos para establecer en cada caso si la responsabilidad sería objetiva o subjetiva. Además, pareciera que en todos los casos, de alguna forma existe tanto un actuar automatizado de los computadores como un actuar humano.

6.3. Extensión de la responsabilidad civil extracontractual

En principio los daños sufridos por el titular de los datos serán morales, en mérito a que los bienes jurídicos protegidos serán la intimidad y la privacidad, ya que los datos incluidos en las bases de datos están directamente vinculados con la persona titular de los mismos. Esto sucede en los casos en que se incluyan datos que fueren falsos o erróneos, determinados como pertenecientes a una persona en una base de datos, o en casos de cesiones de datos efectuadas en contrariedad para con las disposiciones normativas y sin autorización del titular de los mismos, o en los supuestos en los que no se mantenga la confidencialidad de los datos, o éstos no fueren suprimidos o bloqueados cuando así deba procederse.

Alejandra Gils, establece que incluso *“el daño moral se presume en caso de ataque a la intimidad por la sola realización del hecho antijurídico que provoca la ofensa a las afecciones legítimas del sujeto perturbado y tornan exigible un resarcimiento”*³⁹. Este daño moral debe indemnizarse al titular de los datos personales que lo haya sufrido.

Si bien en principio los daños provenientes del tratamiento de datos personales afectan intereses extrapatrimoniales como la privacidad, la intimidad, el honor, la dignidad, también pueden generar afectación a intereses patrimoniales. Esto

39 A. GIL: *Régimen legal de las bases de datos y habeas data ... op. cit.*

sucede más frecuentemente cuando los daños deriven de un banco de datos cuyo destino sea la prestación de servicios de información crediticia. Asimismo, pueden generarse perjuicios económicos como consecuencia de daños emergentes de otro tipo de bancos de datos, ya que puede derivar la pérdida de un trabajo o la oportunidad de conseguirlo, la pérdida de clientes o de su reputación.

“El hecho ilícito no recae directamente en el patrimonio sino en un derecho de la personalidad, lo cual al producir un desmedro de la identidad de la persona implicada le puede causar una repercusión patrimonial”⁴⁰.

En aquellos casos de personas que han sido damnificadas por el tratamiento de datos fueren personas jurídicas, difícilmente podría sostenerse que éstas tienen intimidad, en tanto esto es una condición intrínsecamente humana. Así, la afectada únicamente podría invocar un perjuicio económico que se deriva de la afectación de su identidad, su buen nombre o su reputación.

Los daños deben ser indemnizados al damnificado por el responsable de la base de datos y éstos serán aquéllos derivados tanto como una consecuencia mediata como inmediata del hecho dañoso.

7. Responsabilidad civil del principal por el hecho del dependiente

Tanto en los casos de responsabilidad civil contractual cuanto en los de extracontractual, los daños pueden producirse por la actuación de una persona dependiente del responsable de una base de datos. En estos casos, el principal debe responder ante el damnificado por el hecho del dependiente.

En los casos de responsabilidad civil contractual, la obligación de responder del principal por los hechos del dependiente tiene su fundamento en la obligación de garantía que recae sobre el principal, mientras que en el caso de responsabilidad extracontractual, su fundamento está en que la obligación de reparación se extiende a quienes se encuentran bajo la dependencia del titular.

Bustamante Alsina ha establecido que:

...el principal debe asumir el daño ocasionado por su dependiente actuando en vista del fin fijado por aquél, o utilizando los medios puestos a su disposición, aunque hubiere actuado contra la prohibición del principal o con abuso de las funciones⁴¹.

La responsabilidad del principal por el hecho del dependiente se genera en la culpa *in vigilando* o *in eligendo* de este último.

Tanto en los casos de un tipo de responsabilidad como de otro, es objetiva, por lo tanto, el principal solamente se libera de su obligación de indemnizar a la

⁴⁰ A. GIL: *Régimen legal de las bases de datos y habeas data ... op. cit.*

⁴¹ Jorge BUSTAMANTE ALSINA: *Teoría general de la responsabilidad civil*, Editorial Abeledo – Perrot, Buenos Aires, 1993.

víctima en caso de demostración de la culpa de esta última, o de un tercero por el cual no debe responder, o la existencia de caso fortuito o fuerza mayor que lo eximan de responder.

De todas formas, el principal que hubiere pagado al damnificado por el hecho de un subordinado tiene derecho a reclamarle lo pagado.

8. Responsabilidad civil del funcionario público

La primera determinación a realizar es la relativa a qué debe entenderse por funcionario público. Los diferentes ordenamientos jurídicos establecen conceptualizaciones al respecto, con mayor o menos amplitud.

En términos generales, la coincidencia se verifica en torno a la determinación que indica que se trata de una persona que ejerce función pública en una entidad estatal, que ha sido integrado a través de designación u otro procedimiento legalmente establecido.

En este sentido, la referencia es a dos requisitos: a) ejercicio de funciones públicas, con independencia de su naturaleza y b) la actividad debe prestarse en entidades estatales, habiendo sido incorporado a través de los procedimientos que los ordenamientos jurídicos prevén a tales efectos.

Deben también considerarse comprendidos, en una noción amplia, aquellas personas que prestan servicios al Estado, hayan sido elegidos por la ciudadanía o designados por las autoridades competentes, cualquiera sea su jerarquía funcional y la función estatal que desempeñan.

En relación con la responsabilidad del funcionario público, se entiende la obligación de reparar económicamente los daños causados a terceros o al Estado, y que sean consecuencia de una acción u omisión culposa o dolosa.

En este sentido, este concepto de responsabilidad comprende en consecuencia:

- a) La existencia de un bien jurídico a ser protegido.
- b) El deber jurídico de adecuación de la actuación al orden jurídico.
- c) La obligación de soportar las sanciones civiles derivadas de la lesión provocada al bien jurídico que se protege.
- d) La existencia de procedimientos destinados a hacer efectiva la aplicación de tales sanciones y con ello el principio de juridicidad.

Indudablemente esta responsabilidad será de tipo extracontractual en mérito a que no será el resultado de ninguna obligación contractual incumplida. Ésta implica la existencia de una relación jurídica frente a otro sujeto que sufrió un perjuicio, ante el cual debe responder.

Es decir que se plantea esta situación dada la existencia de determinados hechos o actos que invaden la esfera jurídica ajena, verificándose un vínculo

entre la persona a quien pueden imputarse los hechos o actos y el sujeto jurídico cuyo derecho se reputa lesionado.

Quien se entienda es responsable civilmente, está obligado a la reparación, indemnizando el daño causado, encontrándose en el marco de una esfera de tipo pasivo, transfiriéndose el daño de la persona que lo sufrió a quien provocó el perjuicio.

La fundamentación de la obligación resarcitoria es el daño valorado como reparable, siendo su objetivo el aseguramiento de la integridad patrimonial de quienes fueron damnificados.

Ahora bien, es pertinente tener presente cuáles son los presupuestos de la responsabilidad civil del funcionario público:

- a) Acción u omisión: se requiere la intervención de un agente público, sea ésta de naturaleza activa o pasiva, debiendo tener un carácter antijurídico, en tanto acto contrario al ordenamiento jurídico.
- b) Culpabilidad: esto implica que la acción u omisión sea atribuible a la culpa o dolo del funcionario público, debiendo por tanto existir imputabilidad subjetiva.
- c) Daño: se trata de un detrimento en la esfera jurídica de un sujeto, ya que sin éste no habría responsabilidad civil, pues ésta implica la obligación de reparar un perjuicio.
- d) Nexo causal: es necesaria la existencia de una relación de causalidad entre conducta y daño, el que funciona como condición indispensable para que el perjuicio sea atribuido al funcionario público. El daño debe imputarse al sujeto que lo causa en tanto requisito necesario para la existencia de imputabilidad objetiva.

Ahora bien, cuando un funcionario pone su actividad a favor de la entidad pública de que se trate, no actúa como sujeto autónomo sino como un elemento que lo integra, por lo que puede afirmarse que es el Estado mismo el que actúa a través de la actividad de sus agentes.

El Estado no es concebible en forma aislada de sus funcionarios que lo hacen tangible frente a los administrados. Sus acciones u omisiones comprometen a la persona jurídica, consecuentemente si el servidor público actuó incorrectamente, no lo hizo o lo efectuó en forma tardía, estos extremos se atribuyen al Estado.

Entonces bien, así como el principal debe responder por los daños causados por sus subordinados, el Estado debe hacerlo por los daños causados por los funcionarios y empleados públicos en el ejercicio o en ocasión de sus funciones. Por tanto, esta responsabilidad se basa en una obligación de garantía y es objetiva.

El Estado únicamente se eximirá de responder en caso que exista culpa de la víctima o de un tercero por el cual no debe responder, caso fortuito o fuerza mayor que lo eximan de responder.

No es extraña la configuración de una importante cantidad de daños imputables al Estado en materia de tratamiento de datos personales, ya que el Estado tiene multiplicidad de bases de datos de todos los tipos y con diferentes finalidades. Por tanto, la potencialidad de daño de estos bancos de datos es exponencial. El Estado debe realizar las tareas y contralores necesarios para evitar que se generen daños a partir del tratamiento de datos personales efectuado por medio de sus bancos de datos.

9. Actores en Internet

La Red de redes genera una multiplicidad de vínculos y conexiones de diversa índole, entre ellas, aquéllas de naturaleza contractual y extracontractual son numerosas.

Los servidores –computadores centrales en el manejo de Internet– se conectan entre sí a través de canales de banda ancha de importante capacidad, lo que implica el uso de máquinas de gran capacidad y velocidad. Los usuarios comunes están imposibilitados de conectarse en forma directa a la Red; deben efectuarlo mediante los denominados proveedores de acceso (IAP).

9.1. Proveedores de acceso

Los proveedores de acceso a Internet son quienes prestan la infraestructura de conexión a través de un server conectado a un nodo.

Se trata de un servidor, al que se conectan los usuarios para obtener acceso a los múltiples servicios que ofrecen por el resto de los servidores de Internet.

Los proveedores de servicios en Internet (ISP) cumplen distintas actividades con focalización en los usuarios. Éstas se efectúan en forma aislada o conjunta, con diferentes articulaciones.

Puede identificarse a quien únicamente provee la red, esto es, la infraestructura técnica, a través de líneas telefónicas, cables coaxiales, fibra óptica, o antenas que establecen conexión con un satélite y viabilizan la vinculación del usuario con el proveedor de acceso. Este rol puede asimismo, ser desempeñado por el propio proveedor de acceso que tenga a disposición mecanismos técnicos de conexión entre la localización del usuario y el servidor.

9.2. Proveedores de alojamiento

El proveedor de alojamiento de las páginas web es otro proveedor. El *hosting* es un contrato por el cual el prestador del servicio concede a su cocontratante, a cambio del pago de un precio en dinero o en forma gratuita, el derecho al alojamiento de archivos informáticos en un servicio –que podrá ser propio del prestador o únicamente gozar de un derecho de uso sobre él–, que quedan a disposición del público. El prestador brinda el alojamiento sobre hardware propio

o ajeno, con software propio o ajeno y con diferentes combinaciones de esas modalidades como sobre el hardware propio y con software ajeno o a la inversa⁴².

Este derecho de alojamiento es libre cuando cualquier persona puede dejar un archivo –identificándose o no–, o limitado, en la medida que el prestador solamente permita que se dejen archivos por parte de personas determinadas y con autorización a esos efectos. Asimismo, se consideran abiertos o cerrados, dependiendo de las posibilidades de ingreso sin restricciones o debiendo colocar algún *password*.

Estos servicios pueden ser prestados sea por una única empresa o por varias.

9.3. Proveedores de contenidos

Los autores y los editores pueden ser quienes incorporen en forma directa contenidos de una web, así como también pueden hacerlo otros titulares de derechos que ingresan sus obras a la red, al igual que las empresas de software.

Tradicionalmente se clasifica a los contenidos en “propios” y “de terceros”; “ilícitos” y “nocivos”⁴³.

Los contenidos ilícitos refieren a informaciones o comunicaciones ilegítimas o ilegales que violan alguna disposición normativa cuyo destino es la tutela de derechos personalísimos, delitos informáticos (inobservancia de leyes marcarias, de propiedad intelectual, derechos de autor o delitos sexuales, tráfico de personas, racismo, pornografía infantil, entre otros).

El contenido nocivo se vincula con información o materiales que expresan opiniones o creencias políticas, religiosas, culturales y que pueden considerarse ofensivas respecto de terceras personas.

En este sentido, por ejemplo es interesante considerar el caso en que se declaró procedente la acción de daños y perjuicios interpuesta por una modelo, sobre la base de la exhibición de su imagen en una página web, dado que el consentimiento para difundir su imagen no había sido otorgado para Internet, sino para medios gráficos y filmicos, y éste no era suficiente, lo que implica requerir la autorización expresa para su uso.

9.4. Buscadores

Los denominados «buscadores» en Internet son servicios que facilitan enlaces a otros contenidos o incluyen en los suyos instrumentos de búsqueda de contenidos.

⁴² Carlos PARELLADA: *Responsabilidad por la actividad anónima en Internet*, Editorial La Ley, Buenos Aires, 2007.

⁴³ Mónica MARTÍNEZ: “Responsabilidad de los operadores de la red que en su interacción producen daños», en *Revista de Derecho Informático* N° 41. Consultable en: www.alfa-redi.org/rdi-articulo.shtml?x=1003

Su pertenencia es al género motores de búsqueda que son sistemas informáticos que indexan archivos almacenados en servidores web. Son bases de datos que incorporan en forma automática páginas web a través de robots de búsqueda en la Red. Al momento de pedirse información en relación con algún tema, el buscador desarrolla la búsqueda a través de palabras clave o con árboles jerárquicos y temáticos. El resultado es una lista de direcciones web en las que se mencionan temas relacionados con las palabras clave indicadas.

Otra especie son los índices temáticos, esto es, sistemas de búsqueda por temas o categorías jerarquizados, aunque también suelen incluir sistemas de búsqueda por palabras clave. Se trata, en definitiva de bases de datos de direcciones web elaboradas en forma manual, esto es, que hay personas encargadas de asignar cada página web a una categoría o tema determinado.

Su operatividad es en forma automática, y generalmente contienen más información que los directorios comunes de información. Sin embargo, estos últimos también han de construirse a partir de búsquedas preferentemente automatizadas o a partir de avisos dados por los creadores de páginas, esto último con la prevención de que puede ser limitativo. La mayoría de los buscadores internacionales importantes de utilización habitual y conocidos son del tipo *spiders*, que necesitan de muchos recursos para su funcionamiento; recorren las páginas para recopilar información sobre los contenidos de éstas. Al buscarse información en los motores, éstos consultan su base de datos y presentan resultados clasificados por su relevancia. De la web los buscadores pueden almacenar desde la página de entrada a todas las páginas. Cada cierto tiempo, los motores revisan las páginas web, y actualizan los contenidos de su base de datos por lo que no es poco frecuente que los resultados de la búsqueda estén desactualizados.

9.5. Usuarios

El usuario de Internet tiene la posibilidad de efectuar una serie de actividades, tales como integrarse en un espacio de conversación (chat), enviar correos electrónicos, fijar sus mensajes en un simple tablón de anuncios, entre otras acciones. Su identificación no es personal, sino técnica, en el sentido de que su computadora verifica la existencia de una dirección IP (*Internet Protocol*), que puede ser operada por cualquier persona que tenga acceso al lugar en que ella se encuentra.

Además, las IP pueden ser asignadas en forma aleatoria por el proveedor del servicio de acceso⁴⁴.

44 Fernando GALINDO: "La regulación de Internet", en *La Ley, Revista jurídica española de doctrina jurisprudencia y bibliografía* N° 18, EDILEXSA S.A., Madrid, 1997.

10. Responsabilidad por contenidos publicados en la web

Los acontecimientos que tienen lugar en Internet no suceden en los espacios territoriales donde los participantes o los servidores se encuentran físicamente ubicados. Para localizar estos hechos es que comúnmente se habla de ciberespacio.

Lo cierto es que se trata de un conjunto de informaciones codificadas binariamente que transita en circuitos digitales y redes de transmisión. El desarrollo de las Tecnologías de la Información y la Comunicación ha afectado profundamente las nociones de espacio y de tiempo, así como las de proximidad y de distancia.

En este contexto, se plantea la cuestión de a quién se imputa la responsabilidad por daño cuando un contenido en la web es ilícito o nocivo.

El problema del anonimato relativo de los usuarios y de los contenidos ilícitos y nocivos que éstos pueden publicar en la Red, es una de las principales preocupaciones que presenta a la responsabilidad civil la actividad de Internet.

Si es posible identificar al autor del contenido dañino no hay duda de que se aplican las reglas generales de la responsabilidad. Cuando ello no es posible, se debaten dos posiciones.

10.1. El proveedor de servicios de Internet (ISP) como intermediario

La postura que aparece como predominante en el derecho y la jurisprudencia comparados, sostiene que el ISP es un simple prestador de los equipos e instrumentos necesarios para la transmisión de información, motivo por el cual la regla es su no responsabilidad.

Los proveedores de servicios, salvo cuando revisten la calidad de autores del contenido, son meros intermediarios, que no tienen el control de los contenidos que se incluyen en sus páginas. Se determina que están, técnica y fácticamente, imposibilitados de desarrollar funciones de control, y que, en último caso, si fuera posible, su implementación incrementaría exponencialmente los costos del sistema.

A su vez se establece que constituiría una especie de privatización de la censura, ya que el proveedor de alojamiento debería juzgar la licitud o ilicitud o la nocividad de los contenidos propuestos.

También se afirma que es equivocada la aplicación de las normas referidas a los medios de comunicación, ya que Internet solo ofrece un recurso tecnológico, y que el proveedor del servicio de alojamiento no es un editor, en el sentido de la responsabilidad en la prensa.

Desde el punto de vista económico, se indica que un criterio de responsabilidad objetiva en cabeza de los proveedores de alojamiento puede concluir en una

concentración de la oferta en empresas capaces de soportar los costos de los incidentes⁴⁵.

Críticamente se agrega que influye en este criterio la mayor fuerza de convencimiento que ostentan los *lobbies* de los proveedores, frente a la debilidad de los consumidores de tales servicios⁴⁶.

Para esta posición solo cuando el proveedor de contenidos es el autor de la incorporación a la Red del contenido ilícito o nocivo que daña, su conducta tendrá las consecuencias por el hecho propio. En los otros casos, no es responsable quien solo puso el medio tecnológico a disposición del autor del daño.

10.1.1. Proveedores de acceso

La Directiva de Comercio Electrónico del Parlamento Europeo (Directiva CE 200/31) establece como principio la no responsabilidad por los contenidos. El artículo 12 establece que en los servicios de la sociedad de la información, consistentes en la transmisión en una red de comunicaciones de datos facilitados por el destinatario del servicio o en facilitar el acceso a una red de comunicaciones, no es posible la consideración del prestador de servicio de este tipo como responsable de los datos transmitidos. Este responde únicamente cuando los ha originado o modificado, o ha seleccionado los datos o sus destinatarios.

La actividad de transmisión y concesión de acceso “*engloba el almacenamiento automático, provisional y transitorio de los datos transmitidos siempre que ese almacenamiento sirva sólo para ejecutar la transmisión y que su duración no supere el tiempo razonable necesario*” para ello.

Esta disposición normativa se complementa con el artículo 13 sobre la denominada “memoria tampón (caching)”, que establece que al momento de prestarse un servicio de la sociedad de la información consistente en transmitir por una red de comunicaciones datos facilitados por el destinatario del servicio, el prestador del servicio no puede ser considerado responsable del almacenamiento automático, provisional y temporal de esta información. Esto es así siempre que éste fuera realizado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a su solicitud, a condición que el prestador de servicio no hubiere efectuado modificaciones en la información, verifique cumplimiento de las condiciones de acceso a la información, de las disposiciones normativas relativas a la actualización de la información, especificadas de manera ampliamente reconocida

⁴⁵ Giovanni RICCIO: “La responsabilidad civil de los proveedores de Internet”, en *Revista de Responsabilidad Civil y Seguros*, Madrid, 2002.

⁴⁶ Carlos PARELLADA: *Responsabilidad por la actividad anónima en Internet... op. cit.*

y utilizada por el sector, no interfiera en el uso lícito de tecnología ampliamente reconocida y utilizada por el sector, con la finalidad de obtención de datos vinculados con la utilización de la información.

Se requiere que actúe con prontitud para el retiro de la información que hubiera almacenado, o imposibilite el acceso a ella en cuanto tenga conocimiento efectivo de que la información ha sido retirada del lugar de la Red en que se encontraba inicialmente. Igual situación se verifica si conoce que se ha imposibilitado el acceso a información o que un tribunal o una autoridad administrativa han ordenado retirarla o impedir su acceso.

Esto es independiente que un tribunal o autoridad administrativa de conformidad con los sistemas jurídicos de los estados miembros, exija al prestador de servicios poner fin a una infracción o impedirla.

10.1.2. Proveedores de alojamiento

La Directiva Europea 2000/31, en su artículo 14, establece que cuando se preste un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio, el prestador de servicios no puede considerarse como responsable de los datos almacenados a petición del destinatario, si carecía de conocimiento efectivo en relación con la licitud de la actividad o la información de que se tratare. En relación con una acción por daños y perjuicios, no puede considerarse responsable si no tenía conocimiento de hechos o circunstancias por los que la actividad o la información revelaran su carácter ilícito. En igual sentido, se plantea la exigencia que en cuanto tenga conocimiento de estos elementos se actúe con prontitud para retirar los datos o hacer que su acceso sea imposible.

Esto no rige cuando el destinatario del servicio actúa bajo la autoridad o el control del prestador de servicios.

Por su parte, el artículo 15 determina que los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los artículos anteriores.

Sin perjuicio de lo señalado, si es factible la determinación de obligaciones tendientes a que los prestadores de servicios de la sociedad de la información comuniquen con prontitud a las autoridades públicas competentes, los presuntos datos ilícitos o las actividades ilícitas llevadas a cabo por destinatarios de su servicio o información que facilite la identificación de los destinatarios de su servicio con los que hayan celebrado acuerdos de almacenamiento.

En la ley española de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE) 34/2002, las disposiciones siguen los lineamientos de la Directiva, pero con algunas especificaciones. Se concreta que el “conocimiento efectivo” se verifica cuando un órgano competente declara la ilicitud de los

datos y ordena su retirada, o incluso cuando se imposibilita el acceso a ellos, o se declara la existencia de la lesión y el prestador conoce la correspondiente resolución.

Por otro lado, de acuerdo con lo preceptuado por el artículo 16 están previstos procedimientos de detección y retirada de contenidos que los prestadores deben aplicar en función de la existencia de acuerdos voluntarios y de otros medios de conocimiento efectivo que pueden determinarse.

En Estados Unidos, luego del debate ocurrido en algunos procesos por injurias en los que los tribunales recurrieron a veces a las reglas referidas a la responsabilidad editorial y otras veces a los habituales criterios de imputación fundados sobre la culpa, la *Communications Decency Act* estableció la no equiparación de los proveedores de servicios de Internet con los sujetos que operan en el sector de la prensa impresa. Sin embargo, en 1997, ésta fue declarada atentatoria contra la libertad de expresión consagrada en la Primera Enmienda y por tanto inconstitucional por la Corte Suprema Norteamericana, esencialmente porque se formuló de forma muy general al prohibir el acceso a sitios “con material considerado patentemente ofensivo e indecente”, un concepto demasiado ambiguo y vago, a una persona de 18 años; incluso se sancionaba con penas de hasta U\$S 250.000 y dos años de cárcel, a todo aquél que difundiera o colocara a disposición de menores de 18 años ilustraciones o textos patentemente ofensivos o indecentes en un foro on line de acceso público.

En los casos de violación de *copyright*, los tribunales determinaron en una primera instancia a las reglas de la responsabilidad refleja pero el legislador prefirió invertir las soluciones jurisprudenciales al dictar la *online Copyright Infringement Liability Limitation* que forma parte de la *Digital Millenium Copyright Act* de 1998, en función de la que los proveedores, que podrían ser llamados a responder por los ilícitos cometidos en la red, solo lo hacen a título de partícipes.

En Francia, la jurisprudencia planteó la cuestión en términos de responsabilidad objetiva, pero la Ley 200/719 optó por soluciones capaces de compatibilizar los intereses contrapuestos. El autor o editor de una obra que, a título oneroso o gratuito, ingresa a un sitio, con el consentimiento del que provee el acceso, es responsable civilmente por los daños que causen sus opiniones cuando éstos se generen. El proveedor que le permite el acceso podría llegar a ser responsable en forma concurrente, pero únicamente en determinadas situaciones.

El Código de Autoreglamentación de Italia de 1997, sienta un principio general en que establece que “*el proveedor de contenidos es responsable de la información que pone a disposición del público*”, aclarando que “*ningún otro sujeto de Internet puede ser considerado responsable, salvo que se demuestre su participación activa*”, determinándose que se entiende por participación activa cualquier participación directa que se verifica para con la elaboración de un contenido.

Alemania tiene una ley vinculada con los servidores desde 1997, modificada para receptar la norma comunitaria sobre comercio electrónico.

Se registró uno de los casos más célebres sobre responsabilidad de los prestadores de servicios informáticos que significó la condena del director de la *Compuserve* alemana, juzgado culpable por haber hospedado dos *news groups* utilizados por pedófilos para intercambiar imágenes.

Las disposiciones de la Ley sobre Proveedores Informáticos no fueron consideradas aplicables, ya que a juicio del tribunal, el proveedor debió conocer el contenido de los servicios ofrecidos en atención a la particularidad de los nombres utilizados - alt.sex, alt.erotica -.

10.2. El ISP como organizador u editor

Para otra corriente⁴⁷, el ISP es un editor de medios de comunicación, cuya responsabilidad es controlar el contenido de los mensajes y del sitio que otorga en alojamiento. La regla, por lo tanto, es la responsabilidad del ISP.

Se determina que así lo exige el carácter de organizador del servicio que reviste el ISP y su condición profesional, enfatizándose el beneficio económico que éste percibe por el desenvolvimiento de su actividad.

Por otra parte, se rebate el argumento de la privatización de la censura al indicarse que no funciona en materia de responsabilidad por los daños causados por la prensa siendo que los editores pueden disponer la publicación o no según sus propios criterios de prevención.

Tampoco se consideran válidas las dificultades técnicas ya que se admite en materia de responsabilidad por el hecho de un tercero que, en tanto no configuren caso fortuito ajeno, el alojador debe afrontar la responsabilidad, quedándole habilitado el recurso de repetición contra el autor.

Se señala que el principal responde por los hechos de sus dependientes aunque sean atribuibles únicamente a éstos, en tanto la función haya adquirido una relevancia causal de modo tal que el hecho dañoso –con alta probabilidad– no hubiera ocurrido sin la concurrencia de la función. Precisamente, en estos casos, entre la conducta del principal y el daño, la relación causal no muestra adecuación –en el sentido que no es la conducta del principal la causa del daño–, sino el carácter de condicio sine qua non; si la función no hubiere concurrido, el daño probablemente no se hubiere producido.

Es justificada entonces, la responsabilidad de quien ha puesto a disposición del mundo un medio para dañar; y mayor razonabilidad verifica cuando se considera que la organización del medio ha posibilitado la impunidad en razón de la falta de individualización del autor del acto dañoso.

47 C. PARELLADA: *Responsabilidad por la actividad anónima en Internet ... op. cit.*

11. Responsabilidad de los buscadores

Los buscadores –de acuerdo con la regla más extendida– no son responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que no tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan sea ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización. Teniendo este conocimiento, deben actuar con diligencia para suprimir o inutilizar el enlace correspondiente.

Por tanto, serían responsables si conocen la actividad ilícita que realiza un usuario que es abonado a su servicio y no retiran los datos o no impiden su acceso.

La Cloud Computing. Una visión Argentina

Horacio Fernández Delpech*

SUMARIO: I. Introducción. II. Características. III. Servicios. IV. Diferentes implementaciones. V. Ventajas. VI. Problemas que plantea la *Cloud Computing* en la República de Argentina. 1. Competencia, jurisdicción y ley aplicable. 2. Transferencia internacional de datos. 3. Niveles de seguridad ofrecidos. 4. Propiedad intelectual de los contenidos. 5. Garantías de responsabilidad.

Resumen

El presente artículo estudia la importancia actual de los servicios de *cloud computing* para empresas y consumidores, junto con la problemática que plantea su implementación desde el punto de vista jurídico en la República Argentina. Luego de un análisis general donde se describen las principales características de estos servicios y sus ventajas, se analizan aspectos relacionados con la jurisdicción, ley aplicable, la protección de datos de carácter personal en los casos de transferencias internacionales de datos y la propiedad intelectual de los contenidos, así como la correspondiente responsabilidad de los prestadores de este tipo de servicios.

Palabras clave: Computación en la nube. Problemática jurídica. Jurisdicción. Competencia. Propiedad intelectual. Transferencia de datos.

Abstract

This paper examines the current importance of cloud computing services for businesses and consumers, along with some legal issues originated by their implementation in Argentina. After a general analysis, which describes the main features of these services and benefits, legal issues like jurisdiction, applicable law, personal data protection in international transfers of data, and intellectual property are analyzed, along with the liability of providers of such services.

Keywords: Cloud computing. Legal issues. Jurisdiction. Intellectual property. Data protection.

Recibido: 20/9/2015 • Aceptado: 28/10/2015

* Abogado argentino, especialista en Derecho Informático, Profesor Universitario

I. Introducción

La *cloud computing* o computación en la nube, es un servicio que se presta a través de Internet y que consiste en la migración de las informaciones y actividades informáticas de una persona u empresa, a computadoras y sitios de *hosting* de un tercero, con quien se celebra un contrato a tal fin. Este concepto no es algo nuevo, ya que desde hace varias décadas se viene hablando de él como una nueva aplicación que se hace efectiva realmente hace unos pocos años

Estos sitios de terceros donde se aloja la información, se encuentran ubicados en lo que llamamos “*la nube*”, que es un espacio donde datos y aplicaciones de negocios pueden ser almacenados en forma remota, y a los que se puede acceder desde cualquier lugar vía web, sin necesidad de utilizar software y hardware de la empresa usuaria del servicio.

Con el avance en la implementación de este sistema las empresas dejan de comprar, instalar y administrar software en servidores propios, para pasar a manejarse a través de los servidores de terceros que se encuentran en la nube, y que se contratan. De esta forma se economizan gastos y se facilita como veremos la tarea de las empresas.

El Instituto Nacional de Estándares y Tecnología (NIST), nos dice que

El cómputo en la nube es un modelo que permite el acceso ubicuo, conveniente y bajo demanda de red a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que puedan ser rápidamente proveídos con esfuerzos mínimos de administración o interacción con el proveedor de servicios. Este modelo en la nube promueve la disponibilidad y se compone de cinco características esenciales, tres modelos de servicios y cuatro modelos de implementación¹.

La *cloud computing* se formaliza mediante un contrato que nos permite tener acceso a esa información y al software necesario, en cada oportunidad que se requiera.

En el *cloud computing* existe un proveedor del servicio con el que el usuario celebra un contrato que le permite hospedar sus archivos digitales en sitios de *hosting* del proveedor que se encuentran diseminados en diferentes lugares del mundo, y acceder a estos en cualquier momento, asimismo puede crear sus propias aplicaciones o usar de las aplicaciones que le ofrece el proveedor del servicio.

Debemos agregar que la exacta ubicación geográfica de las informaciones y datos que hemos subido a un sistema de *cloud* no siempre es posible determinarla, ya que en algunos casos la totalidad de la información es alojada en determinados servidores de la empresa de *cloud* que se encuentran

¹ National Institute of Standards and Technology.

geográficamente ubicados en un país determinado, pero en muchos otros casos, por diferentes motivos entre ellos cuestiones de costos, la información se fragmenta y se guarda en diversos servidores ubicados en lugares diferentes del mundo.

La *cloud computing* pareciera que tiene una reciente aparición, sin embargo ha sido el mecanismo usado ya desde hace años por las principales cuentas de correo electrónico, Hotmail y Yahoo entre otras.

II. Características

Conforme nos ilustra Julio Téllez Valdéz, en un reciente libro², las cinco características mencionadas en la definición del NIST son:

1. *Autoservicio a la carta*

Un consumidor puede abastecerse unilateralmente de capacidades de computación, como tiempo de servidor y almacenamiento en red, según sus necesidades, de forma automática, sin requerir la interacción humana con cada proveedor de servicios.

2. *Amplio acceso a la red*

Las capacidades están disponibles en la red y se accede a ellas a través de mecanismos estándar que promueven el uso de plataformas heterogéneas tanto ligeras como pesadas (por ejemplo, teléfonos móviles, computadoras portátiles y otros dispositivos).

3. *Reservas de recursos en común*

Los recursos computacionales del proveedor proponen servir en común a varios consumidores que utilicen un modelo de multiposesión, con diferentes recursos físicos y virtuales dinámicos y reasignados de acuerdo con la demanda de los consumidores. Existe un sentido de independencia de la ubicación física en la que el cliente generalmente no requiere tener control o conocimiento sobre la ubicación exacta de los recursos suministrados, aunque se puede especificar una ubicación a un nivel más alto de abstracción (por ejemplo, país, estado, o centros de datos). Algunos ejemplos de recursos son: almacenamiento, procesamiento, memoria, ancho de banda de red y máquinas virtuales.

4. *Rapidez y elasticidad*

Las capacidades pueden suministrarse de manera rápida y elástica, en algunos casos, de manera automática, para poder realizar de forma rápida el

² Julio TÉLLEZ VALDÉZ. *Lex Cloud Computing*. Estudio Jurídico del Cómputo en la Nube de México. ISBN 9786070240065 Videoteca Virtual del Instituto de Investigaciones Jurídicas de la Universidad Autónoma de México

redimensionado correspondiente. En cuanto al consumidor, las capacidades disponibles para abastecerse a menudo aparecen como ilimitadas y se pueden adquirir en cualquier cantidad y en cualquier momento.

5. *Servicio supervisado*

Los sistemas de nube controlan y optimizan el uso de los recursos de manera automática, utilizando una capacidad de medición en un cierto nivel de abstracción adecuado para el tipo de servicio (por ejemplo, almacenamiento, procesamiento, ancho de banda, y cuentas de usuario activas). El uso de recursos puede seguirse, controlarse y notificarse, lo que aporta transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

Debemos decir también, que con las características que la *cloud* aparece ahora, podemos considerarlo un nuevo paradigma que ha surgido y se ha desarrollado de forma tal en los últimos años que ha revolucionado el manejo y tratamiento de la información en las empresas.

Hasta no hace muchos años toda empresa debía tener equipos informáticos con una gran capacidad de almacenamiento y procesamiento de datos, para poder depositar allí toda la información que requería procesar, asimismo debía tener los programas de software necesario para poder procesar toda esa información. Con la aparición de la *cloud computing* el modelo cambia substancialmente, lo que importa ahora no es tener gran capacidad de almacenamiento y software, sino que se debe tener un rápido acceso a Internet, ya que toda la información de la empresa pasa a estar almacenada en archivos externos a los que se puede acceder vía Internet y usar y procesar, incluso con el software que el proveedor del servicio de *cloud* nos ofrece.

III. Servicios

Horacio Granero define la *cloud computing* como

...el sistema informático que ofrece la migración o la externalización de los equipos de computación y de los programas o las funciones de procesamiento de datos a un prestatario de servicios que otorga su almacenamiento a través de los servidores diseminadas sin identificación necesaria de su ubicación, por un precio determinado o determinable³.

Estos servicios se agrupan fundamentalmente en tres niveles diferentes

- La Infraestructura como servicio (IaaS)
- El software como servicio (SaaS)
- La plataforma como servicio (PaaS)

³ HORACIO GRANERO. Problemas legales de la «cloud computing» elDial.com - DC14B2. Publicado el 12/11/2010.

1. La infraestructura como servicio (IaaS)

Esta modalidad es posiblemente la más básica y usada. En ella el proveedor presta al usuario únicamente el servicio de hospedaje de archivos digitales, permitiendo que el usuario acceda a estos en forma remota y desde cualquier dispositivo, con la única condición de acreditarse mediante una clave.

De esta forma el usuario evita almacenar grandes cantidades de información y al mismo tiempo puede usar esa información él o sus autorizados desde cualquier lugar y en cualquier momento.

2. El software como servicio (SaaS)

En esta variante se suma a lo anterior, que se ofrece una amplia variedad de aplicaciones de sistemas operativos que el usuario puede ejecutar para su uso directamente desde la nube

3. La plataforma como servicio (PaaS)

En esta modalidad el proveedor del servicio, además de brindar el alojamiento a los archivos digitales, junto con una serie de aplicaciones de sistemas operativos para que sean usadas por el usuario, le ofrece también una plataforma para el desarrollo de aplicaciones informáticas.

IV. Diferentes implementaciones

Habitualmente se habla de cuatro modelos de implementación de la *cloud computing*, y al respecto me permito transcribir lo que Julio Téllez Valdéz nos dice:

...los modelos de implementación de los servicios en la nube pueden ser los siguientes:

a) Nube privada. Significa que la infraestructura de la nube es operada exclusivamente para la organización usuaria. Puede ser administrada directamente por dicha organización o por un tercero, y puede existir “on-premise” u “off-premise” (es decir, con los recursos informáticos ubicados en las mismas instalaciones de la organización, o fuera de ella, respectivamente).

b) Nube comunitaria. Significa que la infraestructura de la nube es compartida por diversas organizaciones usuarias, que usualmente da servicio a una comunidad en particular, que comparten requerimientos o propósitos comunes (ya sea de misión, requerimientos de seguridad, políticas, consideraciones de cumplimiento normativo, etcétera). La nube puede ser administrada por dichas organizaciones o por un tercero y puede existir on-premise u off-premise.

c) Nube pública. Significa que la infraestructura de la nube es disponible al público en general o a un gran sector industrial y es detentada por una organización que provee servicios en la nube.

d) Nube híbrida. Significa que la infraestructura de la nube está compuesta de una o más nubes (privada, comunitaria o pública), que se mantienen como entidades individuales, pero que están unidas por tecnología estándar o propietaria que permite la portabilidad de datos y aplicaciones.

En cuanto a su naturaleza jurídica, el servicio de *cloud* podríamos encuadrarlo como un contrato bilateral de servicios, ya que las partes asumen obligaciones recíprocas y es también de carácter oneroso.

Podríamos agregar que, en muchas oportunidades, es un contrato de adhesión, ya que se celebra entre algunas pocas grandes empresas que ofrecen el servicio y los usuarios en general.

Se ha dicho también que es un contrato de consumo, celebrado generalmente por medios electrónicos, y regido por la Ley de Defensa del Consumidor. Esto es correcto en la medida que el usuario contratante del servicio reúna las características de consumidor, que conforme el art. 1 de la ley 24240 de Defensa del Consumidor, ...re estos servicios y sus ventajas,as principales izan en general el funcioamos tenidos y la correspondiente responsabilidad en l “*es la persona física o jurídica que adquiere o utiliza bienes o servicios en forma gratuita u onerosa como destinatario final, en beneficio propio de su grupo familiar o social*”. En caso de empresas que no reúnan este carácter no puede calificarse a este contrato como un contrato de consumo, y consecuentemente no le rigen las normas de la Ley de Defensa del Consumidor

V. Ventajas

Todos los servicios que ofrece el *cloud computing* otorgan grandes ventajas a los usuarios, pudiendo resumirse las principales:

- No es necesario almacenar archivos digitales en la infraestructura del usuario, ya que todos esos archivos pasan a estar en la nube, en servidores del proveedor del servicio;
- Se reducen los costos de hardware y fundamentalmente de software del usuario;
- El servicio se puede utilizar tanto por el usuario que lo contrató, como por las personas que éste indique. Esto ocurre generalmente cuando se trata de empresas, en las cuales todos los empleados autorizados pueden acceder en cualquier momento, simultáneamente o no y desde cualquier lugar a la información almacenada en la nube y trabajar sobre ella, conforme lo que se ha llamado modelo de “multiposesión” (*multi-tenancy*).
- El acceso a los datos se efectúa desde cualquier lugar que tenga conexión a Internet;
- Es una solución a nivel de copias de seguridad, respaldo y *backup*;

- Los servicios de *cloud backup* permiten tener actualizadas automáticamente versiones anteriores de los datos, evitando problemas de almacenamiento y también de procesamiento;
- Los servicios de *cloud* poseen escalabilidad, que significa que el usuario puede crecer para responder a necesidades más exigentes. Esto es crucial sobre todo para las empresas. Con la nube, la escalabilidad está garantizada sin tener que invertir más de lo necesario en previsión de que las necesidades aumenten. Si un usuario de la nube necesita más o menos capacidad de proceso o de almacenamiento, el proveedor de la nube se lo facilitará casi en tiempo real. Eso optimiza los recursos en todo momento ya que se puede abastecer unilateralmente de diferentes capacidades de procesamiento, tiempos de utilización del servidor, etc. según las necesidades del cliente en cada momento.
- La *cloud* es una gran solución a nivel de gobierno electrónico, en donde cada vez se recurre más a ella, ya que es una herramienta muy poderosa para incrementar la eficiencia en la prestación de los servicios públicos y la administración pública, implicando grandes ahorros y aumentando la eficiencia de los servicios del estado

VI. Problemas que plantea la *cloud computing* en la República de Argentina

Pero así como existen ventajas, también existen posibles problemas que se deben analizar al resolver suscribir un contrato de *cloud*, fundamentalmente cuando se trata de proveedores de *cloud* extranjeros, como ocurre en la mayoría de los casos. Esos problemas están referidos a:

- Competencia, jurisdicción y ley aplicable;
- Transferencia internacional de datos en el marco de la ley de protección de datos personales;
- Niveles de seguridad ofrecidos;
- Propiedad intelectual de los contenidos
- Garantías de responsabilidad

1. Competencia, jurisdicción y ley aplicable

En caso de incumplimientos y la consecuente necesidad de litigar, nos preguntamos cuál es la competencia y jurisdicción aplicable, así como en qué forma resolvemos el problema de la elección de la legislación aplicable.

En general los proveedores de servicios de *cloud* extranjeros, establecen en los contratos la prórroga de jurisdicción a tribunales extranjeros en relación al usuario argentino.

Estas cláusulas de prórroga de jurisdicción deben considerarse en principio válidas, sin embargo, el art. 37 la Ley de Defensa del Consumidor al referirse a los términos abusivos y cláusulas ineficaces de los contratos de consumo, establece en su inc. B que se tendrán por no convenidas las cláusulas “*que importen renuncia o restricción de los derechos del consumidor o amplíen los derechos de la otra parte*”.

Debemos recordar también que el art. 36 de la Ley de Defensa del Consumidor que regula los contratos de consumo con entidades financieras y de crédito, establece que “*...será competente, para entender en el conocimiento de los litigios relativos a contratos regulados por el presente artículo, siendo nulo cualquier pacto en contrario, el tribunal correspondiente al domicilio real del consumidor*”.

Es de aplicación también a los contratos de consumo, la Resolución 26/2003 de la Secretaria de Coordinación Técnica, que fue dictada en el marco de la normativa de defensa del consumidor, y que establece que son consideradas abusivas las cláusulas de los contratos de consumo en las que

...se disponga que las acciones judiciales puedan entablarse en jurisdicción distinta del lugar del domicilio del consumidor al tiempo de la celebración del contrato, excepto cuando se disponga que la acción se entable en el lugar del domicilio real del consumidor al tiempo en que aquélla se inicie.

De allí que, si se trata de contratos de adhesión, en que la jurisdicción pactada, diferente de la argentina, resulte desfavorable para el usuario argentino por afectar una defensa efectiva de derechos previstos constitucionalmente o por implicar un ejercicio abusivo del poder de negociación, este podría al momento de confeccionar o cumplir el contrato, cuestionar la validez de la cláusula conforme las normas antes citadas, en la medida que se trate de un contrato de consumo regido por la ley 24240, conforme lo explicáramos en el punto II anterior.

Resalto que en nuestra opinión, la posibilidad de cuestionar la validez de esta cláusula debe tener un debido fundamento en la afectación de derechos previstos en la constitución e implicar un ejercicio abusivo del poder de negociación.

De más está decir que ello posiblemente provocaría un conflicto de jurisdicción de muy difícil solución, atento a la carencia de una normativa internacional al respecto

Otro problema se plantea con relación a la ley aplicable a estos contratos, ya que la mayoría de los proveedores de servicio de *cloud* establecen que los servicios convenidos se regirán por legislaciones de países extranjeros. Es así como los principales proveedores de *cloud* de EE.UU., establecen la aplicación de la ley de EE.UU.

Si bien la autonomía de la voluntad es aquí también totalmente válida a este respecto, las partes deben sujetarse a los principios del orden público internacional conforme al art. 14 del Código Civil, en particular su inciso segundo⁴.

También es importante tener en cuenta acá que el art. 21 establece que las convenciones particulares no pueden dejar sin efecto las leyes en cuya observancia estén interesados el orden público y las buenas costumbres.

Por último destacamos que la deslocalización de la información hace necesario preparar y contemplar en el contrato de *cloud* procedimientos adecuados a fin de lograr la validez jurídica de las evidencias electrónicas almacenadas en la nube.

Es conveniente en este sentido la creación de una base de datos central que refleje los archivos almacenados, el uso de la nube y en dónde se deben identificar los servidores que custodian los datos, qué tipo de datos y el uso que se realiza de los mismos de tal forma que en cualquier momento puedan ser aportados en un litigio con terceras partes.

2. Transferencia internacional de datos

Es importante destacar también que cuando entre los servicios que ofrece en el contrato el proveedor del servicio de *cloud*, se incluye la transferencia de datos personales a países extranjeros⁵, o se trata de empresas extranjeras en donde se presume que los datos serán transferidos al extranjero, se hace plenamente aplicable el art. 12 de la Ley 25326 de Protección de Datos Personales de la y el art. 12 del Decreto 1558 reglamentario de la ley.

El art. 12 de la ley establece:

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.
2. La prohibición no regirá en los siguientes supuestos:
 - a) Colaboración judicial internacional;
 - b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior;

4 Art. 14. Las leyes extranjeras no serán aplicables:

- 1° Cuando su aplicación se oponga al derecho público o criminal de la República a la religión del Estado a la tolerancia de cultos o la moral y buenas costumbres;
- 2° Cuando su aplicación fuere incompatible con el espíritu de la legislación de este código;
- 3° Cuando fueren de mero privilegio;
- 4° Cuando las leyes de este código, en colisión con las leyes extranjeras, fuesen más favorables a la validez de los actos.

5 Esta situación ha sido llamada por muchos flujo transfronterizo de datos

- c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;
- d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;
- e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Por su parte el art. 12 del Decreto 1558/2001 dispone:

La prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente la cesión.

No es necesario el consentimiento en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta. Facúltase a la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES a evaluar, de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional. Si llegara a la conclusión de que un Estado u organismo no protege adecuadamente a los datos personales, elevará al PODER EJECUTIVO NACIONAL un proyecto de decreto para emitir tal declaración. El proyecto deberá ser refrendado por los Ministros de Justicia y Derechos Humanos y de Relaciones Exteriores, Comercio Internacional y Culto.

El carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración de tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales.

Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales.

Conforme al juego armónico de estas normas legales, se hace necesario analizar, previo a la firma de un contrato de *cloud*, si el prestador del servicio es argentino o extranjero.

En el primer caso, si se trata de un proveedor argentino que no tenga prevista la transferencia de datos a servidores ubicados en el extranjero, no existiría problema alguno, ya que no serían de aplicación las normas referidas.

Pero por el contrario, si el proveedor del servicio es extranjero o se van a transferir datos a servidores ubicados en el extranjero, debemos analizar si corresponde a un Estado que proporciona un nivel adecuado de protección o no, ya que las normas mencionadas prohíben la transferencia de datos personales a países que no proporcionen niveles adecuados de protección, salvo que se de algunos de los casos especiales de excepción en que no rige tal prohibición y que menciona el art. 12 de la LPDP y el art. 12 de su Decreto reglamentario.

Hacemos presente que España, según lo dispuso la Dirección Nacional de Protección de Datos Personales (DNPDP) posee nivel adecuado de protección, por lo que en ese caso no existiría prohibición alguna⁶, pero por el contrario, EE.UU. no cuenta con tal beneficio pues no ha sido declarado por la Argentina como país seguro. En numerosos dictámenes la DNPDP ha sostenido que EE.UU. no posee un adecuado nivel de protección⁷.

Consecuentemente, en el supuesto que en el contrato con una empresa de EE.UU. se establezca la transferencia de datos personales al extranjero, o el contrato sea con una empresa que prevea la transferencia de datos a servidores en EE.UU, es de plena aplicación la prohibición del art. 12, quedando entonces en ese supuesto dos posibles alternativas:

1. Solicitar a los titulares de los datos personales a transferir su consentimiento expreso para tal transferencia, conforme al primer párrafo del art. 12 del Decreto Reglamentario, solicitud esta de difícil cumplimiento cuando se trata de bases de datos de muchas personas.

6 En Europa, la Directiva de protección de datos permitió que la Comisión Europea efectuara una investigación respecto de la protección ofrecida en los diferentes países, creándose así una "lista segura" de países que cumplen con los estándares a los cuales se los considera automáticamente adecuados. La República Argentina, no bien dictada la ley de Protección de Datos Personales 25326, fue incluida en esa lista, lo que se dispuso por el Dictamen 4/2002 y Decisión del 30 de junio de 2003 de la Comisión Europea. EE.UU. por el contrario no es parte de la lista, básicamente porque tiene un enfoque diferente a Europa con relación a la privacidad. Para solucionar este problema y poder transferir datos personales entre los EE.UU y los países miembros de la UE, en julio de 2000 la UE y el Departamento de Comercio de EE.UU. acordaron unos principios de protección de la información conocidos como *Safe Harbor*, que permiten a las empresas de EE.UU. transferir, almacenar o utilizar información personal sobre residentes en países miembros de la UE y, a la vez, cumplir con el criterio de nivel adecuado de protección que figura en la Directiva sobre protección de datos de la UE. Las empresas de EE.UU que cumplan con criterios *Safe Harbor* son consideradas por los países miembros de la UE y las organizaciones que operan en dichos países como entidades que cumplen con el criterio de nivel adecuado de protección de la mencionada Directiva.

7 Dictámenes DNPDP Nros: 248/05; 270/06; 008/08; 017/09; 028/09; 07/11;12/13, entre otros.

2. Establecer un marco contractual adecuado, en un contrato que debe ser aprobado por la DNPDP, que debe otorgar el permiso pertinente conforme al tercer párrafo del art. 12 del Decreto Reglamentario. La competencia de la DNPDP para entender en estas cuestiones resulta del art. 29 de la LPDP. Hago presente que para facilitar el trámite la DNPDP ha implementado un formulario especial, el certificado C 01⁸, y otorga el permiso pertinente al aprobar los contratos de transferencia que le son sometidos a su consideración.

Este contrato, como lo menciona Marcelo Temperini⁹ debe contener:

- Identificación del exportador y el/los importador/es de los datos;
- Indicar la ubicación de la base de datos;
- Definir como ley aplicable al tratamiento de datos del contrato de servicios a la Ley N° 25.326;
- Se precisen la naturaleza de datos personales que se transferirán;
- La declaración que el tratamiento de los datos se realizará en un total de acuerdo con los principios y disposiciones de la Ley N° 25.326;
- Indicar la finalidad a la que serán destinados dichos datos, verificando que cumpla con los requisitos del art. 4 de la Ley N° 25.326;
- Precisar las medidas de seguridad a las que se sujetará la transferencia y el tratamiento de datos personales, verificando que la misma cumpla con las pautas habituales del sector y con la normativa vigente;
- El compromiso del importador que los datos recibidos serán tratados en un todo y sin excepciones según las instrucciones del exportador y las disposiciones de la Ley N° 25.326, aceptando que se le apliquen las facultades de la DNPDP y respetando los derechos de los titulares de los datos conforme Ley N° 25.326, como ser los derechos de acceso, rectificación, actualización, confidencialidad y supresión;
- La declaración del importador manifestando que la legislación local aplicable no le impide cumplir con las obligaciones pactadas;
- La obligación de destruir, y en su caso reintegrar al exportador, los datos personales objeto de la transferencia cuando finalice el contrato;
- Se respetará la jurisdicción de los Tribunales argentinos por cualquier conflicto vinculado a la protección de los datos personales que afecte al titular del dato;
- El compromiso por parte de importador de no divulgar ni transferir los datos personales a terceros con excepción que: 1) se establezca de manera específica en el contrato o se requiera para la prestación de servicios de tratamiento, o 2) la cesión sea requerida por una ley aplicable o autoridad competente, en la medida que no excedan lo necesario en una sociedad democrática, es decir, cuando constituyan *una medida necesaria para la*

⁸ “Certificado C.01” de Aprobación de Transferencia Internacional

⁹ Marcelo I. Temperini. Marco Normativo de Protección de Datos Personales de Argentina en los Servicios de Cloud Computing. Publicado en http://www.elderechoinformatico.com/publicaciones/mtemperini/JAHO_CC_DP_Temperini.pdf

salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o administrativas, o la protección del interesado o de los derechos y libertades de otras personas, en cuyo caso deberán notificar de manera inmediata y por escrito al exportador para evaluar si dicha transferencia afecta las disposiciones de protecciones de datos personales locales y en consecuencia afecte la continuidad del contrato.

Todos estos requisitos los encontramos mencionados como cumplidos en numerosos dictámenes de la DNPDP que han aprobado contratos de transferencia internacional de datos con países que no proporcionan niveles de protección adecuados, en particular EE.UU.

Concluimos entonces que la cuestión relativa al nivel adecuado de protección de datos del país con el que firmamos un contrato de *cloud* o del país a donde serán trasladados los datos, es un tema importante a tener en cuenta, fundamentalmente en el caso de que ese país no haya sido declarado por la Argentina como con un nivel adecuado de protección.

3. Niveles de seguridad ofrecidos

Otro problema que puede plantear la *cloud* es el relacionado con los niveles de seguridad de la información que ofrece el sistema para los datos almacenados en la nube.

Este es uno de los principales problemas que presentan los servicios de *cloud*, ya que los titulares de la información que se transfiere a la nube tienen una total pérdida de control de esa información.

Debemos recordar que sin perjuicio que el art. 25 de la LPDP establece que cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación, el art. 25 del Decreto 1558 Reglamentario de la ley, establece que los contratos de prestación de servicios de tratamiento de datos personales deberán contener los niveles de seguridad previstos en la LPDP, en la propia reglamentación y en las normas complementarias que dicte la Dirección Nacional de Protección de Datos Personales, así como se debe mantener la confidencialidad y reserva de la información obtenida.

El art. 9 de la LPDP establece que el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado, así como que queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

Esta norma es de plena aplicación al proveedor de *cloud* con quien celebramos el contrato y tiende a prevenir la adulteración o pérdida que se puede producir de los datos personales transferidos a la nube.

La disposición 11 de la DNPDP establece las medidas de seguridad para el tratamiento y conservación de los datos personales contenidos en archivos, registro, bancos y bases de datos públicas no estatales y privados. Allí se establecen tres niveles de seguridad, básico, medio y crítico, conforme la clase de datos tratados, y para cada uno de estos niveles se establecen distintas medidas de seguridad

Consecuentemente, tal como lo explica Marcelo Temperini¹⁰, en el contrato que se firme con el proveedor de *cloud* se debe considerar especialmente:

- Prohibición de que la empresa proveedora utilice los datos personales para fines diferentes a los dispuestos en el contrato.
- Disponer expresamente que la empresa proveedora solamente procesará la información siguiendo instrucción y órdenes del titular contratante.
- Prohibición de que la empresa proveedora ceda los datos a terceros, ni aún para su conservación.
- Prever la supresión de los datos personales para el caso de finalización de la relación de servicios.
- Obligar a la empresa proveedora a tener implementada sobre los datos personales, los niveles de seguridad exigidos por la Autoridad de Control en la Disposición 11, así como a mantener la confidencialidad y reserva de la información tratada.
- Exigir la existencia de una política de seguridad con un análisis adecuado de riesgos e incidentes posibles.

Es importante dejar bien documentada la relación entre las partes, siendo el primer requisito la existencia de un contrato de prestación de servicios de tratamiento de datos personales, en el cual deberá aclararse que la empresa prestadora de los servicios se compromete a cumplir con los niveles de seguridad previstos en la ley, la reglamentación y las normas complementarias que dicte la DNPDP, como así también las obligaciones que surgen en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida.

Este tipo de compromisos sobre seguridad, confidencialidad y reserva no revisten mayores problemas para las grandes empresas que prestan esta clases de servicios. Por ejemplo, es el caso de Google, quien dentro de sus Políticas de Privacidad expresa que cumple los principios de privacidad y de garantía de seguridad establecidos a través del programa *Safe Harbor* de Estados Unidos, nivel que es suficiente para cubrir tanto las exigencias legales en materia de

¹⁰ Marcelo TEMPERINI. “Marco normativo de Protección de Datos Personales de Argentina en los Servicios Cloud Computing”. Publicación: Simposio de Informática y Derecho. Publicada en las *Jornadas Argentinas de Informática* N° 40 - 2011. ISSN 1850-2814.

datos personales de la Unión Europea, así como las de Argentina, que sigue el mismo modelo europeo¹¹.

Por lo demás existen varios estándares que se refieren a la seguridad de la información. Si bien ninguno de ellos se refiere expresamente al ámbito de la *cloud computing*, pueden ser usados en ésta, ya que son de aplicación general. Nos referimos a las Series ISO-IEC 27000, que comprenden los estándares desarrollados publicados por la *International Organization Standardization* (ISO) y por la *International Electrotechnical Commission* (IEC), a fin de proporcionar un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización pública o privada.

No obstante, la empresa u organización interesada en la migración de servicios a la nube, deberá asegurarse que la prestadora asuma y garantice estas obligaciones, ya que en caso de incumplimiento, como podría ser en el caso de fuga de información, será la empresa contratante quien debe responder ante los titulares de los datos personales.

Entre las demás obligaciones que señala la legislación, destacamos la prohibición de realizar algún tipo de cesión. Ello significará que la prestadora de servicios deberá realizar los procesos automatizados de manera personal, sin posibilidad de transferir la información tratada a un tercero, ni siquiera para fines de almacenamiento.

4. Propiedad intelectual de los contenidos

En materia de propiedad intelectual, debemos recordar primero que las obras de software se encuentran protegidas por el régimen de derechos de autor de la ley 11723, desde el año 1998 en que se dictó la ley 25036, que modificando el art. 1 de la ley 1173, incorporó expresamente a los programas de computación fuente y objeto, y a las compilaciones de datos o de otros materiales, dentro de las obras protegidas por el régimen de derechos de autor.

Conforme este régimen, solo el titular de una obra de software puede disponer de su obra y autorizar la reproducción de la misma. Esa disposición de la obra se ejerce fundamentalmente mediante el otorgamiento de licencias de uso.

¹¹ Estados Unidos adoptó una forma sectorial de regular, por lo que cuenta con varias normativas a nivel de estados y a nivel federal. Esta forma de regular no es bien vista por los europeos por la falta de generalidad y de principios mínimos establecidos para todas las clases de datos y para todos los sectores. Teniendo esto en cuenta es que los proveedores de servicios de *cloud* que quieran comercializar sus servicios en Europa deben inscribirse bajo un esquema llamado "*Safe Harbor*". Este esquema fue negociado en el 2000 entre USA y Europa para resolver la cuestión. De esta forma los proveedores pueden inscribirse bajo este esquema y comprometerse a cumplir con todos los principios de protección de datos. La lista de proveedores es pública y está disponible para ser consultada en cualquier momento. Trabajo de Investigación efectuado por Josefina Patiño en la Cátedra de Derecho Informático de la Especialización en Derecho de la Alta Tecnología de la Universidad Católica Argentina U.C.A., 2011 (no publicado).

En los servicios de *cloud computing*, el tema de la propiedad intelectual puede ser visto desde dos ángulos diferentes:

- Desde la protección de derechos de propiedad de la empresa proveedora del servicio, que nos provee un software que utilizamos en línea;
- Desde la protección de los derechos de propiedad del usuario contratante del servicio *cloud*, ya sea por un software propio o por cualquier información u activo intangible con derechos de propiedad intelectual que tiene instalado o incluye en el material que se sube a la nube.

En el primero de los casos, es habitual encontrar en los contratos de *cloud* celebrados entre el proveedor y el usuario, cláusulas de protección de los elementos de software o de otro tipo que se brindan a los usuarios.

Es así como encontramos en los contratos con las principales empresas de *cloud*, cláusulas que expresan:

Por el presente acuerdo, usted acepta que el proveedor del servicio de cloud o sus proveedores de licencias, son los propietarios de todos los derechos, títulos e intereses asociados a los Servicios, incluidos todos los derechos sobre la propiedad intelectual que actúen sobre ellos, independientemente de si los mencionados derechos están registrados o no y de donde existan. Asimismo, reconoce que los Servicios pueden contener información considerada confidencial por el proveedor del servicio de cloud y se compromete a no revelar dicha información sin el consentimiento previo de este.

Con relación a las licencias de software que posee el proveedor de *cloud* y que cede para su uso al consumidor del servicio, es común también encontrar cláusulas al respecto en donde se ceden al usuario la autorización para que pueda utilizar dicho software en forma limitada al objeto del contrato suscripto. Por ello la empresa proveedora del servicio regula en los contratos cuáles y con qué limitaciones son los derechos que cede al usuario para que este pueda utilizar en el servicio de *cloud*.

Con relación a la segunda cuestión planteada, o sea con relación a los derechos de propiedad intelectual del usuario contratante del servicio *cloud*, ya sea por un software propio o por cualquier información u activo intangible con derechos de propiedad intelectual que tiene instalado o incluye en el material que se sube a la nube, también deben ser contempladas en el contrato, ya que aquí también hay una cesión temporal sobre los contenidos que se subirán a la nube.

En algunos contratos de grandes empresa de *cloud* es común encontrar la siguiente cláusula:

11. Su licencia del Contenido(11.1 Usted conservará los derechos de autor y cualquier otro derecho que ya posea del Contenido que envíe, publique o muestre en los Servicios o a través de ellos. Al enviar, publicar o mostrar Contenido, estará concediendo a una licencia permanente, internacional, irrevocable, no exclusiva y que no está sujeta a derechos de autor para reproducir, adaptar, modificar, traducir, publicar, representar y mostrar públicamente, así como para distribuir, cualquier Contenido que envíe, publique o muestre en los Servicios o a través de ellos. Esta licencia se otorga con el único propósito de permitir a publicar, distribuir y promocionar los Servicios y puede revocarse para determinados Servicios, según lo estipulado en las Condiciones adicionales asociadas.

5. Su contenido. El proveedor de cloud no reclama la propiedad del contenido que usted proporcione en el servicio, excepto de aquél cuya licencia le haya concedido. El contenido seguirá siendo de su propiedad. El proveedor de cloud tampoco controla, comprueba ni aprueba el contenido que usted y otros usuarios pongan a disposición en el servicio.

Es importante destacar que, con relación a los derechos de propiedad intelectual del usuario contratante del servicio *cloud*, es conveniente que éste haya efectuado el depósito y registro de la obra que prescriben los arts. 57 a 64 la ley 11723¹², ya que ello garantiza los derechos sobre la obra y crea dos importantes presunciones *iuris tantum*:

- Que lo que se ha depositado y registrado constituye una obra intelectual.
- Que el depositante y registrante es el autor o editor de la obra según sea el caso.

5. Garantías de responsabilidad

Todo el que presta un servicio debe otorgar garantías sobre tal prestación y hacerse cargo de las consecuencias dañinas que el mismo pueda causar. Esto que parece tan simple y básico, muchas veces no lo encontramos en los contratos de *cloud*, donde por el contrario encontramos cláusulas en las cuales la empresa proveedora exime su responsabilidad en diversas circunstancias, por ejemplo por la eliminación o fallos al almacenar información de un usuario, así como por

¹² Los arts. 62 t 63 de la ley 11723 establecen que el depósito de las obras, hecho por el editor, garantiza totalmente los derechos del autor sobre su obra y los del editor sobre su edición. Tratándose de obras no publicadas, el autor o sus derechohabientes pueden depositar una copia del manuscrito con la firma certificada del depositante. Asimismo que la falta de inscripción trae como consecuencia la suspensión del derecho del autor hasta el momento en que la efectúe, recuperándose dichos derechos en el acto mismo de la inscripción, por el término y condiciones que corresponda, sin perjuicio de la validez de las reproducciones, ediciones, ejecuciones y toda otra publicación hecha durante el tiempo en que la obra no estuvo inscripta. No se admitirá el registro de una obra sin la mención de su pie de imprenta. Se entiende por tal la fecha, lugar, edición y la mención del editor.

los daños que puedan causarse de alguna forma por un mal tratamiento de la información.

Es por ello que es importante analizar detenidamente el contrato entre usuario y proveedor para eliminar o limitar estas cláusulas.

Muchas veces, cuando se trata de contratos con grandes empresas y en las cuales el usuario para a ser un adherente de ese contrato por cuando no posee poder de negociación, esas cláusulas perduran y le es difícil al usuario oponerse a estas limitaciones de responsabilidad.

Cuando el contrato de *cloud* reúne la característica de contrato de consumo, juegan todas las defensas del régimen de protección del consumidor, en particular el art. 37 la Ley de Defensa del Consumidor que al referirse a los términos abusivos y cláusulas ineficaces de los contratos de consumo, establece en su inc. B que se tendrán por no convenidas las cláusulas “*que importen renuncia o restricción de los derechos del consumidor o amplíen los derechos de la otra parte*”.

Es también importante recordar que el art. 40 de la Ley de Defensa del Consumidor establece que si el daño al consumidor resulta del vicio o defecto de la cosa o de la prestación del servicio responderá el productor, el fabricante, el importador, el distribuidor, el proveedor, el vendedor y quien haya puesto su marca en la cosa o servicio y que la responsabilidad es solidaria, sin perjuicio de las acciones de repetición que corresponda. Sólo se liberará total o parcialmente quien demuestre que la causa del daño le ha sido ajena.

Las polémicas cláusulas de paridad en la contratación turística electrónica: ¿Prohibición absoluta o aceptación de cláusulas de paridad relativa?

Apol·lònia Martínez Nadal*

SUMARIO: I. Introducción. Concepto y finalidad. II. Problemática jurídica. Valoración. III. Reacción empresarial. Posibles de vías de solución: 3.1. Iniciativas sectoriales. Las directrices de HOTREC: las prácticas equitativas en la distribución en línea. Eficacia. 3.2. El recurso al Derecho de la Competencia: denuncias nacionales como prácticas desleales. 3.2.1 Planteamiento general: distintas denuncias nacionales ante autoridades nacionales de competencia. 3.2.2 El caso alemán: Sentencia del Tribunal Superior de Justicia de Düsseldorf de 9 de enero de 2015. 3.2.3 La actuación coordinada de las autoridades de competencia de Francia, Italia y Suecia y su aceptación de los compromisos de Booking respecto de la cláusula de paridad. Hacia una cláusula de paridad relativa. 3.3. Intervención legislativa: la prohibición absoluta del legislador francés. IV. Conclusión

Resumen

En la actualidad es indudable la importancia económica de los contratos de colaboración entre las OTA (*Online Travel Agencies*) y los empresarios hoteleros para la comercialización por medios electrónicos de plazas de alojamiento. No obstante, en el marco de estos contratos de colaboración surgen problemas derivados de la situación de desigualdad de las partes que plantea la posibilidad de prácticas desleales. Una de las prácticas cuestionadas, a la que dedicamos este trabajo, es la imposición de las denominadas cláusulas de paridad en virtud de las que se prohíbe al hotelero vender a un precio inferior al pactado con la OTA por cualquier otro canal, tanto online como

Recibido: 30/10/2015 • Aceptado: 8/11/2015

* Catedrática de Derecho Mercantil. Universidad de las Illes Balears (España). Especialista en Derecho del Turismo y Derecho de las nuevas Tecnologías. Responsable del Grupo de Investigación "Derecho y Nuevas Tecnologías". Autora de nueve monografías, más de 70 artículos y capítulos de libro. Vocal adscrita a la Comisión General de Codificación para la elaboración de la nueva Propuesta de Código Mercantil español, donde ha sido responsable de la regulación de los contratos turísticos. apollonia.martinez@uib.es

offline. Estas cláusulas han sido objeto de distintos pronunciamientos restrictivos o incluso prohibitivos de su utilización. Al análisis jurídico de estas cláusulas, y a su presente y futuro, a la vista de estos pronunciamientos, dedicamos este trabajo.

Palabras clave: Turismo. Establecimientos de alojamiento. Cláusulas de paridad, OTA (*Online Travel Agencies*). Práctica desleal.

Abstract

Nowadays there is no doubt about the economic importance of contracts between OTA (*Online Travel Agencies*) and hotel owners for selling by electronic means accommodation places. However, under these contracts the possibility of unfair practices arise because of the unequal position of the parties. One of these practices is the imposition of so-called “parity clauses”: with these clauses the hotelier is prohibited to sell at a lower price than the price agreed with the OTA by any other channel, both online and offline. We have found different resolutions that restrict or even prohibit the use of the “parity clauses”. We dedicate this paper to the legal analysis of these clauses.

Key words: Tourism. Accommodation establishments. Parity clauses. Unfair practice.

I. Introducción concepto y finalidad¹

Las denominadas cláusulas de paridad, objeto de este trabajo, son cláusulas impuestas en muchos casos por los portales online de reservas de habitaciones (las denominadas abreviadamente OTA, siglas de *Online Travel Agencies*) a los empresarios de alojamiento turístico (en adelante también, y simplificada, hoteleros) y en virtud de las cuales aquellos impiden a estos dar mejores condiciones (básicamente, mejores precios) al cliente final u a otros portales online o incluso cualesquiera otros canales de venta.

También se denominan en la práctica del sector cláusulas “*Most Favoured Nation*” (MFN). En realidad, la expresión y denominación “cláusula de nación más favorecida” tiene su origen en el comercio internacional. Se entiende por tal, la disposición adoptada en un tratado internacional, en cuya virtud una de las partes contratantes concede a la otra o a las otras, o todas las intervinientes se conceden entre sí, el trato de “nación más favorecida”, lo que significa que el Estado concedente se obliga a dar al Estado beneficiario el mismo trato, por lo menos, que el otorgado a los terceros más beneficiados en una determinada

¹ Este trabajo se ha realizado en el marco del proyecto DER2012-32063 “Turismo y Nuevas Tecnologías; en especial, el régimen jurídico de las denominadas centrales de reservas turísticas” (Investigador principal: Apol·lònia Martínez Nadal) financiado por el Ministerio de Economía y Competitividad y Desarrollado en la Universidad de las Illes Balears.

esfera de relaciones. Supone, en consecuencia, una concesión de las mejores condiciones, en un ámbito concreto de relaciones internacionales.

En el ámbito de las relaciones contractuales entre particulares se ha importado esta expresión, propia del Derecho internacional, y en el caso concreto de la contratación turística que analizamos, ha sido acogida no solo en la terminología propia del sector sino incluso también en pronunciamientos jurisprudenciales. Su finalidad es, esencialmente, la misma que las cláusulas MFN del comercio internacional: mantener precios idénticos para el mismo tipo de habitación y condiciones de reserva idénticas en todos los canales online y offline. Así, p.ej., estas cláusulas obligan a los empresarios de alojamiento a los que se imponen a ofrecer a Booking.com, uno de las OTA más relevantes en el ámbito europeo, los mismos o mejores precios de habitación que los que puedan ofrecer por cualquier otro canal de distribución en línea o presencial.

La imposición de este tipo de cláusulas ha de enmarcarse en el ámbito de las relaciones interempresariales entre las centrales de reservas (OTA), que aparecen materialmente, como intermediarios, y los prestadores de servicios de alojamiento (los titulares de los establecimientos)².

En principio, tales relaciones pueden considerarse como un instrumento de colaboración interempresarial, beneficioso para el hotelero, que aumenta su potencial número de clientes, y beneficioso también para el consumidor, que tiene acceso directo a un mayor número de ofertas, incluso con opiniones de otros usuarios que pueden ser útiles para la adopción de su decisión final.

Sin embargo, el problema viene dado por la desigual posición de las partes de estos contratos de colaboración. En Europa, la estructura y dimensión de los grandes portales de ventas (con tendencias próximas al oligopolio, por cuanto unos pocos gestionan la mayoría de reservas online), contrasta con la estructura del sector de alojamiento, caracterizado por una estructura atomizada con multitud de empresarios hoteleros, la mayor parte de ellos titulares de pequeñas y medianas empresas³.

Curiosamente, con la irrupción de las nuevas tecnologías en la comercialización de servicios turísticos, algunas previsiones apuntaban a la

² Para una aproximación a la naturaleza y régimen jurídico de estas entidades, cfr., MARTINEZ NADAL, A., "Las centrales electrónicas de reservas turísticas", *Estudios de Derecho Mercantil. Libro homenaje al Prof. J. A. Gómez Segade*, pág. 967-984, Madrid, 2013, pág. 967-984.

³ Según Hosteltur (http://www.hosteltur.com/192000_justicia-alemana-declara-ilegales-clausulas-paridad.html, fecha de consulta: 3-2-2015), en la actualidad existen tres grandes portales de Internet realizando el 90% de reservas en la Unión Europea a través de agencias de viajes online (el más importante con diferencia es Booking.com) La dimensión de estos grandes portales contrasta con la de los cerca de 200.000 hoteles que existen en Europa, la mayor parte de ellos, pequeñas empresas con menos de 10 trabajadores Cfr., también, más extensamente al respecto, Roland Schegg, *European Hotel Distribution Study 2014: The Rise of Online Intermediaries*, Institute for Tourism of the University of Applied Sciences Western Switzerland Valais, July 2014.

minimización de la intermediación, en el sentido de que cobraría importancia la venta directa a través de la propia web del hotelero en detrimento del papel de las agencias de viaje. Sin embargo, resulta que, al cabo de unos años, efectivamente la pérdida de importancia de las agencias de viajes tradicionales, muchas de las cuales han desaparecido, es innegable; pero, correlativamente, a la vista de la situación actual, ha adquirido una importancia esencial una nueva forma de intermediación, la de las OTA que, por sus dimensiones y posición en el mercado, están imponiendo una serie de condiciones a los hoteleros. De forma que, frente a la anunciada “desintermediación” se ha producido en realidad una “hipermediación”.

Por tanto, en la práctica, existe una posición de poder de los grandes portales y, correlativamente, una situación de desventaja de los pequeños hoteleros en la negociación de estos contratos de colaboración. Por ello, las pequeñas y medianas empresas del sector hotelero pueden verse amenazadas por la realización de prácticas ilícitas por parte de sus socios colaboradores (OTA) en la comercialización online. Existen distintas prácticas cuya licitud está siendo cuestionada en estos momentos: entre otras, el anuncio de falta de disponibilidad o de últimas plazas disponibles⁴, la publicación de comentarios negativos por terceros⁵ o también las cláusulas de paridad en las que centramos este trabajo.

II. Problemática jurídica. Valoración

Las denominadas cláusulas de paridad han sido consideradas en muchas ocasiones como abusivas por el sector hotelero por implicar un perjuicio no solo para los empresarios de alojamiento afectados sino también para los consumidores:

a) En efecto, para el empresario hotelero, tales cláusulas suponen un perjuicio ya que no puede siquiera vender directamente por la misma cantidad que él recibe de la OTA, esto es, el precio por ella ofrecido al público con el descuento de la comisión cobrada al hotelero. Y, en cambio, cuando son las OTA las que realizan la gestión de cobro, ellas sí pueden reducir el precio

⁴ Cfr., respecto de la problemática jurídica de estos anuncios sobre disponibilidad de plazas por parte de las OTA, FLAQUER RIUTORT, J., “Las OTA y falta de disponibilidad de plazas ¿una práctica desleal?”, *Diario La Ley*, nº 8436, 2014; y también, del mismo autor, “Reflexiones jurídicas sobre determinadas prácticas en la comercialización turística on line”, *Revista Aranzadi Dº y NNTT*, nº 38, 2015.

⁵ Cfr., respecto de la problemática jurídica de la publicación de comentarios negativos o incluso falsos sobre establecimientos de alojamiento por parte de terceros en páginas web, en particular, en los denominados “review sites”, MARTÍNEZ NADAL, A., “Reputación on-line y comentarios negativos de terceros”, *Estudios Homenaje al prof. R. Illescas*, 2015 (en prensa), y MARTÍNEZ NADAL, A., “Publicación en páginas web de valoraciones falsas e incidencia en la reputación digital de los empresarios de alojamiento: ¿práctica desleal?”, *Revista de Derecho Mercantil*, 2015 (en prensa).

porque pueden decidir comercializar rebajando el precio de venta al público a costa de su margen.

Por ello, se considera por el sector hotelero que este tipo de cláusulas son contrarias a la libertad empresarial de los empresarios de alojamiento, ya que no tienen la posibilidad de decidir por ellos mismos los precios y las condiciones de las habitaciones en los diferentes canales de distribución; porque, en efecto, la prohibición no solo afecta a la venta directa por el propio empresario hotelero sino también a las ventas por cualesquiera medios de distribución, sean online, sean offline.

b) Y, además, las cláusulas de paridad también suponen un perjuicio para los consumidores, pues no existe un libre funcionamiento del mercado que permita una mejora, y reducción, de precios a favor de los usuarios finales.

Dado el perjuicio derivado de estas cláusulas de paridad, cabe plantear los instrumentos de que disponen los empresarios afectados por su imposición para actuar frente a las mismas.

Recordemos, de entrada, que, como hemos señalado, estas cláusulas se imponen en el ámbito de los contratos de colaboración interempresarial que vinculan a las OTA con los empresarios de alojamiento, contratos atípicos, que no tiene una regulación propia y específica⁶. Sin embargo, no parece ser el ámbito contractual, ni la negociación del contenido del contrato por las partes, la vía de solución de forma general, por cuanto, como hemos expuesto, existe con frecuencia una posición de desigualdad entre la partes contractuales que impide cualquier negociación al respecto y que, por el contrario, permite prácticas por parte de las OTA en la comercialización online cuya licitud es cuanto menos cuestionable y en algunos casos ha sido ya, como hemos apuntado, efectivamente cuestionada⁷.

⁶ Esta nota de atipicidad y falta de regulación específica es, en general, característica de los contratos turísticos interempresariales. En la Propuesta de Código Mercantil elaborada por la Comisión General de Codificación se intentó colmar esta laguna proponiendo la regulación básica de algunos de estos contratos interempresariales; sin embargo, tal propuesta de regulación no prosperó y fue suprimida ya en el Proyecto de Ley aprobado por el Consejo de Ministros, por considerarla innecesaria. Cfr., más extensamente al respecto, MARTINEZ NADAL, A., “La regulación de los contratos turísticos en la propuesta de código mercantil de la sección mercantil de la Comisión General de Codificación”, *Hacia un nuevo Código Mercantil* (coord. Por Alberto Bercovitz Rodríguez-Cano), 2014, pág. 469-481

⁷ En efecto, como hemos apuntado, existen en Francia pronunciamientos judiciales sobre el carácter ilícito de los avisos de falta de disponibilidad de plazas publicados en la web de las OTA, por cuanto puede existir disponibilidad en otros canales de venta; cfr., al respecto, FLAQUER RIUTORT, J., “Las OTA y falta de disponibilidad de plazas ¿una práctica desleal?”, *cit.* Por otra parte, y respecto de la publicación de comentarios negativos, el empresario turístico está expuesto a opiniones vertidas por terceros en una página web ajena sobre la que, en principio, no tiene control: pueden ser opiniones subjetivas, informaciones verdaderas o falsas, vertidas por clientes reales o clientes inexistentes, clientes anónimos o identificados. Es cierto que en las relaciones contractuales interempresariales que vinculan al hotelero con la OTA podría abordarse y regularse

A la vista de lo expuesto, se pone de manifiesto que, de forma general, el empresario de alojamiento, de forma individual, difícilmente puede hacer frente a este tipo de prácticas por la vía contractual. Ante la imposibilidad de negociación, la solución, o más bien, vía de escape, para algunos hoteleros ha sido la finalización de sus contratos con las OTA que les imponen tales condiciones. Aunque ello es algo excepcional, dada la dependencia de los hoteleros de estos intermediarios⁸.

Por ello, por una parte, ante la debilidad de la eventual iniciativa individual de los empresarios afectados, han surgido iniciativas sectoriales de interés. Es el caso del documento elaborado por HOTREC, asociación representativa de la industria hotelera europea (Asociación europea de Hoteles, Bares y Cafeterías)⁹, denominado “*Benchmarks of Fair Practices in Online Distribution*”, que incluye, como veremos, un apartado dedicado precisamente a las cláusulas de paridad de precios¹⁰.

el tema de las opiniones negativas por terceros, pero no olvidemos que, en estos momentos, quienes tienen la posición económica dominante en esa relación contractual son habitualmente las OTA, que acaban imponiendo sus condiciones a los proveedores de servicios turísticos. Y el problema mencionado se agrava cuando tales opiniones se expresan a través de otras entidades que no son en sentido estricto intermediarios, aun cuando influyen de forma indirecta pero muy relevante en la actividad de comercialización de servicios turísticos: son los denominados *Online Review Sites* o sitios de valoración online que permiten a la persona interesada en una determinada prestación (p.ej. alojamiento) búsquedas y comparativas sobre los servicios turísticos ofrecidos por distintos proveedores y también la expresión de opiniones sobre tales servicios por parte de sus usuarios. Precisamente respecto de estas entidades, TripAdvisor, ha de mencionarse la sanción que le ha sido recientemente impuesta en Italia por la *Autorità Garante de la Concorrenza e del Mercato*. En concreto, el organismo regulador de la competencia en Italia ha impuesto una multa de 500.000 euros a TripAdvisor por considerar que no ha aplicado los controles necesarios para evitar críticas fraudulentas. En particular, conforme al criterio de la Autoridad de la Competencia italiana, las conductas examinadas de TripAdvisor consistentes en la difusión de información sobre el carácter auténtico, verdadero y genuino de los comentarios publicados en su web presentan las características de una práctica comercial desleal. Cfr., más extensamente al respecto, MARTINEZ NADAL, A., “Publicación en páginas web de valoraciones falsas e incidencia en la reputación digital de los empresarios de alojamiento: ¿práctica desleal?”, *Revista de Derecho Mercantil*, 2015, (en prensa).

⁸ Ante la imposibilidad de negociación, la solución, o más bien, vía de escape, para algunos hoteleros ha sido la finalización de sus contratos con las OTA que les imponen tales condiciones. Aunque sea algo excepcional, dada la dependencia de los hoteleros de estos intermediarios, así ha ocurrido en Escandinavia donde algunos grupos hoteleros de relevancia (First Hotels, Nordic Choice, Scandic Hotels y Thon Hotels) no han renovado sus contratos con Expedia ante los problemas derivados de la paridad y las comisiones aplicadas por las OTA. Cfr., al respecto, “Hoteles Escandinavia finalizan sus contratos con Expedia. Ante problemas sobre paridad y comisiones”, <http://www-hosteltur.com>, fecha de consulta: 3-2-2015.

⁹ HOTREC es la entidad representativa de hoteles, restaurantes, bares y establecimientos similares en Europa; aglutina a 42 asociaciones nacionales representativas del sector, formadas principalmente por pequeñas y medianas empresas pertenecientes a 28 países europeos.

¹⁰ HOTREC “*Benchmarks of Fair Practices in Online Distribution*”, <http://www.hotrec.eu> (última consulta: abril 2015). HOTREC, “*Benchmarks of Fair Practices in Online Distribution*”, <http://www.hotrec.eu> (última consulta: abril 2015).

Y, por otra parte, ante la insuficiencia de la vía contractual para hacer frente a este tipo de cláusulas, el sector hotelero, en distintos países de la Unión Europea, ha recurrido al Derecho de la competencia desleal y ha optado por denunciar este tipo de prácticas como desleales ante las respectivas autoridades nacionales en la materia.

A ambas iniciativas dedicamos el apartado siguiente.

III. Reacción empresarial. Posibles vías de solución

3.1. Iniciativas sectoriales: las directrices de HOTREC: las prácticas equitativas en la distribución en línea. Eficacia.

Como hemos apuntado, HOTREC, como entidad representativa del sector hotelero europeo, ha elaborado el documento “*Benchmarks of Fair Practices in Online Distribution*”, que, en su versión de 2014, aprobada en Riga, incluye un apartado dedicado a las cláusulas de paridad de precios.

Este documento ha sido elaborado por los miembros de HOTREC por el creciente número de hoteleros preocupados por el trato injusto recibido por parte de los intermediarios. Según se señala en el Preámbulo del documento, existen más 200.000 hoteles y establecimientos similares en todo Europa (la mayoría de ellos pequeñas y medianas empresas) a los que resulta a menudo difícil de soportar el poder de los intermediarios en la distribución en línea. Por ello, se proponen en el documento una serie de puntos de referencia que se plantean como propuestas de solución para conseguir un mercado más transparente y equilibrado que permitirá, en última instancia, que los clientes tomen decisiones basándose en una información transparente y fiable.

Como hemos señalado, la industria hotelera, estructurada de forma atomística mayoritariamente a través de pequeñas y medianas empresas, tiene cada vez mayor dependencia de un número de intermediarios cada vez más reducido y con mayor peso. De ahí que un número cada vez mayor de hoteles considere que está perdiendo el control de su producto como consecuencia de la presión ejercida por los intermediarios para la distribución electrónica. Y, por ello, los empresarios hoteleros consideran que se enfrentan en el campo de la distribución digital a prácticas desequilibradas e injustas. Para hacer frente a esta situación, HOTREC publica estos puntos de referencia para unas prácticas equitativas en la distribución en línea a fin de mantener los mercados transparentes, abiertos y competitivos en beneficio de los clientes, intermediarios y hoteles.

Entre esas prácticas poco equitativas denunciadas por los hoteleros se incluye, precisamente, el tema de la paridad de precios. Tal como se apunta en el preámbulo del documento de HOTREC, el precio es uno de los elementos respecto del que los hoteleros consideran haber perdido el control por la presión de sus socios en la distribución, las OTA; y, por ello, reivindican la transparencia

y competitividad de los mercados en beneficio de clientes, intermediarios y hoteleros¹¹.

Y al tema de la paridad de precios se dedica el apartado 2, que, con un encabezado genérico titulado “*No mandatory rate parity*”, se concreta en el siguiente contenido:

Rate parity mandatorily imposed by distribution partners maintains identical rates for the same room type and identical booking conditions across all online and even offline channels. This wide spread term is levering out the pricing as a key market instrument at the disposition of the hotel entrepreneur and distorts competition results. There is already official reference stating that rate parity is in breach of European competition rules.

Por tanto, tras definir la paridad de precios impuesta por los distribuidores como aquella que mantiene precios idénticos para el mismo tipo de habitación e idénticas condiciones de reserva en todos los canales de distribución online e incluso offline, HOTREC apunta los efectos de tal cláusula sobre el empresario hotelero. En concreto, se señala que la amplia difusión de este tipo de cláusula está apalancando el precio como instrumento clave del mercado a disposición del empresario hotelero y distorsiona los resultados de la competencia; por tanto, en la línea que ya hemos expuesto, se viene a señalar su incidencia sobre la libertad empresarial y el libre funcionamiento del mercado. Y, como también hemos indicado, se apunta hacia el Derecho de la competencia señalando la existencia de pronunciamientos oficiales en el sentido de que la paridad de precios vulnera las reglas europeas en materia de competencia. Lo cual nos lleva a la segunda vía de reacción empresarial que analizamos en este trabajo.

Acabamos este subapartado señalando que, obviamente, el documento de HOTREC que analizamos no es un documento vinculante para los agentes implicados; el contenido de sus apartados no pasaría de ser una simple recomendación, e incluso, en el caso de la cláusula de paridad de precios, un reflexión sobre el contenido y efectos de la misma. No obstante, para dar a conocer el documento, y la previa problemática existente, la industria hotelera lo ha hecho llegar a las instituciones comunitarias y ha mantenido contactos con los principales sitios web de Europa que intervienen la comercialización online de plazas de alojamiento.

