Normas de Comercio Electrónico en Materia de Seguridad y Privacidad y su Reflejo en Colombia

Electronic commerce rules in matter of security and privacy and its reflection in Colombia

JORGE RICARDO PALOMARES G.
Abogado de la Universidad Santo Tomás-Bogotá, Legum Magister (LL.M.) Universität Konstanz-Alemania. Docente Tutor de la Maestría en Derecho Público de la Universidad Santo Tomás-Bogotá, Investigador del Proyecto "Globalización del Derecho Privado", Dirigido por la Universidad Santo Tomás-Bogotá y la Deutsche Gesellschaft für die Internationale Zusammenarbeit GIZ
jorge26859@hotmail.com.

Lawyer of the Universidad Santo Tomás, Bogotá. Legum Magister (LL.M.) University of Konstanz, Germany. Tutor professor of the Master in public law of the Universidad Santo Tomás, Bogotá. Investigator of the project "Globalization of private law", directed by the Universidad Santo Tomás, Bogotá and the Deutsche Gesselschaft für die Internationale Zusammenarbeit GIZ.
Jorge26859@hotmail.com

Fecha de recepción: 8 de junio de 2011
Fecha de Evaluación: 22 de agosto de 2011
Fecha de aceptación: 23 de septiembre de 2011

RESUMEN. El presente escrito hace una breve presentación de la existencia de una pluralidad de normas –de distinto origen- que convergen en la regulación del Comercio Electrónico, especialmente en materias como seguridad y privacidad.

Asimismo se describe cómo dichas normas funcionan en Colombia e interactúan con la Ley 527 de 1999.

PALABRAS CLAVE. Comercio Electrónico, Nueva Lex Mercatoria, normas self regulation, normas internacionales, normas regionales, normas nacionales, seguridad, privacidad, Ley 527 de 1999.

ABSTRACT. This paper gives a brief presentation of the existence of a plurality of rules -of different origin-, which converge in the regulation E-commerce, especially in issues such as security and privacy. It also describes how these rules work in Colombia and interact with Act 527 of 1999.

KEY WORDS. Electronic Commerce, New Lex Mercatoria, self regulation norms, international norms, regional norms, national snorms, security, privacy, Act 527 of 1999.

Tipo de Artículo: Reflexión Académica

Introducción

Si bien el comercio electrónico no es un contrato en sí mismo, sino un factor esencial para la existencia e interacción de la Nueva Lex Mercatoria en el contexto global. Éste se ha constituido en el segundo escenario de realización de contratos, el cual cuenta con unas características propias (KOBRIN S., 2001: 690 ss.) que requieren, a su vez, del diseño de unas normas que se adecuen a su funcionamiento y garanticen, de modo efectivo, no sólo los Derechos de quienes participan en las relaciones contractuales, sino de aquellos que pueden llegar a ser afectados por los contratos celebrados por los agentes del comercio electrónico.

En el presente artículo, avance de investigación del Proyecto "Globalización del Derecho Privado" dirigido por la Universidad Santo Tomás y la Deutsche Gesellschaft für die Internationale Zusammenarbeit (GIZ), se analizará cómo el Comercio Electrónico ha modificado algunas de las normas propias de la Nueva Lex Mercatoria y cómo ésta, mediante el concepto de *self regulation*, ha creado normas tendientes a regular determinados comportamientos de la Business Community. Analizado lo anterior, se cuestionará si en Colombia se puede hablar de la existencia de normas reguladoras del Comercio electrónico y cómo ellas han ingresado en el Ordenamiento Jurídico colombiano, es decir, si han ingresado a través de la actividad de los particulares mediante el ejercicio de su Autonomía de

la Voluntad –*self regulation*- o a través de las formas propias de regulación estatal –legislativo, ejecutivo y judicial-.