De esta forma, estos principios o criterios contenidos en el documento de HOTREC, sin ser norma jurídica en sentido estricto, podrían llegar a considerarse

¹¹ “*Rate, distribution and product sovereignty must remain with the hotel. Whereas this general market principle should be a matter of course, an increasing number of hotels is losing control of their genuine product as a consequence of emerging pressure by distribution partners. Therefore, HOTREC releases these Benchmarks of Fair Practises in Online Distribution to keep the markets transparent, open and competitive for the benefit of guests, intermediates and hotels...*” (HOTREC, *Benchmarks of Fair Practices in Online Distribution*, Preamble).

como parte del “*soft law*” que se caracteriza, como es sabido, no por imponer soluciones sino más bien por intentar convencer a las partes involucradas, creando un estado de opinión favorable a su cumplimiento y persiguiendo, también, en última instancia, influir en eventuales iniciativas legislativas que pudieran existir al respecto.

3.2. El recurso al Derecho de la competencia: denuncias nacionales por prácticas desleales.

3.2.1. Planteamiento general: distintas denuncias ante organismo nacionales de control de la competencia.

Como hemos apuntado, ante la insuficiencia de la vía contractual para hacer frente a este tipo de cláusulas de paridad de precios, debido a la posición de desigualdad de las partes contractuales, el sector hotelero, en distintos países de la Unión Europea (también, como apuntaremos, en EE.UU.), ha recurrido al Derecho de la competencia desleal y ha optado por denunciar este tipo de prácticas que consideran desleales ante las respectivas autoridades nacionales de la competencia.

Entre los procedimientos de mayor importancia iniciados cabe mencionar los siguientes:

1) En 2010, la OFT británica (*Office of Fair Trading*) comenzó una investigación que desembocó en un procedimiento contra Expedia, Booking.com e IHG (*Intercontinental Hotels Group*). Este procedimiento se centraba en las restricciones de las OTA a poder ofrecer descuentos sobre las tarifas fijadas.

2) En 2012 se inició ante la autoridad competente en Alemania (*Bundeskartellamt*) un procedimiento contra HRS.com (*Hotel Reservation Service*), la OTA dominante en el mercado alemán, en el que se analizaba la licitud, desde la perspectiva del Derecho de la competencia, de las cláusulas de paridad de precios y de las cláusulas de paridad de disponibilidad. A la finalización de este procedimiento y la subsiguiente resolución judicial dictada a raíz del mismo dedicamos el siguiente subapartado.

3) En un país no miembro de la Unión Europea, Suiza, se inició en diciembre de 2012 un procedimiento de la *Wettbewerbskommission* (WEKO) contra Expedia, Booking.com y HRS no sólo por la existencia en sus contratos de *MFN clauses* sino, por primera vez, por un posible abuso de posición de dominio de estos intermediarios en la negociación.

4) En California, EE.UU., también en 2012 se inicia un procedimiento en el que se enjuician las *MFN clauses* de Expedia, Booking.com, Travelocity, Priceline, Sabre, Orbitz, Hotels.com; pero también de los hoteleros: IHG, Marriot, Kimpton, Starwood, etc...

5) Recientemente, y volviendo al ámbito europeo, en Francia, Italia y Suecia se han procedido contra Booking.com en los que se discute si las cláusulas de paridad de precios son o no ilícitas de competencia.

3.2.2. El caso alemán: Sentencia del Tribunal Superior de Justicia de Düsseldorf de 9 de enero de 2015

Como hemos anticipado, y del mismo modo que en otros países europeos, los empresarios de alojamiento alemanes recurrieron a la autoridad nacional en materia de competencia ante las cláusulas de paridad de precios impuestas por las OTA. A raíz de estas denuncias, el 20 de diciembre de 2013 la agencia de competencia alemana prohibió a HRS (OTA dominante en el mercado alemán) el uso de cláusulas de paridad en sus contratos con hoteles.

La agencia de competencia alemana concluyó, en línea con los argumentos hasta ahora expuestos, que estas cláusulas constituyen una clara violación del Derecho de la competencia, alemán y europeo.

Por ello, desde marzo de 2014 HRS no ha aplicado las citadas cláusulas en los contratos con hoteles en Alemania. Pero, al mismo tiempo, disconforme con el criterio de la agencia de competencia alemana, HRS interpuso recurso contra esta prohibición ante el Tribunal Superior de Düsseldorf. Paralelamente al procedimiento judicial contra HRS, la agencia alemana de competencia investiga, a instancias de la queja presentada por la hotelería alemana, las cláusulas de paridad en los contratos de Booking.com y Expedia.

En fecha reciente, el día 9 de enero de 2015, el Tribunal Superior de Justicia de Düsseldorf resolvió el recurso de la OTA HRS contra la decisión de la Agencia federal alemana de competencia (*Bundeskartellamt*) relativa a las llamadas cláusulas de paridad de precios.

Con esta sentencia del Tribunal Superior de Düsseldorf, se confirma la posición de la hostelería europea en el sentido de que, desde el punto de vista legal, las cláusulas de paridad impuestas por los portales de reservas (OTA) a los hoteleros en los contratos de distribución representan una clara y flagrante restricción de la competencia.

Obviamente, la mencionada sentencia del tribunal de Düsseldorf ha sido muy recibida por el sector hotelero europeo, que considera que dicha resolución cambiará el *statu quo* de la distribución hotelera europea y que constituye un paso muy importante en la recuperación de la libertad empresarial para el empresario hotelero europeo.

No obstante, no puede olvidarse que estrictamente la sentencia tiene efectos limitados a las partes y al país en que ha sido dictada. Por ello, la posición de HOTREC ante la misma se debate entre la opción de:

a) Iniciar acciones legales a nivel europeo para que la Autoridad de competencia europea prohíba las cláusulas de paridad para todo el territorio de la Unión Europea.

b) O, por el contrario, confiar en que el denominado «efecto dominó» acabe por prohibir, de forma progresiva y en distintas velocidades, las cláusulas de paridad en toda la Unión Europea. Como elementos que pueden propiciar este efecto expansivo, se considera relevante que existan ya procesos contra otras OTA (p.ej., Booking y Expedia) en Alemania, Francia y los países nórdicos. Y las expectativas del sector hotelero son que, en caso de que existan nuevos pronunciamientos contrarios a las cláusulas de paridad en algunos otros países, de forma voluntaria las OTA eliminen las condiciones de paridad por restricción de la competencia, por lo que, conforme a las previsiones hoteleras, en dos o tres años serían historia¹².

3.2.3. La actuación coordinada de las autoridades de competencia de Francia, Italia y Suecia y su aceptación de los compromisos de Booking respecto de la cláusula de paridad. Hacia una cláusula de paridad relativa

Aunque en principio cabría dudar de la expansión a la totalidad del ámbito de la Unión Europea de los criterios establecidos por una sentencia dictada por un tribunal nacional por aplicación voluntaria por parte los agentes afectados (en nuestro caso, las OTA), no puede negarse que, en principio, parece existir un dato significativo a favor de este efecto expansivo.

En efecto, probablemente no es casualidad que Booking.com, a menos de un mes vista para del fallo de la justicia alemana, anunciara compromisos para acabar con las cláusulas de paridad con la finalidad de poner fin a las investigaciones en Francia, Suecia e Italia.

En respuesta a estas investigaciones, Booking.com se compromete a abandonar el requisito de paridad en los precios que el hotel propone a otras agencias de viajes en Internet. Ello permitiría a los hoteles ofrecer diferentes precios a diferentes webs de comercialización. No obstante, el hotel seguirá estando obligado a ofrecer a Booking.com los mismos precios o mejores que los que ofrece en sus propios canales de distribución. Estos compromisos se aplicarían en todo el espacio económico europeo.

No obstante, obsérvese que, en realidad, tal compromiso no supone la supresión absoluta, y por tanto, el fin de las cláusulas de paridad, ya que el hotel sigue estando sometido a tal exigencia para sus propias ventas directas. De ahí que este compromiso no suponga una supresión absoluta de la exigencia de

¹² Hosteltur (http://www.hosteltur.com/192000_justicia-alemana-declara-ilegales-clausulas-paridad.html, fecha de consulta: 3-2-2015)

paridad sino que, más bien, sería una cláusula de exigencia relativa que no afectaría a todos los canales de distribución.

Pese a ello, el día 21 de abril de 2015 distintas autoridades nacionales de competencia (en Francia, Italia y Suecia) han aceptado, tras distintas negociaciones y pruebas, la propuestas presentadas por Booking. En concreto, tal como informa la autoridad de la competencia francesa, en coordinación con la Comisión Europea y las autoridades de Italia y Suecia, se han obtenido compromisos particularmente extensos de Booking.com con el objetivo de impulsar la competencia entre plataformas de reservas online y dar los hoteles más libertad en materia comercial y de precios¹³.

En concreto, Booking.com efectivamente se compromete a modificar la cláusula de paridad de precios y eliminar cualquier cláusula que imponga obligaciones de paridad en cuanto a la disponibilidad de habitaciones o condiciones comerciales. Y ello no solo en relación con las plataformas, sino también con canales offline de venta directa por parte de los hoteleros. Los empresario de alojamiento, en consecuencia, pueden aplicar libremente precios más bajos y/o mejores condiciones comerciales a las plataformas que actúan en competencia con Booking. Y, en particular, también pueden ofrecer precios inferiores a los que se muestran en la página web Booking.com través de sus canales de venta fuera de línea (las reservas *in situ*, por teléfono, fax, correo electrónico, mensajería instantánea, los puntos de venta físicos de las agencias de viajes, etc...), siempre y cuando estos precios no se publiquen en el sitio web del hotel. También pueden ofrecer precios inferiores a los que se muestran en la página web Booking.com a los clientes que son miembros de los programas de fidelización.

Estos compromisos, asumidos por 5 años, han entrado en vigor a partir del día 1 de julio de 2015. La autoridad de la competencia llevará a cabo una evaluación intermedia, con la participación de ambas partes, sobre la efectividad de los compromisos el 1 de enero de 2017 a más tardar.

Estas medidas, según las autoridades de competencia implicadas (Francia, Suecia e Italia), constituyen un conjunto equilibrado que cumple con los objetivos perseguidos:

- a) Deberían dar un impulso a la competencia entre Booking.com y las agencias de viajes online de la competencia, permitiendo la reducción de las comisiones cobradas a los hoteles;
- b) También mejoran la posición de los hoteleros, recuperando de forma notable su libertad comercial y de fijación de precios;
- c) Y mantienen al mismo tiempo el modelo económico de las agencias de viajes online, que ofrecen a los consumidores de forma gratuita potentes servicios de búsqueda y de comparación.

13 <http://www.autoritedelaconcurrence.fr> (fecha de consulta: 29-5-2015).

Este procedimiento se ha llevado a cabo en el contexto europeo de la cooperación reforzada. Francia, Suecia e Italia han trabajado juntos, en estrecha coordinación con la Comisión Europea, para obtener compromisos similares de Booking.com en estos tres países¹⁴.

Otras autoridades nacionales de competencia en Europa han iniciado procedimientos en relación con las mismas prácticas. Por ello, han seguido con gran interés la evolución de la cooperación reforzada y ahora probablemente tendrá en cuenta la posibilidad de ampliar estos compromisos a su propio mercado.

Sin embargo, estos compromisos, de entrada, no han sido bien aceptados por el sector hotelero europeo¹⁵. Así, HOTREC, con ocasión de la 70ª Asamblea General de la entidad celebrada en Luxemburgo, debatió y acordó una declaración oficial sobre las decisiones tomadas, con fecha 21 de abril 2015, por las autoridades francesas, italianas y suecas de competencia en cuanto a la aceptación de los compromisos de Booking.com para resolver los casos nacionales de competencia sobre las cláusulas de paridad:

1) HOTREC subraya que las cláusulas de paridad son contrarias a la competencia.

2) La industria hotelera europea se niega a ver limitada su libertad empresarial por estos compromisos a la fijación de precios y condiciones para herramientas de comunicación offline (por ejemplo, teléfono, fax).

3) HOTREC se refiere a las decisiones como un primer paso, pero insuficiente.

4) HOTREC no está convencido de los supuestos efectos positivos de los compromisos.

5) HOTREC señala que de tenerse en cuenta que, en este momento, en la actualidad hay dos enfoques igualmente validados a nivel europeo para abordar

¹⁴ Bruno Lasserre, Presidente de la autoridad de la competencia, Giovanni Pitruzzella, el presidente de la autoridad de competencia italiana y Dan Sjöblom, director general de la autoridad de competencia de Suecia han declarado lo siguiente:

“Con la coordinación de la Comisión Europea, nuestras tres autoridades han colaborado de una manera sin precedentes en nuestras investigaciones sobre plataformas de reserva en línea. Hoy podemos anunciar que hemos decidido aprobar compromisos que nos ofrece el líder del mercado, Booking.com. Los compromisos se han mejorado significativamente después de una prueba de mercado.

Estos nuevos compromisos limitan el uso por parte de Booking.com de la exigencia paridad de precios como parte de su modelo de negocio basado en comisiones y aumentan sustancialmente el margen de maniobra de los hoteles. Los compromisos ofrecidos por Booking.com implican un justo equilibrio para los consumidores en Francia, Italia y Suecia, la restauración de la competencia y, al mismo tiempo, preservan servicios de búsqueda y comparación gratuitos y de fácil uso y el fomento de la floreciente economía digital” (<http://www.autoritedelaconcurrence.fr>, fecha de consulta: 29-5-2015).

¹⁵ HOTREC General Assembly’s statement on the decisions taken on 21 April 2015 on the commitments of Booking.com (24-4-2015), <http://www.hotrec.eu> (fecha de consulta: 29-5-2015).

la cuestión de las cláusulas de paridad en los contratos hoteleros. Por una parte, la vía de la negociación, como ha ocurrido en Francia, Italia y Suecia; y, por otra parte, el enfoque de una prohibición total de cláusulas MFN, como en Alemania.

6) Los miembros de HOTREC considerarán apelar estas decisiones de las autoridades de competencia.

3.3. Intervención legislativa: la prohibición absoluta del legislador francés

En este complejo contexto de existencia de distintos pronunciamientos en distintos países sobre las cláusulas de paridad, en julio de 2015 la Asamblea Nacional de Francia aprobó la prohibición total de las cláusulas de paridad en el sector hotelero francés. Por tanto, en los contratos entre hoteleros y OTA queda prohibida la utilización de cualquier cláusula de paridad, sea absoluta (la que afecta a todos los canales de venta), sea simplemente relativa (por afectar solo a determinados canales). Con ello el legislador francés pretende garantizar la seguridad de sus hoteleros de controlar los precios de sus servicios en cualquier canal de venta, sea online u offline, sea directo o con terceros intermediarios.

Obsérvese que esta iniciativa legal francesa contrasta con la decisión de la Autoridad francesa de Competencia que, como señalábamos en el apartado anterior, de forma coordinada con las respectivas autoridades de Suecia e Italia, consideró admisibles, conforme al Derecho de la competencia, los compromisos de Booking que, en el fondo, implicaban una cláusula de paridad relativa, que afectaba solo a determinados canales de venta.

V. Conclusión

En la actualidad es indudable la importancia económica de los contratos de colaboración entre las OTA y los empresarios hoteleros para la comercialización por medios electrónicos de plazas de alojamiento.

No obstante, en el marco de estos contratos de colaboración surgen problemas derivados de la situación de desigualdad de las partes en sus relaciones interempresariales. En concreto, la posición de dominio de las OTA frente la posición de mayor debilidad del pequeño y mediano empresario hotelero plantea la posibilidad de prácticas ilícitas y desleales por parte de las OTA. Una de las prácticas cuestionadas, como hemos visto, es la imposición de las denominadas cláusulas de paridad en virtud de las que se prohíbe al hotelero vender a un precio inferior al pactado con la OTA por cualquier otro canal, tanto online como offline.

Obviamente, dada la frecuente posición de desigualdad, no puede hallarse solución al problema a través de la negociación de las partes en el ámbito de la relación contractual. Y, ante la insuficiencia de la vía contractual, cobra gran importancia el recurso al Derecho de la competencia. Como hemos visto, por

esta vía se han obtenido pronunciamientos de distintas autoridades nacionales de la competencia, e incluso alguna resolución judicial de un tribunal alemán, en el sentido de prohibir este tipo de cláusulas por infracción del derecho de la competencia, por afectar a la libertad empresarial y el libre funcionamiento del mercado.

A la vista de estos pronunciamientos prohibitorios sobre la materia en Alemania, y a la espera de los que previsiblemente se debían producir de forma próxima, cabía esperar un efecto expansivo y que, de forma voluntaria, las OTA eliminaran las condiciones de paridad por restricción de la competencia.

No en vano, como hemos visto, alguna de las OTA dominantes en el mercado europeo anunció compromisos para acabar con las cláusulas de paridad. Tales compromisos tendrían efecto en todo el ámbito de la Unión Europea y, como hemos visto, tras distintas negociaciones, han sido recientemente aceptados por varias autoridades supervisoras de la competencia de distintos países europeos (Francia, Suecia e Italia). En realidad, tales compromisos ya aceptados no suponen una supresión total de la exigencia de paridad.

Pues el compromiso consiste en suprimir la exigencia de paridad en los precios que el hotel propone a otras agencias de viajes en Internet. Y también para los canales offline de venta directa por parte de los hoteleros. Pero no para sus ventas directas online (salvo clientes de programas de fidelización). De forma que el hotel podrá ofrecer diferentes precios a diferentes webs pero seguirá estando obligado a ofrecer a la OTA los mismos precios o mejores que los que ofrece en sus propios canales electrónicos de distribución.

De ahí que este compromiso no suponga una supresión absoluta de la exigencia de paridad; más bien pasaríamos de una cláusula de exigencia absoluta de paridad a una cláusula de exigencia relativa que no afectaría a todos los canales de distribución. Y, de ahí, también el descontento inicial del sector hotelero, que pretendía la prohibición absoluta de este tipo de cláusulas, en el sentido del pronunciamiento de los tribunales alemanes.

Téngase en cuenta, finalmente, que, en este complejo contexto de existencia de distintos pronunciamientos en distintos países sobre las cláusulas de paridad, en julio de 2015 la Asamblea Nacional de Francia aprobó la prohibición total de las cláusulas de paridad en el sector hotelero francés. Como hemos señalado, esta iniciativa legal francesa contrasta con la conocida decisión de la Autoridad francesa de competencia que, de forma coordinada con las respectivas autoridades de Suecia e Italia, consideró admisibles, conforme al Derecho de la competencia, los compromisos de Booking que, en el fondo, implicaban una cláusula de paridad relativa, que afectaba solo a determinados canales de venta.

La cuestión de las cláusulas de paridad en los contratos de colaboración entre hoteleros y OTA sigue, pues abierta. Y en estos momentos hay dos enfoques a nivel europeo para abordar esta cuestión. Por una parte, la vía de la negociación, como ha ocurrido en Francia, Italia y Suecia; y, por otra parte, el enfoque de una prohibición total de cláusulas MFN, como ocurre en Alemania

por decisión judicial, e, incluso con mayores efectos, de forma más reciente, en Francia, por decisión del legislador.

Lo que parece indudable es que la existencia de diferentes vías de solución en distintas jurisdicciones no favorece la obtención de una solución uniforme para un problema transfronterizo en una economía globalizada sino que, más bien, dificulta y complica el camino hacia la misma.

El contrato electrónico laboral

Sulmer Paola Ramírez*

SUMARIO: 1. Las Tecnologías de la Información y las Comunicaciones en el ámbito contractual. 2. El contrato de trabajo en soporte electrónico. 2.1. Sujetos. 2.2. Características. 2.3. Elementos esenciales. 2.4. Elementos objetivos. 3. Postulados del Derecho laboral en el contrato de trabajo electrónico. 4. Principios generales del Derecho del trabajo aplicables a los contratos electrónicos laborales. 5. Sujección del contrato electrónico laboral a la Ley Orgánica del Trabajo, los trabajadores y las trabajadoras. 6. Valor jurídico del contrato electrónico laboral. 7. La presunción de laboralidad en Venezuela.

Resumen

Las Tecnologías de la Información y las Comunicaciones han impactado las relaciones laborales desde su inicio hasta su fin. En el ámbito contractual es posible que la voluntad de las partes se exprese a través de mensajes de datos en soporte electrónico, surgiendo así la figura del contrato electrónico. En el presente trabajo se estudia la posibilidad de celebrar contratos laborales por medios electrónicos, llegando a la conclusión que es factible un contrato electrónico laboral, si en el mismo se verifica la presencia de los postulados tradicionales del Derecho del trabajo.

Palabras clave: Contrato electrónico. Mensajes de datos. Contrato electrónico Laboral. Postulados del Derecho del trabajo.

Abstract

Information Technology and Communications has impacted labor relations from its beginning to its end. In the field of contracts, it is possible to express will of the parties through data messages electronically; the consequence of this arise to electronic contracts. This paper analyses the possibility of concluding employment contracts by

Recibido: 31/10/2015 • Aceptado: 15/11/2015

* Abogada, Especialista en Derecho del Trabajo y Seguridad Social UCAT; Especialista en Derecho Administrativo UCAT, Especialista en Negocios con América Latina IDEC Universidad Pompeu Fabra Barcelona España, Doctoranda del Doctorado en ciencias Mención Derecho UCV. Coach Certificada por IDEAR y la ICI -International Association of Coaching Institutes. Profesora Universitaria y Asesora de Empresas Públicas y Privadas. sulmerp@yahoo.com

electronic means, reaching the conclusion is it possible an electronic contract in this field, if the presence of the traditional principles of labor law is verified.

Key Words: Electronic Contract. Data messages. Employment Contracts. Principles of Labor Law.

1. Las Tecnologías de la Información y las Comunicaciones en el ámbito contractual

Etimológicamente, el vocablo contrato proviene de “cum” y “traho”, venir en uno, ligarse, aunarse, siendo por tanto un acto de voluntades¹. En su acepción común, el contrato significa un pacto o convenio, oral o escrito, entre partes que se obligan sobre materia o cosa determinada, y a cuyo cumplimiento pueden ser compelidas².

En Derecho, el contrato, es un negocio jurídico bilateral capaz de crear, reglamentar, modificar, transmitir, o extinguir una relación jurídica de cualquier naturaleza entre las partes que concurren a su celebración. Siendo eficaz tanto en lo que se refiere a vínculos de naturaleza personal (de contenido patrimonial o extra patrimonial) entre las partes, esto es, derechos de créditos (lo que se llama eficacia personal del contrato) como en lo referido al estado de los derechos reales (la llamada eficacia real del contrato)³.

El Código Civil patrio, en su artículo 1.133, define el contrato como una “*Convención entre dos o más personas para constituir, reglar, transmitir, modificar o extinguir entre ellos un vínculo jurídico*”.

Las definiciones anteriores evidencian la voluntad de las partes como elemento fundamental en el contrato, siendo esa misma voluntad en la que se basa la libertad contractual como principio de interpretación del documento electrónico, y es esa misma voluntad por regla general, la que decide el objeto del contrato, el tiempo, el lugar, los medios empleados para la celebración, o ejecución del mismo, entre otros aspectos.

Las TIC han influido en la elección de las partes al momento de contratar, ampliando no solo el objeto de los contratos, sino los medios empleados para la celebración de los mismos, permitiendo el desarrollo de nuevas categorías de contratos como los contratos informáticos y los contratos electrónicos.

1 CARRASCOSA LÓPEZ, V., POZO ARRANZ M. A., RODRÍGUEZ DE CASTRO, E. P.: “La Contratación Informática: El nuevo Horizonte Contractual” Editorial Comares Tercera Edición 2000 p. 6.

2 Diccionario de la Lengua Española. Disponible: <http://lema.rae.es/drae/?val=contrato> Consulta: 18/10/2011.

3 MELICH-ORSINI, J. *Doctrina General del Contrato* Caracas: Editorial Jurídica Venezolana, tercera edición, 1997, p. 26.

2. El contrato de trabajo en soporte electrónico

La conjunción de los principios de libertad contractual y equivalencia funcional, según los cuales, las partes están en plena libertad de elección del medio a utilizar para celebrar sus contratos, entendiéndose que tanto la forma en soporte papel como la elección de contratar en soporte electrónico, con el cumplimiento de las respectivas formalidades, se equiparan en su valor jurídico probatorio, hace factible la elección del soporte empleado para la manifestación de la voluntad en un negocio jurídico.

El contrato de trabajo, es un negocio jurídico bilateral a través del cual, una persona se compromete a prestar sus servicios en forma subordinada a favor de otra persona natural o jurídica, quien a su vez se compromete a pagarle una remuneración por la prestación de dichos servicios.

Tradicionalmente, el contrato de trabajo ha reposado sobre soporte papel, siendo exigida a efectos de su validez, la firma de cada una de las partes plasmada por regla general en forma autógrafa (manuscrita).

El uso de las TIC, ha impactado el Derecho del Trabajo, al igual que como ha ocurrido en las distintas ramas del Derecho, siendo posible que ese negocio jurídico bilateral plasmado tradicionalmente en soporte papel, esté contenido en soporte electrónico, e incluso que los medios electrónicos intervengan según el caso, en la fase de generación, perfeccionamiento y consumación o cumplimiento del contrato.

Planteada esta realidad, salta a la vista la existencia del contrato electrónico laboral, definido como un acuerdo de voluntades formado y/o ejecutado a través de medios electrónicos, mediante el cual una persona natural se obliga a prestar sus servicios en favor de otra persona natural o jurídica, mediante una remuneración.

2.1. Sujetos

Al igual que en los contratos de trabajo en soporte papel, el trabajador y el patrono son las partes del contrato electrónico laboral, pero, en este último, a diferencia del contrato de trabajo en soporte papel, se hace necesaria en la mayoría de los casos, la intervención de un tercero denominado intermediario, que si bien no es parte en la relación jurídico laboral, si interviene en la misma permitiendo la comunicación entre las partes de dicha relación. Así tenemos que los sujetos del contrato electrónico laboral, son tres, a saber:

- Trabajador, entendido como la persona natural que presta sus servicios bajo la subordinación y dependencia de otra persona natural o jurídica
- Patrono o empleador, que es aquella persona natural o jurídica que tenga bajo su dependencia a uno o más trabajadores, en virtud de una relación laboral.

- Intermediario, es aquella persona que permite la comunicación entre el trabajador y el patrono. Generalmente es un proveedor de servicios de Internet conocido por sus siglas en inglés como ISP (*Internet Service Provider*), encargado de proporcionar al usuario el suministro de acceso mediante la conexión a Internet, también pueden prestar servicios de almacenamiento y gestión de correo electrónico, elaboración y administración de páginas web, acceso a sistemas de conferencias electrónicas, transmisión de archivos, acceso a bases de datos entre otros. En aquellos contratos electrónicos laborales celebrados vía telefónica, el intermediario será el operador de telefonía fija o móvil según el caso.

Para facilitar que el patrono y el trabajador puedan tener acceso a Internet, los ISP deben contar con una conexión permanente a Internet, para lo cual deben obtener previamente la disponibilidad suficiente de líneas telefónicas y las correspondientes asignaciones de números IP del ente encargado de asignarlos, para luego proporcionar a cada usuario la respectiva dirección IP y un identificador único para la lectura de su correo electrónico⁴.

En Venezuela, como intermediarios de los contratos electrónicos en general y por ende de los contratos electrónicos laborales, se encuentran en la actualidad CANTV y su filial Movilnet, Inter, Movistar, entre otros; en Colombia los principales ISP son ETB, Telefónica, Claro y Une, y en España Jazztel, Movistar de España, ONO, Orange España y FON entre otros, solo por citar algunos países, destacando que cada país tiene sus propios ISP.

2.2. Características

El contrato electrónico laboral, comparte las características del contrato laboral tradicional en soporte papel, y adicionalmente el uso de los medios electrónicos en la formación y/o ejecución de dicho contrato, lo hace sujetos de ciertas distinciones propias del uso de dichos medios.

Como características comunes al contrato de trabajo en soporte papel y al contrato electrónico laboral, se puede señalar que ambos son contratos sinalagmáticos que originan obligaciones para ambas partes; consensuales, ya que se perfeccionan por el simple consentimiento de las partes sin estar sujeto a formalidad alguna, así mismo son onerosos, conmutativos, de tracto sucesivo e *intuitu personae*.

La característica de contrato conmutativo deriva de la certeza que ambas partes de la relación de trabajo tienen acerca de sus pretensiones, mientras que se considera oneroso el contrato de trabajo, ya que tanto el trabajador como el patrono se benefician recíprocamente de la prestación del otro. La característica

4 RICO CARRILLO, M. (2005): "Comercio Electrónico Internet y Derecho" Editorial Legis, Segunda Edición. p 42.

de tracto sucesivo o ejecución continuada, responde a que los efectos del contrato en cuestión, no se agotan en un solo acto, sino que se van verificando conforme el desarrollo de la relación de trabajo, sin olvidar el carácter de intuitu personae que implica que la obligación del trabajador de prestar los servicios pactados no puede ser delegada por éste en otra persona.

El uso de los medios electrónicos presente en los contratos laborales, hace que se debata al igual que como ocurre con el contrato electrónico general, si el mismo pertenece a la categoría de contratos entre presentes o entre ausentes, adoptándose con mayor fuerza la tesis según la cual, independientemente de la ubicación geográfica de las partes, (indicador de la clasificación de contratos entre presentes y entre ausentes), se emplean los contratos de formación instantánea⁵, para aquellos casos en los que la oferta y la aceptación se da en un mismo momento en tiempo real, (tal y como ocurriría con el contrato entre presentes) y los contratos de formación sucesiva⁶ en los que el concurso de la oferta y la aceptación se da en tiempos diferidos (como ocurriría con el contrato entre ausentes).

La naturaleza de contrato de adhesión presente en los contratos electrónicos, caracterizados por las diferencias entre los proveedores y los usuarios, se encuentra también presente en los contratos electrónicos laborales, pero por razones distintas al de los primeros.

En los contratos electrónicos laborales, el patrono quizás no sea el que mejor dominio tenga del uso de la técnica (como ocurre en los contratos electrónicos generales) pero si es el que cuenta, por regla general, con mayor poder adquisitivo que le permite establecer su empresa y colocar sus propias reglas que se traducen en cláusulas contractuales a las cuales el trabajador decide sujetarse y tiene el empleo o no sujetarse y probablemente no va a ser empleado por dicho patrono.

Ni la Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios de Venezuela, ni las leyes de protección al consumidor vigentes en los distintos países, por regla general, le son aplicables a los contratos electrónicos laborales a pesar de ser contratos de adhesión en la mayoría de los casos. Pero esto no indica, que los trabajadores se encuentren desamparados ante tales cláusulas.

La protección de los trabajadores es mucho más amplia que la de los consumidores o usuarios, ya que, existen en los países miembros de la Organización Internacional del Trabajo, una serie de normas a nivel interno e internacional que protegen a los trabajadores, y son presentadas como principios rectores del Derecho del trabajo, tal es el caso del principio de irrenunciabilidad de los derechos de los trabajadores que en Venezuela hace que sean consideradas nulas, todas las estipulaciones que impliquen la renuncia o menoscabo a los

⁵ Contratos realizados generalmente a través del teléfono, el chat en tiempo real, videoconferencia en tiempo real.

⁶ Contratos realizados generalmente vía correo electrónico, fax, entre otros.

derechos de los trabajadores, independientemente que el trabajador en ejercicio de su autonomía de la voluntad, y de la expresión libre de su consentimiento las haya aceptado. Este principio al igual que otras de las normas consideradas como principios generales del derecho del trabajo, son analizados más adelante en este artículo.

2.3. Elementos esenciales

Como todo acuerdo de voluntades que persiga crear, modificar o reglar un vínculo jurídico, el contrato electrónico laboral, al igual que el contrato de trabajo y el contrato electrónico en general, debe formarse partiendo del consentimiento de las partes, además de tener un objeto determinado y una causa lícita, resaltando que para su validez se requiere la capacidad de los contratantes y la ausencia de vicios del consentimiento, esto de conformidad con lo establecido en los artículos 1.141 y 1.142 del Código Civil de Venezuela, aplicables como marco general al contrato electrónico laboral. De forma tal, que los elementos esenciales requeridos para la existencia del contrato electrónico laboral son:

- El objeto: en los contratos electrónicos laborales, al igual que en los contratos de trabajo en soporte papel, el objeto del contrato, está constituido por las prestaciones recíprocas del trabajador y del patrono, que se traducen a su vez en obligaciones de cada una de las partes, así el trabajador debe prestar el servicio en los términos pactados y el patrono debe remunerar en la forma debida dicha prestación de servicio.

Son aplicables al contrato electrónico laboral, los mismos requisitos que la doctrina y el Derecho positivo reconocen al objeto del contrato en general, así, el objeto del contrato electrónico laboral, debe ser posible, lícito, determinado o determinable.

Aquellos contratos que tengan por objeto la prestación de un servicio informático que son considerados por ello contratos informáticos, pueden llegar a ser contratos informáticos laborales si dicha prestación de servicio se realiza bajo los postulados de las relaciones de trabajo, a saber, prestación personal del servicio, ajenidad, subordinación y remuneración, que serán desarrollados más adelante.

- La causa es el fin objetivo e inmediato que persiguen las partes al contratar, teniendo un enfoque distinto para el trabajador y para el patrono o empleador. Para el primero, la causa del contrato es la obtención de la remuneración por el servicio prestado bajo subordinación, mientras que para el patrono la causa del contrato, es la obtención de los frutos o utilidad de la actividad del trabajador.

Al igual que el objeto del contrato, la causa o fin perseguido por las partes debe ser lícita, por lo que está prohibida la celebración de contratos con causas que vayan en contra de la Ley, las buenas costumbres o el orden público.

En materia de contratos de trabajo y contratos electrónicos laborales, puede existir la expresión de una causa que sea falsa, verificada generalmente en la simulación de contratos que persiguen evadir las normas rectoras de las relaciones laborales y por ende los efectos patrimoniales derivados de las prestaciones de servicio subordinadas propias de los contratos de trabajo ya sea en soporte papel o electrónico (contrato electrónico laboral). Si por el contrario, el contrato tiene la apariencia de un contrato de trabajo, independientemente de su soporte, y no lo es realmente, el contrato es nulo como contrato de trabajo, por falta de causa.

- El consentimiento es uno de los elementos esenciales de todo contrato, no escapando a ello el contrato electrónico laboral. El asentimiento de las partes a obligarse recíprocamente en el cumplimiento de sus respectivas prestaciones, es lo que hace posible la existencia del contrato de trabajo en soporte papel o electrónico (contrato electrónico laboral). Este consentimiento debe ser manifestado en forma libre, por persona capaz, con ausencia de error, dolo o violencia, ya que de lo contrario el mismo estaría viciado, siendo causa de anulabilidad del contrato.

El uso de los medios telemáticos e informáticos en la oferta de servicios y la oferta de trabajo, publicadas en páginas web dedicadas al fomento de las relaciones laborales (Ej. LinkedIn, Bumeran, Uniempleo, entre muchísimas otras) son ejemplos de la **fase de generación del contrato electrónico laboral**, en los que la información está dirigida a números indeterminados de personas, que permite a cada una de ellas, analizar los planteamientos propuestos por cada una de las partes.

Cuando la oferta de trabajo o de prestación de servicios es dirigida a una persona determinada, el medio electrónico empleado con mayor frecuencia, es el correo electrónico, pudiendo ser utilizado igualmente pero con menor frecuencia para este primer contacto, el teléfono y el fax.

Las TIC hacen posible igualmente que las entrevistas propias de la fase de generación de los contratos, se realicen mediante chat o videoconferencia, lo que permite evaluar al aspirante al cargo ofrecido y a su vez que éste evalúe a la empresa. Es posible de igual modo que dichas entrevistas se realicen vía telefónica o por cualquier otro medio electrónico, propio de los contratos electrónicos.

El momento en que las declaraciones de voluntad del patrono y del trabajador coincidan en un mismo sentido, exponiendo su ánimo de celebrar un contrato de trabajo, mediante el cual el trabajador acepta ejecutar un servicio por cuenta del patrono y bajo su subordinación y éste a su vez, acepta remunerarle dicho

servicio, hace entender que se está en la **fase de perfeccionamiento del contrato**, siendo aplicable en el caso de los contratos electrónicos laborales, salvo excepción, las mismas reglas que sobre el envío, recepción y acuse de recibo de los mensajes de datos, proceden para el caso de los contratos electrónicos generales y que en Venezuela están contenidas principalmente en la Ley de Mensaje de Datos y Firmas Electrónicas.

Cabe destacar que en el contrato electrónico laboral, tanto el patrono como el trabajador pueden desempeñar los roles de aceptante y oferente, ya que la iniciativa de comenzar un contrato de trabajo, puede partir del futuro trabajador mediante una oferta de servicios o del futuro patrono que efectúa una oferta de trabajo dirigida bien sea a una determinada persona o a un grupo indeterminado de personas, como se señaló.

Como excepción a las reglas de envío, recepción y acuse de recibo del mensaje de datos, en materia de contratos electrónicos laborales, la sola aceptación de la oferta de trabajo, no perfecciona el contrato, en virtud que bien puede el futuro empleador, negarse a contratar a la persona que se presenta con ánimo de aceptar la oferta, si considera que no satisface el perfil del cargo solicitado, estando en la misma libertad de rechazar la oferta de trabajo, el aspirante a trabajador, si considera que la oferta realizada no le satisface.

En el Derecho laboral venezolano, en atención al principio de no discriminación, no le está permitido al oferente empleador, rechazar la aceptación de la oferta de trabajo realizada, alegando razones basadas en la raza, sexo, edad, estado civil, sindicalización, religión, opiniones políticas, nacionalidad, orientación sexual, discapacidad u origen social del aceptante, ya que se considera que dicha discriminación menoscaba el derecho al trabajo y es contraria a los postulados de la Constitución patria. Asimismo, está prohibido en una oferta de trabajo, hacer mención a condición alguna vinculada en forma directa o indirecta con las razones anteriormente señaladas, ya que se considera que cualquier mención al respecto, podría resultar discriminatoria, dando lugar a las respectivas sanciones de Ley⁷.

Independientemente del medio electrónico empleado para plasmar las ofertas de trabajo y la oferta de prestación de servicios respectivamente, el momento en que coincidan las voluntades del trabajador y del patrono aceptando los términos de la prestación subordinada de servicio por cuenta del patrono y de la remuneración, se entiende que se ha perfeccionado el contrato.

Por regla general, a partir del perfeccionado el contrato, es que las partes están obligadas a ejecutar sus respectivas prestaciones, pero los contratos de trabajo en soporte papel y los contratos electrónicos laborales, son excepción a dicha regla, ya que en virtud del principio de realidad de los hechos sobre las formas, lo que efectivamente determina el inicio del cumplimiento de las

⁷ De conformidad con lo establecido en el artículo 21 de la Ley Orgánica del Trabajo, los Trabajadores y las Trabajadoras.

prestaciones, es la ejecución de la prestación de servicio por parte del trabajador a favor del patrono, independientemente del momento en que el contrato se haya perfeccionado.

Cabe destacar, que si el retardo en el inicio de la ejecución de la prestación de servicio por parte del trabajador, es imputable al patrono (salvando el tema probatorio), por regla general, y como excepción de lo anteriormente expuesto, el patrono debe cumplir con su prestación, vale decir, el pago de la remuneración que se haya pactado.

En el contrato electrónico laboral, la **fase de cumplimiento del contrato**, dada su naturaleza de contrato de tracto sucesivo se verifica durante toda la relación laboral, ya sea en forma tradicional, asistiendo a una estructura física conocida habitualmente como empresa o establecimiento, o fuera de dicha estructura mediante el uso de los medios telemáticos e informáticos, siendo procedente el análisis del uso de las TIC en la prestación del servicio, para determinar la existencia del Teletrabajo.

2.4. Elementos objetivos

El uso de los medios electrónicos en las fases del contrato electrónico laboral, hace indispensable la mención de por los menos dos elementos adicionales a los ya señalados. Dichos elementos son:

- El mensaje de datos, es también un elemento del contrato electrónico laboral, que permite soportar electrónicamente el consentimiento del patrono y del trabajador, elemento indispensable para la formación del contrato, así como el soporte de cualquier otro tipo de información inteligible en formato electrónico o similar que emanada del patrono y del trabajador, pueda ser almacenada o intercambiada por cualquier medio.

- El Sistema de Información (SI), como elemento del contrato electrónico laboral, permite generar, procesar, enviar, recibir y archivar de cualquier forma los mensajes de datos de los patronos y los trabajadores, empleando para ello, un conjunto de elementos que interactúan entre sí con dichos fines.

3. Postulados del Derecho laboral en el contrato de trabajo electrónico

El contrato electrónico laboral, es el resultado del uso de las TIC en el nacimiento de las relaciones de trabajo, en virtud que la voluntad de las partes es manifestada en soportes electrónicos en lugar del tradicional soporte papel que contiene el denominado contrato de trabajo.

Las legislaciones laborales, por regla general, no regulan en forma expresa al contrato electrónico laboral, pero tampoco se desprende de sus normas, que

el soporte papel, deba ser el único medio empleado para plasmar el consentimiento del trabajador y del patrono.

Los postulados del Derecho laboral, son los que en realidad van a determinar si el negocio jurídico bilateral realizado por las partes es objeto de tutela del Derecho laboral. En tal sentido, la verificación de dichos postulados en una relación de trabajo, llevará a la convicción de la existencia de un contrato de trabajo tradicional soportado en papel, o la existencia de un contrato electrónico laboral contenido en soporte electrónico.

Así, planteada la importancia de la presencia de los postulados del Derecho laboral en el contrato electrónico laboral, se señala que además de requerírsele para su existencia el consentimiento de las partes, un objeto que pueda ser materia de contrato, una causa lícita, y la presencia del mensaje de datos y los sistemas de información como sus elementos objetivos, debe desprenderse del mismo, el compromiso de una prestación personal de servicio, con ajenidad, subordinación y mediante la respectiva remuneración, siendo estos los postulados propios del Derecho laboral que permiten diferenciar al contrato electrónico laboral de los demás contratos electrónicos en los que existan prestaciones de servicio. Postulados que con un enfoque especial en la legislación laboral venezolana, se explican de la siguiente manera:

a. La prestación personal del servicio: mediante este postulado, se reafirma el carácter *intuitio personae* del contrato electrónico laboral, e implica que la labor pactada, solo puede ser ejecutada por el trabajador contratado a tal efecto, sin que éste pudiese delegar dicha ejecución en otra persona, de forma tal, que saldrían de la esfera de protección jurídico laboral, aquellas relaciones que buscan solo el resultado de la prestación del servicio, sin importar la persona que ejecuta el mismo.

Conteste con lo anteriormente expuesto, el artículo 53 de la Ley Orgánica del Trabajo, Las Trabajadoras y Los Trabajadores de Venezuela, establece como requisito indispensable para que surja la presunción de laboralidad, que exista una prestación personal del servicio y que otra persona reciba el mismo. En el mismo sentido se ha pronunciado en forma pacífica la jurisprudencia patria al señalar:

(...) Insertos en este orden de ideas, interesa concluir que toda relación jurídica en la que se pretenda atribuir la connotación de laboralidad, se hace forzoso previamente, el evidenciar la prestación de un servicio personal de un sujeto a quien reconocemos como trabajador, para con otro, a quien calificamos como patrono⁸.

8 Sala de Casación Social del Tribunal Supremo de Justicia, N° 489, 13-08-2002 (Mireya Beatriz Orta de Silva contra Federación Nacional de Profesionales de la Docencia, “Colegio de Profesores de Venezuela”). Disponible: <http://www.tsj.gov.ve/decisiones/scs/Agosto/RC489-130802-02069.htm> Consulta: 15/07/2012.

El alcance del elemento “prestación personal del servicio”, en principio podría identificarse con la presencia física en forma simultánea y en un mismo espacio de la persona del trabajador y de su patrono o la persona que a éste represente, pero gracias a las TIC esa “prestación personal del servicio” se puede cumplir ejecutando el servicio desde cualquier lugar independientemente de la ubicación del trabajador y del patrono, sin que pierda su naturaleza de elemento de la relación laboral. Solo deberían implementarse en estos casos, medidas de seguridad que garanticen la identificación del prestador del servicio, utilizándose las claves, firmas electrónicas, los reconocedores de huellas dactilares, reconocedores de voz, entre otras herramientas de seguridad.

b. La subordinación: es el elemento característico de toda relación laboral objeto de los contratos de trabajo y de los contratos electrónicos laborales, al establecerse las obligaciones del trabajador en cuanto al horario de trabajo, sus funciones, la supervisión por parte del empleador, entre otros aspectos, es explicada por Manuel Ossorio, como:

...sujeción a la orden, mando o dominio de uno; por lo que dicese subordinada de la persona sujeta a otra o dependiente de ella. Esta subordinación tiene importancia en Derecho Público, por lo que se refiere a la dependencia jerárquica de los empleados de menor jerarquía a los de mayor jerarquía, tanto en el orden civil como en el judicial, en el eclesiástico y en el militar. Dentro del orden Privado, su principal importancia se encuentra en el Derecho del Trabajo; ya que la subordinación o dependencia del empleado al empleador, constituye una de las características del contrato de la relación de trabajo⁹.

Por su parte el Dr. Rafael Caldera¹⁰ considera que la subordinación jurídica consiste en la obligación asumida por el trabajador, de someterse a las órdenes o instrucciones del patrono, lo que supone para él una merma de su libertad y justifica en su favor una legislación que lo ampare.

Criterio que la autora comparte, al considerar que estando el trabajador sujeto a las órdenes del patrono, y viendo mermada su libertad de acción, es necesaria la existencia de un ordenamiento jurídico que contenga en forma expresa, las obligaciones y derechos de cada una de las partes, en procura de mantener un justo y real equilibrio.

El Dr. Fernando Villasmil¹¹, vincula la subordinación con el derecho definiendo lo que para él es subordinación jurídica:

⁹ Disponible: <http://es.scribd.com/BR%C3%8BN%C3%90%C3%82/d/202240-Diccionario-de-Ciencias-Juridicas-Politicasy-Sociales-> Consulta: 19/07/2012.

¹⁰ CALDERA, R. *Derecho del trabajo*, Tomo I, 2da. Edición. Buenos Aires: El Ateneo, 1960, p 270.

¹¹ BERNARDONI, BUSTAMANTE, CARBALLO, DÍAZ y Otros, *Comentarios a la Ley Orgánica del Trabajo*; Volumen I Barquisimeto: Jurídicas Rincón, 2001, p 136.

Se entiende por subordinación jurídica, la situación del trabajador que lo somete a la obligación de cumplir las órdenes e instrucciones del empleador, en la prestación de servicio. Esta forma de subordinación que también se ha denominado <<subordinación jerárquica>> se puede resumir como lo hace el maestro Pla Rodríguez, en la posibilidad para una de las partes (el empleador) de imprimir, cuando lo crea necesario, una cierta dirección a la actividad de la otra (el trabajador).

En lo que respecta a la subordinación como elemento de la relación de trabajo, la Sala Social del Tribunal Supremo de Justicia, en sentencia de fecha 12 de junio de 2001 con ponencia del magistrado Omar Alfredo Mora Díaz¹², asentó:

... el elemento de la relación de trabajo denominado subordinación, consiste en la obligación que tiene el trabajador, de someterse a las órdenes y directrices que trace el empleador para el desenvolvimiento de su actividad laboral; ello en virtud de que durante la jornada de trabajo, se ve mermada su capacidad de libre actuación, por no poder realizar, a su libre albedrío, cuestiones de índole laboral sin la autorización de su patrono.

En este sentido, el profesor mexicano Mario De La Cueva¹³, afirma: “*donde exista subordinación como poder jurídico, esto es como principio de autoridad, habrá relación de trabajo y faltando ese elemento estaremos en presencia de un contrato de derecho civil*”.

De lo dicho anteriormente, se desprende que la subordinación o dependencia es piedra angular que colabora en gran medida a identificar cuando se está en presencia de una relación laboral originada soportada en forma electrónica (contrato electrónico laboral) o en soporte papel (contrato de trabajo) o sin soporte como el contrato verbal, en el que existe sometimiento al poder de dirección, al poder disciplinario y en sus casos al poder reglamentario del empresario o empleador, o cuando se está ante otro tipo de contrato.

Las TIC han modificado la forma de ejercer el poder de dirección, el poder disciplinario y el poder reglamentario del empleador o patrono sobre el trabajador. Una llamada telefónica, un mensaje de datos vía correo electrónico, o publicado en las redes sociales o mediante un mensaje telefónico o los llamados “PING” entre otros, permite que el patrono le comunique al trabajador cualquier información, desde la forma en que debe prestar el servicio, hasta una

¹² Sala de Casación Social del Tribunal Supremo de Justicia N° 124 12-06-2001 (Román García Machado contra Banco Hipotecario de Inversión Turística de Venezuela, C.A. INVERBANCO). Disponible: <http://www.tsj.gov.ve/decisiones/scs/Junio/c124-120601-01056.htm> Consulta: 13/06/2012.

¹³ DE LA CUEVA, M. *El Nuevo Derecho Mexicano del Trabajo*, 3° Edición. México: Porrúa. S.A., 1975, p 513.

amonestación llegando a la notificación de la finalización de la relación de trabajo, sin olvidar la supervisión que puede ser ejercida con el uso de las TIC.

A manera de ejemplo de supervisión mediante el uso de las TIC, se puede citar el caso de la implantación de un sistema de posicionamiento global conocido por sus siglas en inglés como GPS (*Global Positioning System*), permitiéndole al empleador conocer la ubicación exacta de su trabajador, al mismo tiempo que verifica su jornada laboral, y la prestación del servicio en el lugar que le ha sido asignado, entre otros aspectos. Esta supervisión anteriormente era posible, solo con el traslado físico del patrono o su representante hasta el lugar donde se suponía debía encontrarse el trabajador prestando el servicio.

c. Ajenidad: este postulado vino a determinar con mayor certeza la existencia o no de una relación de trabajo, ya que la subordinación se encuentra por lo general en todos los contratos prestacionales, como mecanismo para la adaptación de la conducta de las partes, a los fines de garantizar la concreción del objeto mismo del negocio jurídico¹⁴. Se encuentra la ajenidad, presente en aquellas relaciones donde los resultados de la realización de una actividad, no repercuten directamente en la persona que la ejecuta, sino en la persona que la recibe, siendo esta última, la beneficiaria de dicha actividad.

La ajenidad se manifiesta en los frutos materiales e inmateriales (quien trabaja no se apropia de los frutos del trabajo), o en los riesgos (quien trabaja no asume los riesgos del trabajo) o en el mercado (es el empleador quien ofrece al mercado los resultados del trabajo).

Dicho en otras palabras, al haber ajenidad, la utilidad patrimonial del trabajo se atribuye al empleador. Los bienes y servicios producidos por el trabajador no le reportan a éste un beneficio económico directo, sino que tal beneficio corresponde al empleador que a su vez, compensa al trabajador con una parte de esa utilidad¹⁵.

La Sala de Casación Social del Tribunal Supremo de Justicia¹⁶, estableció que existirá ajenidad:

Cuando quien presta el servicio se inserta dentro de un sistema de producción, añadiendo valor al producto que resulta de ese sistema, el cual pertenece a otra persona, dueña de los factores de producción, que asume los riesgos del proceso productivo y de la colocación del producto, obligándose a retribuir la prestación recibida; es lógico justificar que este ajeno adquiera la potestad de organizar y dirigir el mecanismo para la obtención de tales frutos, y es precisamente en este

14 Sala de Casación Social del Tribunal Supremo de Justicia, N° 702 27-04-2006 (Francisco Juvenal Quevedo Pineda, contra sociedad mercantil Cervecería Regional C.A.) Disponible: <http://www.tsj.gov.ve/decisiones/scs/Abril/0702-270406-051635.htm> Consulta: 16/08/2012.

15 SIERRA, E. (1999) "Teletrabajo: una aproximación al concepto y regulación jurídico-laboral" Comunicación a la Ponencia Temática III, X Congreso Nacional de Derecho del Trabajo y la Seguridad Social. España: Ministerio de Trabajo y Asuntos Sociales, p 885.

16 Sala de Casación Social del Tribunal Supremo de Justicia, N° 702 27-04-2006, *op. cit.*

estado cuando la dependencia o subordinación se integra al concepto de ajenidad, como una emanación de la misma. De modo que el trabajo dependiente deriva del hecho de prestar un servicio por cuenta de otro.

Las dificultades que existen para la detección de la ajenidad en las relaciones de trabajo sin uso de las TIC no difieren en gran medida de las existentes en aquellas relaciones de trabajo que utilizan las TIC en la prestación del servicio. En estas últimas, la ajenidad en la titularidad de los medios de producción resulta especialmente útil para individualizar el criterio de laboralidad.

La dependencia tecnológica, que se verifica con la propiedad o no del *Know-How* deviene como elemento de contraste, especialmente en aquellas actividades de alto valor añadido, de suerte que si el sujeto ha creado de forma autónoma el software que utiliza, será expresión de su independencia, mientras que quien opera sobre el *Know-How* ajeno, necesita recurrir a los programas bases de datos y ayuda de terceros para conseguir resultados originales, lo que hará mediante su integración en la unidad productiva del titular.

En cuanto a que sea el patrono quien aporte los instrumentos necesarios para desempeñar la actividad, la jurisprudencia ha sido pacífica al considerar que este hecho contribuye a apreciar la existencia de una relación laboral. En el caso de relaciones de trabajo en las que la prestación del servicio involucra el uso de las TIC, se hablaría de la titularidad del sistema Informático incluido el videoterminal, línea telefónica, hardware, software, entre otros instrumentos de trabajo.

d. Remuneración: la remuneración, al igual que la ajenidad y subordinación o dependencia, es un postulado del Derecho laboral, y se define como la contraprestación que recibe el trabajador por la prestación de sus servicios subordinados. En el caso del Derecho laboral venezolano, tiene su fundamento legal principalmente en los artículos 35 y 54 de la Ley Orgánica del Trabajo, las Trabajadoras y los Trabajadores, en los que se establece la obligación de remunerar la prestación de un servicio en la relación de trabajo.

El uso de las TIC en las relaciones laborales, ha permitido variantes en las formas de pago de la remuneración, añadiéndose a los tradicionales cheques y sobres de pago con dinero en efectivo, el pago mediante transferencias electrónicas, que brindan mayores estándares de seguridad tanto para el trabajador como para el patrono.

4. Principios generales del Derecho del trabajo aplicables a los contratos electrónicos laborales

Los principios generales del Derecho del trabajo son las reglas generales que deben ser respetadas tanto para la elaboración de las normas que regulan las relaciones laborales, como para la interpretación de las mismas, siendo

aplicables a los contrato de trabajo en soporte papel, al contrato electrónico laboral y a toda relación laboral en general independientemente de la existencia o no de contrato. Dentro de los principios señalados destacan los siguientes:

a. Irrenunciabilidad de los derechos laborales, según el cual, cualquiera fuere su fuente, es nula toda acción, acuerdo o convenio que implique renuncia o menoscabo de estos derechos.

b. Prevalencia de la realidad sobre las formas o apariencias, el Derecho laboral tutela la efectiva prestación de servicio subordinado, por cuenta ajena, independientemente de la forma que esta adopte, en otras palabras, la denominación del contrato no es el eje rector de la tutela a aplicar, sirve de guía pero lo que realmente se observa es el desarrollo de dicha prestación de servicios y el cumplimiento en ella de los postulados tradicionales del Derecho del trabajo, como son prestación personal del servicio, ajenidad, subordinación y remuneración.

c. *In dubio pro operario*, en atención al cual en caso de plantearse dudas razonables en la interpretación de una norma, deberá adoptarse aquella que más favorezca al trabajador.

d. Principio de no discriminación por razones de política, sexo, raza, credo o por cualquier otra condición, que abarca todas las fases del contrato, vale decir, la fase de generación, perfeccionamiento y cumplimiento o consumación.

e. Aplicación de la normas más favorable, en virtud del cual si se plantearan dudas razonables en la aplicación de dos o más normas, será aplicada aquella que más favorezca al trabajador o trabajadora. En este caso, la norma seleccionada será aplicada en su integridad.

La consagración de los señalados principios en las cartas magnas de los distintos países, es fundamental para el desarrollo armónico de las prestaciones de servicio sujetas al Derecho del trabajo y especialmente las derivadas de contratos electrónicos laborales, que gracias a los medios electrónicos permiten con bastante frecuencia la vinculación jurídica laboral entre partes sujetas a distintas legislaciones. Estos principios, como se dijo, son seguidos por regla general por los países miembros de la Organización Internacional del Trabajo (OIT), haciendo referencia a Venezuela, Colombia, Argentina, Costa Rica, y con mayores diferencias por su situación socio-política Cuba, solo como una pequeña muestra latinoamericana de la consagración de los principios generales del derecho del trabajo, Así:

La Constitución venezolana en su artículo 89 ratifica la protección del Estado hacia el hecho social trabajo y establece en forma expresa tal y como se señaló en el punto anterior, sus principios rectores, destacando entre otros, la irrenunciabilidad de los derechos laborales, la prevalencia de la realidad sobre

las formas o apariencias, el in dubio pro operario, el principio de no discriminación por razones de política, sexo, raza, credo o por cualquier otra condición.

Por su parte, la Carta Magna colombiana, igualmente en forma concentrada, establece en su artículo 53, los principios mínimos fundamentales que deben ser tomados en cuenta por la ley que regule el trabajo, así entre otros señala: la irrenunciabilidad a los beneficios mínimos establecidos en las normas laborales, el in dubio pro operario, la primacía de la realidad sobre las formalidades establecidas por los sujetos de las relaciones laborales, la igualdad de oportunidades para los trabajadores, entre otros.

Las constituciones de Argentina, Costa Rica y Cuba por citar otros países latinoamericanos, establecen de forma dispersa, en varios artículos, algunos de los principios rectores del trabajo, señalados en las Constituciones de Venezuela y Colombia, así: la Constitución de Costa Rica, establece en forma expresa, solo dos de los principios anteriormente señalados, a saber: principio de la no discriminación y principio de la irrenunciabilidad de los derechos laborales.

El principio de la no discriminación, está establecido en el artículo 68 de la Constitución costarricense, pero con una orientación distinta al de la Constitución venezolana, ya que solo se enfoca con relación al salario, ventajas o condiciones de trabajo, haciendo la salvedad que en igualdad de condiciones se debe preferir al trabajador costarricense, lo que a primeras luces pareciera ir en contra del postulado de no discriminación, pero se acepta en la medida que se favorece al nacional.

En lo que respecta al principio de la irrenunciabilidad de los derechos laborales, la Constitución de Costa Rica, establece de una forma general, este principio, al señalar en su artículo 74 que: “Los derechos y beneficios a que este capítulo se refiere son irrenunciables”, cabe destacar que el referido artículo 74, es el último artículo del Capítulo Único del Título V Titulado Derechos y Garantías Sociales, que contiene a su vez, en su artículo 56 la consagración del derecho al trabajo.

Por su parte la Constitución argentina, en su artículo 14, hace mención a la irrenunciabilidad de los derechos, pero solo la establece en forma expresa, en lo que respecta a los beneficios de la seguridad social otorgados por el Estado. En lo que respecta al principio de no discriminación, el capítulo titulado nuevos derechos contiene en su artículo 43 el derecho que tiene toda persona a interponer el recurso de amparo, contra cualquier forma de discriminación, de lo que puede inferirse que la discriminación es contraria a los principios constitucionales, mención que se hace en un capítulo distinto al que contiene el derecho del trabajo, pero como es un enunciado general, a juicio de quien escribe abarca igualmente el derecho del trabajo y las discriminaciones que en el puedan producirse.

La igualdad como principio general está consagrada en el Capítulo VI de la Constitución cubana, en el que se sanciona toda discriminación por motivo de

raza, color de la piel, sexo, origen nacional, creencias religiosas y cualquiera otra lesiva a la dignidad humana. Se destaca el hecho que no hace mención expresa relativa a discriminaciones producidas con ocasión del trabajo, ni por motivos políticos, quedando a la libre interpretación de los operadores jurídicos, si dichas discriminaciones pueden ser encuadradas dentro de la frase que señala cualquier otra discriminación lesiva a la dignidad humana o si por el contrario si está permitida la discriminación por razones políticas.

5. Sujeción del contrato electrónico laboral a la Ley Orgánica del Trabajo, los Trabajadores y Trabajadoras

La Ley Orgánica del Trabajo, los Trabajadores y las Trabajadoras de Venezuela, define en su artículo 55 el contrato de trabajo, como

... aquel mediante el cual se establecen las condiciones en las que una persona presta sus servicios en el proceso social de trabajo bajo dependencia, a cambio de un salario justo, equitativo y conforme a las disposiciones de la Constitución de la República Bolivariana de Venezuela y esta Ley.

Por su parte el artículo 58 de la referida Ley, señala: *“El contrato de trabajo se hará preferentemente por escrito, sin perjuicio de que pueda probarse la existencia de la relación de trabajo en caso de celebrarse en forma oral...”*

De lo anteriormente expuesto, se desprende que la ley laboral venezolana, centra la existencia del contrato de trabajo en los postulados del Derecho laboral ya analizados, señalando que el mismo se hará preferentemente por escrito, pero no hace mención expresa al soporte en que debe reposar dicho contrato, siendo por ende permitido que el mismo conste en soporte papel, soporte electrónico y hasta en forma verbal.

El principio de equivalencia funcional establecido en los artículos 4 y 16 de la Ley de Mensaje de Datos y Firmas Electrónicas LMDFE, a través del cual se equipara el valor jurídico probatorio de los mensajes de datos con los documentos escritos y de la firma autógrafa con la firma electrónica, faculta a los patronos y trabajadores a celebrar negocios jurídicos bilaterales que tengan por objeto el nacimiento y/o regulación de relaciones laborales soportadas electrónicamente, vale decir, los faculta para la celebración de contratos electrónicos laborales.

Los contratos electrónicos laborales, son documentos electrónicos bilaterales que persiguen la creación y/o regulación de relaciones laborales, y que por estar soportado en mensajes de datos, les son aplicables cada una de las normas analizadas en detalle al abordar el tema de los documentos electrónicos, fundamentadas principalmente en la LMDFE de Venezuela.

Por vía de ejemplo, se señala que la sugerencia de escritura del contrato establecida en el citado artículo 58 de la ley laboral, se satisface mediante un documento electrónico, si la información contenida en el mensaje de datos en el que reposa el contrato electrónico laboral, es accesible para su ulterior consulta¹⁷, mientras que la suscripción de dicho contrato, es realizada a través del uso de la firma electrónica¹⁸ en sustitución de la firma autógrafa, y el momento y lugar de su perfeccionamiento por regla general está determinado por el concurso de las voluntades patrono y del trabajador, regidos por las reglas de envío y recepción de los mensajes de datos, entre otros aspectos.

En el caso de los contratos laborales electrónicos por acuerdo entre las partes puede tratarse de cualquier firma electrónica adoptada por las partes con la finalidad de otorgar autenticidad al acuerdo, en el entendido que no es necesario el uso de la firma electrónica basada en un certificado expedido por un proveedor de servicios de certificación acreditado ante la Superintendencia de Servicios de Certificación Electrónica. A tal efecto, es necesario recordar que la propia LMDFE, en su artículo 16 indica los requisitos que debe cumplir la firma electrónica, salvo que las partes dispongan otra cosa, lo cual permite a las partes pactar el tipo de firma electrónica a utilizar en sus relaciones contractuales.

Determinada la procedencia de la celebración de contratos electrónicos laborales en Venezuela, resta señalar que en atención a lo establecido en el artículo 59 de la Ley Orgánica del Trabajo, los Trabajadores y las Trabajadoras, el contrato electrónico laboral, debe contener las especificaciones siguientes:

- El nombre, apellido, cédula de identidad, nacionalidad, edad, estado civil, domicilio y dirección de las partes, en este caso, dadas las características propias del contrato electrónico laboral, se sugiere además del domicilio físico de las partes, su domicilio virtual, pudiendo ser entre otras una dirección de correo electrónico, entendiéndose que los mensaje de datos que allí lleguen, se entenderán que fueron entregados en el domicilio del destinatario del mensaje.

Es de vital importancia, que en ejercicio de la libertad contractual, principio rector de todo documento electrónico, como lo es el contrato electrónico laboral, el trabajador y el patrono, deben fijar las reglas a aplicar para determinar el momento, de envío y recepción de la información contenida en un mensaje de datos y el uso del acuse de recibo si así lo acuerdan. Esto permite, demostrar el cumplimiento de las obligaciones por cada una de las partes, señalando por ejemplo la entrega por parte del patrono de las respectivas notificaciones de nuevos riesgos laborales a los trabajadores, o la entrega del trabajador en forma tempestiva de la labor encomendada, entre otros tantos supuestos.

¹⁷ Aplicación del artículo 8 de la Ley de Mensaje de Datos y Firmas Electrónicas.

¹⁸ Aplicación de los artículos 16 y siguientes de la Ley de Mensaje de datos y Firmas Electrónicas.

También, debe identificarse la firma electrónica que va a ser usada por cada una de las partes, entre otros aspectos tendientes a probar la autoría de los mensajes. En caso de utilizar certificados electrónicos debe hacerse mención de las reglas de uso de los mismos.

- Cuando se trate de personas jurídicas, los datos correspondientes a su denominación y domicilio y la identificación de la persona natural que la represente, siendo aplicable lo señalado en el punto anterior, respecto al domicilio virtual, y al uso de la firma electrónica y del certificado electrónico

- La denominación del puesto de trabajo o cargo, con una descripción de los servicios a prestar, que se determinará con la mayor precisión posible. Por regla general, en las relaciones de trabajo soportadas en contratos electrónicos laborales, es bastante frecuente el uso de los medios electrónicos en la prestación del servicio, siendo por ende requerido que en el contrato electrónico laboral, se deje sentado la forma de uso de dichos medios y su empleo en la ejecución de la labor encomendada, so pena de afectar derechos fundamentales del trabajador como el derecho a la intimidad y al secreto de las comunicaciones.

- La fecha de inicio de la relación de trabajo, que como se dijo, en virtud del principio de realidad de los hechos sobre las formas, está directamente relacionada con el inicio de la prestación de servicio, a menos, que éste se retrase por causas imputables al patrono.

Cabe hacer la salvedad, que en los contratos electrónicos en general, el inicio del cumplimiento de las obligaciones de cada una de las partes coincide normalmente con el momento del perfeccionamiento del contrato. En el caso de los contratos electrónicos laborales, el momento del perfeccionamiento se verifica con el concurso de voluntades pero el inicio de la ejecución de las prestaciones de cada una de las partes, puede estar diferido por voluntad de las mismas.

- La indicación expresa del tipo de contrato a celebrar¹⁹, vale decir, contrato a tiempo indeterminado, en el que no hay un tiempo límite de prestación de servicio, contrato a tiempo determinado que concluirá por la expiración del término convenido y no perderá su condición específica cuando fuese objeto de una prórroga o contrato por una obra determinada que deberá expresar con toda precisión la obra a ejecutarse por el trabajador.

¹⁹ Los artículos 62, 63, 64 y 65 de la LOTTT, establecen las condiciones y causas de celebración de cada tipo de contrato. Normas que como ya se dijo, deben ser cumplidas igualmente en el contrato electrónico laboral.

- La indicación del tiempo de duración, cuando se trate de un contrato a tiempo determinado.
- La obra o la labor que deba realizarse, cuando se trate de un contrato para una obra determinada.
- La duración de la jornada ordinaria de trabajo, sugiriéndose en este aspecto el señalamiento por lo menos en forma general, del uso de los medios electrónicos para verificar el cumplimiento de dicha jornada, además de los métodos tradicionales de supervisión del horario de trabajo.
- El salario estipulado o la manera de calcularlo y su forma y lugar de pago, así como los demás beneficios a percibir. La forma y lugar de pago de las relaciones laborales soportadas en contratos electrónicos, generalmente tiene vinculación directa con la red, empleándose los medios de pago electrónico, con preferencia en las transferencias electrónicas, aspecto que debe ser contenido igualmente en el contrato electrónico laboral, con indicación preferiblemente para efectos probatorios del banco y el número de cuenta en el cual se depositará el salario y demás beneficios laborales.
- El lugar donde deban prestarse los servicios, que dependerá del tipo de trabajo pactado, pudiendo dichos servicios ser ejecutados en una sede física determinada, o a través del uso de las TIC sin importar la ubicación física del trabajador (teletrabajador itinerante) o en sedes móviles.
- La mención de las convenciones colectivas o acuerdos colectivos aplicables, según el caso.
- El lugar de celebración del contrato de trabajo, que en el caso de los contratos electrónicos laborales, se entenderá que el contrato se celebró en el lugar del perfeccionamiento del contrato, vale decir, en el lugar en el que coincidieron las voluntades del patrono y del trabajador. Pero, por ser considerado el trabajador el débil económico, la ley lo protege, pudiendo a nivel de reclamación, intentar la misma donde se encuentre domiciliado o en el lugar donde haya prestado el servicio o en el domicilio de la empresa, haciendo caso omiso al lugar de perfeccionamiento del contrato e incluso al lugar señalado por las partes.
- Cualesquiera otras estipulaciones lícitas que acuerden las partes.

El patrono deberá dejar constancia de la fecha y hora de haber entregado al trabajador el contrato electrónico laboral, mediante acuse de recibo debidamente suscrito por éste, lo que puede hacerse utilizando la herramienta de sellado de

tiempo, o los certificados electrónicos según sea el caso, o simplemente con el envío de un correo electrónico de parte del trabajador que deje constancia de esta situación.

Es importante destacar, que el patrono debe conservar hasta por 10 años (tiempo máximo de prescripción) contados a partir de la finalización de la relación de trabajo objeto del contrato electrónico laboral, el soporte de dicho contrato, por ser ésta una exigencia legal y dado su eventual uso como medio de prueba, la característica más aconsejable del soporte para su grabación es “... una memoria estable, de acceso directo, no estática (removible), permanente, imborrable, ingrabable y que el proceso de grabación sea lo más directo posible, reproduciendo fielmente la voluntad de los contratantes y con métodos y sistemas estándar”²⁰.

6. Valor jurídico del contrato electrónico laboral

Para determinar el valor jurídico del contrato electrónico, es conveniente, traer a colación los principios rectores del comercio electrónico en relación con el documento electrónico, principios aplicables al contrato electrónico laboral por ser éste un documento electrónico laboral bilateral. Estos principios se mencionan en forma ilustrativa en esta parte, siendo los siguientes:

- Principio de equivalencia funcional²¹, que permite equiparar los efectos que producen los contratos que se plasman en soporte papel y son firmados en forma autógrafa por su autor, con los efectos derivados de sus homólogos, los contratos electrónicos, que tienen un soporte y firma electrónica.
- Principio de neutralidad tecnológica, que implica el respeto al uso de cualquier tecnología, impidiendo que se favorezcan unas tecnologías sobre otras, lo que responde a la velocidad de desarrollo e innovación de las TIC que conllevarían a la no vigencia de la norma o contrato que establezca una determinada tecnología para ser usada. Este principio permite celebrar el contrato a través de distintos dispositivos electrónicos.
- Principio de libertad contractual, empleado en la de interpretación de los contratos electrónicos. Se fundamenta en el ejercicio de la autonomía de la voluntad de las partes, quienes deciden libremente emplear en la relación laboral medios electrónicos, ya sea para manifestar su voluntad, para conservar su declaración, para ejecutar lo pactado, o para verificar el cumplimiento de cualquier aspecto que haya sido acordado.

20 BARRIUSO RUIZ, C.: “La Contratación Electrónica”, *op. cit.*, p. 225. Se recomienda su lectura para ampliar la información sobre los sistemas de soportes electrónicos más usuales y sus características.

21 Artículos 4 y 16 de la Ley de Mensaje de Datos y Firmas Electrónicas de Venezuela.

- Principio de inalteración del Derecho preexistente de obligaciones y contratos, que indica que lo acordado en un contrato electrónico laboral, no puede sufrir modificación alguna que esté basada solo en el medio que se utilizó como soporte de las declaraciones de voluntad de las partes.
- Principio de buena fe, que a su vez es un principio general del Derecho, que hace referencia a la observancia de una conducta de honradez, de respeto y lealtad por cada una de las partes del contrato electrónico laboral.

En sintonía con lo expuesto, la Ley Modelo de la CNUDMI²² sobre Comercio Electrónico, norma guía para la interpretación de todo contrato electrónico internacional, y por extensión al contrato electrónico laboral, establece el reconocimiento jurídico de los contratos soportados en mensaje de datos (contratos electrónicos), al señalar que: “*No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos...*”

Por su parte y como expresión de la aplicación de los principios antes señalados, el artículo 15 de la LMDFE de Venezuela, establece que: “*En la formación de los contratos, las partes podrán acordar que la oferta y aceptación se realicen por medio de Mensajes de Datos*”. Dando cabida legal, al empleo del contrato electrónico laboral que por su naturaleza está contenido en un mensaje de datos y que por ley sustantiva no le es exigido su soporte en papel, siendo por ende procedente el soporte electrónico.

7. La presunción de laboralidad en Venezuela

El inicio de una relación laboral, está determinado por el actuar de seres humanos, que con su conducta permiten o pactan la prestación de un servicio en beneficio de una persona distinta a la que ejecuta dicha prestación, lo que se desarrolla con el cumplimiento de ciertas condiciones.

En el campo del Derecho al estar en presencia de supuestos que involucren conductas humanas voluntarias y conscientes de las que se deriven efectos jurídicos, como es el caso de las relaciones de trabajo, se estará hablando por regla general de un “acto jurídico” que se diferencia del “hecho jurídico” en cuanto que el segundo hace referencia principalmente a un hecho de la naturaleza, como el nacimiento o la muerte, mientras que el acto jurídico envuelve la ya señalada conducta humana consciente y voluntaria a la que el ordenamiento jurídico le otorga efectos jurídicos²³.

En las relaciones de trabajo, se presta un servicio en beneficio de otra persona, pudiendo ser dicha prestación sencillamente permitida por el beneficiario

²² Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

²³ MELICH-ORSINI, José: *Doctrina General del Contrato*, Editorial Jurídica Venezolana, Caracas, 1997, p. 21.

sin que haya existido para ello una manifestación de voluntad en forma expresa²⁴, o tratarse de declaraciones de voluntad, destinadas a producir un efecto jurídico, como el caso ya estudiado del contrato de trabajo en soporte papel o electrónico es entendido como un negocio jurídico bilateral dirigido a realizar un facio ut des, en los que el deudor se compromete a cumplir una obligación de “hacer” recibiendo como contraprestación por parte del acreedor una obligación de «dar»²⁵.

En la legislación laboral venezolana, más trascendente que la existencia de un contrato de trabajo sea cual fuere su soporte, lo que efectivamente enciende toda alarma indicativa de tutela jurídico laboral, es la presunción de la existencia de una relación laboral, que se verifica con la prestación personal de un servicio por cuenta ajena, subordinado y mediante una remuneración. Esta posición forma parte de la corriente anticontractualista, que basa la existencia de la relación jurídica en el hecho de la incorporación efectiva del trabajador a la empresa, cualquiera sea el acto que le haya dado nacimiento.

La tesis anticontractualista, tuvo su origen en Europa y posteriormente fue desarrollada en América Latina por el maestro Mario de la Cueva²⁶, quien al referirse a la relación de trabajo señaló:

...es una situación jurídica objetiva que se crea entre un trabajador y un patrono por la prestación de un trabajo subordinado, cualquiera que sea el acto o la causa que le dio origen (...) El derecho del trabajo, es un derecho protector de la vida, de la salud y de la condición económica del trabajador, parte del supuesto fundamental de la prestación del servicio y es, en razón de ella, que impone al patrono cargas y obligaciones.

El artículo 53 de la Ley Orgánica del Trabajo, los Trabajadores y las Trabajadoras, establece la referida presunción de la relación laboral, al señalar lo siguiente: “...se presumirá la existencia de la relación de trabajo, entre quien preste un servicio personal y quien lo reciba”.

De lo anteriormente expuesto, se desprende que el legislador venezolano, dejó abierta la posibilidad de iniciar una relación de trabajo mediante un acuerdo previo de las partes, plasmado en soporte papel o electrónico (contrato electrónico laboral) o el inicio de dicha relación, sin previo acuerdo, solo sujetándose a el resultado de la conjunción entre el “acto” del prestador de servicio y la actitud pasiva del beneficiario del servicio de permitir dicha prestación en su favor.

24 Lo que hace referencia a la presunción de la existencia de una relación de trabajo, en los términos establecidos en el artículo 53 de la Ley Orgánica del Trabajo, Los Trabajadores y las Trabajadoras, tema que será abordado en forma detallada más adelante.

25 MELICH-ORSINI, José: *Doctrina General del Contrato*, op. cit. p. 24, 32.

26 DE LA CUEVA, M. (1975) *El Nuevo Derecho Mexicano del Trabajo*, 3ª Edición. México: Porrúa. S.A. p. 187 – 188.

El hecho de no existir un acuerdo previo entre el prestador del servicio y el beneficiario del mismo, no implica la liberación de obligación alguna, ya que al estar ante la existencia de la relación laboral, automáticamente nace para el patrono beneficiario del servicio, la obligación de remunerar al trabajador que ha prestado el servicio en cuestión, lo que guarda plena sintonía con el artículo 54 de la LOTTT, que establece que *“La prestación de servicio en la relación de trabajo será remunerada”*.

Cabe destacar que la presunción de la relación laboral, es una presunción *iuris tantum*, por lo que admite prueba en contrario, pudiendo desvirtuarse la existencia de una relación de trabajo y todas las obligaciones originadas de su presunta existencia. Para desvirtuar la existencia de relación laboral, debe probarse que los ya explicados, postulados tradicionales del Derecho laboral, a saber: la prestación personal del servicio, la remuneración, la ajenidad y la subordinación, no se verificaron en la relación objeto de análisis.

Desvirtuar la existencia de la relación laboral es un carga del patrono, ya que la presunción de su existencia se aplica en beneficio del trabajador, así como también se presumen ciertas, hasta prueba en contrario, todas las afirmaciones realizadas por el trabajador o trabajadora sobre el contrato de trabajo verbal o el contrato electrónico laboral o en soporte papel que no se consiga o no sea exhibido en juicio, esto de conformidad con lo establecido en el único aparte del artículo 58 de la referida ley laboral.

La transferencia tecnológica: ¿Desarrollo de una política pública en Venezuela?*

Nayibe Chacón Gómez**

SUMARIO: I. Presentación y delimitación del tema. II. El concepto de soberanía a lo «venezolano». III. ¿Alcanzar la soberanía tecnológica debe ser un cometido de las Políticas Públicas en Venezuela? IV. Implicaciones de la transferencia tecnológica. V. Conclusiones

Resumen

El contenido del presente trabajo versa sobre un análisis a lo “venezolano” del concepto de *soberanía* y dentro de esta la llamada *soberanía tecnológica* que se puede alcanzar a través de la transferencia tecnológica, la cual se presenta como una necesidad para el desarrollo de la nación. De igual forma se revisan situaciones político-sociales que se encuentran entrelazadas en la dinámica tecnológica, tales como la llamada “fuga de cerebros” y su consecuencia. Finalmente, se atiende al proceso que envuelve la transferencia tecnológica y sus efectos económicos para la nación.

Palabras clave: Soberanía tecnológica. Transferencia tecnológica. Fuga de cerebros.

Abstract

The present work is an analysis of the concept of Sovereignty Technology that can be reached across the Transfer of Technology, necessary for the development of the nation. Of equal form there are checked situations that are interlaced in the technological dynamics, such as the so called “brain drain” and his consequences.

Key words: Technological Sovereignty. Technological Transfer. Brain Drain.

Recibido: 29/10/2015 • Aceptado: 16/11/2015

* Trabajo preparado para su presentación en el *XII Simposio Venezolano de Ciencia Política*, organizado por el Instituto de Estudios Políticos de la Universidad Central de Venezuela, Caracas, del 4 al 6 de noviembre de 2013.

** Profesora Asociada del Instituto de Derecho Privado de la Facultad de Ciencias Jurídicas y Políticas de la Universidad Central de Venezuela. nayibe.chacon@ucv.ve nayibechacon@yahoo.es

I. Presentación y delimitación del tema

Desde el año 2002 dentro del glosario de términos que utilizamos los venezolanos se encuentra el de “soberanía tecnológica”, entendido como la no dependencia tecnológica a ningún otro país, especialmente si se trata del “Imperio”. Ahora bien, los caminos que conducen a esa soberanía, son de muy diversas índoles y requieren de un gran compromiso de la nación para poder alcanzarla.

La transferencia tecnológica tiene su lugar junto al desarrollo endógeno, la investigación e innovación pertinente y de calidad, la democratización del conocimiento, entre otras, como herramienta para arribar a la “soberanía tecnológica”; es así como presentamos algunas consideraciones entorno a las implicaciones de la transferencia tecnológica como medio para el desarrollo nacional, dentro de las áreas estratégicas contempladas en el *Programa de la Patria 2013-2019*¹.

Manuel Guerrero Gaitán en su tesis doctoral, titulada: “*Hacia el equilibrio contractual en los procesos de transferencia internacional de tecnología en América Latina*”, publicada por la Universidad de Alicante, expone que la transferencia tecnológica representa la forma más adecuada para mitigar la situación de dependencia tecnológica que tienen los países en vías de desarrollo con los países tecnológicamente desarrollados, toda vez que la producción de conocimiento no es homogénea en todos los países. “*Podemos afirmar que nos encontramos ante lo que podríamos denominar una “concentración del conocimiento” en la que solo una pequeña parte del mundo se ubican en los principales productores de conocimientos tecnológicos*”². De allí la importancia del estudio de la transferencia tecnológica como condición necesaria para la llegar a la soberanía tecnológica en Venezuela.

II. El concepto de soberanía a lo “venezolano”:

Se entiende por soberanía:

Es el carácter supremo de un poder que no admite a ningún otro por encima de él, ni en concurrencia con él. Sin embargo, esta noción se remonta a la época del Imperio Romano y se amplía en las concepciones de Rousseau y de Bodin, quienes consideraban la soberanía como un poder absoluto e ilimitado. Pero la

¹ <<http://www.oncti.gob.ve/images/pdf/programapatria.pdf>> (2013).

² GUERRERO GAITÁN, Manuel. *Hacia el equilibrio contractual en los procesos de transferencia internacional de tecnología en América Latina*. Tesis Doctorales Universidad de Alicante. [en línea] Disponible en: http://rua.ua.es/dspace/bitstream/10045/24508/1/Tesis_Guerrero.pdf

noción de soberanía absoluta ha hecho crisis y se ve restringida por la interacción permanente que existe entre los Estados de la comunidad mundial³.

Así, el concepto de soberanía como un elemento esencial al Estado, implica la abnegación de ciertos aspectos de la personalidad internacional de todos los Estados para constituir la sociedad internacional, formada por los Estados libres, con todos los elementos a que hemos hecho referencia.

No obstante ser la soberanía una sola, presenta dos aspectos: de una parte, la *soberanía interior o inmanente*, que es aquella que se ejerce dentro de los límites de su territorio y sobre los individuos residentes en ese Estado⁴; de otra parte, la *soberanía externa o transeúnte*, que es aquella que se refiere a la independencia de un Estado respecto de los otros; es aquella facultad en virtud de la cual un Estado actúa como persona jurídica internacional, con poder suficiente para adquirir compromisos y pactar obligaciones⁵.

En este sentido, la idea tradicional de soberanía es entendida como sinónimo de límites o fronteras territoriales y reconocimiento del país por parte de sus pares internacionales, se encuentra hoy claramente desdibujada.

3 GAVIRIA LIÉVANO, E. (1988). *Derecho Internacional Público*. Tercera Edición. Editorial Temis, S.A. Bogotá, 1988. p. 50.

4 Nuestra Constitución consagra la soberanía interior o inmanente, puesto que el Estado venezolano es soberano y posee la plenitud de jurisdicción para reglamentar todo lo referente a su territorio, en el artículo 11:

La soberanía plena de la República se ejerce en los espacios continental e insular, lacustre y fluvial, mar territorial, áreas marinas interiores, históricas y vitales y las comprendidas dentro de la línea de base rectas que ha adoptado o adopte la República; el suelo y subsuelo de éstos; el espacio aéreo continental, insular y marítimo y los recursos que en ellos se encuentren, incluidos los genéticos, los de las especies migratorias, sus productos derivados y los componentes intangibles que por causas naturales allí se hallen. El espacio insular de la República corresponde al archipiélago de Los Monjes, archipiélago de Las Aves, archipiélago de Los Roques, archipiélago de La Orchila, isla La Tortuga, isla La Blanquilla, archipiélago Los Hermanos, islas de Margarita, Cubagua y Coche, archipiélago de Los Frailes, isla La Sola, archipiélago de Los Testigos, isla de Patos e isla de Aves; y, además las islas, islotes, cayos y bancos situados o que emerjan dentro del mar territorial, en el cubre la plataforma continental o dentro de los límites de la zona económica exclusiva. Sobre los espacios acuáticos constituidos por la zona marítima contigua, la plataforma continental y la zona económica exclusiva, la República ejerce derechos exclusivos de soberanía y jurisdicción en los términos, extensión y condiciones que determinen el derecho internacional público y la ley. Corresponde a la República derechos en el espacio ultraterrestre superyacente y en las áreas que son o puedan ser patrimonio común de la humanidad, en los términos, extensión y condiciones que determinen los acuerdos internacionales y la legislación nacional.

5 El artículo 1° de nuestra Constitución consagra la soberanía externa o transeúnte: La República Bolivariana de Venezuela es irrevocablemente libre e independiente y fundamenta su patrimonio moral y sus valores de libertad, igualdad, justicia y paz internacional en la doctrina de Simón Bolívar, el Libertador. Son derechos irrenunciables de la Nación la independencia, la soberanía, la inmunidad, la integración territorial y la autodeterminación nacional.

La doctrina apunta que

...un Estado soberano es una comunidad humana perfecta y permanente que se gobierna plenamente a sí misma, está vinculada a un ordenamiento jurídico funcionando regularmente en un determinado territorio y en inmediata conexión con el Derecho Internacional cuyas normas en general respeta⁶.

Como dijéramos en la presentación, desde el año 2002 el concepto de *soberanía* para los venezolanos es mucho más amplio que las cuestiones de geografía, se destacan expresiones como *soberanía alimentaria*, que tiene su máximo exponente con la creación en el año 2004 del Ministerio del Poder Popular para la Alimentación; y la *soberanía petrolera* con la modificación en el año 2003 de la estructura de PDVSA y del Ministerio de adscripción.

Actualmente, el contenido del concepto de soberanía se encuentra íntimamente ligado a la figura de la no dependencia en los sectores económicos y productivos, de otros países igualmente soberanos, esto como respuesta al cambio de visión de la geopolítica internacional.

En palabras del autor francés Juillet Alain, *la tecnología define la soberanía mundial*⁷, es por esto que la necesidad de lograr la soberanía tecnológica en Venezuela debe conducir a la transformación e implementación de mecanismos sobre la apropiación social del conocimiento, y evitar la llamada “fuga de cerebros”⁸. La migración de científicos y tecnólogos, e incluso de los ejecutivos o gerentes y de los trabajadores calificados, llamado también “drenaje de cerebros”, es un fenómeno que se viene verificando en el mundo desde hace mucho tiempo; principalmente en los países latinoamericanos, desde la década de los noventa “... se ha agravado por el proceso de globalización, que se caracteriza no sólo por el incremento y la diversificación de los flujos de información, comercio e inversiones a nivel internacional, sino también por la creciente movilización de recursos humanos altamente capacitados”⁹, hábiles de atender la demanda en aumento de mano de obra calificada de las naciones industrializadas.

Se han denunciado como causas de la migración las persecuciones políticas o religiosas, principalmente en los países que sufrieron las consecuencias de la

6 MONROY CABRA, Marcos Gerardo: *Derecho Internacional Público*. 4º Edición, Editorial Temis, S.A. Bogotá, 1998. p. 175.

7 ALLAIN, Juillet: *La tecnología define la soberanía mundial*. [en línea] Disponible en: <http://www.laflecha.net/canales/ciencia/noticias/200405261>.

8 A los efectos de la presente investigación tomaremos en consideración un contenido bastante amplio de la expresión “fuga de cerebros”, puesto que no nos limitamos a entender por “cerebros” solamente a los científicos o graduados con honores universitarios, sino que también incluimos la migración de la mano de obra calificada.

9 DEL BONO, Tulio: “La fuga de cerebros pone en riesgo el futuro”. *La Nación*, Buenos Aires, 12 de noviembre de 2003. p. 15 Opinión. [en línea] Disponible en: http://www.raices.secyt.gov.ar/novedades/fuga_cerebros.htm

Segunda Guerra Mundial. En la actualidad las causas son otras –aunque no podemos descartar las primeras- se originan, básicamente, en razones especialmente económicas.

La baja inversión total –pública y privada- que se destina a financiar la actividad científica y tecnológica provoca que nuestros investigadores perciban salarios entre diez y veinte veces más bajos que los que rigen en los países más desarrollados y deban trabajar con equipamiento de infraestructura que en muchos casos son obsoletos. También impide una posibilidad más fluida para disponer de más cargos en el sistema nacional de ciencia y tecnología, porque no crean nuevos puestos de trabajo y porque se “congelan” las vacantes que se producen¹⁰.

Resulta sumamente interesante el punto, como elemento que mina la posibilidad de lograr en algún momento la codiciada soberanía tecnológica, toda vez que podemos arribar a una conclusión crítica y a la vez paradójica: los países subdesarrollados o en vía de desarrollo forjan los cerebros y la mano de obra calificada que luego sirve a los intereses de las empresas transnacionales y finalmente a la economía de los países más poderosos del mundo permitiendo la hegemonía de los países tecnológicamente soberanos.

III. ¿Alcanzar la soberanía tecnológica debe ser un cometido de las Políticas Públicas en Venezuela?

Las Políticas Públicas han sido definidas como programas que el gobierno desarrolla en función de un problema o situación nacional. De igual forma, al hablar de Políticas Públicas se hace referencia a las actividades de las instituciones u organismos del gobierno, actuando directamente o indirectamente, dirigidas a tener una influencia sobre los ciudadanos.

En este sentido, la transferencia tecnológica, como mecanismo para lograr la soberanía tecnológica, se presenta con un marco conceptual de Política Pública, estructurado desde nuestra norma fundamental, citando a Tibusy Lugo, en su artículo del año 2009 “*La transferencia tecnológica en el Marco de la Apropiación Social del Conocimiento en la República Bolivariana de Venezuela: Aspectos de Política Pública, Legales y Cognitivos*”, es a partir de la Constitución de 1999, que nuestro país “ha logrado definir una política tecnológica y articulada dentro del ámbito político, legal e institucional”.

En Venezuela la incorporación de las Tecnologías de Información y Comunicación, han revestido no solamente un carácter de hecho social¹¹ sino también se han agregado al catálogo de derechos de los ciudadanos. En la

¹⁰ DEL BONO, Tulio: “La fuga de cerebros...”, *ob. cit.*, p. 15

¹¹ El empleo en todos los ámbitos de nuestra vida de los medios electrónicos, han dado lugar a que nuestra sociedad sea conocida como una “Sociedad de la Información y del Conocimiento”, la cual conjuga por una parte, el concepto de Sociedad, y por otra parte, el concepto y alcance de

Constitución de la República Bolivariana de Venezuela del año 1999, se agregaron normas sobre el empleo de las Tecnologías de Información y Comunicación como herramientas para el desarrollo del país.

En la Exposición de Motivos de la Carta Magna del 1999 se lee:

La ciencia, la tecnología, el conocimiento en general, la innovación y sus aplicaciones y los servicios de información, se declaran de interés público, por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. A tales fines, el Estado creará un sistema nacional de ciencia y tecnología que agrupe, coordine y fomente el desarrollo de la investigación en el país, al cual destinará recursos suficientes. La empresa privada también deberá contribuir con sus recursos al desarrollo de esta actividad.

Los artículos 60¹², 108¹³ y 110¹⁴ del texto constitucional evidencian

...la influencia de la tecnología en el ámbito jurídico, al consagrarse el acceso a la tecnología como un derecho fundamental de los ciudadanos, reconociéndose

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

¹² “Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos”.

¹³ “Los medios de comunicación social, públicos y privados, deben contribuir a la formación ciudadana. El Estado garantizará servicios públicos de radio, televisión y redes de bibliotecas y de informática, con el fin de permitir el acceso universal a la información. Los centros educativos deben incorporar el conocimiento y aplicación de las nuevas tecnologías, de sus innovaciones, según los requisitos que establezca la ley”.

¹⁴ “El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos

dentro de los derechos culturales, el carácter de interés público de la ciencia, la tecnología, el conocimiento y la innovación...¹⁵

Luego, se le 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 a los procesos de enseñanza¹⁶.

En opinión de la Profesora Rico Carrillo, que compartimos, la trascendencia que ha tenido la consagración del acceso y uso de las Tecnologías de Información y Comunicación dentro del catálogo de los derechos fundamentales, es verificable en la adopción de distintos textos legales que obligan a la Administración a facilitar el empleo de medios tecnológicos en sus relaciones con los administrados¹⁷.

Así, el artículo 110 antes transcrito,

...establece la obligación del Estado de reconocer el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional¹⁸.

En definitiva son normas que postulan la necesidad de conseguir la soberanía tecnológica.

No obstante, nuestro país no era ajeno de la importancia y las implicaciones del desarrollo de la tecnología, desde finales de la década del cincuenta se evidencia la evolución histórica del aparato institucional de la ciencia y la

fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía".

¹⁵ RICO CARRILLO, Mariliana: "La consagración del derecho de acceso a la tecnología en la Constitución de la República Bolivariana de Venezuela de 1999". AR: *Revista de Derecho Informático*. Editorial Alfa-Redi. No. 055 – Febrero, 2003.

¹⁶ RICO CARRILLO, Mariliana: "La consagración del derecho...", *ob. cit.*

¹⁷ RICO CARRILLO, Mariliana: "La consagración del derecho...", *ob. cit.*

¹⁸ BREWER CARIAS, Allan: "La Constitución de 1999 (con texto oficial de la Constitución Gaceta Oficial N° 5.453 Extraordinario del 24-03-2000)". Tercera Edición. *Colección Textos Legislativos*, N° 20. Editorial Jurídica Venezolana. Editorial Arte. Caracas, 2001. p. 193.

tecnología en Venezuela, así entre el año 1959 y el año 2005, tiene especial importancia la creación en el año 1955 del Instituto Venezolano de Investigaciones Científicas (IVIC) —como expresión de la concreción de un organismo emblemático del quehacer científico nacional— y la presentación del Plan Nacional de Ciencia, Tecnología e Innovación, “*período en el cual el contexto ha estado signado por tres visiones distintas del desarrollo: el modelo de sustitución de importaciones, el modelo neoliberal y el actual modelo de desarrollo endógeno*”¹⁹.

Por otra parte, la mayoría de las leyes que han entrado en vigencia en los años posteriores a la modificación constitucional del año 1999 han tenido en común, un capítulo o una sección referida a la implementación de las Tecnologías de Información y Comunicación en la actividad que regula la ley en cuestión.

Es así como el Estado venezolano se ha acondicionado para recibir las tecnologías y ofrecer el marco jurídico que éstas requieren para un mejor desenvolvimiento, en la búsqueda de proporcionar una mayor calidad tanto a la gestión pública como a la vida de cada uno de los venezolanos, todo en miras de alcanzar la codiciada soberanía tecnológica.

Esto se encuentra delineado en el Plan Nacional de Ciencia, Tecnología e Innovación²⁰, como una herramienta que contribuirá con hacer posible un desarrollo endógeno, sustentable y humano a través del incentivo y desarrollo de procesos de investigación, producción y transferencia de conocimiento de calidad y pertinentes a los problemas y demandas fundamentales que afectan actualmente a la sociedad venezolana y los que potencialmente (mediano y largo plazos), pudieran impactar las áreas económicas, sociales y culturales donde la ciencia, tecnología e innovación desempeñan un rol fundamental.

Construir una cultura científico-tecnológica que oriente sus potencialidades y capacidades hacia la transformación de la sociedad venezolana, a partir de la configuración de valores y modelos de acción que la hagan pertinente, integral, de producción colectiva, comprometida con la inclusión y la vida en el planeta²¹.

En este orden de ideas, las Políticas Públicas para el desarrollo de la soberanía tecnológica, se han presentado no solo como políticas educativas, sino también con la creación de fondos de capitales públicos y privados, a través de la legislación en materia de ciencia, tecnología e innovación, sin dejar de lado el establecimiento

19 Ministerio de Ciencia y Tecnología: *Plan Nacional de Ciencia, Tecnología e Innovación. Construyendo un futuro sustentable. Venezuela, 2005-2030*. Primera Edición, Octubre 2005. p. 31.

20 Ministerio para Poder Popular para Ciencia y Tecnología, *Plan Nacional de Ciencia 2005-2030*. [en línea] Disponible en: <http://www.mct.gob.ve/publico/home/home.php> (2013).

21 Ministerio para Poder Popular para Ciencia y Tecnología, *Plan Nacional de Ciencia, ob. cit.*

de beneficios impositivos para incentivar la inversión privada, nacional y extranjera, en sectores que se han descrito como estratégicos para la nación.

IV. Implicaciones de la transferencia tecnológica

La transferencia tecnológica se presenta como una herramienta para el desarrollo nacional, cuando la misma es vista no como un negocio sino como un medio de acceso a la tecnología necesaria para el progreso del país, que de otra forma no será accesible.

Debemos tener en consideración que nuestra principal industria, la industria petrolera, desde los orígenes de la explotación ha requerido ingentes inversiones en tecnología; y no es la única, todo lo concerniente a telecomunicaciones y más recientemente nuestra incursión en el carrera espacial con la puesta en órbita de dos satélites, industrias altamente tecnológicas y que actualmente se encuentra en manos del Estado, requieren para su funcionamiento la innovación tecnológica, pero que no se quede solo en las empresas privadas y normalmente extranjeras, sino que ese conocimiento sea transferido a capaces receptores nacionales, en otras palabras personal técnico con aptitudes para recibir la nueva tecnología. Así, la transferencia tecnológica es un mecanismo por el que el Estado accede a los recursos o activos tecnológicos que necesita para innovar.

El citado autor Guerrero Gaitán, anota que existen tres (3) vías fundamentales para la realización de la Transferencia Tecnológica, a saber: 1. Los acuerdos de cesión y licencia; 2. Inversión extranjera directa; y 3. Adquisición de equipos e intermediación de productos²².

En Venezuela, de conformidad con el citado Plan Nacional de Ciencia y Tecnología, se busca desarrollar programas de valoración de la investigación a fin de facilitar la transferencia e innovación tecnológica con pertinencia social en las áreas estratégicas para el desarrollo nacional, y en el marco de la cooperación internacional se propicia el intercambio, la transferencia y difusión científico-tecnológica, en el marco de los convenios, redes y proyectos de integración, dados los lineamientos de política multipolar establecidos en la Constitución de la República Bolivariana de Venezuela y la política de cooperación en ciencia, tecnología e innovación orientada hacia la diversificación de las relaciones internacionales; así la transferencia tecnológica se ha presentado bajo las siguientes figuras:

- 1) Contratos de colaboración entre el Estado y los centros del conocimiento (universidades, organismos de investigación y centros tecnológicos);
- 2) Alianzas estratégicas y cooperación alrededor de la investigación y desarrollo, tecnología e innovación;

22 GUERRERO GAITÁN, Manuel: *Hacia el equilibrio contractual...*, ob. cit.

- 3) Creación de empresas del Estado cuya fundamentación es científica y tecnológica;
- 4) Personal especializado en la gestión de gestores de innovación y desarrollo y transferencia tecnológica; y
- 5) Transferencia de tecnología a nivel macroeconómico (entre países y en cooperación al desarrollo).

En palabras del autor Javier González Sabater, fundador del *Instituto de transferencia de tecnología y conocimiento*, en el *Manual de transferencia de tecnología y conocimiento*²³, la transferencia tecnológica es un movimiento, que va desde el proveedor de la tecnología y/ o conocimiento (universidad, centro de investigación, empresa, otro país) hacia el receptor que adquiere la tecnología, en nuestro caso, sería el Estado venezolano, a cambio de una contraprestación económica, en el marco del Sistema Nacional de Ciencia, Tecnología e Innovación; y más recientemente en el marco de la regulación de la Inversión Extranjera.

De conformidad con lo establecido en el Decreto No. 1.438 con Rango, Valor y Fuerza de Ley de Inversiones Extranjeras de fecha 17 de noviembre de 2014, publicado en la Gaceta Oficial No. 6.152 Extraordinario de fecha 18 de noviembre de 2014, la Transferencia Tecnológica es definida como:

El suministro desde el exterior, de un conjunto de conocimientos técnicos expresados o no en derechos de propiedad industrial, necesarios para la transformación productiva, la prestación de servicios y la comercialización de bienes, calificados como tales por el Centro Nacional de Comercio Exterior mediante contrato debidamente aprobado y registrado ante el mencionado órgano, conforme a los procedimientos, requisitos, vigencias y condiciones que se establezcan en el Reglamento del presente Decreto con Rango, Valor y Fuerza de Ley.

Para que la transferencia tecnológica cumpla el cometido de ser una herramienta para “la transformación productiva” y en consecuencia para alcanzar la soberanía tecnológica, será necesario que la transferencia que se verifique sea no solo de elementos tecnológicos sino de conocimiento, es decir que no se limite a una entrega de licencias de uso de patentes o de derecho de autor o venta de bienes y prestación de servicios, sino que abarque la formación del personal e incluso la adecuación social y cultural que permita la mejor recepción de la tecnología y la posibilidad de apropiarse socialmente de la misma, a través de la trasmisión del conocimiento científico (“se trata del dominio del estado del arte de una disciplina científica y del método científico que permite la creación de nuevo conocimiento”) y del conocimiento técnico (“conocimiento y

²³ GONZALEZ SABATER, Javier: *Manual de transferencia de tecnología y conocimiento*. Instituto de transferencia de tecnología y conocimiento. Edición 2, Enero 2011.

habilidades técnicas, generalmente ocultos –como parte del saber hacer y experiencias de las personas de una organización- o de dominio público destinados a prestar servicios más o menos avanzados de: asesoramiento, consultoría, asistencia, ingeniería, ensayos, formación o similares”²⁴ que permita la creación de nuevo conocimiento y el mejor aprovechamiento de la tecnología.

Para estos fines, en el año 2008 fue creada la Comisión Presidencial para la Apropriación Social del Conocimiento mediante el Decreto No. 6.148 de fecha 10 de junio de 2008, publicado en la Gaceta Oficial No. 38.956 de fecha 19 de junio de 2008; ya que la Apropriación Social del Conocimiento,

constituye una Estrategia de Política Pública que busca la asimilación y adaptación de los conocimientos científicos-tecnológicos, acordados en los respectivos contratos comerciales, en la plataforma tecnológica del país, mediante la transferencia de tecnología y la formación de talento humano nacional a nivel operativo, técnico, profesional y científico, con la finalidad de desarrollar y fortalecer capacidades tecnológicas endógenas...²⁵

La Comisión Presidencial para la Apropriación Social del Conocimiento ha sido creada con carácter permanente, y tiene por objetivo detectar las necesidades internas en tecnologías y su dominio, identificando la capacidad real de países aliados que permitan implantar soluciones en el país, mediante la formulación de proyectos estratégicos para potenciar los procesos de innovación tecnológica y producción de bienes y servicios, que prevean la formación y capacitación del talento humano que a mediano y largo plazo deba asumir la generación del conocimiento, con miras a la implantación en el país de productos tecnológicos.

Es preciso señalar que los procesos de transferencia no pueden ser vistos como escenarios exclusivos o excluyentes, es decir, que corresponden solamente a un grupo de investigadores o innovadores, sino que actualmente con el uso de las propias redes de interconexión social, especialmente Internet, se habla de *transferencia tecnológica 2.0*,

...que supone un cambio de mentalidad en la manera de gestionar esta disciplina desde los centros de conocimiento hacia las empresas, y principalmente desde las universidades. Internet y la cultura de lo abierto están modificando la forma de competir, innovar y relacionarse, tanto a nivel empresarial como social²⁶.

24 GONZALEZ SABATER, Javier: *Manual de transferencia de...*, ob. cit., p. 26.

25 RIVERO, Luis: *Análisis Crítico de Políticas Nacionales de Ciencia, Tecnología e Innovación – Venezuela*. [en línea] Disponible en: <https://luisrivero.wordpress.com/2012/04/25/analisis-critico-de-politicas-nacionales-de-ciencia-tecnologia-e-innovacion-venezuela/>

26 GONZALEZ SABATER, J. (2012) *Transferencia de Tecnología 2.0. Conectar hoy con empresas desde universidades y centros tecnológicos*. The Transfer Institute.

VI. Conclusiones

En este punto debemos concluir que para alcanzar la soberanía tecnológica se requiere del diseño e implementación de Políticas Públicas en materia de transferencia tecnológica y transferencia del conocimiento, a través de la adecuación de planes de inversión no solo para el pago de la contraprestación en los contratos de transferencia por parte de las empresas del Estado como receptoras, sino de una significativa inversión en la formación e incentivo del personal científico y técnico llamados a masificar los beneficios de la tecnología transferida y crear con esa base nuevos conocimientos y desarrollos que permitan el logro de los cometidos del Estado.

Posibles soluciones a problemas de la audiencia de casación penal telemática

Gustavo Adolfo Amoni Reverón*

SUMARIO: I. Introducción. II. Modos de participación en la audiencia de casación penal telemática. III. Problemas de la audiencia de casación penal telemática. 1. Identificación de los intervinientes a distancia. 1.1. Método de identificación legal. 1.2. Método de identificación en la práctica de la Sala de Casación Penal. 1.3. Método de identificación en la audiencia de casación penal telemática. 2. Publicidad de la audiencia de casación penal. 3. Suspensión de la audiencia. 4. Privacidad de la comunicación entre las partes y sus representantes judiciales. 5. Diseño de la sala de audiencias. 5.1. La sala de audiencias de casación penal: referencia empírica venezolana. 5.2. La sala de audiencias de casación penal telemática. 5.2.1. Sistema de videoconferencia. 5.2.2. Equipamiento de la sala de audiencias y reorganización de la ubicación de los intervinientes si fuera necesario. IV. Conclusión.

Resumen

La audiencia de casación penal debe celebrarse en la sede del Tribunal Supremo de Justicia. Esto supone traslados y otros gastos que pueden evitarse mediante la videoconferencia, la cual trae ciertos problemas, a los que aquí se proponen algunas soluciones, entre otros: la identificación de los participantes, lo cual se logra con la cédula de identidad igual que ocurre tradicionalmente; la limitación a la publicidad de la audiencia, para lo cual, se podrá comisionar a un tribunal para participar desde allí, evitando la grabación y difusión de la audiencia; la continuidad de la audiencia, de modo que si se interrumiere la transmisión, la Sala podrá ordenar su celebración nuevamente por videoconferencia o de la forma tradicional, garantizando la celeridad

Recibido: 15/10/2015 • Aceptado: 17/11/2015

* Abogado *summa cum laude* de la Universidad de Carabobo (2004), abogado de la Sala de Casación Penal (desde 2005), especialidad en Ciencias Penales y Criminológicas y en Derecho Procesal en la Universidad Católica “Andrés Bello” (Trabajos de grado en desarrollo). Profesor de postgrado de la Universidad Católica “Andrés Bello” (desde 2012) y profesor de pregrado (por concurso público de oposición) de la Universidad Central de Venezuela (desde 2015).

procesal. Resumiendo, los obstáculos advertidos para la audiencia de casación penal virtual encuentran soluciones prácticas y en las leyes vigentes.

Palabras clave: Videoconferencia. Casación penal. Audiencia. Justicia electrónica. TIC.

Abstract

The criminal hearing at the Supreme Court of Justice must be held at the Supreme Court's building. This involves transfers and other expenses that can be avoided through videoconferencing, which brings certain problems. In order to solve them we propose some possible solutions: the identification of participants, which is achieved with the identity card as traditionally occurs; publicity of the audience, for which, the Supreme Court can commission a court near the declarant in order to avoid the recording and broadcasting of the hearing; the continuation of the hearing, so that if the transmission is interrupted, the Supreme Court may order again the celebration of the hearing by videoconference or by the traditional way, ensuring celerity of justice. In short, the perceived obstacles to celebrate the virtual criminal appeal hearing find solutions in practice and on current laws.

Key words: Videoconference. Criminal appeal. Hearing. e-justice. ICT

I. Introducción

La audiencia de casación penal presenta el inconveniente de que únicamente puede llevarse a cabo en un lugar, para todos los casos, sin importar dónde se haya desarrollado el juzgamiento de instancia.

Dicho lugar no es otro que la sede del Tribunal Supremo de Justicia, ubicada en Caracas. Tal situación implica que los abogados privados, el acusado y las víctimas, deban trasladarse a la capital del país si quieren participar en la audiencia, y en caso contrario, el acusado será representado por un defensor público autorizado para actuar ante la Sala de Casación Penal, como sucede en todos los casos con los fiscales que llevaron el proceso en instancia y Corte de Apelaciones, Cortes Superiores de Responsabilidad de Adolescentes o la Corte Marcial, quienes no lo continuarán conociendo durante el procedimiento de casación, puesto que para ello se han designado fiscales especiales para actuar ante la Sala referida, por disposición legal.

Sin embargo, desde que la tecnología permite la comunicación audiovisual en tiempo real entre personas alejadas físicamente, luce innecesario seguir acudiendo a esta práctica tradicional de forma exclusiva, sin brindar la posibilidad de actuación directa a los interesados según su voluntad, concretamente, mediante videoconferencia.

Por tal motivo, se precisarán y analizarán algunos problemas que apareja la intervención en la audiencia de casación penal valiéndose de las Tecnologías de la Información y Comunicación (TIC) y se ofrecerán posibles soluciones al respecto.

En este sentido, el presente artículo se iniciará fijando los modos de participación en la audiencia de casación penal telemática, para continuar, en segundo lugar, determinando inconvenientes vinculados con la identificación de los intervinientes a distancia, con la publicidad de la audiencia de casación penal, con la continuidad de la transmisión de las intervenciones a distancia, con la privacidad de la comunicación entre las partes y sus representantes judiciales y con el diseño de la sala de audiencias.

A medida que se avanza en la precisión de tales dificultades, se irán aportando soluciones desde la normativa jurídica vigente, sin perjuicio de ofrecer propuestas legislativas cuando fuere necesario, para finalizar con un resumen de lo expuesto, a modo de conclusión.

II. Modos de participación en la audiencia de casación penal telemática

La audiencia de casación penal telemática no requiere indefectiblemente una sede física para su realización, ya que al celebrarse por medios electrónicos de transmisión de imagen y sonido, nada impide, desde el punto de vista fáctico, que pudiera efectuarse sin que las personas que deban intervenir estuvieran en el mismo lugar.

Aun así, considerando que el uso de las tecnologías de información y comunicación (TIC) en el proceso jurisdiccional en sede casacional surge como una opción para evitar que los sujetos procesales tengan que trasladarse hasta el lugar donde se ubica el Tribunal Supremo de Justicia para intervenir en dicho acto¹, la desaparición física de la sala de audiencias no incrementaría los medios de acceso a la administración de justicia, sino que sustituiría la audiencia tal y

¹ La posibilidad de intervención jurisdiccional mediante videoconferencia, en especial de los imputados, testigos y expertos, se justifica, entre otras razones: 1) para proteger niños y adolescentes y otros testigos vulnerables de confrontarse con el imputado; 2) para reducir el riesgo de evasiones y de problemas derivados de las evasiones, como daños personales y despliegues policiales masivos; 3) para aumentar la posibilidad de participación de testigos que de otra forma no intervendrían en el proceso; y, 4) para reducir retardos generados porque el imputado (o cualquiera de los intervinientes no judicial) no se presentare a tiempo ante el tribunal por razones de tráfico automotor u otras razones (Van der Vlis, Evert-Jan. *La videoconferencia en los procesos penales*. pág. 13. Consultado el 23 de octubre de 2015 en: http://www.videoconference-interpreting.net/wp-content/uploads/2014/04/02_vanderVlis.pdf). En sentido similar: VEGA DUEÑAS, Lorena C. "La videoconferencia. ¿Un recurso útil al servicio de los medios de prueba?". *Fodertics, estudios sobre Derecho y Nuevas Tecnologías*, España, Andavira, 2012, pág. 411.

como existe hoy día, por su versión digital², lo cual es contrario al espíritu participativo que inspira el uso de la videoconferencia³.

Por tanto, en el presente análisis se evaluarán diversas modalidades en las que puede celebrarse la audiencia de casación penal, considerando para ello la ubicación de los intervinientes respecto de la sala de audiencia, la cual se debe mantener para quienes elijan interactuar de cuerpo presente ante la Sala de Casación de Penal; es decir, se determinará cómo puede ejecutarse la audiencia de casación penal teniendo en cuenta si los intervinientes se encuentran o no en la sede del tribunal, sin más razones que su voluntad de presentarse personal o electrónicamente ante el juzgador colegiado.

Conforme a lo antes indicado, debe precisarse que para lograr la validez de la audiencia de casación penal se requiere la participación de tres sujetos procesales:

1. El Tribunal Supremo de Justicia, quien actuará en Sala de Casación Penal⁴, mediante los cinco magistrados⁵ que la integran junto al secretario y al alguacil⁶;
2. El defensor privado⁷ o público⁸, sin perjuicio del supuesto legal de autodefensa⁹; y,

2 En este sentido, el Plan Europeo de Justicia Electrónica 2009-2013 promueve el uso de las Tecnologías de información y comunicación en el proceso jurisdiccional, incluyendo la videoconferencia. Este plan está orientado a permitir tres funciones básicas: a) acceder a la información judicial, en especial a las bases de datos penales de los Estados Miembros, b) desmaterialización de los procesos, lo que supone comunicación electrónica entre un tribunal y las partes; y c) comunicación entre órganos jurisdiccionales valiéndose de medios tecnológicos como la videoconferencia (consultado el 23 de octubre de 2015 en: <http://eur-lex.europa.eu/LexUriServ.do?uri=OJ:C:2009:075:0001:0012:EN:PD>).

3 Según Barbara Piattoli, la videoconferencia debería contribuir a resolver problemas ligados a la participación del imputado en el proceso jurisdiccional (de todos los intervinientes, estimamos nosotros), no solo para contribuir con el desarrollo de la fase cognoscitiva sino también para garantizar su intervención en la audiencia (Piattoli, Barbara. "Nuove tecnologie e nuove garanzie: L'assunzione della prova tramite videoconferenza", en *L'area di libertà, sicurezza, e giustizia: Alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia*, italia, giuffrè editore, 2007, pág. 154)

4 Artículo 7 de la Ley Orgánica del Tribunal Supremo (LOTSJ) de Justicia publicada en la Gaceta Oficial de la República Bolivariana de Venezuela nro. 39.522 del 1º de octubre de 2010.

5 Artículo 10: "El quórum requerido para la deliberación en cada una de las Salas es la mayoría absoluta de los miembros que la deban integrar".

6 Artículo 8 de la Ley Orgánica del Tribunal Supremo de Justicia.

7 Parte *in fine* del artículo 141 del Decreto con Rango, Valor y Fuerza de Ley del Código Orgánico Procesal Penal (DLCOPP) publicado en la Gaceta Oficial de la República Bolivariana de Venezuela nro. 6.078 Extraordinario del 15 de junio de 2012: "El imputado o imputada no podrá nombrar más de tres defensores o defensoras, quienes ejercerán sus funciones conjunta o separadamente, salvo lo dispuesto en el artículo 148 de este Código, sobre el defensor o defensora auxiliar".

8 Numeral 3 del artículo 127 DLCOPP

9 Artículo 139 DLCOPP

3. El acusador, rol que podrá desempeñar, según el caso, el representante del Ministerio Público¹⁰ solo o junto a la víctima querellante¹¹ (quien actuará asistida o representada por su apoderado judicial privado¹² o por un representante de la Defensoría del Pueblo en quien hubiera delegado el ejercicio de sus derechos¹³), o el acusador privado, en los delitos de acción dependiente de instancia de parte agraviada¹⁴ que tuvieren casación, igualmente asistido o representado por abogado.

Adicionalmente, podrán participar la víctima-no-querellante y el acusado, sin que su ausencia impida el desarrollo de la audiencia¹⁵. Incluso, podrán intervenir testigos cuando el recurso se fundamente en un defecto de procedimiento sobre la forma en que se realizó el acto, en contraposición a lo señalado en el acta del debate o la sentencia, y no pudiere ser utilizado o no se hubiere empleado el medio de grabación de la voz, videograbación u otro medio de reproducción similar que prevé la ley¹⁶.

En consecuencia, si se atiende a la ubicación de los referidos sujetos procesales durante la celebración de la audiencia de casación penal (según se encuentren dentro o fuera de la sala de audiencias), esta pudiera verificarse de múltiples formas, principalmente: 1. Todos los intervinientes ubicados a distancia entre sí (manteniendo la presencia del tribunal en la sede judicial por las razones expuestas); 2. El acusado ubicado a distancia de la sala de audiencias y su defensor en la sala; 3. El defensor junto al acusado y ambos ubicados a distancia de la sala de audiencias; 4. El defensor separado del acusado y ambos a distancia de la Sala; 5. La víctima, querellante o no, a distancia de la Sala de audiencias y el apoderado judicial en la sala; 6. La víctima, querellante o no, junto al apoderado judicial y ambos ubicándose a distancia de la sala de audiencias; 7. La víctima, querellante o no, separada del apoderado judicial y ambos a distancia de la Sala; 8. El representante del Ministerio Público o el acusador privado, según corresponda, a distancia de la sala de audiencias; 9. Los testigos ubicados a distancia de la sala de audiencias; entre otras configuraciones.

En todos esos casos será necesario que el Tribunal Supremo de Justicia pueda:

¹⁰ Artículo 11 DLCOPP.

¹¹ Artículo 278 DLCOPP.

¹² Artículo 87 de la Ley Orgánica del Tribunal Supremo de Justicia: “Para actuar en cualquiera de las Salas del Tribunal Supremo de Justicia se requiere la asistencia jurídica de abogado o abogada que cumpla los requisitos que exige el ordenamiento”.

¹³ Artículo 124 del Decreto con Rango, Valor y Fuerza de Ley del Código Orgánico Procesal Penal.

¹⁴ Artículo 391 DLCOPP.

¹⁵ Cuarto aparte del artículo 458 DLCOPP.

¹⁶ Artículo 455 DLCOPP.

1. Identificar al acusado, al defensor, al representante del Ministerio Público, a la víctima y a su apoderado judicial, así como a los testigos, cuando actúen fuera de la sala de audiencias, y que estos, a su vez, tengan la seguridad de estar desplegando sus actos ante el Tribunal Supremo de Justicia;
2. Limitar la publicidad de la intervención por videoconferencia, cuando fuere pertinente;
3. Regular la continuidad de la audiencia ante eventuales interrupciones en la transmisión de las intervenciones a distancia;
4. Garantizar la privacidad de la comunicación a distancia entre la víctima y su representante judicial, así como también entre el acusado y su defensor, y;
5. Reordenar la sala de audiencia a fin de permitir la participación de los sujetos procesales que decidan actuar de modo telemático sin impedir la actuación plena por los medios tradicionales.

Veamos los problemas prácticos que genera cada una de estas situaciones y cómo pudieran resolverse.

III. Problemas de la audiencia de casación penal telemática¹⁷

1. Identificación de los intervinientes a distancia

1.1. Método de identificación legal

En lo tocante a la identificación de los sujetos procesales que intervienen en la audiencia de casación penal, el DL (Decreto con Rango, Valor y Fuerza de Ley del Código Orgánico Procesal Penal) prevé que el imputado “... será identificado por sus datos personales y señas particulares”¹⁸; que a los testigos “...se les interrogará sobre su nombre, apellido, edad, estado civil,

¹⁷ En Estados Unidos de América se han advertido problemas vinculados al uso de la videoconferencia en el ámbito procesal. La reducción de la calidad de la comunicación entre el imputado y los demás participantes en la audiencia, la disminución de la capacidad judicial de controlar el proceso, así como la existencia de complicaciones en cuanto a la comunicación, que afectan negativamente la calidad y efectividad de la asistencia legal, son algunas de las trabas destacados. Además, se ha afirmado que la videoconferencia puede perjudicar el derecho a la confrontación, al debido proceso, y el derecho a la asistencia legal efectiva, incluso, se corre el riesgo de que las partes miren una imagen en una pantalla en lugar de tener un verdadero contacto visual (VAN DER VLIS, Evert-Jan. *La videoconferencia en los procesos penales*. pág. 17. Consultado el 23 de octubre de 2015 en: http://www.videoconference-interpreting.net/wp-content/uploads/2014/04/02_vanderVlis.pdf).

¹⁸ Artículo 128 DLCOPP, el cual, estatuye además que: “Se le interrogará, asimismo, sobre su lugar de trabajo y la forma más expedita para comunicarse con él. Si se abstiene de proporcionar esos datos o lo hace falsamente, se le identificará por testigos o por otros medios útiles. La duda sobre los datos obtenidos no alterará el curso del proceso y los errores sobre ellos podrán ser corregidos en cualquier oportunidad”.

*vecindad, profesión u oficio...*¹⁹; y que la víctima: 1) al actuar como denunciante, deberá identificarse e indicar su domicilio o residencia y firmar el acta o escrito de denuncia²⁰, 2) al actuar como acusadora privada, deberá expresar “... *Su nombre, apellido, edad, domicilio o residencia y número de cédula de identidad...*”²¹, y 3) al actuar como querellante, manifestará su “... *nombre, apellido, edad, estado, profesión, domicilio o residencia...*”²².

De esta regulación del texto adjetivo penal se evidencia que los intervinientes se identificarán con sus datos personales, pero no se expresa si bastará su sola manifestación y habrá que confiar en su buena fe o si debe constar alguna prueba sobre sus afirmaciones; para ello, debe acudirse a la normativa legal en materia de identificación, específicamente, al Decreto con Rango, Valor y Fuerza de Ley Orgánica de Identificación (DLOI)²³, según el cual, los venezolanos se identificarán mediante dos documentos: 1) con el acta de nacimiento (los menores de 9 años de edad), y 2) con la cédula de identidad²⁴.

Ahora bien, para la actuación judicial, el DLOI estatuye expresamente que la cédula de identidad es el documento principal de identificación²⁵, como se manifestó antes, para los venezolanos de nueve años de edad, o más.

Y es que la cédula de identidad incluye casi en su totalidad lo que el DLOI califica de elementos de identificación: “... *nombres, apellidos, sexo, fecha de nacimiento, lugar de nacimiento, los dibujos de sus crestas dactilares y cualquier otro medio de identificación*”²⁶.

Salvo el lugar de nacimiento, en la cédula de identidad constan los nombres, apellidos, año de nacimiento y la huella dactilar del sujeto identificado. En cuanto al sexo, si bien no se indica expresamente, se evidencia del género usado para indicar el estado civil (Ej. soltero o soltera), situación jurídica que constituye un elemento de identificación adicional en la cédula de identidad, junto a la firma autógrafa, y la fotografía, que funge de “... *otro medio de identificación*”.

Por su parte, los extranjeros se identificarán con pasaporte o cualquier otro documento permitido por tratados internacionales suscritos y ratificados por la República con el país de origen, o con cédula de identidad, en los casos de migración temporal o permanente previstos en la ley²⁷.

Por otra parte, en lo que concierne a la identificación de los abogados privados (defensor y apoderado judicial de la víctima), además de la cédula de identidad, deben demostrar su condición profesional (capacidad de postulación) para actuar

19 Artículo 213 DLCOPP.

20 Artículo 268 DLCOPP.

21 Artículo 393 DLCOPP.

22 Artículo 276 DLCOPP.

23 Publicada en la Gaceta Oficial nro. 6.155 Extraordinario del 19 de noviembre de 2.014.

24 Artículo 3 DLOI.

25 Artículo 13 DLOI.

26 Artículo 4° DLOI.

27 Artículo 8° DLOI.

ante el Tribunal Supremo de Justicia²⁸; es decir, para ejercer la profesión de abogado deben estar inscritos en un Colegio de Abogados y en el Instituto de Previsión Social del Abogado²⁹, que son los requisitos exigidos en el ordenamiento jurídico para ello, como lo manifestó la Sala de Casación Penal en la sentencia nro. 273 del 8 de mayo de 2015:

... para actuar ante la Sala de Casación Penal del Tribunal Supremo de Justicia no se requiere un requisito adicional a los previstos en la Ley de Abogados y en el Código Orgánico Procesal Penal para intervenir en el resto de los tribunales del país; es decir, basta con poseer título de abogado (artículo 3 de la Ley de Abogados); encontrarse en el libre ejercicio de la profesión (artículos 5 y 6 de la Ley de Abogados), salvo en los casos de los defensores públicos y fiscales del Ministerio Público; y estar inscrito en un Colegio de Abogados y en el Instituto de Previsión Social del Abogado (artículo 7 de la Ley de Abogados).

Ahora bien, en lo tocante a los defensores públicos y fiscales del Ministerio Público, la situación es diferente dado que su participación en la audiencia de casación penal responde a una competencia legal que impone su previa designación para ello; en consecuencia, los intervinientes ante el Tribunal Supremo de Justicia no serán los mismos funcionarios que actuaron en los grados procesales previos, en especial, debe resaltarse que no serán los mismos que hubieren presentado el recurso de casación o su contestación, según corresponda.

A propósito de esto, luce oportuna una breve digresión: lo indicado en el párrafo previo se explica pensando en una audiencia a la que debe acudir, únicamente, en persona; sin embargo, esta situación no encuentra justificación ante las posibilidades que ofrecen los medios telemáticos, de ahí que la actuación ante la Sala de Casación Penal por parte de un funcionario exclusivo para tal fin pudiera parecer tan útil como la designación de uno para actuar exclusivamente ante las cortes de apelaciones, por lo cual pudiera considerarse en un reforma legal que el fiscal del Ministerio Público o el Defensor Público que han llevado la causa en instancia, pudieran participar en la audiencia de casación si así lo decidieren; sin perjuicio de mantener, adicionalmente, la posibilidad de nombrar un fiscal o defensor ante la Sala, para evitar traslados obligatorios y garantizar la presencia real en la sede judicial.

²⁸ Artículo 87: “Para actuar en cualquiera de las Salas del Tribunal Supremo de Justicia se requiere la asistencia jurídica de abogado o abogada que cumpla los requisitos que exige el ordenamiento”.

²⁹ Ley de Abogados (Gaceta Oficial nro. 33.357 del 25 de noviembre de 1985). Artículo: 7 “Quien haya obtenido el título de Abogado de la República, de conformidad con la Ley, deberá inscribirse en un Colegio de Abogados y en el Instituto de Previsión Social del Abogado para dedicarse a la actividad profesional” y artículo 78. “Son miembros del Instituto de Previsión Social del Abogado todos los Abogados de la República que se hayan inscrito en un Colegio de Abogados, de conformidad con el Artículo 7 de la presente Ley”.

Retornando al tópico bajo análisis, tal y como se acaba de comentar, el régimen actual supone que se nombre, al menos, un defensor público ante la Sala de Casación Penal³⁰. Así lo hará el Defensor Público General³¹, mediante oficio dirigido al Tribunal Supremo de Justicia, oportunidad en la cual se identificará al defensor con su cédula de identidad.

Igualmente, el fiscal del Ministerio Público será nombrado por la máxima autoridad del órgano público que representa, en este caso, por el Fiscal General de la República³², para lo cual, también se dirigirá oficio al Tribunal Supremo de Justicia, identificándose al fiscal designado mediante su cédula de identidad.

Como puede advertirse, en todos los casos se requerirá presentar la cédula de identidad y adicionalmente, para los casos de abogados ejerciendo representación judicial privada, el carnet de inscripción en un Colegio de Abogados.

1.2. Método de identificación en la práctica de la Sala de Casación Penal

Al acudir a la sede del Tribunal Supremo de Justicia para intervenir en la audiencia de casación penal para la cual fueron citados, el imputado o la víctima, así como también el defensor privado o el apoderado judicial de la víctima, se identificarán mostrando su cédula de identidad, y adicionalmente, los referidos abogados privados deberán mostrar el carnet de inscripción en un colegio de abogados, sin que la falta de este último documento les impida actuar.

Antes de comenzar la audiencia, la referida documentación será presentada ante el alguacil, quien dará cuenta de ello al Secretario judicial, en la Secretaría de la Sala de Casación Penal cuando los participantes anuncien su comparecencia para el acto procesal con ocasión del cual fueron citados.

En el caso del Defensor Público con competencia para actuar ante la Sala de Casación Penal del Tribunal Supremo de Justicia, la referencia empírica más reciente (junio de 2015) se materializó de la manera siguiente: El ciudadano designado dirigió comunicación a la Secretaria de la Sala de Casación Penal informándole que en razón de resolución emitida por el Defensor Público General se resolvió la creación de la Defensoría Pública Tercera con competencia para actuar ante las Salas Plena y de Casación Penal del Tribunal Supremo de Justicia y que además se le designaba para ocupar dicho cargo. En el mismo escrito se solicitó la tramitación necesaria a fin de que le fuera emitida la acreditación correspondiente por parte del Tribunal Supremo de Justicia y se anexó copia de

³⁰ Artículos 95 y 96 de la Ley Orgánica de la Defensa Pública (LODP) en la Gaceta Oficial nro. Gaceta Oficial nro. 39.021, de fecha 22 de septiembre de 2008.

³¹ Artículo 14 LODP.

³² Artículos 32 y 35 de la Ley Orgánica del Ministerio Publicada en la Gaceta Oficial nro. 39.683 del 27 de mayo de 2011.

la resolución donde consta su nombramiento, en el cual se identifica con sus nombres, apellidos y número de cédula de identidad.

En consecuencia, una vez otorgada la credencial pertinente por parte del Tribunal Supremo de Justicia, la identificación del citado funcionario antes de comenzar la audiencia se efectúa mediante tal documento y por conocimiento personal de los miembros de la Sala de Casación Penal, verificando siempre que se hubiese designado para intervenir en el proceso en concreto.

El procedimiento se repite, con las variaciones del caso, con el representante del Ministerio Público designado para actuar ante la Sala de Casación Penal.

Llegados a este punto es necesario enfatizar que la Sala de Casación Penal no sigue otro método que el previsto en la ley para identificar a quienes se presentan en la sala de audiencias afirmando tener derecho a intervenir.

De tal manera, no existe en la práctica de la Sala de Casación Penal un mecanismo de identificación que exceda de las previsiones legales citadas, bastando la presentación de la prueba documental de identificación que prescribe la ley.

Por tanto, cabe preguntarse: Si la audiencia de casación penal se realizare a distancia, ¿bastaría el mismo modo de identificación requerido para la audiencia tradicional o sería necesario agregar algún otro medio de identificación o incluso, exigir un mecanismo de identificación diferente? A esto, se responderá en el epígrafe siguiente.

1.3 Método de identificación en la audiencia de casación penal telemática

La audiencia de casación penal debe desarrollarse en un salón adecuado para que los juzgadores presencien la discusión sobre el recurso de casación que se desarrollará entre el recurrente y la otra parte, de modo que las partes y los representantes judiciales puedan decidir, libremente, si desean apersonarse a la sede jurisdiccional del modo tradicional o si escogen hacerlo por medio de la telemática.

En el segundo caso, no importa cuál de los sujetos procesales elija participar a distancia, ya que su identificación siempre será igual: mostrando la cédula de identidad y en el caso del Defensor Público y del representante del Ministerio Público ante la Sala de Casación Penal, pueden hacerlo mostrando la credencial que les asigna el Tribunal Supremo de Justicia o igualmente, con la cédula de identidad.

Esta simple manera de comprobar la identidad de quien se presenta a la audiencia, también puede efectuarse por videoconferencia³³, mostrando ante la

³³ El argumento para incluir la posibilidad de usar videoconferencia en la Unión Europea radica en que la calidad de la videoconferencia es de tal forma que constituye una decisión responsable usarla en el contexto de la cooperación judicial (VAN DER VLIS, Evert-Jan. *La*

cámara, la cédula de identidad y el carnet de inscripción en un colegio de abogados, o la credencial emitida por el Tribunal Supremo de Justicia, según el caso.

De manera que la identificación telemática no representa dificultades insalvables, dado el método previsto en la ley patria y seguido en la práctica judicial de la Sala de Casación Penal, puesto que en ambos casos, se identifica a la persona del mismo modo: viendo su cédula de identidad. No hay sistemas de identificación biométricos, pruebas de ADN, ni artefactos de análisis de la autenticidad de la cédula de identidad; es la vista humana, y en el caso de la presencia tangible, el tacto, los medios por los que se verifica que una persona sea quien dice ser, exhibiendo para ello su documento de identificación.

A título comparativo, es oportuno comentar que en España, el artículo 299 de la Ley Orgánica del Poder Judicial prevé que en caso de intervención procesal mediante videoconferencia, el secretario judicial del juzgado o tribunal acreditará, desde la propia sede judicial, la identidad de las personas mediante la previa remisión o la exhibición directa de la documentación, por conocimiento personal, o por cualquier otro medio procesal idóneo.

Sobre la base de la experiencia citada, no resulta impensable que la verificación de la identidad pueda hacerse en un acto telemático previo a la audiencia virtual, mostrando al Alguacil o directamente al Secretario de la Sala de Casación Penal, la cédula de identidad, pudiendo comprobarse, según corresponda, que quien se presente sea el abogado que ostenta la representación requerida para actuar en la audiencia, por ser el último designado al efecto. Tal acto previo deberá comunicarse en la citación para garantizar que el interviniente a distancia efectúe este trámite necesario para poder actuar en la audiencia de casación penal telemática.

Cuando la declaración se hiciera desde la sede del tribunal comisionado, la verificación de la identidad de quien se presente afirmando ser la persona citada puede hacerse igual que en el caso anterior o incluso, puede llevarse a cabo por parte del alguacil de dicho órgano. Para ello, el Tribunal Supremo de Justicia anexará al oficio de comisión una copia de los documentos donde conste la designación y juramentación del defensor o del poder otorgado al representante judicial de la víctima. En caso de revocación del defensor para el momento de la audiencia, el nuevo profesional del derecho deberá juramentarse, bien sea a distancia ante el Tribunal Supremo de Justicia o ante el operador judicial desde donde se emita la declaración.

En España, Carolina Fons Rodríguez³⁴ considera que el art. 229 de la Ley Orgánica del Poder Judicial español debe interpretarse de manera que el

videoconferencia en los procesos penales. pág. 15. Consultado el 23 de octubre de 2015 en: http://www.videoconference-interpreting.net/wp-content/uploads/2014/04/02_vanderVlis.pdf.

³⁴ LA VIDEOCONFERENCIA EN EL PROCESO CIVIL (LA TELEPRESENCIA JUDICIAL). <http://www.uv.es/coloquio/coloquio/comunicaciones/sp2fon.pdf>

secretario del tribunal al cual le compete acreditar la identidad del declarante no sea el del tribunal que conoce la causa a distancia sino aquel desde donde se emita la declaración.

Sin embargo, en el caso venezolano, tal como se expresó antes, no pareciera haber razones para diferenciar la posibilidad de identificar a una persona viendo su cédula de identidad directamente, que viéndola proyectada en una pantalla; por tanto, se estima que la visualización del documento de identificación del declarante a distancia es equiparable a su visualización inmediata, cumpliéndose con ello el método legal y práctico de identificación de los intervinientes en la audiencia de casación penal.

Con lo expresado hasta ahora se resuelve el problema de la determinación de la identidad, y con ello de la legitimación y representación de los participantes ante el órgano jurisdiccional, pero no sucede lo mismo con la identidad de los miembros del Tribunal Supremo de Justicia.

En el caso español, la citada Ley Orgánica del Poder Judicial prevé en el numeral 4 del artículo 230 que: “*Los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce...*”.

De modo que el texto jurídico aludido reconoce la problemática que apareja este asunto: ¿Cómo sabrán los intervinientes que están actuando ante la Sala de Casación Penal del Tribunal Supremo de Justicia?

La respuesta parece ser simple: por hecho notorio, que es la misma manera por la que saben que se encuentran en la sala de audiencias de la Sala de Casación Penal cuando acuden en persona para actuar en juicio.

Concretamente, así como en la práctica no parece creíble que alguien ponga en duda que la sala de audiencias de la Sala de Casación Penal del Tribunal Supremo de Justicia está ubicada en el piso cuatro del edificio del Tribunal Supremo de Justicia, ubicado al final de la avenida Baralt, en la esquina «Dos Pilitas», municipio Libertador, parroquia Altagracia, Caracas, Republica Bolivariana de Venezuela, cuando se encuentre en dicho recinto para una participar en una audiencia de casación, de la misma manera, no podrá negarse que se está actuando ante los magistrados de la Sala cuando la conexión se realice mediante un enlace obtenido de la página de internet del Máximo Tribunal, cuya información tiene el mismo carácter oficial que la información impresa que emitan, según lo dispuesto en el artículo 18 de la Ley de Infogobierno.

En consecuencia, si una persona debe acceder a la página de internet oficial del Poder Judicial tendrá garantías de que la comunicación será con los magistrados del Tribunal Supremo de Justicia y no con terceros no autorizados.

Incluso, para mayor seguridad, el interesado pudiera recibir una comunicación en papel, o electrónica con firma digital o certificada, emanada del Tribunal Supremo de Justicia, manifestándole la forma en la que se satisfará su petición

de participar en la audiencia³⁵ valiéndose de los avances de la telemática, y así evitar trasladarse hasta la sede física judicial.

Recapitulando lo expresado, se advierte que el método de identificación personal que establece la ley para las actuaciones judiciales, consiste en mostrar la cédula de identidad a la autoridad judicial, lo cual, también puede hacerse a distancia, enseñando el documento ante la cámara de video para que su imagen sea proyectada en una pantalla a la vista de quienes deban comprobar la identificación del interviniente en la audiencia o simplemente, mostrarla a la autoridad judicial desde donde se emita la declaración.

Además, al acceder al sistema telemático que pudiera estar disponible en la página de Internet del Máximo Tribunal o que se indique en la citación que reciba el sujeto procesal que intervendrá en la audiencia de casación penal, tendrá la seguridad de estar actuando ante los integrantes de la Sala de Casación Penal, dejando de lado cualquier duda razonable al respecto.

Así, es importante destacar que en virtud de que la declaración del sujeto procesal que intervenga a distancia pudiera ser transmitida por Internet y no por canales de comunicación exclusivos del Poder Judicial, surge un nuevo problema pero esta vez vinculado a los límites de la publicidad de la audiencia, aspecto que se abordará a continuación.

2. Publicidad de la audiencia de casación penal

El artículo 458 COPP prevé que la audiencia de casación penal será pública, norma que debe interpretarse en conjunto con los artículos que regulan la publicidad de las fases procesales previas, especialmente con el juicio oral y público, el cual tendrá tal carácter salvo las excepciones de ley³⁶ y cuando el tribunal decidiera lo contrario por estimar que se perturbaría el normal desarrollo del juicio³⁷.

En este sentido, así como el tribunal de juicio puede limitar la publicidad de la audiencia, la Sala de Casación Penal del Tribunal Supremo de Justicia pudiera hacerlo, por las mismas razones.

No obstante, la audiencia es pública³⁸ y no habría más impedimento para difundirla, incluso en los medios de comunicación³⁹, salvo en los casos previstos en la ley y por voluntad del tribunal, sobre la base de la regulación normativa constitucional y procesal penal aplicable.

³⁵ Puesto que se trata de un derecho de los intervinientes quienes pueden escoger, con independencia entre sí, si actúan asistiendo personalmente a la sala de audiencias o lo hacen por videoconferencia.

³⁶ Artículo 15 COPP.

³⁷ Artículo 316 COPP.

³⁸ Para Evert-Jan Van der Vlis, la publicidad de la audiencia queda satisfecha si cualquier miembro del público (el público en general según la capacidad de la sala de audiencias, consideramos nosotros a fin de equiparar lo más posible la audiencia telemática y la tradicional) puede sentarse

Ello genera que el lugar desde donde participará el interviniente a distancia en la audiencia de casación penal pudiera ser aquél que él mismo escogiere, salvo que la ley prescribiere que la audiencia fuere privada o que el tribunal considere conveniente para el normal desarrollo del proceso limitar la publicidad a los presentes en la sala de audiencias. En ese caso, la transmisión deberá efectuarse desde una sede jurisdiccional o recinto de reclusión para procesados, según el caso, previa comisión o decisión judicial.

Lo anterior se justifica ya que si el declarante a distancia actuare desde un lugar en el que mantuviere el control, tendría la posibilidad fáctica de transmitir en vivo la audiencia y difundirla en los medios de comunicación, incluyendo Internet, o grabarla y publicarla posteriormente, en la oportunidad que lo decidiera, lo cual no ocurre así en caso de transmitir la intervención desde una sede judicial, controlada por el juzgador, unipersonal o colegiado.

En este orden de ideas, es importante destacar que el interviniente mediante TIC deberá ser citado expresamente para una audiencia totalmente pública, limitada a los presentes en la sala de audiencias o privada, de modo que sepa que solo en el primer caso pudiera transmitir su participación desde cualquier lugar que le permita actuar por videoconferencia, mientras que en los otros dos supuestos, deberá hacerlo desde una sede judicial equipada con los implementos correspondientes.

En síntesis, la publicidad judicial no limita la transmisión de la audiencia de casación penal en los medios de comunicación, incluida Internet, por lo que el sujeto procesal que participe en la audiencia de casación penal podrá hacerlo desde donde prefiera, pero, si la Sala de Casación Penal, por los supuestos de ley o por razones de buen desarrollo del proceso debiere o decidiera, respectivamente, descartar o restringir la publicidad, entonces deberá comisionar a un tribunal de la localidad más cercana al domicilio del declarante para que le proporcione un lugar, bajo su autoridad, para la participación a distancia, garantizándose niveles de seguridad suficientes para evitar que terceros no autorizados logren acceder a la transmisión de la audiencia reservada.

en la sala de audiencias del modo acostumbrado, visibilizando adecuadamente las pantallas (VAN DER VLIS, Evert-Jan. *La videoconferencia en los procesos penales*. pág. 21. Consultado el 23 de octubre de 2015 en: http://www.videoconference-interpreting.net/wp-content/uploads/2014/04/02_vanderVlis.pdf).

³⁹ A criterio de Lorena Vega, la videoconferencia permite mayor publicidad de las actuaciones judiciales porque más personas podrán seguir el proceso sin necesidad de estar en la sala de audiencias (Lorena C. VEGA DUEÑAS. “La videoconferencia. ¿Un recurso útil al servicio de los medios de prueba?”. *Fodertics, estudios sobre Derecho y Nuevas Tecnologías*, España, Andavira, 2012, pág. 414).

3. Suspensión de la audiencia

Otro aspecto que necesariamente debe tomarse en cuenta al momento de organizar la participación en la audiencia de casación penal por medios telemáticos, es la posibilidad de que tal acto procesal se suspenda, incluso, varias veces y hasta por un lapso indeterminado, como consecuencia de interrumpirse la transmisión de alguna de las intervenciones a distancia.

Tales interrupciones pueden deberse a dificultades vinculadas con: 1) aspectos técnicos propios de la transmisión en el lugar donde se encuentre el participante a distancia, los cuales pudieran estar vinculados con el sistema informático utilizado (Ej. Retraso en la transmisión) o con el equipo de recepción de la señal (Ej. Daños del sistema de sonido); 2) aspectos técnicos en la sede del Tribunal Supremo de Justicia; o 3) situaciones comunes a ambos ámbitos geográficos, lo que pudiera surgir como consecuencia de la suspensión o fallas en el servicio de electricidad o de telecomunicaciones.

En todos estos casos, el Magistrado Presidente, como director del debate, deberá procurar la culminación de la audiencia de casación penal el mismo día o dentro del menor lapso posible. Así lo prescribe el principio de concentración que informa el proceso penal: **Artículo 17:** “Iniciado el debate, éste debe concluir sin interrupciones en el menor número de días consecutivos posibles”.

Teniendo esto en cuenta, mientras se dicta la normativa legal o reglamentaria pertinente, corresponderá al Presidente de la Sala de Casación Penal, en su condición de director del debate⁴⁰, mantener el orden en la audiencia⁴¹ interrumpida decidiendo si se suspende la audiencia por el lapso que estime prudencial para solventar el problema u ordena su diferimiento, según la duración de la interrupción.

De modo que ante la imposibilidad de continuación de la audiencia de casación penal, luego de un tiempo prudencial, el cual se propone que pudiera ser de 45 minutos desde el momento de la interrupción⁴², la Sala de Casación Penal, siguiendo las previsiones del COPP, declarará la suspensión de la audiencia y anunciará el día y hora en que continuará el debate, lo cual valdrá como citación para todas las partes⁴³, salvo las que no lograren establecer comunicación con

40 Numeral 5 y único aparte del artículo 22 LOTSJ.

41 Numeral 11 y único aparte del artículo 22 LOTSJ

42 Este es el tiempo promedio aproximado de duración de una audiencia de casación penal según apreciación empírica del autor. Además, así como el lapso de intervención de los participantes en la audiencia de casación penal no está fijado en las leyes (diez minutos para cada una de las intervenciones iniciales, cinco minutos para la réplica y la contrarréplica, respectivamente, y no está definido para el imputado sino que el Presidente de la Sala estimará cuándo fuere suficiente su exposición), de la misma manera, el Magistrado Presidente de la Sala de Casación Penal, mientras se dicta la regulación legal pertinente, pudiere establecer el lapso que razonablemente estimare conveniente.

43 Artículo 319 COPP.

la Sala mientras no se hubiere diferido la audiencia, a las cuales habrá que citar, preferiblemente, mediante la dirección de correo electrónico indicada en el expediente o por cualquier otro medio legal que sirva al efecto⁴⁴.

Incluso, abonaría al principio de seguridad jurídica, que en la citación para la audiencia virtual requerida al momento de presentar el recurso de casación penal, se indicara que la audiencia quedará diferida para el momento que se determinará en una nueva citación, luego de transcurrido el tiempo referido en el párrafo anterior.

Con ello, se evita que el participante a distancia tenga que esperar indefinidamente a que se restablezca la conexión, lo cual pudiera ocurrir incluso horas después de la interrupción, por miedo a que ante su inasistencia telemática se continuare la audiencia sin la parte ausente y en el caso del acusado, se le designare un defensor ante la Sala en lugar del abogado de confianza con el que estaba participando antes de la interrupción de la comunicación.

El procedimiento expresado puede seguirse válidamente puesto que al no estar regulada jurídicamente tal situación, la Sala de Casación Penal puede aplicar el procedimiento que juzgare más conveniente para la realización de la justicia, siempre que tenga fundamento legal⁴⁵.

En este orden, es necesario fijar un procedimiento con base de derecho para resolver qué hacer en caso de suspensión de la audiencia de casación penal telemática, y así ofrecer seguridad jurídica a los intervinientes a distancia.

En especial, debe enfatizarse que sería factible que el sujeto procesal que estuviera participando a distancia interrumpiera dolosa o culposamente la audiencia, en el primer supuesto, por razones de estrategia procesal fraudulenta, en cuyo caso, pudiera establecerse que ante una nueva interrupción el solicitante de la audiencia telemática deberá acudir de cuerpo presente a la sede judicial so pena de continuarse la audiencia con las partes que asistan, con la intervención del defensor público ante la Sala, si el defensor privado no concurriera oportunamente.

En el problema hipotético descrito se toma como referencia para resolverlo la regulación procesal penal establecida para la negativa del imputado de acudir a la audiencia preliminar⁴⁶ o al debate oral y público⁴⁷, incorporada en la reforma del texto adjetivo penal de 2012, según lo determina el artículo 98 LOTSJ (Ley Orgánica del Tribunal Supremo de Justicia) para los casos de ausencia de regulación especial con ocasión de los procesos que cursen ante el Tribunal Supremo de Justicia⁴⁸.

44 Numeral 4 del artículo 91 LOTSJ y único aparte del artículo 85 *eiusdem*.

45 Artículo 98 LOTSJ.

46 Artículo 310 COPP.

47 Artículo 327 COPP.

48 En España, la Ley de Enjuiciamiento Criminal prevé que el imputado podrá declarar en la fase de investigación y en la fase del plenario mediante videoconferencia (Lorena Cecilia Vega, “La

De no actuarse de esta manera se corre el riesgo de extender indefinidamente la celebración de la audiencia de casación penal con los inconvenientes que ello supone para la debida administración de justicia, en especial cuando se trata de la posible verificación de la prescripción extraordinaria de la acción penal.

Y es que, bien sea que la imposibilidad en la realización de la audiencia telemática se produzca por causas imputables al interviniente a distancia, a la Sala de Casación Penal o a circunstancias extraordinarias, el director de la audiencia deberá considerar, razonadamente, si insistirá en la práctica a distancia de la audiencia correspondiente o si ordenará su celebración de forma tradicional.

Al respecto, debe reiterarse que la audiencia de casación penal virtual no es un derecho absoluto de los interesados sino que responde tanto a la realidad jurídica como fáctica del sistema de justicia y de los propios sujetos procesales que ejerzan algún rol activo en el desarrollo del debate sobre el recurso de casación.

Ello quiere decir que el Presidente de la Sala de Casación Penal puede limitar el ejercicio de este derecho a relacionarse con la Sala de Casación Penal por los medios informáticos de ley, cuando las circunstancias denoten que lejos de favorecer la celeridad procesal y el derecho a la defensa, las TIC redunden en la obstaculización del buen desarrollo de la administración de justicia accesible, idónea, expedita, sin dilaciones indebidas sin formalismos ni reposiciones inútiles que garantiza la Constitución⁴⁹.

4. Privacidad de la comunicación entre las partes y sus representantes judiciales

En el desarrollo de la audiencia de casación penal, puede suceder que el acusado quiera comunicarse en privado con su defensor, así como también que la víctima quiera hacerlo con su representante judicial, según lo permite el artículo 332 COPP durante el debate oral y público, aplicable supletoriamente a la audiencia de casación conforme a lo establecido en el artículo 98 LOTSJ, tantas veces citado.

Tal norma prevé que el acusado podrá hablar en todo momento con su defensor, sin que por ello la audiencia se suspenda y siempre que no interrumpa la audiencia, por lo cual se le ubicará a su lado.

Pero cuando la audiencia se celebra por medios telemáticos y la parte está separada de su abogado, será necesario establecer un medio para garantizarle tal derecho.

Esto pudiera resolverse, simplemente, permitiendo eliminar el sonido que se transmite desde el lugar donde se encuentre la parte y su abogado, para que no

videoconferencia: ¿Un recurso útil al servicio de los medio de prueba?”, en *Fodertics. Estudios sobre derecho y Nuevas tecnologías*, Española, Andavira, 2012, pág. 411.

⁴⁹ Artículo 26 de la Constitución.51Numeral 1 del artículo 15 LOTSJ.

se escuche en la audiencia lo que ellos conversen, usando, por ejemplo, un teléfono celular o algún otro medio de comunicación autorizado por la Sala en atención a la buena marcha de la audiencia de casación penal.

Tal modalidad permitiría comunicar privadamente al acusado con su defensor o defensores, y a la víctima con su(s) representante(s) judicial(es) sin que se perturbe necesariamente la audiencia.

En todo caso, si el contacto telecomunicacional al que tienen derecho las partes resultare en algún tipo de molestia a los presentes en la sala de audiencia, el alguacil podrá intervenir⁵⁰ para requerir que cese la comunicación de la manera que se está produciendo, resguardando en consecuencia, la majestad del acto y el derecho a la defensa.

Lo mismo podrá ordenar el Presidente de la Sala de Casación Penal en aras de posibilitar un debate sobre el recurso de casación, que sea adecuado para que los intervinientes puedan participar en un plano de igualdad de oportunidades, respetando el derecho del otro a expresarse sin interrupciones y con plena atención de los magistrados.

5. Diseño de la sala de audiencias

5.1. La sala de audiencias de casación penal: referencia empírica venezolana

La sala de audiencias de la Sala de Casación Penal está organizada en tres secciones. La sección más amplia es el área dispuesta para el público, la cual cuenta con capacidad de cincuenta asientos ubicados en filas de diez y con inclinación ascendente, de la primera hacia la última fila.

La segunda sección, o sección central, está reservada para las partes y sus abogados. En ella se encuentran cuatro mesas con dos o tres sillas cada una, a las cuales se le pueden incluir más, si fuera necesario, y están dispuestas de la manera siguiente:

1. Una mesa con tres sillas está ubicada a la derecha del público y a la izquierda de los magistrados. Allí se ubica el Secretario de la Sala, un asistente del Secretario y el Alguacil. A la derecha del Secretario, de pie, se encuentra un funcionario de la Guardia Nacional Bolivariana, quien complementa la seguridad junto a dos funcionarios de seguridad que se ubican en la puerta de la Sala y otro más en la puerta de la antesala.

2. En la segunda mesa se ubica el defensor y el imputado, de frente a los magistrados, de espalda al público y diagonal a la ubicación de la mesa anterior.

⁵⁰ Numeral 1 del artículo 15 LOTSJ.

3. A la izquierda, y en línea recta, se localiza la tercera mesa, igualmente frente a los magistrados y de espaldas al público. Este es el espacio del representante del Ministerio Público.

4. La cuarta mesa puede observarse a la izquierda del público y a la derecha de los magistrados, exactamente frente a la primera mesa y al otro extremo de la sala de audiencias. Es el lugar en el que le corresponde situarse a la víctima y a su representante judicial.

Por último, la tercera sección conforma lo que pudiera denominarse: el estrado. Es el sitio donde se encuentran los cinco magistrados durante la audiencia, y es más elevado que el área central, donde se ubican las partes y los abogados intervinientes. Este sector está separada del resto de la sala de audiencias por un escritorio que se extiende de un extremo a otro de la sala, desde la pared donde se encuentra la víctima y su representante legal, según el caso, hasta la pared donde se ubica la Secretaria y los demás funcionarios mencionados. Desde allí hay una visión frontal de todos los intervinientes y del público presente.

Debe destacarse que en todas las mesas, así como en el estrado, se ubican micrófonos para que los participantes efectúen sus declaraciones, salvo que prefieran hacerlo a viva voz, siempre que los magistrados y la otra parte escuchen con claridad la exposición.

5.2. La sala de audiencias de casación penal telemática

Cuando la audiencia de casación penal incluya la actuación telemática de al menos un participante, será imprescindible reorganizar la sala dispuesta para ello⁵¹, con miras a lo cual debe tenerse presente la necesidad de instalar un sistema de videoconferencia y de dotar la sala de audiencias de los demás implementos necesarios, cambiando la ubicación de los intervinientes si fuera necesario y teniendo en cuenta que todos los intervinientes deben contar con la posibilidad de interactuar como si estuvieran reunidos en el mismo lugar; es decir, verse, oírse y hablarse entre sí.

Tales implementos han sido clasificados por Patricia Estévez Huevra⁵² en seis grupos, atendiendo a la función que desempeñan:

⁵¹ Al respecto puede consultarse la Guía sobre videoconferencias en procedimientos judiciales transfronterizos, disponible en: https://e-justice.europa.eu/content_manual-71-es.do

⁵² (Patricia ESTEVÉZ HUEVRA: “La viabilidad de los medios telemáticos en el acto de conciliación de la audiencia previa”. *Fodertics, estudios sobre Derecho y Nuevas Tecnologías*, España, Andavira, 2012, pág. 178). La clasificación de la autora citada incluye seis grupos, siendo el sexto: “Cámara, micrófono, altavoz y mando a distancia para videoconferencia”; no obstante, como tales dispositivos encuadran en los cinco anteriores, menos el mando a distancia para videoconferencia, se substituyó por el indicado en el texto.

1. Elementos de entrada de video: cámara de video estándar o cámara de Internet.
2. Elementos de salida de video: monitor de computadora, televisor o proyector de video *beam* y pantalla.
3. Elementos de entrada de audio: micrófono.
4. Elementos de salida de audio: altavoces o auriculares⁵³
5. Elementos de transferencia de datos: se refiere a la red informática a utilizar, que según su alcance, Sandra Henríquez⁵⁴ califica de red de área local (LAN, por las siglas en inglés de *Local Area Network*), red de área local virtual (VLAN, por las siglas en inglés de red de área local virtual), red de campus (CAN, por las siglas en inglés de *Campus Área Network*), red de área metropolitana (MAN, por las siglas en inglés de *Metropolitan Área Network*) o red de área extensa (WAN, por las siglas en inglés de *Wide Área Network*), red de almacenamiento de área (SAN, por las siglas en inglés de *Storage Área Network*), red irregular o Internet.
6. Elementos de procesamiento de datos: computadora, programa informático y/o equipo de videoconferencia.

Específicamente, los elementos necesarios en el lugar de emisión y recepción de la señal van a depender del modelo de videoconferencia que se use, como se verá a continuación.

5.2.1. Sistema de videoconferencia

La videoconferencia puede celebrarse mediante un “sistema dedicado o profesional”, fabricado especialmente para cumplir esta función⁵⁵, o a través de un “sistema de escritorio”, que se logra agregando a una computadora los distintos elementos indicados en el epígrafe anterior.

En el primer caso se alude a la instalación de un sistema de videoconferencia que pudiera requerir equipo especial para ello, tanto en el lugar de remisión como en el de recepción, el cual, lógicamente debe interoperar.

En el segundo supuesto, se hace referencia al uso de un programa informático de pago del que disponga el Tribunal Supremo de Justicia para tal fin y que el interviniente a distancia deberá instalar en su computadora o acceder a él

⁵³ En cuanto a los auriculares, esto impediría al resto de la audiencia escuchar la declaración a distancia, aunque pudiera considerarse en caso de audiencias privadas en los supuestos previstos en las leyes. No obstante, pareciera que pudieran ser una opción valiosa para el declarante a distancia.

⁵⁴ Consultado el 10 de octubre de 2015 en <https://gobiernoti.wordpress.com/2011/10/04/tipos-de-redes-informaticas/>

⁵⁵ Patricia ESTÉVEZ HUEVRA: “La viabilidad de los medios telemáticos en el acto de conciliación de la audiencia previa”. *Fodertics, estudios sobre Derecho y Nuevas Tecnologías*, España, Andavira, 2012, pág. 178.

mediante Internet, con un nombre de usuario y una clave otorgada por la Sala de Casación Penal para el caso concreto; o simplemente, se trataría de utilizar un sistema de videoconferencia gratuito de los que se ofrecen en Internet.

No importa el método seguido, en todos los casos se logra la comunicación bidireccional y en tiempo real de los intervinientes, con las particularidades que se indicarán de seguidas.

El primer caso garantiza mejores resultados en cuanto a seguridad y calidad⁵⁶ de la transmisión pero trae como desventaja los costos que implica y la posible incompatibilidad entre marcas comerciales según la tecnología usada. Normalmente este supuesto se aplicaría para la intercomunicación entre el Tribunal Supremo de Justicia y los demás tribunales del país.

El segundo supuesto no requiere inversión alguna del participante por videoconferencia pero sí del Tribunal Supremo de Justicia quien deberá pagar al fabricante o desarrollador del programa por el uso del mismo; sin embargo, la legislación nacional comenzó a promover el uso de programas de computación libres, comenzando con el Decreto nro. 3.390 del 23 de diciembre de 2004, mediante el cual se disponía que la Administración Pública Nacional emplearía prioritariamente Software Libre desarrollado con Estándares Abiertos en sus sistemas, proyectos y servicios informáticos⁵⁷.

Posteriormente, el Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado⁵⁸, prescribió que los sistemas de información interoperables y servicios de información deberán ser desarrollados bajo estándares abiertos y Software Libre⁵⁹.

Pero fue la Ley de Infogobierno el texto jurídico que restringió contundentemente el uso de programas de información por cuyo uso tuviera que pagar el Estado; así se prevé que el Poder Público y el Poder Popular colaborarán para alcanzar la consolidación del uso de las tecnologías de información libres en el Estado⁶⁰, y concretamente que el Poder Público, donde se incluye al Tribunal Supremo de Justicia, solo empleará programas informáticos en software libre⁶¹, en especial luego de la entrada en vigencia de la ley, salvo

⁵⁶ Respecto de la calidad de la emisión, el encabezado del artículo R53-38 del Código Procesal Penal Francés prevé que las características técnicas de los medios de telecomunicación deben asegurar una retransmisión fiel, leal y confidencial respecto de terceros.

⁵⁷ Gaceta Oficial de la República Bolivariana de Venezuela nro. 38.095 de fecha 28 de diciembre de 2004, derogado por la Ley de Infogobierno.

⁵⁸ Decreto nro. 9.051 15 de junio de 2012 publicado en la Gaceta Oficial nro. 39.945 del 15 de junio de 2012.

⁵⁹ Artículo 35.

⁶⁰ Artículo 29.

⁶¹ Artículo 34. Además, la importancia del uso de programas de computación libres destaca cuando se promueve su uso, como se observa en los artículos 39, 63

las excepciones expresamente establecidas en la ley y previa autorización del ente competente⁶².

En este orden, el mismo texto de derecho prevé que el uso de programas de computación que no sean libres deberá ser autorizado por la Comisión Nacional de las Tecnologías de Información y solo cuando no exista un programa desarrollado que lo sustituya o se encuentre en riesgo la seguridad y defensa de la Nación⁶³.

Incluso, la ley impone el pago de una contribución especial al órgano o ente del Poder Público o del Poder Popular que sea autorizado a adquirir, usar y actualizar un software privativo⁶⁴ y establece, de forma transitoria⁶⁵, que el Poder Judicial elaborará planes para implementar el uso de las tecnologías de información libres en su gestión con las personas; de ahí que al ser la audiencia de casación penal, la ocasión para la interacción directa entre la Sala de Casación Penal y las personas, puede concluirse que debe recurrirse al uso de programas de computación libres.

De acuerdo con lo expresado, el Tribunal Supremo de Justicia debe usar programas de computación libres para la celebración de la audiencia de casación penal telemática.

Para finalizar este tópico, la videoconferencia también pudiera ejecutarse mediante programas informáticos gratuitos que se encuentran en Internet, lo cual, si bien no constituye *software* libre, no genera erogaciones por parte del Poder Público, por lo que pudiera admitirse su uso, aunque con ello no se estaría siguiendo a cabalidad la letra de la ley ante la falta de acceso al código fuente.

5.2.2. Equipamiento de la sala de audiencias y reorganización de la ubicación de los intervinientes si fuera necesario

Este último epígrafe se refiere a los recursos técnicos requeridos para que se materialice la presencia en la sala de audiencias mediante las tecnologías de información y comunicación. Estos dependerán del sistema que se instaure, el cual, pudiera requerir unos elementos precisos, o ser compatible con cualquier componente.

En todo caso, en la sala de audiencias serán necesarias al menos dos cámaras que permitan al interviniente a distancia observar a los magistrados y a la otra parte, así como también disponer de una vista general de la sala y en especial del público asistente; igualmente, será necesario que los micrófonos por los que se comunican los presentes capten con suficiente claridad las intervenciones, para garantizar el derecho a la defensa.

62 Disposición final primera.

63 Artículo 66.

64 Artículo 67.

65 Disposición transitoria tercera.

Igualmente ocurre con la proyección de la imagen del declarante a distancia, la cual deberá ser percibida por el juzgador de la manera más parecida posible a la presencia real de quien interviene a distancia.

En este caso, la situación puede resolverse incorporando una cámara en el medio de la sala de audiencias, concretamente en el techo, o en algún otro lugar que no corra el riesgo de ser manipulada.

En cuanto a la imagen que recibirán los magistrados del interviniente a distancia, esta puede proyectarse en una pantalla ubicada al lado de los asientos dispuesto para el público y frente a los magistrados, o mediante monitores colgados en el techo, sin interrumpir la visibilidad de los presentes, o ubicados en el suelo, delante de las mesas donde le corresponde sentarse al Ministerio Público y a la defensa, siempre que la víctima y su apoderado también tengan visibilidad sobre los intervinientes a distancia.

Por su parte, deberá incorporarse uno o dos monitores en las paredes ubicadas a ambos lados del estrado, de frente al público para que se tenga acceso visual en mejor condición que la actual, donde se ve a la defensa, al acusado y al representante del Ministerio Público, de espalda al público, pero frente a los magistrados.

IV. Conclusión

Celebrar la audiencia de casación penal por medios telemáticos trae consigo ciertas dificultades vinculadas con la identificación de los intervinientes a distancia, a los límites a la publicidad de la audiencia, al modo de regular las eventuales suspensiones, a la privacidad de la comunicación de las partes y sus representantes judiciales, y al diseño de la sala de audiencias.

Cada una de estas situaciones pudieran resolverse sobre la base de la normativa jurídica vigente, las cuales, sin embargo, deberán ser consideradas en una eventual reforma legislativa. En este sentido, los supuestos indicados pudieran remediarse así:

1. En cuanto a la identificación de los participantes y del Tribunal Supremo de Justicia:

Dado que el método de identificación personal que establece la ley para las actuaciones judiciales, consiste en mostrar la cédula de identidad a la autoridad judicial, no se advierten diferencias insalvables entre hacerlo directamente ante el tribunal o valiéndose para ello de la cámara de video por la que se participará en la audiencia, ello sin perjuicio de mostrarla directamente a la autoridad competente del tribunal o centro de reclusión desde donde se participare, si fuere el caso.

En lo relacionado a la identificación de los miembros de la Sala de Casación Penal, el actuante a distancia sabrá que lo hace ante el Tribunal Supremo de

Justicia si se coloca un enlace de acceso a la audiencia virtual en la página de internet del Máximo Tribunal o si accediere a la dirección electrónica que se le indicare en la citación correspondiente.

2. En lo concerniente a la publicidad de la audiencia

Como la publicidad judicial no impide la transmisión de la audiencia de casación penal en los medios de comunicación, incluyendo Internet, el sujeto procesal que participe en la audiencia de casación penal podrá hacerlo desde donde prefiera, salvo que la Sala, por las razones legales o de buen desarrollo del proceso, decidiere asegurar que la audiencia no será difundida, por lo que deberá comisionar a un tribunal de la localidad más cercana al domicilio del declarante para que actúe desde allí.

3. Atendiendo a la interrupción de la transmisión de los actos de la audiencia

En caso de interrumpirse la transmisión de alguna de las intervenciones a distancia en la audiencia de casación telemática, por cualquier causa que impida su celebración lo antes posible en este formato, el Magistrado Presidente de la Sala de Casación Penal resolverá, razonadamente, si se mantiene su ejecución bajo esta modalidad ese mismo día u otro, o si ordenará su celebración de la forma tradicional, en otra oportunidad, explicando estos supuestos en la citación para la audiencia que fue interrumpida.

4. Respecto de la comunicación privada a distancia

Si cualquiera o ambas partes estuvieren separadas de sus representantes judiciales, estando solo uno en la sala de audiencias, deberá autorizarse el uso de un sistema de comunicación privado entre ellos, siempre que no incomodare el normal desarrollo de la audiencia respecto de los presentes en la sala de audiencias; en todo caso, el alguacil o el magistrado presidente deberán velar porque se mantenga el orden en la sala.

5. En lo que se refiere al diseño de la sala de audiencias

La intervención a distancia de al menos un sujeto procesal en la audiencia de casación penal supone reorganizar la sala dispuesta para ello, incluyendo la incorporación de un sistema de videoconferencia, y demás implementos requeridos al efecto, que deberán funcionar con software libre, por disposición legal.

En definitiva, los obstáculos advertidos para llevar a cabo la audiencia de casación penal virtual encuentran soluciones en la práctica y en el ordenamiento

jurídico vigente, el cual favorece su implementación y permite resolver los problemas detectados en el presente estudio, no obstante, lo idóneo sería contar con una regulación jurídica especial para evitar la diversidad interpretativa que pudiera surgir, y consolidar la participación telemática en la audiencia de casación penal.

2000 - 2015: 15 aniversario del Sistema Nacional e-México*

Erika Yamel Munive Cortés**

SUMARIO: 1. Introducción: el Sistema Nacional e-México. 2. Marco jurídico. 3. Marco organizacional. 4. Retos a los que se enfrenta. 5. Ventajas generadas. 6. Desaciertos. 7. Centros de Acceso Público a las Tecnologías de la Información y Comunicación. 8. Consideraciones finales.

Resumen

En este documento se presenta un breve análisis exploratorio del despliegue que ha tenido el Sistema Nacional e-México a lo largo de 15 años, para ello, ha sido necesario hacer un recorrido desde el momento en que se introducen las Tecnologías de la Información y Comunicación (TIC) a la Administración Pública Federal en 1971, hasta la entrada en vigor de la Ley General de Transparencia en 2015. Se presenta un análisis del marco jurídico y organizacional del Sistema Nacional e-México, se exponen los desafíos que ha afrontado, los aciertos que ha logrado y también se muestran los inhibidores y las omisiones que han incidido en su desarrollo, posteriormente se hace una presentación general de los Centros Comunitarios Digitales (CCD) y en último lugar se presentan algunas reflexiones para fortalecer su continuidad en el tiempo.

Palabras Clave: Administración Pública. Gobierno electrónico. México. Políticas Públicas. Transparencia.

Abstract

This document presents a brief analysis of the deployment of the National e-Mexico System over 15 years. This analysis goes from the introduction of ICT in federal public administration in 1971 to the recently entry into force of the General Transparency Law

Recibido: 1/11/2015 • Aceptado: 8/12/2015

* Documento desarrollado a partir del capítulo III de: Erika Yamel Munive Cortés: *Diseño de estrategias de divulgación ciudadana para Programas de Gobierno Electrónico en México*, Tesis inédita de Posgrado – Maestría en Administración. Facultad de Contaduría Pública. Benemérita Universidad Autónoma de Puebla. México, 2008.

** Licenciada y Maestra en Derecho Corporativo Internacional por la Escuela Libre de Derecho de Puebla, Máster en Informática y Derecho por la Universidad Complutense de Madrid, Máster en Estudios Sociales de la Ciencia y la Tecnología por la Universidad de Salamanca. Candidata a Doctora en Estudios Jurídicos por la Universidad Rey Juan Carlos.

in 2015. It also presents an analysis of the legal and organizational framework of the National e-Mexico System, giving special attention to the challenges faced by the Good Government Agenda, our discussion examines different factors for achieving the success of The Mexican e-government strategy; it also shows the dominant factors inhibiting e-Government implementation in Mexico. This paper also gives a general presentation of The Digital Community Centers; by the end of this document you will find some suggestions for improving e-Mexico System continuity management.

Keywords: Public Administration. Electronic Government. México. Public policy. Transparency.

1. Introducción: el Sistema Nacional e-México

En México, la integración de las nuevas tecnologías a la Administración Pública inició en 1971 con el Comité Técnico Consultivo de Unidades de Informática (CTCUI), trabajo que fue reformulado posteriormente por el Instituto Nacional de Estadística, Geografía e Informática (INEGI)¹.

El INEGI convocó a mediados de 1993 a especialistas de los sectores público, académico y privado para integrar el grupo consultivo de política informática, su misión consistió en analizar la situación del país y proponer recomendaciones sobre políticas informáticas; en octubre de 1994 se publicó el documento “Elementos para un programa Estratégico en informática”, posteriormente se realizaron foros de discusión en torno a este documento y las recomendaciones surgidas formaron parte del Plan Nacional de Desarrollo 1995-2000, en el cual se concede importancia especial al uso y desarrollo de las tecnologías como herramienta de apoyo para lograr los objetivos nacionales.

El día 1 de diciembre de 2000 Vicente Fox Quesada, Presidente Constitucional de los Estados Unidos Mexicanos, pronunció las siguientes palabras:

Doy instrucciones al Secretario de Comunicaciones, a Pedro Cerisola, de iniciar a la brevedad el proyecto e-México, a fin de que la revolución de la información y las comunicaciones tenga un carácter verdaderamente nacional y se reduzca la brecha digital entre los gobiernos, las empresas, los hogares y los individuos, con un alcance hasta el último rincón de nuestro país².

Este es el punto de partida al trabajo del Consejo del Sistema Nacional e-México.

¹ Martín HILBERT; Sebastián BUSTOS; João Carlos FERAZ: Estrategias nacionales para la sociedad de la información en América Latina y el Caribe <http://repositorio.cepal.org/bitstream/handle/11362/4087/S2005015.pdf?sequence=1> <http://www.cepal.org/es> [consulta: 2015, octubre 1]

² <http://www.redgealc.net/sitio/contenido/2068/> [consulta: 2015, octubre 1]

En marzo de 2001 se llevó a cabo el “Foro de Consulta Ciudadana del Sistema Nacional e-México”, fue organizado por temas específicos: Infraestructura Tecnológica, Infraestructura Informática, e-Gobierno, e-Salud, e-Educación, e-Economía y Marco Jurídico, Regulatorio, Tarifario, las conclusiones del foro fueron sumadas al Plan Nacional de Desarrollo 2001-2006, en él se indicó la necesidad de implantar el Sistema Nacional e-México como una política pública del gobierno. El 31 de agosto del mismo año, se presentó al Presidente de la República y a los titulares de las Secretarías de Educación, Función Pública, Salud, Economía y Comunicaciones y Transportes, un esquema funcional del Sistema Nacional e-México, en el que se propuso el alineamiento de los objetivos de dichas dependencias con el Sistema, conformándose así el Consejo del Sistema Nacional e-México, el cual a partir de febrero de 2009 es denominado Coordinación de la Sociedad de la Información y el Conocimiento (CSIC)³.

En diciembre de 2001 se asigna la Coordinación General del Sistema Nacional e-México a la Secretaría de Comunicaciones y Transportes (SCT) a través de un Coordinador Operativo, dándole personalidad jurídica; durante este año Sotelo⁴ observa las siguientes características en el aprovechamiento de las tecnologías de la información:

- Desarticulación y división de la Administración Pública Federal.
- Las dependencias utilizaban irracionalmente el patrimonio público debido a la redundancia de inversiones, recursos y acciones informáticas; (366,000 computadoras y 12,300 sistemas de información).
- Ausencia de plan estratégico de tecnología de información para la Administración Pública Federal.
- Baja efectividad de las acciones de informática en la Administración Pública Federal.
- Las inversiones y acciones de informática eran predominantes en aspectos no sustantivos de las dependencias.
- La construcción de un sistema integral de información para la Administración Pública Federal era limitado por las dificultades tecnológicas.

En julio de 2002 se constituyó el Fideicomiso e-México para administrar, invertir y controlar los recursos necesarios para la operación de los proyectos del Sistema Nacional e-México, además, se incorporó un Comité Técnico encargado de elaborar y aprobar las políticas, bases y lineamientos necesarios para la planeación, programación, presupuestación, contratación, gasto y control de adquisiciones, arrendamientos y servicios que realicen las dependencias o

³ <http://inclusiondigital.mx/csic.php> [consulta: 2015, octubre 1]

⁴ Abraham SOTELO NAVA: “Innovación gubernamental El proyecto de e –gobierno”, *Revista Política Digital*, Año 1 (Núm. 1), México. Nexos, 2001, p. 22. http://www.politicadigital.com.mx/pics/edito/multimedia/396/filearton80_multimedia.pdf
www.politicadigital.com.mx [consulta: 2015, octubre 1]

entidades participantes en dicho sistema. El 15 de julio de 2002 la Secretaría de Comunicaciones y Transportes firmó los Convenios Intersecretariales de Conectividad e-México con las Secretarías de Educación Pública, Salud, Desarrollo Social, el Instituto Nacional para la Educación de los Adultos y el Centro de Desarrollo Municipal, con esto se da el primer paso hacia la intercomunicación, de las grandes microregiones del país.

El 6 de junio de 2003 fue inaugurada la primera Red Satelital e-México, la cual cubrió 3,200 localidades del país y todas las Cabeceras Municipales; esta red conectó a más del 60% de la población de México; el Presidente de la República dio un impulso personal al desarrollo del Sistema Nacional e-México al hacer frecuentes referencias al tema en sus discursos públicos, por ejemplo, en el discurso inaugural de la primera red satelital afirmó:

... con el Sistema e-México incorporaremos a nuestro país a la Sociedad de la Información, reduciendo la brecha digital, la brecha entre los que tienen acceso a las tecnologías de la información y el conocimiento y los que no la tienen; un paso fundamental hacia la equidad, hacia la igualdad de oportunidades que estamos impulsando⁵.