Para ello, se hará una breve aproximación al concepto de Comercio Electrónico así como sus características de *internacionalidad* y de *no vectorialidad* (I); partiendo de esta aproximación, se estudiará como el Comercio Electrónico configura un nuevo espacio de relaciones sociales y modifica las normas de las mismas, especialmente contractuales, que constituyen expresiones de la Nueva Lex Mercatoria, como los Principios UNIDROIT y normas CNUDMI (II); posteriormente se analizará la necesidad de regulación del Comercio Electrónico y los actores que participan de ella, así como las formas de hacerlo que, básicamente, pueden resumirse en normas de *self regulation* –expresión de la Nueva Lex Mercatoria-, normas híbridas –*Safe Harbor*-, normas regionales, normas internacionales y normas nacionales –tendientes a ser reproducción de las tres anteriores- (III); finalmente, se describirán las normas que han ingresado en el Estado colombiano y su relación con las otras normas, especialmente con las normas producidas por la CNUDMI (IV).

I. Concepto de Comercio Electrónico

La Red, en la actualidad, es considerada como un nuevo espacio de carácter virtual (KOBRIN, 2001: 688), que amplía las relaciones sociales de distintos tipos –personales, culturales, económicos, entre otros-. Una de las relaciones inmersas en la Red, que ha tenido especial significado en las economías de los distintos Estados, son las relaciones comerciales, las cuales son entendidas como relaciones de *Comercio Electrónico*. Para algunos autores, el *Comercio Electrónico* puede entenderse como el conjunto de actividades comerciales que implican la transmisión de datos informáticos para la celebración de contratos entre personas o para la realización de actividades que estén relacionadas con los mismos –pagos, *downloads*, envío de información, entre otros-[i]. Para otros autores, el *Comercio Electrónico* se entiende como un escenario virtual en el cual se realizan las distintas actividades comerciales, tales como compraventa de bienes y servicios, operaciones bancarias y otras[ii]. La única diferencia existente entre una y otra consiste en el reconocimiento que hace la segunda de un espacio. Mientras que en la primera la definición se centra sólo en las actividades, la segunda no entiende el *Comercio Electrónico* como operaciones, sino como un espacio en el cual ocurren las mismas. Sin importar esta distinción –la cual ha sido desarrollada actualmente por la doctrina-, es necesario agregar que el *Comercio Electrónico* no sólo cubre la esfera de las actividades comerciales propiamente

dichas, sino también aquellas que impliquen la afectación de un Derecho, tal como la Propiedad Intelectual –Derechos de Autor y Propiedad Industrial-.

Este nuevo espacio, a su vez, cuenta con unas caracterísitcas especiales que lo diferencian del espacio físico y, por tanto, de la forma de realización de las actividades comerciales. Dichas características son: a) virtualidad; b) no vectorialidad y; c) internacionalidad. *La virtualidad* (KOBRIN S., 2001: 689 ss.) consiste en la forma de relacionarse los agentes económicos. Mientras que las relaciones comerciales en el espacio físico implica, generalmente, la presencia y el contacto directo entre los agentes económicos –bien sea persona a persona o persona a intermediario-, el *Comercio Electrónico* implica una relación virtual, es decir, los contactos se realizan mediante el intercambio de E-Mails, aceptación de términos y condiciones en una Website –como es el caso de los *Clickwraps* y los *Browserswraps*-, los cuales no implican un contacto directo o personal real.

La no vectorialidad (KOBRIN S., 2001: 691 ss.) se entiende como la imposibilidad de indentificación geográfica y temporal de una relación comercial. Mientras que en el espacio físico las relaciones comerciales pueden identificarse en un punto geográfico y en un momento concreto –por ello es posible "ubicarlas en un mapa"-, el *Comercio Electrónico* no pueden identificarse de igual forma. Por ejemplo, mientras que Yahoo puede tener su domicilio principal en Estados Unidos, la prestación de sus servicios se realizan en cualquier lugar donde exista posibilidad

de acceso a su Website. Asimismo, un ciudadano, cuyo Domicilio es Colombia, puede estar en el Aeropuerto de Zürich, de paso, y comprar un E-Libro ofrecido por Yahoo-España. A diferencia de la compraventa en el espacio físico, en este caso no es fácil determinar cuál es la ubicación geográfica concreta de realización del contrato, pues en él, no hay una entrega física del libro –que es simplemente descargado-, y confluyen distintas ubicaciones geográficas en una sóla operación virtual.