En mayo de 2004 el Foro Internacional *Stockholm Challenge* de Suecia, reconoció al Portal e-México como uno de los diez mejores portales de gobierno del mundo y el portal (www.gob.mx) que formó parte del Sistema Nacional e-México en el Pilar e-Gobierno, obtuvo el primer lugar, además se pusieron en operación 3,287 estaciones terrenas terminales que permitieron el funcionamiento de igual número de CCD, en adición a los 3,200 instalados durante 2003. En ese mismo año Pérez Mazatán -coordinador del sistema-, optó por una estrategia focalizada que llevó a una reorganización interna del Sistema Nacional e-México en tres áreas: 1. Relación interinstitucional: para coordinar acciones con otras dependencias y la iniciativa privada, 2. Planeación estratégica: para elegir los proyectos más viables, 3. Manejo de los proyectos: para guiarlos.

En junio de 2005, el gobierno de México recibió el premio "*Application of Information and Communications Technology in Government: e-Government*", por parte de la Organización de las Naciones Unidas, gracias a su pilar e-Gobierno, adicionalmente en diciembre del mismo año, en su publicación anual "*e-Government Survey*", se distingue al portal e-México como mejor práctica a nivel mundial; ese mismo mes se emitió el Acuerdo por el cual se establece la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE)⁶, para apoyar todos los procesos gubernamentales en materia del gobierno electrónico.

⁵ <http://fox.presidencia.gob.mx/actividades/discursos/?contenido=5475>

<http://fox.presidencia.gob.mx/> [consulta: 2015, octubre 1]

⁶ <http://cidge.gob.mx/> [consulta: 2015, octubre 1]

El 1 de febrero de 2006 se realizó la primera reunión de la CIDGE, la Comisión fue presidida por el Secretario de la Función Pública; titular de la dependencia responsable de promover los mecanismos de comunicación e intercambio de información al interior de la Administración Pública Federal, su objetivo consiste en gestionar la participación ordenada de todos los sectores, con el fin de crear sinergias y aprovechar recursos, establecer una coordinación que utilice las mejores prácticas de gobierno electrónico nacionales e internacionales, y utilizar medios, como la firma electrónica, de forma homogénea.

La CIDGE tiene en su estructura un Consejo Ejecutivo, integrado por los responsables de las Unidades de Tecnologías de Información y Comunicación de las dependencias que además son los que establecen los compromisos y apoyos para ejecutar los programas delineados; los ejecutores son los Consejos Técnicos, que desarrollarán los proyectos específicos, en estos participarán los miembros de acuerdo con su especialidad y competencia.

Hasta julio de 2006 la ciudadanía tuvo acceso a 1.876 trámites y servicios electrónicos gubernamentales en línea, los cuales fueron proporcionados por las dependencias y entidades de la Administración Pública Federal mediante portales de Internet, centros de atención telefónica, quioscos y ventanillas de atención al ciudadano, en esa fecha se encontraban en operación 7.500 CCD⁷. En relación a la conectividad se trabajó en la licitación de la cuarta red digital satelital, incluyendo también la instalación de 800 estaciones terrenas terminales. Respecto a los contenidos se tiene registrado que hasta agosto, existían 46.000 usuarios de Internet y más de treinta millones de páginas desplegadas; en materia de sistemas, se implementaron diversos programas para acercar la tecnología a las personas y que ayuden en los procesos de trámites gubernamentales, como la segunda etapa de e-Licencias y CAPACINET⁸ -Plataforma de Servicios de Capacitación en Línea- ofrece 59 cursos de consulta y brinda acceso a materiales y cursos remotos⁹. En 2006 funcionaban 7.500 CCD y la SCT, logró abrir cerca de 10,000 puntos de acceso a Internet en centros comunitarios unidos por una red satelital¹⁰.

En México existen varias oficinas encargadas de los proyectos de gobierno electrónico:

- A nivel federal: dentro de la Secretaría de la Función Pública (SFP) existe la Unidad de Gobierno Electrónico y Política de Tecnologías de la

⁷ <http://calderon.presidencia.gob.mx/informe/sexta/>
<http://calderon.presidencia.gob.mx/> [consulta: 2015, octubre 1]

⁸ <http://www.capacinet.gob.mx/> [consulta: 2015, octubre 1]

⁹ <http://fox.presidencia.gob.mx/buenasnoticias/buengobierno/?contenido=26912&pagina=1>

<http://fox.presidencia.gob.mx/> [consulta: 2015, octubre 1]

¹⁰ <http://www3.diputados.gob.mx/camara/content/view/full/218067>

<http://www.diputados.gob.mx> [consulta: 2015, octubre 1]

Información, es la unidad directamente responsable del programa e-México¹¹.

- A nivel estatal: en los estados, generalmente el área de Comunicación Social es quien se responsabiliza del mantenimiento del portal y de los enlaces, en algunos estados existen Secretarías de Comunicación y Enlace.
- A nivel municipal: existen iniciativas descontroladas y escasas que intentaron coordinarse a través del programa e-local, coordinado por el Instituto Nacional para el Federalismo y el Desarrollo Municipal (INAFED), en algunos municipios existe una subdirección de enlace.

México ocupó el lugar 31 del Ranking General (presencia del gobierno en la red) con un índice de 0.6061 en 2004; sin embargo, en 2003 ocupaba el sitio número 30. En el Índice Web (Infraestructura de Telecomunicaciones) México estuvo en el sitio 11º con un índice 0,8192; en 2005 se encontró entre los 6 países en vías de desarrollo que hicieron los mayores esfuerzos para el desarrollo de servicios electrónicos; respecto al Índice de e-preparación (disposición de la población para usar el e-gobierno), México se encontraba en la 6ª posición con un índice 0,7619 manteniendo el mismo lugar que en 2004¹².

En 2007, el Comité de Informática de la Administración Pública Estatal y Municipal (CIAPEM A.C.) cuya creación tuvo lugar en 1978, renace para impulsar el desarrollo y aprovechamiento de proyectos relacionados con la Tecnología de la Información y las Comunicaciones en los gobiernos estatales y municipales. En abril de 2007 Alejandro Hernández Pulido, es nombrado coordinador del Sistema Nacional e-México y hasta septiembre del mismo año, se encontraban funcionando 9.200 CCD.

En el Estudio AMIPCI 2008 de Nuevas Tecnologías de Internet en México se destaca¹³:

1. el número estimado de usuarios de Internet en territorio nacional durante el 2007 es de 23.7 millones, mayores a 6 años de edad;

11 http://www.funcionpublica.gob.mx/pt/obligaciones_transparencia_art_7/sfp/_facultades/unidades/dgepti.html

www.funcionpublica.gob.mx [consulta: 2015, octubre 1]

12 United Nations: "Global e-government Readiness report 2005 From e-government to e-inclusion", Department of Economic and Social Affairs, Division for Public Administration and Development Management. New York, USA, 2005, p. 141.

<http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021888.pdf>

www.unpan1.un.org [consulta: 2015, octubre 1]

13 https://www.amipci.org.mx/estudios/nuevas_tecnologias/2008_Nvas_Tecnologias_Internet_Mx.pdf

www.amipci.org.mx [consulta: 2015, octubre 1]

2. el número de computadoras con acceso a Internet en México es de 11.1 millones;
3. 42% de los internautas son hombres.

La SCT ha definido al Sistema Nacional e-México como el instrumento de política pública diseñado por el Gobierno de México para conducir y propiciar la transición de México hacia la sociedad de la información y el conocimiento, diseñando los servicios digitales para el ciudadano del siglo XXI y considera que el Sistema Nacional e-México es un sistema dinámico e integrador, que articula de manera efectiva los intereses de los distintos niveles de gobierno, de diversas entidades y dependencias públicas, de los operadores de redes de telecomunicaciones, de las cámaras y asociaciones vinculadas a las Tecnologías de la Información y Comunicaciones, la academia, agentes económicos, así como de diversas instituciones, a fin de ampliar la cobertura de servicios digitales básicos de aprendizaje, salud, economía, gobierno, ciencia, tecnología y otros servicios a la comunidad, también se le define como un conjunto de estrategias, líneas de acción y metas para propiciar, mantener y fortalecer el uso de las computadoras y la Internet, para impulsar a la sociedad hacia los beneficios que ofrecen los avances tecnológicos de la información y la comunicaciones –participación digital– para llevar al país hacia la sociedad de la información y el conocimiento¹⁴.

Pérez indica que el Sistema Nacional e-México:

...es el instrumento de la sociedad mexicana para llevarla a la sociedad de la información, mediante la transformación de los servicios digitales de aprendizaje, que incluyen educación para la vida y el trabajo, de salud en todos sus ámbitos; de promoción económica a las pequeñas y medianas empresas; y de un gobierno más transparente y cercano al ciudadano¹⁵.

Según el artículo 2o. del Acuerdo de la Comisión Intersecretarial fracción VIII, se define como gobierno electrónico a:

...las políticas, acciones y criterios para el uso y aprovechamiento de las tecnologías de información y comunicaciones, con la finalidad de mejorar la entrega de servicios al ciudadano; la interacción del gobierno con la industria; facilitar el acceso del ciudadano a la información de éste, así como hacer más eficiente la gestión gubernamental para un mejor gobierno y facilitar la interoperabilidad entre las Dependencias y Entidades.

14 http://www.e-mexico.gob.mx/work/resources/LocalContent/5099/2/docto_emexico.doc
www.e-mexico.gob.mx [Consulta: 2007, enero 8]

15 <http://www.politicadigital.com.mx/?P=leernoticia&Article=622>
<http://www.politicadigital.com.mx> [consulta: 2015, octubre 1]

La Oficina de la Presidencia para la Innovación Gubernamental lo define como la

Innovación continua en la entrega de servicios, la participación de los ciudadanos y la forma de gobernar mediante la transformación de las relaciones externas e internas a través de la tecnología, la Internet y los nuevos medios de comunicación.

El Gobierno Federal planteó como prioridad el desarrollo de un sistema que permita a todos los mexicanos acceder a las nuevas tecnologías de la información y comunicaciones, bajo tres criterios principales, que el sistema sea:

1. federalista: integración de los tres niveles de gobierno (municipal, estatal y federal);
2. transparente y para todos los mexicanos: confiable, seguro, efectivo, que genere certidumbre a los usuarios y ofrezca igualdad de oportunidades en el acceso al sistema.
Y que el sistema no sea:
 1. una carga onerosa para el gobierno: su desarrollo no debe generar una carga económica para la sociedad.

El establecimiento del Sistema Nacional e-México implicó la creación de ordenamientos jurídicos que establecerían las normas que han de seguirse en el desarrollo de numerosos aspectos vinculados al uso de los programas de gobierno electrónico.

2. Marco jurídico

La Constitución Política de los Estados Unidos Mexicanos¹⁶: Permite el libre acceso a la información oficial de acuerdo al contenido del artículo 6:

La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito o perturbe el orden público; el derecho a la información será garantizado por el Estado.

En ese mismo artículo se ha incluido el derecho de acceso a Internet al adicionar en 2013 el siguiente párrafo:

El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones,

¹⁶ <http://www.ordenjuridico.gob.mx/Constitucion/articulos.php>
<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.

El artículo 8 indica:

Los funcionarios y empleados públicos respetarán el ejercicio del derecho de petición, siempre que esta se formule por escrito, de manera pacífica y respetuosa; pero en materia política solo podrán hacer uso de ese derecho los ciudadanos de la República.

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental del 11 de junio de 2002¹⁷, establece en el artículo 2 lo siguiente:

Toda información gubernamental a que se refiere esta Ley es pública y los particulares tendrán acceso a la misma en los términos que ésta señala». Y en el artículo 7 estipula:

Con excepción de la información reservada o confidencial prevista en esta Ley, los sujetos obligados deberán poner a disposición del público y actualizar... entre otra, la siguiente información:

1. Su estructura orgánica;
2. Las facultades de cada unidad administrativa;
3. El directorio de servidores públicos, desde el nivel de jefe de departamento o sus equivalentes;
4. La remuneración mensual por puesto, incluso el sistema de compensación, según lo establezcan las disposiciones correspondientes;
5. Las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos;
6. Los servicios que ofrecen.

Con el fin de promover y difundir el ejercicio del derecho a la información y proteger los datos personales en poder de las dependencias y entidades, se crea el Instituto Federal de Acceso a la Información Pública (IFAI), que a partir de la entrada en vigor de la Ley General de Transparencia el 5 de mayo de 2015¹⁸, cambió su nombre por el de Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

¹⁷ <http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo13220.pdf>
<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

¹⁸ <http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo102911.pdf>
<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

El Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental del 10 de Junio de 2003¹⁹, aplicable al Poder Ejecutivo Federal, sus dependencias y entidades y en general a cualquier otro órgano que forme parte de la Administración Pública Federal, establece, entre otras disposiciones, las siguientes:

1. La Unidad de Enlace de cada dependencia y entidad será la responsable de poner a disposición del público dicha información.
2. La información deberá estar contenida en un sitio de Internet de acceso público y general, visible desde el portal principal del sitio de Internet de la dependencia o entidad, indicando la fecha de su actualización, así como un vínculo al sitio de Internet del Instituto.
3. La información deberá presentarse de manera clara y completa, de forma tal que se asegure su calidad, veracidad, oportunidad y confiabilidad
4. El mismo sitio de Internet deberá contener las direcciones electrónicas, los domicilios para recibir correspondencia y los números telefónicos de la Unidad de Enlace, de los servidores públicos habilitados y del responsable del sitio mencionado.

Aunado a ello, el IFAI publicó en 2004 los Lineamientos en materia de clasificación y desclasificación de información relativa a operaciones fiduciarias y bancarias, así como al cumplimiento de obligaciones fiscales realizadas con recursos públicos federales por las dependencias y entidades de la Administración Pública Federal, el 30 de septiembre de 2005 emite los Lineamientos de Protección de Datos Personales para las Dependencias y Entidades de la Administración Pública Federal²⁰ y en 2013 los Lineamientos del aviso de privacidad²¹.

El Decreto sobre Firma Electrónica del 29 de Agosto de 2003, reforma y adiciona diversas disposiciones del Código de Comercio en materia de Firma Electrónica, establece las obligaciones y facultades para acceder al Registro Público de Comercio, la inscripción electrónica al mismo, disposiciones sobre

19 <http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo88480.pdf>

<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

20 <http://201.159.134.38/obtenerdoc.php?path=/Documentos/FEDERAL/o345451.doc&nombreclave=o345451.doc>

<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

21 <http://201.159.134.38/obtenerdoc.php?path=/Documentos/FEDERAL/o3451915.doc&nombreclave=o3451915.doc>

<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

mensajes electrónicos y firmas digitales, más adelante, en 2012 se expide la Ley de Firma Electrónica Avanzada²² y en 2014 su Reglamento²³.

El Código Civil Federal²⁴, con las reformas del 29 de mayo de 2000, reconoce la celebración de actos jurídicos a través de medios electrónicos, ópticos o de cualquier otra tecnología, añadiéndose los «medios tecnológicos» como una forma idónea para expresar el consentimiento. Por su parte, el Código Federal de Procedimientos Civiles²⁵, reconoce como prueba, la información contenida en los medios electrónicos, ópticos o en cualquier otra tecnología, dando una serie de reglas para su valoración por parte del juzgador.

La Ley Federal de Protección al Consumidor²⁶ con la reforma de 2004, reconoce la utilización de medios electrónicos, ópticos o cualquier otra tecnología en la instrumentación de las operaciones que celebren los proveedores con los consumidores, dando las bases sobre las cuales habrán de realizarse dichas operaciones (confidencialidad, certeza, seguridad en la información proporcionada al consumidor), previendo sanciones administrativas para el caso de que los proveedores no cumplan con dichas disposiciones.

En 2011 se expide el Reglamento del Sistema Nacional de Afiliación y Vigencia de Derechos, de la base de datos única de derechohabientes y del expediente electrónico único del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado²⁷. Y en 2013 el Reglamento para el uso y operación de la Firma Electrónica Avanzada en el Instituto Federal Electoral²⁸.

Dentro del Plan Nacional de Desarrollo 2001-2006²⁹, no se establece una política específica en materia de gobierno electrónico, se indica “*un componente electrónico de gobierno cada vez mayor*” (p.11) y “*la ampliación de la infraestructura digital para llegar hasta los grupos más rezagados del desarrollo*”. (p.56). Se menciona indirectamente al Sistema Nacional e-México cuando se establece en su capítulo 6, apartado 6.3, número 2, inciso b “Elevar y extender la competitividad del país”, dentro del Área de “Crecimiento con calidad”, que

22 <http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo67194.pdf>

<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

23 <http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo93113.pdf>

<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

24 <http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo17186.pdf>

<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

25 <http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo17190.pdf>

<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

26 <http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo12974.pdf>

<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

27 <http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo88707.pdf>

<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

28 <http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo88692.pdf>

<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

...el gobierno desempeña un papel importante en la adopción generalizada de tecnología digital del país, para ello, el gobierno desarrollará un sistema nacional que permita el acceso a la mayor parte de la población a través de las nuevas tecnologías de la informática, y que éstas sean el vehículo natural que intercomunique a los ciudadanos entre sí, con el gobierno y con el resto del mundo.

El Plan Nacional de Desarrollo 2007-2012³⁰, no menciona nada respecto al Sistema Nacional e-México, la palabra computadora aparece en 5 ocasiones, Internet 7 veces; en el capítulo de fomento al empleo se sugiere:

...crear un portal del empleo en el que, a través de internet, se reúna toda la información en el tema laboral para el uso de buscadores de empleo, empresas, gobiernos e investigadores. Será éste un instrumento permanente, único y virtual que facilitará el encuentro entre la oferta y la demanda de trabajo a nivel nacional para los sectores público y privado.

No obstante, este objetivo se puede considerar redundante, ya que en 2007 se encontraba operativo el portal (www.chambanet.gob.mx) dependiente de la Secretaría del Trabajo y Previsión Social y también existían los portales (www.trabajaen.gob.mx) y (www.conacyt.gob.mx), el primero a cargo de la Secretaría de la Función Pública y el segundo referente al Consejo Nacional de Ciencia y Tecnología, el cual ofrece vacantes de empleo para sus becarios investigadores, ambos continúan funcionando, cada portal se dirige a diversos grupos poblacionales, cuya búsqueda de empleo resulta adecuada al nivel educativo de cada segmento, ya que en chambanet se ofertaban empleos para un nivel educativo básico, en trabajaen, se recluta personal con formación mínima de licenciatura y en la web del CONACYT, se requiere incluso de personas que posean postdoctorado.

También se puede leer la palabra Internet en el apartado de cultura, arte, deporte y recreación:

...una línea de acción prioritaria en la política cultural del Gobierno de la República será el respaldo a las distintas manifestaciones de la cultura y el arte populares: artes plásticas, escénicas y literarias, y sus manifestaciones actuales como fotografía, video y las opciones en internet.

²⁹ http://www.diputados.gob.mx/LeyesBiblio/compila/pnd/PND_2001-2006_30may01.doc

<http://www.diputados.gob.mx/> [consulta: 2015, octubre 1]

³⁰ http://www.diputados.gob.mx/LeyesBiblio/compila/pnd/PND_2007-2012_31may07.doc

<http://www.diputados.gob.mx/> [consulta: 2015, octubre 1]

Internet se menciona por tres ocasiones en la sección de Telecomunicaciones, la cual planteaba facilitar la conexión a Internet a cuando menos 60% de la población del país al finalizar dicha administración, para lograrlo se buscó incrementar la competencia entre concesionarios y que bajasen los precios³¹.

Por su parte el Plan Nacional de Desarrollo 2013-2018³², dentro de las Estrategias Transversales para el desarrollo nacional incluye un apartado denominado: Gobierno Cercano y Moderno, el cual optimizará el uso de los recursos públicos, utilizará las nuevas tecnologías de la información y comunicación e impulsará la transparencia y la rendición de cuentas. La palabra electrónico aparece en el apartado reservado a la Seguridad Nacional y contempla el uso de medios electrónicos en áreas estratégicas; también se incluye en la sección referente a la democratización del acceso a servicios de telecomunicaciones, al indicar como línea de acción el fomento de la inversión para ofrecer servicios electrónicos que mejoren el valor agregado de las actividades productivas; además, por primera vez se incluye un apartado de indicadores, entre ellos se encuentra el índice de desarrollo de gobierno electrónico; también se hace referencia a las propuestas ciudadanas que se recibieron mediante documentos electrónicos. La palabra Internet se utiliza 15 veces, respecto a la cultura se pretende desarrollar una Agenda Digital para formar integralmente a los ciudadanos, también se menciona el establecimiento de una Estrategia Digital Nacional; es importante mencionar que se genera una línea de acción encaminada a la difusión de contenidos mediante portales digitales de promoción.

La Agenda Presidencial de Buen Gobierno en México desarrollada por el presidente Vicente Fox, indicó la visión a largo plazo del gobierno y los seis ejes para realizar el Buen Gobierno: un gobierno honesto y transparente, profesional, de calidad, digital, con mejora regulatoria, que cueste menos³³.

El Modelo Estratégico para la Innovación y la Calidad Gubernamental de la Oficina de la Presidencia para la Innovación Gubernamental de 2001³⁴, tuvo como propósito dar valor agregado a lo que hace el gobierno, dicho valor se basó en la capacidad que las diferentes dependencias gubernamentales poseen para mejorar sus procesos internos y generar resultados que beneficien a la sociedad mexicana.

31 Octavio CARDENAS: "Marginan a e-México" Excelsior, 6 de Junio, México. Nuevo Excelsior, 2007. http://www.nuevoexcelsior.com.mx/27_2690.htm

www.excelsior.com.mx/ [Consulta: 2007, enero 8]

32 http://www.diputados.gob.mx/LeyesBiblio/compila/pnd/PND_2013-2018_20may13.doc

<http://www.diputados.gob.mx/> [consulta: 2015, octubre 1]

33 http://www.cca.org.mx/ec/cursos/ap044/contenido/contenidos/m5_tema3/modelo_ap.htm

<http://www.centroscomunitariosdeaprendizaje.org.mx/> [consulta: 2015, octubre 1]

34 http://www.cca.org.mx/apoyos/ap073/mod2/mod_est.pdf

<http://www.centroscomunitariosdeaprendizaje.org.mx/> [consulta: 2015, octubre 1]

El Programa Sectorial de Telecomunicaciones y Transportes 2001-2006³⁵ de la Secretaría de Comunicaciones y Transportes menciona los siguientes objetivos:

1. Promover la conectividad y generación de contenidos digitales (datos, sonidos e imágenes) vía Internet, a precios accesibles, entre aquellos individuos y familias, de menores ingresos, que viven en comunidades urbanas y rurales del país, con más de 400 habitantes, a fin de apoyar su integración al desarrollo económico y social de México, reduciendo la brecha digital que, por desgracia, existe hoy en día en México.
2. Capacitar en el uso de las nuevas tecnologías de la información y difusión del conocimiento a las familias de dichas comunidades, con énfasis en su autosuficiencia para consultar y generar contenidos vía Internet en apoyo a sus particulares necesidades de educación, cultura, salud y desarrollo económico.
3. Poner a disposición de la población en general, la información referente a los servicios que prestan los gobiernos federal, estatal y municipal, a fin de que exista transparencia y equidad en los mismos y se ayude a disminuir el tiempo que actualmente requiere la realización de diversos trámites y mejorar su eficiencia.

El Programa Sectorial de Telecomunicaciones y Transportes 2007-2012³⁶, hace referencia a la cobertura limitada de banda ancha e Internet y a la falta de colaboración interinstitucional del Sistema Nacional e-México; la estrategia 8.2.4 se refiere al Sistema Nacional e-México como medio para llevar al país a la Sociedad de la Información y Conocimiento. En el Programa Sectorial de Telecomunicaciones y Transportes 2013-2018³⁷ se pretende llevar conectividad de banda ancha a sitios públicos del país, sin embargo no se hace ninguna referencia al Sistema Nacional e-México.

El Proyecto de Acuerdo por el que se establece el Modelo para el Desarrollo del Gobierno Electrónico en la Administración Pública Federal³⁸, promueve y consolida el desarrollo, uso y aprovechamiento de las tecnologías de información e intercomunicación por vía electrónica, mediante la coordinación de las dependencias que estableció la Secretaría de la Función Pública y por conducto de las coordinadoras de sector de las entidades paraestatales.

35 <http://legismex.mty.itesm.mx/progs/p-sct-02txt.pdf>
www.legismex.com.mx/cms/ [consulta: 2015, octubre 1]

36 <http://www.seneam.gob.mx/transparencia/ARCHIVOS/Comunicaciones.DOF.PDF>
<http://www.seneam.gob.mx/> [consulta: 2015, octubre 1]

37 <http://www.ordenjuridico.gob.mx/Documentos/Federal/wo89400.doc>
<http://www.ordenjuridico.gob.mx> [consulta: 2015, octubre 1]

38 http://www.funcionpublica.gob.mx/pt/difusion_disposiciones_juridicas/doctos/proy-acuerdo-modelogob.pdf
<http://www.funcionpublica.gob.mx/> [consulta: 2015, octubre 1]

En 2004 la Secretaría de Gobernación a través del Instituto Nacional para el Federalismo y el Desarrollo Municipal brindó las Metodologías en Materia de Tecnologías de la Información para Gobiernos Locales. Este documento presentó seis herramientas metodológicas que permitieron captar la situación real respecto a la apropiación de las Tecnologías de la Información y Comunicación a través de los puntos siguientes: tipología municipal, niveles de gobierno electrónico, ficha de diagnóstico municipal en materia de tecnologías de la información, índice de información de gobiernos locales, criterios para la evaluación de páginas web de gobiernos locales, formulario para la sistematización de mejores gobiernos locales.

Para el establecimiento del Sistema Nacional e-México fue necesario elaborar una estructura perfectamente delimitada, en la que tomando en cuenta las diversas necesidades poblacionales, se localizase rápidamente la información.

3. Marco organizacional

El Sistema Nacional e-México se organizó en tres grandes ejes:

A) Conectividad: es la infraestructura tecnológica utilizada para ofrecer el servicio universal a todos los mexicanos. Se concentró en dos aspectos:

1. Las inversiones que realizan operadores de redes de telecomunicaciones para incrementar la infraestructura y cobertura del servicio telefónico en los hogares mexicanos, previendo pasar de las 12 líneas por cada 100 habitantes en el año 2000 a 25 líneas por cada 100 habitantes en el 2006, sin embargo este objetivo no se cumplió ya que los datos indican que hasta 2013 se habían alcanzado únicamente 16.8 líneas telefónicas por cada 100 habitantes³⁹. Para lograr la conectividad cada dependencia aportó algo, la conexión se efectuaría por medios alámbricos e inalámbricos, ya sean satelitales o terrestres, y sería provista por la Secretaría de Comunicaciones y Transporte, que licitaría el contrato con los proveedores de servicios. Se firmaban contratos por 55 meses para que los proveedores recuperasen su inversión, ya que cobrarían 499 pesos mensuales por el servicio a cada Centro Comunitario Digital⁴⁰.

39 <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tnf126&s=est&c=19381>
www.inegi.gob.mx [consulta: 2015, octubre 1]

40 Gobierno de la República: "Agenda 2002. Arranca e-México" *Revista Política Digital*, Año 1 (Núm. 6), México. Nexos, 2001, p. 52
http://www.politicadigital.com.mx/pics/edito/multimedia/401/filearton85_multimedia.pdf
<http://www.politicadigital.com.mx> [consulta: 2015, octubre 1]

2. Conectividad satelital: la primera Red Satelital e-México, cubrió 3,200 localidades del país, se incluyen todas las Cabeceras Municipales y cubre a más del 60% de la población de México. La cobertura satelital del Sistema Nacional e-México se concentró en las regiones de mayor marginación en el desarrollo social, educativo y económico. Se creó una red de CCD que sirvió para dar conectividad a las poblaciones y familias que por limitaciones económicas y geográficas no cuentan con la infraestructura de telecomunicaciones necesaria para tener acceso dentro de su hogar. Los CCD, son inmuebles gubernamentales (escuelas, bibliotecas, hospitales, palacios municipales, oficinas de correos o de telégrafos, u otros lugares específicos) donde se instalaron equipos de cómputo y de comunicaciones que proporcionan a la población, los servicios y contenidos que forman parte del Sistema Nacional e-México⁴¹.

B) Contenidos: son los servicios estructurados en plataformas digitales integrales, en temas prioritarios para la sociedad, como: el aprendizaje, la capacitación, la cultura, la salud, el comercio y la economía, la información y los trámites con los diferentes niveles de gobierno, así como también otros servicios útiles a la comunidad: bolsas de trabajo, servicios de emergencia, etc.

El portal de e-México fue constituido por cuatro pilares o secciones fundamentales: e-Gobierno, e-Economía, e-Salud, e-Aprendizaje. A ellos se sumaron dos grandes apartados que son DiscapaciNET y e-Migrantes. Cada pilar se rige por un comité integrado por instituciones públicas y privadas especializadas en cada uno de los temas y cuya función consiste en valorar y aprobar los contenidos, proveer información y servicios⁴². En todos los casos e-México participa como un miembro más del Comité que sólo ofrece la metodología de trabajo, la plataforma tecnológica, propuestas editoriales y, en ocasiones, también aporta recursos. La Secretaría de la Función Pública se encarga de e-Gobierno; la de Economía de e-Economía; e-Salud está a cargo de la Secretaría de Salud y el e-Aprendizaje depende de la Secretaría de Educación Pública (SEP). Alrededor de esta estructura central coexisten 11 secciones laterales, denominadas comunidades, enfocadas a grupos muy

41 Mariano Garza - Cantú Chávez: “Los Centros Comunitarios Digitales” *Revista Política Digital*, Año 4 (Núm. 22), México. Nexos, 2005, pp. 18-21

http://www.politicadigital.com.mx/pics/edito/multimedia/417/filearton101_multimedia.pdf
<http://www.politicadigital.com.mx> [consulta: 2015, octubre 1]

42 Gobierno de la República: “Tema central, Los contenidos de e-México” *Revista Política Digital*, Año 4 (Núm. 22), México. Nexos, 2005, pp. 28-33.

http://www.politicadigital.com.mx/pics/edito/multimedia/417/filearton101_multimedia.pdf
<http://www.politicadigital.com.mx> [consulta: 2015, octubre 1]

específicos: adultos mayores, empresarios, mujeres, campesinos, estudiantes, familia, niños, migrantes, indígenas, visitantes, educación especial.

Para decidir los contenidos a incluir en el portal, las instituciones participantes aportaron su experiencia respecto de lo que demanda la ciudadanía, se realizaron estudios de apropiamiento a través de los promotores de los CCD para saber qué es lo que la gente pide y en Campus e-México se analizaron las propuestas y comentarios relacionados con las necesidades de los usuarios. El portal e-México tuvo como objetivo ayudar a que la gente encuentre con mayor facilidad lo que necesita, el portal no entró en conflicto con el portal ciudadano (www.gob.mx) porque, éste tiene como misión llevar los trámites del gobierno en línea y e-México concentra los contenidos para luego referenciarlos, con el objeto de que el usuario localice rápidamente lo que quiere a través de sus 4 pilares:

- e-Gobierno: se utilizó como medio para que todos los mexicanos, en el ámbito federal, regional, estatal y municipal, puedan ejercer su derecho a estar informados y acceder a los servicios que ofrece el Estado, a través de la mega red del Sistema Nacional e-México.
 - e-Economía: aspiró a acelerar el proceso de desarrollo de la economía digital en las empresas, especialmente las micro, pequeñas y medianas, para incrementar la competitividad de la economía mexicana; así como desarrollar la cultura de digitalización de la sociedad, particularmente en los consumidores.
 - e-Salud: pretendía elevar el nivel de bienestar y de salud de la sociedad, mediante la integración de un sistema tecnológico y de contenido social. Puso al alcance de toda la población mexicana información médica integral, que contribuyó al desarrollo humano y de las instituciones del sector salud, eliminando las barreras de acceso a la información y a los servicios de salud y seguridad social.
 - e-Aprendizaje: brindó nuevas opciones de acceso a la educación y capacitación, que estimularon el aprendizaje como un medio para el desarrollo integral de los mexicanos, promoviendo que la educación fuera accesible para cualquier persona, respetando su identidad y su entorno cultural.
- C) Sistemas: es la infraestructura tecnológica que apoya a la red para transportar los servicios digitales o contenidos productivos a la población en general, también es la generación y desarrollo de nuevas herramientas para el enriquecimiento y evolución del sistema destacando:

- Portal e-México: se usó como una ventana del sistema hacia todos los usuarios, tanto nacionales como extranjeros.
- Portal e-Salud: tuvo como objetivos:
 1. Contribuir en la mejora de la calidad y en la cobertura de los servicios de salud, dio prioridad a las localidades de mayor marginación, mediante un sistema de tele-salud de alto contenido social
 2. Fortalecer la capacitación y educación continua del personal de salud, independientemente de su lugar de adscripción, mediante programas tele-transmitidos y adecuados a necesidades específicas, por nivel de atención y rama de actividad
 3. Coadyuvar a la modernización de los procesos de gestión y administración de los servicios de salud, mediante sistemas y opciones telemáticas y automatizadas
- Portal Discapacinet: tuvo la misión de impulsar y promover el establecimiento, difusión, ampliación y cumplimiento de la política de gobierno para fomentar la promoción e integración social de las personas con capacidades especiales, fortaleciendo los programas institucionales mediante una eficiente coordinación intersecretarial, proponiendo modificaciones al marco jurídico y administrativo y promoviendo la participación de las organizaciones de la sociedad civil a través de proyectos ciudadanos.
- Red Privada Virtual: permitió reducir significativamente los costos de operación en telecomunicaciones y optimizar los procesos intra-intergubernamentales, además de ofrecer un mejor y más eficiente servicio a los ciudadanos.
- Centro de Datos: se concibió como el equipamiento y sistema necesario para concentrar los sistemas y ligar los contenidos con los cuales operaría el Sistema Nacional e-México en su primer nivel de estructura de información.
- Punto Neutral de Acceso a la Red: se refería al lugar donde se intercambiaba el tráfico de las redes de datos de todos los operadores de redes públicas y en su caso las privadas que se requieran, de manera que este sistema optimizó el acceso a los servicios digitales de e-México y de todo el flujo de información de Internet del país, sin necesidad de que el tráfico que se generara en la plataforma de servicios de e-México saliera a otros puntos para intercambiarse. También buscó optimizar los procesos entre operadores del país sin necesidad de que se establecieran acuerdos específicos entre ellos para operar de manera eficiente.

- D) Capacitación e inducción: son procesos que apoyaron a los usuarios del sistema a su comprensión, uso inteligente y mejor aprovechamiento, también son métodos probados y certificados para invitar a la sociedad a que sea responsable y participe de las oportunidades que conllevan las nuevas tecnologías.
- E) Apropiamiento: se refiere a la adopción consciente y natural de los servicios digitales por parte de la población. La aceptación del uso y aprovechamiento del sistema, como una práctica común y necesaria en la vida diaria de los mexicanos.

Debido a la diversidad geográfica, cultural y económica existente a lo largo y ancho del país, el Sistema Nacional e-México se vio obligado a superar una serie de dificultades, que a corto plazo resulta imposible vencer, por lo tanto su proyección debe incluirse dentro del Plan Nacional de Desarrollo de varios sexenios.

4. Retos a los que se enfrenta

Los principales inconvenientes a los que se enfrentó el Sistema Nacional e-México son los siguientes:

1. El acceso universal: se necesitaba generar un entorno de igualdad de oportunidades para el acceso a la información y el conocimiento;
2. La participación digital: era preciso integrar esfuerzos de todos los actores públicos y privados para la creación, acumulación y distribución de la información y del conocimiento;
3. El apropiamiento: se requería lograr un uso inteligente de las nuevas tecnologías para el bienestar de todos los mexicanos.

Aunado a lo anterior, también existieron retos tecnológicos en la eficiencia de los CCD:

1. La instalación de los CCD: fue necesario considerar la dispersión geográfica de las instalaciones, la conectividad disponible, así como la cantidad de equipos necesarios para brindar sin problemas el mismo servicio y durante largas jornadas de trabajo diariamente, por ello se optó un sistema de instalación desatendida, en el que no se requería que el administrador de cada centro requiriese determinado nivel de especialidad.
2. El mantenimiento y administración de aplicaciones y datos: el desarrollo tecnológico permite que la preservación de los equipos se realice de forma remota; desde centros de comando y a través Internet, se

resolvieron problemas derivados del uso de los equipos, sin necesidad de trasladarse a cada centro.

3. Las políticas de uso de los equipos: los usuarios poseyeron privilegios diferenciados para el aprovechamiento de la infraestructura, los criterios que guiaron el diseño de esas políticas fueron: 1) Los usuarios serán en su mayoría usuarios inexpertos en el manejo de equipos de cómputo, 2) El propósito de los CCD fue brindar herramientas de provecho y de recreación sana, es por ello que se debe asegurar que los usuarios tengan acceso solamente a las herramientas que estarán en posibilidad de controlar, reduciendo los riesgos de contaminación de virus informáticos, la instalación de programas no autorizados, la desconfiguración de computadoras y sobre todo, asegurar que los equipos sean usados acorde al fin para el que han sido destinados.

A pesar de ser diversos los desafíos a los que se enfrentó el Sistema Nacional e-México, actualmente se pueden observar varios avances en múltiples aspectos, al haberse incorporado las Tecnologías de la Información y Comunicación como medio para mejorar la comunicación entre gobierno y ciudadano.

5. Ventajas generadas

La Red de Gobierno Electrónico de América Latina y el Caribe⁴³ indicó que los principales beneficios que ha logrado el establecimiento del Sistema Nacional e-México en la República Mexicana son:

- incrementar la eficiencia gubernamental;
- mejorar la calidad de los servicios;
- mejorar el desempeño de políticas específicas;
- mejorar el desempeño de la política económica;
- reformar al Estado;
- crear confianza entre gobiernos y ciudadanos;
- tener servicios públicos disponibles desde cualquier lugar y en cualquier momento;
- transparentar el acceso a la información pública;
- incrementar la participación del ciudadano en las decisiones públicas;
- reducir los costos operacionales del gobierno.

Para multiplicar todas estas ventajas, el gobierno se percató de la necesidad de crear junto con el Programa de Gobierno Electrónico diversos espacios para que la población tuviera fácil acceso a los servicios telemáticos que se empezaban

43 www.redgealc.net/archivos/documentos/Tijuana1.pdf
www.redgealc.net [consulta: 2007, enero 8]

a ofrecer, por tal motivo, se adaptaron en diversos lugares de la República Mexicana, los Centros de Acceso Público a las Tecnologías de la Información y Comunicación.

Los aciertos que ha tenido el Sistema Nacional e-México se pueden catalogar desde algunos de los ejes en que fue organizado:

- A) Conectividad: ha producido un aumento en el uso de banda ancha⁴⁴;
- B) Contenidos:
 - e-Gobierno: ha incrementado la calidad y el alcance de los servicios, especialmente a través de la iniciativa de Datos Abiertos⁴⁵;
 - e-Economía: el portal Compranet ha impulsado la automatización de las etapas del proceso de contratación gubernamental;
- C) Sistemas: aún se encuentran en funcionamiento los CCD y se sigue aprovechando gran parte de la infraestructura estatal⁴⁶.

No obstante, el gobierno electrónico en México ha sufrido fallos a lo largo de estos años, ya que esta nueva forma de prestar servicios está atravesando diversas fases de establecimiento en todo el mundo⁴⁷, por tanto, aún no se puede garantizar que las estrategias empleadas en un país van a ser exitosas en algún otro.

6. Desaciertos

Los errores que ha tenido el Sistema Nacional e-México también se pueden organizar desde los mismos ejes que lo formaron:

- A) Conectividad: los Centros Comunitarios Digitales que iniciaron su funcionamiento junto con el Sistema Nacional e-México, desaparecieron documentalmente en 2015; la reforma en materia de telecomunicaciones que se impulsó por el Gobierno Federal⁴⁸, provocó que a partir de marzo de 2015 se

44 http://www.inegi.org.mx/prod_serv/contenidos/espanol/bvinegi/productos/metodologias/MODUTIH/MODUTIH2013/MODUTIH2013.pdf

<http://www.inegi.org.mx> [consulta: 2015, octubre 1]

45 <http://datos.gob.mx/impacto/historias/homicidios-frontera-armas-eeuu.html>

<http://datos.gob.mx> [consulta: 2015, octubre 1]

46 <http://www.sct.gob.mx/despliega-noticias/article/en-marcha-la-red-nacional-de-centros-comunitarios-digitales-en-todo-el-pais/>

www.sct.gob.mx [consulta: 2015, octubre 1]

47 http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2015/08/04/090224b08304ca10/1_0/Rendered/PDF/One0step0forwa0ent0and0accountable0.pdf

<http://www-wds.worldbank.org> [consulta: 2015, octubre 1]

48 <http://www.sct.gob.mx/despliega-noticias/article/en-marcha-la-red-nacional-de-centros-comunitarios-digitales-en-todo-el-pais/>

[/www.sct.gob.mx](http://www.sct.gob.mx) [consulta: 2015, octubre 1]

manejasen mediáticamente como una iniciativa innovadora que ha surgido durante el gobierno de Enrique Peña Nieto y a partir de entonces se les asigna el nombre de: Centros Comunitarios de Capacitación y Educación Digital.

B) Contenidos:

- e-Gobierno: Existe falta de voluntad política respecto a la introducción de las TIC en la vida de los mexicanos, tal como lo demuestran los Planes Nacionales de Desarrollo analizados, además no se ha favorecido la comunicación con los ciudadanos a través de la retroalimentación⁴⁹;
- e-Economía: No se ha elaborado ninguna previsión relacionada con las debacles económicas que afectan la evolución de este tipo de proyectos;
- e-Educación: Las instituciones educativas aún cuentan con muy pocas computadoras y muchas de ellas ni siquiera tienen acceso a Internet, el analfabetismo tecnológico continúa siendo una desventaja dominante en la población, por ello es obligatorio incluir políticas públicas que fomenten la generación de conocimiento a través del uso de la tecnología⁵⁰;

C) Sistemas: la inversión federal en ciencia y tecnología sigue siendo insuficiente⁵¹ y el Fideicomiso 2058 e-México, conformado para coadyuvar con la operación del Sistema Nacional e-México, ha recibido rigurosas críticas por parte de la Auditoría Superior de la Federación, ya que en su informe de 2012 concluye que: “*el Titular de la Coordinación de la Sociedad de la Información y el Conocimiento, no vigiló la debida ejecución de los proyectos integrados al Fideicomiso*”⁵².

A pesar de estos tropiezos, en noviembre de 2013 se logró establecer una Estrategia Digital Nacional⁵³, que serviría de guía para acercar las TIC a los ciudadanos hasta que finalice el sexenio de Enrique Peña Nieto, de este modo, el Sistema Nacional e-México podrá seguir adelante, aunque quizás con otra

49 <http://www.revistazocalo.com.mx/45-zocalo/5483-presidencia-omite-retroalimentacion-en-redes.html>

<http://www.revistazocalo.com.mx/> [consulta: 2015, octubre 1]

50 <http://www3.inegi.org.mx/sistemas/descarga/?c=100>

www.inegi.org.mx [consulta: 2015, octubre 1]

51 <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=etec18&s=est&c=19181>

www.inegi.org.mx [consulta: 2015, octubre 1]

52 http://www.asf.gob.mx/Trans/Informes/IR2012i/Documentos/Auditorias/2012_1183_a.pdf

www.asf.gob.mx [consulta: 2015, octubre 1]

53 <http://cdn.mexicodigital.gob.mx/EstrategiaDigital22Dic2014.pdf>

www.presidencia.gob.mx/edn/ [consulta: 2015, octubre 1]

denominación, debido a la escasa claridad en el manejo de los recursos asignados al Fideicomiso 2058 e-México. No obstante, es importante mencionar que uno de los grandes aciertos del Sistema Nacional e-México fue el establecimiento de los CCD, su éxito se concretó porque en su desarrollo participaron tanto el Sector Público como el Sector Privado y la población civil.

7. Centros de Acceso Público a las Tecnologías de la información y comunicación

Para poder conocer las diversas formas de acceso a las Tecnologías de la Información y Comunicación que existen, es necesario conocer su definición y posteriormente hacer un breve recorrido a través de las numerosas denominaciones que reciben los modelos existentes en Latinoamérica hasta llegar al análisis de los CCD mexicanos. En 2006 Maeso y Hilbert consideran como Centros de Acceso Público a las Tecnologías de información y comunicación (CAPT) a “*aquellos centros públicos donde se presta acceso a las TIC a la sociedad, entendida ésta en su conjunto, sea con o sin conexión a Internet*”⁵⁴. Esta definición se basa en la convenida en el Taller Mundial de Indicadores de Acceso a las TIC, celebrado en la Ciudad de México en Noviembre de 2004, en él se definió este tipo de centros como:

...aquel punto, lugar, centro o establecimiento de acceso a Internet disponible al público, a tiempo completo o parcial. Los CCD, los Internet cafés, bibliotecas, centros educativos y otros establecimientos similares, forman parte de este grupo, siempre y cuando se permita el acceso al público en general. Todos estos centros deben poner a disposición del público al menos una computadora para el acceso a Internet.

Telecentro: Proenza, Bastidas-Buch y Montero en 2001 indicaron que se trata de un “*local compartido que provee acceso al público a tecnologías de información y comunicaciones*”⁵⁵. Sin embargo Maeso y Hilbert

⁵⁴ Óscar MAESO (Fundación Chasquinet); Martin HILBERT: *Centros de acceso público a las tecnologías de información y comunicación en América Latina: características y desafíos*. Publicación de las Naciones Unidas, 2006, pp. 97-99.

<http://www.martinhilbert.net/centros-de-acceso-publico-a-las-tic-en-america-latina-caracteristicas-y-desafios/>

<http://www.martinhilbert.net/> [consulta: 2015, octubre 1]

⁵⁵ Francisco PROENZA; Roberto BASTIDAS-BUCH; Guillermo MONTERO: *Telecentros para el desarrollo socioeconómico y rural en América Latina y el Caribe Oportunidades de inversión y recomendaciones de diseño con especial referencia a Centroamérica*, Documento de trabajo. Banco Interamericano de Desarrollo División de Programas Sociales, Departamento de Operaciones, Unidad Rural, Departamento de Desarrollo Sostenible, Unidad de Tecnología de Información para el Desarrollo, Unión Internacional de Telecomunicaciones Sector de Desarrollo de las Telecomunicaciones, FAO Centro de Inversiones, Washington, D.C.2001, Págs. VIII-XI.

determinan que los CAPT se denominan de diversas formas en América Latina y el Caribe, ya que toman en consideración sus objetivos particulares, razones históricas, factores políticos o sociales; las denominaciones más aceptadas son las siguientes:

- CAPT gubernamental: Telecentros o Infocentros;
- CAPT privado con objetivos sociales: Telecentros o Infocentros Comunitarios;
- CAPT privado con objetivos comerciales: Cybercafés;
- CEAT público: Programas de Informática educativa para centros del sistema estatal;
- CEAT privado: Programas de Informática educativa para centros de educación privados.

Además Maeso y Hilbert manifiestan que los Centros educativos de acceso a las tecnologías (CEAT), son programas de acceso a las TIC ubicados en instituciones educativas y se caracterizan por dar acceso solamente a las personas relacionadas con la institución y reciben las siguientes denominaciones:

- Centros Tecnológicos Comunitarios (Argentina),
- Comunitarios Digitales (México),
- Comunitarios para el aprendizaje múltiple (México)⁵⁶,
- Telecentros (Centroamérica / Africa / ONGs),
- Infocentros comunitarios (Venezuela),
- Centro para la democratización de la información (Brasil).

Los CCD, fueron resultado de la suma de voluntades de diferentes dependencias de la Administración Pública Federal y de otras Instituciones gubernamentales. Generalmente un CCD era patrocinado por una dependencia o institución gubernamental que proporcionaba el lugar, los muebles y el equipamiento de cómputo⁵⁷. El Sistema Nacional e-México proveía la conectividad satelital para suministrar los servicios digitales, las dependencias o instituciones que patrocinaron un CCD e-México recibieron como beneficio

[http://www.academia.edu/480858 Telecentros para el desarrollo socioecon%C3%B3mico y rural en Am%C3%A9rica Latina y el Caribe](http://www.academia.edu/480858_Telecentros_para_el_desarrollo_socioecon%C3%B3mico_y_rural_en_Am%C3%A9rica_Latina_y_el_Caribe)

<http://www.academia.edu> [consulta: 2015, octubre 1]

⁵⁶ Rossy Lorena LAURENCIO MEZA: Internet como medio para el desarrollo social: una mirada desde los Centros Comunitarios de Aprendizaje Múltiple. Corporación Colombia Digital, Observatorio del Desarrollo Digital, www.colombiadigital.net/informacion/docs/Intsocial_dcom_d.pdf

www.colombiadigital.net [consulta: 2007, enero 8]

⁵⁷ La fuente de información primaria para realizar los diversos apartados que integran este documento ha sido el sitio web: www.e-mexico.gob.mx/. [consulta: 2007, enero 8]

toda la plataforma de servicios del Sistema Nacional e-México. Los cuatro servicios que aportan los CCD a las comunidades de todo el país, son: acceso a Internet, uso de equipos de cómputo con paquetería diversa, impresión de archivos y documentos, asesoría y capacitación al público en general.

Público objetivo:

- Estudiantes: alumnos de todos los niveles y edades pueden hacer uso de los equipos como complemento a su formación académica, para consultar información de todo el mundo y tomar cursos de capacitación;
- Maestros: los profesores se pueden beneficiar de los CCD para su actualización académica y a través de la consulta de contenidos educativos para el desarrollo de sus funciones docentes;
- Amas de casa: las amas de casa y en conjunto los padres de familia pueden conocer los servicios públicos disponibles en su comunidad, municipio o estado; así como información en materia de salud, deporte, cultura y entretenimiento;
- Además de los anteriores, también pueden beneficiarse de los CCD adultos mayores, indígenas, campesinos, comerciantes, empresarios, servidores públicos, profesionistas, turistas, entre otros.

El despliegue del Sistema Nacional e-México incluyó 3.661 CCD en escuelas primarias, secundarias, preparatorias y bibliotecas; 167 en gobiernos municipales; 1.033 en centros de salud; 1.562 en Centros del Instituto Nacional de Educación para Adultos, INEA-CONEVYT; 700 centros - Secretaría de Desarrollo Social (SEDESOL); y 77 en oficinas federales. En 2005 existían en total 7.500 CCD. Para el año 2006, se planeaba tener en marcha más de 10.000 CCD. La población que hace uso de los CCD, en la mayoría de los casos, sólo pagó las cuotas de recuperación requeridas para cubrir los costos marginales para la operación y mantenimiento de los CCD.

Actividades de los CCD: en los CCD se desplegaron actividades educativas, de formación y capacitación y también servicios como correo electrónico, de manera que se aprovecharon las computadoras para resolver problemas de la vida cotidiana, como la educación, la capacitación para el trabajo y la utilización de diversos servicios en línea que el gobierno puso a disposición de la ciudadanía. Los CCD conformaron un espacio con computadoras e Internet, el cual podía ser utilizado sin necesidad de saber computación, ya que siempre disponían de un especialista que ayudaba a los usuarios a realizar estas actividades. Algunas de las actividades que se realizaron eran: capacitación y asesoría, soporte técnico, atención a usuarios, difusión y promoción, apoyo a procesos comunitarios, vinculación interinstitucional, rescate cultural e histórico.

Uso de los CCD⁵⁸:

1. SEP: la SEP ostentó más de la mitad de los CCD, y para hacerse cargo de ellos comisionó al Instituto Latinoamericano de la Comunicación Educativa (ILCE). La SEP proporcionó el dinero para iniciar el funcionamiento de los CCD; el ILCE ofreció a las Secretarías de Educación de los Estados la oportunidad de tener conectividad a cambio de que abriesen las puertas del centro al público en general. El ILCE suministró a cada escuela una máquina que funcionaba como servidor y en ella se encontraban todos los contenidos de Red Escolar⁵⁹. La otra gran fuente de información a la que se dio acceso fue el portal SEPiensa⁶⁰, en él se ofrecieron contenidos vinculados a la educación básica, para reforzar la formación académica y cívica;
2. SEDESOL: los CCD a cargo de esta Secretaría también tuvieron un enfoque educativo, sin embargo, en ellos el reto era diferente, ya que pretendían instituir Centros Comunitarios de Aprendizaje (CCA). Esta estrategia formó parte del programa Microrregiones (diseñado para atender a municipios de alta, y muy alta marginación)⁶¹. Los CCA se ubicaron en lugares poco comunicados, sin una infraestructura básica, su economía era de autoconsumo, el capital social pobre y no tenían capacidad para generar redes. Para este programa, la conectividad que ofrecía el sistema e-México fue uno de los ingredientes para mejorar las condiciones de vida de estas comunidades. Los CCA buscaban promover los proyectos productivos de la comunidad por medio del acceso a información técnica y al conocimiento de sus mercados, de esta manera, los productores locales usaban el centro para dar un valor agregado a sus productos y encontrar mejores alternativas para venderlos. SEDESOL creó el portal de los Centros Comunitarios de Aprendizaje⁶², enfocado a la educación, cuyos contenidos fueron desarrollados por la SEP y el INEA, a través del portal se dio acceso en línea a educación básica, media y superior y se ofrecieron cursos básicos de computación en lenguas indígenas. Los CCA se hospedaron en recintos proporcionados por los municipios, que le pagaban al encargado de operarlo y pagaban también la conectividad, SEDESOL únicamente suministraba los equipos.
3. El Instituto Nacional para Educación de Adultos (INEA): el modelo del INEA fue muy diferente. Establecieron el esquema de plaza comunitaria, que era un aula tradicional donde se estudia con libros; un aula de medios,

58 <http://www.politicadigital.com.mx/?P=leernoticia&Article=623>

<http://www.politicadigital.com.mx> [consulta: 2015, octubre 1]

59 <http://red.ilce.edu.mx/> [consulta: 2015, octubre 1]

60 <http://sepiensa.org.mx/> [consulta: 2015, octubre 1]

61 <http://www.microrregiones.gob.mx/catloc/> [consulta: 2015, octubre 1]

62 <http://www.centroscomunitariosdeaprendizaje.org.mx/> [consulta: 2015, octubre 1]

donde se observaban videos desarrollados por la Universidad Nacional Autónoma de México (UNAM) y el ILCE, y la Plaza Comunitaria en sí, que contaba con 10 computadoras, y en ella se utilizaron los contenidos desarrollados para el portal del Consejo Nacional de Educación para la Vida y el Trabajo (CONEVyT), sitio que contiene todas las herramientas para que jóvenes y adultos con rezago educativo estudien la primaria y secundaria, así como otros temas útiles para la vida cotidiana. Al igual que en el caso de SEDESOL, los alumnos estaban registrados en el sistema y se llevaba un seguimiento de las materias que cursaban. En este caso, la manera de medir el éxito de una plaza comunitaria fue a través de los certificados de primaria y secundaria que se otorgaron —aunque sólo una parte de la formación se encontraba directamente relacionada con el uso de la computadora—.

4. Secretaría de Salud: no todos los CCD tuvieron objetivos educativos; los administrados por la Secretaría de Salud estuvieron abiertos para el uso de pacientes y profesionales, principalmente para que pudieran acceder a las páginas de salud. Los principales usuarios de estos CCD fueron los propios empleados de las clínicas. Los médicos y enfermeras los utilizaron para realizar consultas acerca de normas médicas, síntomas de enfermedades, etcétera;
5. INAFED: apoyó a los municipios con recursos financieros para instalar CCD, no se marcó un objetivo específico para estos centros, e incluso se ignora cuál ha sido el uso que se les ha dado en la mayoría de los casos, aunque se sabe que algunos de sus principales usuarios fueron estudiantes de secundaria y preparatoria, así como funcionarios públicos que aprovecharon la tecnología para comunicarse con otros funcionarios.

Margáin sostuvo que: *“el modelo de CCD más exitoso es, sin lugar a dudas, el del INEA, luego sigue el de Oportunidades, y el menos exitoso es el de Salud, porque tienen muchos menos componentes culturales”*⁶³.

Sustentabilidad de los CCD: el Gobierno Federal aportó recursos para ponerlos a funcionar, sin embargo no podrá, encargarse de su mantenimiento para siempre.

La SEP, se hizo cargo del pago de los primeros seis meses de conectividad de la primera red y pagó un año de la segunda. La SEDESOL, buscó que las comunidades formaran un comité de apoyo a los CCA; si un CCD era útil para la comunidad, ellos encontrarían la manera de mantenerlo. El camino más viable a mediano plazo, podría ser un modelo de gestión autónomo de los centros, es decir, que sean administrados por las organizaciones locales a quienes beneficia:

63 <http://www.politicadigital.com.mx/?P=leernota&Article=622&c=9>
<http://www.politicadigital.com.mx> [consulta: 2015, octubre 1]

hospitales y clínicas, escuelas, municipios, etc. El promotor ha sido el factor clave para el apropiamiento de los centros; es la figura que mostró su utilidad a la sociedad; cuando los promotores pertenecen a la propia comunidad de vecinos, resultaba mejor. Para que la comunidad encuentre beneficios en los CCD, es básico que existan contenidos locales que les favorezcan.

El promotor de los CCD: Garza-Cantú define al promotor o facilitador como la persona encargada de apoyar a los visitantes que acuden al CCD en sus dudas con respecto al uso de Internet y las computadoras. Son personas capacitadas para orientar a la gente que no ha tenido conocimientos informáticos a usar fácilmente las computadoras, sin importar su edad, su grado de estudios o su condición social. Son la figura central del éxito de los CCD⁶⁴.

Los promotores eran los responsables del mantenimiento y administración de los centros comunitarios, así como del asesoramiento y capacitación de los usuarios. Al interior de los centros comunitarios, los promotores supervisaban el buen funcionamiento de los equipos y apoyaban a los usuarios en sus búsquedas de información y uso de las computadoras. Al exterior, eran promotores del CCD en su comunidad, para que la población en general conociera los servicios que se proporcionaban y se beneficiara de ellos. Los modelos de promotores fueron muy distintos en cada dependencia; a unos promotores se les pagó, a otros no; para unos era tiempo extra, y otros más podían estudiar en la universidad virtual mientras trabajaban como promotores⁶⁵.

Oseguera destacó que era necesario crear un esquema económico que permitiera organizar un modelo particular de promotores. La SCT no era dueña de los CCD por ello no pudo instrumentar alguna acción que incentivara a los promotores⁶⁶.

El ILCE capacitó a los responsables de los centros, CONACULTA y la fundación UNETE, fortaleció y equipó bibliotecas. El ILCE desarrolló un esquema para entrenar a los promotores que se divide en dos partes, la presencial y la virtual. Al principio se llevaba a la Ciudad de México a los coordinadores estatales de las distintas dependencias para capacitarlos, entregarles manuales, videos y, posteriormente, se les proporcionaba asesoría a distancia, con el objeto de que se encargaran de capacitar a los promotores de los CCD. El esquema

64 Mariano GARZA - Cantú CHÁVEZ: "Tema central", *Revista Política Digital*, Año 4 (Núm. 22), México. Nexos, 2005, pp. 24-47

http://www.politicadigital.com.mx/pics/edito/multimedia/417/filearton101_multimedia.pdf
<http://www.politicadigital.com.mx> [consulta: 2015, octubre 1]

65 <http://www.politicadigital.com.mx/?P=leernoticiaprint&Article=624>

<http://www.politicadigital.com.mx> [consulta: 2015, octubre 1]

66 Juan Antonio OSEGUERA: "El sistema Nacional e-México", *Revista Política Digital*, Año 4 (Núm. 22), México. Nexos, 2005, pp. 16-18

http://www.politicadigital.com.mx/pics/edito/multimedia/417/filearton101_multimedia.pdf
<http://www.politicadigital.com.mx> [consulta: 2015, octubre 1]

no resultó, ya que se perdió el control y la capacitación que hicieron no fue la adecuada. Posteriormente se viajó a los estados, para capacitarlos directamente. Los cursos comprendían cuatro competencias básicas que servían para poner en funcionamiento un centro:

- 1) Operación: abrir el local, encender las computadoras, soporte técnico, etcétera.
- 2) Administración: recibir a los usuarios y registrarlos; saber cuáles eran las necesidades del CCD y hacer lo necesario para resolverlas.
- 3) Facilitación: crear un entorno amable para el usuario y enseñarle los aspectos básicos para la utilización del equipo de cómputo: encender la computadora, operarla, navegar en Internet, abrir el correo electrónico, enviar y recibir mensajes.
- 4) Promoción: conocer y difundir los servicios disponibles en Internet que pueden servir a la gente.

A los promotores, se les instruyó en temas específicos según la dependencia a la que pertenecían y se les dieron ideas para que los centros fueran autosustentables. Esta capacitación se complementó con actividades en línea que ofrecía el Campus e- México, que consistía en tres cursos:

- servicios del gobierno mexicano: los promotores conocieron el tipo de trámites gubernamentales que puede hacer la gente en línea;
- creación de páginas Web: aprendieron a crear miniportales en los que se ofrecía información respecto a sus comunidades;
- búsqueda de información en Internet.

Cada curso tuvo una duración promedio de cinco semanas y se trabajaba en grupos de 30 personas, existían foros donde se intercambiaban experiencias, y un *newsletter* donde se publicaron noticias, ideas e información de interés para los promotores, creando así una cadena de apoyo mutuo y de valor. También existió un sistema de apoyo técnico para que los promotores resolvieran los problemas con los que se enfrentaban diariamente. La labor del promotor radicó en lograr que la comunidad se apropiara de los CCD, es decir, hacer que los ciudadanos se beneficiaran de estos centros.

Modelos de promotores: la SEP era la dependencia que tenía más CCD y por ende mayor número de promotores. Eran coordinados por las Secretarías de Educación Estatales y eran hombres y mujeres, en la misma proporción, entre los 26 y 35 años de edad. La mitad eran maestros, mientras que el resto se repartía entre técnicos y voluntarios. El principal problema que enfrentó la

SEP en sus CCD fue la alta rotación de los promotores⁶⁷, debido a que no tuvo una política general para su manejo. El modelo que se consideró más exitoso fue el de los centros de INEA/ CONEVyT, donde los promotores recibían una gratificación de alrededor de 2 mil pesos mensuales, por un trabajo que exigía jornadas de ocho a 10 horas diarias y donde se trabajaba incluso sábados y domingos.

Otro modelo exitoso fue el de los promotores de los CCA de SEDESOL en los que, gracias a un acuerdo con el Tecnológico de Monterrey, se les ofrecía la oportunidad de estudiar en el Tec Milenio con una beca del 100%. Así, aquellos que no tenían la preparatoria concluida podían estudiarla y aquellos que ya la tenían podían estudiar una carrera. Generalmente estos promotores eran jóvenes de la misma comunidad que en algún momento salieron a Estados Unidos o a un centro urbano y que tuvieron la oportunidad de aprender computación. Que fueran miembros de la comunidad ayudó mucho para que comprendiesen sus problemas y necesidades. A cambio de su trabajo recibieron capacitación y, lo más importante, acceso a la educación del Tecnológico de Monterrey. Gracias a este incentivo, la rotación disminuyó, a pesar de que la remuneración económica era muy variable, ya que dependía de cada municipio. Otra vertiente en la que trabajó SEDESOL consistió en desarrollar un sistema para que las comunidades evalúen a los promotores, de tal suerte que cuando cambia un presidente municipal se determina de manera más objetiva la permanencia o no del promotor en funciones.

En contraste con los casos anteriores, los CCD de la Secretaría de Salud no contemplaron la figura del promotor. Tuvieron un responsable del centro, que por lo general era el que sabía más de computación en la clínica, y para quien el CCD sería una más de sus responsabilidades, por el mismo sueldo. Un caso similar fue el de los CCD correspondientes al INAFED, donde existe gran desconocimiento sobre la situación de los promotores administrados por los municipios.

Las Plazas Comunitarias e-México: la plaza comunitaria es un lugar donde los jóvenes y adultos tuvieron acceso a oportunidades educativas y formación para el trabajo, con el uso combinado e integrado de tres ambientes educativos: asesoría presencial, sala de video y TV educativa, sala de cómputo e Internet⁶⁸. Los responsables eran el Sistema Nacional para la Educación de Adultos (CONEVt e INEA). 29 Institutos Estatales y 3 delegaciones. El objetivo de las plazas comunitarias consistía en aplicar programas de alfabetización, primaria y secundaria a mayores de 15 años. El Instituto Estatal instalaba la plaza en un espacio convenido con la comunidad, la autoridad municipal, la autoridad estatal,

67 <http://www.politicadigital.com.mx/?P=leernoticia&Article=623>
www.politicadigital.com.mx [consulta: 2015, octubre 1]

68 http://www.somece.org.mx/videoconferencias/plazas_comunitarias.pdf
www.somece.org.mx [consulta: 2007, enero 8]

o con alguna organización social, civil o religiosa, el equipo y recursos educativos se adquirieron a través del presupuesto Federal asignado al INEA, la SCT proporcionó la conectividad a cada una de las plazas, El Instituto Estatal contrató y capacitó 2 figuras operativas: un apoyo técnico y un promotor, el Instituto Estatal operó los servicios educativos que se ofrecieron en la plaza de acuerdo a las normas curriculares y apoyó la coordinación con otras entidades usuarias de la plaza.

Red Escolar: fue uno de los proyectos más sustentables, gracias a la infraestructura con que contaba y la colaboración que mantuvo con distintas instituciones [SEP, el ILCE y la Red Satelital de Televisión Educativa (EDUSAT), entre otras]. Contó con un gran número de Centros de Acceso Público a las Tecnologías de Información y Comunicación en el país: 2500, cantidad casi semejante a los CCD instalados hasta el año 2003 por el proyecto gubernamental e-México (3200 CCD).

Internet en mi Biblioteca: con el apoyo y coordinación de la Fundación UNETE y otras instancias gubernamentales, privadas y sociales, la sostenibilidad del proyecto Internet en mi Biblioteca se aseguró durante varios años⁶⁹.

Aunadas a las anteriores, existen otras formas de acceso a las Tecnologías de la Información y Comunicación, tanto públicas como privadas, sin embargo, en este documento, solamente serán tratadas, las formas de acceso público.

Aula Móvil: la SEP puso en operación la primera “Aula Móvil” mediante la cual se dió capacitación en computación a alumnos y a profesores. Este equipo, que se diseñó conjuntamente con la empresa Microsoft y la Unión de Empresarios para la Tecnología en Educación (UNETE), recorrió todo el país para capacitar a niños, jóvenes y profesores⁷⁰.

Enciclopedia: fue una herramienta tecnológica creada para estimular el aprendizaje del estudiante respecto a la currícula contenida en los libros de texto gratuito de la SEP; ofrecía diferentes recursos para que el alumno profundizara y ampliase su horizonte en relación con cada uno de los temas. El costo total que se pronosticó sumó 200 millones de pesos, aunque el creador del sistema: Felipe Bracho Carpizo, aseguró, “estamos buscando convenios para que sea más económico”. Así, para el 2006, se esperaba que al menos 165 mil

69 <http://www.cnca.gob.mx/cnca/nuevo/diarias/090999/internet.html>
www.cnca.gob.mx [consulta: 2007, enero 8]

70 Presidencia de la República: “En operación la primera Aula Móvil”, *Las buenas noticias*, miércoles 16 de febrero de 2005.
<http://fox.presidencia.gob.mx/buenasnoticias/?contenido=16770&pagina=1&palabras=aula+movil>
www.fox.presidencia.gob.mx [consulta: 2015, octubre 1]

aulas de todo el país y en todos los grados estuviesen equipadas con este sistema para aprender⁷¹.

En abril de 2015 se pone en marcha la Red de Puntos México Conectado⁷², a través de ella se proporciona capacitación en mecánica, programación, robótica, emprendimiento y en el desarrollo de habilidades digitales, también pretende fomentar la cultura y la creatividad mediante el uso de la tecnología⁷³, esta red está integrada por 32 Centros Comunitarios de Capacitación y Educación Digital, uno en cada estado de la República; el proyecto México Conectado cuyo objetivo consiste en promover el derecho constitucional de acceso a banda ancha e Internet, brinda el apoyo principal a estos centros.

8. Consideraciones finales

Los principales aciertos generados durante la gestión de Vicente Fox han sido:

- la creación del portal e-Mexico para promover el uso de servicios de salud, educación, gobierno, ciencia y tecnología en la sociedad, con el fin de intentar reducir la brecha digital existente en la población;
- la instalación de la infraestructura necesaria para poner en marcha al portal;
- el desarrollo atinado de los contenidos del portal.

Sin embargo también tuvo algunos desaciertos, ya que el Sistema Nacional E-México no tuvo objetivos claros y no hubo una planeación para generar contenidos de calidad e incluso existió desconocimiento sobre los alcances y la influencia de Internet en la sociedad. El Sistema Nacional e-México se manejó como un programa prioritario de gobierno que tuvo metas muy amplias y su avance no fue concordante con lo planeado. Aunado a ello, tuvo una gran vulnerabilidad política debido a que no se estableció como una política pública, por lo tanto, los políticos en turno lo podrán finalizar en el momento en que sus impulsores queden fuera del ámbito de toma de decisiones o cuando se les requiera la entrega de información respecto al destino y aprovechamiento de la inversión reservada para desarrollar el Sistema Nacional e-México, tal como

71 Presidencia de la República: “Enciclopedia, el mundo al alcance de sólo un clic”, *Las buenas noticias*, miércoles 27 de octubre de 2004.

<http://fox.presidencia.gob.mx/buenasnoticias/?contenido=15664&pagina=2&palabras=enciclopedia>
www.fox.presidencia.gob.mx [consulta: 2015, octubre 1]

72 <http://www.pmc.gob.mx/> [consulta: 2015, octubre 1]

73 <http://www.promotoresdigitales.mx/noticias/sct-pone-en-marcha-la-red-de-puntos-mexico-conectado>

<http://www.promotoresdigitales.mx> [consulta: 2015, octubre 1]

ocurrió a finales de 2014⁷⁴. Esto nos lleva a corroborar que en el aspecto económico, carece de mecanismos alternativos de financiamiento, de modo que se puede convertir en algo incosteable, el software propietario tiene altos costos; a mediano plazo será necesario renovar el hardware y en algunas ocasiones se tendrán que sufragar los gastos causados por desastres naturales. Aunado a ello, la falta de información sobre sus avances, su financiamiento y el manejo de sus recursos, han generado gran desconfianza para la sociedad, por ello es imperativo generar un mecanismo de evaluación que mida los avances, el reparto de recursos y el resultado que han tenido los CCD en las comunidades donde se han ubicado.

En lo social, se necesita atender a todos los sectores y no solo a grupos marginales y además se debe confeccionar una Agenda Digital planificada a largo plazo que no dependa íntegramente del presupuesto gubernamental.

De todo lo anterior podemos colegir que en México el gobierno electrónico aún se encuentra en pleno desarrollo y que ha presentado diversos aciertos y desaciertos, por tal motivo, es válido reestructurar su organización y funcionamiento, para redirigirlo hacia un objetivo claro y preciso, en el que no se pierdan de vista principalmente a los ciudadanos y a sus múltiples necesidades. Sin embargo, no resulta legítimo ocultar y anular el camino que se ha recorrido, pues la experiencia adquirida durante estos 15 años ha favorecido el ingreso de México a la Alianza para el Gobierno Abierto⁷⁵, no obstante aún no se le puede considerar como un país abierto y transparente, incluso en el índice 2015 de Gobierno Abierto elaborado por el *World Justice Project*⁷⁶ se ha calificado muy bajo a México⁷⁷. El 15 aniversario del Sistema Nacional e-México se celebrará únicamente si la SCT entrega la información referente al Fideicomiso 2058 e-México, ya que este será el primer paso hacia la verdadera transparencia del gobierno electrónico y abierto en México.

74 <http://inicio.ifai.org.mx/Historico/Sesi%C3%B3n%20Pleno%2029-10-14.pdf>

<http://inicio.ifai.org.mx/SitePages/ifai.aspx> [consulta: 2015, octubre 1]

75 <http://www.opengovpartnership.org/es> [consulta: 2015, octubre 1]

76 <http://worldjusticeproject.org/rule-of-law-index> [consulta: 2015, octubre 1]

77 http://imco.org.mx/politica_buen_gobierno/indice-del-estado-de-derecho-2015-via-world-justice-project/

<http://imco.org.mx/home/> [consulta: 2015, octubre 1]

Comercio electrónico y redes sociales: nuevo paradigma negocial

Miguel Arrieta Zinguer*

SUMARIO: I. Comercio electrónico. II. Redes sociales. III. El desarrollo de las redes sociales en la Sociedad de la Información. IV. Impacto de las redes sociales en el comercio electrónico en Internet. El denominado *Social Commerce*. V. Conclusiones.

Resumen

El presente trabajo tiene por objeto el estudio del desarrollo de las redes sociales en Internet y su influencia en el comercio electrónico, especialmente en el comercio electrónico con consumidores. Entre los principales aspectos analizados destacan el impacto de las redes sociales en el ámbito del mercadeo, la medición de la calidad de servicios al cliente, y la utilidad de estos medios como instrumentos de fidelización de la clientela.

Palabras clave: Comercio electrónico. Redes sociales. Sociedad de la Información. Internet.

Abstract

This work aims to study the development of social networks and its influence on e-commerce, especially in electronic commerce where consumers intervene. Among the main issues analyzed in this paper, the impact of social networks in the field of marketing, measurement of the quality of customer service, and the use of these means in campaigns to increase customer loyalty are emphasized.

Keywords: E-commerce. Social Networks. Information Society. Internet.

Recibido: 15/11/2015 • Aceptado: 9/12/2015

* Abogado (UCAT, 1990), Magíster en Gerencia de Empresas (UNET, 1996), Especialista en Derecho Mercantil (UC 1999), Especialista en Derecho Tributario (UCAT, 2006), Doctorando en Ciencias Gerenciales (UNEFA) y en Ciencias, Mención Derecho (UCV). Profesor Asociado de la UCAT y de Postgrado en la UCAB, UCAT, ULA, UNEFA, ENAHP y Universidad Yacambú. Asesor Gerencial.

I. Comercio electrónico

La época que vivimos en la actualidad se caracteriza por la concientización acerca de la importancia que las Tecnologías de la Información y la Comunicación, tienen para el manejo de los más diversos aspectos de la vida cotidiana. Este fenómeno trae como consecuencia una nueva apertura de tecnologías y culturas que determina un creciente flujo de información, bienes e ideas, generando de esta manera transformaciones sociales sin precedentes. La realización de negocios y contratos por medios electrónicos constituye una realidad en desarrollo desde finales del Siglo XX, el cual se ha visto favorecido por lo demás por otro fenómeno económico que le está estrechamente vinculado, que es la globalización económica, conforme a la cual las actividades y fenómenos económicos generan consecuencias relevantes en todo el mundo, lo cual plantea sin duda una paradoja en la realidad comercial actual, toda vez que se presentan importantes oportunidades para aprovechar la globalización de los mercados, no obstante estos mercados se transforman con rapidez, lo cual determina que las empresas deben aprovechar las economías de escala, así como segmentar y globalizar las ofertas de bienes y servicios.

En este orden de ideas, uno de los fenómenos que ha determinado un mayor crecimiento e influencia desde el punto de vista de la utilización de las TIC, es precisamente, el comercio electrónico, y particularmente el comercio electrónico en Internet, que por su ductilidad, alcance global y facilidad de integración, facilita el intercambio de contenidos, acceso a información con carácter global y ha tenido, por lo demás un importante efecto sobre diversos aspectos de la vida humana contemporánea. Este crecimiento del comercio electrónico en Internet ha determinado un crecimiento exponencial en la oferta de bienes y servicios, hasta el punto de ofrecerse un abanico de oportunidades casi paralelo al del mercado ordinario.

La concepción del comercio electrónico, comprende en sentido amplio, tal como advierte Sarra, A. (2000, 278), cualquier transacción comercial efectuada por medios electrónicos, es decir, incluye la utilización del fax, télex, el teléfono, los EDI (*Electronic Data Interchange*) e Internet¹. Por su parte, la Organización Mundial del Comercio ha señalado que el comercio electrónico, es: “...*la producción, publicidad, venta y distribución de productos vía redes de telecomunicaciones...*” de donde resulta que en general, se estima que el comercio electrónico se compadece con el comercio electrónico en internet. La utilización de las redes telemáticas para concluir operaciones comerciales no es una novedad absoluta, puesto que los medios indicados se han empleado

¹ El comercio electrónico directo comprende a aquellas actividades en las cuales el pedido, despacho y pago se realiza por medios electrónicos (comprende productos y bienes susceptibles de ser digitalizados), mientras que el comercio electrónico indirecto comprende aquellas actividades donde el pedido y el pago se realiza por medios electrónicos, mientras que el despacho se realiza por medios comerciales tradicionales.

desde hace décadas para facilitar o concluir negocios jurídicos comerciales. No obstante, en sentido restringido, que es el más utilizado en la actualidad, se entiende por comercio electrónico el realizado a través de redes (abiertas o cerradas) mediante la relación entre oferta y demanda, mediante la utilización de herramientas electrónicas y de telecomunicaciones.

La posibilidad cierta que personas en cualquier país del mundo puedan efectivamente adquirir o vender bienes o servicios de cualquier naturaleza, ensancha sin lugar a dudas las posibilidades comerciales, aparte de colocar a los vendedores de bienes o prestadores de servicios ante mercados cada vez más globales y diversos, trayendo nuevas oportunidades de negocio, una mayor competitividad, una reducción de costos y una mayor celeridad en el desarrollo de las relaciones comerciales. De otra suerte, el comercio electrónico puede además, ser beneficioso para los consumidores, pues les permite realizar la adquisición de productos y servicios en cualquier lugar y permitiéndoles una oferta más diversa y amplia. No obstante la utilización del comercio electrónico también acarrea riesgos e incertidumbres que se derivan de aspectos controvertidos, tales como el lugar y momento de perfeccionamiento de las operaciones comerciales electrónicas, los problemas derivados de la seguridad en las redes informáticas, la delimitación de la responsabilidad entre los diversos actuantes en las operaciones comerciales electrónicas, entre otros.

Acerca de la relación entre comercio electrónico y contratación por medios electrónicos², resultan esclarecedoras las palabras de Rodner, J. (2001, 36):

El comercio electrónico no es una fuente nueva de obligaciones. La naturaleza vinculante de las relaciones en una operación de comercio electrónico, nace con base en la figura jurídica subyacente que forma parte de la relación. En la mayoría de los casos de comercio electrónico estamos frente a simples contratos de compraventa o contratos de servicio. El comercio electrónico está constituido por actos o negocios jurídicos de naturaleza unilateral o bilateral los cuales corresponden, en su gran mayoría, a contratos tipo dentro de la mayoría de los países de Derecho civil.

De manera que el comercio electrónico tiene como elementos resaltantes, que: a) se transnacionalizan los efectos de las operaciones comerciales, dado que los límites geográficos y políticos carecen de importancia, puesto que se realizan fundamentalmente mediante la utilización de redes abiertas, como por ejemplo la red Internet que, por su propia naturaleza acorta las distancias y facilita la realización de operaciones comerciales entre personas ubicadas en lugares distantes, allende las fronteras políticas y geográficas que establecen

² Se debe distinguir entre los contratos informáticos, que son aquellos que tienen como objeto bienes o servicios informáticos, de la contratación electrónica que se refiere a la realización de los contratos por medios informáticos, donde se trata de los mismos contratos del mundo material (civiles, mercantiles, administrativos, etc.), pero que se celebran por medios electrónicos.

los diversos países; b) ausencia de barreras de entrada, puesto que la rapidez, facilidad y relativamente bajo costo que implica para una persona o empresa realizar operaciones comerciales electrónicas que impliquen la oferta de bienes y servicios por Internet; c) necesidad de una regulación uniforme que permita la solución de las disputas de carácter comercial, generadas como consecuencia de las operaciones comerciales realizadas en lugares distantes³, independientemente de los montos objeto de los contratos y del lugar de realización de los mismos, toda vez que una verdadera masificación del comercio electrónico requerirá la existencia de mecanismos jurídicos para la solución de los conflictos que se puedan producir; d) necesidad de actualización y adecuación del marco legislativo regulador de las operaciones comerciales, con el objeto de reconocer las nuevas instituciones y medios que se precisan para la realización de las operaciones comerciales electrónicas en un entorno comercial abierto⁴; e) la consecución de normativa de carácter internacional con carácter uniforme que permita una regulación más o menos equitativa para las operaciones de carácter electrónico que se realicen entre individuos o empresas ubicados en diversos países.

Respecto al fundamento legal del comercio electrónico, se debe considerar que si bien es cierto que en Venezuela, a diferencia de lo que ocurre en otros países, no existe una regulación específica en materia de comercio electrónico⁵; también es cierto que existe una normativa específica que brinda un sustento conceptual-normativo a las operaciones comerciales electrónicas, como es la Ley sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE), que otorga y reconoce eficacia y valor jurídico a la firma electrónica, al mensaje de datos y

3 La normativa mercantil general venezolana no posee una regulación específica para el caso de la contratación comercial entre ausentes (excepción hecha por la normativa de la Ley de Mensajes de Datos y Firma Electrónica, en cuanto le resulte aplicable), no obstante en España, la Ley N° 47 de 2002, que recoge las normas de la Directiva 97/7 de la C.E. en materia de contratos a distancia, así como el Real Decreto N° 1906 de 1999, acerca de la contratación electrónica con condiciones generales de contratación, que determinan normas específicas para estas modalidades contractuales.

4 Es preciso establecer que la concepción del comercio electrónico ha evolucionado paulatinamente, puesto que en la actualidad la realización de las operaciones comerciales electrónicas, realizadas inicialmente mediante redes cerradas y únicamente entre empresas, mediante el comercio electrónico indirecto, hasta las operaciones comerciales realizadas mediante redes abiertas, con protocolos de información independientes, de manera que las redes interempresariales (EDI), han evolucionado hasta el desarrollo de las intranets y de la creación de elementos que permiten no solo el intercambio de información y manifestación de voluntades contractuales en tiempo real y de manera remota, sino la utilización de los medios electrónicos de pago, de tal suerte que en las operaciones que forman parte del comercio electrónico directo, conforme el cual el pedido, pago, despacho y entrega se realiza por medios electrónicos.

5 Aun cuando existe, desde el año 2014 un Proyecto de Ley de Comercio Electrónico en la Asamblea Nacional de Venezuela, que más que regular la realización de operaciones comerciales electrónicas, apunta hacia el establecimiento de condiciones y requisitos para la realización de las mismas en el ámbito venezolano.

a toda información inteligible en formato electrónico, independientemente de su soporte material, lo cual permite que las operaciones que se realicen en el comercio electrónico sean consideradas plenamente equivalentes e igualmente válidas a las realizadas sobre soporte papel. De igual modo, la norma en cuestión determina la validez jurídica de la firma otorgada por medios electrónicos, lo que a su vez, permite la celebración de contratos por medios electrónicos.

II. Redes sociales

Las redes sociales han ganado un sitio relevante en la sociedad actual, habida cuenta de la posibilidad de interactuar entre las personas que las utilizan, así como la factibilidad de generar espacios de convivencia que permiten socializar, trabajar o hacer negocios de forma colaborativa. Su crecimiento ha sido tal, que se han tornado en principal medio de vinculación e información para muchos individuos en las sociedades contemporáneas. De hecho, para Téllez, J. (2011,3), las redes sociales se pueden conceptualizar, como:

...un espacio de diálogo y coordinación, a través del cual se vinculan personas u organizaciones en función de un objetivo común y sobre la base de normas y valores compartidos. Las redes sociales han permitido generar relaciones de colaboración, poner en común recursos, desarrollar actividades en beneficio de los participantes, ampliar y estrechar vínculos, crear sentido de pertenencia y socializar conocimientos, experiencias y saberes, al establecer relaciones de intercambio y reciprocidad.

Como puede apreciarse, el establecimiento de redes sociales constituye hasta cierto punto una consecuencia de la necesidad del ser humano de vivir en comunidad, del instinto gregario que nos hace pertenecer a una sociedad, y que determina la necesidad de vincularse con otros seres humanos para la interacción y desarrollo de sus actividades cotidianas. Es por ello, que podría decirse que el ser humano, desde que nace ingresa a numerosas redes, que a su vez se integran en redes de redes, que se van tejiendo sin cesar. La primera de ellas es sin duda la familia, que se crea sobre la base de lazos de consanguinidad y afinidad en primer término y luego por factores como la vecindad, amistad, compañerismo, intereses comunes. Posteriormente esas redes se integran entre sí en los diversos niveles de organización (condominios, consejos comunales, comunidades, organizaciones, asociaciones, clubes deportivos o sociales, etc.). Esta integración y pertenencia a diversas redes representa un elemento que permite su desarrollo humano que lo capacita para cumplir los objetivos que implica el buscar un sitio dentro de la sociedad.

Las redes constituyen entonces formas de interacción social que representan un intercambio constante entre personas, grupos e instituciones, cuya característica esencial es representar un sistema en constante cambio y

que se configura por integrantes que se identifican por tener necesidades y problemas similares, que a su vez se integran en la red para potenciar sus recursos, afrontar los problemas y lograr la resolución de los mismos. Con respecto a la concepción de las redes sociales, Mires, F. (2011), considera que:

En cierto modo, las redes son relaciones que toman la (imaginaria) forma de redes. Ahora, una red, o conjunto de relaciones, no es un hecho determinado a priori, sino que, por ser redes, son tejidas, del mismo modo que para que existan relaciones, estas deben ser contraídas. ¿Pero quién teje las redes? No queda más alternativa que responder: los actores que la constituyen. Por lo tanto, el tejido no es independiente de los tejedores. Quiere decir que en la construcción de una red no hay ningún plan preconcebido, o una lógica que la preceda, sino los actores, al relacionarse, son quienes la van configurando.

Se puede apreciar entonces, que las redes sociales son estructuras que construyen los mismos ciudadanos a lo largo de su existencia, mediante un tejido incesante que depende en parte de condiciones propias del ser humano, pero también del grado de desarrollo que haya conseguido la sociedad, así como de las necesidades propias de cada individuo, quien va construyendo esas estructuras reticulares sin cesar.

III. El desarrollo de las redes sociales en la Sociedad de la Información

Ahora bien, queda claro que el ser humano construye redes para su interacción y desarrollo. No obstante, lo que nos ocupa en este caso es el desarrollo de las redes en la sociedad de la información, en ese tránsito en que nos encontramos hacia la consecución de la sociedad del conocimiento. En este ámbito, estas redes toman un nuevo papel y se reconfiguran en redes informáticas que permiten la interacción entre los seres humanos para el desarrollo de sus actividades relevantes y cotidianas, mediante el uso de plataformas de tecnologías de la información y las comunicaciones. De esta forma nos referimos a las redes sociales como reconfiguración de los mecanismos sociales de intercambio de información y comunicación en la sociedad actual; lo cual se manifiesta en las denominadas Redes Sociales en Internet (en lo sucesivo RSI).

Estas RSI constituyen un espacio creado para intercambiar información, que permiten interactuar con otras personas, en un entorno particularmente abierto, que se construye constantemente sobre la base de los aportes que los integrantes de la propia red realizan. De allí que la participación resulta un elemento esencial para la configuración y crecimiento de las redes. No obstante, también debemos considerar que estas redes sociales representan en primer término un sistema, una plataforma que permite a terceros generar contenidos o bien crear aplicaciones, integrándose en un entorno colaborativo y de intercambio.

Las RSI, son entonces manifestaciones de la existencia de la Sociedad en Red de la que nos habla Castells, M. (2010,18) y que concibe como: “...*la sociedad que yo analizo como una sociedad cuya estructura social está construida en torno a redes de información a partir de la tecnología de información microelectrónica estructurada en Internet*”. Estas estructuras, sin duda constituyen redes reales, que existen y cumplen una función social, aunque se localicen en el ciberespacio y existan redes sociales paralelas en el mundo analógico. Las redes sociales online son el reflejo de una sociedad imbricada en los fenómenos de la conectividad propio de las nuevas tecnologías de la información y las comunicaciones, con los aspectos altamente positivos y negativos que dicha realidad representa, como son por ejemplo el incremento de la participación, mayor posibilidad de comunicación, caudal casi infinito de información y posibilidad de unir a las personas independientemente de las fronteras geográficas y políticas, pero también presentan problemas derivados de la preservación de la privacidad del individuo, la posibilidad de comisión de delitos por vías electrónicas y la falta de confianza en la veracidad de las informaciones.

En cuanto a la relación que existe entre la sociedad de la información y el desarrollo de las redes sociales como manifestación de ese tránsito hacia la “Sociedad en Red”, propugnada por este autor, Castells, M. (2010, 13), opina que:

...más que ver la emergencia de una nueva sociedad, totalmente on line, lo que vemos es la apropiación de Internet por redes sociales, por formas de organización del trabajo, por tareas, al mismo tiempo que muchos lazos débiles, que serían demasiado complicados de mantener off line, se pueden establecer on line. Por ejemplo, uno de los elementos más interesantes en esto es el desarrollo de organizaciones de interayuda entre las personas mayores: el *Seniornet* en Estados Unidos es una de las redes más populares de información, de ayuda, de solidaridad, de reforzamiento de una vivencia compartida, etc. O las redes de información religiosa y de compartir valores religiosos. O las redes de movilización social.

De modo que si bien, no cabe duda de que el surgimiento de las redes sociales en Internet son consecuencia clara del establecimiento de la reconfiguración de la sociedad como consecuencia del advenimiento de la revolución tecnológica, y particularmente de la masificación del uso de Internet, no cabe duda que constituyen una suerte de trasposición al ámbito digital de las redes sociales que caracterizan a las sociedades humanas contemporáneas. Ahora si bien existe cierta ‘tensión’ entre los conceptos de redes sociales, en el sentido de las redes del mundo analógico y las redes sociales virtuales o redes en Internet, no cabe duda de que dichos conceptos no son tampoco antagónicos.

Fundamentalmente, las RSI, se constituyen como una plataforma establecida para el intercambio de información, elemento fundamental para las relaciones

económicas y sociales dentro de la sociedad tecnificada, por cuanto el control sobre la información implica control y poder. Sin embargo, uno de los mayores problemas a la hora de analizar las redes sociales, al igual que con otros fenómenos sociales y culturales generados por la aparición y desarrollo de tecnología, es que se encuentra en plena evolución y que cuando se quiere estudiar el fenómeno ya ha cambiado.

Algunas personas y autores estiman, quizá deslumbrados por el lustre de la explosiva expansión de las RSI que favorecen o hacen más próximas las relaciones entre los seres humanos. Otros por el contrario, estiman que la excesiva exposición a las redes sociales produce aislamiento e incomunicación, y que se sustituyen las relaciones interpersonales, por relaciones virtuales, frías y distantes. No obstante, siguiendo a Castells, M., por el contrario, se considera que las redes sociales sólo hace que se fortalezcan los lazos débiles que se establecen entre los miembros, sin que puedan sustituirse los lazos fuertes (familiares, de amistad, de vinculación laboral, de pertenencia a determinada organización, partido o asociación), que sí se pueden favorecer por el uso de tales tecnologías. Díaz Gandasegui, V. (2011), estima que:

...lo que ocurre es que Internet es apta para desarrollar lazos débiles, para crear lazos débiles, pero no es apta para crear lazos fuertes, como media, y es excelente para continuar y reforzar los lazos fuertes que existen a partir de relación física. En fin, en esto, que parece también bastante lógico, lo que me importa es que viene avalado empíricamente por la síntesis de los estudios que se han desarrollado. En este sentido, la tendencia que se está desarrollando es hacia la disminución de la sociabilidad de base comunitaria física tradicional.

Este tipo de redes sociales constituyen entonces, sitios electrónicos personalizables dedicados a la convivencia entre personas de cualquier parte del mundo. Sus posibilidades son inmensas, ya que cada compañía que desarrolla estas páginas e imprime capacidades distintas y particularizadas para que los usuarios las agreguen y utilicen. De allí que no cabe duda de que las RSI, han traído consigo un impacto social profundo que se pone de manifiesto de forma evidente.

Esta importancia y rápido crecimiento de las redes sociales, así como el explosivo crecimiento del número de usuarios, no es lo único que determina el interés mundial en las redes sociales⁶, sino que factores como su utilización en

6 Este interés mundial por la incidencia que las RSI están teniendo en los más diversos aspectos de la vida del hombre, quedan en evidencia, por ejemplo en el "Dictamen del Comité Económico y Social Europeo sobre el tema "Repercusión de las redes sociales de comunicación e interacción en el ciudadano/consumidor"", que estableció entre otras cosas resaltantes que: *"El CESE reconoce la importancia cultural, política y social de las redes sociales de comunicación en Internet (RSC) como instrumento de comunicación e interacción entre las personas, en el marco del ejercicio del derecho fundamental a la libertad de expresión. Al mismo tiempo, el CESE toma nota del interés económico asociado al desarrollo de las RSC, en concreto su potencial para*

diferentes ámbitos como por ejemplo en las campañas políticas⁷, para promover movimientos sociales⁸, como elemento para la vinculación ciudadana, para la obtención de información, para el establecimiento de comunicación próxima entre personas distantes, para expresar gustos e intereses, y sobre todo para la generación e intercambio de contenidos entre las personas integrantes o usuarias de dichas redes sociales.

Dentro de los atractivos que las personas, particularmente, los más jóvenes encuentran en las RSI, y que han determinado en parte el éxito que han obtenido, se encuentran, según Parra Castrillón, E. (2010,194): “*Aspectos como la presencia transcultural o la omnipresencia hacen que las redessociales se comprometan como nodos productores y consumidores de información*”. Esto ha determinado parte de su éxito, en virtud de la posibilidad de comunicar a personas distantes, vincularlas conforme sus intereses, gustos y preferencias, así como la posibilidad de compartir contenidos multimedia, imágenes, video, etc., que la convierten en herramientas increíblemente poderosas para la vinculación humana. Estas transformaciones en la forma de comunicarnos, se ponen en evidencia, según Díaz Gandasegui, V. (2010, 2), en el hecho de que: “*Las redes sociales se convierten en paradigma del hipertexto, en el que la palabra escrita, la imagen y el material audiovisual consiguen mantener a sus usuarios informados y entretenidos, fusionando así a los medios de comunicación masivos y personales, de entretenimiento y prácticos*”. En consecuencia, los integrantes de las redes sociales, encuentran en ellas, un espacio de que les permiten concentrarse, compartir y vincularse en virtud de sus intereses y gustos, así como crear y compartir contenidos, y lo más importante, determina una especial segmentación y personal vinculación de las personas conforme sus particularidades.

La importancia de las RSI, no sólo debe verse desde el punto de vista del indudable impacto que han tenido desde el punto de vista social, ni tampoco por el evidente éxito que ha tenido en cuanto a la masificación que se ha producido

actividades de comunicación comercial y de mercadotecnia de diversos tipos”. Unión Europea (2010) **Dictamen 2010/C 128/12**. Publicado en el *Diario Oficial de la Unión Europea* (18.5.2010), disponible en fuente electrónica, en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:128:0069:0073:ES:PDF>

⁷ La campaña para la elección presidencial de Barack Obama en los Estados Unidos empleó intensivamente las redes sociales como Twitter y Facebook, no sólo para hacer promoción y propaganda, sino además, para recaudar fondos, y para establecer vínculos con los electores.

⁸ Ambientalistas, de protestas sociales y ciudadanas. Este elemento se puso particularmente de manifiesto con las protestas en el año 2010 en Irán, tras las elecciones en ese país, así como los movimientos sociales y políticos en países como Túnez y Egipto, durante el año 2011 (por sólo citar dos casos), que determinaron cambios en el sistema político de dichos países, a pesar de que son países donde impera la censura y control político sobre los medios de comunicación, lo cual no obsta para que los ciudadanos encontraran en las redes sociales, medios de expresión y difusión de información acerca de la realidad interna y lograran utilizarlos como medio para convocar manifestaciones y para dar a conocer los desmanes cometidos por las autoridades.

por el impactante número de usuarios que actualmente supera los 1.000 millones de personas, y la inmensa penetración de estos servicios, así como el hecho de que la mayoría de los usuarios de Internet utilizan las redes sociales⁹. La impronta que las mismas han impreso debe además ser ponderada, por cuanto según Redondo, J. (2010):

Estas cifras y esta inmensa velocidad de implantación no son más que la punta del iceberg de un movimiento cualitativo en los medios de mucho mayor calado: las personas son ahora las que crean los contenidos; los medios tradicionales y la publicidad convencional difuminan su influencia, y nos hallamos, posiblemente, ante la quinta y más importante revolución de los medios de comunicación de la historia.

En efecto, la trascendencia que desde el punto de vista de los cambios en cuanto a la forma de vincularse los seres humanos (que incluyen claro está, la posibilidad de generar y servir de plataforma para la realización de negocios) es innegable, al punto de que se estima que entra dentro de la categoría de las revoluciones, las cuales según Esparza, D. (2010), sólo comprenden cuatro episodios en el mundo de la comunicación en los últimos 500 años, que serían en primer lugar la invención de la imprenta y las innovaciones que permitieron el desarrollo del libro (Siglo XV); en segundo lugar, la invención del telégrafo, hace cerca de 200 años, como medio radioeléctrico de comunicación que inicia el ámbito de las comunicaciones, precursor de las comunicaciones diacrónicas propias del uso del teléfono, en tiempo real y por medio de la voz. El tercer hito está representado por la aparición de los medios de grabación (hace unos 150 años), inicialmente por medio de la fotografía y posteriormente mediante los fotogramas en movimiento que dio paso a la cinematografía. La cuarta Revolución estaría representada por los cambios desde hace un siglo, determinados por la explotación del espectro electromagnético, seguido de la televisión. Cada uno de estos hitos en la comunicación humana representaron además importantísimos cambios sociales, en cuanto a la forma de comunicarse los seres humanos, de vincularse entre sí, aparte del modelaje social consecencial a dicha realidad.

⁹ Un informe basado en cifras de Nielsen para diciembre de 2009. Conforme dicho estudio, los usuarios estuvieron conectados para el año 2009 una media de 5h 35min en sitios de redes sociales, en contra de las 3h 4min que estuvieron durante el año anterior (fundamentado en los hábitos de navegación web en EEUU, Reino Unido, Australia, Brasil, Japón, Suiza, Alemania, Francia, España e Italia). Por su parte, en América Latina, por ejemplo, la penetración del uso de las Redes Sociales, pasó de un 78% para el año 2008, a un 87,2 %, para el año 2009 (en el mismo período, en Venezuela pasó de un 69,1 % a un 77,1 %), conforme un estudio de ComScoreWorldMetrix.

IV. Impacto de las redes sociales en el comercio electrónico en Internet. El denominado *Social Commerce*

El crecimiento exponencial en el número de usuarios de las RSI, aunado a factores esenciales tales como el desarrollo de redes informáticas cada vez más poderosas en cuanto a capacidad de transmisión y almacenamiento de la información, la convergencia de los servicios de comunicaciones que permiten integrar gran variedad de recursos para los usuarios han generado un importante interés en cuanto a la posibilidad de su utilización con fines de naturaleza comercial, mediante la integración de negocios de alta rentabilidad y un alto grado de especialización, ha dado paso a una nueva e importante manifestación del comercio electrónico, como es el denominado '*Social Commerce*' o comercio electrónico mediante las redes sociales, que determina uno de los nuevos derroteros de la actividad comercial electrónica.

Usualmente las RSI, en sus inicios comenzaron únicamente como elementos para el contacto entre las personas por medios electrónicos, así como para el intercambio de información y generación de contenidos que, no obstante, no parecían tener muy definidos sus modelos de negocios (los servicios en la mayor parte de las RSI son gratuitos), que fueron generándose sobre la base de las posibilidades de su aplicación y generación sobre la base de dos factores claves, la propensión hacia las actividades de publicidad y mercadeo, y la susceptibilidad para generación de aplicaciones de comercio electrónico directo e indirecto. Las RSI por lo demás, permiten a los usuarios la utilización de herramientas y aplicaciones que facilitan la vinculación entre los participantes en las mismas, tales como blogs, chats, podcast, RSS, wikis, etc., los cuales propenden por una parte hacia la promoción de la vinculación socio-afectiva, así como la elevación de la eficiencia en actividades de trabajo como la gestión del conocimiento, resolución de problemas, innovación y generación de trabajo colaborativo entre los usuarios.

El crecimiento del uso de las RSI ha impactado positivamente el comercio electrónico en Internet, especialmente para los modelos de negocios B2C ('*Business to Consumer*' o comercio electrónico entre empresa y consumidor), lo cual puede apreciarse desde el punto de vista de las ventajas que representa para los consumidores y para las empresas. Desde la perspectiva de los consumidores, el uso de las RSI se puede apreciar (especialmente para los usuarios más jóvenes), facilita el compartir opiniones y recomendaciones respecto de los productos, empresas, marcas, productos y proveedores en Internet. Esto ha modificado los hábitos de compra de los consumidores que suelen, antes de tomar una decisión de compra, consultar las opiniones y experiencias de otros consumidores, cuestión que se facilita sensiblemente mediante el uso de las RSI, toda vez que si bien es cierto que las principales páginas de comercio electrónico contienen aplicaciones que permiten intercambiar y valorar a los proveedores, la información proveniente de las

redes es ponderada como más pertinente, mediante sistemas más interactivos, fluidos, informales y confiables.

Desde el punto de vista de los empresarios que desarrollan sus actividades de comercio electrónico mediante las redes sociales; éstas presentan toda una serie de beneficios, dentro de las cuales se destacan las siguientes: 1) facilitan la implementación de estrategias innovadoras de 'marketing viral' (boca a oído), las cuales permiten contar con una mayor segmentación y especialización, sobre nichos de mercado específicos, lo cual optimiza a su vez, la utilización de los recursos de mercadeo¹⁰. No sólo constituye un canal extremadamente barato, sino que además es un canal particularmente confiable; 2) se constituyen en una fuente de información confiable, que desarrolla la retroalimentación similar a un 'focusgroup', respecto del diseño de los productos y servicios, sus funcionalidades, campañas publicitarias, etc., en el sentido que permiten una valoración sobre los productos y servicios de la empresa, aparte de conferir una valoración neutral, más confiable para el consumidor; 3) permiten incrementar el tráfico hacia un determinado sitio web, con la particularidad de que permiten optimizar el mismo, en virtud de su segmentación, garantizando un tráfico cualificado (la información se mueve directamente entre personas focalizadas que se mueven por intereses comunes); 4) permiten generar valor en las relaciones con los clientes a través políticas de fidelización de los clientes mediante prácticas de mercadeo destinadas a establecer vínculos más próximos con la clientela (premios, descuentos, promociones, sensibilización); 5) resultan un elemento de particular utilidad para potenciar las actividades de servicio al cliente, puesto que permiten interactuar con los clientes y consumidores para atender sus necesidades, inquietudes y reclamos sobre los productos y servicios que se venden o prestan.

Las RSI pueden servir de plataforma operativa para el comercio electrónico¹¹. En la actualidad las redes sociales permiten a los usuarios comunicarse, chatear, postear sus opiniones, jugar, compartir fotos y videos (generar contenidos); pero la importancia cardinal que estas plataformas pueden tener para las empresas desde el punto de vista del comercio electrónico radica en las oportunidades que pueden representar para la venta de contenidos relacionados con el entretenimiento (juegos, imágenes, videos, contenidos musicales en

¹⁰ Existen plataformas virtuales que auxilian a los empresarios virtuales para optimizar el contenido de sus páginas web, con la finalidad de hacerlas más atractivas y efectivas, desde el punto de vista del mercadeo, tales como 'AdWords' y para obtener ingresos por los linkeos efectivos que se realicen, mediante la plataforma 'AdSense', ambas de Google.

¹¹ Si por ejemplo, desde un sitio comercial electrónico se utiliza la plataforma 'Facebook Connect', esto le permitiría acceder a las cuentas en la red social Facebook, sin salir de la tienda virtual. De modo que cuando se inicia la sesión (log in), el sitio comercial tendría la información del perfil del usuario, la cual podría ser utilizada para remitirle información comercial personalizada, lo cual permite establecerla conforme sus gustos, lo cual a su vez, podría ser visto por la red de amigos del usuario particular. Otras redes sociales como 'MySpace' y 'Twitter', tienen funcionalidades similares.

formatos digitales), así como materiales que permitan promocionar productos o servicios, o bien encontrar nuevos clientes, y sobre todo para fomentar las compras ‘*on line*’, mediante tiendas virtuales y promover actividades de comercio electrónico directo o indirecto.

Queda claro entonces que resulta extremadamente útil y señala uno de los derroteros del comercio electrónico hacia el futuro inmediato, la utilización de las RSI, por cuanto representa una prioridad indeclinable aprovechar las herramientas que interactúan en la actualidad en el universo de la denominada ‘web 2.0’¹², lo cual impone un esfuerzo de adaptación, así como la constitución de los marcos conceptuales y legales que permitan determinar las principales normas que puedan regular los diversos planos de relaciones que se pueden establecer.

En tal sentido se debe tomar en consideración que respecto a la validez de las operaciones que se efectúen en el ámbito de estas operaciones comerciales electrónicas, se aplicarán las normas de la Ley sobre Mensajes de Datos y Firmas Electrónicas, que regula la validez y eficacia de las operaciones comerciales realizadas por medios electrónicos, la cual complementa la normativa civil y mercantil igualmente vigente¹³. Cobran por lo demás, particular relevancia las “condiciones y términos legales”, que deben establecerse, tanto dentro de las páginas web que realizan tradicionalmente las operaciones comerciales electrónicas (tiendas virtuales, páginas temáticas, centros comerciales virtuales, etc.), como dentro de la regulación específica de las propias RSI, que deben tomar en consideración, por una parte, factores como la privacidad de la información de carácter comercial y de carácter personal que cursará por las redes; la protección de la propiedad intelectual de los contenidos (propiedad industrial y derechos de autor); así como el cumplimiento de la normativa protectora de los derechos de los consumidores y usuarios, y los mecanismos para la resolución de los conflictos que se puedan producir. De igual modo, se debe disciplinar por vía contractual las relaciones entre la página web en particular (tienda virtual, por ejemplo), con la red social de que se trate, con la finalidad de regular las relaciones comerciales de vínculos (*web linking agreements*), de tal suerte que se fijen con claridad las diversas estipulaciones contractuales que surjan a consecuencia del tráfico que curse entre dichos actores comerciales electrónicos, así como los demás asuntos que se presenten

¹² Este término está comúnmente asociado con las aplicaciones web que facilitan el compartir información, la interoperabilidad, el diseño centrado en el usuario y la colaboración en la World Wide Web, que son propios de la tecnología actual, y su orientación hacia la prestación de servicios en la web.

¹³ De igual modo, por tratarse de relaciones que tocarán las relaciones de las empresas con los consumidores, se deberá cumplir las disposiciones de la Ley Orgánica de Precios Justos, que a diferencia de la derogada Ley de Defensa de las Personas en el Acceso a los Bienes y Servicios, no tiene un capítulo dedicado a las operaciones de Comercio Electrónico (existe un Proyecto de Ley de Comercio Electrónico actualmente en discusión en la Asamblea Nacional).

respecto de uso de marcas, tecnología y software aplicables, propiedad intelectual de los contenidos cursados, etc.

V. Conclusiones

El advenimiento de la Sociedad de la Información, ha traído profundas transformaciones sociales que han impactado diversos aspectos de la vida humana. En el ámbito mercantil, el comercio electrónico comprende la realización de actividades comerciales en sentido amplio mediante la utilización de las TIC. El comercio electrónico en Internet, ha generado transformaciones profundas en el ámbito negocial, por cuanto se representa una desmaterialización (más bien electrificación) del soporte de los contratos que lo comprenden, así como la masificación de la contratación por medios informáticos.

Las redes sociales surgen como producto de las múltiples relaciones que se establecen entre los seres humanos, creando espacios de colaboración y apoyo. La trasposición de esta realidad en el ámbito de la Sociedad de la Información, ha llevado a desarrollar las denominadas Redes Sociales en Internet, que se han establecido sobre la premisa de las múltiples relaciones de los integrantes de las mismas, y las cuales constituyen ámbitos de intercambio de información que permiten interactuar con otras personas en un entorno abierto que se construye de forma colaborativa, mediante los aportes de los miembros de las mismas, y en las cuales se intercambian opiniones, deseos, contenidos de diversa índole. Estas RSI tienen una gran importancia desde el punto de vista del comercio electrónico, por cuanto por una parte constituyen espacios en los cuales las empresas pueden vincularse efectivamente con sus clientes, así como conocer sus deseos, intereses y opiniones respecto de los productos y servicios que ofrecen, así como optimizar las relaciones de servicio al cliente, y del denominado ‘mercadeo viral’; contando con la ventaja de una segmentación y personalización de los servicios adaptándolos a las necesidades específicas del cliente o usuario. Aparte de lo anterior, las RSI, poseen un enorme potencial para la vinculación de espacios comerciales electrónicos donde realizar operaciones de comercio electrónico directo o indirecto, que permitan vender contenidos digitales o bien productos físicos mediante la vinculación de las páginas de comercio electrónico (tiendas virtuales, portales, centros comerciales virtuales, etc.), con las RSI, con la finalidad de prestar servicios especializados y especialmente adaptados a las particulares necesidades de los consumidores.

Queda claro pues, que la vinculación de las RSI para actividades de comercio electrónico abre un amplio panorama en pleno desarrollo, que vislumbra un futuro amplio en oportunidades y que aunado a otras tendencias vinculadas con la convergencia tecnológica de los medios de comunicación, representada entre otras por las posibilidades de integrar estas redes sociales y otras manifestaciones de comercio electrónico con la telefonía móvil, con la computación móvil, el comercio mediante las ‘tablets’ y pc-tv o televisión con acceso a Internet;

representarán nuevos horizontes fértiles para el desarrollo de nuevas oportunidades de desarrollo en el ámbito comercial.

CONFERENCIAS

XIX Congreso Iberoamericano de Derecho e Informática.
Federación Iberoamericana de Asociaciones de Derecho e Informática.
Medellín, agosto 2015

Protección de datos y servicios públicos y privados de *Cloud Computing* en España y Europa*

Lorenzo Cotino Hueso**

SUMARIO: 1. La cara y la cruz de los servicios de la nube. 1.1. La cara: aproximación a los servicios de la nube, una de las mayores revoluciones tecnológicas de los últimos tiempos y su importancia económica y social. 1.2. La cruz: los riesgos de seguridad y privacidad 2. Los sujetos y la regulación actual y futura de la protección de datos en la nube 2.1. Quién es quién en la nube a los efectos de la normativa de protección de datos. 2.2. Las cuestiones clave de protección de datos y las insuficiencias de la regulación actual. 2.3. La nube en el esperado Reglamento europeo de protección de datos. Hacia una regulación nebulosa. 3. El tratamiento jurídico de algunas cuestiones clave que plantea la nube en materia de protección de datos. 3.1. La diligencia y responsabilidad legales del usuario de la nube, transparencia de la empresa de *cloud*. 3.2. Un elemento clave para el cliente y la empresa de *cloud*: el conjunto contractual y la subcontratación. 3.3. La cobertura legal de las transferencias internacionales de las empresas de *cloud* contratadas y subcontratadas: cláusulas contractuales tipo y normas corporativas vinculantes 4. Algunas exigencias del uso de la nube por las Administraciones

Aceptado por el Comité Académico para ser presentado en el XIX Congreso Iberoamericano de Derecho e Informática celebrado en Medellín, agosto 2015. Aprobado por la Junta Directiva de FIADI para ser publicado en la *Revista Derecho y Tecnología*, el 13 de octubre de 2015.

* El presente estudio se realiza merced a ayuda para estancia en la empresa de servicios en la nube Occentus Network (AEST/2015/023). Asimismo, en el marco del Proyecto “Régimen jurídico constitucional del Gobierno 2.0-Open government. Participación y transparencia electrónicas y uso de las redes sociales por los poderes públicos” (DER2012-37844) y “El avance del Gobierno Abierto. Régimen jurídico constitucional de la implantación de políticas de transparencia, acceso a la información, datos abiertos, colaboración y participación especialmente a través de las TIC y del gobierno electrónico” (DER2015-65810-P), del Ministerio de Economía español y producto de investigación en el marco del proyecto “Gobierno abierto: participación, transparencia, datos abiertos, colaboración y gobierno en línea. Problemas y barreras jurídicas al desarrollo y gestión de la información pública” financiado por la Corporación Universitaria de Sabaneta - Unisabaneta-, línea de “Derecho Público”, Grupo de Investigación Pólemos, registro Colciencias COL0111291

** (www.cotino.es), Profesor titular, Catedrático de Derecho Constitucional de la Universidad de Valencia, Coordinador de la Red de especialistas en Derecho de las Nuevas Tecnologías de la Información y Comunicación (TICs) www.derechotics.com. e-mail: Lorenzo.Cotino@uv.es

Resumen

El estudio describe los servicios de la nube y sus perspectivas, así como los riesgos y problemas más importantes, en particular respecto de la seguridad y la privacidad. Se señalan algunas deficiencias de la vieja y superada regulación nacional y europea de protección de datos aplicable a la nube, corregidas en alguna medida por la acción de instituciones de protección de datos en los últimos años. Se observa también el proyecto reglamento europeo de protección de datos y se expone la tendencia a reforzar las obligaciones del prestador de servicios de nube (normalmente una gran corporación), que es “encargado”, para que el cliente de la nube, que es el “responsable”, pueda cumplir sus obligaciones. Igualmente se detallan exigencias respecto del conjunto contractual y la subcontratación de servicios y la necesidad de autorización de las transferencias internacionales de datos con terceros países (cláusulas contractuales tipo y *Binding Corporate Rules*). Para concluir se hace una breve aproximación a algunas exigencias jurídicas de los servicios de la nube cuando son prestados a las Administraciones públicas en España.

Abstract

The study describes the cloud services and its features, as well as the most important risks and challenges, particularly regarding security and privacy. Some shortcomings of the old and overcome national and European regulation applicable to the cloud, corrected in some way by the action of data protection institutions in recent years, are also indicated. European regulations proposed regarding data protection is also observed, and the trend to reinforce the obligations of the cloud service provider (usually a corporation), which is “the processor”, for the customer of the cloud, which is the “controller”, can meet their obligations. Detailed requirements regarding the contractual set and outsourcing of services, and the need for authorization of international transfers of data with third countries (contractual clauses and *Binding Corporate Rules*) are also explained. The study ends with a brief reference to some legal requirements of cloud services when they are provided to the public authorities in Spain.

1. La cara y la cruz de los servicios de la nube

Que la nube es un futuro ineludible que es ya presente, no hay duda. Que su uso genera toda una serie de retos y cuestiones jurídicas, tampoco. La atención científica y académica de la nube se ha centrado, como es normal, en los aspectos tecnológicos. Sin embargo, pese a ser esencial el enfoque jurídico para el desarrollo del *cloud*, no es mucha la literatura jurídica española sobre la materia,

aunque con estudios muy destacables¹, como en México². Es algo mayor la atención en el ámbito europeo y anglosajón³, o de EEUU⁴. Pese a que son diversas las cuestiones jurídicas que suscita la nube, por razones de espacio, el presente estudio focaliza el análisis en lo más vinculado a seguridad y protección de datos y algunas cuestiones vinculadas al uso de servicios de *cloud* por las Administraciones. Ello sin perjuicio las crecientes facultades –y dificultades– de investigación de la nube y los deberes de colaboración de las empresas⁵.

1.1. La cara: aproximación a los servicios de la nube, una de las mayores revoluciones tecnológicas de los últimos tiempos y a su importancia económica y social

El desarrollo de los sistemas informáticos ha evolucionado, se puede decir que de manera natural⁶, hacia la nube, el *cloud computing*. En un lustro, buena parte de la información mundial estará en la nube, ya se trate de información pública o de sujetos privados, ya se trate de información privada o reservada o información de libre acceso. Pese a algunos escépticos sobre su importancia⁷ Estamos ante una de las mayores revoluciones tecnológicas de los últimos

¹ En español, sin perjuicio de las obras que se citan más adelante, una pionera atención los trabajos de Leenes y Miralles en *IDP. Revista de Internet, Derecho y Política*. N.º 11. UOC. Especialmente destaca la monografía MARTÍNEZ i MARTÍNEZ, Ricard (2013). De especial valor son los documentos institucionales de la AEPD (2013) y del GRUPO DEL ARTÍCULO 29 (2012)

² En México, una descripción completa del tema en TÉLLEZ VALDÉS (2014).

³ Hay estudios iniciales, como VAN GYSEGHEM (2010) En cualquier caso, en Europa destacan sin duda alguna los distintos estudios jurídicos realizados en los últimos años y publicados desde el Queen Mary School of Law Legal Studies en razón del cloudlegalproject.org con apoyo de Microsoft. Y desde 2014 se insituye el Microsoft Cloud Computing Centre (www.mccrc.eu/) del Queen Mary con la U. de Cambridge. Se puede acceder a casi todas las publicaciones jurídicas tanto en SSRN como en cloudlegalproject.org, aunque no a la monografía MILLARD de (2013).

⁴ Sobre el régimen jurídico de la nube en Estados Unidos SOLOVE (2014). Y sobre disparidades y posibles choques entre normativa americana y europea de protección de datos para la nube, SCHWARTZ, (2013).

⁵ Sobre el tema, mi ponencia “Derechos fundamentales e investigación criminal de la información que está en la *nube*”, en el Congreso Internacional “Seguridad en libertad”, Universidad de Konstanz, 15 – 21 de junio de 2015. Al respecto, hay que tener especialmente en cuenta el Proyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal aprobado el 13 de marzo de 2015, que regula el “registro de dispositivos de almacenamiento masivo de información”. Especialmente hay que tener en cuenta el artículo 588 septies a) y el esencial deber de colaboración de los prestadores regulado en los artículos 588 ter e) 588 septies b) y 588 octies. Al tiempo hay que tener especialmente en cuenta las mayores barreras a la investigación de la nube que imponen las empresas a través de la encriptación como reacción al caso *Snowden*.

⁶ Así, GRUPO DEL ARTÍCULO 29, *Dictamen 05/2012*, pág. 5

⁷ Así, LARRY ELLISON, CEO de Oracle en 2009 diría que “Las nubes son vapor de agua. [...] Esto no es más que un ordenador conectado a una red” en Venturebeat, acceso en <http://goo.gl/pCXfj2> Y un importante analista de Gartner diría el 8.10.2010 que la nube está en la cima de las “expectativas infladas”. Así, en “Gartner Hype Cycle 2010: Cloud Computing at the Peak of Inflated Expectations”, en *Readwrite.com*, <http://goo.gl/bkwr9T>

tiempos. Y, como cualquier proceso evolutivo, el avance de la computación en nube como paradigma tecnológico mundial representa un desafío en todos los órdenes.

La nube supone⁸ una nueva forma de prestación de los servicios de tratamiento de la información que permite al usuario no hacer inversiones de infraestructura, sino que utiliza la que pone a su disposición el prestador del servicio. Como avanzara Carr en 2005, para las corporaciones las TIC dejan de ser una propiedad, para pasar a ser un servicio que adquieren como usuarios⁹. El usuario dispone virtualmente de sus bases de datos, correo electrónico, nóminas o gestión de recursos humanos, etc. a través de Internet, mientras que físicamente dicha información puede estar deslocalizada, en cualquier lugar del mundo. El mismo prestador de servicios de nube puede a su vez deslocalizar dicha información, compartiendo o subcontratando servicios en otra escala y de forma dinámica, esto es, según las necesidades. De este modo, se proporciona un servicio a demanda. Uno de los caracteres básicos del *cloud* es la optimización de la asignación y coste de los recursos a las necesidades, lo mismo que la elasticidad de los servicios de la nube y su adaptación a las necesidades específicas. El usuario externaliza sus servicios y no tiene que gestionar la infraestructura, el sistema informático sino que lo hace el prestador de servicios de nube. Al tiempo de reducir costes (locales, equipos y conocimientos informáticos, personal especializado, etc.), la eficacia del servicio está más garantizada así como la seguridad, que quedan en manos de proveedores especializados. Los prestadores, por lo general, son grandes proveedores con infraestructuras complejas, si bien también hay lugar para prestadores intermedios con servicios añadidos y personalizados.

Los servicios de la nube pueden ser variados según diversos criterios. Interesa en este sentido recordar lo que implica la nube privada, pública o híbrida. Cuando se trata de nube privada, hay una infraestructura informática dedicada exclusivamente e individualmente para su usuario. La información queda bajo el control de dicho individuo que es el responsable. La infraestructura puede ser del mismo usuario o puede tratarse de un servicio que le prestan de manera exclusiva, de modo que no participan terceros en esta relación ni se comparten los servicios de información. Es como un centro de datos convencional a distancia, si bien con la referida característica de la optimización de los recursos a las necesidades. Por el contrario, la nube pública implica que la infraestructura es del prestador de servicios. El prestador presta sus servicios de forma abierta a los distintos usuarios, entidades heterogéneas, que comparten dicha infraestructura a través de internet. Los usuarios no tienen otra relación que la

⁸ Para una aproximación general y en especial las definiciones, se sigue: MELL (2009); GRUPO DEL ARTÍCULO 29, "Dictamen 05/2012... cit. págs. 29 y ss.; ENISA (2009); AGPD (2013 a) AGPD (2013 b)

⁹ CARR (2005) pág. 68.

de ser usuarios del servicio. El usuario transfiere en buena medida el control sobre sus datos. Hay soluciones intermedias, así, se considera nube híbrida cuando determinados servicios se ofrecen de forma pública y otros de forma privada. También se habla de “nubes comunitarias” cuando la infraestructura informática es compartida por varias organizaciones en beneficio de una comunidad de usuarios específica. Ningún proveedor de nube pública puede garantizar siempre una calidad de servicio (sobre la base de acuerdos de nivel de servicio) capaz de responder a la naturaleza crítica del servicio, por lo que organizaciones grandes o medias siempre necesitarán nube privada. Ahora bien, basarse sólo en una nube privada, aunque puede ser factible y aconsejable desde una perspectiva de seguridad y eficacia, puede no ser viable a largo plazo por razón de los costes.

Cabe también hacer referencia a los tres modelos de servicios que suelen aplicarse a las soluciones en nube, tanto públicas como privadas: Infraestructura de nube como servicio (*IaaS*), Nube de Software como servicio (*SaaS*), y Plataforma como Servicio (*PaaS*).

La infraestructura de nube como servicio (*IaaS*) es como el servicio en bruto de dar almacenamiento y alojamiento masivo en servidores remotos, sustituyendo a los sistemas informáticos de empresa. El usuario ha de tener sus aplicaciones. En la nube de software como servicio (*SaaS*) el usuario cuenta con aplicaciones en la nube como una aplicación de contabilidad, de correo electrónico, un *workflow*, un programa para la gestión documental de su empresa, hojas de cálculo, herramientas de tratamiento de textos, agendas y registros informatizados, calendarios compartidos, etc. Así, el prestador proporciona en línea distintos servicios de aplicaciones y los pone a disposición de los usuarios finales de modo que el usuario ya no necesita contar con ellos en la organización. Una opción intermedia es la plataforma como servicio (*PaaS*), en la que se proporcionan herramientas para construir aplicaciones, como bases de datos o entornos de programación sobre las que el usuario puede desarrollar sus propias soluciones. El usuario desarrolla y aloja aplicaciones que bien destina a su organización o a terceros y, en todo caso, no necesita equipos o programas específicos o adicionales a nivel interno.

Se pueden señalar características esenciales de los servicios en la nube¹⁰:

- Autoservicio a la carta: el usuario se abastece unilateralmente de sus necesidades informáticas sin interacción humana.
- Amplio acceso a la red a través de diversos terminales.
- Posible uso común de recursos, asignados y reasignados dinámicamente según necesidades.

¹⁰ CLOUD SECURITY ALLIANCE (CSA), (2009).

- Rapidez y elasticidad a escala de suministro de capacidades según necesidades, con redimensionamiento inmediato que llevan a que aparezcan como ilimitadas para el usuario que las puede adquirir al momento.
- Deslocalización, por cuanto se cuenta con el servicio a distancia con independencia material de dónde éste se preste.
- Servicio supervisado por el prestador de servicios que controla y optimiza el uso de recursos. El uso de recursos puede seguirse, controlarse y notificarse, lo que aporta transparencia tanto para el proveedor como para el consumidor del servicio utilizado.
- Costes reducidos, convirtiendo gastos de capital (habitualmente inversiones grandes) en gastos de funcionamiento, de servicios, con barreras de entrada reducidas.
- Seguridad, en principio aumenta por la centralización de datos y concentración de las medidas de seguridad, a cargo de proveedores especializados.

La nube implica cambios sociales y económicos muy trascendentes. La empresas, desde la más grande a la más pequeña actúan en mercados abiertos y globales y lo hacen en buena medida utilizando los servicios online descritos. La mayor parte de los usuarios acceden a contenidos y aplicaciones que están o se ejecutan en la nube. El trabajo online y el “Bring Your Own Device” (*BYOD*, “trae tu propio dispositivo”) se está generalizando. Alrededor de un 90% de los empleados (en los países desarrollados) utilizan sus propios dispositivos para el trabajo o acceder a distancia a la información de la empresa, con los peligros y fisuras de seguridad que ello puede generar¹¹. Desde la perspectiva económica y como se recuerda desde Europa¹², el sector de las TIC es directamente responsable del 5 % del PIB europeo, con 660.000 millones de euros. Y más allá de esta cantidad, contribuye especialmente al crecimiento de la productividad general al elevado grado de dinamismo e innovación inherente al sector y a su capacidad para transformar el modo de funcionamiento de otros sectores. Así, implica un 20 % directamente del sector de las TIC y un 30 % de las inversiones en TIC). Un estudio para Microsoft¹³ afirma que el *cloud computing* creará cerca de 14 millones de nuevos empleos en todo el mundo en 2015, de ellos, 134.000 corresponderían a España¹⁴. En nuestro país hay

11 Sobre el tema acaba de aparecer la monografía de PUYOL MONTERO (2015).

12 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Bruselas, 26.8.2010. COM(2010) 245 final/2. Pág. 5

<http://www.agendadigital.gva.es/documents/128745511/128746769/agenda-digital-europeaES.pdf/08065334-7f50-418e-a3ab-87210fc1eb85>

13 GANTZ (2012).

14 Esta afirmación por Microsoft España en <http://www.microsoft.com/spain/prensa/noticia.aspx?inford=/2012/03/n009- cloud-Computing-generara-millones-de-empleos>

algunas agrupaciones sectoriales, vinculadas al ámbito europeo¹⁵. Otros estudios afirman la creación de hasta 800.000 empleos en Europa para el mismo periodo¹⁶. Los beneficios de la nube se estiman en 1,1 billones (europeos) de dólares¹⁷. Ello, y el ya comentado ahorro de costes y el aumento de la productividad que proporciona el *cloud computing*, provocará una importante reinversión por parte de las organizaciones, y por consiguiente, el crecimiento del empleo. Los poderes públicos son conscientes del potencial de la nube y así se aprecia con claridad en los objetivos en las *Agendas* digitales europea¹⁸ y, especialmente, en la española¹⁹. Es más, se tiene en cuenta que una mejora del marco jurídico de protección de datos puede contribuir al desarrollo del sector²⁰.

1.2. La cruz: los riesgos de seguridad y privacidad

Sin perjuicio de las muchas posibles ventajas, también el uso de la nube presenta diferentes inconvenientes generales, a saber: la disponibilidad de las aplicaciones está sujeta a la disponibilidad de acceso a Internet; puede darse un ambiente propicio para el monopolio y el crecimiento exagerado en los servicios; hay un avance continuo en las aplicaciones y servicios lo cual conlleva cierto lastre para el aprendizaje en empresas de orientación no tecnológica; hay riesgos de sobrecarga en los servidores de los proveedores y la centralización de las

15 Así, en España la Agrupación “Cloud Network (http://www.agrupacion_cloud.com/) o Euro Cloud España <http://www.eurocloudspain.org>, miembro de CEIM – CEOE. En el sector de la seguridad en general, cabe tener especialmente en cuenta a la Asociación Española para el Fomento de la Seguridad de la Información *ISMS Forum Spain* (<https://www.ismsforum.es>), con 120 empresas y más de 800 profesionales asociados. También cabe tener en cuenta la *Cloud Security Alliance* (<https://cloudsecurityalliance.org>), con *ISMS* en España tiene la iniciativa *Cloud Security Alliance* España (*CSA-ES*) que reúne a miembros representativos de la industria del *cloud* Computing en España. En este ámbito Se trata de un foro de debate que promueve el uso de buenas prácticas para garantizar la seguridad y privacidad en el entorno del *cloud* Computing y en el marco del cual se difunden estudios como el reciente *ISMS -CSA-ES (2014)*

16 BERGER (2012).

17 GANTZ... *cit.* pág. 2.

18 COMISIÓN EUROPEA, *Una Agenda Digital para Europa*. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Bruselas, 26.8.2010. COM(2010) 245 final/2, acceso en español en <http://www.agendadigital.gva.es/documents/128745511/128746769/agenda-digital-europeaES.pdf/08065334-7f50-418e-a3ab-87210fc1eb85>

19 *Agenda Digital para España*, Ministerio de Industria, Energía y Turismo y por el Ministerio de Hacienda y Administraciones Públicas, Febrero de 2013. www.agendadigital.gob.es

Entre los seis grandes objetivos y en el marco del desarrollo de la economía digital (el 2, pág. 5) y se propone “potenciar el desarrollo y uso del *cloud* computing” (pág. 6). Asimismo, entre las propuestas para “Potenciar las industrias de futuro” (apdo. 2.6, págs. 28 y ss.) se considera la nube como “oportunidad industrial” y se formulan diversas propuestas concretas.

20 Así, *ibídem*, en concreto el punto 6, apdo. 4.3, pág. 42.

aplicaciones y el almacenamiento de los datos origina una interdependencia de los proveedores de servicios²¹.

No obstante, y por lo que aquí más interesa, un riesgo esencial es la seguridad y la privacidad. Es cierto que –como se dijo– los servicios de la nube mejoran la seguridad y privacidad: la información no queda diluida en los numerosos usuarios responsables de ficheros no familiarizados con lo informático, la seguridad y la legalidad, sino concentrada en manos de especialistas en seguridad con grandes equipos, formación e infraestructura. No obstante, la información del usuario ya no queda localizada en la organización y bajo su control, sino que queda más o menos expuesta a terceros, ya por su acceso a las infraestructuras de los prestadores de servicios de nube, ya por los riesgos de seguridad en las continuas conexiones entre el usuario y el prestador.

Los informes mundiales sobre seguridad en la nube²² han descrito los riesgos más importantes. Las preocupaciones que derivan de estos informes se centran en aspectos de la gestión de los datos, fundamentalmente en la propiedad de los mismos y la forma de operarlos y tratarlos por parte de los proveedores, así como en la identificación y control de acceso a los recursos. El grupo del artículo 29, por ejemplo, divide los riesgos en la falta de control de los datos y la falta de transparencia: por cuanto a la falta de control, dice que se manifiesta en falta de disponibilidad, de portabilidad, de integridad, de confidencialidad, la complejidad y la dinámica de la cadena de subcontratación. Falta de aislamiento de datos de los distintos usuarios, falta de transparencia, no ser conscientes de las amenazas y riesgos, la existencia de múltiples encargados del tratamiento y subcontratistas y, por último, las diferentes zonas geográficas, fuera o dentro de la Unión Europea²³.

La *Cloud Security Alliance* (CSA) señala como amenazas el abuso y mal uso del *cloud computing* (especialmente en servicios *IaaS* y *PaaS* – infraestructura y plataforma como servicio); el uso de interfaces y *API* (*Application Programming Interface*) poco seguros, que son los que sirven para que el usuario controle e interactúe con los recursos contratados. Recuerda la CSA que la autenticación, acceso, cifrado de datos, etc. del usuario se realiza a través de estas herramientas y pueden generar problemas de seguridad tanto intencionados como forma accidental.

En cualquier caso, se insiste en que la amenaza interna es una de las más importantes, esto es, el riesgo que procede del prestador de servicios de la nube, puesto que tiene acceso de forma natural a los datos y aplicaciones de la empresa. También se insiste en los problemas derivados de las tecnologías

21 Estos riesgos se siguen entre otros en *Wikipedia*, voz: “computación en la nube” http://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube

22 Como los informes elaborados por el Grupo del artículo 29, la *Cloud Security Alliance* (CSA), Gartner o, en España, Inteco ya citados o que se citan a continuación.

23 GRUPO DEL ARTÍCULO 29, “Dictamen 05/2012... cit. pág. 6 y ss.

compartidas, dado que los componentes físicos, el hardware, no fueron diseñados para una arquitectura de aplicaciones compartidas. Asimismo, en la nube, aumenta el riesgo de la fuga de información, debido a la propia arquitectura de la misma, el número de interacciones se multiplica. De igual modo, se afirman los riesgos por desconocimiento de con quién se comparte la infraestructura o los intentos de acceso no autorizados pueden resultar muy importantes a la hora de decidir la estrategia de seguridad²⁴.

A los anteriores riesgos y problemas, Gartner añade otros riesgos de la nube, como es el teletrabajo y acceso a datos fuera de las instalaciones de la empresa (*BYOD*). La deslocalización de la información y el desconocimiento de dónde y en qué país están alojados los datos. También, respecto de la nube pública, se señala el riesgo que implica que varios clientes compartan la misma infraestructura, por ello, el proveedor debe garantizar el aislamiento de los datos de los respectivos clientes. De igual modo, se han señalado las dificultades que entraña la nube para la investigación de actividades ilegales, que en entornos *cloud* puede ser una actividad casi imposible, porque los datos y *logs* (registros de actividad) de múltiples clientes pueden estar juntos e incluso desperdigados. Por último, se indica el riesgo de la viabilidad a largo plazo, puesto que el mercado es cambiante y cabe la posibilidad de que el proveedor sea comprado o absorbido por alguno con mayores recursos²⁵.

En España y a la vista de estos problemas, INTECO ha insistido en las claves de garantizar que los datos están almacenados de forma segura y aislados, pese a que se comparta la infraestructura y sistemas con otros clientes del servicio de la nube. De ahí la importancia de la autenticación de identidad de los usuarios y la eficaz eliminación o saneamiento de datos cuando corresponde, por el riesgo también de los recursos compartidos. Asimismo se recuerdan las amenazas de ataques de denegación de servicio, fallos del equipamiento y desastres naturales que amenazan la disponibilidad de la información por el usuario. Y para ello, es esencial que el prestador de servicios dé respuesta a los incidentes de seguridad, esto es, la verificación, el análisis del ataque, la contención, la recolección de evidencias, la aplicación de remedios y la restauración del servicio²⁶.

Como recuerda la CSA, el objetivo, al fin y al cabo, es garantizar el ciclo de vida de la seguridad de la información, que consiste en seis fases: creación, almacenamiento, uso, compartición (hacer accesible la información a otros), archivo a largo plazo y, por último, destrucción. Y en la nube los retos clave al respecto se centran en²⁷: (1) la geo-localización de los datos. Debe existir una

24 Estos riesgos son los reflejados por CLOUD SECURITY ALLIANCE, (2010).

25 GARTNER (2011).

26 INTECO-CERT, (2011) págs. 24 y ss.

27 Se sigue de CLOUD SECURITY ALLIANCE (CSA), *Guía para la Seguridad ... cit.* en concreto, cap. 5, "Gestión del ciclo de vida de la información", por Geir Arild Engh-Hellesvik, Wing Ko, Sergio Loureiro, Jesus Luna, Rich Mogull, Jeff Reich, págs. 21 y ss.

garantía de que los datos estén donde legalmente sea posible. (2) Garantizar que los datos sean eliminados de manera efectiva y completa cuando se considere que son “destruidos”. (3) Que no se mezclen –especialmente los datos sensibles– con datos de otros clientes en su uso, almacenamiento o tránsito. Y (4), garantías de recuperación y restauración de datos con planes efectivos de *backup* frente reescritura de datos o destrucción. Pues bien, lo que aquí se sostiene es que el ámbito de la legalidad y privacidad se inserte en el ciclo de vida de la seguridad de la información. Como recientemente ha señalado Martínez²⁸, tras la primera fase de expansión y generalización de los servicios de la nube y su significativa reducción de costes, hay que esperar la madurez de un mercado que debe exigir seguridad, privacidad y cumplimiento de la legalidad, cuestión a la que ahora se dedica la atención.

2. Los sujetos y la regulación actual y futura de la protección de datos en la nube

2.1. Quién es quién en la nube a los efectos de la normativa de protección de datos

A los efectos de la normativa de protección de datos, es bien relevante determinar quién es quién en la prestación de servicios de la nube. Se trata de una cuestión inicialmente compleja²⁹, sobre la que hoy hay bastante claridad. Pues bien, como ha recordado el Grupo del artículo 29³⁰ y la Agencia Española de Protección de Datos (AEPD)³¹, el prestador de servicios de nube es, en términos del art. 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), un “encargado” del tratamiento de datos, que actúa para la organización cliente del servicio en la nube contratado. Y el usuario o cliente es, en términos de legislación de datos, el “responsable” de dicho tratamiento (quien decide sobre la finalidad, contenido y uso del tratamiento). El “responsable” al fin y al cabo es quien decide la contratación de dichos servicios, el mantenimiento o no de sus propios sistemas de información, la modalidad de nube y la tipología de servicios que contrata y la elección del proveedor. Y esta responsabilidad de quien utiliza servicios de la nube, al derivarse de la aplicación de la ley, no puede alterarse contractualmente³². No obstante, el marco contractual como luego se aprecia, es clave para la definición de papeles y es prueba objetiva de la diligencia de las partes, así como juega un papel básico para la legalidad de las transferencias de datos internacionales.

28 MARTÍNEZ i MARTÍNEZ (2014).

29 Así, dedica buena parte del mismo a esta cuestión LEENES, Ronald (2010).

30 GRUPO DEL ARTÍCULO 29, “Dictamen 05/2012... cit.

31 Tanto en AGPD, *Guía* como en AGPD, *Orientaciones* (2013).

32 AGPD, *Orientaciones para prestadores... cit.*

Aunque no necesariamente en todos los casos, el encargado, esto es, la empresa que presta servicios de la nube, normalmente será una gran corporación que cuenta con una posición prevalente en la contratación. De ahí que quien contrata servicios de la nube queda en una posición compleja por cuanto es “responsable” y la posición prevalente del prestador de servicios –encargado del tratamiento- puede ser un obstáculo para cumplir sus obligaciones. El futuro reglamento europeo de protección de datos en la línea de lo afirmado por el Grupo del artículo 29 de la UE, busca equilibrar la asimetría que puede producirse por esta preeminencia de los prestadores de servicios de la nube y sus usuarios³³.

2.2. Las cuestiones clave de protección de datos y las insuficiencias de la regulación actual

Como desde sus inicios puso en evidencia la Declaración de Independencia del Ciberespacio de 1996³⁴, no son pocos los problemas que implica en general la regulación de Internet³⁵. Y la regulación de la nube no es en modo alguno ajena a estos problemas. En el ámbito de la nube, Reed³⁶ ha insistido recientemente en modelos de co-regulación transnacional, en especial se insiste en que es necesario reforzar la legitimación de las normas. Y tal legitimación debe venir de la mano de un *regulador nebuloso* (“*cloud-regulator*”) que genere las normas con la participación de la comunidad afectada (instituciones, individuos y las entidades empresariales implicadas), pero que sea aceptada por los Estados e instituciones, que tienen que hacer valer tales normas.

Aunque no de manera exclusiva, el fenómeno de la nube atrae la cuestión de la protección de datos³⁷, que es la que centra mayormente aquí el interés. Y en materia de protección de datos, la ley aplicable es la del lugar del cliente de servicios de la nube³⁸, quien como se ha expuesto *supra*, es el responsable del tratamiento. Así pues, al usuario de servicios de la nube se le aplicará su ley nacional y, en consecuencia, el centro de atención es la Directiva 95/46/CE sobre protección de datos y, obviamente para España su transposición a través

33 GRUPO DEL ARTÍCULO 29, “Dictamen 05/2012... cit.

34 Redactada por John Perry Barlow, Fundador de Free, Fronteras Electrónicas en Davos (Suiza) el 8 de febrero de 1996. http://www.internautas.org/documentos/decla_inde.htm

35 Sobre la problemática de la regulación de la red, referencia obligada LESSIG (2001) y en español MUÑOZ MACHADO (2000). En general y más actual es la reflexión de Reed (2012) capítulo 4.

36 REED (2013)., Acceso en SSRN y cloudlegalproject.org

37 Además de los estudios que se de modo más concreto, un análisis general de la cuestión, FERNÁNDEZ-ALLER (2012). También, una aproximación general, GARCÍA MEXÍA (2010).

38 Así en especial GRUPO DEL ARTÍCULO 29, “Dictamen 05/2012... cit. pág. 8 y Dictamen 8/2010 sobre la ley aplicable http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf

de la LOPD y su desarrollo reglamentario. También habrá que seguir la Directiva 2002/58/CE (modificada por la Directiva 2009/136/CE)³⁹.

Miralles⁴⁰ ha sintetizado los aspectos más relevantes del nexo de la protección de datos y el *cloud computing*: 1) La pérdida de control sobre el tratamiento de la información, tanto por parte de las personas afectadas como por parte del responsable del tratamiento, y las consecuencias que se puedan derivar de ello (seguridad, confidencialidad, ejercicio de derechos, etc.); 2) Las dificultades de encajar jurídicamente y con suficiente agilidad las situaciones de tratamiento de los datos por cuenta de terceros: el encargado del tratamiento *cloud* y las posibles subcontrataciones. 3) Las problemáticas derivadas del movimiento internacional de datos. 4) Y, por último, la resolución efectiva de los incidentes relacionados con la vulneración del derecho fundamental en la protección de datos personales en situaciones de multiterritorialidad.

Frente a estos retos principales que con más detalle se analizan *infra*, no son pocas las disparidades y posibles choques entre normativa americana y europea de protección de datos para la nube⁴¹. Como especialmente recuerda Marzo, para la nube, la Directiva 95/46/CE está muy desfasada y se ha convertido en una traba para las relaciones entre Europa y los terceros países. Como luego se aprecia, el Grupo del Artículo 29 y la AEPD han sido proactivos en los últimos años para colmar las lagunas e incertidumbres de una normativa no concebida para la nube. En todo caso, dado que las empresas y administraciones públicas españolas no pueden abandonar el barco del “progreso tecnológico”⁴², necesariamente tienen que arriesgarse a contratar servicios de *cloud computing* sin un marco jurídico adecuado. La rigidez normativa sitúa a Europa y a su industria en una posición de clara desventaja competitiva frente al desarrollo de modelos de negocio de nube por la industria de los terceros países. La alternativa, obviamente, es desarrollar grandes plataformas de *cloud* europeas respetuosas de las garantías europeas. Y no parece que pueda aventurarse este futuro.

2.3. La nube en el esperado Reglamento europeo de protección de datos. Hacia una regulación nebulosa

Como es sabido, desde enero de 2012 se maneja el texto de un futuro Reglamento europeo de protección de datos del que hay diversas versiones y parece ser que se aprobará en 2016. Aunque lamentablemente no hay referencia

³⁹ Dicha norma respecto de la confidencialidad de las comunicaciones y del tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas en las redes públicas de comunicaciones (operadores de telecomunicaciones), si tales servicios se prestan a través de soluciones en la nube, lo cual no es extraño.

⁴⁰ MARTÍN MIRALLES (2010).

⁴¹ Un análisis concreto sobre disparidades y posibles choques entre normativa americana y europea de protección de datos para la nube, SCHWARTZ, (2013).

⁴² MARZO PORTERA (2012) pág. 225.

expresa a los servicios de la nube, obviamente la regulación se proyecta para el *cloud computing*⁴³. Entre otros aspectos, el Reglamento destaca por la figura del delegado de protección de datos (DPO, *data protection officer*, arts. 35-37). Dicha persona, en nuestro caso, de la empresa cliente que contrata servicios de la nube, habrá de asumir el conocimiento y decisiones en la materia. A este respecto, la empresa que provee servicios de la nube también deberá de generar todas unas buenas prácticas y transparencia sobre su actuación para facilitar la actividad y carga de responsabilidad del DPO.

También y especialmente, en razón del futuro Reglamento europeo puede tener mucha proyección en el ámbito de la nube la exigencia de la privacidad por diseño y por defecto⁴⁴:

El principio de protección de datos desde el diseño requiere la integración de la protección de datos en todo el ciclo de vida de la tecnología, desde la primera fase de diseño hasta su despliegue final, su utilización y su eliminación definitiva. Debe abarcar asimismo la responsabilidad por los productos y servicios utilizados por el responsable o el encargado del tratamiento. El principio de protección de datos por defecto exige que la configuración de la privacidad de los servicios y productos cumpla por defecto los principios generales de protección de datos, como la minimización de los datos y la limitación de los fines⁴⁵.

También y para estimular el cumplimiento, se prevé que estas exigencias de privacidad por defecto y en el diseño que pasen a ser “un requisito previo para las licitaciones de contratos públicos” (art. 23. 1 bis, versión marzo 2014). No obstante, tras casi cuatro años desde el primer texto conocido, habrá que ver la regulación final que en su caso se apruebe.

Y además de la regulación ya contenida en el futuro artículo 23, puede pensarse que ésta se concretará y de manera mucho más precisa a través actos delegados y normas técnicas por parte de la Comisión Europea que están previstos (art. 23. 2º y 3º y art. 86). Puede así esperarse que en unos años diversos servicios de la nube pasen a ser un sector bastante regulado. Ahora bien, no hay que obviar el cumplimiento de modelos y esquemas de certificación específicos para los entornos de nube facilita y garantiza la elección del proveedor por el cliente. En este punto, dentro de las normas ISO 27000 de seguridad de la información, es especialmente destacable la muy reciente ISO/IEC 27018:2014

43 HON, W. Kuan y otros. (2014) HON, W. Kuan y otros (2015). En español, sobre el futuro reglamento hay un amplio comentario de 500 págs. de SEMPERE SAMANIEGO (2014).

44 En general cabe seguir el término y desarrollo por Anna Cavoukian, entonces Comisionada de Información y Privacidad de la Autoridad de Protección de Datos de Ontario (Canadá). De referencia, el Centro de Investigación impulsado por ella <http://www.privacybydesign.ca/>

45 Considerando 61 en la versión de marzo de 2014 por el Parlamento Europeo. *Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento.*

de 27 de julio de 2014⁴⁶ de seguridad en la nube. Se hace difícil pensar que la futura normativa técnica que haga la Comisión Europea en razón sus competencias ejecutivas en del desarrollo del futuro Reglamento europeo no tengan una conexión con la normativa técnica privada.

Como se ha señalado, muy posiblemente cuando se desarrolle esta normativa técnica (pública, claro está), habrá de tenerse en cuenta los usos, prácticas y autorregulación técnica ya consolidados en el sector. De ahí es posible que resulte la *regulación nebulosa* (“*cloud regulation*”), la co-regulación transnacional del sector con ciertas garantías de exigibilidad y cumplimiento.

3. El tratamiento jurídico de algunas cuestiones clave que plantea la nube en materia de protección de datos

3.1. La diligencia y responsabilidad legales del usuario de la nube, transparencia de la empresa de *cloud*

Según se ha señalado, el cliente de servicios de la nube es “responsable” de protección de datos y la empresa proveedora de servicios, “encargado”. El usuario de nube como responsable tiene obligación legal de diligencia para “*velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto*” en la normativa de protección de datos personales (art. 20.2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, RLOPD). El usuario de nube –responsable LOPD- debe hacer una ponderación de riesgos a partir de toda la información que sea posible. La AGPD ha adoptado un papel activo para difundir el conocimiento de esta responsabilidad y de los elementos de juicio para tomar decisiones⁴⁷. Así, por ejemplo, ha señalado las preguntas que debe formularse la empresa o Administración (a través del futuro delegado de protección de datos) antes de contratar servicios de nube.

Y para poder desarrollar esta labor por el responsable, es esencial la transparencia por parte de la empresa prestadora de servicios de la nube. Como han señalado las instituciones y autoridades de protección de datos, la transparencia es “*un principio esencial que debe presidir las relaciones entre las partes, especialmente en los casos en que el proveedor de servicios ocupa una posición preeminente sobre los clientes*”⁴⁸ (especialmente

⁴⁶ “Tecnología de la información - Técnicas de seguridad - Código de conducta para la protección de la información de identificación personal (PII) en nubes públicas que actúan como procesadores PII”.

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498

En español, sobre esta nueva norma técnica, una descripción <http://blog.segu-info.com.ar/2013/06/iso-27017-iso-27018-e-iso-27036-guias.html>

⁴⁷ AGPD, *Guía* (2013).

⁴⁸ AGPD, *Orientaciones* (2013).

PYMES, microempresas, profesionales o Administraciones públicas sin gran estructura orgánica). Esta diligencia se traduce en exigencias importantes de transparencia al prestador de servicios para conocer sus garantías y si cumple lo exigible por la normativa y tomar las decisiones. El prestador de servicios de nube debe informar a los clientes de todos los subcontratistas de los respectivos servicios en nube y de todos los lugares donde los datos puedan ser almacenados, en especial, los lugares fuera del Espacio Económico Europeo-EEE). También el cliente deberá disponer de información significativa sobre las medidas técnicas y de organización aplicadas por el proveedor⁴⁹.

Y como señala el Grupo del Artículo 29 de la UE⁵⁰, respecto del futuro Reglamento europeo, la empresa de *cloud* (encargado del tratamiento) que no se atenga a las instrucciones del responsable del tratamiento, será considerado responsable del tratamiento y estará sujeto a las normas específicas en materia de control conjunto. Ello se realiza precisamente para equilibrar la situación habitual de preeminencia del prestador de servicios de la nube respecto del usuario, responsable del tratamiento, especialmente si se trata de una PYME.

A estas obligaciones de la empresa que presta servicios de nube⁵¹, hay que sumar tradicionales exigencias a un encargado que aloja datos⁵². Y cabe recordar en este sentido que han de venir recogidas en contrato (art. 12 LOPD). Entre tales obligaciones, una vez acabe la relación contractual, está la destrucción, devolución de los datos al responsable o su transferencia a la nueva empresa contratada (art. 12. 2º y 3º LOPD y art. 22 RLOPD). En una versión inicial del Reglamento europeo de protección de datos, se incluyó un derecho a la portabilidad que, no obstante, se ha eliminado en versiones posteriores. Y en cuanto a las medidas de seguridad que ha de cumplir la empresa de la nube, serán “*las mismas que las impuestas al responsable del fichero*” (arts. 9 y 12.2 de la LOPD)⁵³. En este sentido cabe recordar que el artículo 81. 8º RLOPD permite aplicar diferentes niveles de seguridad a un fichero. Asimismo, el encargado del tratamiento debe de elaborar el correspondiente documento de seguridad (art. 82.2º RLOPD).

Por lo expuesto y en la práctica, tendrá un especial interés comprobar las relaciones reales de la empresa de servicios de la nube con los clientes según sus perfiles. En este sentido cabrá prestar atención al papel activo de empresa y clientes en la definición del lugar que les corresponde como encargado y responsable de tratamiento. Asimismo, será de especial interés para la

49 GRUPO DEL ARTÍCULO 29, “Dictamen 05/2012... cit. Ver apartado 3.4.1.1 pág. 18

50 *Ibidem*, págs. 26 y ss.

51 Cabe destacar el reciente estudio AAVV. ENATIC, (2014). Ahí se analiza la responsabilidad de la empresa atacada, ya como cliente, ya como proveedora de servicios de las responsabilidades.

52 En particular recogidas en el Informe 574/2009 de la AEPD sobre Carácter de encargado del tratamiento de un prestador de servicios de alojamiento (acceso en web AEPC).

53 *Ibidem*, en el mismo sentido Informe 620/2009.

potenciación de los servicios de la nube descubrir las mejores prácticas para que la relación sea equilibrada entre uno y otro y tendente a la confianza y al mejor cumplimiento de las exigencias de seguridad y legales. Sin duda y en la práctica, es clave el papel pedagógico de la empresa de servicios de la nube y su proactividad en la difusión de información en incluso formación para sus clientes.

3.2. Un elemento clave para el cliente y la empresa de *cloud*: el conjunto contractual y la subcontratación

El contrato es la expresión de la relación jurídica entre el cliente – responsable– y el proveedor de servicios de la nube –encargado– y su existencia y unos contenidos mínimos se derivan del artículo 12 LOPD. Más allá de la exigencia formal, el contrato entre el encargado y el responsable es un indicador de la diligencia y responsabilidad del usuario de la nube (responsable). Pese a ser una responsabilidad del cliente, el “responsable”, en la práctica y realidad de la nube, la empresa de servicios de la nube (encargado) debe tener preparado un cuerpo contractual fuerte para dar toda la confianza y seguridad jurídica a sus clientes (responsables). Dicho cuerpo contractual normalmente se instrumenta por el contrato particular, que remite a unas condiciones generales de contratación que, a su vez, habitualmente remiten a un documento técnico de “Acuerdo de Nivel de Servicio”. También en los casos de consumidores, pueden ser relevantes jurídicamente los folletos o información comercial que haya accedido el cliente. Todo este conjunto contractual juega un papel clave en los servicios de la nube como garantía no sólo de las partes, sino del cumplimiento de la legalidad y la seguridad jurídica.

Además, y como es más que habitual en los servicios de nube, intervendrán empresas subcontratadas⁵⁴, es decir, el proveedor de nube empleará a su vez otros servicios de nube para realizar su prestación como socios, *partners*, *resellers*, *cloud builders* etc. Y en este caso la normativa (en especial el artículo 21. 2º RLOPD) exige mayores garantías, como ha ratificado la STS de 15 de julio de 2010, FJ 10⁵⁵. Así, las garantías deben darlas los socios de prestadores de nube, en cualquiera de las figuras de *reseller*, agregadores de servicios de *cloud*, *cloud builders*, proveedores de aplicaciones, etc., y que proporcionan servicios contratando directamente con los clientes.

⁵⁴ Entre otros, dedica alguna atención a las subcontrataciones FERNÁNDEZ-ALLER, Celia, “Algunos retos... cit. págs. 137-138

⁵⁵ En el recurso de legalidad frente a este precepto, que es desestimado y se da por buena la obligación de que el encargado del tratamiento comunique al responsable la necesidad de subcontratar y con quién pretende hacerlo. Tanto en AGPD, *Guía para clientes ... cit.* como en AGPD, *Orientaciones para prestadores... cit.* se recuerda que se exige: “La identificación de los servicios y la empresa a subcontratar informando de ello al cliente (incluido el país en el que desarrolla sus servicios si están previstas transferencias internacionales de datos). Que el cliente

El Grupo del artículo 29 ha recordado diversos contenidos y garantías en el contrato de servicios de nube⁵⁶, los mismos tiene su reflejo en la guía de la AEPD para los clientes de servicios⁵⁷. Y hay que buscar un cuerpo contractual equilibrado entre las responsabilidades de cliente (responsable del tratamiento) y empresa de nube (encargada del tratamiento)⁵⁸.

- Entre ellos está la mencionada garantía de la portabilidad, esto es, que al concluir el servicio, los datos se devuelvan al cliente o se transfieran a un nuevo proveedor de nube tras el contrato.

- También debe recogerse claramente la obligación para el proveedor de nombrar a todos los subcontratistas contratados⁵⁹. Se recogerá que el proveedor hará públicos todos sus subcontratistas, por ejemplo a través de un registro digital público. Y a este respecto debe garantizarse que el cliente conozca cualquier cambio por si quiere oponerse al mismo o rescindir el contrato⁶⁰.

- También ha de tener garantías efectivas frente a una posible infracción del contrato por el proveedor⁶¹.

- El contrato debe determinar medidas de seguridad técnica y de organización (en virtud del artículo 17, apartado 2, de la Directiva).

- De igual modo⁶², debe especificar las instrucciones del cliente al proveedor e incluir el objeto y el calendario del servicio, niveles de servicio objetivos y mensurables y las sanciones correspondientes (financieras o de otro tipo).

- Deberá asimismo precisar las medidas de seguridad que deben respetarse, en función de los riesgos del tratamiento y de la naturaleza de los datos, en consonancia con los requisitos correspondientes y con sujeción a las medidas más estrictas previstas en la legislación nacional de los clientes.

- Habrá se indicarse que sólo las personas autorizadas deberán tener acceso a los datos, con una cláusula de confidencialidad por lo que respecta al proveedor y sus empleados.

- El contrato también deberá exigir al proveedor que notifique toda solicitud jurídicamente vinculante de divulgar datos personales presentada por las autoridades policiales o judiciales a menos que dicha divulgación esté prohibida por otras razones. El cliente deberá garantizar que el proveedor rechazará cualquier solicitud de divulgación jurídicamente no vinculante.

pueda tomar decisiones como consecuencia de la intervención de subcontratistas y la celebración de un contrato entre el prestador de servicios de *cloud computing* y los subcontratistas con garantías equivalentes a las incluidas en el contrato con el cliente⁵⁷.

⁵⁶ GRUPO DEL ARTÍCULO 29, "Dictamen 05/2012... cit. págs. 9 y ss. y 14 y ss.

⁵⁷ AGPD, *Guía (2013)*.

⁵⁸ Un análisis de de los contratos, BRADSHAW Y OTROS (2010).

⁵⁹ GRUPO DEL ARTÍCULO 29, "Dictamen 05/2012... cit. págs. 9 y ss. Como se ha señalado, obligación confirmada por la STS de 15 de julio de 2010, FJ 10.

⁶⁰ *Ibidem*, págs. 23 y ss.

⁶¹ *Ibidem* punto 3.3.2 pág. 11.

⁶² *Ibidem*. 23 y ss.

- También se recomienda que contractualmente el proveedor de servicios coopere con el responsable del fichero, el cliente, para controlar el tratamiento y facilitar el ejercicio por los interesados de sus derechos a acceder, corregir o suprimir sus datos (ARCO).

- De igual modo, contractualmente debe reforzarse la obligación del proveedor de que se notifique al cliente toda violación de seguridad para que éste, a su vez, cumpla con la obligación legal de notificar violaciones a sus clientes.

- El contrato deberá reflejar que el cliente pueda auditar y solicitar el registro de las operaciones de tratamiento realizadas por el proveedor y sus subcontratistas. Para ello, no obstante, la mejor práctica es que contractualmente se acepten certificaciones y auditorías de terceros con plena transparencia. Así, el contrato puede reflejar la validez de tales auditorías y la facilitación de copia de la misma al cliente.

- El contrato siempre remitirá a garantías del nivel de prestación de servicios que impliquen el estándar de garantía de la disponibilidad, integridad, confidencialidad, aislamiento, posibilidad de intervención y portabilidad⁶³.

No hay que olvidar que no sólo están en juego los derechos e intereses de las partes, sino la garantía de un derecho fundamental de muchos sujetos afectados que pueden quedar afectados por estar sus datos personales e información en juego.

3.3. La cobertura legal de las transferencias internacionales de las empresas de *cloud* contratadas y subcontratadas: cláusulas contractuales tipo y normas corporativas vinculantes

Casi por defecto, el uso de nube implica el trasiego internacional de datos⁶⁴, bien porque el prestador de servicios esté en el extranjero, bien porque, como se ha indicado, lo natural en la nube es la subcontratación de servicios por los prestadores de servicios. El marco normativo y las instituciones deben adaptarse a esta realidad al tiempo de garantizar la seguridad, privacidad y el cumplimiento de la legalidad permitiendo tales las transferencias internacionales de datos. Y debe permitirse las mismas al tiempo de asegurar que el responsable, esto es, el cliente, sigue manteniendo la capacidad de tomar decisiones.

⁶³ *Ibidem* pág. 16.

⁶⁴ Sobre el tema, cabe seguir el AEPD Informe 2001-0000, *Transferencias Internacionales de datos para la realización de un tratamiento por cuenta del responsable del fichero*. Acceso en web AEPD. En la doctrina en general MARZO PORTERA y ORTEGA GIMÉNEZ, (2013), autores de dos tesis doctorales sobre el tema. De un lado, GUASCH PORTA (2012). Asimismo, la premiada tesis doctoral ORTEGA GIMÉNEZ (2014).

Los datos fácilmente no estarán en España ni en territorio europeo y es posible que los datos o el prestador estén en países terceros que no cuenten con un nivel adecuado de protección de datos (Suiza, Canadá, Argentina, Guernsey, Isla, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y ciertas compañías estadounidenses)⁶⁵. En tales casos, por principio es requisito una autorización del Director de la AGPD para permitir la transferencia internacional de datos (art. 33 LOPD). Y el incumplimiento de esta obligación es falta muy grave (artículo 44.4 d) LOPD).

Ahora bien, tal autorización resultará automática si se siguen las cláusulas contractuales tipo de la Comisión Europea (artículo 26.2º de la Directiva 95/46/CE de protección de datos)⁶⁶. Así, cabe seguir especialmente la Decisión 2010/87/UE, (DOUE L 39 de 12 de febrero de 2010), centrada en la subcontratación por un encargado del tratamiento establecido en un tercer país, de sus servicios de tratamiento a un subencargado establecido en un tercer país. Como se dijo respecto del contrato, éste debe estipular de modo concreto cómo el prestador de servicios ha de aplicar los principios de la protección de datos, al tiempo de ofrecer un nivel de cumplimiento de las normas, facilitar su cumplimiento a las partes y dar vías de recurso y garantías a los perjudicados para ello.

Por su parte y de forma paralela, la AEPD elaboró en 2012 un nuevo conjunto de cláusulas contractuales para facilitar la subcontratación que ha de preverse en el contrato⁶⁷. Se necesitan determinadas adaptaciones del entorno de la

65 Respecto de estos países hay Decisiones de la Comisión europea desde 2000 en las que se expresa que sí que reúnen garantías similares, a saber:

- Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.
- Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001.
- Argentina. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.
- Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.
- Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.
- Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.
- Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.
- Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010.
- Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.
- Uruguay. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.
- Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.

Además, es singular y central el caso de EEUU, dado que se considera que sí que cumple el nivel adecuado respecto de las entidades que cumplen con los principios de puerto seguro “*safe harbour*”. Así, decisión de la Comisión sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, en el DOCE L 215, de 25 de agosto de 2000. Puede consultarse qué entidades sí que cumplen con tales principios en <https://safeharbor.export.gov/list.aspx>

66 Sobre el tema, los trabajos ya referidos de Giménez y Marzo y GUASCH PORTAS, Vicente y SOLER FUENSANTA (2014). También GARCÍA DEL POYO (2012), en especial, 186 y ss.

67 Las mismas fueron conocidas con ocasión del Expediente TI/00126/2012 en la página de la AEPD, así como la publicación oficial del “Acuerdo de Apertura del Período de Información Pública” en el BOE de 20-09-2012. El contenido es similar al de las cláusulas tipo de la Comisión.

nube (para evitar tener diferentes contratos por cliente entre un proveedor y sus subencargados) lo que podría implicar la necesidad de una autorización previa de la autoridad de protección de datos competente. La ventaja para las empresas de *cloud* españolas es que si se logra la autorización de transferencia de datos siguiendo estas cláusulas contractuales, no se precisa en general una ulterior si se mantiene lo establecido en el contrato. Sólo tendrán que notificar –no pedir autorización–no autorice– cada nueva transferencia internacional para que ésta quede registrada⁶⁸.

Otra vía para legalizar la transferencia internacional de datos es la adopción de reglas corporativas vinculantes. Se trata de dar respuesta a las sociedades multinacionales que deben realizar trasiego internacional de datos dentro del grupo. Así, se adoptan las normas de funcionamiento y buenas prácticas (*Binding Corporate Rules*) son aprobadas por autoridades de protección de datos y han de ser efectivamente asumidas y cumplidas por las empresa multinacional⁶⁹. Ello puede permitir que empresas de nube puedan prestar sus servicios aprovechando la natural participación de otras empresas subcontratadas de fuera de la Unión Europea.

4. Algunas exigencias del uso de la nube por las administraciones

Son diversos los retos técnicos⁷⁰ y, por lo que aquí interesa, jurídicos que suscita el uso de la nube por las Administraciones⁷¹. Si la Administración externaliza servicios en la *nube*, tendrá que asegurarse de que de las entidades con las que contrate cumplen requisitos normativos. Y lo mejor será asegurar la expresión de estas obligaciones en los pliegos de cláusulas administrativas generales (art. 98 Ley 30/2007, de 30 de octubre), de cláusulas administrativas particulares (art. 99) y en su caso, los pliegos de prescripciones técnicas (art. 100).

Aunque actualmente no lo hace, la ley habría de expresar la prohibición de externalización en supuestos específicos en razón de una mayor exigencia de confidencialidad y seguridad e incluso establecer determinadas garantías al prestador en casos determinados.

68 Entre otros, lo explican GUASCH PORTAS, Vicente y SOLER FUENSANTA José Ramón, “Cloud computing... cit. págs. 263 y ss.

69 Al respecto, ver GRUPO DEL ARTÍCULO 29, “Dictamen 05/2012... cit. pág. 22 así como Comisión Europea, “Un enfoque global de la protección de los datos personales en la Unión Europea”, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Bruselas, 4.11.2010, COM(2010) 609 final.

70 Al respecto, en especial, CATTEDDU, (2011) 2011 en http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/es_governmental_clouds_enisa.pdf

71 La cuestión ha sido estudiada esencialmente por VALERO TORRIJOS (2012), quien remite también a PAQUETTE, S., JAEGER, P.T. y WILSON, S.C.

Una cautela esencial del prestador de servicios de la nube es evitar que la información pública en la nube no pueda verse alterada. La falla de seguridad o que la información quede fuera de control, como es obvio y recuerda Catteddu⁷², puede poner en compromiso la soberanía y control gubernamentales sobre la información y los datos.

Más allá de las obligaciones dimanantes de la normativa de protección de datos que se aplica a las administraciones, en razón de la normativa de gobierno electrónico, la Administración pública habrá de confirmar las versiones de la información o documentación que en su caso genere la entidad prestataria de los servicios en la nube. Asimismo y especialmente la entidad prestadora de nube tendrá que asegurar “la identificación de los usuarios y el control de accesos” (art. 31. 3º Ley 11/2007). También y si es necesario, habrá de integrar la referencia temporal de la información o documentación (art. 29 Ley 11/2007). Tales acciones habrán de satisfacerse por el prestador de servicios y no sólo frente a la Administración contratante, sino también de cara a las otras administraciones con las que la Administración haya de compartir información.

Además de las obligaciones de seguridad de la información en razón de la normativa de protección de datos y del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, es fundamental el cumplimiento de la interoperabilidad, y cumplir sus detalladas normas para, entre otros, garantizar la eficaz conexión de la información en la nube con otras entidades públicas o privadas (art. 8. 1 ENI). El contrato o la relación jurídica con la empresa de nube habrá de reflejar estas exigencias.

Por cuanto a la conexión entre el uso público de la nube y la actuación automatizada, en España desde la Ley 11/2007 desapareció la anterior obligación por la que las Administraciones habían de aprobar previamente las aplicaciones (antiguo art. 45.4 de la Ley 30/1992). Desde entonces sólo recae la obligación para la Administración General del Estado de que se establezcan previamente el “*órgano u órganos competentes para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente*” (art. 39 LAE). Así pues al menos se pretende asegurar que las decisiones administrativas al respecto siguen criterios previos. De igual modo, la actuación automatizada en la nube requerirá de sistemas de firma electrónica. Dado que la prestación de servicios en la nube es bien posible que sea a través de una empresa habrá que extremar la precaución para evitar el uso indebido de la actuación automatizada por parte de la entidad o su personal.

Finalmente cabe plantearse con Valero el juego de responsabilidades por daños y perjuicios por una mala nube pública prestada por una empresa privada. En este supuesto, el artículo 198 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, será “obligación del contratista indemnizar todos los daños y

72 CATTEDDU, D.D. *Seguridad y Resistencia... cit. pág. 41.*

perjuicios” a terceros en la ejecución del contrato. Pero la responsabilidad será de la Administración si ésta “hubiere impuesto ciertas condiciones que motivaran la producción del daño”. Obviamente la responsabilidad variará según se los diferentes servicios de nube: por el funcionamiento de la infraestructura (IaaS), plataforma (PaaS) o aplicaciones de servicios de nube (SaaS). Y, como señala Cattedu⁷³, van a desempeñar un papel fundamental en este tema, de un lado, los acuerdos de nivel de servicio (ANS) detallados, que especifican los niveles de funcionamiento del proveedor de servicios en la nube y, del otro, las cláusulas contractuales que asignan derechos obligaciones.

⁷³ *Ibidem* pág. 46.

Democracia deliberativa y participación ciudadana electrónica

Jacqueline Guerrero Carrera*

SUMARIO: I. Introducción. II. Acerca de la democracia deliberativa. III. Participación ciudadana y tecnología. IV. Ideas finales.

Resumen

El presente trabajo discute la teoría de la democracia deliberativa y la participación ciudadana que emplea Tecnologías de la Información y Comunicación, denominada e-participación, con el objetivo de analizar la posibilidad de que la deliberación pública se realice en el entorno virtual. La investigación establece los niveles en los que se desarrolla la participación ciudadana electrónica (e-participación). La deliberación pública es un nivel elevado y de difícil realización, si se considera que para este fin la participación ciudadana está directamente relacionada con factores como: la cultura política, el acceso a la información, las competencias digitales de los ciudadanos y los derechos digitales.

Palabras clave: Democracia deliberativa. Derechos digitales. e-participación. Libertad de expresión

Abstract

This paper discusses the theory of deliberative democracy and citizen participation which uses Information Technology and Communication, called e-Participation, with the aim of analyzing the possibility of public debate takes place in the virtual environment. The research establishes the levels at which e-Participation is developed. Public deliberation is a high level and difficult to perform, considering that for this purpose citizen participation is directly related to factors such as political culture, access to information, digital skills of citizens, and digital rights.

Keywords: Deliberative Democracy. Digital Rights. E-participation. Freedom of Speech.

Aceptado por el Comité Académico para ser presentado en el XIX Congreso Iberoamericano de Derecho e Informática celebrado en Medellín, agosto 2015. Aprobado por la Junta Directiva de FIADI para ser publicado en la *Revista Derecho y Tecnología*, el 13 de octubre de 2015.

* Docente de la Facultad de Derecho de la Universidad de Las Américas, UDLA, Ecuador. jacqueline.guerrero@udla.edu.ec

I. Introducción

Discutir sobre democracia deliberativa, participación ciudadana y tecnología no es nuevo; sin embargo, no se ha agotado el análisis del rol que las Tecnologías de la Información y Comunicación deben tener en relación con la democracia, y la verdadera capacidad de las TIC para configurar una esfera virtual de deliberación, así como para promover una ciudadanía más activa, como aportes para la profundización de la democracia o la mejora en la calidad de la misma.

La crisis de la democracia representativa, que ha generado un déficit democrático, ha contribuido al surgimiento de nuevas formas de participación ciudadana, incluyendo aquellas que emplean como medio a las TIC en el marco de la Sociedad Red.

El análisis de la relación entre la democracia deliberativa y la participación ciudadana, entendida ésta última como un hecho político que implica la posibilidad de que el ciudadano influya en la toma de decisiones, permite abordar el tópico central del trabajo relativo a los mecanismos tecnológicos participativos y la posibilidad de que en el contexto de la e-participación se pueda realizar la deliberación pública de los temas de interés colectivo por medios electrónicos.

La principal conclusión da cuenta que aún es muy difícil pensar en una deliberación democrática digital, pues pese a las potencialidades de las Tecnologías de Información y Comunicación para generar espacios que permitan a los ciudadanos expresarse y relacionarse con el Estado en todos sus niveles, la deliberación pública implica elementos complejos y depende de factores que trascienden a la tecnología misma.

II. Acerca de la democracia deliberativa

La democracia deliberativa, como modelo teórico de democracia, reivindica la participación ciudadana con el fin de que los ciudadanos puedan influir en las decisiones políticas, a través de la deliberación pública. Es también un ideal, que precisa de la participación individual de los ciudadanos en la deliberación pública de los temas de interés colectivo que les afectan.

La Ley Orgánica de Participación Ciudadana del Ecuador considera que la deliberación pública es “*el intercambio público y razonado de argumentos, así como el procesamiento dialógico de las relaciones y los conflictos entre la sociedad y el Estado, como base de la participación ciudadana*” (LOPC, 2010, Art. 4). Ciertamente la deliberación pública no solo implica el intercambio de ideas y opiniones, sino se traduce en la discusión argumentada que se realiza con ciertas condiciones, las cuales a decir de Carlos Nino son:

- a) La participación de todos los interesados en la discusión y la decisión; b) que esa participación se desarrolle sobre una base *razonable* de igualdad y sin mediar ningún tipo de coerción; c) que los participantes del debate público

puedan expresar sus intereses y justificarlos con *argumentos genuinos*; *d*) que el grupo que pone en obra la deliberación tenga una dimensión tal que maximice la posibilidad de alcanzar un resultado correcto; *e*) que no existan minorías sistemáticamente *aisladas*; *f*) que aquellos que participan en el debate no se encuentren bajo la influencia de *emociones extraordinarias*. (Nino citado en Montero, 2006, p. 323)

La democracia deliberativa se construye por el aporte conceptual de categorías como: ciudadanía, opinión pública, participación ciudadana y derecho; y es la respuesta a dos de los principales desafíos de los estados modernos: el multiculturalismo y la globalización, pues la deliberación democrática permite definir los presupuestos normativos del Estado en la diversidad. (Habermas citado en Domínguez, 2013, p. 303-304). Además la participación ciudadana activa y la aceptación de los posibles afectados por las normas determinan la legitimidad de las mismas (Habermas, 2008, p. 9)

La democracia deliberativa no se opone a la democracia representativa y por tanto no cuestiona las instituciones de las democracias modernas en sí mismas, sino que discute la posibilidad real de considerar los intereses y aportes de los ciudadanos para la toma de decisiones que atañen a la sociedad. Esto supone la existencia de un ciudadano activo, interesado por los temas que atañen a la sociedad, con compromiso social, y con ciertas competencias para el ejercicio ciudadano, incluyendo las denominadas competencias digitales.

Las competencias digitales se generan a partir de la alfabetización digital de los individuos, es decir de sus conocimientos, aptitudes y habilidades para ser usuarios de las TIC, y están relacionadas con la actuación ciudadana; implican capacidades y actitudes relativas a la ciudadanía digital, seguridad informática, protección de la privacidad y de los datos personales, gobierno electrónico, entre otras. Por tanto, no todos los usuarios de TIC, incluyendo a los nativos digitales, disponen de estas competencias, pues lo común es que dispongan de competencias básicas relacionadas con actividades de entretenimiento: uso de redes sociales, manejo de recursos en línea, búsqueda de información, acceso a servicios básicos, etc. La participación ciudadana electrónica depende de las competencias digitales que tengan los individuos, siendo por tanto la alfabetización digital uno de los desafíos para los Estados.

La democracia deliberativa supone la existencia de mecanismos de participación institucionalizados, que generen los espacios o la denominada *esfera pública*, en los cuales confluyan ideas y opiniones diferentes. La esfera pública en la Sociedad Red incluye al ciberespacio, que constituye un espacio natural para el libre flujo de ideas y contenidos, y para que las personas expresen sus opiniones, intercambien puntos de vista y se conecten con otros ciudadanos en todo el mundo. Aunque, las características del ciberespacio pueden representar problemas para la deliberación y la democracia. Por ejemplo, el denominado *poder de filtrar* que brindan las herramientas tecnológicas, es decir la posibilidad ilimitada de seleccionar con exactitud la información que se desea recibir o los

individuos y grupos con los que se desea tener contacto, que evidentemente no incluirán visiones opuestas. Es importante también la posibilidad de fragmentación por la formación de comunidades que limita los intereses colectivos y sociales, por lo que puede generarse polarización. (Sunstein, 2003, p.57) La conformación de las comunidades virtuales lejos de posibilitar la deliberación, refuerza las ideas comunes, pudiendo generar polarización.

III. Participación ciudadana y tecnología

La participación ciudadana, que no es igual que la participación política, puede entenderse como el mecanismo que permite a la ciudadanía involucrarse en la actividad pública, con el propósito de influir en los procesos de toma de decisiones en todos los niveles, escalas y sectores de la gestión pública (Maldonado, 2008, p.243). Por esta razón la participación ciudadana sirve de base para la democracia electrónica¹.

Los artículos 61 y 95 de la Constitución del Ecuador consagran el derecho de los ciudadanos a participar en los asuntos de interés público, que podrá ser ejercido por los ciudadanos de forma individual o colectiva², estableciéndose su participación de manera protagónica en la toma de decisiones, planificación y gestión de los asuntos públicos, así como en el control popular, como parte del proceso de construcción del poder ciudadano. En todo caso se precisa que la participación ciudadana en los asuntos de interés público es un derecho que se ejercerá a través de los mecanismos de democracia representativa, directa y comunitaria, siendo la deliberación pública un principio rector.