De la *virtualidad* y la *no vectorialidad* se deriva la tercera característica del *Comercio Electrónico*, la *internacionalidad* (KOBRIN S., 2001: 696 ss.). Si las relaciones comerciales realizadas al interior del *Comercio Electrónico* se caracterizan por no ser de contacto directo y por no contar con una unidad geográfica concreta donde puedan ser ubicados los agentes de las relaciones comerciales, debido a la localización de cada uno de ellos, se puede decir que las relaciones comerciales realizadas en el espacio virtual son de carácter internacional. Ello quiere decir que no es posible afirmar que la compra de un E-Libro se realizó en Zürich y, por tanto, las reglas de Derecho serían las de Suiza, sino que se está frente a una relación internacional.

Estas tres características han llevado a cuestionarse sobre las normas que deben regir las relaciones realizadas en el *Comercio Electrónico* y quiénes deberían ser los encargados de la producción de dichas normas. Un primera respuesta podría

buscarse en el Derecho Internacional Privado. Sin embargo, este no es compatible en ninguno de sus aspectos con el *Comercio Electrónico*, especialmente por dos razones: a) el Derecho Internacional Privado es un Derecho que se fundamenta, para la resolución de conflicto de leyes, en criterios geográficos puntuales (UMAÑA CH., 2006: 54), tales como el lugar de celebración del contrato y lugar de ejecución del mismo, criterios que en el *Comercio Electrónico* son difíciles de establecer (KOBRIN S., 2001: 694; REMÓN J., 2002: 70) y; b) las normas de Derecho Internacional Privado son, por tendencia, leyes nacionales diseñadas con criterios internos y, por tanto, no son normas de aplicación universal o uniforme, lo que implicaría conflictos en la regulación de las relaciones comerciales mayores que los conflictos propios de las relaciones en el espacio físico (MUÑOZ J., 2009: 167).

Una segunda alternativa se propone desde la *self regulation* (FARREL H., 2003: 288; KOBRIN S., 2001: 697 s.; LÓPEZ F., 2010: 127 s.). Esta alternativa propone una producción normativa a cargo de los agentes que intervienen directamente en el *Comercio Electrónico*, es decir, a cargo de los comerciantes o miembros de la *Business Community* que son quienes, en ejercicio de sus actividades, celebran habitualmente contratos y, por tanto, han diseñado –bien sea mediante costumbres u otras formas- ciertas normas de conducta que se ajustan no sólo al *Comercio Electrónico*, sino a los constantes cambios de las tecnologías de la información. Sin embargo, dejar la regulación del *Comercio Electrónico* en manos

de los particulares se ha considerado, especialmente en aquellos países con la fórmula de Estado Social de Derecho, como no conveniente, teniendo en cuenta tres argumentos: a) la probabilidad de diseñar normas que lleguen a restringir el ingreso o participación en el *Comercio Electrónico* a quienes, así sean comerciantes o consumidores, no conozcan o dominen criterios altamente técnicos o no gocen de ciertas condiciones económicas (GARCÍA B., 2009: 80 ss.) ; b) los particulares regularían, básicamente, relaciones que estén directamente vinculadas con la actividad contractual, pero no existiría certeza respecto a la regulación situaciones que impliquen la protección de Derechos tales como la dignidad e integridad física y derechos de Propiedad Intelectual, como es el caso de la comercialización de pornografía infantil y las Website de intercambio de música, videos u otros, y; c) el nivel de protección que los particulares le puedan dar a elementos como la seguridad y la privacidad, reflejadas en el flujo de datos personales en la celebración de contratos.