Al ser la participación ciudadana un derecho debe suponer la participación individual de los ciudadanos de forma libre, que permita tener una deliberación de calidad, es decir alcanzar lo que José Luis Martí (2008, p. 7) denomina *calidad reflexiva de la participación democrática*.

Con base en las disposiciones constitucionales, en el 2010 se aprobó la Ley Orgánica de Participación Ciudadana, con el objeto de establecer instancias, mecanismos, instrumentos y procedimientos de deliberación pública, entre el Estado y la sociedad, a fin de sentar las bases para el funcionamiento de la democracia participativa. (LOPC, 2010, art. 1). Así también la norma dispone

1 Democracia digital, e-democracia, ciberdemocracia y democracia electrónica son algunas expresiones utilizadas para hacer referencia a las nuevas formas de relacionamiento del Estado con los ciudadanos, a través de las TIC, especialmente en aspectos políticos. Pero no existen acuerdos conceptuales pues se trata de un ámbito que está en proceso de construcción. En todo caso debe sentarse que la democracia electrónica no se limita al uso de herramientas como: chats, correo electrónico, foros políticos o el voto electrónico, sino que esencialmente emplea las TIC para la participación ciudadana.

2 Conforme el Art. 2 de la Ley Orgánica de Participación Ciudadana son sujetos de derechos de participación ciudadana todas las personas en territorio ecuatoriano, las ecuatorianas y los ecuatorianos en el exterior, colectivos, comunas, comunidades, pueblos y nacionalidades indígenas, pueblos afroecuatorianos y montubios.

la implementación de la democracia electrónica en los gobiernos autónomos descentralizados, los cuales “expedirán políticas específicas e implementarán mecanismos concretos para la utilización de los medios electrónicos e informáticos en los procesos de información, consulta, constitución de grupos, foros de discusión y diálogos interactivos” (LOPC, 2010, Art. 100). El principal medio para el cumplimiento de esta disposición será el portal web institucional, que será transaccional, para permitir el diálogo e interacción con la comunidad.

Más allá de cómo se conciba la participación ciudadana, es importante establecer los niveles de relacionamiento entre el Estado y los ciudadanos, que podría implicar la participación y posteriormente analizarlos desde la perspectiva del uso de herramientas tecnológicas.

Considerando las disposiciones legales del Ecuador, estos niveles al menos son tres: 1) difusión de información; 2) consulta; y 3) discusión y diálogos interactivos. Considerando la escala de Arnstein (Arnstein citado por Colombo, p.3) se pueden establecer cinco niveles de participación: 1) información; 2) comunicación; 3) consulta; 4) deliberación; y, 5) decisión. El primero es de nivel básico, el segundo y tercero son intermedios y los dos últimos son los niveles más elevados de participación.

La difusión de información constituye el nivel más bajo en la relación entre el Estado y los ciudadanos, es decir el menos complejo y respecto del cual las TIC tienen un uso notable. Este nivel está en relación con temas de transparencia y rendición de cuentas. El nivel de comunicación es un nivel intermedio que busca facilitar el diálogo entre los ciudadanos y el gobierno, para lo cual se puede apelar a recursos básicos como el correo electrónico.

El nivel de consulta es de complejidad media y por tanto involucra herramientas especiales, a través de las cuales se recabe la opinión de los ciudadanos con fines específicos. En este nivel existen buenas experiencias en e-participación, como por ejemplo en la elaboración de los presupuestos participativos.

La deliberación y la toma de decisiones representan los niveles de mayor complejidad y por tanto los de más difícil materialización en entornos virtuales. Las preocupaciones pasan por la seguridad de los medios electrónicos o la forma cómo éstos pueden traducir los argumentos de los ciudadanos para que se reflejen en las decisiones que se adopten.

Las escasas experiencias reales de participación ciudadana electrónica, en el nivel de discusión y deliberación, afirman las potencialidades que tiene las TIC para lograr una participación activa, pero la dificultad de que se pueda pensar en una deliberación digital en países como el Ecuador. Este es el caso de la *Ciudad Digital de Amsterdam*, que además de redimensionar el concepto de la esfera pública ha materializado la participación ciudadana y la posibilidad de deliberación en temas de interés colectivo. (Castells, 2003: 189-200). A nivel local, una experiencia que es importante analizar es la denominada *Consensus, ciudadanos en red*, que es un proyecto específico de empleo de las TIC para promover la participación ciudadana on line en los municipios de Cataluña. Es

un modelo mixto pensando en los cinco niveles de participación ciudadana, algunos de los cuales ofrecen espacios de participación totalmente en Internet³ y otros complementan acciones de participación presencial.

Finalmente, es importante señalar que la e-participación está directamente relacionada con elementos como: la cultura política, el acceso a la información, la brecha digital o la estratificación digital, las competencias digitales de los ciudadanos y los derechos que permitan la actuación ciudadana, siendo éste último tema de especial trascendencia, por lo que se analiza brevemente a continuación.

No existe una aproximación conceptual única respecto de los derechos digitales e incluso hay quienes sostienen que su referencia es innecesaria⁴, pues no se trata de nuevos derechos sino de los mismos derechos fundamentales que tenemos reconocidos. Sin embargo, bajo la etiqueta de los derechos digitales o ciberderechos, se ha desarrollado una serie de iniciativas con el objetivo de afrontar la problemática de la protección de los mismos en entornos virtuales, especialmente Internet.

En relación con la e-participación hay un conjunto de derechos que se considerarían como mínimos para promover la cultura participativa electrónica, como los siguientes:

- Derecho de acceso
- Derecho de libertad de expresión
- Derecho de asociación
- Derecho a la privacidad, a la protección de datos y al olvido

No sería posible hablar de e-participación si los ciudadanos no tienen garantía de acceso a las Tecnologías de Información y Comunicación, incluyendo Internet y ahora a los dispositivos móviles, con ciertas características básicas como: calidad del servicio, costo marginal, banda ancha, etc. Es fundamental también la garantía del derecho de asociación, que constituye la base para el activismo digital, que es una forma de expresión de la participación ciudadana.

Pero sin duda el derecho a la libertad de expresión, que es uno de los pilares fundamentales de todo sistema democrático, tiene absoluta trascendencia tratándose de la participación ciudadana en los espacios virtuales, particularmente

³ Es preciso señalar que si bien cuando se piensa en participación ciudadana electrónica, Internet es el medio paradigmático, existen otros dispositivos electrónicos que pueden servir para la participación como los dispositivos móviles.

⁴ Neelie Kroes, Vicepresidenta de la Comisión Europea y responsable de la Agenda Digital de la Unión Europea, sostiene que los derechos digitales no existen, pues no hay como diferenciarlos de los derechos fundamentales y éstos no tienen un límite en cuanto a su reconocimiento y garantía, incluso en el ámbito de Internet. Por tanto, los derechos digitales son intrínsecos de los derechos y libertades de los ciudadanos.

Internet, como forma de desarrollo de la cultura participativa, que luego permitirá la participación y la deliberación en los espacios institucionalizados⁵.

Internet sin duda es un foro público potente, en el cual los ciudadanos deben ejercer su derecho a la libertad de expresión con absolutas garantías, pero la deliberación que es parte de la participación ciudadana difícilmente podría realizarse en espacios abiertos y sin una estructura determinada.

IV. Ideas finales

La relación entre la tecnología y la democracia es indiscutible, así como la potencialidad de las TIC para el desarrollo de los procesos participativos, y aunque pueden anticiparse los resultados en cuanto a la mejora de la comunicación entre el Estado y los ciudadanos por el uso de medios tecnológicos, sigue en duda el hecho de que las TIC permitan la deliberación y el debate entre los ciudadanos, lo cual implica un nivel elevado de participación ciudadana y uno de los aspectos más complicados de la e-participación, pues tiene complejidades de orden técnico como: la forma en que las herramientas de e-participación traducirán los argumentos y opiniones de los ciudadanoso barreras como la brecha digital individual o colectiva.

La posibilidad de que se realice una deliberación democrática totalmente virtual, constituye un ideal y representa un desafío para las democracias, pues deben superarse barreras como: el acceso a Internet, la brecha digital, el analfabetismo digital y la falta de cultura participativa. Sin embargo, es imperioso que se empleen las TIC para promover la participación ciudadana, al menos en niveles básicos de difusión de información y comunicación.

Finalmente, existe una reflexión obligada respecto de la participación ciudadana electrónica en Ecuador, pues pese a tener normativa específica sobre el tema, de rango constitucional y legal, e incluso contar con un Consejo de Participación Ciudadana y Control Social, no existen avances en cuanto a la generación de espacios para que los ciudadanos intervengan y aporten en la toma de decisiones a través de medios electrónicos.

⁵ Aunque la realidad de Latinoamérica es menos dramática que la de otras partes del mundo, en nuestra región los esfuerzos no apuntan a la garantía del derecho de libertad de expresión en internet, sino por el contrario a encontrar mecanismos legales o de otro tipo para censurar, vigilar y silenciar a los internautas.

Plataformas ciudadanas de participación como herramientas del ejercicio de la libertad de expresión en Internet

Olivia Andrea Mendoza Enriquez*

SUMARIO: I. Introducción. II. Libertad de expresión en Internet. III. Plataformas electrónicas como forma de participación ciudadana. A. Méxicoleaks. IV. Marco jurídico en relación con la libertad de expresión en Internet. V. Medidas de censura contra la libertad de expresión en Internet. VI. Conclusiones.

Resumen

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC), ha permitido nuevas formas de difusión de contenidos a través de las plataformas electrónicas de participación ciudadana en Internet.

Dichas plataformas son alimentadas por la información de interés público que los usuarios proveen, en el ejercicio del derecho a la libertad de expresión y tienen por objetivo promover la participación ciudadana. Esto ha replanteado la relación entre los derechos humanos e Internet, lo cual supone un nuevo espacio para la garantía de los mismos, pero que a su vez también funge como un lugar idóneo para la vulneración de dichos derechos. El presente trabajo abordará dicha problemática y dará una aproximación a la afectación al ejercicio de la libertad de expresión en Internet, particularmente en las plataformas antes citadas.

Palabras clave: Internet. Libertad de expresión. Plataformas electrónicas de participación ciudadana.

Aceptado por el Comité Académico para ser presentado en el XIX Congreso Iberoamericano de Derecho e Informática celebrado en Medellín, agosto 2015. Aprobado por la Junta Directiva de FIADI para ser publicado en la *Revista Derecho y Tecnología*, el 13 de octubre de 2015.

* Licenciada en Derecho y Maestra en Derecho con especialidad en Derecho Económico por la Benemérita Universidad Autónoma de Puebla. Candidata a Doctora en Derecho por la misma universidad. Profesora Investigadora de tiempo completo del Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. Profesora de Educación a Distancia de la Facultad de Derecho de la UNAM. Email: olivia.mendoza@infotec.com.mx andymendoza1@hotmail.com

Abstract

The development of Information and Communications Technology (ICT) has allowed new ways of sharing information through online public participation platforms.

These platforms are fed by the public interest information that users provide, in the exercise of the right to freedom of speech and aim to promote citizen participation. This has redefined the relationship between human rights and the Internet, which represents a new space to protect them, but also becomes a place for the violation of such rights. This paper addresses this problem, and provides a close look to the ways that freedom of speech is affected in the platforms referred above.

Keywords: Internet. Freedom of Speech. Online Public Participation Platforms

I. Introducción

En el planteamiento del desarrollo de las Tecnologías de la Información y Comunicación TIC, la aparición y evolución de Internet desempeña un rol importante, al ser un instrumento de acceso a los derechos humanos bajo nuevas manifestaciones; sin embargo también ha representado afectaciones en algunos de estos derechos. Para el caso particular del presente trabajo, analizaremos cómo la libertad de expresión se ha visto afectada, al establecerse mecanismos de censura que tratan de evitar la percepción negativa de los ciudadanos respecto de la actuación de los representantes del Estado.

Dicho lo anterior, es importante destacar que a medida que Internet adquiere en mayor forma la característica de universal, la relación entre éste y los derechos humanos, tiene mayor importancia y complejidad, ya que el uso de la Red afecta casi todas las esferas de la sociedad.

En este sentido, una nueva forma de difusión de información surge con las Plataformas de Participación Ciudadana, que permiten denunciar actos contrarios a derecho, cometidos por representantes del Estado, en donde la información es corroborada por un grupo multidisciplinario detrás de la conformación de dichas plataformas, lo que le otorga veracidad a los contenidos ahí establecidos.

Estas plataformas surgen como mecanismos de ejercicio de libertad de expresión en Internet, al hacer denuncias y difundir información de interés colectivo; sin embargo, la aparición de estos nuevos modelos, afecta los intereses de algunos Estados, principalmente en países como México, en donde, a consecuencia de estas plataformas, se han puesto en marcha diversas formas de censura que contravienen a toda luz los principios del ejercicio de la libertad de expresión de los usuarios de Internet.

II. Libertad de expresión en Internet

La libertad de expresión es un derecho humano consagrado en diferentes instrumentos jurídicos nacionales e internacionales que surge como característica de las democracias modernas al empoderar al ciudadano frente al Estado.

La justificación de la libertad de expresión se ha basado fundamentalmente en tres cuestiones: su carácter esencial para el autogobierno democrático, la incidencia en el gradual descubrimiento de la verdad, y el derecho del individuo a expresar su personalidad¹.

La primera de ellas radica en la libertad de información para la conformación de la opinión pública y la transparencia del sistema; la segunda, invoca el derecho al descubrimiento de la verdad; y la tercera es la más próxima a la libertad de expresión, ya que tiene su origen en el individuo mismo.

Lo anterior, tiene congruencia con la afirmación de Walton al decir que “*no existe ninguna sociedad abierta ni democrática sin libertad de información y de comunicación*”²; por lo tanto, las cuestiones comunicativas en Internet, no están exentas, y deben tener el reconocimiento de la libertad de expresión y comunicación.

Se debe destacar que las decisiones que conciernen a los alcances de la libertad de expresión, surgen de la interacción entre marcos de derechos internacionales, gobiernos nacionales, empresas privadas como las proveedoras de servicio de Internet que pueden abrir o cerrar el acceso a la información o la expresión, ciudadanos que utilizan Internet como medio de expresión y organizaciones de la sociedad civil³.

En este sentido, en una sociedad como en la que vivimos, la información es poder y el poder se hace decisivo cuando la tecnología convierte informaciones parciales y dispersas en informaciones más organizadas, por lo que la reglamentación jurídica de la misma, reviste un interés prioritario, lo que hace evidente que para la opinión pública y el pensamiento filosófico, jurídico y político constituya un problema nodal en relación al establecimiento de garantías que tutelen a los ciudadanos frente a la eventual erosión y asalto tecnológico de sus derechos y libertades⁴.

Una vez que se habló de la libertad de expresión en su concepción tradicional, es importante traer a colación que Internet ha permitido expandir el ejercicio de

1 Véase ROSENFELD, Michel, “El nacimiento y la evolución de los derechos humanos en Estados Unidos”, *Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol*, Valencia, números 18 y 19.

2 Véase WOLTON, Dominique, *Internet ¿y después?*, Barcelona, Gedisa, 2000.

3 *Mapeando los derechos en Internet y la libertad de expresión*, Monitor Mundial sobre la Sociedad de la Información 2011, Derechos en Internet y democratización. Consultado en: www.giswatch.org el 30 de mayo de 2015.

4 PÉREZ LUÑO, Antonio, *Los derechos humanos en las sociedades tecnológicas*, España, Universitas, 2012, p. 23.

la misma, al acceder a la información en tiempo real sin discriminación de ésta. Dicha ventaja ha ocasionado que los Estados se replanteen los alcances del uso de la Red, particularmente de las Plataformas de Participación Ciudadana, y las repercusiones en el ámbito político que esto podría conllevar.

En la práctica, la mayoría de Estados imponen límites a la libertad de expresión, en razón de la censura política, las normas sociales, cuestiones religiosas y por protección del derecho a la privacidad, lo cual no ha sido ajeno a la libertad de expresión en Internet, en donde queda poco claro cuáles son los criterios en relación con la censura de información contenida en plataformas que tienen por objetivo promover la participación ciudadana y sobre todo, difundir información de interés colectivo, lo cual en principio no contraviene los límites internacionalmente aceptados.

Por otro lado, el anonimato de la información final a disposición de los usuarios de Plataformas de Participación Ciudadana, hace que la libertad de expresión resulte atractiva para ejercerse a través de Internet, por lo que vale la pena destacar que las medidas de verificación de la información deben implementarse con particular cuidado.

Cabe mencionar que los límites del derecho a la privacidad de las personas involucradas en la información contenida en las Plataformas de Participación Ciudadana –sobre todo tratándose de servidores públicos–, termina cuando dicha información demuestra ser de interés colectivo, y se haya obtenido derivada del ejercicio de funciones públicas; es decir, como representantes de cualquier órgano de gobierno.

Aunado al anonimato, la forma de publicación ha sido modificada por el uso de Internet, ya que el alcance es mayor y no se circunscribe solo a un espacio específico, sino al acceso en cualquier parte del mundo, lo cual hace nuevamente atractivo el ejercicio de la libertad de expresión en la Red.

Una vez que se ha determinado que Internet constituye una forma novedosa en el ejercicio de la libertad de expresión, se debe mencionar que a la par de la evolución de ésta, han aparecido nuevos métodos de censura a la información contenida en la Red, lo cual vulnera a toda luz la libertad de expresión, afectando la dignidad y la libertad humana.

Dicho lo anterior, analizaremos que la libertad de expresión consagrada en diversos ordenamientos jurídicos, tiene una doble vertiente: individual e institucional.

En virtud de la primera, son derechos subjetivos que otorgan ciertos poderes a personas concretas, y la segunda refiere a elementos básicos para la construcción de la opinión pública, elemento esencial para un régimen democrático⁵.

La libertad de expresión conlleva una diversidad de ideas implícitas en las sociedades democráticas, en donde el individuo debe ser respetado; sin embargo,

5 Véase FERNÁNDEZ RODRÍGUEZ, José Julio, *Op. Cit.*, nota 3, p. 36.

Internet como instrumento tecnológico de la comunicación, en últimas fechas, ha tenido diversos hechos que vulneran la libertad de expresión de los usuarios de la red. Con esto, surge un nuevo planteamiento del problema, en donde Internet es la nueva frontera en la lucha por los derechos humanos, incluida la libertad de expresión.

Hoy en día, la tecnología desempeña un papel primordial en dicha comunicación, y en diversas ocasiones, no es neutral, ya que puede usarse en beneficio o perjuicio de la humanidad⁶.

La tecnología adquiere significación en el contexto al que responde; es decir, un contexto ideológico que escoge opciones y rechaza otras⁷.

La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura UNESCO, por su parte asume la responsabilidad de promover la libertad de expresión en Internet y la ha incorporado en su Programa Ordinario; asimismo, ha establecido que el principio de la libertad de expresión no se debe aplicar únicamente a los medios de comunicación tradicionales, sino también a Internet y todos los tipos de plataformas de comunicación de reciente aparición que contribuyen al desarrollo, la democracia y el diálogo⁸.

A manera de conclusión del presente apartado, el artículo 19 de la Declaración Universal de Derechos Humanos reconoce la libertad de expresión a través de cualquier medio, e Internet no es una excepción, por lo que debe ser tarea de los Estados garantizar el acceso efectivo de sus ciudadanos a la Red y sobre todo, impulsar la participación ciudadana a través de plataformas que efficienten y transparente la actividad estatal.

III. Plataformas electrónicas como forma de participación ciudadana

Existen tecnologías que apoyan los procesos de comunicación e información, que son aquellas que sirven para recolectar, sistematizar y distribuir información entre emisores y receptores⁹.

Uno de los aspectos más importantes en el uso de dichas tecnologías, es la forma en la que se relacionan con la protección a los derechos humanos. En el caso concreto de las plataformas electrónicas de participación ciudadana, han surgido como un fenómeno novedoso que pone al alcance de los usuarios una

6 Véase DÍAZ MULLER, Luis, "Tecnología y derecho a la intimidad: nuevos desafíos jurídicos", *Boletín Mexicano de Derecho Comparado*, México, número 90, 1997.

7 Véase FERNÁNDEZ RODRÍGUEZ, José Julio, *Lo público y lo privado en Internet. Intimidad y libertad de expresión en la Red*, Universidad Nacional Autónoma de México, 2004, p. 33.

8 Consultado el 23 de mayo de 2015 en: <http://www.unesco.org/new/es/communication-and-information/freedom-of-expression/freedom-of-expression-on-the-internet/>

9 DONOSO ABARCA, Lorena, *Derechos humanos y derechos fundamentales en la sociedad red*, Ciudadanas 2020 II, Instituto Chileno de Derecho y Tecnologías, Chile, 2013.

herramienta para el ejercicio de derechos humanos, tales como el de la libertad de expresión y acceso a la información.

Estas plataformas han abierto nuevos canales para expresarse con un alcance y cobertura mayor, por lo que el Estado y las grandes corporaciones tienen interés en que se regule el funcionamiento de las mismas.

La información en las páginas de Internet, suele estar desordenada y sin una comprobación de la veracidad de la misma, por lo que las plataformas de participación ciudadana surgen como una alternativa para poner a disposición de los usuarios, información veraz de interés colectivo, lo que ha otorgado confiabilidad en el uso de las mismas.

Este tipo de plataformas contribuyen al modelo de democracia participativa en donde cualquier usuario puede enviar información que será publicada, una vez haya pasado los filtros de veracidad, lo que a su vez propicia un empoderamiento del ciudadano frente al Estado.

Otro aspecto a destacar de las plataformas de participación ciudadana –como ya se ha dicho– es el anonimato de la información proporcionada, lo que facilita la difusión de ideas en sociedades en donde el temor a la represalia o el terror de Estado implican cierta censura. Esto hace ver a las TIC, particularmente a las plataformas en comento, como liberadoras de ideas e información y como instrumentos de acceso a los derechos humanos.

En este sentido, las TIC han propiciado nuevas formas de ejercicio de los derechos y pueden contribuir a un reforzamiento del tejido participativo de las sociedades democráticas¹⁰.

Dicho lo anterior, analizaremos el funcionamiento de la plataforma de participación ciudadana, denominada Méxicoleaks, la cual ha causado controversia en todos los contextos, al poner en evidencia al Estado mexicano en sus actuaciones.

A. Méxicoleaks

De acuerdo con su página de Internet, esta plataforma tiene como objetivo fungir como herramienta para enviar información de interés público a medios de comunicación y organizaciones civiles a través de tecnologías seguras que garantizan el anonimato de la fuente. Esto, con fundamento en la transparencia y la participación ciudadana para construir en la sociedad la justicia y la democracia.

El éxito en el funcionamiento de esta herramienta radica en que la información una vez recibida es verificada y analizada, y una vez que se ha comprobado la veracidad de la misma, es publicada en los medios de comunicación adheridos a la plataforma.

¹⁰ PÉREZ LUÑO, Antonio, *Op. Cit.*, nota 4, p. 22.

Otro de los objetivos establecidos en la plataforma, es que el impacto de la información revelada sea amplificado al máximo, tanto a nivel mediático como civil y legal.

Aunado a lo anterior, otro elemento a destacar es que los creadores de la plataforma detectaron la seguridad en el proceso de envío como proceso primordial en el funcionamiento de la misma, por lo que ponen a disposición del usuario, un sistema de navegación que no permite localizar la IP de la computadora donde se envía la información. Se debe decir que ponen a disposición del usuario un manual detallado, en caso de requerir información adicional o ayuda en el envío de información bajo esta modalidad.

Como se dijo en apartados anteriores, el anonimato tiene especial influencia en el éxito del envío y publicación de información, por lo que esta plataforma también lo garantiza, a través de mecanismos de software que hacen que la persona que analice la veracidad de la información no pueda conocer la dirección o algún dato que tenga que ver con el envío de la información. En este rubro se debe decir que la seguridad de la información no puede garantizarse al cien por ciento tratándose de programas informáticos; sin embargo, proporciona al usuario la certeza suficiente en materia de seguridad de la información¹¹.

IV. Marco jurídico en relación con la libertad de expresión en Internet

Diversos tratados internacionales prevén en su contenido la libertad de expresión e información. Ejemplo de ello son las siguientes disposiciones:

Artículo 13 de la Declaración Americana de Derechos del Hombre, artículo 8 de la Declaración Universal de la UNESCO, sobre la Diversidad Cultural, entre otros instrumentos internacionales de derechos humanos.

Artículo 19 de la Declaración Universal de Derechos humanos, que dice “todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”¹².

Artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que establece: “1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas, sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.

¹¹ Información consultada el 20 de mayo de 2015 en: www.mexicoleaks.mx

¹² Declaración Universal de los Derechos Humanos. Consultado el 12/06/2012 en: http://www.derechoshumanos.net/normativa/normas/1948DeclaracionUniversal.htm?gclid=COngo7Cz_LACFYsaQgodb30ZcA.

El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.

2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial”¹³.

Artículo 19 punto 2 del Pacto Internacional de Derechos Civiles y Políticos, que a la letra dice: “Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección”¹⁴.

Artículo 13 punto 1 de la Convención Americana de Derechos Humanos: “Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección”¹⁵.

Punto 1 de la Declaración Conjunta sobre Libertad de Expresión e Internet¹⁶, que establece como principios generales los siguientes:

“a. La libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación. Las restricciones a la libertad de expresión en Internet solo resultan aceptables cuando cumplen con los estándares internacionales que disponen, entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad (la prueba tripartita).

b. Al evaluar la proporcionalidad de una restricción a la libertad de expresión en Internet, se debe ponderar el impacto que dicha restricción podría tener en la

13 Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Consultado el 15/06/2012 en:

<http://www.derechoshumanos.net/normativa/normas/europa/CEDH/1950ConvenioProteccionDerechosHumanosyLibertadesFundamentales.htm#a10>

14 Pacto Internacional de Derechos Civiles y Políticos. Consultado el 13/06/2012 en: <http://www.cinu.org.mx/onu/documentos/pidcp.htm>.

15 Convención Americana de Derechos Humanos o Pacto de San José Costa Rica. Consultado el 10/06/2012 en: <http://www.oas.org/juridico/spanish/tratados/b-32.html>

16 Es un mecanismo internacional de promoción de la libertad de expresión en internet, el cual fue adoptado el 1º de junio de 2011.

capacidad de Internet para garantizar y promover la libertad de expresión respecto de los beneficios que la restricción reportaría para la protección de otros intereses.

c. Los enfoques de reglamentación desarrollados para otros medios de comunicación —como telefonía o radio y televisión— no pueden transferirse sin más a Internet, sino que deben ser diseñados específicamente para este medio, atendiendo a sus particularidades.

d. Para responder a contenidos ilícitos, debe asignarse una mayor relevancia al desarrollo de enfoques alternativos y específicos que se adapten a las características singulares de Internet, y que a la vez reconozcan que no deben establecerse restricciones especiales al contenido de los materiales que se difunden a través de Internet.

e. La autorregulación puede ser una herramienta efectiva para abordar las expresiones injuriosas y, por lo tanto, debe ser promovida.

f. Deben fomentarse medidas educativas y de concienciación destinadas a promover la capacidad de todas las personas de efectuar un uso autónomo, independiente y responsable de Internet (alfabetización digital)¹⁷.

El ordenamiento en comento, marca una pauta importante, ya que reconoce que el principio de libertad de expresión no se debe aplicar únicamente a los medios de comunicación tradicionales, sino también a Internet, ya que es éste, el que suministra un volumen sin precedentes de recursos para la información y el conocimiento, y abre nuevas oportunidades de expresión y participación.

Asimismo, diversas constituciones garantizan el derecho a la libertad de expresión en los países democráticos; en el caso de México, son los artículos 6º y 7º de la Constitución Política de los Estados Unidos Mexicanos.

En este sentido, se está iniciando un movimiento de la doctrina jurídica y de la jurisprudencia de los países con mayor grado de desarrollo tecnológico tendente al reconocimiento del derecho a la libertad informática y a la facultad de autodeterminación en la esfera informativa¹⁸.

V. Medidas de censura contra la libertad de expresión en Internet

El ejercicio de la libertad de expresión en Internet, ha causado severos problemas a los Estados, por lo que algunos de ellos han emprendido acciones de censura para controlar la información que circula en la Red, particularmente para el caso concreto, la información contenida en las Plataformas de Participación Ciudadana.

En un contexto internacional, algunas autoridades han clausurado y confiscado servidores, como es el caso de Italia. Otro ejemplo de ello son países como China o Afganistán, en donde un conjunto de leyes, controles policiales e

17 Declaración Conjunta sobre Libertad de Expresión e Internet. Consultado el 27/06/2012 en: <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&IID=2>

18 PÉREZ LUÑO, Antonio, *Op. Cit.*, nota 4, p. 23.

infraestructura de telecomunicaciones han hecho que se controle la información a la que acceden sus ciudadanos.

Se puede discutir acerca de la eficacia de esos controles, pero no de su existencia ni de sus consecuencias, entre las cuales, se encuentran: páginas web y servidores cerrados, espacios de Internet poco accesibles, e incluso internautas encarcelados.

En el caso de México, la plataforma de participación ciudadana denominada Méxicoleaks, ha sufrido acciones que buscan instrumentar nuevas formas de censura hacia la información que podría difundirse a través de las mismas. Estas acciones de censura, no siempre van encaminadas al control de la información en la plataforma misma, sino que pueden ir más allá con el amedrentamiento a periodistas para que no impulsen la creación, desarrollo y uso de las mismas.

En este sentido, es importante destacar que la reciente Ley General de Transparencia y Acceso a la Información Pública de México, sancionará a aquel servidor público que use, sustraiga o divulgue sin causa legítima, la información que se encuentre bajo la custodia de otros servidores públicos o a la cual tenga acceso o conocimiento con motivo de su empleo, cargo o comisión¹⁹. Derivado de lo anterior, se observa que el concepto de causa legítima es subjetivo, quedando a la libre interpretación.

A continuación hablaremos de las medidas instrumentadas por los gobiernos, que en un contexto nacional o internacional, vulneran en mayor o menor medida la libertad de expresión en la red.

Dichas medidas, las dividiremos en dos:

- a) Medidas adoptadas por las empresas privadas o por los usuarios de la red, y;
- b) Medidas utilizadas por los gobiernos, ya sea en un contexto nacional o internacional.

Para el caso de las medidas adoptadas por los gobiernos, encontramos en documentos como ACTA (Acuerdo Comercial Antifalsificaciones), TTP (Acuerdo Transpacífico de Cooperación Económica) y el Convenio sobre la

¹⁹ Artículo 206. La Ley Federal y de las Entidades Federativas, contemplarán como causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, al menos las siguientes:

...
IV. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, sin causa legítima, conforme a las facultades correspondientes, la información que se encuentre bajo la custodia de los sujetos obligados y de sus Servidores Públicos o a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
...

Ciberdelincuencia (Convenio de Budapest), disposiciones que podrían vulnerar en mayor o menor medida la libertad de expresión de los usuarios de Plataformas de Participación Ciudadana.

En el caso de México, la reciente reforma en materia de telecomunicaciones, dota de facultades a las autoridades para intervenir medios electrónicos, lo cual podría derivar en una violación de derechos humanos, particularmente en el caso de la libertad de expresión en la Red²⁰.

En este sentido, la reciente iniciativa de la Ley Federal para Prevenir y Sancionar los Delitos Informáticos, incluye la definición de “terrorismo informático” como la difusión de información con el objetivo de causar pánico y desestabilización de la paz pública, lo cual tendría una sanción. Desde esta óptica, cualquier información divulgada a través de las plataformas ciudadanas de participación, podrían considerarse como terrorismo informático²¹.

VI. Conclusiones

La libertad de expresión es un derecho humano, reconocido y consagrado en la mayoría de Constituciones de los gobiernos democráticos; sin embargo, hay un evidente retroceso en este campo, ya que bajo diversas justificantes, la libertad de expresión de los usuarios de Internet es vulnerada.

Se deben generar mecanismos de equilibrio entre el avance de las TIC y la efectiva protección de los derechos humanos.

Las Plataformas de Participación Ciudadana, constituyen un nuevo modelo de transparencia y supervisión del ejercicio estatal.

La libertad de expresión en Internet ha empoderado al ciudadano frente a actos del Estado, lo cual contribuye a la construcción de una sociedad más justa, con menores índices de corrupción.

La libertad de expresión en Internet colabora con la democracia de los países; asimismo cumple con la función de poner a disposición de los usuarios información para la toma de decisiones responsable e informada.

²⁰ De acuerdo a información de la Red de Defensa de los Derechos Digitales, una investigación de Joanna Zuckermann y Christine Murray señala que en 2014, las solicitudes de información por parte de representantes del Estado Mexicano sobre llamadas telefónicas incrementó a 55 mil, un aumento de 25% respecto a 2013. Esta subida coincide con la entrada en vigor de la Ley Federal de Telecomunicaciones, que preocupa tanto a activistas como a las mismas empresas proveedoras de servicios. Información disponible en:

https://r3d.mx/2015/10/15/aumentan-solicitudes-de-datos-a-telefonicas-a-raiz-de-la-leytelecom/?utm_content=bufferc3280&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer

²¹ Consultado el 30/10/2015 en: https://www.fayerwayer.com/2015/10/la-absurda-y-peligrosa-leyfayad/?utm_content=bufferaa7be&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer

Datos abiertos, ¿derecho humano?, ¿política pública? o ambas cosas

Marcelo Bauzá*

SUMARIO: 1. Tecnologías y espacio jurídico. 2. El derecho a la vuelta de la esquina. 3. Qué son los “datos abiertos”. 4. Acercándonos al cuerpo jurídico de la noción. 5. Una línea dicotómica. 6. Datos abiertos en la línea de los Derechos Humanos. 7. Técnica y libertades: un doble examen. 8. Paradigmas jurídicos beneficiados con los datos abiertos. 9. Principios a tener en cuenta. 10. La situación uruguaya en la materia. 11. Conclusiones.

Resumen

El presente trabajo analiza desde una óptica jurídica el uso en forma libre y abierta de los datos públicos. El estudio del tema se enfoca en una doble perspectiva: como parte de los derechos humanos vinculados a los derechos de información y comunicación, y como una estrategia que impulsa el gobierno y administración en línea, con el fin de optimizar el uso de la información pública y proporcionar un mejor servicio a la ciudadanía. A título de ejemplo se hace una referencia a la situación uruguaya en esta materia.

Palabras clave: Datos abiertos. Derechos Humanos. Políticas públicas. Gobierno electrónico.

Abstract

This paper analyzes from a legal view the free and open use of public data. The study is focused in two main features: as part of human rights, linked to the right to information and communication, and as a strategy promoted by the government and administration online, in order to optimize the use of public information and provide better services to citizens. A reference to the situation in Uruguay regarding to this matter is given as an example.

Keywords: Open Data. Human rights. Public politics. E-government.

Aceptado por el Comité Académico para ser presentado en el XIX Congreso Iberoamericano de Derecho e Informática celebrado en Medellín, agosto 2015. Aprobado por la Junta Directiva de FIADI para ser publicado en la *Revista Derecho y Tecnología*, el 13 de octubre de 2015.

* Director del Instituto de Derecho Informático de la Facultad de Derecho (UDELAR-Uruguay). Ex Vicepresidente de FIADI www.fiadi.org. Profesor Adjunto de Informática Jurídica (UDELAR-Uruguay). Profesor de Ética Profesional en la Carrera de Ingeniería Informática (UDE-Uruguay). Profesor del Diploma en Fundamentos de Informática Médica (UDE-Uruguay). Ex Asesor Letrado I de AGESIC periodo 2008-2014.

1. Tecnologías y espacio jurídico

No se dice nada original cuando se afirma que el desarrollo digital en la sociedad contemporánea continúa incrementándose de forma exponencial, y que muchos indicadores muestran que así será también en el devenir. Tampoco se descubre nada nuevo cuando se constata el modo periódico y regular en que aparecen nuevas corrientes, nuevas tendencias, y nuevos colectivos humanos (de expertos o simplemente de interesados en el asunto de que se trate) en pos de cierto tipo de realizaciones de alcance social, más un largo etcétera alrededor del uso de las TIC en la sociedad.

Es lo que sucede también con los *datos abiertos*. Sin embargo hablar de «datos abiertos» en un foro jurídico implica un cierto grado de compromiso, una cierta responsabilidad y si se quiere una especie de prevención. Al menos yo me hago cargo del tema dentro de este tipo de enfoques. Porque para conocer la parte tecnológica del mismo tema, incluso su lado organizacional tanto o más importante que el anterior, hay que ser especialista en tecnologías y en gestión en las organizaciones en su caso, competencias ambas que no poseo.

Este tema, como tantos otros de la sociedad digital (el gobierno y administración electrónicos hacen parte del mismo paradigma), nacen bajo la estrella del desarrollo de la sociedad de la información y el conocimiento, al que se suma el cambio de los procesos burocráticos estatales, a partir todo ello –sobre todo lo segundo– de las políticas públicas emanadas de institucionalidades relativamente recientes, creadas con tal propósito, por ejemplo en nuestro país, Uruguay, la AGESIC.

Como tal los “datos abiertos” constituyen también un tema multidisciplinario. Un tema que posee algunos focos y ciertas improntas de rango jurídico, sin llegar a configurar el elemento central que les da vida y movimiento según me apresuro a señalar desde mi percepción y experiencia.

Hay pues una responsabilidad en cuanto a encuadrar y transmitir lo que uno pueda más o menos conocer del asunto, pero haciéndolo dentro de las limitantes expuestas. Lo que en otras palabras supone concentrarse en aquello que sí puede y sí debe aportar el Derecho.

Para eso hay que desbrozar el análisis, y ponerle foco a lo nuestro, a lo jurídico, dejando que otras disciplinas y otras experiencias, se ocupen del resto del asunto. Es lo que yo me propongo hacer en esta comunicación, o al menos intentarlo: hablar más de Derecho y menos de gestión y tecnologías; solo lo suficiente de lo segundo como para entender mejor lo primero.

En éste como en tantos otros asuntos propios de la actual sociedad contemporánea, que vienen promovidos a partir del uso incremental de la técnica, se aprecia un mismo y curioso fenómeno: mucha gente actuando, proveniente de diversos campos de formación y experiencia, con mayor o menor cuota de intervención, analizando, opinando y contribuyendo al afianzamiento real de este tipo de desarrollos en la sociedad real, a partir de iniciativas genéricas

originadas e impulsadas, por lo general, desde fuera de fronteras, a las que el país se supone que no puede darle la espalda.

No nos enojemos con esta sempiterna foraneidad, ni tampoco nos asombremos más con este tipo de constataciones. Es el síndrome de la sociedad global en que nos hallamos inmersos, y propiamente de la “sociedad-red” en que nos ubica CASTELLS. Todo está enlazado. Pero eso no quita la necesidad, a mi juicio, de tomar conciencia del espacio propio en que nos toca movernos, profundizar y tratar de incidir. Y tampoco quita la necesidad de ser conscientes de los límites de este espacio, de que no lo ocupamos todo sino que estamos acompañados. Este tipo de balances es el precio para evitar convertirnos en inmutables o insensibles ante el cambio de la sociedad si vamos por lo primero rebajando la nota propiamente jurídica al tratar el asunto, o en opinólogos rudimentarios si avanzamos en lo segundo vale decir en caso de invadir terrenos para los que no hemos sido formados.

En resumen, no son los juristas los que están en primera fila en esta tarea, pero que tampoco se piense lo inverso, o sea que no hay ya nada que aportar desde el campo jurídico.

2. El derecho a la vuelta de la esquina

El Derecho en tanto ciencia y obrar resulta un instrumento formidable de ingeniería social, siempre que se lo conciba y se lo aplique con inteligencia y realismo. El Derecho es, además, una disciplina insoslayable de conocimiento y observancia, puesto que siempre tiene algo que ver con la mayoría de los asuntos humanos.

Me voy a permitir extenderme de modo breve sobre este necesario rol, y sus límites, ya ubicados dentro de la cuestión Informática, Estado y Sociedad. Lo hago a partir de una cita tomada de un modesto documento que ambientara un “llamado de comunicaciones” a uno de los tantos congresos que se celebran sobre estos temas en distintos puntos del planeta, y que permanece hoy día publicado en la web, librado a la consulta pública. Me refiero en este caso a un Congreso celebrado en la Facultad de Derecho la Universidad de Murcia el año pasado, donde también me apresuro a decir que no estuve presente ni tenía remota idea del mismo hasta que encontré este pequeño texto revisando Internet (“gugleando” como decimos todos hoy día) en procura de armar esta contribución con cierta consistencia.

La cita me ha parecido muy ilustrativa sobre cómo debemos auto limitarnos y auto referenciarlos la gente de Derecho, cuando aspiramos ocuparnos de los asuntos de la Sociedad Digital por el lado de nuestras competencias propias, o sea las competencias jurídicas.

Es evidente que, frente al enorme portento que han adquirido estas temáticas en los últimos veinte años, hemos quedado descolocados –si alguna vez estuvimos mejor– para abordarlas en todas sus facetas. Pero a la vez se nos pone por

delante aquello en lo que sí debemos intervenir, y que a nadie más que a la gente de Derecho, le sigue correspondiendo abordar en profundidad. He ahí la buena senda para quien se diga especialista en Derecho Informático, o aspire serlo. Ahora cito sin más preámbulo el documento español de referencia:

El actual desarrollo de la tecnología permite que la gestión de la información administrativa se pueda convertir en un instrumento esencial para la transformación de las estructuras y el funcionamiento de las Administraciones Públicas, de manera que se facilite el incremento de la eficacia y de la eficiencia. Sin embargo, dicho proceso no puede suponer un menoscabo de las garantías jurídicas; más aún, el Derecho está llamado a cumplir un relevante papel en la medida que la tecnología permite reforzar el cumplimiento de las exigencias normativas». *Llamada a comunicaciones. Congreso Derecho TICs-SICARM 2014. Facultad de Derecho de la Universidad de Murcia. 23 y 24 de octubre de 2014.*

El origen y brevedad la cita no empañan, a mi juicio, la exactitud e importancia del pensamiento que anida detrás de ella. Se está diciendo, y comparto, que no podemos ocuparnos de todo el edificio. Pero al mismo tiempo se está diciendo que sí debemos ocuparnos de lo que necesariamente nos compete, posiblemente uno de sus cimientos, e incluso que deberíamos hacerlo bajo una impronta optimista de concebir un Derecho positivo en la materia, destinado a “reforzar el cumplimiento” normativo a través de las tecnologías, cuestión que no siempre se aprecia así en la realidad, tanto desde dentro como desde fuera de nuestras filas.

O sea que el Derecho, al fin y al cabo y como se lo mire, debe mezclarse y comprometerse en estos procesos de cambio social por vía de las tecnologías. Yo diría que debe hacerlo casi que en forma militante, por la importancia de lo que está en juego. Esa es la manera de estar a la altura de su rol y cumplirlo a cabalidad, articulando las nuevas realidades con el requerido respeto y desarrollo de los derechos humanos involucrados en tales procesos.

Quiero agregar que no me encuentro en las filas de los que creen que el Derecho solo debe ser el gendarme garantista ante cualquier fenómeno con vocación a ser regulado por la norma jurídica. Debe serlo sí, pero también debe ser otras cosas más. Un Derecho exclusivamente represor y controlador, no va con mi forma de ser ni con mi formación profesional. Tengo para mí que el Derecho en la Sociedad y el Estado actuales, de cara las TIC y sus procesos constantemente en aumento, un Derecho bien concebido y mejor aplicado, es necesario que agregue múltiples funciones igualmente importantes y benefactoras que se suman a la primeramente nombrada. El Derecho le sirve a la Sociedad Digital como promotor y facilitador de las nuevas realidades sociales a las que aquella abre rumbo y destino. Existen iniciativas múltiples y procesos encontrados en todo este formidable avance, todo lo cual pugna por abrirse camino con apego al uso de TIC. El Derecho puede y debe contribuir a facilitar todo esto.

Y también a regular, a poner orden, paz y seguridad entre los actores que intervienen, siendo muchos los terrenos a intervenir bajo esta impronta por más que –curiosamente– se asiste al mismo tiempo al discurso no regulador de Internet.

Pero claro está, todas estas otras funciones no pasan por arriba a la primera, la de poner freno ante el desborde o conculcación de un derecho subjetivo por medio de la técnica. Y sin desmedro de la importancia de todas ellas, a cierta hora se emparejan o encolumnan como funciones que también están al servicio de la primera o, por lo menos, actúan y devienen siempre con alineamiento y respeto, a la función garantista.

Hay que ser conscientes y atentos, así, del alcance y límites de nuestro rol. No somos, ni de cerca (me refiero a los cultores del Derecho en todas sus especialidades, incluyendo el Informático), los que estamos construyendo las nuevas tendencias y realidades del instrumento tecnológico volcado al espacio social; por ende no podemos derivar nuestra participación o protagonismo hacia todas las instancias, métodos de trabajo, etc. que presenta este terreno y tantos otros emparentados, porque no nos corresponde hacerlo. Sin embargo las realidades están ahí y constituyen el objeto de nuestra atención, por lo cual tampoco nos podemos ir al extremo de que nos resulten ajenas. Debemos preocuparnos por conocerlas lo mejor posible, por entrar al suficiente examen de ellas, pero también por terminar poniendo lo nuestro, aquello de lo que nunca debemos abdicar so pena de reducir o desconocer nuestra verdadera función, la de analizar y evaluar el fenómeno pero siempre bajo la lupa del principio o la norma jurídica, que ya es bastante.

3. Qué son los “datos abiertos”

Se trata de uno de los movimientos (nos tienta aludir a “movidas” pero puede parecer descalificador y no es nuestro propósito) que emergen dentro del prolífico universo de las redes de información y comunicación globales en el mundo actual. El tema se ha instalado en diversos escenarios tanto de organismos públicos como de la sociedad civil, adquiriendo prestancia suficiente como para convertirse en una de las varias Políticas de Estado en numerosos países que se ocupan de la Sociedad de la Información y el Conocimiento así como del Gobierno y la Administración Electrónicos. Incluso representa una de las políticas específicas más claras en cuanto a propender a un ligamen y participación entre el Estado y la Sociedad Civil, si se las compara con otros temas de gobierno y administración electrónicos más proclives a volcarse hacia uno u otro sector.

El movimiento o tendencia en examen aboga por utilizar en forma libre y abierta los datos que están en la órbita de los organismos estatales y semi estatales, a través de iniciativas y proyectos que surgen tanto de las propias entidades públicas como de la iniciativa privada.

Sin perjuicio de este rasgo o definición básicos, el tema reposa en varios fundamentos, y hasta en optimistas promesas cuya decantación en la realidad actual no siempre aparece clara y completa, advirtiéndose la relatividad del fenómeno en reflexiones rotundas como las de Fabrizio Scrollini, estudioso fuertemente dedicado a estos temas y Coordinador de la Iniciativa Latinoamericana de Datos Abiertos: “Solo abrir un dato nunca cambió la realidad de nadie, ni redujo la brecha de desigualdad. Solo abrir un dato por sí mismo no hace eso. Milagros no hay...”. En igual medida de parsimonia se mueven algunos Informes de Tendencias como el español que a continuación citamos: “A pesar de que el Open Data es un concepto que ha venido ganando cada vez mayor atención, su auténtico potencial está todavía empezando a descubrirse”.

Parece advertirse, entonces, que este asunto requiere de su prueba de fuego en cuanto a lograr una aceptación en la sociedad real que termine por darle crédito en términos de utilización efectiva de las nuevas aplicaciones creadas a partir de utilizar datos abiertos.

En ese camino se está, no lo negamos. Pero mientras tanto, no pasa de configurar una de las varias políticas o desiderátums de la sociedad digital, con resultados a constatarse. Una política que también aprovecha y se encauza mediante el apoyo e impulso de institucionalidades estatales funcionales al tema (me refiero al espacio orgánico del gobierno y la administración electrónicos), llamada a probar su eficacia real en términos de la calidad y volúmenes que vayan adquiriendo las iniciativas y realizaciones concretas en la materia.

4. Acercándonos al cuerpo jurídico de la noción

El concepto profundo conocido bajo el nombre de “datos abiertos” (*open data* en inglés) remite en última instancia a una filosofía y una práctica basadas en uno de los pilares de los derechos fundamentales. Se trata de un pilar de todas las épocas, o podríamos decir que claramente instalado a partir de la Revolución Francesa, que se amplifica y adquiere ribetes propios en el contexto actual de una sociedad post industrial sometida al constante influjo de las Tecnologías de Información y Comunicación, con repercusiones sociales a veces inmediatas, a veces lanzadas hacia el porvenir bajo perspectivas de imposible pronóstico definitivo.

Referimos al pilar de la libertad, y más concretamente el pilar de la libertad de información, que tiene muchas formas y fórmulas de ejercicio. Basta pensar que esta libertad de información se ha ido construyendo y afirmando a través de instrumentos de *mass media* y en sucesivas capas históricas. Estas capas se han ido agregando sin anularse unas con otras, pero sí sacudiendo y modificando el edificio en su conjunto. Ayer fue la prensa, primero escrita, luego oral y radiotelevisiva. Hoy día es Internet y todo lo que permite, habilita y

estimula el medio para favorecer el acceso y utilidad de la información a favor de toda la población.

Para no ir demasiado lejos con este tipo de reflexiones, digamos que esta filosofía o práctica denominada “datos abiertos” alude a un movimiento de ideales, a unos desafíos asumidos en pos de un determinado objetivo social a todas luces benéfico: hacer que los datos públicos terminen por estar disponibles y en manos de sus titulares, los administrados, el pueblo si se quiere. Para que ello ocurra sin tropiezos se debe operar en los terrenos informativos donde no existen restricciones de derechos de autor, patentes u otros mecanismos de control. Incluso se deben superar, entre otros fenómenos, ciertos atavismos fuertemente instalados en la cultura burocrática, como “secretismo estatal”.

Se trata de abonar el conocimiento universal y sin barreras de ningún tipo, salvo las estrictamente necesarias, que coinciden con las especificadas en las leyes de acceso a la información pública (ej. nuestra ley 18.381 del 2008 cuando trata las informaciones reservadas y confidenciales como excepción a la regla del carácter público de la información en manos del Estado y entidades públicas en general).

Bajo esta óptica, la temática en examen dispone de una plataforma de lanzamiento ético similar a la que disponen otros movimientos y comunidades que pugnan por “lo abierto” en aras del progreso cultural y científico, como son el software libre, el código abierto (*open source* en inglés) y el acceso libre (*open access* en inglés).

5. Una línea dicotómica

Desde la visión centrada en el individuo y sus derechos, el tema de los “datos abiertos” ubica, así, su mojón propio. Y lo hace en la línea del desarrollo y el afianzamiento históricos de los derechos humanos vinculados a la información y comunicación, adonde pertenecen el derecho de información lato sensu, el derecho al conocimiento y la cultura de los pueblos, el derecho también de los pueblos, pero más concretamente de los administrados, a la buena gestión por parte del Estado, operadores y responsables de la cosa pública.

Siempre en el plano jurídico, pero en este caso atendiendo otros valores que no afinan exclusivamente en el espacio de los DD.HH., el movimiento de los datos abiertos se inserta también en la línea de propender a la transparencia de la *res* pública, y el combate contra la corrupción de gobernantes y administradores de todo nivel.

Pero no son éstas, las jurídicas, las únicas visiones del mismo fenómeno. Para quienes proponen, orientan y, en definitiva, edifican las políticas públicas de cada país en materia de “sociedad de la información y el conocimiento”, lo cual engloba lo concerniente al propio aparato estatal (portales aglutinadores y simplificadores de suministros informativos y consecución de trámites, etc.), la misma cuestión es abordada muchas veces como una *estrategia*. Una estrategia

¿para qué? La respuesta expresada por sus propios impulsores es que los datos abiertos son una de las estrategias que existen para favorecer el gobierno y administración en línea.

Esta última visión está presente en todas las institucionalidades nacionales e internacionales que se ocupan del tema. Por ejemplo entre otras, es lo que surge de los lineamientos en la materia elaborados por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, que considera el “gobierno en línea” como “estrategia de buen gobierno”, y a su vez ocupándose del «modelo de datos abiertos» en orden ajustado a la referida estrategia, poniendo como fundamento de este ligamen entre sucesivas estrategias, la afirmación de que aquel modelo “*permite operativizar y administrar la oferta y demanda de los datos de acceso público que actualmente poseen las entidades del Estado Colombiano*”.

De manera que tenemos dos visiones, me animaría a decir que al estilo de la mayoría de los asuntos que hacen al Gobierno y Administración Electrónicos. La visión apegada a los DD.HH. por un lado, y la visión si se quiere burocrática o tecnocrática, vinculada en este caso a los hacedores de planes y mejoras en el aparato estatal y la sociedad, a través de las TIC.

Una aparente dicotomía que existe pero que no debe asustar, en principio. No debe verse a priori una contradicción forzosa entre ambas visiones, una jurídica, otra política. Lo que debe intentarse es que ninguna fagocite a la otra, en especial que la visión tecnocrática no se trague o mal utilice a la visión jurídica.

6. Datos abiertos en la línea de los Derechos Humanos

Para no ir más lejos, digamos que bajo la expresión “Datos Abiertos” (Open Data) anida el

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

El planteo, que es muy cierto y descriptivo, me hace acordar a esos juegos de mesa donde el jugador en cierto momento recibe la mala nueva de “retroceda dos casilleros”. ¿Por qué digo esto? Lo digo porque si la información es pública SIEMPRE debió estar a disposición de los ciudadanos en forma reutilizable, sin necesidad de que ahora viniera la moderna concepción y política de los datos abiertos a sustentarlo.

Es decir que aquí no hay nada nuevo, al menos del punto de vista de la alta teoría jurídica. No nos confundamos ni adormezcamos. El mandato jurídico

profundo siempre estuvo, otra cosa es que se lo llevara a la práctica. Nos parece que este mandato viene desde fondo de la más entrañable teoría del Derecho y la justicia, o sea el hecho de que el Estado abra al público sus fondos informativos cuando éstos no tienen el carácter exceptuado de ser secretos o reservados, también conforme a derecho.

Pero está muy bien que se haya venido postreramente, posiblemente cuando el estado de avance de la tecnología y su repercusión social lo permitieron, a reconocer y desenvolver un derecho que ya existía, mediante el expediente posibilitador de su práctica eficaz, esto es la nueva categorización de los datos abiertos. Al fin y al cabo es la misma concepción naturalista que impera ante cualquier derecho que merezca arribar al nivel de DD.HH.: son todos derechos *preexistentes* a los que en determinado momento histórico se les da un reconocimiento y operatividad que en muchos casos no disponían con anterioridad.

El caso es que no puede, no debe, ocultarse, que la doctrina del dato abierto enlaza con las mejores tradiciones de afianzamiento progresivo en los Estados y Sociedades, del Derecho de Información. Si no lo hiciéramos, estaríamos actuando con una ligereza impropia.

Detengámonos un poco en este proceso, no del punto de vista histórico que nos llevaría un largo análisis, sino del punto de vista de los pocos pero esenciales conceptos nucleares, que demuestran el constante afianzamiento y desarrollo que ha merecido este Derecho o Libertad de Información.

Según URIOSTE BRAGA

...de las distintas categorías de información derivan diferentes posibilidades de relaciones interindividuales. Así, la información privada tiene una difusión limitada a la tutela que decida su titular, quien será en definitiva quien disponga su medida de alcance. Mientras que en la información pública nos encontramos con una disposición abierta, pues ella, por su naturaleza, está disponible para cualquier receptor que pueda y quiera acceder a la misma. En este caso el acceso dependerá de la voluntad del receptor, que además decidirá si su actitud será meramente pasiva o se transforma en activa, mediante la búsqueda y posterior difusión.

Todo esto está contemplado en los grandes pactos internacionales, por mencionar a los más conocidos la Declaración de DD.HH. de 1948 y la Convención Americana sobre DD.HH - Pacto de San José de Costa Rica, bajo la apretada consigna de «libertad de buscar, recibir y difundir informaciones e ideas». Ni que decir que esta libertad se constituye también en pivote referencial e impostergable de otros derechos, como son el “*tomar parte libremente de la vida cultural de la comunidad, a gozar de las artes y a participar en el progreso científico y en los beneficios que de él resulten*”, previsión que también contienen los pactos internacionales mencionados, en particular la Declaración de 1948.

Tendrían que venir otras oleadas siempre vinculadas con el “derecho de información”, para completar y sobre todo para mejorar su ejercicio (porque a mi concepto ya estaba todo dicho de entrada, solo había que mejorar la efectividad). Es así que aparece el más moderno “derecho de acceso a la información pública” y la llamada “transparencia administrativa”, ambas de la mano para obtener mejores resultados aún, en este portentoso andamiaje entre derechos, deberes y obrares públicos.

Recordemos que en nuestro Derecho positivo esta nueva dimensión del derecho de información constituida por el “derecho de acceso a la información pública”, viene definida por el legislador en el *Artículo 3° de la Ley N° 18.381 (Derecho de acceso a la información pública)*.- *El acceso a la información pública es un derecho de todas las personas, sin discriminación por razón de nacionalidad o carácter del solicitante, y que se ejerce sin necesidad de justificar las razones por las que se solicita la información.*

Y es de recordar también, que el “derecho de acceso a la información pública” encarta no solamente a ese derecho en tanto derecho subjetivo, facultativo de ser ejercido o no por su titular, sino además un conjunto de obligaciones o cargas de las administraciones públicas para adelantarse al ejercicio de este derecho, publicando de oficio una serie de informaciones sin esperar al ejercicio de aquél derecho subjetivo particular. Es la llamada “transparencia activa” (art. 5 de la Ley).

A nuestro entender, la doctrina y política de datos abiertos configura de alguna manera otra vía de ejercicio de la transparencia activa, o más bien la generalización de ésta a su máxima expresión desde el momento que la información estatal, no siendo secreta o reservada, debe publicarse, toda ella y en formatos reutilizables.

En asuntos de Derecho vinculados a las Tecnologías de Información y Comunicación con destino al gran público y la sociedad en su conjunto, resulta ser de este modo una buena guía pensar las cosas de cara a “la persona”. Se trata de una postura que prácticamente va de la mano con pensar en clave de “derechos subjetivos” todos los fenómenos sociales, en este caso de derechos apoyados y mejorados en su ejercicio por vía de la tecnología.

Los datos abiertos pueden hacer del mundo un lugar mejor» apologizan algunos analistas como Kevin MERRIT, director general de Socrata, la empresa que hizo posible la ya mítica Data.gov en EEUU, pionera del tema.

Frente a este tipo de afirmaciones no podemos olvidar que nuestro universo jurídico persigue el mismo objetivo, y eso le lleva a tener que ocuparse y encontrarse con esta clase de movimientos, de alcance mundial.

Por lo tanto una buena impronta para ponerle foco jurídico al tema, es ocuparse del qué, e inmediatamente luego del mejor cómo de esta nueva concepción –quizás no tan nueva– del dato abierto.

7. Técnica y libertades: un doble examen

Hablar de “datos abiertos” como política de Estado dirigida a estimular la cultura digital y la participación de la sociedad en emprendimientos y servicios que ya no quedan en manos exclusivas de los administradores públicos, es hablar derechamente de “tecnología y libertades”.

El gobierno electrónico, y desde luego uno de sus segmentos más pujantes como es la Administración electrónica, resultan de difícil entendimiento –y sobre todo de difícil aceptación– si desde su concepción inicial, y su aplicación consecuente, no pasan por este cerno de las libertades y los derechos de las personas.

Esto es parte del escenario actual de la gobernanza, que al menos a mí no me gusta seccionarla en “electrónica”, porque no concibo en este punto la tecnología como factor predominante sino como factor integrado junto a otros elementos. Es por ello que prefiero hablar de “gobernanza” a secas, entendiéndola como ese vasto plan de organización y acción, multidisciplinario y completo, apostado a la conducción de los asuntos públicos, de una manera no autorreferencial sino de una manera relacional y multidireccional, orientada hacia la calidad y la eficacia de la gestión pública en toda la extensión que la democracia y el republicanismo merecen.

- El caso es que el respeto y el mejor ejercicio de las libertades, su conceptualización y su análisis a cualquier efecto, son insumos insoslayables para cualquier plan de mejoramiento de la sociedad. No pocos casos (hasta podría decirse que en todos los casos en última instancia), ésto que se denomina “libertad” (en todas sus expresiones, incluyendo la libertad de información), casi que constituye la propia misión o designio de dichos planes.

- De cara a las tecnologías, tenemos pues a las libertades, que son postulados a respetar y procrear dentro del Estado Democrático y Social de Derecho, tanto por los gobernantes y administradores como por los gobernados y administrados. Las tecnologías liberan, promueven, mejoran la condición humana. Pero esas mismas tecnologías requieren en paralelo a su desenvoltura, del marco jurídico que las encaucen, sobre todo cuando afectan las libertades y derechos de las personas.

En todo este proceso de encuentro entre Sociedad, Tecnologías y Derecho, las libertades poseen o adquieren dos facetas o cuños, que dan respuesta o continente al uso altamente diseminado y socializado de las tecnologías:

- 1) El cuño si se quiere negativo o de defensa, representado por aquellas reglas de derecho destinadas a mitigar o contrarrestar los avances perniciosos de la técnica por sobre rasgos básicos de la personalidad humana (intimidad, honor, expresión, protección de su imagen y datos, etc.).

2) El cuño si se quiere positivo, manifiesto en lo que nos importa ahora destacar con relación al aspecto prestacional del Estado, en tanto cumplidor de cometidos y dador de servicios. Esta segunda función estatal, ya no de control o represiva, genera una contrapartida de demandas concretas del individuo. Demandas para poder vincularse mejor que en el pasado con el prestador estatal, e incluso con sus pares miembros de la sociedad, y con ello poder mejorar su condición de bienestar. En este caso nos encontramos ante *“la informática actuando al servicio del hombre, y no como restrictiva de los derechos fundamentales”* (LIMBERGER).

Es entonces en este segundo cuño, el relativo al rol prestacional del Estado, donde se ancla el concepto de “ciudadanía” y más concretamente la llamada “ciudadanía digital”. Términos de dudosa imposición todavía en el lenguaje científico, cuyos significados ya están impuestos de muy anterior data tanto en Ciencia Política como en Derecho bajo determinados caracteres, no necesariamente coincidentes con el alcance que ahora se le pretende dar. Pero igualmente son conceptos que están siendo utilizados en los ámbitos donde se promueve y construye el gobierno electrónico (pensemos por ejemplo la Carta Iberoamericana de Gobierno Electrónico), e incluso son tratados por alguna doctrina especializada aunque incipiente si se la compara con otros aspectos del gobierno electrónico.

8. Paradigmas jurídicos beneficiados con los datos abiertos

Queda claro así, que el tema de los “datos abiertos” es uno de esos temas que, al menos para mí, despierta la curiosidad de establecer los hilos conductores, que alumbran y justifican la reflexión jurídica.

Estos hilos son varios. Es sabido que el movimiento nace de la mano de la concepción del “gobierno abierto” a partir o fundamentalmente apoyado en iniciativas del Gobierno Obama.

También es cierto que la cuestión posee amplias resonancias y vínculos con otros movimientos y filosofías cercanos, en este caso provenientes de la sociedad civil, como son el software libre y el *open acces*.

Sin embargo, la cuestión que nos ocupa adquirió rápidamente perfiles propios, en tanto política específica generada desde los ámbitos estatales hacia la sociedad, pretendiendo generar una cultura de reutilización de la información pública. Objetivo ambicioso, por cierto. De ahí ciertas prudencias señaladas antes en este mismo trabajo.

Para comenzar es necesario preguntarse, ¿es este un tema más dentro de una larga cartera de iniciativas sociales, culturales o políticas, que han venido generándose en la sociedad de la información por décadas? En otras palabras más crudas si se quiere, ¿estaremos ante una moda, como tal pasajera, entre las tantas que nos ofrece la sociedad tecnológica?

La respuesta que nos merece esta interrogante de partida es que no se trata de una moda pasajera, sino de algo enraizado en otros postulados subyacentes, en otros justificativos arraigados ciento por ciento en claves de entendimiento más profundas.

Es por ello que nos parece oportuno recalcar en ese lecho sobre el cual yace y se desarrolla el tema de los datos abiertos, que supone la concepción e instalación efectiva en la sociedad, de sistemas de información que miran y responden a las necesidades y aspiraciones del ciudadano.

Llegados a este punto nos encontramos con dos grandes tópicos. Nos encontramos con el buen hacer de la Administración, pero al mismo tiempo nos encontramos también con el “derecho subjetivo” por no tildarlo de entrada –según creo correspondería hacerlo– de DD.HH.

Poner a trabajar en el terreno social estas dos puntas de madeja no es nada sencillo, ni tarea de un día como ha quedado dicho. Supone contar con una política decidida y eficaz de beneficio para la población.

Y sin embargo siempre terminamos hablando de desiderátums jurídicos. Tanto el buen hacer administrativo como los derechos de la gente, son asuntos jurídicos. Si hay algo que el Estado y los gobernantes deben entender y procurar, es el bien de los ciudadanos mediante el ejercicio de funciones y servicios acordes a lograrlo. El desarrollo de sistemas de información abiertos, puede y debe servir a esta filosofía de la “buena administración”. Pero no es solamente la información, en tanto bien preciado y su tutela, lo que está en juego. Es también el servicio o producto que esa información permite conformar para beneficio de una comunidad. Para esto último es necesaria la modernización del Estado y las estructuras de la Administración Pública, porque no bastará juntar una información de aquí y otra de allá, y luego ponerla en el portal. La estrategia y su logística para llevarla a cabo, requieren bastante más que ello.

Recapitulando respecto de los anunciados hilos conductores de los datos abiertos hacia el foco jurídico, tendríamos los siguientes vínculos de servicio hacia varios postulados jurídicos contemporáneos, varios de ellos coincidentes con derechos subjetivos, otros más afincados en deberes de los poderes públicos de seguir el ritmo de la modernidad para el mayor bien común.

Veamos cuales son estos ligámenes:

- Acceso a la información, el conocimiento y la cultura, partiendo de la base que una buena parte de esos datos yacen en los archivos públicos, estatales y no estatales.
- Dinamización del capital informativo de carácter público, para reutilizarlo a favor de la innovación social, y la iniciativa privada. Pasa indudablemente por una mejora real de los archivos estatales, tradicionalmente descuidados por no decir abandonados.
- Generación de instrumentos que colaboren con arribar a administraciones públicas incorruptas y transparentes en su accionar, apoyadas en servidores

públicos merecedores de tal designio en toda su dimensión. “Por mis frutos me conoceréis” o algo así reza los textos antiguos. En el caso del funcionario público, el conocimiento vendrá por lo que dejó escrito.

- Gestión simplificada y eficiente de los órganos estatales y paraestatales, para lo cual resulta condición necesaria, aunque no suficiente, la incorporación de tecnologías a los procesos burocráticos consecuentes con aquél designio.

9. Principios a tener en cuenta

Son de las cosas que hay que saber, y en las que habitualmente se informan y basan las regulaciones derecho positivo, prácticamente lo único a regular en la materia (a excepción de normativa promotora y facilitadora).

Varias organizaciones y expertos se han ocupado en todas partes, de catalogar estos principios, recogiendo de este modo la lista de requisitos y encuadres por donde se desenvuelve el movimiento mundial de los datos abiertos.

Por su grado de análisis e impacto de receptividad en la comunidad especializada, enunciaremos de forma breve los principios enunciados en 2010 por la “Sunlight Foundation” con sede en Washington, a saber:

1. Completitud. Se debe tender a ello, o sea procurar la publicación de la totalidad de lo registrado por cada tema.

2. Primariedad. Se requiere la publicación de datos originarios, no de ulteriores versiones, con la trazabilidad de recogida correspondiente.

3. Disponibilidad oportuna. Esto supone asegurar la factibilidad del acceso tan pronto el dato es recogido. La facilitación en tiempo real maximiza el valor de los datos en términos de su utilidad pública. Hay datos más sensibles que otros al paso del tiempo, lo cual también es factor de prioridad para la recogida y publicación.

4. Facilidad de acceso físico y electrónico. De lo que se trata es de eliminar o atemperar lo más posible todo tipo de barreras. Desde los requisitos de presencialidad y los farragosos formularios, hasta procurar sistemas de búsquedas y descargas electrónicos, sencillos y autosuficientes.

5. Procesables por máquina. No se trata solamente de acceder a la lectura sino también de utilizar los datos liberados para construir aplicaciones y servicios, factor que requiere su procesabilidad posterior a la publicación.

6. No discriminación. Es otro requisito tendiente a eliminar barreras. Desde exigir registros o afiliaciones previos, hasta permitir el acceso a través de determinadas aplicaciones y no otras. Esto significa el acceso de cualquier persona, en cualquier momento, sin tener que identificarse ni proporcionar justificación alguna para hacerlo.

7. Uso de estándares abiertos. Referido a los programas con los cuales se publican los datos, para evitar dependencias y/o costos derivados de tener que utilizar programas de posterior tratamiento que muchas veces tienen costo.

8. No licenciamiento. Ninguna regulación que suponga restringir la utilización pública de los datos, salvo aquello relativo a seguridad y privacidad.

9. Disponibilidad permanente. Lo que asegura la capacidad de encontrar la información durante todo tiempo. E indicación de cambios de los datos liberados cuando ello suceda.

10. Costos de uso. La regla es evitar contraprestaciones al acceso y reutilización de una información que es por naturaleza pública, o sea de todos, admitiéndose cierta cuantificación de costos marginales.

10. La situación uruguaya en la materia

Prácticamente todo lo que se puede saber sobre el estado del arte en Uruguay acerca del movimiento de “datos abiertos”, se encuentra en las institucionalidades públicas y privadas consultables por web.

Desde el “catálogo” de aplicaciones consultable en línea a título de “portal de datos abiertos” y que incluye los “términos de uso” como documento típicamente jurídico (<https://catalogodatos.gub.uy/>), hasta lo que vienen desarrollando las organizaciones y personas que concentran esfuerzos para imponer el tema en la sociedad civil (<http://datauy.org/>).

La Agencia de Gobierno Electrónico y Sociedad de la Información ha dedicado y dedica esfuerzos en la misma dirección. En su sitio web www.agesic.gub.uy se encuentra profusa información al respecto, como son la identificación del área responsable del tema así como la difusión de la guía de apertura de datos, la publicación del mencionado catálogo, noticias y novedades, etc.

La única norma jurídica uruguaya en la materia, hasta donde sabemos, es el Decreto 259/012 del Poder Ejecutivo del 13-08-2012, por el cual se aprueba el “Plan de Acción de Gobierno Abierto de Uruguay 2012” que se agrega por anexo en la publicación oficial respectiva, y se considera parte integrante del Decreto.

El mismo Decreto contiene una adhesión al documento internacional denominado “Declaración sobre Gobierno Abierto” de setiembre de 2011, suscrito por la “Sociedad de Gobierno Abierto”. Y se encomienda el avance en las metas consignadas en tales documentos.

11. Conclusiones

1. Nos parece loable afincar la concepción teórica y práctica de los datos abiertos, así como su filosofía y hasta la ideología que están detrás de esta concepción y la sustentan, en enclaves y marcos jurídicos, no solamente político-gubernamentales.

2. Ese enclave jurídico no puede ser otro, como elemento central, que el Derecho de Información en tanto DD.HH. de amplios y distintos contornos.

Derecho éste modernamente entendido no solo como una situación pasiva a ser movilizada por los titulares del mismo, sino como un conjunto de condiciones e instrumentos, que el Estado tiene el deber de prever y poner a disposición de la comunidad, para que ésta aproveche y pueda construir prestaciones de alcance social de un modo proactivo, no necesariamente de origen y administración estatales.

3. Hay así un pasaje de la “información” concebida como derecho, al concepto pro-activo de la “información” concebida como servicio. Antes el Derecho regulaba y esperaba el acontecer derivado. Pocas veces programaba, al menos al nivel de comunidades e individuos. Con las TI cambia la dinámica, se es proactivo, y el nuevo Derecho debe acomodarse y adoptar este nuevo, o no tan frecuente, rol programador, facilitador. Todo ello sin desmedro del siempre vigente rol garantista.

4. La moderna línea conceptual que refiere a “derechos ciudadanos” vinculados estrechamente con la apropiación y uso sociales de las tecnologías de la información y comunicación, encuentra en el espacio de acciones conformadas a partir de la apertura de datos estatales, un territorio vastísimo y proficuo. Ambos elementos, derechos ciudadanos y datos abiertos, tienen un punto de encuentro natural y estimulante, algo así como una meta preanunciada desde el clásico Derecho de Información pasando a sus otros estadios o desarrollos contemporáneos. Todo lo cual permite esperar que se nutran mutuamente, derechos ciudadanos y datos abiertos, en saludable sinergia, sacando puntales de fuerza y avance mutuos. Para lo que no debe perderse de vista el designio final: la mejor estancia del individuo en la sociedad contemporánea.

Historia clínica electrónica

Novas, Natalia Soledad*
Novas, Jorge Alberto**
Ruani, Humberto Félix***
Ruani, Humberto Martín****

Dedicamos este trabajo, hecho con mucho amor, al más reciente miembro de la FIADI, nuestro querido *Humberto Luca Ruani Novas*, conocido también como H4.

SUMARIO: I. Introducción. II. La protección de datos personales. La inmediatez de acceso a la información y los datos sensibles. III. Registración de los accesos a las historias clínicas y Responsabilidad profesional. IV. Funcionamiento en Argentina. Derecho Comparado y estándares Interjurisdiccionales. V. Conclusiones

Resumen

Sin duda, la salud de las personas es un tema de enorme trascendencia, que en la era de la información, no escapa a los conflictos contemporáneos. La información médica de cada persona, no solo debe estar protegida por cuestiones de privacidad, sino también por cuestiones jurídicas y sociales. Por otro lado, el acceso a este tipo de información puede salvaguardar un derecho aún más importante y urgente, la vida de las personas. En este trabajo intentamos establecer las bases del equilibrio que estos derechos y necesidades que imponen.

Aceptado por el Comité Académico para ser presentado en el XIX Congreso Iberoamericano de Derecho e Informática celebrado en Medellín, agosto 2015. Aprobado por la Junta Directiva de FIADI para ser publicado en la *Revista Derecho y Tecnología*, el 13 de octubre de 2015.

* Novas Natalia soledad. Médica Cardióloga. Especialista en Medicina Interna por la Asociación Médica Argentina –AMA-, Especialista en Emergentología, Coordinadora de la Unidad de Diagnóstico Rápido del Sanatorio Colegiales (Buenos Aires). natynovas@hotmail.com.ar

** Novas, Jorge Alberto. Médico Universidad de Buenos Aires. Especialista en medicina Interna. jorgea_novas@hotmail.com

*** Ruani, Humberto Félix. Abogado. Notario. Presidente de la Asociación Argentina de Informática Jurídica –AAIJ-, Miembro del Instituto de Derecho Informático del Colegio Público de Abogados de Capital Federal –CPACF-(Arg.) ruani@interserver.com.ar

**** Ruani, Humberto Martín. Abogado, Doctorando en Derecho en la Universidad de Ciencias Empresariales y Sociales. Presidente del Comité Organizador del XV Congreso Iberoamericano de Derecho e Informática. Miembro del Instituto de Derecho Informático del CPACF, Tesorero de la AAIJ. hruani@hotmail.com

Palabras clave: Historia clínica electrónica. Responsabilidad profesional. Privacidad. Urgencia médica. Salud. Derecho.

Abstract

No doubt, people's health is a very important issue, in the Information Age, it is not exempt from today's conflicts. Health data of every person, not only must be protected due to privacy issues, but also due to legal and social issues. Furthermore, access to this information can safeguard an important and urgent right, the life of people. In this paper we attempt to establish the basis of the balance of these rights and the needs arised from them

Keywords: Electronic Key Records. Professional Liability. Privacy. Medical Emergency. Health. Law. Right.

I. Introducción

Como primer acercamiento, comenzaremos por definir el objeto del presente trabajo, identificando por separado y en su conjunto, los conceptos que lo definen.

La (Real Academia Española, 2015)¹ indica que *historia* significa “*Narración y exposición de los acontecimientos pasados y dignos de memoria, sean públicos o privados*”, y otra de sus acepciones según la misma fuente es “*Conjunto de los acontecimientos ocurridos a alguien a lo largo de su vida o en un periodo de ella*”. Mientras que *clínica* está definida como “*Ejercicio práctico de la medicina relacionado con la observación directa del paciente y con su tratamiento*”. (Real Academia Española 2, 2015)². Por último, la RAE define también al término *historia clínica* como la “*Relación de los datos con significación médica referentes a un enfermo, al tratamiento a que se le somete y a la evolución de su enfermedad*” (Real Academia Española, 2015)³.

Por otro lado, (Jervas J, 2000)⁴ entiende que:

...La historia clínica electrónica (HCE), también denominada historia clínica informatizada (HCI), es el registro mecanizado de los datos socia les,

1 Real Academia Española. (2015). *Diccionario de la Real Academia Española de Letras*. Recuperado el 29 de mayo de 2015, de <http://lema.rae.es/drae/?val=historia+clinica>

2 Real Academia Española 2. (2015). *Real Academia Española*. Recuperado el 29 de Mayo de 2015, de <http://lema.rae.es/drae/?val=historia+clinica>

3 Real Academia Española. (2015). *Diccionario de la Real Academia Española de Letras*. Recuperado el 29 de mayo de 2015, de <http://lema.rae.es/drae/?val=historia+clinica>

4 JERVAS J., P. F. (2000). *La Historia Clínica electrónica en Atención Primaria, Fundamento Clínico, Teórico y Práctico*, (págs. 17-32).

preventivos y médicos de un paciente, obtenidos de forma directa o indirecta y constantemente puestos al día.

Por lo expuesto, podemos definir la historia clínica electrónica para este trabajo, como *“El documento informatizado, donde se encuentra registrada información civil, médica y jurídica de relevancia. En la que debe constar todo ejercicio práctico de la medicina relacionado con la observación directa del paciente y con su tratamiento, a lo largo de su vida o de un período de la misma”*.

Los antecedentes médicos de cada paciente (estrechamente llamados historia clínica) Constituyen un nexo fundamental entre el campo asistencial y las áreas de sistemas.

Decimos estrechamente llamados historia clínica, porque en este trabajo interesa la registración de todos los antecedentes médicos de una persona, sin detenernos a analizar de dónde surgen los mismos, la idea es que se consigne la mayor cantidad de datos posible, que permita el logro de la información necesaria para el tratamiento inmediato y oportuno del paciente, como un elemento fundamental para la toma de decisiones, especialmente en situaciones de crisis o emergencia médica.

En cuanto abordamos el tema, aparecen ciertas cuestiones conexas, que analizaremos en el siguiente orden:

- La protección de datos personales. La inmediatez de acceso a la información y los datos sensibles.
- Registración de los accesos a las historias clínicas y responsabilidad profesional.
- Funcionamiento en Argentina, Derecho comparado y estándares interjurisdiccionales. Homogenización del sistema de historias clínicas electrónicas

II. La protección de datos personales. La inmediatez de acceso a la información y los datos sensibles

Cuando nos referimos a una historia clínica, no podemos pasar por alto, que es un documento que excede el ámbito médico, trascendiendo en el jurídico. Las historias clínicas son generalmente una prueba definitiva en cuestiones de responsabilidad de los profesionales de la salud y de las instituciones prestadoras de servicios de esta área.

Las legislaciones iberoamericanas son unánimes respecto a que la titularidad de la historia clínica, pertenece al paciente. Pero por otro lado, ¿Hasta dónde llega la responsabilidad del médico si un paciente se negara a facilitarle su historia clínica u ocultara información sobre ella?

Quienes realizamos este trabajo, nos desenvolvemos en esas ramas y entendemos que hay principalmente dos circunstancias diferentes y tienen que ver con la posibilidad de expresar voluntad del paciente. Entendemos que las historias clínicas electrónicas, deberían tener una parte de acceso general, donde cualquier profesional de la salud que se encuentre con un paciente en estado de inconsciencia, pueda escanear una huella dactilar o un iris y obtener información de esa persona que no sea de tipo sensible, pudiendo por ejemplo encontrar datos de familiares, fármacos a los que resulta alérgico e intervenciones o estudios médicos recientes, debiendo contar con autorización del paciente o de sus familiares o personas designadas en la historia clínica, para acceder al total de la información, que incluye datos sensibles si los hubiera.

Lo referido en el párrafo anterior, entendemos que debe hacerse mediante un sistema de codificación que permita dejar registro en la historia clínica, del profesional que realizó la consulta, los datos a los que accedió y la razón por la cual lo hizo.

El otro punto es la capacidad del paciente de retener para sí, los datos de su historia clínica o de ocultar parte de la misma. En los casos en que el paciente se encuentra en estado de consciencia, el mismo puede decidir qué hacer con sus datos, pero por supuesto que la responsabilidad del profesional de la salud se limitará al cumplimiento de los protocolos médicos sobre la base de la información con la que cuenta, recordemos que en el campo de la prestación de servicios de salud, la responsabilidad es siempre de medios y no de resultados.

Las consecuencias de la divulgación del estado de salud de una persona, puede originarle a ésta serios perjuicios. Por lo que deben extremarse las medidas de protección de la información registrada.

Como adelantáramos anteriormente, debe ser el paciente quien determine las personas que puedan tener acceso a la información, pero este principio debería reconocer limitaciones, resulta muy claro el caso en el que el paciente llega a un centro hospitalario en estado de inconsciencia y para tratarlo es necesario saber qué medicinas se le pueden suministrar, si es alérgico, si tiene enfermedades que limitan los procedimientos o fármacos a los que se pueda someter al paciente, etc. Principalmente teniendo en cuenta que en muchos casos no se cuenta siquiera con la identidad certera del paciente. Resulta muy destacable, el hecho de que la falta de información o de registros médicos, puede hacer peligrar la salud e incluso la vida de una persona, cuando por acción u omisión de un profesional que desconoce antecedentes del enfermo, se realiza un procedimiento erróneo, o se deja de intervenir al mismo cuando fuera necesario.

Este trabajo propone como aporte a la resolución del problema, que los profesionales de la salud puedan tener acceso a la identidad del paciente, a través de datos biológicos como las huellas dactilares, mientras que para acceder a la información de la persona ya identificada, deberán tener una clave de acceso profesional, cuya utilización quedará grabada en el sistema de consulta

de dicha historia clínica. El acceso a la historia clínica electrónica a su vez estará condicionado por la reserva de datos sensibles o enfermedades cuya divulgación pueda generar un serio perjuicio al paciente en cualquier sentido.

En el equipo multidisciplinario que conformamos para este trabajo, encontramos muchas dificultades para conciliar el derecho a la privacidad de los pacientes, con la praxis médica y el sistema de salud.

Supongamos que se presenta a la consulta un paciente portador de HIV con una neumonía, el mismo requiere aislamiento para evitar posibles contagios que pueden agravar su condición por encontrarse inmunodeprimido; pero si el paciente prefiere preservar dicha información (que es portador de HIV) y no acceder a compartir su historia clínica con el equipo médico, no solo estará empeorando gravemente su estado de salud, sino que además retrasará el correcto diagnóstico, utilizando además múltiples recursos del sistema de salud hasta descartar otras posibilidades mediante estudios que conllevan insumos, recursos humanos, tiempo y un seguro empeoramiento del estado del paciente. Por otra parte, los formados en leyes entendemos que los derechos de las personas, en especial aquellos personalísimos como la privacidad, no pueden estar supeditados a la economía de los recursos. Una colisión de derechos de difícil solución. Al respecto, sí es importante destacar que hay acuerdo unánime al considerar que el derecho personal de una persona –por ejemplo de privacidad–, debe ceder cuando exista un riesgo cierto de que la protección de ese derecho, implique un mal mayor en relación a otras personas o a su propia salud. Es decir que si una persona se encuentra inconsciente, es siempre preferible vulnerar su derecho de privacidad y salvar su vida. También es preferible ante la posibilidad concreta de una enfermedad contagiosa de alto riesgo de contagio o con posibilidades de convertirse en una pandemia, los profesionales de la salud, podrán vulnerar la privacidad del paciente respecto de su historia clínica, a los fines de evitar un mal mayor.

Solo como ejemplo, y sin perjuicio de un mejor desarrollo posterior, el Estado español, ha considerado a través de los “principios estratégicos” del Instituto de Información Sanitaria del Gobierno Español⁵ que:

...Resulta imprescindible mantener equilibrados en el nivel más alto posible, dos valores: La disponibilidad de la información para el ciudadano y los profesionales que deban prestarle atención sanitaria y la protección de su intimidad, representada aquí por los datos que afectan a su salud. De tal manera que, ningún profesional que deba actuar en beneficio de su estado de salud, tenga impedimento alguno para acceder a aquellos datos que requiera el ejercicio de su función, pero nadie sin legitimidad para ello pueda acceder. El primero deriva del principio de beneficencia y el segundo deriva del

⁵ Instituto de Información Sanitaria del Gobierno Español. (2010). *Sitio Web del Ministerio de Sanidad, Servicio Social e Igualdad del estado Español*. Recuperado el 29 de Mayo de 2015, de http://www.msssi.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf

principio de autonomía. Obviamente ninguno de ellos debe supeditarse al otro y ambos deben ser preservados por igual en el mayor nivel posible...

Defendiendo de este modo ambas posturas, pero estableciendo un criterio claro, de que nada debiera obstaculizar la correcta prestación del servicio de salud, aunque también es cierto que no contempla específicamente el caso en que el paciente se negara a compartir su historia clínica.

III. Registración de los accesos a las historias clínicas y responsabilidad profesional

Se deben tener en cuenta dos valores esenciales, como son el acceso a datos de salud relevantes, con intención de agilizar y mejorar la calidad de atención del paciente y la protección de la intimidad de dichos datos.

La protección de los datos personales hace necesario que quienes tengan acceso al sistema queden registrados en oportunidad de su consulta, ya que la divulgación de datos sensibles o el mal aprovechamiento de la información obtenida podrán dar lugar a la reparación de los daños y perjuicios que sufra el paciente. Es por esto que la consulta sobre la información, el contenido de la información obtenida y los eventuales procedimientos o estudios realizados sobre cada paciente, deben quedar registrados. Asimismo, debe quedar registro de quienes accedieron y/o cargaron datos en el sistema. Entendiendo por registro, el nombre y matrícula profesional de quien haya intervenido.

IV. Funcionamiento en Argentina. Derecho comparado y estándares interjurisdiccionales. Homogenización del sistema de historias clínicas electrónicas

En Argentina no se cuenta con un modelo estandarizado de historia clínica electrónica. Las provincias de La Pampa y San Luis están implementando un modelo de historia clínica, al igual que la Ciudad Autónoma de Buenos Aires, pero es exclusiva de la red de hospitales públicos y a la fecha las instituciones de salud pueden optar por implementarla o no, siendo las primeras una minoría del total. A su vez, pueden implementar el modelo de historia clínica electrónica que consideren más conveniente sin contar con parámetros estandarizados en cuanto al formato o acceso y protección de datos. Las diferentes instituciones de salud, no se hallan interconectadas en red; por lo tanto, no se puede acceder a la historia clínica del paciente que fue asistido en un centro de salud, salvo que se le haya dado un resumen de dicha atención. Esto puede generar problemas en la atención del paciente, al no saber con certeza que estudios diagnósticos o procedimientos le fueron realizados en la asistencia previa.

Las historias clínicas deben ser trabajadas con estándares internacionales, utilizando idiomas comunes, con posibilidad de traducción que respete los

protocolos y consignas médicas, con la finalidad de que cualquiera sea el lugar donde se encuentre el paciente y cualquiera sea el profesional que deba asistirlo, cuente con la información necesaria para la toma de decisiones médicas.

El ingreso de la información al sistema debe ser homogéneo en cuanto a sus formas, su idioma y su contenido, ya que sería inútil la carga de información si la misma no puede ser aprovechada en el momento en que resulte necesaria. Para ello es necesario la aplicación de protocolos médicos que permitan la carga y aprovechamiento de la información en forma sencilla, práctica y eficiente. Estos protocolos deberán contar con una vocación universal, requiriendo una capacitación profesional en tal sentido.

El modelo de historia clínica electrónica deberá ser único para todas las instituciones de salud que se hallen interconectadas. El mismo deberá constar en su esquematización con un resumen donde puedan encontrarse datos relevantes para la atención del paciente, así como antecedentes patológicos, alergias, medicación habitual, motivos de internación previa, etc. El resumen de historia clínica es la “carta de presentación” del paciente. El documento debe ser solo para lectura, sin posibilidad de modificarse la información ya escrita, solo pudiendo adicionar datos de la nueva atención, a causa de impedir el falseamiento de la información. En el caso de haber cometido un error en el ingreso de los datos, se deberá salvar en forma adecuada con la leyenda error. La finalidad del resumen de historia clínica, es dar conocimiento del estado del paciente y sus antecedentes, a fin de que este reciba una adecuada asistencia para la dolencia que presenta.

La historia clínica electrónica también deberá contar con el registro de la atención en consultorios externos, urgencias, de internación. Tendrá que constar de informes acerca de la actividad de enfermería y permitir el acceso a la visualización de estudios diagnósticos (laboratorio, imágenes) y procedimientos realizados. Este tipo de registros contienen información sumamente detallada acerca de la salud del paciente, por lo tanto debe establecerse que personas pueden acceder a la misma.

Por esto debemos tener en cuenta los principios de beneficencia y autonomía, para ejercerlos adecuadamente en pro de que el aporte de información sobre el paciente no sea malversada, dejando claro quiénes pueden acceder a cada tipo de información y que el único dueño de toda esta data es el propio paciente.

Según lo presentado en la Jornada Internacional “Historia Clínica Electrónica e Interoperabilidad en el Sector Salud”, realizada en Perú, (Mezarina, 2015)⁶ define los conceptos de información clínica básica y sensible de la siguiente manera: La básica comprende datos como antecedentes patológicos, alergias, medicación, cirugías previas, etc. Mientras que la información sensible, abarca

6 MEZARINA, L. R. (26 de Febrero de 2015). *Sitio del Ministerio de Salud del Gobierno Peruano*. Recuperado el 29 de Mayo de 2015, de <http://www.minsa.gob.pe/renhice/documentos/pres/L01%20Proyecto%20de%20Reglamento%20RENHICE%20-%20Leonardo%20Rojas.pdf>

la salud física y mental, las características físicas y emocionales, los hábitos y hechos familiares. El proyecto del Gobierno peruano, da al paciente, la posibilidad de preservar la información sensible de la vista de los profesionales de la salud, ya que el sistema le permite no solo acceder a consultar sus registros, sino también a seleccionar la parte de los mismos que pretende proteger.

El tratamiento de la HCE, es de una enorme complejidad y debe abarcar un sinfín de cuestiones más que las tratadas en este trabajo, las que por los límites de extensión del mismo, nos limitaremos solo a enunciar:

Principios y derechos de los ciudadanos en relación con la historia clínica. La responsabilidad profesional y empresarial sobre las historias clínicas. Diferencias principales entre los servicios sanitarios públicos y los servicios sanitarios privados. La centralización de las historias clínicas y su conservación. La aceptación de los consentimientos informados en las historias clínicas electrónicas. La seguridad como garantía de la integridad y de la confidencialidad de la historia clínica. El deber de secreto. F) el derecho de acceso del paciente a la historia clínica. El acceso a la historia clínica por personas distintas al interesado. La cesión de la historia clínica. El acceso a la historia clínica por los profesionales sanitarios, por el personal de administración y gestión y por el personal de inspección. La cesión de la historia clínica para fines epidemiológicos, de salud pública y de investigación. La cesión de la historia clínica a la administración sanitaria, a las compañías aseguradoras, a los órganos judiciales y a las fuerzas y cuerpos de seguridad del estado.

Dirigiremos nuestro aporte, a una sociedad globalizada y con una tecnología informática desbordante en cuanto a su crecimiento más allá de considerar si la historia clínica es manual o informatizada, es pública o privada, es local provincial, nacional regional o internacional, apuntaremos a los derechos humanos en juego, como ser los que protegen la vida, la salud, la intimidad.

Todos ellos apuntan a la protección del individuo y del conjunto de individuos que integran una sociedad, por esta razón no podemos encontrar conflictos donde no los hay.

Si protegemos el derecho de un individuo, con mayor razón protegeremos los derechos de la suma de individuos, razón por la cual los primeros pueden ver limitadas sus aspiraciones personales, pero serán ampliamente compensados al protegerse al conjunto social del cual forman parte.

El camino a seguir se nutrirá con la estandarización de los elementos a consignar en la historia clínica electrónica, la identificación cierta de responsables en cuanto a su confección, custodia, difusión, conservación, y la protección formal y económica de los derechos de cada individuo para que la vulneración de su intimidad –sin que causas de bien común lo justifiquen– sea sancionada severamente y dé lugar a una indemnización adecuada, que desaliente a los

responsables a infringir sus deberes de protección de datos personales de los pacientes.

V. Conclusiones

Luego de la investigación cuyo resultado es el presente trabajo, podemos concluir lo siguiente:

- 1) En la actualidad, todos los Estados que constitucionalmente garanticen el derecho a la atención médica, a la salud y/o a la vida, deben tener como directriz, tomar toda acción tendiente a garantizar esos derechos. La informatización de las historias clínicas y la accesibilidad a las mismas, es una responsabilidad ineludible de los sistemas de salud estatales.
- 2) Resulta sumamente importante que ante una emergencia médica, los profesionales cuenten con la más amplia y detallada historia clínica, ya que ésta puede ser la diferencia entre la vida o la muerte de una persona.
- 3) Para los casos en los que los pacientes llegan a una guardia de urgencias en estado de inconsciencia, que el médico pueda identificar al paciente por datos biométricos como huellas dactilares, o el iris del enfermo, para poder así acceder a su historia clínica y conocer los datos relevantes, será un gran avance y definitivamente, un aporte que salvará muchas vidas.
- 4) A los efectos de proteger no solo la integridad física del paciente, sino la salud, que para la (Organización Mundial de la Salud, 1946)⁷ se trata de “*Un estado de completo bienestar físico, mental y social, no solamente la ausencia de enfermedad o dolencia*”, resulta imprescindible conservar la privacidad de los datos personales relativos a la historia clínica de los pacientes y sus eventuales enfermedades. Para garantizar esto, es que todos aquellos que accedan a este tipo de información sensible, deberán quedar registrados y serán responsables por lo que hagan con dicha información.

Estas mejoras en la salud, pueden ser compartidas y potenciadas por las diversas jurisdicciones nacionales e internacionales, que respetando un protocolo único, puedan incluso cruzar los límites nacionales, pudiendo realizar consultas de historias clínicas de distintos países.

Colegimos en que en caso de colisión entre la difusión de los datos sensibles obrantes en la historia clínica digital de un paciente y el riesgo cierto e inminente de daño para la sociedad (riesgo de una pandemia) deberán prevalecer los intereses de la sociedad, aun a costa del sacrificio de datos sensibles de un paciente. Nótese que para ello deberán instrumentarse legislativamente

⁷ Organización Mundial de la Salud. (1946). Constitución de la Organización Mundial de la Salud.

disposiciones que liberen al profesional médico de su responsabilidad en lo atinente el secreto profesional, y que este recurso será aplicable luego de agotar todas las posibilidades.

De preservar los derechos personalísimos del paciente en cuanto a los datos registrados en su historia clínica, que declinara su primacía solo ante el riesgo cierto e inminente de un daño a los intereses sociales, que en última instancia será en beneficio de la suma de todos los intereses individuales.

LEGISLACIÓN

**REGLAMENTO (UE) N° 524/2013
DEL PARLAMENTO EUROPEO Y DEL CONSEJO**

de 21 de mayo de 2013

**sobre resolución de litigios en línea en materia de consumo y por el
que se modifica el Reglamento (CE) n° 2006/2004 y la Directiva
2009/22/CE**

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN
EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo¹,

De conformidad con el procedimiento legislativo ordinario²,

Considerando lo siguiente:

- 1) En el artículo 169, apartado 1 y apartado 2, letra a), del Tratado de Funcionamiento de la Unión Europea (TFUE) se establece que la Unión debe contribuir a lograr un alto nivel de protección de los consumidores mediante las medidas que adopte en virtud del artículo 114 del TFUE. En el artículo 38 de la Carta de los Derechos Fundamentales de la Unión Europea se dispone que en las políticas de la Unión ha de garantizarse un nivel elevado de protección de los consumidores.
- 2) Con arreglo al artículo 26, apartado 2, del TFUE, el mercado interior implica un espacio sin fronteras interiores, en el que está garantizada la libre circulación de mercancías y servicios. Para que los consumidores tengan confianza en la dimensión digital del mercado interior y se beneficien de ella es necesario que tengan acceso a formas sencillas, eficientes, rápidas y asequibles de resolver los litigios derivados de la compraventa de mercancías o de la prestación de servicios en línea. Ello reviste especial importancia cuando los consumidores realizan compras transfronterizas.

¹ DO C 181 de 21.6.2012, p. 99.

² Posición del Parlamento Europeo de 12 de marzo de 2013 (no publicada aún en el Diario Oficial) y Decisión del Consejo de 22 de abril de 2013.

- 3) En su Comunicación de 13 de abril de 2011 titulada «Acta del mercado único –Doce prioridades para estimular el crecimiento y reforzar la confianza– "Juntos por un nuevo crecimiento"», la Comisión identificó la legislación sobre resolución alternativa de litigios, incluida la dimensión del comercio electrónico, como una de las doce prioridades para estimular el crecimiento y reforzar la confianza en el mercado único.
- 4) La fragmentación del mercado interior dificulta los esfuerzos orientados a impulsar la competitividad y el crecimiento. Asimismo, la desigualdad en la disponibilidad, calidad y conocimiento de medios sencillos, eficientes, rápidos y asequibles para solucionar litigios derivados de la compraventa de mercancías o de la prestación de servicios en toda la Unión constituye una barrera dentro del mercado interior que socava la confianza de los consumidores y los comerciantes en las compraventas transfronterizas.
- 5) En sus conclusiones de 24 y 25 de marzo de 2011 y de 23 de octubre de 2011, el Consejo Europeo invitó al Parlamento Europeo y al Consejo a adoptar, antes de que terminase 2012, un primer conjunto de medidas prioritarias con el fin de dar un nuevo impulso al mercado único.
- 6) El mercado interior es una realidad en la vida diaria de los consumidores cuando viajan, compran y pagan. Los consumidores son los protagonistas del mercado interior y, por lo tanto, deben estar en el centro de todas las consideraciones al respecto. La dimensión digital del mercado interior se está convirtiendo en algo esencial tanto para los consumidores como para los comerciantes. Cada vez son más los consumidores que compran en línea, y el número de comerciantes que venden en línea va en aumento. Es importante que los consumidores y los comerciantes puedan realizar transacciones en línea, por lo que resulta indispensable dismantelar los obstáculos existentes y potenciar la confianza de los consumidores. La disponibilidad de un sistema de resolución de litigios en línea fiable y eficiente podría contribuir en grado importante al logro de este objetivo.
- 7) La posibilidad de recurrir a procedimientos de resolución de litigios sencillos y asequibles puede impulsar la confianza de consumidores y comerciantes en el mercado único digital. No obstante, consumidores y comerciantes siguen enfrentándose a obstáculos para encontrar soluciones extrajudiciales, especialmente en los litigios que se derivan de transacciones transfronterizas en línea. Por esa razón, este tipo de litigios a menudo queda sin resolver.
- 8) La resolución de litigios en línea ofrece una solución extrajudicial sencilla, eficiente, rápida y asequible para los litigios derivados de transacciones en línea. Sin embargo, en la actualidad faltan mecanismos que permitan a los

consumidores y a los comerciantes resolver este tipo de litigios por medios electrónicos. Ello redundaría en detrimento del consumidor, constituye una barrera, en particular, para las transacciones transfronterizas en línea, y crea condiciones desiguales para los comerciantes, obstaculizando así el completo desarrollo del comercio en línea.

- 9) El presente Reglamento debe aplicarse a la resolución extrajudicial de litigios iniciados por consumidores residentes en la Unión frente a comerciantes establecidos en la Unión que estén amparados por la Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo³.
- 10) Con el fin de garantizar que la plataforma de resolución de litigios en línea también pueda utilizarse para los procedimientos de resolución alternativa de litigios (en lo sucesivo, «procedimientos de resolución alternativa») que permitan a los comerciantes presentar reclamaciones contra los consumidores, el presente Reglamento debe asimismo aplicarse a la resolución extrajudicial de litigios entablados por comerciantes frente a consumidores para los que entidades de resolución alternativa de litigios (en lo sucesivo, «entidades de resolución alternativa») incluidas en la lista con arreglo al artículo 20, apartado 2, de la Directiva 2013/11/UE ofrezcan procedimientos de resolución alternativa pertinentes. La aplicación del presente Reglamento a dichos litigios no debe imponer a los Estados miembros la obligación de garantizar que las entidades de resolución alternativa ofrezcan este tipo de procedimientos.
- 11) Aunque los principales beneficiarios de la plataforma de resolución de litigios en línea sean concretamente los consumidores y los comerciantes que efectúen operaciones transfronterizas en línea, el presente Reglamento debe aplicarse también a las transacciones nacionales en línea, con el fin de garantizar unas condiciones equitativas efectivas en materia de comercio electrónico.
- 12) El presente Reglamento ha de entenderse sin perjuicio de la Directiva 2008/52/CE del Parlamento Europeo y del Consejo, de 21 de mayo de 2008, sobre ciertos aspectos de la mediación en asuntos civiles y mercantiles⁴.
- 13) La definición de «consumidor» debe incluir a las personas físicas que actúen con fines ajenos a sus actividades comerciales o empresariales, a su oficio

³ Véase la página 63 del presente Diario Oficial.

⁴ DO L 136 de 24.5.2008, p. 3.

o a su profesión. No obstante, si el contrato se celebra con un propósito en parte relacionado y en parte no relacionado con la actividad comercial de la persona (contratos de doble finalidad) y el propósito comercial es tan limitado que no predomina en el contexto general del suministro, dicha persona también debe considerarse un consumidor.

- 14) La definición de «contrato de compraventa o de prestación servicios celebrado en línea» debe abarcar un contrato de compraventa o de prestación servicios en que el comerciante, o el intermediario del comerciante, haya ofrecido mercancías o servicios a través de un sitio de internet o por otros medios electrónicos y el consumidor haya encargado dichas mercancías o servicios en dicho sitio de internet o por otros medios electrónicos. También debe aplicarse a los casos en que el consumidor acceda al sitio de internet o a otro servicio de la sociedad de la información mediante un dispositivo electrónico móvil como, por ejemplo, un teléfono móvil.
- 15) El presente Reglamento no debe aplicarse a los litigios entre consumidores y comerciantes que se deriven de contratos de compraventa o de prestación de servicios no celebrados en línea ni a los litigios entre comerciantes.
- 16) El presente Reglamento debe considerarse conjuntamente con la Directiva 2013/11/UE, en la que se exige a los Estados miembros que garanticen la posibilidad de someter a una entidad de resolución alternativa todos los litigios entre consumidores domiciliados y comerciantes establecidos en la Unión que se deriven de la compraventa de mercancías o la prestación de servicios.
- 17) Los Estados miembros deben animar a los consumidores a que, antes de someter su reclamación a una entidad de resolución alternativa a través de la plataforma de resolución de litigios en línea, se pongan en contacto con el comerciante por cualquier medio adecuado con el fin de resolver el litigio de forma amistosa.
- 18) El objetivo del presente Reglamento es crear una plataforma de resolución de litigios en línea en el ámbito de la Unión. La plataforma de resolución de litigios en línea debe adoptar la forma de un sitio de internet interactivo que ofrezca una ventanilla única a los consumidores y a los comerciantes que quieran resolver extrajudicialmente litigios derivados de transacciones en línea. La plataforma de resolución de litigios en línea debe facilitar información general sobre la resolución extrajudicial de litigios contractuales derivados de contratos de compraventa o de prestación de servicios celebrados en línea entre comerciantes y consumidores. La plataforma

debe permitir a consumidores y comerciantes presentar reclamaciones rellenando un formulario electrónico de reclamación disponible en todas las lenguas oficiales de las instituciones de la Unión, y adjuntar los documentos pertinentes. Debe transmitir las reclamaciones a una entidad de resolución alternativa competente para conocer del litigio en cuestión. La plataforma debe ofrecer gratuitamente un sistema electrónico de tramitación de asuntos que permita a las entidades de resolución alternativa tramitar el procedimiento de resolución del litigio con las partes a través de la plataforma de resolución de litigios en línea. Las entidades de resolución alternativa no deben estar obligadas a utilizar el sistema de tramitación de asuntos.

- 19) La Comisión debe ser la responsable del desarrollo, funcionamiento y mantenimiento de la plataforma de resolución de litigios en línea y proporcionar todos los medios técnicos necesarios para el funcionamiento de la plataforma. La plataforma de resolución de litigios en línea debe ofrecer una función de traducción electrónica que permita a las partes y a la entidad de resolución alternativa disponer de la información que se intercambie a través de la plataforma de resolución de litigios en línea y que resulte necesaria para la resolución del litigio, en su caso en versión traducida. Dicha función debe poder tratar todas las traducciones necesarias y apoyarse en una intervención humana, si fuera necesario. Asimismo, a través de la plataforma de resolución de litigios en línea, la Comisión debe proporcionar información a los reclamantes sobre la posibilidad de solicitar ayuda a los puntos de contacto de resolución de litigios en línea.
- 20) La plataforma de resolución de litigios en línea debe permitir el intercambio seguro de datos con las entidades de resolución alternativa y respetar los principios que subyacen en el Marco Europeo de Interoperabilidad adoptado con arreglo a la Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC)⁵.
- 21) La plataforma de resolución de litigios en línea debe ser accesible, en particular, a través del portal «Tu Europa» creado de conformidad con el anexo II de la Decisión 2004/387/CE, que ofrece a las empresas y a los ciudadanos de la Unión acceso a información en línea y servicios interactivos multilingües paneuropeos. La plataforma de resolución de litigios en línea debe ocupar un lugar destacado del portal «Tu Europa».

⁵ DO L 144 de 30.4.2004, p. 62.

- 22) Una plataforma de resolución de litigios en línea a escala de la Unión debe basarse en entidades de resolución alternativa existentes en los Estados miembros y respetar las tradiciones jurídicas de estos. Por consiguiente, las entidades de resolución alternativa que reciban una reclamación a través de la plataforma de resolución de litigios en línea deben aplicar sus propias normas de procedimiento, incluidas las normas sobre costas. No obstante, mediante el presente Reglamento se pretende establecer una serie de normas comunes aplicables a dichos procedimientos para garantizar su eficacia. Entre ellas deben figurar normas para garantizar que la resolución de litigios no exija la comparecencia de las partes o de sus representantes ante la entidad de resolución alternativa, salvo que sus normas de procedimiento contemplen esa posibilidad y las partes presten su consentimiento.
- 23) El hecho de garantizar que todas las entidades de resolución alternativa incluidas en la lista con arreglo al artículo 20, apartado 2, de la Directiva 2013/11/UE estén registradas en la plataforma europea de resolución de litigios en línea debe permitir una cobertura total de la resolución extrajudicial en línea de litigios derivados de contratos de compraventa o de prestación de servicios celebrados en línea.
- 24) El presente Reglamento no debe ser un obstáculo al funcionamiento de cualesquiera entidades de resolución de litigios ya existentes que operen en línea ni de cualquier mecanismo de resolución de litigios en línea ya existente en la Unión. Tampoco debe impedir que las entidades o mecanismos de resolución de litigios tramiten litigios en línea que les hayan sido sometidos directamente.
- 25) Deben designarse en cada Estado miembro puntos de contacto de resolución de litigios en línea que cuenten al menos con dos asesores de resolución de litigios en línea. Los puntos de contacto de resolución de litigios en línea deben ofrecer apoyo a las partes implicadas en un litigio sometido a través de la plataforma de resolución de litigios en línea sin estar obligados a traducir los documentos relacionados con el litigio. Los Estados miembros deben tener la posibilidad de atribuir la responsabilidad de los puntos de contacto de resolución de litigios en línea a sus centros de la Red de Centros Europeos del Consumidor. Los Estados miembros deben recurrir a esta posibilidad para permitir que los puntos de contacto de resolución de litigios en línea se beneficien plenamente de la experiencia de los centros de la Red de Centros Europeos del Consumidor en la facilitación de la resolución de litigios entre consumidores y comerciantes. La Comisión debe crear una red de puntos de contacto de resolución de litigios en línea para facilitar la cooperación entre estos, y proporcionar, en cooperación con los Estados

miembros, una adecuada formación para los puntos de contacto de resolución de litigios en línea.

- 26) El derecho a la tutela judicial efectiva y el derecho a un juez imparcial forman parte de los derechos fundamentales establecidos en el artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea. La resolución de litigios en línea no está concebida ni puede concebirse para sustituir a los procedimientos judiciales, ni debe privar a consumidores o comerciantes de su derecho de recurso ante los órganos jurisdiccionales. Por lo tanto, el presente Reglamento no debe impedir a las partes ejercer su derecho de acceso al sistema judicial.
- 27) El tratamiento de la información con arreglo al presente Reglamento debe estar sujeto a estrictas garantías de confidencialidad y ajustarse a las normas de protección de datos personales establecidas por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos⁶ y por el Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos⁷. Dichas normas deben aplicarse al tratamiento de datos personales efectuado con arreglo al presente Reglamento por los distintos actores de la plataforma de resolución de litigios en línea, independientemente de que actúen solas o con esos otros actores.
- 28) Los titulares de los datos deben ser informados sobre el tratamiento de sus datos personales en la plataforma de resolución de litigios en línea y prestar su consentimiento a dicho tratamiento, y ser informados sobre sus derechos respecto de dicho tratamiento; para ello la Comisión debe poner a disposición del público una nota exhaustiva de protección de la intimidad y explicar, en un lenguaje claro y sencillo, el tratamiento efectuado bajo la responsabilidad de los distintos actores de la plataforma, con arreglo a los artículos 11 y 12 del Reglamento (CE) n° 45/2001 y a la legislación nacional adoptada con arreglo a los artículos 10 y 11 de la Directiva 95/46/CE.
- 29) El presente Reglamento debe entenderse sin perjuicio de las disposiciones de la legislación nacional sobre confidencialidad en el contexto de la resolución alternativa de litigios.

⁶ DO L 281 de 23.11.1995, p. 31.

⁷ DO L 8 de 12.1.2001, p. 1.

- 30) Con el fin de garantizar una amplia sensibilización de los consumidores sobre la existencia de la plataforma de resolución de litigios en línea, los comerciantes establecidos en la Unión que celebren contratos de compraventa o de prestación de servicios en línea deben proporcionar en sus sitios de internet un enlace electrónico a dicha plataforma. Además, los comerciantes deben proporcionar su dirección de correo electrónico para que los consumidores dispongan de un primer punto de contacto. Una parte importante de los contratos de compraventa y de prestación de servicios en línea se celebra a través de mercados en línea, los cuales agrupan o facilitan las transacciones en línea entre consumidores y comerciantes. Dichos mercados son plataformas en línea que permiten que los comerciantes pongan sus productos y servicios a disposición de los consumidores. Por consiguiente, tales mercados en línea deben estar sujetos a la misma obligación de proporcionar un enlace electrónico a la plataforma de resolución de litigios en línea. Esta obligación debe entenderse sin perjuicio de lo dispuesto en el artículo 13 de la Directiva 2013/11/UE con respecto a la obligación para los comerciantes de informar a los consumidores sobre los procedimientos de resolución alternativa que amparen a dichos comerciantes y sobre si se comprometen o no a recurrir a los procedimientos de resolución alternativa de litigios con los consumidores. Además, esta obligación debe entenderse sin perjuicio de lo dispuesto en el artículo 6, apartado 1, letra t), y el artículo 8 de la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, relativa a los derechos de los consumidores⁸. El artículo 6, apartado 1, letra t), de la Directiva 2011/83/UE establece, para los contratos con consumidores celebrados a distancia o fuera del establecimiento, que el comerciante debe informar al consumidor sobre la posibilidad de recurrir a un mecanismo no judicial de reclamación y recurso al que esté sujeto el comerciante y los métodos para tener acceso al mismo, antes de que el consumidor quede vinculado por el contrato. Por las mismas razones de sensibilización de los consumidores, los Estados miembros deben fomentar que también las asociaciones de consumidores y las asociaciones empresariales proporcionen un enlace electrónico al sitio de internet de la plataforma de resolución de litigios en línea.
- 31) A fin de tener en cuenta los criterios por los cuales las entidades de resolución alternativa definen sus respectivos ámbitos de actuación, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE a fin de adaptar la información que los reclamantes deben proporcionar en el formulario electrónico de reclamación disponible en la plataforma de resolución de litigios en línea. Reviste especial

⁸ DO L 304 de 22.11.2011, p. 64.

importancia que la Comisión lleve a cabo las consultas adecuadas en la fase preparatoria, incluyendo consultas a expertos. A la hora de preparar y elaborar los actos delegados, la Comisión debe velar por una transmisión simultánea, puntual y adecuada de los documentos pertinentes al Parlamento Europeo y al Consejo.

- 32) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución relativas al funcionamiento de la plataforma de resolución de litigios en línea, a las modalidades de presentación de reclamaciones y a la cooperación con la red de puntos de contacto de resolución de litigios en línea. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n° 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión⁹. Debe utilizarse el procedimiento consultivo para la adopción de actos de ejecución relativos al formulario electrónico de reclamación, debido a su carácter puramente técnico. Debe utilizarse el procedimiento de examen para la adopción de las normas relativas a las modalidades de cooperación entre los asesores de resolución de litigios en línea de la red de puntos de contacto de resolución de litigios en línea.
- 33) En relación con la aplicación del presente Reglamento, la Comisión debe consultar, si procede, al Supervisor Europeo de Protección de Datos.
- 34) Dado que el objetivo del presente Reglamento, a saber, crear una plataforma de resolución de litigios en línea para litigios en línea que se rijan por normas comunes, no pueden ser alcanzados de manera suficiente por los Estados miembros debido a la dimensión o a los efectos de la acción y, por consiguiente, pueden lograrse mejor a nivel de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.
- 35) El presente Reglamento respeta los derechos fundamentales y observa los principios reconocidos, en particular, en la Carta de los Derechos Fundamentales de la Unión Europea y, en concreto, en sus artículos 7, 8, 38 y 47.

⁹ DO L 55 de 28.2.2011, p. 13.

- 36) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n° 45/2001 emitió su dictamen el 12 de enero de 2012¹⁰.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Capítulo I
Disposiciones Generales

Artículo 1
Objeto

El objetivo del presente Reglamento es contribuir, a través de la consecución de un elevado nivel de protección del consumidor, al correcto funcionamiento del mercado interior, en particular de su dimensión digital, proporcionando una plataforma europea de resolución de litigios en línea que facilite la resolución extrajudicial de litigios entre consumidores y comerciantes en línea de forma independiente, imparcial, transparente, eficaz y equitativa.

Artículo 2
Ámbito de aplicación

1. El presente Reglamento se aplicará a la resolución extrajudicial de litigios relativos a obligaciones contractuales derivadas de contratos de compraventa o de prestación de servicios celebrados en línea entre un consumidor residente en la Unión y un comerciante establecido en la Unión mediante la intervención de una entidad de resolución alternativa incluida en la lista con arreglo al artículo 20, apartado 2, de la Directiva

2013/11/UE en la que intervenga una plataforma de resolución de litigios en línea.

2. El presente Reglamento se aplicará a la resolución extrajudicial de los litigios contemplados en el apartado 1 iniciados por un comerciante frente a un consumidor, en la medida en que la legislación del Estado miembro de residencia habitual del consumidor admita que tales litigios se resuelvan a través de la intervención de una entidad de resolución alternativa.

3. Los Estados miembros informarán a la Comisión de si su legislación permite o no que los litigios indicados en el apartado 1 iniciados por un comerciante frente a un consumidor se resuelvan a través de la intervención de una entidad de resolución alternativa. En el momento en que las autoridades competentes notifiquen la lista contemplada en el artículo 20, apartado 2, de la Directiva 2013/11/UE, informarán a la Comisión de cuáles son las entidades de resolución alternativa competentes para conocer de tales litigios.

4. La aplicación del presente Reglamento a los litigios contemplados en

¹⁰ DO C 136 de 11.5.2012, p. 1.

el apartado 1 iniciados por un comerciante frente a un consumidor no impondrá a los Estados miembros la obligación de garantizar que las entidades de resolución alternativa ofrezcan procedimientos de resolución extrajudicial de este tipo de litigios.

Artículo 3
**Relación con otros actos
jurídicos de la Unión**

La presente Directiva se entenderá sin perjuicio de las disposiciones de la Directiva 2008/52/CE.

Artículo 4
Definiciones

1. A efectos del presente Reglamento, se entenderá por:

a) «consumidor»: un consumidor con arreglo a la definición del artículo 4, apartado 1, letra a), de la Directiva 2013/11/UE;

b) «comerciante»: un comerciante con arreglo a la definición del artículo 4, apartado 1, letra b), de la Directiva 2013/11/UE;

c) «contrato de compraventa»: un contrato de compraventa con arreglo a la definición del artículo 4, apartado 1, letra c), de la Directiva 2013/11/UE;

d) «contrato de prestación de servicios»: un contrato de prestación de servicios con arreglo a la definición del artículo 4, apartado 1, letra d), de la Directiva 2013/11/UE;

e) «contrato de compraventa o de prestación de servicios celebrado en línea»: un contrato de compraventa o de prestación de servicios en el que el comerciante o su intermediario haya ofrecido mercancías o servicios a través de un sitio de internet o por otros medios electrónicos y el consumidor haya encargado dichas mercancías o servicios en dicho sitio de internet o por otros medios electrónicos;

f) «mercado en línea»: un prestador de servicios de la sociedad de la información, conforme a la definición del artículo 2, letra b), de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)¹¹, que permite a los consumidores y comerciantes celebrar contratos de compraventa y de prestación de servicios en línea en el sitio de internet del mercado en línea;

g) «medio electrónico»: un equipo electrónico de tratamiento (incluida la compresión digital) y almacenamiento de datos en el que todas las operaciones de transmisión, envío y recepción se hagan por medios alámbricos, radiofónicos, ópticos u otros medios electromagnéticos;

h) «procedimiento de resolución alternativa de litigios» (en lo sucesivo, «procedimiento de resolución alternativa»): procedimiento de resolución

¹¹ DO L 178 de 17.7.2000, p. 1.

extrajudicial de litigios a que se refiere el artículo 2;

i) «entidad de resolución alternativa de litigios» (en lo sucesivo, «entidad de resolución alternativa»): una entidad de resolución alternativa con arreglo a la definición del artículo 4, apartado 1, letra h), de la Directiva 2013/11/UE;

j) «parte reclamante»: consumidor o comerciante que haya presentado una reclamación a través de la plataforma de resolución de litigios en línea;

k) «parte reclamada»: consumidor o comerciante contra quien se haya presentado una reclamación a través de la plataforma de resolución de litigios en línea;

l) «autoridad competente»: una autoridad con arreglo a la definición

del artículo 4, apartado 1, letra i), de la Directiva 2013/11/UE;

m) «datos personales»: toda información sobre una persona física identificada o identificable (en lo sucesivo, «titular de los datos»). Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

2. El lugar de establecimiento del comerciante y de la entidad de resolución se determinará, respectivamente, de acuerdo con el artículo 4, apartados 2 y 3, de la Directiva 2013/11/UE.

Capítulo II

Plataforma de Resolución de Litigios en Línea

Artículo 5

Establecimiento de la plataforma de resolución de litigios en línea

1. La Comisión desarrollará la plataforma de resolución de litigios en línea y será responsable de su funcionamiento, incluidas todas las funciones de traducción necesarias a efectos del presente Reglamento, de su mantenimiento, su financiación y la seguridad de los datos con los que opere. La plataforma de resolución de litigios en línea deberá ser de fácil utilización por los usuarios. En el desarrollo, el

funcionamiento y el mantenimiento de la plataforma de resolución de litigios en línea se velará por el respeto de la intimidad de sus usuarios desde la fase de diseño («protección de la intimidad mediante el diseño») y por que, en la medida de lo posible, dicha plataforma sea accesible y utilizable por todas las personas, incluidos los usuarios vulnerables («diseño para todos»).

2. La plataforma de resolución de litigios en línea constituirá una ventanilla única para los consumidores y comerciantes que deseen resolver

extrajudicialmente los litigios incluidos en el ámbito de aplicación del presente Reglamento. Será un sitio de internet interactivo al que se podrá acceder de forma electrónica y gratuita en todas las lenguas oficiales de las instituciones de la Unión.

3. La Comisión facilitará el acceso a la plataforma de resolución de litigios en línea, de modo apropiado, a través de sus sitios de internet, proporcionando información a los ciudadanos y a las empresas de la Unión y, en particular, a través del portal «Tu Europa» creado de conformidad con la Decisión 2004/387/CE.

4. La plataforma de resolución de litigios en línea desempeñará las siguientes funciones:

a) facilitar un formulario electrónico de reclamación que la parte reclamante pueda rellenar, de conformidad con el artículo 8;

b) informar de la reclamación a la parte reclamada;

c) determinar la entidad o entidades de resolución alternativa competentes y transmitir la reclamación a la entidad de resolución alternativa que las partes hayan acordado utilizar, de conformidad con el artículo 9;

d) ofrecer gratuitamente un sistema electrónico de tramitación de asuntos que permita a las partes y a la entidad de resolución alternativa tramitar en línea el procedimiento de resolución de litigios a través de la plataforma de resolución de litigios en línea;

e) proporcionar a las partes y a la entidad de resolución alternativa la traducción de la información que sea necesaria para la resolución del litigio y que se intercambie a través de la plataforma de resolución de litigios en línea;

f) facilitar un formulario electrónico del que se servirán las entidades de resolución alternativa para transmitir la información contemplada en el artículo 10, letra c);

g) proporcionar un sistema de comentarios que permita a las partes expresar su opinión sobre el funcionamiento de la plataforma de resolución de litigios en línea y sobre la entidad de resolución alternativa que haya conocido de su litigio;

h) poner a disposición pública lo siguiente:

i) información general sobre la resolución alternativa de litigios como forma de resolución extrajudicial de litigios,

ii) información sobre las entidades de resolución alternativa incluidas en la lista con arreglo al artículo 20, apartado 2, de la Directiva 2013/11/UE que sean competentes para conocer de los litigios incluidos en el ámbito de aplicación del presente Reglamento,

iii) un manual

iv) información

v) datos

5. La Comisión velará por que la información mencionada en el apartado 4, letra h), sea exacta, esté actualizada y se presente de manera clara, comprensible y fácilmente accesible.

6. Las entidades de resolución alternativa incluidas en la lista con arreglo al artículo 20, apartado 2, de la Directiva 2013/11/UE que sean competentes para conocer de los litigios incluidos en el ámbito de aplicación del presente Reglamento se registrarán electrónicamente en la plataforma de resolución de litigios en línea.

7. La Comisión, mediante actos de ejecución, adoptará medidas relativas a las modalidades de ejercicio de las funciones contempladas en el apartado 4 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 16, apartado 3, del presente Reglamento.

Artículo 6

Ensayo de la plataforma de resolución de litigios en línea

1. A más tardar el 9 de enero de 2015, la Comisión realizará un ensayo de la funcionalidad técnica y la facilidad de utilización por el usuario de la plataforma de resolución de litigios en línea y del formulario de reclamación, también en lo que atañe a la traducción. El ensayo se realizará y se evaluará en cooperación con expertos de los Estados miembros y de representantes de los consumidores y de los comerciantes en materia de resolución de litigios en línea. La

Comisión presentará un informe al Parlamento Europeo y al Consejo sobre el resultado del ensayo y adoptará las medidas oportunas para resolver los problemas potenciales con objeto de garantizar el funcionamiento efectivo de la plataforma de resolución de litigios en línea.

2. En el informe a que se refiere el apartado 1 del presente artículo, la Comisión determinará asimismo las medidas técnicas y organizativas que se propone aplicar para garantizar el cumplimiento por la plataforma de resolución de litigios en línea de los requisitos de protección de la intimidad previstos en el Reglamento (CE) n°45/2001.

Artículo 7

Red de puntos de contacto de resolución de litigios en línea

1. Cada Estado miembro nombrará un punto de contacto de resolución de litigios en línea y comunicará a la Comisión su nombre y datos de contacto. Los Estados miembros podrán conferir la responsabilidad de los puntos de contacto de resolución de litigios en línea a sus centros de la Red de Centros Europeos del Consumidor, a las asociaciones de consumidores o a cualquier otro organismo. Cada punto de contacto de resolución de litigios en línea incorporará al menos a dos asesores de resolución de litigios en línea.

2. Los puntos de contacto de resolución de litigios en línea prestarán apoyo a la resolución de litigios rela-

cionados con reclamaciones presentadas a través de la plataforma de resolución de litigios en línea y desempeñarán las siguientes funciones:

a) previa solicitud, facilitar la comunicación entre las partes y la entidad de resolución alternativa competente, lo que podrá incluir, en particular:

- i) prestar ayuda para la presentación de la reclamación y, en su caso, de la documentación pertinente,
- ii) facilitar a las partes y a las entidades de resolución alternativa información de carácter general sobre los derechos que asisten al consumidor, en relación con los contratos de compraventa o de prestación de servicios, en el Estado miembro del punto de contacto de resolución de litigios en línea del que forme parte el correspondiente asesor de resolución de litigios en línea,
- iii) facilitar información sobre el funcionamiento de la plataforma de resolución de litigios en línea,
- iv) facilitar a las partes explicaciones sobre las normas de procedimiento aplicadas por las entidades de resolución alternativa identificadas,
- v) informar a la parte reclamante sobre otras vías de recurso cuando no sea posible resolver un litigio a través de la plata-

forma de resolución de litigios en línea;

b) presentar cada dos años a la Comisión y a los Estados miembros un informe de actividad basado en la experiencia práctica obtenida en el desempeño de sus funciones.

3. El punto de contacto de resolución de litigios en línea no tendrá obligación de desempeñar las funciones indicadas en el apartado 2 cuando se trate de litigios cuyas partes tengan su residencia habitual en el mismo Estado miembro.

4. No obstante lo dispuesto en el apartado 3, los Estados miembros, atendiendo a las circunstancias nacionales, podrán decidir que el punto de contacto de resolución de litigios en línea desempeñe una o varias de las funciones indicadas en el apartado 2 cuando se trate de litigios en los que las partes tengan su residencia habitual en el mismo Estado miembro.

5. La Comisión creará una red de puntos de contacto (en lo sucesivo, «red de puntos de contacto de resolución de litigios en línea») que permitirá la cooperación entre los puntos de contacto y contribuirá al desempeño de las funciones enumeradas en el apartado 2.

6. La Comisión convocará, al menos dos veces al año, una reunión de los miembros de la red de puntos de contacto de resolución de litigios en línea para permitir un intercambio de buenas prácticas y debatir los posibles

problemas recurrentes encontrados durante la utilización de la plataforma de resolución de litigios en línea.

7. La Comisión, mediante actos de ejecución, adoptará las normas relativas a las modalidades de cooperación entre los puntos de contacto de resolución de litigios en línea. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 16, apartado 3.

Artículo 8

Presentación de reclamaciones

1. Para presentar una reclamación ante la plataforma de resolución de litigios en línea, la parte reclamante rellenará el formulario electrónico de reclamación. El formulario de reclamación deberá ser de fácil utilización por el usuario y fácilmente accesible a partir de la plataforma de resolución de litigios en línea.

2. La información que debe presentar la parte reclamante deberá ser suficiente para determinar la entidad de resolución alternativa competente. Dicha información se enumera en el anexo al presente Reglamento. La parte reclamante podrá adjuntar documentos en apoyo de su reclamación.

3. A fin de tener en cuenta los criterios por los cuales las entidades de resolución alternativa incluidas en la lista con arreglo al artículo 20, apartado 2, de la Directiva 2013/11/UE y que tramitan litigios al amparo

del presente Reglamento definen sus respectivos ámbitos de actuación, la Comisión estará facultada para adoptar actos delegados con arreglo al artículo 17 del presente Reglamento para adaptar la información enumerada en el anexo del presente Reglamento.

4. La Comisión establecerá mediante actos de ejecución las normas relativas a las modalidades del formulario electrónico de reclamación. Dichos actos de ejecución se adoptarán con arreglo al procedimiento consultivo contemplado en el artículo 16, apartado 2.

5. Mediante el formulario electrónico de reclamación y sus documentos adjuntos se procesarán únicamente datos que sean exactos, pertinentes y no excesivos con relación a los fines para los que se recaben.

Artículo 9

Tramitación y transmisión de reclamaciones

1. Las reclamaciones presentadas ante la plataforma de resolución de litigios en línea se tramitarán si todas las secciones necesarias del formulario electrónico de reclamación han sido cumplimentadas.

2. Si el formulario de reclamación no se ha cumplimentado en su totalidad, se informará a la parte reclamante de que la reclamación no puede seguir tramitándose a no ser que se facilite la información que falte.

3. Al recibir un formulario de reclamación cumplimentado en su totalidad, la plataforma de resolución de litigios en línea transmitirá la reclamación de un modo fácilmente comprensible y sin demora a la parte reclamada, en una de las lenguas oficiales de las instituciones de la Unión por la que haya optado dicha parte, junto con los datos siguientes:

a) la información de que las partes deben ponerse de acuerdo sobre una entidad de resolución alternativa a la que habrá de transmitirse la reclamación y de que, si las partes no llegan a un acuerdo o no se identifica ninguna entidad de resolución alternativa competente, la reclamación no podrá seguir tramitándose;

b) la información sobre la entidad o entidades de resolución alternativa que sean competentes para resolver el litigio, si constan mencionadas en el formulario electrónico de reclamación o si la plataforma de resolución de litigios en línea las determina basándose en la información facilitada en el formulario;

c) en caso de que la parte reclamada sea un comerciante, un requerimiento a declarar en un plazo de diez días naturales:

- si se compromete o está obligado a recurrir a una entidad de resolución alternativa concreta para resolver los litigios con consumidores, y
- salvo en caso de que esté obligado a recurrir a una entidad de resolución alternativa

concreta, si está dispuesto a recurrir a cualesquiera de las entidades de resolución alternativa a que se refiere la letra b);

d) en caso de que la parte reclamada sea un consumidor y el comerciante esté obligado a recurrir a una entidad de resolución alternativa concreta, un requerimiento a aceptar en el plazo de diez días naturales dicha entidad o, en caso de que el comerciante no esté obligado a recurrir a una entidad de resolución alternativa concreta, un requerimiento a que seleccione una o más de las entidades de resolución alternativa a que se refiere la letra b);

e) el nombre y los datos de contacto del punto de contacto de resolución de litigios en línea en el Estado miembro en que esté establecida o resida habitualmente la parte reclamada, así como una breve descripción de las funciones contempladas en el artículo 7, apartado 2, letra a).

4. Una vez que reciba de la parte reclamada la información prevista en el apartado 3, letras c) o d), la plataforma de resolución de litigios en línea comunicará a la parte reclamante de un modo fácilmente comprensible y sin demora, en una de las lenguas oficiales de las instituciones de la Unión por la que haya optado dicha parte, la información siguiente:

a) la información a que se refiere el apartado 3, letra a);

b) en caso de que la parte reclamante sea un consumidor, la información sobre la entidad o entidades de resolución alternativa comunicadas por el comerciante conforme al apartado 3, letra c), y un requerimiento a aceptar una entidad de resolución alternativa en el plazo de diez días naturales;

c) en caso de que la parte reclamante sea un comerciante que no esté obligado a recurrir a una entidad de resolución alternativa concreta, la información sobre la entidad o entidades de resolución alternativa comunicada por el consumidor conforme al apartado 3, letra d), y un requerimiento a aceptar una entidad de resolución alternativa en el plazo de diez días naturales;

d) el nombre y los datos de contacto del punto de contacto de resolución de litigios en línea en el Estado miembro en que esté establecida o tenga su domicilio habitual parte reclamante, así como una breve descripción de las funciones contempladas en el artículo 7, apartado 2, letra a).

5. La información contemplada en el apartado 3, letra b), y en el apartado 4, letras b) y c), incluirá una descripción de las siguientes características de cada entidad de resolución alternativa:

a) la denominación, los datos de contacto y la dirección del sitio de internet de la entidad de resolución alternativa;

b) en su caso, las tarifas del procedimiento de resolución alternativa;

c) el idioma o idiomas en que podrá tramitarse el procedimiento de resolución alternativa;

d) la duración media del procedimiento de resolución alternativa;

e) el carácter vinculante o no vinculante del resultado del procedimiento de resolución alternativa;

f) los motivos por los cuales la entidad de resolución alternativa podrá negarse a conocer de un litigio determinado con arreglo al artículo 5, apartado 4, de la Directiva 2013/11/UE.

6. La plataforma de resolución de litigios en línea transmitirá la reclamación automáticamente y sin demora a la entidad de resolución alternativa a la que las partes hayan acordado someter el litigio de conformidad con los apartados 3 y 4.

7. La entidad de resolución alternativa a la que se haya transmitido la reclamación informará sin demora a las partes de su aceptación o negativa a tramitar el litigio de acuerdo con el artículo 5, apartado 4, de la Directiva 2013/11/UE. La entidad de resolución alternativa que haya aceptado tramitar el litigio informará asimismo a las partes sobre sus normas de procedimiento y, en su caso, sobre las costas del procedimiento de resolución de litigios de que se trate.

8. Si, transcurridos 30 días naturales desde la presentación del formulario

de reclamación, las partes no hubieran llegado a un acuerdo sobre una entidad de resolución alternativa, o si la entidad de resolución alternativa se negara a conocer del litigio, se pondrá fin a la tramitación de la reclamación. Se informará a la parte reclamante de la posibilidad de ponerse en contacto con un asesor de resolución de litigios en línea para obtener información de carácter general sobre otras vías de recurso.

Artículo 10
Resolución del litigio

La entidad de resolución alternativa que consienta en tramitar una reclamación con arreglo al artículo 9 del presente Reglamento:

- a) concluirá el procedimiento de resolución alternativa dentro del plazo contemplado en el artículo 8, letra e), de la Directiva 2013/11/UE;
- b) no requerirá la comparecencia de las partes o de sus representantes, a no ser que las normas de procedimiento contemplen esa posibilidad y las partes lo consientan;
- c) transmitirá sin demora la siguiente información a la plataforma de resolución de litigios en línea:
 - i) la fecha de recepción del expediente de reclamación,
 - ii) el objeto del litigio,
 - iii) la fecha de conclusión del procedimiento de resolución alternativa,

iv) el resultado del procedimiento de resolución alternativa;

d) no estará sujeta a tramitar el procedimiento de resolución alternativa a través de la plataforma de resolución de litigios en línea.

Artículo 11
Base de datos

La Comisión tomará las medidas necesarias para crear y mantener una base de datos electrónica en la que almacenará la información tratada con arreglo al artículo 5, apartado 4, y al artículo 10, letra c), teniendo debidamente en cuenta lo dispuesto en el artículo 13, apartado 2.

Artículo 12
Tratamiento de datos personales

1. Se concederá acceso a la información, incluidos los datos personales, relacionada con un litigio y almacenada en la base de datos contemplada en el artículo 11 únicamente a la entidad de resolución alternativa a la que se haya remitido el litigio con arreglo al artículo 10 y para los fines contemplados en el artículo 9. También se concederá acceso a esa misma información, en la medida necesaria, a los puntos de contacto de resolución de litigios en línea para los fines contemplados en el artículo 7, apartados 2 y 4.

2. La Comisión tendrá acceso a la información tratada con arreglo al artículo 10 para los fines de seguimiento del uso y funcionamiento de

la plataforma de resolución de litigios en línea y para redactar los informes contemplados en el artículo 21. Tratará los datos personales de los usuarios de la plataforma de resolución de litigios en línea únicamente en la medida necesaria para la utilización y el mantenimiento de dicha plataforma, lo que incluye el seguimiento de la utilización de la plataforma por parte de las entidades de resolución alternativa y los puntos de contacto de resolución de litigios en línea.

3. Los datos personales relacionados con un litigio se almacenarán en la base de datos contemplada en el apartado 1 del presente artículo únicamente durante el tiempo necesario para alcanzar los fines para los que fueron recogidos y para garantizar que los interesados puedan acceder a sus datos personales con el fin de ejercer sus derechos; dichos datos serán borrados automáticamente en un plazo máximo de seis meses a partir de la fecha en que concluya el litigio sometido a la plataforma de resolución de litigios en línea con arreglo al artículo 10, letra c), inciso iii). Dicho período de conservación también se aplicará a los datos personales que la entidad de resolución alternativa o el punto de contacto de resolución de litigios en línea que haya tratado el litigio guarde en archivos nacionales, excepto en el caso de que las normas de procedimiento de la entidad de resolución alternativa o las disposiciones específicas del ordenamiento jurídico nacional contemplen un período de conservación más prolongado.

4. Todo asesor de resolución de litigios en línea será considerado responsable del tratamiento respecto de sus propias actividades de tratamiento de datos en virtud del presente Reglamento, con arreglo al artículo 2, letra d), de la Directiva 95/46/CE, y garantizará que dichas actividades respeten la normativa nacional adoptada en cumplimiento de la Directiva 95/46/CE en el Estado miembro del punto de contacto de resolución de litigios en línea del que forme parte dicho asesor.

5. Toda entidad de resolución alternativa será considerada responsable del tratamiento respecto de sus propias actividades de tratamiento de datos en virtud del presente Reglamento, con arreglo al artículo 2, letra d), de la Directiva 95/46/CE, y garantizará que dichas actividades respeten la normativa nacional adoptada en cumplimiento de la Directiva 95/46/CE en el Estado miembro en el que esté establecida.

6. La Comisión será considerada responsable del tratamiento, con arreglo al artículo 2, letra d), del Reglamento (CE) n° 45/2001, por lo que se refiere a las responsabilidades que le incumben en virtud del presente Reglamento y el tratamiento de datos personales que estas implican.

Artículo 13

Confidencialidad y seguridad de los datos

1. Los puntos de contacto de resolución de litigios en línea estarán

sometidos a las normas de secreto profesional u otras obligaciones equivalentes de confidencialidad establecidas en la normativa del Estado miembro de que se trate.

2. La Comisión adoptará las medidas de carácter técnico y organizativo adecuadas para garantizar la seguridad de la información tratada en virtud del presente Reglamento, incluido un control adecuado del acceso a los datos, un plan de seguridad y la gestión de los incidentes de seguridad, con arreglo al artículo 22 del Reglamento (CE) nº 45/2001.

Artículo 14

Información a los consumidores

1. Los comerciantes establecidos en la Unión que celebren contratos de compraventa o de prestación de servicios en línea y los mercados en línea establecidos en la Unión ofrecerán en sus sitios de internet un enlace electrónico a la plataforma de resolución de litigios en línea. Dicho enlace será de fácil acceso para los consumidores. Los comerciantes establecidos en la Unión que celebren en línea contratos de compraventa o de prestación de servicios deberán informar asimismo a los consumidores de sus direcciones de correo electrónico.

2. Los comerciantes establecidos en la Unión que celebren contratos de compraventa o de prestación de servicios en línea y que se hayan comprometido o estén obligados a recurrir a una o varias entidades de resolución alternativa para resolver los litigios con

los consumidores informarán a estos de la existencia de una plataforma de resolución de litigios en línea así como de la posibilidad de recurrir a tal plataforma para resolver sus litigios. Proporcionarán en su sitio de internet un enlace electrónico a dicha plataforma y, en caso de que la oferta se realice mediante correo electrónico, se incluirá en este dicho enlace. Se facilitará también esa información, en su caso, en los términos y condiciones generales aplicables al contrato de compraventa o de prestación de servicios en línea.

3. Lo dispuesto en los apartados 1 y 2 del presente artículo se entenderá sin perjuicio del artículo 13 de la Directiva 2013/11/UE y de las disposiciones relativas a la información del consumidor sobre procedimientos de resolución extrajudicial de litigios contenidas en otros actos jurídicos de la Unión, que se aplicará además de lo dispuesto en el presente artículo.

4. La lista de entidades de resolución alternativa a que se refiere el artículo 20, apartado 4, de la Directiva 2013/11/UE, así como sus actualizaciones, se publicará en la plataforma de resolución de litigios en línea.

5. Los Estados miembros velarán por que las entidades de resolución alternativa, los centros de la Red de Centros Europeos del Consumidor, las autoridades competentes definidas en el artículo 18, apartado 1, de la Directiva 2013/11/UE y, si procede, los organismos designados de conformidad con el artículo 14, apartado

2, de la Directiva 2013/11/UE proporcionen un enlace electrónico a la plataforma de resolución de litigios en línea.

6. Los Estados miembros animarán a las asociaciones de consumidores y a las asociaciones empresariales a que proporcionen un enlace electrónico a la plataforma de resolución de litigios en línea.

7. Cuando los comerciantes deban facilitar información con arreglo a los

apartados 1 y 2 y a las disposiciones a que se refiere el apartado 3, presentarán, en lo posible, esa información de manera conjunta.

Artículo 15

Función de las autoridades competentes

La autoridad competente de cada Estado miembro evaluará si las entidades de resolución alternativa establecidas en dicho Estado miembro cumplen con las obligaciones definidas en el presente Reglamento.

Capítulo III

Disposiciones Finales

Artículo 16

Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n° 182/2011.

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 4 del Reglamento (UE) n° 182/2011.

3. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n° 182/2011.

4. Cuando el dictamen del comité a tenor de los apartados 2 y 3 deba obtenerse mediante un procedimiento escrito, se pondrá fin a dicho procedimiento sin resultado si, en el plazo para la emisión del dictamen, el

presidente del comité así lo decide o si una mayoría simple de miembros del comité así lo solicita.

Artículo 17

Ejercicio de la delegación

1. Los poderes para adoptar actos delegados otorgados a la Comisión estarán sujetos a las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar actos delegados a que se refiere el artículo 8, apartado 3, se otorgarán por tiempo indefinido a partir del 8 de julio de 2013.

3. La delegación de poderes a que se refiere al artículo 8, apartado 3, podrá ser revocada en todo momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los

poderes que especifique dicha decisión. Surtilá efecto el día siguiente al de la publicación de la decisión en el *Diario Oficial de la Unión Europea* o en una fecha posterior que se precisará en dicha decisión. No afectará a la validez de cualesquiera actos delegados que ya estén en vigor.

4. Tan pronto como adopte un acto delegado, la Comisión lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Un acto delegado adoptado con arreglo al artículo 8, apartado 3, entrará en vigor únicamente si ni el Parlamento Europeo ni el Consejo han formulado objeciones en un plazo de dos meses a partir de la fecha de notificación de dicho acto al Parlamento Europeo y al Consejo, o si, antes de que expire dicho plazo, tanto el Parlamento Europeo como el Consejo han informado a la Comisión de que no tienen la intención de formular objeciones. Dicho plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 18 **Sanciones**

Los Estados miembros determinarán el régimen de sanciones aplicable a las infracciones al presente Reglamento y adoptarán todas las medidas necesarias para garantizar su aplicación. Las sanciones previstas deberán ser eficaces, proporcionadas y disuasorias.

Artículo 19 **Modificación del Reglamento (CE) nº 2006/2004**

En el anexo del Reglamento (CE) nº 2006/2004 del Parlamento Europeo y del Consejo¹² se añade el punto siguiente:

«21. Reglamento (UE) nº 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo (DO L 165 de 18.6.2013, p. 1): artículo 14.»

Artículo 20 **Modificación de la Directiva 2009/22/CE**

La Directiva 2009/22/CE del Parlamento Europeo y del Consejo¹³ queda modificada como sigue:

1) En el artículo 1, apartados 1 y 2, y en el artículo 6, apartado 2, letra b), se sustituyen las palabras «las Directivas enumeradas en el anexo I» por «los actos de la Unión enumerados en el anexo I».

2) En el título del anexo I, se sustituyen las palabras «LISTA DE DIRECTIVAS CONTEMPLADAS» por «LISTA DE ACTOS DE LA UNIÓN CONTEMPLADOS».

3) En el anexo I se añade el punto siguiente:

¹² DO L 364 de 9.12.2004, p. 1.

¹³ DO L 110 de 1.5.2009, p. 30.

«15. Reglamento (UE) nº 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo (DO L 165 de 18.6.2013, p. 1): artículo 14.».

Artículo 21

Informes

1. La Comisión presentará anualmente al Parlamento Europeo y al Consejo un informe sobre el funcionamiento de la plataforma de resolución de litigios en línea, el primero de los cuales se presentará un año después de que dicha plataforma haya entrado en funcionamiento.

2. A más tardar el 9 de julio de 2018 y posteriormente cada tres años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la aplicación del presente Reglamento, que tratará en particular de la facilidad de utilización del formulario de reclamación y de la posible necesidad de adaptar la información enumerada en el anexo del presente Reglamento. El informe irá acompañado, si procede, de propuestas para la adaptación del presente Reglamento.

3. Cuando los informes a que se refieren los apartados 1 y 2 deban presentarse el mismo año, se presentará un único informe conjunto.

Artículo 22

Entrada en vigor

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. El presente Reglamento será aplicable a partir del 9 de enero de 2016, a excepción de las disposiciones siguientes:

– artículo 2, apartado 3, y artículo 7, apartados 1 y 5, que serán aplicables a partir del 9 de julio de 2015,

– artículo 5, apartados 1 y 7, artículo 6, artículo 7, apartado 7, artículo 8, apartados 3 y 4, y artículos 11, 16 y 17, que serán aplicables a partir del 8 de julio de 2013.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Estrasburgo, el 21 de mayo de 2013.

Por el Parlamento Europeo

El Presidente
M. Schulz

Por el Consejo

La Presidenta
L. Creighton

ANEXO

Información que deberá suministrarse al presentar una reclamación

- 1) Indicación de si la parte reclamante es un consumidor o un comerciante.
- 2) Nombre y dirección de correo electrónico y ordinario del consumidor.
- 3) Nombre y dirección de correo electrónico y ordinario del comerciante.
- 4) Nombre y dirección de correo electrónico y ordinario del representante de la parte reclamante, si procede.
- 5) Idioma o idiomas de la parte reclamante, si procede.
- 6) Idioma de la parte reclamada, si se conoce.
- 7) Tipo de mercancía o de servicio a que se refiere la reclamación.
- 8) Indicación de si la mercancía o el servicio fue ofrecido por el comerciante y encargado por el consumidor a través de un sitio de internet o por otros medios electrónicos.
- 9) Precio de la mercancía o del servicio adquirido.
- 10) Fecha en que el consumidor adquirió la mercancía o el servicio.
- 11) Indicación de si el consumidor ha entablado contacto directo con el comerciante.
- 12) Indicación de si el litigio está siendo o ha sido previamente examinado por una entidad de resolución alternativa o por un órgano jurisdiccional.
- 13) Tipo de reclamación.
- 14) Descripción de la reclamación.
- 15) En caso de que la parte reclamante sea un consumidor, indicación de la entidad o las entidades de resolución alternativa que el comerciante esté obligado o se haya comprometido a utilizar con arreglo al artículo 13, apartado 1, de la Directiva 2013/11/UE, si se conocen.
- 16) En caso de que la parte reclamante sea un comerciante, indicación de la entidad o de las entidades de resolución alternativa que este se haya comprometido o esté obligado a utilizar.

JURISPRUDENCIA

La posición del Tribunal Supremo de Justicia venezolano respecto a las pruebas documentales electrónicas

Mariliana Rico Carrillo*

I. Consideraciones previas

Durante el año 2015, el Tribunal Supremo de Justicia venezolano ha emitido diversas sentencias donde nuevamente se ha considerado la prueba documental electrónica, en particular el correo electrónico. De todas estas decisiones, disponibles en el sitio web del TSJ, hemos escogido tres, donde se observan aciertos y contradicciones, éstas últimas provenientes en su mayoría de las partes y de los jueces de primera y segunda instancia, respecto a la admisión, valoración e idoneidad probatoria de estos documentos. Es de destacar que la posición del TSJ sobre este aspecto va adquiriendo mayor claridad y apego a la legislación especial que rige esta materia.

Si bien en algunos casos se procede conforme a la normativa especial aplicable a este tipo de documentos, contenida en la Ley de Mensajes de Datos y Firmas Electrónicas (LMDFE) y se admiten adecuadamente los correos electrónicos como pruebas libres, acompañados de una experticia a efectos de comprobar los requisitos que según el legislador deben estar presentes para que este tipo de documentos pueda desempeñar su función probatoria; en otros, encontramos argumentos de la parte contra quien se promueve la prueba electrónica que contradicen los principios de este cuerpo legal, al intentar negar el valor de los mensajes de datos sobre la base de una supuesta exigencia legal, relativa a la certificación de los equipos informáticos usados en la elaboración y

* Doctora en Derecho mención Cum Laude por la Universidad Carlos III de Madrid. Catedrática de Derecho Mercantil y Nuevas Tecnologías de la Universidad Católica del Táchira (Venezuela). Profesora invitada de la Universidad Carlos III de Madrid en programas de Máster y Doctorado. Árbitro especialista en Nuevas Tecnologías, certificado por la Corte Suprema de Florida de los Estados Unidos de América. Secretaria General de la Federación Iberoamericana de Asociaciones de Derecho Informática. Profesora invitada en diversas universidades e institutos de investigación en España, Estados Unidos y Latinoamérica. Conferencista internacional y autora de numerosas publicaciones en el área de Derecho y Nuevas Tecnologías.

transmisión de estos documentos como condición indispensable a efectos de cumplir tal función, requisito inexistente en la LMDFE.

También se observa que la prueba documental electrónica es privada de su condición probatoria, al negar la posibilidad de exhibición de los mensaje de datos, en los términos consagrados en las normas procesales. Los juzgadores fundamentan su decisión en la imposibilidad material de exhibir el documento, atendiendo a su naturaleza intangible, sin tener en cuenta que la exhibición es un proceso que ha sido diseñado para los documentos en papel y que la propia LMDFE establece el procedimiento y los criterios que deben tomarse en cuenta al momento de valorar el documento electrónico como instrumento probatorio. En razón de estas circunstancias, consideramos pertinente realizar un breve comentario de estas sentencias a objeto de establecer con claridad el procedimiento que debe seguirse a la hora de incorporar un documento electrónico a las actuaciones judiciales y determinar su valor probatorio, prestando especial atención a la forma de promoción, valoración y exhibición de las pruebas documentales electrónicas.

II. Criterios jurisprudenciales relativos a la prueba documental electrónica en las decisiones del TSJ del año 2015

1. Sobre la forma de promoción

Sentencia de Sala de Casación Civil de 27 de marzo de 2015¹

Esta sentencia es de especial relevancia en relación con la forma de promoción de la prueba documental electrónica, ya que sigue los criterios básicos para la aportación de este tipo de pruebas al proceso, establecidos en la LMDFE. Antes de pasar al análisis de su contenido, consideramos pertinente recordar el texto del artículo 4, que en relación con los mensajes de datos dispone:

Los Mensajes de Datos (sic) tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos... 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.

En el caso objeto de la controversia, analizado por la Sala de Casación Social, se promovió como prueba libre un mensaje de datos, junto con el informe de la experticia realizada por los profesionales de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE)

¹ El texto integro de la sentencia está disponible en <http://historico.tsj.gob.ve/decisiones/scc/marzo/175948-exe.000150-27315-2015-11-637.html> (Consulta: 20 de septiembre de 2015)

al servidor de correo electrónico, con el objeto de determinar la autenticidad de los mensajes enviados por medio de este servidor.

Es de destacar que éste es el criterio adecuado en cuanto a la incorporación de la prueba documental electrónica al proceso, ya que la propia LMDFE se refiere específicamente al sistema de prueba libre, regulado en el artículo 395 del Código de Procedimiento Civil venezolano. De acuerdo con este precepto, los medios de prueba libre se promoverán y evacuarán aplicando por analogía las disposiciones relativas a medios de prueba semejantes; en el caso de los correos electrónicos éstos entran en la categoría de documentos y como tales deben valorarse, sólo que se trata de documentos generados mediante técnicas informáticas y dado que el original es el soporte electrónico, será necesario la realización de una experticia para demostrar que el mensaje de datos cumple los requisitos establecidos en la LMDFE para catalogar estos documentos como originales.

En esta oportunidad, además de ratificarse la forma de incorporación al proceso como prueba libre, se demuestra la importancia de la prueba pericial a efectos de certificar la inalterabilidad del mensaje de datos, condición *sine qua non* para determinar el carácter de original de estos documentos. En el caso objeto de análisis, en el informe de la experticia se pudo constatar la integridad de la información. Con fines ilustrativos cabe reproducir el informe los expertos, quienes en el caso planteado concluyen:

Luego de haber analizado el material colectado mediante la aplicación del procedimiento forense antes descrito, cumplimos con informar que aun cuando no se pudo comprobar la identidad de la persona quien emitió los mensajes de correo electrónico, debido a que no están firmados electrónicamente conforme a lo contemplado en la Ley de Mensajes de Datos y Firmas Electrónicas, se pudo constatar a través de la validación de la cabecera y cuerpo del correo electrónico promovido en el escrito de prueba, lo siguiente: Integridad de la información enviada en el correo electrónico. El correo electrónico marcado B1, no fue modificado, manteniendo su integridad respecto a la fuente de la data original contenida en los servidores de correo de la empresa GoDaddy (sic)...

El texto del informe demuestra que el correo electrónico no fue modificado y mantiene su condición de original, tal como lo establece el artículo 7 de la LMDFE.

2. Sobre la valoración de la prueba: originales y copias

Sentencia de Sala de Casación Social de 30 de abril de 2015²

En el juicio laboral en primera instancia, la parte actora desconoció el valor de unos correos electrónicos incorporados al proceso al indicar:

...son documentos que no cumplen con lo contenido en la Ley de Mensaje, Datos y Firmas Electrónicas, pues se trata de un correo electrónico y que conforme a la Ley de Mensajes, Datos, y Firmas Electrónicas y al criterio sostenido por la Sala de Casación Social, debe certificarse el servidor u ordenador del cual emana este correo por el Instituto creado para tal fin, que no pasa en el caso de autos.

En esta oportunidad hemos de precisar que el juzgador no se pronuncia en forma específica sobre estas afirmaciones ni sobre el valor probatorio de los mensajes de datos en formato electrónico (documentos originales), su decisión solo se refiere a los correos electrónicos incorporados en forma impresa a las actas procesales, (copias).

En cuanto al carácter de original del documento electrónico cabe recordar que en sentencias anteriores, el TSJ se ha pronunciado sobre este aspecto al indicar que el soporte original de estos documentos está contenido en la base de datos del computador o en el servidor de la empresa y sobre esto es que debe recaer la prueba (Sentencias de la Sala de Casación Civil de 24 de octubre de 2007 y de 5 de octubre de 2011), sin embargo, no es necesaria la certificación de estos sistemas informáticos por el ente regulador para hacer valer el documento electrónico, como pretende la parte actora.

Respecto a la valoración del correo electrónico en forma impresa, la Sala procedió adecuadamente, siguiendo los principios de la LMDFE que establecen que en estos casos estamos en presencia de una copia, al entender que:

... conforme a el texto legal, la copia de un correo electrónico tiene el mismo valor que una copia simple, de manera que deben desecharse por haber sido cuestionada su certeza (lo que hizo la demandada al ser interrogada por el Juez de Juicio); asimismo, indicó la demandada que la documental inserta a los folios 14, 35 y 36 y del 39 al 73, del 130 al 133, ambos inclusive, son copias simples que desconoce.

² El texto íntegro de la sentencia está disponible en <http://historico.tsj.gob.ve/decisiones/scs/abril/176889-0287-30415-2015-14-036.html> (Consulta: 20 de septiembre de 2015)

Esta apreciación es ajustada a las exigencias legales, por cuanto los correos impresos fueron impugnados y no fue promovido un medio auxiliar de prueba que demostrara su certeza. La confusión en este caso proviene de la parte que intenta desconocer el valor probatorio del correo electrónico, quien incurre en confusión de conceptos al referirse a la necesidad de certificación del servidor u ordenador del cual emana el correo electrónico por parte de Instituto creado para tal fin (SUSCERTE), requisito que en ningún momento es exigido en la LMDFE.

De acuerdo con el artículo 8 de la LMDFE, para valorar un documento electrónico es necesario el cumplimiento de tres requisitos básicos: 1) que la información pueda ser consultada posteriormente (accesibilidad); 2) que conserve el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida (integridad); y 3) que se conserve todo dato que permita determinar el origen y el destino del mensaje de datos, la fecha y la hora en que fue enviado o recibido. El dispositivo citado establece la posibilidad de recurrir a los servicios de un tercero que pueda dar certeza del cumplimiento de estos requisitos, pero se trata de una facultad, mas no de una obligación, y el precepto no se refiere en ningún momento a la certificación de los sistemas informáticos. La previsión contenida en este artículo se refiere a las experticias, que bien pueden ser realizadas por organismos públicos o profesionales del sector privado, a objeto de determinar el cumplimiento de los requisitos legales³.

Como bien puede observarse, la LMDFE no menciona la certificación “...del servidor u ordenador del cual emana este correo por el Instituto creado para tal fin”, como elemento necesario a efectos de conceder valor probatorio a los mensajes de datos. Sobre este aspecto hemos de aclarar que si existe un tipo de certificación electrónica previsto en la ley, pero se refiere al certificado electrónico que atribuye certeza y validez a la firma electrónica que pudiera incorporar el documento, que en todo caso tampoco es un elemento que condicione la idoneidad probatoria de estos mensajes. Como vimos en la sentencia anterior, el propio TSJ ha considerado el valor probatorio de los correos electrónicos mediante un análisis pericial orientado a demostrar la autenticidad e integridad de los mensajes, sin exigir la certificación del computador o

³ Cabe reproducir aquí el contenido del artículo 8, que luego de enumerar los requisitos para considerar la eficacia probatoria de los documentos electrónicos, indica: “*nica en las condiciones previstas, no puede desecharse el documento que no incorpore una firma electrónica; on condici recordar que Toda persona podrá recurrir a los servicios de un tercero para dar cumplimiento a los requisitos señalados en este artículo*”. Como bien puede observarse, en ningún momento el dispositivo menciona que se trata de una certificación, ni se exige que para la practica de la experticia esté facultado únicamente el ente supervisor, que en Venezuela es la Superintendencia de Servicios de Certificación Electrónica.

servidor que se utiliza para el envío del mensaje, ni la existencia de un certificado que avale la firma electrónica.

3. Sobre la exhibición del correo electrónico

Sentencia de la Sala de Casación Social de 25 mayo de 2015⁴

En esta oportunidad la cuestión controvertida se refiere a la negativa de la admisión de un mensaje de datos mediante el procedimiento de exhibición. A efectos de hacer valer su contenido, se solicitó la correspondiente exhibición del documento contemplada en las normas procesales, la cual fue negada por referirse a un correo electrónico que, en opinión del juzgador “... *constituye un documento intangible de imposible exhibición*”.

Esta posición fue ratificada por la Sala de Casación Social al indicar que en el caso concreto, el documento del cual se solicita exhibición es un medio informático, cuyo original consta en el computador, razón por la cual, es imposible su exhibición, salvo la impresión del mismo, que fue consignada por el promovente y admitida por el tribunal como documental, en el auto de admisión de pruebas.

Si bien el procedimiento de exhibición en principio está concebido para los documentos en papel, no es del todo cierto que la naturaleza intangible del documento electrónico impida su incorporación al proceso, en estos casos deben seguirse las previsiones de la LMDFE y solicitar su admisión mediante el sistema de prueba libre, acompañada de la correspondiente experticia a efectos de demostrar el cumplimiento a las exigencias legales necesarias para otorgar valor probatorio a estos nuevos soportes documentales.

En el caso objeto de análisis también se valoró la impresión del correo electrónico consignada, y en cuanto no fue objeto de oposición, se le otorgó el valor probatorio correspondiente, de conformidad con las principios de la LMDFE.

III. Consideraciones finales

Del análisis comparativo de estas decisiones podemos afirmar que en los últimos años, a pesar de ciertas confusiones que se han encontrado en la jurisprudencia del TSJ en períodos anteriores, la posición reiterada en la doctrina de este máximo tribunal, en cuanto a la forma de admisión del documento electrónico es acorde a la LMDFE, por lo tanto deberán seguirse los principios

⁴ El texto íntegro de la sentencia está disponible en <http://historico.tsj.gob.ve/decisiones/scs/mayo/177747-0336-25515-2015-04-764.html> (Consulta: 20 de septiembre de 2015)

establecidos en el CPC para las pruebas libres. Siguiendo estos cuerpos legales, las pruebas documentales electrónicas deben ser promovidas como pruebas libres y, atendiendo a los principios de analogía, su evacuación se llevará a cabo según lo previsto para los documentos elaborados en papel.

En cuanto a la valoración de los mensajes de datos, se observa una mayor claridad y apego a los principios de la LMDFE. En este punto es necesario recordar que para que un documento surta efectos probatorios, no se requiere la certificación de los equipos utilizados en su emisión, transmisión o recepción o la intervención de SUSCERTE (requisito que en algún momento fue considerado erróneamente por la jurisprudencia del máximo tribunal venezolano).

Para determinar el valor probatorio del mensaje de datos el requisito indispensable es su integridad. En los casos que haya que demostrarse esta circunstancia, así como la fecha de recepción o envío, podrán utilizarse los servicios de terceras personas. En relación con este respecto, debemos insistir que no necesariamente debe tratarse de personal de SUSCERTE, ya que se puede recurrir al auxilio de cualquier experto informático a efectos de determinar el cumplimiento de tales exigencias, como lo establece la LMDFE.

También debe recordarse que no puede privarse de valor probatorio al documento electrónico por el hecho de no incorporar mecanismos de autenticación electrónica, como firmas y certificados electrónicos, ya que de acuerdo con los principios del mencionado texto legal, el documento que no incorpore una firma electrónica en las condiciones previstas en la ley, no debe desecharse por esta razón, ya que podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica, como lo dispone el artículo 17 de la LMDFE.

RECENSIÓN

La comercialización del nombre de dominio.
Los bienes jurídicos digitales, el derecho de control y los nombres
de dominio*

LASTIRI SANTIAGO, Mónica.
Marcial Pons, España 2014, 352 pp

Horacio Rangel Ortiz**

Existe una tendencia natural a buscar explicaciones sobre fenómenos desconocidos o novedosos, utilizando razonamientos y reflexiones sobre temas conocidos, con los que los involucrados están familiarizados. El sistema puede arrojar resultados positivos, eso es parte de la evolución de toda disciplina, pero no es siempre así. Esta forma de buscar la explicación de las cosas también suele provocar acomodos y manejos de esa nueva manifestación, marcados por su carácter artificial y hasta incongruente con las peculiaridades de la nueva expresión. Lleva tiempo rectificar o encontrar una solución adecuada, diseñada justamente para explicar esas particularidades que requieren de explicaciones, algunas veces tan novedosas como el fenómeno mismo; en eso consiste precisamente la evolución de toda disciplina. Se conocen muchos ejemplos.

El pensamiento del siglo XVIII encabezado por Carl von Linné redujo la diversidad de la vida sobre la Tierra a dos grandes Reinos: el reino animal y el reino vegetal. Los microorganismos se fueron asignando a uno u otro reino a medida que iban siendo descubiertos atendiendo a criterios que no siempre suscitaban un acuerdo generalizado, sin considerar que en estas formas de vida estaban presentes los elementos para ubicarlos en un reino distinto al de las plantas y los animales. A mediados del siglo XIX se planteó la existencia de un tercer reino, y ello no obstante los libros de texto para la enseñanza de la biología de mediados del siglo XX seguían difundiendo la clasificación de los seres vivos en dos reinos. Tuvieron que transcurrir doscientos años para aceptar que estas

* Publicado en La Ley Mercantil, número 15, junio de 2015.

** Abogado y Doctor en Derecho. Socio de la firma de abogados *RANGEL y RANGEL* en Ciudad de México www.rangelyrangel.com Profesor de Derecho de la propiedad intelectual. Universidad Panamericana. Facultad de Derecho (Posgrado) y UNAM. Facultad de Derecho (Posgrado), Ciudad de México. Expresidente de la Asociación Internacional de Profesores e Investigadores de Propiedad Intelectual (ATRIP) y del Grupo Mexicano de la AIPPI (Asociación Internacional para la Protección de la Propiedad Intelectual). Presidente del Comité de Tratados Internacionales del Grupo Mexicano de la AIPPI horaciorangel@rangelyrangel.com

complejas formas de vida pertenecen a un reino distinto. En el siglo XXI se acepta que la diversidad de los seres vivos puede clasificarse en distintos reinos que pueden ser tres, cuatro, cinco o seis, dependiendo del autor y del criterio empleado por el investigador para proponer la adopción de la categoría taxonómica de reino. La que ha recibido más aceptación y difusión es la teoría de los *cinco reinos* del estadounidense Robert Whittaker (1920-1980), cuya principal aportación a los estudios científicos fue la propuesta de clasificación taxonómica de seres vivos en cinco reinos¹.

Similar fenómeno ocurrió en el mundo jurídico a fines del siglo XIX, cuando se creía que los derechos que recaen sobre los bienes inmateriales necesariamente debían corresponder a cualquiera de las categorías de derechos conocidas hasta entonces, representada por los *derechos personales, derechos de obligaciones y derechos reales*. Fue el jurista belga Edmund Picard el primero en resolverse a crear una nueva categoría de derechos expuesta en su teoría de los *derechos intelectuales*, dada a conocer en una conferencia pronunciada en el Colegio de Abogados de Bruselas en 1873, y explicada más tarde en la obra *Embriology Juridique* publicada en la Revista de Derecho Internacional Privado y de la Jurisprudencia Comparada de Bruselas en 1883².

¹ *Animalia, Plantae, Fungi, Protista y Monera*, dada a conocer en 1969 <https://oggisioggino.wordpress.com/2012/07/19/clasificacion-de-los-seres-vivientes/> En su *Systema Naturae* Carl von Linné (1758) dividía el mundo viviente en dos grandes *Reinos*: el reino animal y el reino vegetal. Está en marcha un ambicioso proyecto denominado *The tree of life web (ToL)*, basado en la filosofía de la sistemática filogenética, en el que biólogos de todo el mundo están colaborando en la construcción de un sistema completo de clasificación filogenético en el que se plasme la unidad y la diversidad de la vida sobre la Tierra. La clasificación de los seres vivos que obtuvo más aceptación y resultó más duradera después de la de Linné fue el sistema de los *cinco reinos* propuesto por R. Whittaker en 1959 y ampliamente divulgado por Lynn Margulis en su obra *Five Kingdoms*. Este sistema divide a los seres vivos en los siguientes cinco reinos: a) Moneras: incluye a todos los organismos procariontes; b) Protistas: incluye a todos los eucariontes unicelulares (antiguos protozoos, algas y hongos unicelulares); c) Fungi: incluye a todos los hongos pluricelulares (que se desgajan así del reino vegetal); d) Plantae: incluye todos los hasta entonces llamados vegetales pluricelulares con excepción de los hongos; e) Animales: incluye a todos los hasta entonces llamados animales pluricelulares o metazoos. La clasificación de Whittaker sigue siendo en la actualidad la más difundida en los libros de texto para la enseñanza de la biología en la educación secundaria. Véase PORTO ANDIÓN Alejandro, *Microorganismos* en: Curso de Biología, Departamento de Biología-Geología - IES María Casares - Oleiros - A Coruña <http://www.bionova.org.es/biocast/tema20.htm>. Véase también *¿A qué reinos pertenecen los microorganismos?* en: *Los seres vivos que sólo se ven al microscopio* http://e-ducativa.catedu.es/44700165/aula/archivos/repositorio/3250/3400/html/12_a_qu_reinos_pertenecen_los_microorganismos.html

² Véase Edmund PICARD, *Embriology juridique. Nouvelle classification des droits – Droit international privé; droits intellectuels*, JOURNAL DE DROIT INTERNATIONAL PRIVÉ ET DE LA JURISPRUDENCE COMPAREE Tome 10, Nos. XI –XII, 1883, pp 565 *et seq.* Los principios que dan sustento a la *teoría de los derechos intelectuales* vuelven a aparecer en la obra de Picard publicada a principios del siglo XX bajo el título *Le Droit Pur*, en la que ratifica la pertinencia de ubicar los derechos que recaen sobre los bienes inmateriales, incorpóreos o intangibles en esa nueva categoría de derechos intelectuales creada por él a fines del siglo XIX. Véase

La lectura de *La comercialización del nombre de dominio* de Mónica Lastiri Santiago, inevitablemente conduce la mente del lector a la obra *Embriology juridique* en la que se expone la teoría de los *derechos intelectuales*. En busca de una explicación convincente que permita aproximarse a la naturaleza de los derechos que recaen sobre los bienes inmateriales, incorpóreos o intangibles, en *Embriology juridique*, Picard examina las manifestaciones de estos derechos, y las contrasta con las de las principales categorías de los derechos patrimoniales, específicamente de los derechos reales, que hasta entonces habían servido para explicar la naturaleza de los derechos sobre los bienes que conforman el patrimonio³. Las conclusiones de Picard muestran lo insatisfactorio que resulta equiparar los derechos sobre los bienes inmateriales a los derechos reales, y los inconvenientes que resultan, desde el punto de vista jurídico, de una apreciación de las cosas en ese sentido. Convencido que la doctrina de los derechos reales no era de utilidad para explicar satisfactoriamente la naturaleza de los derechos de carácter patrimonial que recaen sobre los bienes inmateriales, Picard se decide a crear una nueva categoría de derechos que él llama *derechos intelectuales*. En tiempos contemporáneos a Picard otros ya habían reflexionado sobre la verdadera naturaleza de los derechos patrimoniales que recaen sobre estos bienes incorpóreos, reflexiones encabezadas por el pensamiento del alemán Kçhler⁴, quien se refería al *derecho exclusivo* sobre las obras consideradas como un *bien inmaterial* y, en consecuencia, de naturaleza distinta al derecho de propiedad que se aplica a las cosas materiales; la paternidad de la teoría de los *derechos intelectuales* como una nueva categoría de derechos patrimoniales sobre los bienes inmateriales, le corresponde a Picard.

En líneas anteriores tengo dicho que la lectura de la obra de Mónica Lastiri conduce de modo natural al pensamiento de Picard, y esto es aplicable lo mismo al proceso y al método, que al resultado. En efecto, en *La comercialización del nombre de dominio*, la autora examina en detalle las instituciones jurídicas vigentes a principios del siglo XXI potencialmente aplicables, y las contrasta con los rasgos más característicos de los nombres de dominio, incluyendo las distintas manifestaciones de contenido patrimonial que los han caracterizado a

DROITS INTELLECTUELS: jura in RE intellectuali en: Edmond PICARD, *Le Droit Pur*, Ernest Falmmarion, Editeur, 26 Rue Racine, Paris 1908 <http://gallica.bnf.fr/ark:/12148/bpt6k5463111p/f105.image> Al poco tiempo de la publicación de la obra por el editor francés, la obra de Picard fue traducida a nuestra lengua por el jurista español Alfredo Serrano Reyes: E. Picard, *EL DERECHO PURO*, Librería Gutenberg de José Ruiz, Plaza de Santa Ana, núm 13, Madrid 1911, pp. 98 *et seq.*

³ En esencia, la cuestión radicaba en determinar la pertinencia de acomodar la naturaleza de los derechos patrimoniales que recaen sobre los bienes inmateriales como una manifestación de los derechos reales, en contraste con los derechos personales y derechos de obligaciones respecto de los cuales no se presenta discusión alguna en este ámbito.

⁴ G. Köhler, *Ferchungen aus den Patentrecht*, 1883, citado por BREUER MORENO Pedro Carlos, *Tratado de Patentes de Invención*, Vol. I, Alfredo Perrot, Buenos Aires 1957, p. 58.

partir de las actitudes adoptadas por particulares y autoridades frente a ellos, todo lo cual ha permitido que, de tiempo atrás, se les haya asignado el papel de un bien susceptible de ser adquirido e incluso transmitido en la forma de una compraventa. El análisis de la autora incluye el estudio de sentencias y resoluciones provenientes de la jurisprudencia comparada, que han sido de utilidad para hacer frente a problemas cuya solución no ha podido diferirse a momentos ulteriores y, consecuentemente, marcadas por la precipitación y la premura de las circunstancias. Concedido que estas actuaciones han contribuido a poner un correctivo donde era necesario, el valor de las que ameritan comentario como precedente que sirva de modelo para solucionar contiendas futuras, con frecuencia parece limitado y poco pertinente, *i.a.*, por la fragilidad de los fundamentos que sirvieron de punto de partida para la solución adoptada. La equiparación que suele hacerse de los nombres de dominio con las marcas y los signos distintivos de la empresa, a veces ha funcionado cuando lo que está de por medio es, efectivamente, un signo distintivo, esto es, cuando de manera paralela a las funciones propias de un nombre de dominio, el nombre venía desempeñando funciones distintivas que permitan asignarle la función de una marca u otro signo distintivo. En todos esos casos, las reglas del Derecho marcario han sido herramientas útiles que, con las adaptaciones y ajustes necesarios, han contribuido a la aportación de la solución buscada. La realidad de las cosas es que quienes tienen la necesidad de tomar decisiones en esta materia, debieran pensar en la utilización de las reglas del Derecho marcario –e esto es, las reglas aplicables a las formas de adquisición, conservación, ejercicio, defensa, respeto y terminación de los derechos que recaen sobre las marcas y otros signos distintivos– cuando lo que está de por medio es una situación susceptible de ser regida por estas reglas. Su transportación a situaciones ajenas al Derecho marcario, como mecanismo para suplir las lagunas y silencios de una reglamentación legal de los nombres de dominio, tiene el potencial de conducir a resultados tan insatisfactorios como la problemática misma que se pretende resolver, particularmente cuando la materia involucrada no es una marca ni un signo distintivo propiamente dicho. En *La comercialización del nombre de dominio* su autora destaca los inconvenientes que resultan de la aplicación de las reglas marcarias a situaciones que involucran nombres de dominio en las que no está presente un signo distintivo propiamente dicho. La obra comentada no sugiere la eliminación de estas reglas en el ámbito de los nombres de dominio; antes, al contrario, propone su fortalecimiento con otras de mayor compatibilidad y congruencia con la que se estima la verdadera naturaleza de los nombres de dominio y de los derechos que sobre ellos recaen, incluyendo situaciones en las que lo que está de por medio es sólo un nombre de dominio que no ha cumplido funciones distintivas, bien porque no es susceptible de cumplirlas, o porque siendo susceptible de cumplirlas, no son estas funciones lo que ha estado de por medio, sino fundamentalmente el papel de nombre de dominio.

El método utilizado por la autora para eliminar figuras jurídicas que representan más un enredo que una herramienta útil en esta discusión, es de un rigor pocas veces visto en el análisis de las instituciones legales. La autora en ningún momento da por sentado que el lector conoce lo que ella conoce o ha investigado, o que dicho lector debe tener en estas discusiones el mismo punto de partida que ella, como si las cuestiones jurídicas pertenecieran al terreno del sentido común. Todo planteamiento contenido en la obra al que la autora le ha asignado el papel de fundamento o punto de partida para ulteriores consideraciones y conclusiones en materia de nombres de dominio, está invariablemente precedido y acompañado de un examen pormenorizado de las figuras e instituciones legales que de modo directo e indirecto pueden influir en la discusión. El apartamiento de todo dogmatismo es una constante perceptible en las 322 páginas del texto principal de la obra. Esto no es una constante en las obras jurídicas, muchas de ellas marcadas por su dogmatismo. Por lo demás, en la obra está presente la filosofía de la autora que entiende que el carácter jurídico interdisciplinario de la problemática en la que está de por medio el nombre de dominio, debiera reflejarse en la formación –igualmente plural– de quienes tienen alguna intervención de trascendencia en estos temas, lo mismo en la academia y en la empresa, que en el foro, la judicatura y la legislatura. La necesidad de hablar un mismo lenguaje y, sobre todo, de homogeneizar el universo de participantes en estas discusiones, es permanentemente considerada por la autora, de modo que el lector asimila con especial comodidad, y hasta familiaridad, tecnicismos propios de las distintas instituciones involucradas, lo mismo las jurídicas que las ajenas a lo jurídico. Este manejo sofisticado y metódico de la problemática hace las veces de un filtro que permite desechar lo que se estima constituye un estorbo, y conservar el material jurídico congruente con la institución. Este mismo tratamiento del tema confiere a Mónica Lastiri Santiago la autoridad para ubicar a los nombres de dominio en una nueva categoría de bienes sobre los que recaen derechos patrimoniales que la autora propone designar *bienes jurídicos digitales*, distintos de los *bienes inmateriales* (Kçhler) que Picard llama *choses intellectuelles*⁵, en la segunda mitad del siglo pasado (Lastiri, *La diferencia entre los bienes inmateriales y bienes digitales*, pp. 281 *et seq*). La creación de una categoría de bienes llamados *bienes jurídicos digitales* está precedida de la noción sostenida por la autora de acuerdo con la cual un nombre de dominio es un *atributo de la personalidad*, conclusión que facilita la apreciación del nombre de dominio como un bien jurídico propiamente dicho. La *teoría de los bienes jurídicos digitales* de Lastiri es en sí misma importante por las consecuencias de orden pragmático que de ella pueden resultar, específicamente en la adquisición y transmisión de un nombre de dominio, esto es, en la *comercialización del nombre de dominio*, y la seguridad jurídica que se busca esté presente en este tipo de transacciones. La teoría de los bienes jurídicos digitales de Lastiri es

5 PICARD, *Le Droit Pur*, *op. cit.*, p. 92.

complementada, esto es, enriquecida, con otra aportación de la autora, tan pragmática y útil, como novedosa y sofisticada. Me refiero a la calificación de la autora del tipo de derecho que recae sobre el nombre de dominio como un *derecho de control*, en contraste con otros derechos con los que a veces se le ha relacionado, y hasta confundido, como el derecho exclusivo de propiedad intelectual que recae sobre las marcas y los signos distintivos de la empresa. Consentido que los derechos que recaen sobre los *bienes jurídicos digitales* llamados nombres de dominio no corresponden en rigor a los que hasta hoy han ejercido los titulares y propietarios de derechos de propiedad intelectual sobre los *bienes inmateriales* (Köhler), la autora concluye que sobre ellos recae un *derecho de control*, similar al que se conoce en el mundo de los documentos electrónicos negociables.

Mónica Lastiri da a conocer su teoría de los *bienes jurídicos digitales* y el *derecho de control* que sobre ellos recae con motivo de la defensa de su tesis doctoral en el aula Carlos Escribano destinada a este tipo de ejercicios en la Facultad de Derecho de la Universidad Carlos III de Madrid, ante un Tribunal presidido por el eminente mercantilista don Rafael Illescas Ortiz de la Universidad Carlos III de Madrid e integrado por el distinguido profesor don David Morán Bovio de la Universidad de Cádiz, y por el autor de esta recensión, el cual otorgó por unanimidad a la doctorando la máxima de sobresaliente *cum laude* por el trabajo de investigación elaborado bajo la dirección del profesor César Giner Parreño. A diferencia de la teoría de los *derechos intelectuales* de Picard que esperó diez años desde que fue dada a conocer en el Colegio de Abogados de Bruselas hasta su publicación por la editorial de la Revista de Derecho Internacional Privado y de la Jurisprudencia Comparada de la capital belga, la divulgación de la *teoría de Lastiri* –o *teorías* (las tesis defendidas dijo en aquella ocasión Illescas)– de los *bienes jurídicos digitales* y el *derecho de control* más allá de los ámbitos estrictamente académicos, no ha debido esperar tanto tiempo como aconteció con *Embriology juridique*. Antes que transcurriera un año de la realización del solemne acto académico de la Carlos III de Madrid, la Editorial Marcial Pons ya había puesto a disposición del público *La comercialización del nombre de dominio* de la profesora Mónica Lastiri Santiago.

Desde el punto de vista jurídico, esto es, como ejercicio intelectual, las aportaciones de Lastiri a la discusión de la problemática del nombre de dominio son meritorias y plausibles en grado sobresaliente. Un valor agregado de *La comercialización del nombre de dominio*, y en ello radica la verdadera utilidad de la obra, está representado por las consecuencias que puede acarrear la utilización de los conceptos discutidos en la obra, en la vida de todos los días. Quien tenga en sus manos un ejemplar de la obra, no volverá a enfrentar las negociaciones, discusiones y controversias que a diario suscitan la adquisición, ejercicio, defensa y terminación de los derechos que recaen sobre estos *bienes jurídicos digitales*, de la forma en que antes lo hizo. Si de lo que se trata es de

resolver este tipo de controversias con herramientas estrictamente jurídicas, ningún empresario, abogado, juez, legislador, estudiante, investigador o académico querrá jamás enfrentarse a un colega, un superior, un adversario o una contraparte que haya tenido en sus manos un ejemplar de *La comercialización del nombre de dominio*, sin correr el riesgo de ver inmisericordemente destruidas muchas de las nociones que, por pragmatismo, inercia, costumbre, comodidad, apatía, simpleza, desconocimiento, urgencia o simple premura, han sido utilizadas en el pasado para hacer frente a los problemas que en la vida de todos los días suscita la presencia del nombre de dominio en el mundo de los negocios, esto es, en *la comercialización del nombre de dominio*.

Por los demás, la redacción de la obra permite una lectura agradable, inteligible y amigable, que lejos de mostrar preocupación por exhibir erudición en el tratamiento de temas propios de la metafísica del Derecho, muestra la capacidad de la autora para exponer con claridad y amenidad conceptos jurídicos complejos, provenientes de especialidades jurídicas tan diversas como sofisticadas. Caracterizada la obra lo mismo por acertadas originalidades y críticas que por su orgánico y completo desarrollo, tengo por cierto que la obra de Lastiri –y su teoría de los *bienes jurídicos digitales* y el *derecho de control* que recae sobre los nombres de dominio– habrá de llamar la atención en el público de los juristas del siglo XXI de modo similar a como ocurrió con la teoría de los *derechos intelectuales* expuesta por Edmund Picard en *Embriology Juridique* (1883) o con el sistema de los *Cinco Reinos* de Robert Whittaker (1969), ampliamente divulgado por Lynn Margulis en su obra *Five Kingdoms* (1988).

Ciudad de México, junio de 2015

El pago caputivo en la prestación de servicios médicos

MARTÍNEZ NADAL, Apol.lonia.
Civitas Thomson Reuters Aranzadi, España 2015

Mariliana Rico Carrillo*

Partiendo de una situación que se ha presentado los últimos años en la práctica del sector asegurador, relacionada con la modificación en la redacción de las cláusulas contractuales relativas al pago de los servicios médicos, que permite sustituir el tradicional sistema de pago, calculado sobre la base de la naturaleza del servicio prestado, por un pago caputivo, la Profesora Apol.lonia Martínez Nadal, Catedrática de Derecho Mercantil de la Universidad de las Illes Balears, ha dedicado su más reciente investigación al estudio de las consecuencias que implica el cambio en la forma de remuneración de estos servicios, cuyos resultados se reflejan en el libro *El pago caputivo en la prestación de servicios médicos*, publicado por la prestigiosa editorial Civitas Thomson Reuters en colaboración con la Universidad de las Illes Balears.

En esta oportunidad, la autora nos ofrece una perspectiva económica y jurídica del problema actual que sufre el colectivo de los profesionales de la medicina, derivado de la modificación impuesta unilateralmente en los acuerdos suscritos con algunas compañías aseguradoras, que incide en el sistema de retribución de la prestación de servicios profesionales médicos, considerando perjudicial este tipo de cláusulas (y en cierta manera abusivas), al sustituir el tradicional sistema de pago por un mecanismo donde la remuneración consiste en una cantidad fija, que se determina en función unos cálculos cuya elaboración corresponde únicamente a la entidad aseguradora.

Con la excelente calidad y metodología técnico-jurídica que caracteriza sus trabajos, la Profesora Martínez Nadal nos presenta esta nueva investigación, sistemáticamente organizada en tres partes: en la primera abordan los sistemas de pago en el sector de la salud, con especial referencia a los efectos del pago caputivo, en la segunda se centra en el estudio jurídico de este tipo de pago con referencia al supuesto de hecho planteado y la tercera la dedica a la formulación de las respectivas conclusiones.

* Catedrática de Derecho Mercantil. Universidad Católica del Táchira (Venezuela)

La monografía comienza con una aproximación descriptiva de las implicaciones del pago caputivo en el ámbito sanitario, donde se hace referencia a la existencia de diversos sistemas de pago en los servicios de salud, derivados de la multiplicidad de agentes que intervienen en el sector (beneficiarios, intermediarios financieros y prestadores de servicios médicos) cuyas ventajas e inconvenientes son evaluadas principalmente en función de los objetivos que se pretende alcanzar. En los pagos caputivos, se advierte que aun cuando representan un mecanismo de mayor eficiencia para el intermediario, los riesgos financieros para los prestadores de servicios son mayores, al existir una tarifa única como forma de remuneración. En el extremo opuesto se encuentra el pago por servicios, analizado también en esta primera sección, donde el riesgo para el proveedor es mínimo, en tanto que para la empresa se seguros representa un mecanismo de menor eficiencia. Ante esta situación, se pone de manifiesto la necesidad de seleccionar un sistema de remuneración intermedio, con una distribución de riesgos razonable entre los distintos agentes, para lo cual propone algunas posibilidades de solución como el establecimiento de sistemas mixtos o de un sistema de pago caputivo con ajustes en función del riesgo, considerando éste último el más adecuado en el caso de la prestación de este tipo de servicios, en el entendido que incorpora fórmulas de corrección establecidas sobre la base de distintos criterios que permiten matizar los efectos negativos de un sistema caputivo puro.

La segunda parte, y la más amplia de la obra, está dedicada al tratamiento jurídico del sistema de pago caputivo. En esta sección se tratan dos aspectos de especial relevancia desde la óptica legal, en primer lugar encontramos una referencia a las posibles actuaciones frente a la imposición unilateral por parte de la compañía aseguradora (en una cláusula predispuesta) del sistema de pago caputivo, donde se examinan cuatro aspectos fundamentales: la aplicación de la legislación sobre condiciones generales de contratación, la aplicabilidad de controles de las cláusulas predispuestas, la existencia un mecanismo alternativo de control de contenido, y las posibles acciones individuales y colectivas que pudieran ejercer los afectados. Seguidamente encontramos un apartado donde se examinan los efectos de este tipo de cláusulas a la luz del Derecho de la competencia y se establecen una serie de consideraciones respecto de la aplicación de la normativa en esta materia.

Luego de un exhaustivo estudio de los elementos objetivos y subjetivos que deben tomarse en cuenta para que proceda la aplicación de la normativa sobre condiciones generales de contratación, la Prof. Martínez Nadal concluye que el supuesto en análisis entra dentro del ámbito la legislación especial que regula este tipo de acuerdos, independientemente que el contrato se haya celebrado entre dos profesionales, en el entendido que se trata de una cláusula que no ha sido negociada libremente y que a su vez es perjudicial para la otra parte de la relación contractual, quien se encuentra en una posición notablemente más débil frente a la compañía aseguradora.

A continuación encontramos un amplio recorrido legal, jurisprudencial y doctrinal sobre los distintos controles de las cláusulas predisuestas e impuestas como condiciones generales. Aunque la doctrina mayoritaria es de la opinión que en casos como el planteado, este tipo de cláusula puede ser sometida al control de inclusión o incorporación, pero no al de contenido, por estar limitado este control a los contratos con consumidores, la autora propone como novedosa solución, fundamentada en argumentos normativos y resoluciones judiciales, junto con los Principios de Derecho Europeo de los Contratos, la aplicación del control de contenido al supuesto descrito, al considerar que la cláusula por la que se impone el sistema de pago capitativo es abusiva, en analogía con las circunstancias que determinan la condición de tales cláusulas en detrimento de los derechos de los consumidores, pues no sólo se trata de una cláusula imprecisa, que deja al arbitrio de la compañía de seguros la fijación de la remuneración por los servicios, sino que además implica la traslación total del riesgo económico al profesional al que le ha ido impuesta. Igualmente hemos de resaltar, como novedoso aporte, el planteamiento sobre la posibilidad de aplicar la transparencia, como un tercer mecanismo de control, proveniente de la jurisprudencia alemana y adoptado en la normativa europea sobre cláusulas abusivas en los contratos con consumidores; criterio reconocido recientemente en diversas sentencias del Tribunal Supremo español, aplicable a aquellas cláusulas que por referirse al objeto principal del contrato no pueden someterse a un control de contenido. Finalmente nos presenta como alternativa para catalogar este tipo de cláusulas como abusivas y solicitar su nulidad, la aplicación de las soluciones tradicionales del Derecho privado donde hace referencia a la moral o el orden público como límites de la libertad contractual, la arbitrariedad en la contratación, la cláusula de buena fe y otros mecanismos como el abuso de derecho o los vicios del consentimiento. En esta sección también se incluye una referencia a las acciones previstas en la normativa que regula los contratos con condiciones generales de contratación, donde encontramos una reseña a los dos mecanismos de defensa que otorga la ley: la acción individual, destinada a declarar la nulidad o no incorporación de la cláusula, cuyo estudio es complementado de un minucioso análisis de los legitimados activos, donde también se alude a la posibilidad de ejercer la acción colectiva, que correspondería a los Colegios profesionales en defensa de los intereses de sus colegiados.

En relación con la aplicación de la normativa sobre defensa de la competencia, objeto de desarrollo en el último inciso de esta segunda parte, se evalúan las conductas restrictivas de la competencia que pudiesen presentarse, principalmente el abuso de la posición de dominio y la dependencia económica. Si bien en principio cabría la aplicación de tales normas, al entender que existe una posición de dominio por parte de la entidad aseguradora, derivada de la imposición de precios o de servicios no equitativos, y también una situación de dependencia para los profesionales médicos afectados, hechos que pudieran contribuir al falseamiento de la libre competencia por configurarse como actos

desleales, no es fácil concluir que la aplicación de esta normativa es factible, ya que será necesario determinar en cada caso en concreto si se produce una afectación del mercado, requisito esencial para la aplicación de esta normativa, lo cual no es del todo posible, pues en principio no hay discriminación entre operadores, aún así, y al objeto de salvaguardar los derechos del colectivo médico, se insiste en el hecho que aunque sea de aplicación el Derecho de la competencia existen las vías de actuación propias de la jurisdicción ordinaria.

La tercera parte y última parte recoge en forma explícita y sistemática las conclusiones, donde la autora se enfoca en extraer los principales resultados de su trabajo y defender las posturas expuestas en el cuerpo de la obra. La publicación de este interesante material bibliográfico, producto de la ardua y exhaustiva labor de investigación de la Prof. Martínez Nadal, en relación con un caso real de significativa relevancia en la práctica, representa una importante contribución al área del Derecho, al ser la primera monografía que aborda de una manera integral la efectos económicos y jurídicos del pago capitativo en los servicios médicos, no sólo desde el punto de vista teórico sino práctico. Como principal aporte destacamos la elaboración de novedosos criterios jurídicos, sustentados en normativa y jurisprudencia reciente, destinados a lograr la aplicación del control de contenido en las cláusulas abusivas en los contratos entre profesionales, cuando una de las partes se encuentra en posición de desventaja respecto de la otra, circunstancia que no sólo protegerá al colectivo médico frente a este tipo de actuaciones por parte de las compañías aseguradoras, sino a otros profesionales que se vean afectados por situaciones similares.

Comparative Commercial Contracts: Law, Culture and Economic Development

KOZOLCHYK, Boris, Ph. D.
West Academic Publishing, United States of America, 2014

Mariliana Rico Carrillo*

Luego de años de ardua investigación y experiencia en la práctica del Derecho y la docencia, el Doctor Boris Kozolchyk ha publicado el libro *Comparative Commercial Contracts: Law, Culture and Economic Development*, donde nos ofrece un análisis integral de los contratos comerciales en las diferentes épocas y bajo los distintos sistemas jurídicos y económicos de los períodos históricos más significativos del Derecho mercantil.

Con la excelente calidad y metodología que caracteriza sus trabajos, el Profesor Kozolchyk realiza un minucioso recorrido histórico, jurídico, social y cultural de los contratos mercantiles desde su origen hasta la actualidad, con especial referencia a los principios y prácticas comerciales que han contribuido al desarrollo del Derecho mercantil internacional. Esta magnífica edición en formato electrónico, estructurada en seis partes integradas por treinta capítulos en total, es el resultado de más de 15 años de investigación, donde el autor combina su amplia trayectoria como profesor de Derecho Comercial Comparado de la Universidad de Arizona, con experiencias personales producto de sus visitas a los países más representativos de los distintos sistemas jurídicos objeto de estudio y del intercambio académico con profesionales y alumnos en diferentes cursos de postgrado y doctorado en universidades de reconocido prestigio en Estados Unidos, Europa, Asia y Latinoamérica, donde no podemos dejar de mencionar la Universidad Carlos III de Madrid, hecho que el propio autor relata en su obra.

La primera parte, compuesta por cuatro capítulos, comienza con una perspectiva histórica, antropológica y económica de las sociedades pre-comerciales, a efectos de facilitar al lector una comprensión integral de los principios que gobiernan los contratos mercantiles. Partiendo de la formación

* Catedrática de Derecho Mercantil. Universidad Católica del Táchira (Venezuela).

de las promesas comerciales, se pone de manifiesto la necesidad de profundizar en las fuentes y textos legales en un contexto histórico y socioeconómico, mediante una descripción de las costumbres comerciales y sus valores culturales, cuya importancia se refleja en la vigencia de algunos principios aplicables a los contratos mercantiles, originados en esta incipiente época del comercio. También hace una referencia al Derecho Romano como creador e inspirador de las principales instituciones jurídicas de la civilización occidental, con especial énfasis en su incidencia en la contratación mercantil y la interpretación de los contratos.

En la segunda parte, el autor se centra en el Derecho mercantil de la época medieval, enfocándose en la importante evolución de las instituciones jurídicas, en un período caracterizado por el florecimiento del comercio; sin olvidar la existencia del feudalismo y sus efectos sobre la actividad comercial, al conceder privilegios e inmunidades contractuales sólo a quienes gozaban de determinadas condiciones políticas o militares. En este momento histórico predomina la aplicación de la costumbre como fuente del Derecho mercantil, al igual que es notable el surgimiento de los gremios de comerciantes que se encargan de compilar los usos y prácticas de la época. Entre otras instituciones comerciales, se refiere al amplio desarrollo de los instrumentos de pago y crédito, gracias a la aparición de la letra de cambio. También alude a una serie de prácticas entre comerciantes que constituyen el origen de ciertos contratos mercantiles, como el *joint venture*, el seguro, el préstamo y el arrendamiento financiero. El análisis de estos contratos en la práctica actual es complementado con la jurisprudencia de diversos países, donde destacan algunas sentencias del Tribunal Supremo español. En este apartado encontramos una reseña al Derecho foral español, como Derecho territorial que adopta las costumbres de la época con diferentes formas de penalización para los incumplimientos contractuales, según las distintas clases sociales. Finalmente se resalta el papel de los principios morales y religiosos en la interpretación de los contratos, en especial la aplicación del principio de *pacta sunt servanda*, proveniente del Derecho canónico, a la vez que se analizan aspectos relacionados con la actuación de los comerciantes judíos del Mediterráneo como intermediarios de confianza, las escrituras notariales de las ciudades comerciales italianas y el sistema de los gremios para hacer negocios y su diferencia con el Derecho civil.

En la tercera parte, el Dr. Kozolchik se ocupa del movimiento codificador en Europa. Este segmento está destinado a los códigos civiles y comerciales que han influido significativamente en el Derecho contemporáneo de los contratos, tanto en los sistemas del Derecho civil como en el *Common Law*. La revisión de los textos legales comienza en el capítulo octavo, con el Código Civil francés de 1804, considerado el más influyente de todos los códigos de Derecho privado que siguen el sistema de Derecho civil. En esta sección se hace referencia al *Tratado de Obligaciones de Pothier*, en particular a la definición y clasificación de los contratos, criterios adoptados en la codificación francesa. El capítulo es seguido por el estudio de la precodificación, donde se destaca la labor de los

tribunales y las ferias medievales en la formación del Derecho mercantil. Los capítulos sucesivos se centran en el Código de Comercio francés, el Código Civil y el Código de Comercio alemanes. El autor concluye con un capítulo relativo al papel de los usos y costumbres mercantiles en el proceso de codificación, donde menciona las compilaciones de la Edad Media y su influencia en el Derecho mercantil actual, citando como ejemplos, las Reglas y Usos Uniformes sobre Créditos Documentarios (RUU) y las Reglas para el uso de Términos Comerciales Internacionales (INCOTERMS) de la Cámara de Comercio Internacional. A modo de ilustración, también incorpora una parte de la jurisprudencia alemana relacionada con el Derecho de los contratos y la aplicación de la Convención de Viena sobre Compraventa Internacional de Mercaderías, conocida internacionalmente por sus siglas en inglés CISG.

La cuarta parte, integrada por seis capítulos, tiene por objeto el análisis de la influencia de la codificación europea en Latinoamérica, Rusia y China. El primer capítulo, dedicado a la codificación en Latinoamérica, recalca la relevancia del trasfondo colonial y de una cultura legal cuyas instituciones están diseñadas para proteger los intereses del grupo familiar, costumbre identificada como «familismo». En este período se observa la presencia de un «autoritarismo legal», donde las leyes se hacen cumplir a través de la autoridad de sus gobernantes, sin un proceso de aprobación consensuado con el pueblo. Con rigurosa precisión se detalla el movimiento codificador de los países latinoamericanos, diferenciando la época colonial, donde se observa una fuerte influencia del Derecho español, de la post-colonial, caracterizada por la presencia de los modelos francés y español. También se realza la importancia del Código Civil chileno de 1855 como precursor de la mayoría de los códigos civiles latinoamericanos. En cuanto a la codificación comercial, algunos países se inspiran en los modelos europeos, mientras que otros siguen los principios de los códigos comerciales argentino (1862) y chileno (1865).

A continuación se expone una visión del Derecho comercial soviético desde una doble vertiente. En primer lugar se examina el panorama socio-económico de los contratos comerciales en una sociedad marxista-leninista, donde las leyes estaban orientadas básicamente a regular las transacciones comerciales realizadas por entidades del Estado. El autor señala el predominio del marxismo-leninismo como fuente de la ley oficial de los contratos comerciales y menciona que el fracaso de este sistema pudo deberse, en parte, al intento de erradicar las operaciones comerciales. La comprensión de estas ideologías y su impacto en la contratación mercantil adquiere particular importancia en la actualidad, en el entendido que aún permanecen vigentes en algunos Estados con regímenes autoritarios, donde se pone como ejemplo la situación de ciertos países en Latinoamérica. En segundo lugar se describe la Ley de la propiedad privada de 1990 y el Código Civil de la Federación Rusa de 1995, cuerpo legal integrado por disposiciones civiles y comerciales, siguiendo la orientación de los códigos unificados de Italia y Suiza. En relación con la materia mercantil, el Prof.

Kozolchik se refiere en particular a las disposiciones que regulan el contrato de compraventa, inspiradas en los principios de la CISG.

Los últimos capítulos de la cuarta parte están enfocados en los contratos comerciales en el sistema legal chino. Siguiendo la metodología empleada en toda la obra, se advierte la necesidad de estudiar el contexto histórico-social de este país a efectos de comprender el significado de las leyes y normas actuales provenientes del Derecho consuetudinario. Al igual que en Latinoamérica, en la redacción de las primeras normas subyacen las ideas de «familismo» y «legalismo», donde además está presente la ideología confuciana y neo confuciana. También se estudian los contratos y litigios en la China imperial y bajo la doctrina de Mao Tse-tung, definida por el autoritarismo propio de los sistemas comunistas. Esta sección concluye con una referencia al ordenamiento jurídico vigente y al desarrollo económico de los últimos años, donde predomina el modelo de la economía de mercado socialista. Estos aspectos son examinados minuciosamente por el autor, característica común de todas sus investigaciones.

En la quinta parte encontramos la brillante exposición sobre el sistema jurídico anglosajón relativo a los contratos comerciales. En el caso del Derecho inglés, se describe el auge comercial del siglo XVII, producto de la actividad de inventores, empresarios y financieros, apoyado por el Banco de Inglaterra como fuente primordial del crédito comercial, donde los comerciantes son considerados miembros de la alta burguesía y las prácticas comerciales se basan en la ética y la confianza de las partes. En este relato histórico también se explica el carácter monopolista y mercantilista del comercio internacional entre los siglos XV y XVII y el frecuente intercambio comercial con las colonias americanas durante el siglo XVIII. Finalmente se menciona la importancia de las prácticas equitativas, consideradas como un elemento fundamental en la evolución de los contratos comerciales y el desarrollo de algunos de los instrumentos de pago y de crédito comúnmente usados en la actualidad, como las letras de cambio, los cheques y las cartas de crédito.

En relación con el Derecho estadounidense, el Dr. Kozolchik expone las prácticas, actitudes y valores que inspiraron las instituciones comerciales y los principios que subyacen en la regulación vigente en esta nación, entre los que destacan: la libertad contractual y la buena fe en el cumplimiento de las obligaciones, la protección de la propiedad privada y de la fuerza laboral que genera riqueza, el trato equitativo de las partes en igualdad de condiciones y la protección de terceros que actúan de buena fe. En el entorno histórico resalta la participación de los agricultores en los mercados locales e internacionales, quienes actuaban como verdaderos comerciantes. También alude a importantes prácticas comerciales durante la colonia como la presencia de tiendas que abastecían a la población rural, la existencia de mayoristas que suministraban bienes y otorgaban créditos a los pequeños agricultores y productores y a los comerciantes minoristas, mencionando finalmente la aparición de la figura del factor mercantil. Dentro de las instituciones post-coloniales, se refiere a los

grandes almacenes como predecesores de las actuales tiendas por departamentos, al nacimiento de la banca comercial, a la creación de la Reserva Federal (cuyas funciones se describen con precisión y claridad) y de las agencias de calificación crediticia, pilares fundamentales en el desarrollo de la economía de este país. Este apartado finaliza con una mención a los préstamos garantizados y a la legislación sobre quiebra, como una segunda oportunidad para los comerciantes que han fracasado en sus negocios. Seguidamente encontramos una investigación sobre la legislación comercial desde los primeros años de la independencia hasta nuestros días. El autor parte del sistema dualista de la Constitución de 1789 para explicar el origen de una multiplicidad de leyes federales y estatales orientadas a regular distintos aspectos del comercio, que fueron incorporadas posteriormente en el *Uniform Commercial Code* (UCC), instrumento unificador de la legislación mercantil en el Derecho estadounidense. La regulación sobre prácticas abusivas en la contratación comercial también es objeto de análisis en esta sección. A modo de conclusión, se enfatiza el liderazgo de los Estados Unidos en el fomento del comercio internacional, gracias a la protección de la buena fe y de los terceros compradores, inversionistas y acreedores dentro y fuera de sus fronteras.

La sexta parte, desarrollada en los últimos nueve capítulos y sus anexos, está dedicada a la formación e interpretación de los contratos. El primero de estos aspectos es abordado bajo un método comparativo entre los contratos civiles y comerciales, donde se expone la teoría general de los contratos, resaltando la importancia de las promesas comerciales y la relevancia del momento de formación como elemento clave en la determinación de la validez y del nacimiento de las obligaciones de las partes. Además de referirse a la ley sustantiva, el autor incorpora un significativo estudio de los casos más notables de la jurisprudencia internacional sobre formalidades y solemnidades contractuales. A continuación se ubica el capítulo relativo a la buena fe y la razonabilidad como principios rectores en la interpretación de los contratos comerciales. El concepto de buena fe es analizado bajo la óptica de la interpretación judicial y su reconocimiento legal. En el ámbito comercial, se pone de relieve la presencia de la razonabilidad, la honestidad, la justicia y la equidad como elementos de la buena fe en el marco del UCC. En este apartado también se inserta un apéndice de jurisprudencia internacional sobre la interpretación de los contratos y la aplicación de los principios de razonabilidad y buena fe en el sector comercial.

El capítulo siguiente está destinado a las prácticas comerciales como fuente del Derecho de los contratos. El Dr. Kozolchyk pone de manifiesto la importancia de la elaboración de estas prácticas en la actualidad, citando nuevamente como ejemplo los INCOTERMS y las RUU. A efectos de ilustrar el impacto de esta fuente normativa en la contratación comercial, la investigación se complementa con una mención a las prácticas sobre préstamos garantizados en el Derecho romano y a las normas de cartas de crédito que antecedieron la redacción de

las RUU. Los capítulos sucesivos exponen los procedimientos judiciales comerciales, los remedios extrajudiciales y el cumplimiento específico de la obligación. La obra finaliza con una sección relativa a los daños por incumplimiento de las garantías contractuales, donde se incluye un estudio general del Derecho estadounidense de daños, y una referencia a las normas sobre garantías expresas e implícitas del UCC, que el profesor acompaña con un brillante análisis económico del Derecho.

Esta extraordinaria publicación se nutre de más de 40 años de experiencia del autor en temas relacionados con el comercio internacional, quien es conocido ampliamente por sus excelentes trabajos y su contribución al Derecho mercantil internacional. La exhaustiva investigación que en estas breves líneas se describe, consolida su aportación a esta rama de la ciencia jurídica, a la cual se suma su labor a cargo del *National Law Center For Inter-American Free Trade* (NLCIFT), creado con la finalidad de lograr la uniformidad de las leyes mercantiles en Latinoamérica, donde se ha desempeñado como Director Ejecutivo y Presidente fundador. En el año 2005, durante mi estancia como profesora visitante en la Universidad Carlos III de Madrid tuve el honor de conocer y compartir actividades académicas con tan destacado jurista, hoy me complace reseñar y recomendar la lectura de esta obra, de incalculable valor para la comprensión del Derecho de los contratos comerciales y su papel en el desarrollo económico internacional.



ÍNDICE ACUMULADO

ARTÍCULOS

CONFERENCIAS

CONTRIBUCIONES ESPECIALES

COMENTARIOS ESPECIALIZADOS

RESEÑA LEGISLATIVA

CRÓNICA JURÍDICA

SECCIÓN MONOGRÁFICA

LEGISLACIÓN

NACIONAL
INTERNACIONAL

JURISPRUDENCIA

COMENTARIOS
SENTENCIAS

RECENSIÓN

ARTÍCULOS

AGUILAR TORRES, Jorge.

- El ejercicio de los derechos políticos de los accionistas a través de medios electrónicos en las sociedades anónimas no cotizadas en España. **10**, (2008-2009), 75-91.

ALBA FERNÁNDEZ, Manuel.

- El Convenio de Montreal para la Unificación de ciertas reglas para el Transporte Aéreo Internacional de 1999: el comienzo de una nueva etapa. **5**, (Julio/Diciembre 2004), 121-145

ALVÁREZ CABRERA, Carlos.

- Patentabilidad de las invenciones relacionadas con la computación. **3**, (Julio/Diciembre 2003), 37-50.

ÁLVAREZ CUESTA, Henar.

- El software libre y su posible repercusión en el ámbito universitario español. **6-7**, (Enero/Diciembre 2005), 171-181.

AMONI REVERÓN, Gustavo Adolfo.

- Regulación económica de Internet como elemento de gobierno electrónico en Venezuela. **9**, (Enero/Diciembre 2007), 117-131
- La democracia electrónica: buscando nuevos medios para la participación. **12**, (2011), 127-145
- Posibles soluciones a problemas de la audiencia de casación penal telemática. **16**, (2015), 117-141

APARICIO VAQUERO, Juan Pablo.

- Derecho y tecnología de protección de las obras en formato electrónico. **6-7**, (Enero/Diciembre 2005), 203-227.

ARIAS DE RINCÓN, María Inés.

- La perfección del contrato en el Decreto-Ley de Mensajes de

Datos y Firmas Electrónicas. **2**, (Enero/Junio 2003), 131-150.

- La protección al consumidor en el comercio electrónico. **6-7**, (Enero/Diciembre 2005), 53-71.
- La alternativa de la conciliación por vía electrónica en los conflictos de consumo. **14**, (2013), 37-53

ARRIETA ZINGUER, Miguel.

- Régimen jurídico de la interconexión en las telecomunicaciones en Venezuela. **1**, (2002), 111-128.
- Los aportes en ciencia, tecnología e innovación en Venezuela. **9**, (Enero/Diciembre 2007), 89-116.
- Normativa respecto de las declaraciones de impuestos nacionales por Internet en Venezuela. **11**, (2010), 97-105.
- Comercio electrónico y redes sociales: nuevo paradigma negocial. **16**, (2015), 177-191

BARZALLO, José Luis.

- Derechos de autor y tecnología. **3**, (Julio/Diciembre 2003), 7-36.

BERROCAL LANZAROT, Ana Isabel .

- La defensa de los derechos al honor, intimidad personal y familiar y a la propia imagen de los menores de edad en Internet. **14**, (2013), 55-98

BUITRAGO RODRÍGUEZ, Mariana

- La convocatoria electrónica como vía de notificación alternativa a las asambleas de accionistas en el Derecho venezolano. **10**, (2008-2009), 93-109
- La electronificación en las sesiones del sistema de mercado bursátil en el Derecho venezolano. **13**, (2012), 87-105

- CÁRDENAS, Gilberto.
- Análisis jurisprudencial del artículo 90 del Tratado de la Unión Europea como fundamento jurídico para la liberalización del mercado de las telecomunicaciones. **1**, (2002), 93-110.
- CONTRERAS ZAMBRANO, Josué.
- Manuel. Valoración probatoria del documento electrónico y firma electrónica en el proceso judicial venezolano. **13**, (2012), 27-46
- CREMADES, Javier y SANMARTIN, Javier.
- España: La nueva Ley General de Telecomunicaciones. **5**, (Julio/Diciembre 2004), 7-16.
- CUADRADO GAMARRA, Nuria.
- Los Códigos tipo en la legislación española. **6-7**, (Enero/Diciembre 2005), 73-90.
- CHACÓN GÓMEZ, Nayibe.
- La perspectiva electrónica de los títulos valores: desmaterialización del título valor, **10**, (2008-2009), 133-155.
 - La transferencia tecnológica: ¿Desarrollo de una política pública en Venezuela?. **16**, (2015), 105-116
- CHIQUITO, Andreina.
- El cheque electrónico en la legislación venezolana. **9**, (Enero/Diciembre 2007), 69-88.
- DE LA VEGA JUSTRIBÓ, Bárbara.
- Las nuevas tecnologías en la publicidad del concurso de acreedores. **11**, (2010), 107-130.
 - La mediación por medios electrónicos en la Ley española de mediación de asuntos civiles y mercantiles. **13**, (2012), 133-157
- DELPIAZZO, Carlos E.
- La Informática Jurídica y el Derecho de la Integración del Mercosur. **8**, (Enero/Diciembre 2006), 95-111.
 - Aspectos de la contratación pública electrónica. **11**, (2010), 11-31
- FERNÁNDEZ DELPECH, Horacio.
- Nueva Directiva de la Unión Europea sobre Conservación de Datos de Tráfico. **8**, (Enero/Diciembre 2006), 11-25.
 - La *Cloud Computing*. Una visión Argentina. **16**, (2015), 47-64.
- GALINDO, Fernando.
- Democracia electrónica, Internet y gobernanza, **12**, (2011), 109-125
- GARCÍA CACHAFEIRO, Fernando y GARCÍA PÉREZ, Rafael.
- La tensión entre las restricciones a la libre prestación de servicios de la Sociedad de la Información y los derechos fundamentales y libertades públicas. **3**, (Julio/Diciembre 2003), 151-165.
- GARCÍA MANDALONIZ, Marta y RODRÍGUEZ DE LAS HERAS BALLELL, Teresa.
- "La inquebrantabilidad del principio de la unicidad en la junta general electrónica". **8**, (Enero/Diciembre 2006), 27-47.
- GARRO, Alejandro M., PERALES VÍSCASILLAS, Pilar y PÉREZ PEREIRA, María.
- Comunicaciones Electrónicas en la Convención de Viena de 1980 sobre compraventa internacional de mercaderías (CISG): primera opinión del Consejo Consultivo de la Convención (CISG-AC), **5**, (Julio/Diciembre 2004), 17-40
- GÓMEZ CORDOBA, Ana Isabel y Nelson REMOLINAANGARITA.
- Los sistemas de identificación biométrica y la información biométrica desde la perspectiva de la

- protección de datos personales. **12**, (2011), 69-108
- GRAHAM., James A.
- *La Uniform Dispute Resolution Policy*: Una tentativa de calificación. **2**, (Enero/Junio 2003), 151-159.
- GUISADO MORENO, Ángela.
- La unificación del Derecho contractual europeo en la Era de la Información: movimientos e instrumentos unificadores. **9**, (Enero/Diciembre 2007), 133-158.
- HERNÁNDEZ, Juan Carlos.
- La protección de datos personales en internet y los derechos fundamentales: El Habeas Data. **13**, (2012), 61-85
- HERRERA BRAVO, Rodolfo.
- Los registros de ADN y los derechos fundamentales: ¿Cómo esquivar sin despellejar? **2**, (Enero/Junio 2003), 21-41.
- ILLESCAS ORTIZ, Rafael.
- La equivalencia funcional como principio elemental del Derecho del comercio electrónico. **1**, (2002), 9-23.
 - La Ley 22/2007 sobre Comercialización a Distancia de Servicios Financieros destinados a los Consumidores y la dogmática contractual electrónica. **9**, Enero/Diciembre 2007), 11-26.
- INOSTROZA SÁEZ, Mauricio
- El convenio arbitral electrónico en la Ley de arbitraje española y los textos de Derecho uniforme. **12**, (2011), 53-67
- IRIARTE AHON, Erick.
- Sobre nombres de dominio: una propuesta para el debate. Análisis de la Radicación 1376 del Consejo de Estado colombiano. **2**, (Enero/Junio 2003), 103-129.
- JELEZTCHEVA, María y RODRÍGUEZ GRILLO, Luisa
- Los contratos electrónicos. **11**, (2010), 159-188.
- LAGUNA, Rosa.
- ¿Nueva pedagogía para el *e-learning*? **3**, (Julio/Diciembre 2003), 127-150.
- LASTIRI SANTIAGO, Mónica.
- Autorregulación publicitaria. **1**, (2002), 157-182.
 - El uso de la marca en Second Life. **10**, (2008-2009), 7-43
- LÓPEZ JIMÉNEZ, David
- La autorregulación de la publicidad relativa a apuestas y juegos virtuales: una aproximación desde la perspectiva española. **12**, (2011), 147-185
 - Los deberes precontractuales de información en el ámbito de las transacciones virtuales: a propósito del principio de la buena fe. **13**, (2012), 107-131
- LÓPEZ JIMÉNEZ, David y BARRIO, Fernando.
- Los códigos de conducta reguladores del comercio electrónico en el espacio europeo. Los casos de Alemania, España e Italia. **11**, (2010), 33-68.
- LÓPEZ ZAMORA, Paula.
- Nuevas perspectivas del derecho a la información en la Sociedad de la Información. **6-7**, (Enero/Diciembre 2005), 11-25.
- MACHTA CHENDI, Zulay.
- El servicio público en el sector eléctrico venezolano y Derecho de las Telecomunicaciones. **5**, (Julio/Diciembre 2004), 41-80
- MADRID MARTÍNEZ, Claudia
- La internacionalización del consumo: el consumidor electrónico

- y la realidad venezolana. **12**, (2011), 7-51
- MARESCA, Fernando.
- Protección jurídica del software: un debate abierto. **1**, (2002), 147-156.
- MARTÍNEZ NADAL, Apollònia.
- Derechos de sociedades y Nuevas Tecnologías: aplicaciones presentes y futuras en el Derecho español. **10**, (2008-2009), 45-74
 - Las polémicas cláusulas de paridad en la contratación turística electrónica: ¿Prohibición absoluta o aceptación de cláusulas de paridad relativa?. **16**, (2015), 65-80
- MARTÍNEZ NADAL, Apollònia y FERRER GOMILA, Josep Luis.
- Delimitación de responsabilidades en caso de revocación de un certificado de firma electrónica: soluciones legales de Derecho europeo. **1**, (2002), 53-71.
- MATA, Miguel Ángel.
- La protección al consumidor en la contratación a distancia. **8**, (Enero/Diciembre 2006), 73-94.
- MATTUTAT MUÑOZ, Marjorie.
- La electrificación del procedimiento constitutivo de las sociedades mercantiles en Venezuela. **10**, (2008-2009), 111-131
- MONSALVE GONZÁLEZ, Karlith.
- Valor jurídico de la firma electrónica en el sistema legal venezolano. **10**, (2008-2009), 157-177
- MUNIVE CORTÉS, Erika Yamel.
- 2000 - 2015: 15 aniversario del Sistema Nacional e-México. **16**, (2015), 143-175
- NAHABETIÁN BRUNET, Laura.
- Responsabilidad civil en el marco del Gobierno de la Información. **16**, (2015), 9-46
- OLIVER LALANA, A. Daniel.
- Estrategias de protección de datos en el comercio electrónico. **3**, (Julio/Diciembre 2003), 51-71.
 - Internet como fuente de información accesible al público: pensando el derecho de protección de datos en su contexto social y jurídico. **8**, (Enero/Diciembre 2006), 49-72.
- PANIZA FULLANA, Antonia.
- Análisis jurídico de los *spyware*, *web bugs* y *mail bugs*. (Su problemática utilización en la protección de los derechos de autor). **6-7**, (Enero/Diciembre 2005), 91-113.
 - E-consumidores: aspectos problemáticos en la normativa española. **9**, (Enero/Diciembre 2007), 51-68
- PERALES VISCASILLAS, M^a del Pilar.
- Sobre la perfección del contrato en España: el “popurri” de los “nuevos” artículos 1262 del Código Civil y 54 del Código de Comercio. **2**, (Enero/Junio 2003), 7-19.
 - ¿Forma *escrita* del convenio arbitral?: Nuevas disposiciones de la CNUDMI/UNCITRAL. **9**, (Enero/Diciembre 2007), 27-49
- PÉREZ LUÑO, Antonio Enrique.
- Reflexiones sobre la contratación informática. **4**, (Enero/Julio 2004), 11-21
- PÉREZ PEREIRA, María.
- Proveedores de servicios de certificación: aspectos venezolanos y europeos. **1**, (2002), 33-51.
- PLAZA SOLER, Juan Carlos.
- Los correos electrónicos comerciales no solicitados en el Derecho español, europeo y estadounidense. **3**, (Julio/Diciembre 2003), 73-98.

- PONCE HEINSOHN, Ivonne
- Intervención notarial en la contratación electrónica: Especial referencia a la incorporación del documento público electrónico en el ordenamiento jurídico español y chileno. **11**, (2010), 131-157.
- QUIRÓS HIDALGO, José Gustavo.
- “El régimen de propiedad intelectual del profesorado universitario en España y su relación con los sistemas Open Access”. **6-7**, (Enero/Diciembre) 2005, 183-202.
- RAMÍREZ COLINA, Sulmer Paola.
- El teletrabajo y su sujeción a la Ley Orgánica del Trabajo. **2**, (Enero/Junio 2003), 61-80
 - El contrato electrónico laboral. **16**, (2015), 81-104
- REUSSER MONSÁLVEZ, Carlos.
- Las Bases de Datos de Perfiles de ADN y su (des) Protección en Europa. **5**, (Julio/Diciembre 2004), 147-157
- RICO CARRILLO, Mariliana.
- Firmas electrónicas y criptografía. **2**, (Enero/Junio 2003), 81-101.
- RODRÍGUEZ DE LAS HERAS BALLELL, Teresa
- La responsabilidad de los prestadores de servicios de intermediación y los estratos de la intermediación en la Red. **11**, (2010), 69-96
- RODRÍGUEZ, Gladys Stella.
- Principios jurídicos del contrato electrónico en el marco del comercio B2B: especial referencia a las PYMEs de los países en el desarrollo. **14**, (2013), 11-36.
- SALGADO SEGUÍN, Víctor Alberto.
- La Directiva europea sobre comercio electrónico. **1**, (2002), 73-91.
- SALGUEIRO A., José Ovidio.
- La Ley sobre Mensajes de Datos y Firmas Electrónicas de Venezuela. **1**, (2002), 25-32.
- SÁNCHEZ RODRÍGUEZ, Antonio Jesús.
- Monopolio y competencia en el Derecho comunitario europeo de las telecomunicaciones. **1**, (2002), 129-146.
- SANTANDER RENGIFO, Antonio.
- Una nueva vieja propuesta: la oferta al público por internet bajo la lupa de la Doctrina del Derecho Civil. **5**, (Julio/Diciembre 2004), 81-120.
- SARMIENTO, María Gabriela.
- Anteproyecto de Convención sobre la Contratación Electrónica llevado a cabo por el Grupo de Trabajo IV sobre Comercio Electrónico de la CNUDMI. **3**, (Julio/Diciembre 2003), 99-125.
- SEMENT VIDAL, María José.
- La protección jurídica del denominado “conocimiento libre”. **6-7**, (Enero/Diciembre 2005), 141-170.
- SOTO, Alberto.
- Derecho penal y delitos informáticos: Seguridad de la información, seguridad legal y seguridad jurídica. Una visión en Argentina. **3**, (Julio/Diciembre 2003), 167-178.
- USECHE CASTRO, Yasmin Carolina.
- El dilema entre el derecho a la intimidad y el secreto a las comunicaciones del trabajador y el poder de vigilancia y control del patrono. **13**, (2012), 47-59
- VALERO TORRIJOS, Julián.
- El acceso telemático a la información administrativa: un presupuesto inexcusable para la e-Administración (Análisis desde la perspectiva del Derecho español).

- 6-7, (Enero-Diciembre 2005), 27-51.
- VARGAS LEAL, Luis.
- Regulación de las telecomunicaciones en un ámbito de convergencia tecnológica. **4**, (Enero/Julio 2004), 23-62.
- VÁSQUEZ SÁNCHEZ, María Alejandra.
- La influencia de las nuevas tecnologías en el derecho probatorio venezolano: Los desafíos de la administración de justicia del siglo XXI. **13**, (2012), 9-25
- VÁZQUEZ, Víctor.
- La propuesta de Tratado de la OMPI sobre protección de las interpretaciones y ejecuciones audiovisuales. **6-7**, (Enero/Diciembre 2005), 229-245.
- WACHOWICZ, Marcos y REZENDE, Denis Alcides.
- La Tecnología de la Información y sus impactos en la propiedad intelectual. **2**, (Enero/Junio 2003), 43-59.
- YAYA NARVÁEZ, León David y CANO M., Jeimy J.
- Consideraciones legales y comerciales sobre VoIP en Colombia. **6-7**, (Enero-Diciembre 2005), 115-140.

CONFERENCIAS

- ÁLVAREZ CABRERA, Carlos S.
- Propiedad intelectual y nuevas tecnologías. **4**, (Enero/Julio 2004), 93
 - La ley y la seguridad de la información: una perspectiva regional. **8**, (Enero/Diciembre 2006), 261-272.
- AMONI REVERÓN, Gustavo Adolfo.
- El testamento electrónico. **4**, (Enero/Julio 2004), 193.
- ANTEQUERA, Ricardo Enrique.
- La propiedad intelectual: una herramienta de competitividad para las PYME. **8**, (Enero/Diciembre 2006), 197-208.
- ARAUJO - JUÁREZ, José.
- El nuevo "modelo de regulación" de las telecomunicaciones en Venezuela. **4**, (Enero/Julio 2004), 65-91.
- ARIAS DE RINCÓN, María Inés.
- El derecho de retractarse de los consumidores y usuarios electrónicos. **8**, (Enero/Diciembre 2006), 247-259.
- ARRIETA ZINGÜER, Miguel.
- Tributación e Internet. **4**, (Enero/Julio 2004), 145
- BARZALLO, José Luis.
- Derecho de autor, Internet y libre competencia. **8**, (Enero/Diciembre 2006), 221-245.
- BAUZÁ, Marcelo.
- Datos abiertos, ¿derecho humano?, ¿política pública? o ambas cosas. **16**, (2015), 237-252
- BRANDT GRATEROL, Leopoldo.
- Páginas Web: modalidades de aplicación en el comercio electrónico. **4**, (Enero/Julio 2004), 165

- COTINO HUESO, Lorenzo.
- Protección de datos y servicios públicos y privados de *Cloud Computing* en España y Europa. **16**, (2015), 195-216
- DÍAZ GARCÍA, Alexander.
- Desnaturalización del documento electrónico judicial con la apelación de la sentencia. El nuevo sistema penal acusatorio (El juicio oral) colombiano. **8**, (Enero/Diciembre 2006), 275-301.
- GUERRERO CARRERA, Jacqueline.
- Democracia deliberativa y participación ciudadana electrónica. **16**, (2015), 217-223
- GUERRERO LEBRÓN, María Jesús.
- Trámites de constitución de la Sociedad Limitada Nueva Empresa. **8**, (Enero/Diciembre 2006), 161-175.
- ILLESCAS ORTÍZ, Rafael.
- La continuada –y, a veces, desaparecida– electrificación del Derecho de sociedades mercantiles. **8**, (Enero/Diciembre 2006), 117-159.
- MENDOZA ENRÍQUEZ, Olivia Andrea.
- Plataformas ciudadanas de participación como herramientas del ejercicio de la libertad de expresión en Internet. **16**, (2015), 225-235
- NOVAS, Natalia Soledad; NOVAS, Jorge Alberto; RUANI, Humberto Félix; RUANI, Humberto Martín.
- Historia clínica electrónica. **16**, (2015), 253-262
- ORTA MARTÍNEZ, Raymond J.
- Importancia de la descripción de software y hardware en las pericias informáticas y otros actos judiciales. **4**, (Enero/Julio 2004), 187
- PÉREZ PEREIRA, María.
- España y las nuevas tecnologías: aspectos jurídicos. **4**, (Enero/Julio 2004), 177
 - La evolución de los sistemas de cifrado. **8**, (Enero/Diciembre 2006), 189-193.
- RAMOS HERRANZ, Isabel.
- Presentación VII Jornada de Derecho del Comercio Electrónico. **8**, (Enero/Diciembre 2006), 115-116.
- REMOLINA ANGARITA, Nelson.
- Data protection: aproximación global con énfasis en el caso colombiano. **4**, (Enero/Julio 2004), 109
- RICO CARRILLO, Mariliana.
- El uso de medios electrónicos en la convocatoria a la Junta General de Accionistas. **8**, (Enero/Diciembre 2006), 177-188.
- SÁNCHEZ, Diego.
- Las nuevas tecnologías, el acceso a la información y la participación ciudadana. **8**, (Enero/Diciembre 2006), 209-219.

CONTRIBUCIONES ESPECIALES

CUBEROS DE QUINTERO, María Antonia

- La participación ciudadana y el gobierno electrónico. **9**, (Enero/Diciembre 2007), 161-172.

CANO, Jeimy J.

- Informáticos forenses: los criminalistas informáticos en la sociedad de la información. **9**, (Enero/Diciembre 2007), 173-182.

- ¿Compartir o proteger? Tensiones en la gerencia de la seguridad de la información. **13**, (2012), 161-169

MARTÍNEZ NADAL, Apolonia, HERRERA-JOANCOMARTÍ, Jordi y PÉREZ-SOLÁ, Cristina

- Análisis técnico-jurídico del proceso de Iniciativa Legislativa Popular con recogida de firmas digitales en España, **11** (2010), 191-216.

COMENTARIOS ESPECIALIZADOS

RÍOS RUIZ, Wilson Rafael

- Análisis del Acuerdo Inicial y sus enmiendas planteadas por Google a los autores. Su situación actual. **11**, (2010), 219-244.

MUNIVE CORTÉS, Erika Yamel

- Voto electrónico y protección de datos personales: los avances de la democracia universitaria en el País Vasco. **12**, (2011), 189-208

RESEÑA LEGISLATIVA

ARRIETA ZINGUER, Miguel.

- Comentario al Proyecto de Ley de Responsabilidad Social en Radio y Televisión. **2**, (Enero/Junio 2003), 283-309.

AMONI REVERÓN, Gustavo Adolfo.

- Comentarios a las disposiciones generales del Decreto Ley de Interoperabilidad Electrónica. **13**, (2012), 173-187

CRÓNICA JURÍDICA

ORTA MARTÍNEZ, Raymond J.

- La Informática forense como medio de prueba. **3**, (Julio/Diciembre 2003), 255-260

SÁNCHEZ RODRÍGUEZ, Antonio Jesús

- El servicio de telecomunicaciones a través de las redes eléctricas: *Power Line Communications*

- (PLC). **3**, (Julio/Diciembre 2003), 261-268.
- ALTAMIRA, Matías.
- Mesa virtual de entrada judicial: derechos y responsabilidades. **8**, (Enero/Diciembre 2006), 329-336.
- BUENO DE MATA, Federico.
- Presente y futuro de los dispositivos telemáticos de localización de presos utilizados en España. **12**, (2011), 211-220

SECCION MONOGRÁFICA

Las implicaciones jurídicas de las redes sociales en Internet

- ARRIETA ZINGUER, Miguel.
- El impacto de las redes sociales en el comercio electrónico con consumidores. **14**, (2013), 135-164
- CHACÓN GÓMEZ, Nayibe.
- La responsabilidad de los proveedores de servicio en las redes sociales. **14**, (2013), 207-230
- LÓPEZ JIMÉNEZ, David.
- Las redes sociales como espacios publicitarios: el papel de la autorregulación. **14**, (2013), 165-186
- RAMÍREZ, Sulmer Paola.
- Los contenidos publicados por el trabajador en *Facebook* y sus consecuencias jurídico laborales. **14**, (2013), 187-205
- RICO CARRILLO, Mariliana y LÓPEZ JIMÉNEZ, David.
- Las redes sociales en Internet: consideraciones generales y problemática jurídica. **14**, (2013), 101-112
- RICO CARRILLO, Mariliana.
- El ejercicio de los derechos fundamentales y las libertades públicas a través de *Facebook*. **14**, (2013), 113-134

LÉGISLACIÓN

II.1. Nacional

Decretos

- Decreto N° 825 del 10 de mayo de 2000 mediante el cual se declara el acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político de la República Bolivariana de Venezuela. **1**, (2002), 185-188.
- Decreto N° 1.093 de 24 de noviembre de 2000 mediante el cual se decreta el Reglamento de Interconexión. **2**, (Enero/Junio 2003), 163-180.
- Decreto N° 1.094 de 24 de noviembre de 2000 mediante el cual se decreta el Reglamento sobre Habilitaciones Administrativas y Concesiones de uso y explotación del espectro radio-eléctrico. **2**, (Enero/Junio 2003), 181-207.

- Decreto N° 1.095 de 24 de noviembre de 2000 mediante el cual se decreta el Reglamento de apertura de los servicios de telefonía básica. **2**, (Enero/Junio 2003), 209-245.
- Decreto N° 2.189 de 13 de diciembre de 2002 mediante el cual se decreta el Reglamento sobre los tributos establecidos en la Ley Orgánica de Telecomunicaciones. **2**, (Enero/Junio 2003), 255-280.
- Decreto-Ley de Mensajes de Datos y Firmas Electrónicas. **1**, (2002), 255-273.
- Decreto N° 2.614, de fecha 24 de septiembre de 2003 mediante el cual se decreta el Reglamento de la Ley Orgánica de Telecomunicaciones sobre el Servicio Universal de Telecomunicaciones. **4**, (Enero/Julio 2004), 301-322.
- Decreto N° 3.335, de fecha 12 de diciembre de 2004, mediante el cual se decreta el Reglamento Parcial del Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas. **6-7**, (Enero/Diciembre 2005), 331-344.
- Decreto N° 3.390, de fecha 23 de diciembre de 2004, sobre el uso del software libre en la Administración Pública. **6-7**, (Enero/Diciembre 2005), 345-349.
- Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado. **13**, (2012), 191-215
- Leyes
- Ley especial contra los Delitos Informáticos. **1**, (2002), 275-285.
- Ley Orgánica de Telecomunicaciones. **1**, (2002), 189-253.
- Ley de Responsabilidad Social en Radio y Televisión. **6-7**, (Enero/Diciembre 2005), 249-298.
- Ley Orgánica de Ciencia, Tecnología e Innovación. **6-7**, (Enero/Diciembre 2005), 299-329.
- Ley para la protección de niños, niñas y adolescentes en salas de uso de internet, video juegos y otros multimedia. **8**, (Enero/Diciembre 2006), 305-314.
- Ley de Tarjetas de Crédito, Débito, Prepagadas y demás Tarjetas de Financiamiento o Pago Electrónico, **10**, (2008-2009), 181-202
- Ley Orgánica de Ciencia, Tecnología e Innovación. **12**, (2011), 223-246
- Reglamentos
- Reglamento sobre facturación y recaudación a solicitud y por cuenta de los operadores de los servicios de telefonía de larga distancia nacional y larga distancia internacional de fecha 8 de noviembre de 2004. **8**, (Enero/Diciembre 2006), 315-326.
- Reglamento Parcial de la Ley Orgánica de Ciencia, Tecnología e Innovación referido a los Aportes e Inversión de fecha 9 de octubre de 2006. **9**, (Enero/Diciembre 2007), 207-220.
- Resoluciones
- Resolución contentiva de los atributos de las Habilitaciones Administrativas publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.215 de 8 de junio de 2001. **2**, (Enero/Junio 2003), 247-254.
- Resolución N° 400 de fecha 20 de febrero de 2004, Normas para el Registro de contribuyentes de los tributos de telecomunicaciones. **5**, (Julio/Diciembre 2004), 253-255.
- Resolución N° 401 de fecha 20 de febrero de 2004, Requisitos para declarar y pagar los tributos de telecomunica-

- ciones. **5**, (Julio/Diciembre 2004), 257-261.
- Resolución N° 408 de fecha 9 de marzo de 2004, Condiciones bajo las cuales los operadores de los servicios móviles de telecomunicaciones podrán ofrecer itinerancia o roaming a sus abonados. **5**, (Julio/Diciembre 2004), 263-266.
- Resolución por la cual se dictan “Normas que Regulan los Procesos Administrativos relacionados a la Emisión y Uso de las Tarjetas de Crédito, Débito, Prepagadas y demás Tarjetas de Financiamiento o Pago Electrónico”, **10**, (2008-2009), 203-226.
- Resolución por la cual se dictan “Normas relativas a la Protección de Usuarios y Usuarías de los servicios Financieros”. **12**, (2011), 247-265

Providencias

- Providencia Administrativa que establece el deber de presentación electrónica de las Declaraciones del Impuesto sobre la Renta. **11**, (2010), 247-249
- Providencia Administrativa que establece el deber de presentación electrónica de las Declaraciones del Impuesto al Valor Agregado. **11**, (2010), 251-253

II.2. Internacional

Directivas

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999. **3**, (Julio/Diciembre 2003), 197-211.
- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000. **3**, (Julio/Diciembre 2003), 213-242.
- Directiva 2000/46/CE del Parlamento Europeo y del Consejo, de 18 de septiembre de 2000. **3**, (Julio/Diciembre 2003), 243-252.
- Directiva 2007/64/CE del Parlamento Europeo y del Consejo de 13 de abril de 2007 sobre servicios de pago en el mercado interior. **10**, (2008-2009), 227-301.
- Directiva 2009/64/CE del Parlamento Europeo y del Consejo del 23 de abril de 2009 sobre Protección jurídica de programas de ordenador. **11**, (2010), 341-349.
- Directiva 2010/13/UE del Parlamento Europeo y del Consejo de 10 de marzo de 2010 sobre la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual). **12**, (2011), 267-311

Leyes Modelo

- Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) con la guía para su incorporación al Derecho Interno. **3**, (Julio/Diciembre 2003), 181-190.
- Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001). **3**, (Julio/Diciembre 2003), 191-196.

Legislación española

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. **4**, (Enero/Julio 2004), 219-261.
- Ley 59/2003, de firma electrónica. **4**, (Enero/Julio 2004), 263-300.
- Ley 32/2003, de 3 denoviembre, General de Telecomunicaciones. **5**, (Julio/Diciembre 2004), 161-252.
- Ley 22/2007, de 11 de julio, sobre Comercialización a Distancia de Servicios

- Financieros destinados a los Consumidores. **9**, (Enero/Diciembre 2007), 185-2005.
- Ley 16/2009 de 13 de noviembre, sobre Servicio de Pago. **11**, (2010), 255-304.
- Ley 7/2010 de 31 de marzo, General de la Comunicación Audiovisual. **12**, (2011), 313-393
- Real Decreto 322/2008 de 29 de febrero sobre el régimen jurídico de las entidades de dinero electrónico, **10**, (2008-2009), 303-322.
- Real Decreto 899/2009 de 22 de mayo, se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas. **11**, (2010), 305-340.
- Ley 5/2012, de 6 de julio, de Mediación en Asuntos Civiles y Mercantiles. **13**, (2012), 217-244
- Unión Europea*
- Reglamento (UE) N° 524/2013 del Parlamento Europeo y del Consejo de 21 de mayo 2013 sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) n° 2006/2004 y la Directiva 2009/22/CE. **16**, (2015), 265-289

JURISPRUDENCIA

AMONI REVERÓN, Gustavo Adolfo.

- La citación electrónica. Comentarios al auto N° 339 dictado por el Juscago de Sustanciación de la Sala Político Administrativa del Tribunal Supremo de Justicia, el 7 de agosto de 2012. **14**, (2013), 233-245

ARRIETA ZINGÜER, Miguel.

- La gravabilidad de las actividades de telecomunicaciones y la potestad tributaria municipal. Comentario a la sentencia de 03 de agosto de 2004 del Tribunal Supremo de Justicia venezolano. **5**, (Julio/Diciembre 2004), 269-275.
- Procedencia de la suspensión de los efectos del acto recurrido en materia sancionatoria de telecomunicaciones. Comentario a la sentencia de 09 de noviembre de 2005 del Tribunal Supremo de Justicia. **6-7**, (Enero/Diciembre 2005), 357-364.

- Consideraciones acerca de las redes sociales en Internet como elemento de convicción en la radicación de juicios penales en decisiones del Tribunal Supremo de Justicia. **14**, (2013), 295-304

FERRER CASTRO, Mileidi Paola y Jenny QUINTERO MENDOZA, Carolina.

- Consideraciones sobre el reciente criterio del Tribunal Supremo de Justicia venezolano respecto al tratamiento de los correos electrónicos impresos como medios de prueba. **13**, (2012), 247-252

LASTIRI SANTIAGO, Mónica.

- El contrato de licencia y los nombres de dominio. Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea (Sala Segunda), de 19 de julio de 2012 asunto C-376/11, *Pie Optiek SPRL & Bureau Gevers SA, European Registry for Internet Domains ASBL*. **14**, (2013), 249-252

PALAZZI, Pablo A.

- Google y el derecho a la privacidad sobre las búsquedas realizadas en Internet. **8**, (Enero/Diciembre 2006), 339-349.

RAMÍREZ, Sulmer Paola.

- Valor jurídico probatorio del correo electrónico promovido en formato impreso. Comentarios a la sentencia de la Sala de Casación Civil del Tribunal Supremo de Justicia el 30 de mayo de 2013. **14**, (2013), 265-269

RICO CARRILLO, Mariliana.

- Interposición del recurso de amparo a través de medios electrónicos. Sentencias y comentarios jurisprudenciales. **1**, (2002), 289-319.
- La notificación por medios electrónicos. Comentario a la sentencia de 01 de febrero de 2000 del Tribunal Supremo de Justicia venezolano. **2**, (Enero/Junio 2003), 313-314.
- El valor jurídico de la página Web del Tribunal Supremo de Justicia. **3**, (Julio/Diciembre 2003), 271-273.
- La eficacia probatoria de los correos electrónicos en la jurisprudencia del Tribunal Supremo de Justicia venezolano. **10**, (2008-2009), 325-330.
- Consideraciones sobre la validez de las condiciones generales y particulares de las pólizas de seguros contenidas en soportes documentales electrónicos. **11**, (2010), 353-358.
- De nuevo sobre el valor probatorio de los correos electrónicos en la jurisprudencia del Tribunal Supremo de Justicia venezolano. **12**, (2011), 397-400

- La posición del Tribunal Supremo de Justicia venezolano respecto a las pruebas documentales electrónicas. **16**, (2015), 293-299

SALGUEIRO, José Ovidio.

- El valor probatorio del correo electrónico. Comentario a la sentencia 2201-04 de la Corte Superior del Niño y el Adolescente del Área Metropolitana y Nacional de Adopción Internacional. **6-7**, (Enero/Diciembre 2005), 353-355.

URSO CEDEÑO, Giuseppe.

- Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia que resuelve el Recurso de Colisión intentado entre el artículo 40 de la Ley de Protección al Consumidor y al Usuario y los artículos 145 y 214 de la Ley Orgánica de Telecomunicaciones. **4**, (Enero/Julio 2004), 325-329

Sentencias

Sentencia del Tribunal Supremo de Justicia venezolano de 03.08.2001 sobre el reconocimiento del valor jurídico de la información contenida en el sitio web del Tribunal. **1**, (2002), 320-323.

Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia venezolano de 01 de febrero de 2000. **2**, (Enero/Junio 2003), 315-337

Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia venezolano de 19 de agosto de 2002. **3**, (Julio/Diciembre 2003), 275-277.

Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia venezolano de 05 de agosto de 2003. **4**, (Enero/Julio 2004), 331-338

Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia ve-

- nezolano de 03 de agosto de 2004. **5**, (Julio/Diciembre 2004), 277-305
- Sentencia de la Sala Político-Administrativa del Tribunal Supremo de Justicia venezolano de 8 de noviembre de 2005. **6-7**, (Enero/Diciembre 2005), 365-374.
- In the United States District Court for the Northern District of California San Jose División, fecha 17 de marzo 2006, **8**, (Enero/Diciembre 2006), 351-369.
- Sentencia de la Sala Político Administrativa del Tribunal Supremo de Justicia venezolano de fecha 22 de mayo de 2007 sobre el caso RCTV. **9**, (Enero/Diciembre 2007), 223-259.
- Sentencia de la Sala de Casación Civil del Tribunal Supremo de Justicia venezolano de fecha 24 de octubre de 2007 sobre el valor probatorio de los medios electrónicos. **9**, (Enero/Diciembre 2007), 261-317.
- Sentencia de la Sala de Casación Social del Tribunal Supremo de Justicia venezolano de 5 de marzo de 2007. **10**, (2008-2009), 331-354.
- Sentencia de la Sala Político Administrativa del Tribunal Supremo de Justicia venezolano de 12 de febrero de 2008. **10**, (2008-2009), 355-400.
- Sentencia de la Sala Político Administrativa del Tribunal Supremo de Justicia venezolano de 12 de agosto de 2009. **11**, (2010), 359-373
- Sentencia de la Sala de Casación Social del Tribunal Supremo de Justicia venezolano de 2 de julio de 2010. **12**, (2011), 401-407
- Sentencia de la Sala de Casación Civil del Tribunal Supremo de Justicia venezolano de 5 de octubre de 2011. **13**, (2012), 253-277
- Sentencia de la Sala Político Administrativa. Juzgado de Sustanciación del Tribunal Supremo de Justicia de 7 de agosto de 2012. **14**, (2013), 247-248
- Sentencia del Tribunal de Justicia de la Unión Europea (Sala Segunda), 19 de julio de 2012. **14**, (2013), 253-264
- Sentencia de la Sala de Casación Civil del Tribunal Supremo de Justicia de 30 de mayo de 2013. **14**, (2013), 271-293
- Sentencia de la Sala de Casación Penal del Tribunal Supremo de Justicia de 13 de abril de 2013. **14**, (2013), 305-312
- Sentencia de la Sala de Casación Penal del Tribunal Supremo de Justicia de 12 de abril de 2012. **14**, (2013), 313-324
- Sentencia de la Sala de Casación Penal del Tribunal Supremo de Justicia de 28 de abril de 2011. **14**, (2013), 325-332

RECENSIÓN

PÉREZ PEREIRA, María.

- BARRAL VIÑALS, Immaculada (Coord.) *La regulación del comercio electrónico*. Edt. Dykinson,

Madrid 2003, 207 págs. **3**, (julio/Diciembre 2003), 281-282.

- BRANDT GRATEROL, Leopoldo. *Páginas web: condiciones*,

- políticas y términos legales*. Editorial Legis, Caracas, 2001, 358 págs. **3**, (Julio/Diciembre 2003), 283-284.
- RAMOS HERRANZ, Isabel: *Marcas versus nombres de dominio en Internet*, Iustel, Madrid, 2004, págs. 351. **5**, (Julio/Diciembre 2004), 309-310.
 - RICO CARRILLO, Mariliana: *Comercio electrónico, Internet y Derecho*. Edt. Legis, Caracas, 2003, 277 págs. **3**, (Julio/Diciembre 2003), 285.
- RANGEL GÓMEZ, Horacio.
- LASTIRI SANTIAGO, Mónica. *La comercialización del nombre de dominio*. Los bienes jurídicos digitales, el derecho de control y los nombres de dominio. Ed. Marcial Pons, España (2014), **16**, (2015), 303-309
- RICO CARRILLO, Mariliana.
- BRICEÑO, Francisco (Coord.): *Aspectos legales del comercio electrónico*, Cavecom, Caracas, 2004, 294 págs. **4**, (Enero/Julio 2004), 341-245.
 - BATUECAS CALETRIO, Alfredo: *Pago con tarjeta de crédito: Naturaleza y régimen jurídico*, Revista Aranzadi de Derecho Patrimonial N° 15 (monográfico), Thomson-Aranzadi, Navarra, 2005, 429 págs. **6-7**, (Enero/Diciembre 2005), 377-378.
- MARTÍNEZ NADAL, Apol.lonia. *El pago capitativo en la prestación de servicios médicos*. Civitas Thomson Reuters Aranzadi, España 2015. **16**, (2015), 311-314
 - KOZOLCHYK, Boris, Ph. D. *Comparative Commercial Contracts: Law, Culture and Economic Development*. West Academic Publishing, United States of America, 2014 . **16**, (2015), 315-319
- ALBA FERNÁNDEZ, Manuel.
- RODRÍGUEZ DE LAS HERAS BADELL, Teresa: *El régimen jurídico de los Mercados Electrónicos Cerrados (e-Marketplaces)*, Madrid, Marcial Pons, 2006. **9**, Enero/Diciembre 2007), 321-324.
- LÓPEZ JIMÉNEZ, David.
- RICO CARRILLO, Mariliana: *El pago electrónico en Internet: estructura operativa y régimen jurídico*, Madrid, Thomson Reuters Aranzadi, 2012, 304 páginas. **13**, (2012), 281-284

Reglas para el envío de artículos

1. El material presentado debe ser inédito, entendiéndose que el mismo no ha sido publicado ni sometido para publicación en otro medio de divulgación. El Consejo Editorial se reserva el derecho de publicar de manera excepcional artículos que ya han sido publicados.
2. Los artículos deben estar redactados en programas editores que funcionen en ambiente Windows™ 3.0 o superiores. Los gráficos o imágenes que contenga el artículo deben estar especificados con los formatos o extensiones en que se hicieron (Excel™, Corel Draw™, jpg, gif, bmp, y otros), asimismo, las ilustraciones deben estar numeradas y a continuación del texto (no se aceptarán las que se encuentren al final del artículo). Las revistas podrán decidir no incluirlas, previa comunicación al autor o autores, si éstas no llenan los requisitos técnicos para su reproducción.
3. El texto del artículo debe redactarse tomando en cuenta los siguientes parámetros:
 - 3.1. La primera página debe contener:
 - a) Título del artículo
 - b) Nombre del autor o autores
 - c) Título académico y afiliación institucional
 - d) Dirección del autor y correo electrónico
 - e) Síntesis curricular no mayor a diez (10) líneas
 - 3.2. La segunda página debe contener un resumen no mayor de ciento cuarenta (140) palabras, concentrándose en los objetivos, métodos de estudio, resultados y conclusiones. Al final del mismo se deben incluir las palabras claves en un número no mayor a cinco (5).
 - a) El resumen y las palabras claves deben venir redactadas en español e inglés
 - b) Se podrán aceptar artículos redactados en inglés, francés u otros idiomas sólo en casos especiales, debiendo contener las palabras claves en español e inglés.
 - 3.3. El texto del artículo debe estructurarse en secciones debidamente identificadas, siendo la primera la introducción (o reseña de los conocimientos existentes, limitada estrictamente al tema tratado en el artículo). Las secciones deben identificarse sólo con números arábigos. Cada artículo antes de la primera sección o sección introductoria, debe tener un sumario en el que se enumeren los temas que se van a desarrollar (las secciones en las cuales fue dividido el trabajo).
 - 3.4. Si parte del material trabajado (textos, gráficos e imágenes utilizados) no son originales del autor o de los autores, es necesario que los mismos estén acompañados del correspondiente permiso del autor (o de los autores) y el editor donde fueron publicados originalmente, en su defecto, se debe indicar la fuente de donde fueron tomados.
 - 3.5. En las referencias bibliográficas se debe utilizar el sistema de cita formal, haciendo la correspondiente referencia en las notas a pie de página, las cuales deben ser enumeradas en números arábigos, siguiendo un orden correlativo.

Las citas, en las notas al pie de página, se harán siguiendo los siguientes ejemplos; según se trate de:

A. Libros

Mariano Aguilar Navarro: *Derecho Internacional Privado*, VI. 4a. edición, 2a. reimpresión. Madrid. Universidad Complutense de Madrid, 1982, p.199 (o pp. 200 y ss).

Marino Barbero Santos: "Consideraciones sobre el Estado peligroso y las Medidas de Seguridad, con especial referencia al Derecho Italiano y Alemán". *Estudios de Criminología y Derecho Penal*. Valladolid. Universidad de Valladolid, 1972, pp. 13-61.

Vicente Mujica Amador: *Aproximación al Hombre y sus Ideologías*. Caracas. Editorial Vidabun, 1990.

Hans Kelsen: *Teoría Pura del Derecho*. XVII edición. Buenos Aires. EUDEBA, 1981.

B. Cita sucesiva del mismo libro

M. Aguilar N.: *Derecho Internacional* V.II.... op. cit., p.78 y ss.

C. Obras colectivas

Haydée Barrios: "Algunos aspectos de cooperación judicial internacional en el sistema venezolano de derecho internacional privado". *Libro-Homenaje a Werner Goldschmidt*. Caracas. Facultad de Ciencias Jurídicas y Políticas, Universidad Central de Venezuela. 1997, pp. 383-419. Si se desea citar un determinado párrafo o página se agrega: especialmente, p. 80 o pp. 95-98.

D. Revistas

Gonzalo Parra-Aranguren: "El Centenario de la Conferencia de La Haya de Derecho Internacional Privado". *Revista de la Facultad de Ciencias Jurídicas y Políticas*, N° 85. Caracas. Universidad Central de Venezuela, 1992, pp. 75-100.

E. Cita sucesiva del mismo artículo

G. Parra-Aranguren: "*El Centenario de la Conferencia...*" op.cit., pp.80-85.

F. Citas de jurisprudencia

Orden de citar: Tribunal, N° y fecha de la sentencia, partes y fuentes de publicación.

Ejemplo:

Corte Superior del Distrito Federal, N° ..., 6-5-1969 (Jacques Torfs vs. Clemencia de Mier Garcés), Jurisprudencia Ramirez y Garay, Vol. 21, p. 163.

G Citas de testimonios verbales y entrevistas

Se indicará el nombre de la persona que proporciona la información, la forma como se obtuvo y la fecha. Por ejemplo:

F. Rodríguez. Entrevista, 30/03/1999.

Esta información puede suministrarse siempre que lo autorice quien proporciona la información¹.

H. Citas de páginas web

Si la cita se refiere a un sitio web (cita de carácter general) se coloca el *home page*. Si es una página específica dentro de un sitio web (cita de carácter especial) se debe colocar en primer lugar, la dirección del *link* (sub-página) y en segundo lugar la dirección donde aparece alojada la información, (*home page*). Debe indicarse también la fecha de la consulta, entre corchetes, indicando el año, luego el mes y finalmente el día

Ejemplos:

- a) Cita de carácter general:
www.zur2.com.fipa. [Consulta: 2008, Noviembre 27].
- b) Cita de carácter especial:
 - Tatiana B. de Maekelt: La Ley de Derecho Internacional Privado <http://zur2.com/users/fipa/objetivos/leydip1/tamaek.htm> 10/02/2001.
www.zur2.com.fipa. [Consulta: 2008, Noviembre 27].
 - Haydée Barrios: El Domicilio
<http://zur2.com/users/fipa/objetivos/leydip1/barrios.htm> 8/04/2002.
www.zur2.com.fipa. [Consulta: 200, Noviembre 27].
4. Los artículos deben tener una extensión no mayor de cuarenta (40) cuartillas o páginas, escritas a espacio y medio y con un margen izquierdo de cuatro (4) centímetros. Tipo de letra: Times New Roman 12.
5. Los artículos pueden ser remitidos en un archivo adjunto, a la dirección electrónica: albornoz@ucat.edu.ve, o al correo electrónico del director de la revista:
 - Revista Tachirenses de Derecho: Prof. José Luis Villegas villegas@ucat.edu.ve
 - Revista *Tributum*: Prof. Jesús Manuel Oliveros joliveros@ucat.edu.ve
 - Revista Paramillo: Prof. Felipe Guerrero felipeguerrero11@gmail.com
 - Revista Derecho y Tecnología: Prof. Mariliana Rico marilianarico@yahoo.com
6. Los autores deberán firmar una autorización (en un formato que remitirá a tal efecto) donde se especifica el derecho que tiene la revista, y por ende, la Universidad Católica del Táchira, de reproducir el artículo en este medio de comunicación, sin ningún tipo de retribución económica o compromiso de la Universidad con el autor o los autores, entendiéndose éste como una contribución a la difusión del conocimiento y/o desarrollo tecnológico, cultural o científico de la comunidad o del país en el área en que se inscribe.
7. Cuando se envíen textos que estén firmados por más de un autor, se presumirá que todos los autores han revisado y aprobado el original enviado.

¹ UPEL: *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales*. Caracas. FEDEUPEL. 2003, p. 91.

8. Se reserva el derecho de hacer las correcciones de estilo que se consideren convenientes, una vez que el trabajo haya sido aceptado por el Consejo de Redacción para su publicación.
9. Los artículos serán analizados por un Comité de Árbitros y por un Consejo de Redacción. El cumplimiento de las normas no garantiza su publicación, si el trabajo no es aprobado por estas instancias.
10. La Universidad Católica del Táchira, el editor y el Consejo de Redacción de la revista, no se responsabilizarán de las opiniones expresadas por los colaboradores en sus respectivos artículos.
11. La UCAT se reserva el derecho de distribuir el contenido de la revistas en su página web o en otras páginas de contenido académico o científico.

Article Submissions Guidelines

1. The material must be unpublished, understanding it had not been published or presented to be evaluated by other divulging means. The Editorial Board reserves the right to publish articles, in exceptional cases, when they have already been published.
2. Articles must be redacted in editor programs that work in WindowsTM 3.0 or higher. The graphics or images that present the article must be specified with the formats or extensions where they were made (ExcelTM, Corel DrawTM, jpg, gif, bmp, and others). In the same way, the illustrations must be numbered just after the text (Those illustrations at the end of the article will be not accepted). The journals could decide not to include them, by communication to the author or authors in advance, if they do not fulfill the technical requirements to their publication.
3. The text of the article must be redacted considering the following parameters:
 - 3.1. The first page must have:
 - a) Title of the article
 - b) Author or author's name
 - c) Academic title and institutional affiliation
 - d) Author address and e-mail
 - e) Resume no longer than 10 lines
 - 3.2. The second page must have an abstract no longer than one hundred and forty words (140), focusing on the goals, methodology, results and conclusions. At the end, the key words must be included in a maximum number of five (5).
 - a) The abstract and the key words must be written in Spanish and English.
 - b) Articles in English, French and other languages could be accepted, just in special cases. In all cases they must have the key words in Spanish and English.
 - 3.3. The text article must be structured in clearly identified sections, being the first the introduction (description of the existent knowledge, limited to the subject of the article). The sections must be identified with Roman and Arabic numerals. Each article, before section one or introduction, must have a summary where appear numbered the subjects to be discuss on the paper (sections the article was divided).
 - 3.4. If part of the material (text, graphics, images) is not original of the author or authors, is necessary that this material to be authorized by the original author (or authors) and the editor where were first published, in lack of this, the source where they were taken must be indicated.
 - 3.5. The formal citing system must be used for the bibliographic references, doing the right reference at the foot of the page numbered in Arabic numeral, following a correlative order.

The references in the footnotes will be included according to the following examples:

A. Books

Mariano Aguilar Navarro: *Derecho Internacional Privado*, VI. 4a. edición, 2a. reimpresión. Madrid. Universidad Complutense de Madrid, 1982, p.199 (o pp. 200 y ss).

Marino Barbero Santos: "Consideraciones sobre el Estado peligroso y las Medidas de Seguridad, con especial referencia al Derecho Italiano y Alemán". *Estudios de Criminología y Derecho Penal*. Valladolid. Universidad de Valladolid, 1972, pp. 13-61.

Vicente Mujica Amador: *Aproximación al Hombre y sus Ideologías*. Caracas. Editorial Vidabun, 1990.

Hans Kelsen: *Teoría Pura del Derecho*. XVII edición. Buenos Aires. EUDEBA, 1981.

B. Subsequent quotations of the same book

M. Aguilar N.: *Derecho Internacional V.II...* op. cit., p.78 y ss.

C. Collective Works

Haydée Barrios: "Algunos aspectos de cooperación judicial internacional en el sistema venezolano de derecho internacional privado". *Libro-Homenaje a Werner Goldschmidt*. Caracas. Facultad de Ciencias Jurídicas y Políticas, Universidad Central de Venezuela. 1997, pp. 383-419. Si se desea citar un determinado párrafo o página se agrega: especialmente, p. 80 o pp. 95-98.

D. Journals

Gonzalo Parra-Aranguren: "El Centenario de la Conferencia de La Haya de Derecho Internacional Privado". *Revista de la Facultad de Ciencias Jurídicas y Políticas*, N° 85. Caracas. Universidad Central de Venezuela, 1992, pp. 75-100.

E. Subsequent quotations of the same article

G. Parra-Aranguren: "*El Centenario de la Conferencia...*" op.cit., pp.80-85.

F. Quotation of jurisprudence:

Corte Superior del Distrito Federal, N°..., 6-5-1969 (Jacques Torfs vs. Clemencia de Mier Garcés), Jurisprudencia Ramirez y Garay, Vol. 21, p. 163.

G. Quotation of oral testimonies and interviews

It must include the name of the person providing the information, how it was obtained, and the date:

F. Rodríguez. Entrevista, 30/03/1999.

This information can be provided only if it is authorized by the provider of the information¹.

¹ UPEL: *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales*. Caracas. FEDEUPEL. 2003, p. 91.

H. Quotation of web pages

If a quote refers to an entire website (general citation), should include the reference of the home page. If is a **specific page within a website** (special citation), should include in first place, the link (sub-page) and in second place, the reference of the home page. It should also indicate the date the page was visited. This information should be in listing showing year, month, and day.

- a) General quotation:
www.zur2.com.fipa. [Visited: 2008, Noviembre 27].
- b) Special quotation:
 - Tatiana B. de Maekelt: La Ley de Derecho Internacional Privado <http://zur2.com/users/fipa/objetivos/leydip1/tamaek.htm> 10/02/2001.
www.zur2.com.fipa. [Consulta: 2008, Noviembre 27].
 - Haydée Barrios: El Domicilio
<http://zur2.com/users/fipa/objetivos/leydip1/barrios.htm> 8/04/2002.
www.zur2.com.fipa. [Visited: 200, Noviembre 27].
4. Articles must have a maximum extension of forty (40) pages written in 1.5 space with a left margin of four (4) centimeters. The type letter will be Times New Roman 12.
5. Articles must be sent in an attachment to the e-mail: albornoz@ucac.edu.ve, or to the e-mail of the director of the journal:
 - Revista Tachirensis de Derecho: Prof. José Luis Villegas villegas@ucac.edu.ve
 - Revista *Tributum*: Prof. Jesús Manuel Oliveros joliveros@ucac.edu.ve
 - Revista Paramillo: Prof. Felipe Guerrero felipeguerrero11@gmail.com
 - Revista Derecho y Tecnología: Prof. Mariliana Rico marilianarico@yahoo.com
6. Authors should sign an authorization (a format will be sent to this purpose) where it is specified the right of the journal, as well as the Universidad Católica del Táchira, to publish the article on this divulging means, without any economic retribution or commitment of the University with the author or authors, understanding the article is a contribution to the divulging of knowledge and technological development, cultural or scientific of the community or the country in the area where it is registered.
7. When articles are sign by more than an author, it would be presumed that all authors have been check and approved the original text sent.
8. The right of change of stylus that is considered convenient is reserved, once the article has been accepted by the Editorial Board for its publication.
9. An Arbitral Committee and an Editorial Board will analyze the articles. The observance of these rules does not guarantee the publication of the article if this is not approved by these instances.
10. The Universidad Católica del Táchira, the editor, and the Editorial Board of the journal, are not responsible of the expressed opinions by the collaborating and the articles.

- 11 The Universidad Católica del Táchira reserves the right to distribute the contents of their journals on its website, or on other pages of academic or scientific content.

DERECHO Y TECNOLOGÍA

**VICERRECTORADO ACADÉMICO
DECANATO DE INVESTIGACIÓN Y POSTGRADO**

1/2015 Edición Digital

16/2015 Edición Digital

Revista de Derecho y Tecnología, Enero / Diciembre 2015,
de la Universidad Católica del Táchira.
San Cristóbal - Venezuela

DERECHO Y TECNOLOGÍA

ÍNDICE

DOCTRINA

Artículos

- Laura NAHABETIÁN BRUNET: Responsabilidad civil en el marco del Gobierno de la Información
Horacio FERNÁNDEZ DELPECH: La Cloud Computing. Una visión Argentina
Apolònia MARTÍNEZ NADAL: Las polémicas cláusulas de paridad en la contratación turística electrónica:
¿Prohibición absoluta o aceptación de cláusulas de paridad relativa?
Sulmer Paola RAMÍREZ: El contrato electrónico laboral
Nayibe CHACÓN GÓMEZ: La transferencia tecnológica: ¿Desarrollo de una política pública en Venezuela?
Gustavo Adolfo AMONI REVERÓN: Posibles soluciones a problemas de la audiencia de casación penal telemática
Erika Yamel MUNIVE CORTÉS: 2000 - 2015: 15 aniversario del Sistema Nacional e-México
Miguel ARRIETA ZINGÜER: Comercio electrónico y redes sociales: nuevo paradigma negocial

Conferencias

XIX Congreso Iberoamericano de Derecho e Informática. Federación Iberoamericana de Asociaciones de Derecho e Informática. Medellín, agosto 2015

- Lorenzo COTINO HUESO: Protección de datos y servicios públicos y privados de Cloud Computing en España y Europa
Jacqueline GUERRERO CARRERA: Democracia deliberativa y participación ciudadana electrónica
Olivia Andrea MENDOZA ENRÍQUEZ: Plataformas ciudadanas de participación como herramientas del ejercicio de la libertad de expresión en Internet
Marcelo BAUZÁ: Datos abiertos, ¿derecho humano?, ¿política pública? o ambas cosas
Natalia Soledad NOVAS; Jorge Alberto NOVAS; Humberto Félix RUANI y Humberto Martín RUANI: Historia clínica electrónica

Legislación

Unión Europea

Reglamento (UE) No 524/2013 del Parlamento Europeo y del Consejo de 21 de mayo 2013 sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) no 2006/2004 y la Directiva 2009/22/CE

Jurisprudencia

Mariliana RICO CARRILLO: La posición del Tribunal Supremo de Justicia venezolano respecto a las pruebas documentales electrónicas

Recensión

Selección y comentarios sobre bibliografía jurídica especializada.

Horacio RANGEL GÓMEZ

- LASTIRI SANTIAGO, Mónica. La comercialización del nombre de dominio. Los bienes jurídicos digitales, el derecho de control y los nombres de dominio. Ed. Marcial Pons, España (2014), 352 pp.

Mariliana RICO CARRILLO

- MARTÍNEZ NADAL, Apol. Ionia. El pago caputivo en la prestación de servicios médicos. Civitas Thomson Reuters Aranzadi, España 2015.
- KOZOLCHYK, Boris, Ph. D. Comparative Commercial Contracts: Law, Culture and Economic Development. West Academic Publishing, United States of America, 2014

Índice acumulado