Pese a estos problemas, la *self regulation*, como alternativa de producción normativa no es descartable, si se entiende sólo como una parte del conjunto normativo que debe existir para la regulación de las relaciones al interior del *Comercio Electrónico*. Las normas de *self regulation* se complementan, en atención a los problemas planteados, con normas de carácter institucional (FARREL H., 2003: 278 ss.; KOBRIN S., 2001: 698). Sin embargo, en atención al carácter de internacionalidad del *Comercio Electrónico*, surge el inconveniente del

definir el “cuándo” yel “cómo” debe intervenir el Estado. Si bien el Estado tiene como una de sus funciones la intervención en las relaciones económicas en atención a los Derechos Fundamentales y protección del Orden Público Económico, la regulación aislada implicaría varias complicaciones para un funcionamiento normal del *Comercio Electrónico*.

Para evitar dichos problemas, la tendencia de regulación se ha dejado, en parte, a Organizaciones Internacionales como la Organización para la Cooperación y el Desarrollo Económicos (en adelante OCDE) y en la cesión de competencias a Organizaciones Supranacionales como la Unión Europea (en adelante UE) y la Comunidad Andina de Naciones (en adelante CAN). Tanto las unas como las otras profieren normas de carácter armonizador que buscan un trato igual de las relaciones comerciales. La diferencia entre unas y otras se encuentra en su ámbito territorial de aplicación y en la naturaleza de sus normas. Emitidas las normas por cada una de las Organizaciones Internacionales y Supranacionales, el Estado cumple una función de incorporación y ajuste de las mismas en el contexto nacional, logrando así una producción armónica de normas en materia de *Comercio Electrónico*.

Previo a la presentación de las normas que han sido adoptadas a fin de regular las relaciones del *Comercio Electrónico*, se analizará cómo el mismo ha llevado la modificación de normas de la Nueva Lex Mercatoria, así como de los Principios

UNIDROIT y la formulación de guías legislativas, como la Guía Legislativa de Comercio Electrónico de la CNUDMI.

II. El *comercio electrónico* y las reformas normativas de Nueva Lex Mercatoria

El *Comercio Electrónico* no es un fenómeno reciente. Él existía desde antes de la década de los 90's. La diferencia central radica en su forma de funcionamiendo. Antes de y llegados a los 90's, el *Comercio Electrónico* funcionaba de forma cerrada y contaba con la participación de pocos agentes. Ejemplo de ello es la *Society for Worldwide Interbank Financial Telecommunication* -en adelante SWIFT- (REMOLINA N., 2005: 333), la cual nació en 1973 en Bruselas –Bélgica- como una sociedad encargada de permitir la comunicación entre entidades financieras de distintos países, permitir el procesamiento de datos compartidos y el uso de un lenguaje común entre las mismas entidades.

La figura de sistma cerrado se fue complementando con el sistema abierto de *Comercio Electrónico*, mediante el acceso público a las distitntas tecnologías de la información, especialmente INTERNET (REMOLINA N., 2005: 333), el cual ha venido tomando fuerza desde la segunda mitad de los 90's. Previo a la entrada de INTERNET como sistema abierto del *Comercio Electrónico*, en el ámbito de la

contratación internacional se habían proferido dos instrumentos –considerados de Nueva Lex Mercatoria- relativos a la compraventa internacional de mercaderías y a la contratación internacional. El primer instrumento es la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías –firmado en Viena en 1980 y en vigor desde 1988- (en adelante CCIM) y el segudo son los Principios UNIDROIT de Contratos Internacionales Comerciales –primera versión 1994-. La CCIM corresponde a un conjunto normativo proferido por la CNUDMI[iii] y se encarga de regular las relaciones de compraventa internacional de mercaderías entre comerciantes. Los Principios UNIDROIT son un instrumento creado por el Instituto Internacional para la Unificación del Derecho Privado –con sede en Roma-, sin embargo, su ámbito material no se restringe solamente a la Compraventa Internacional de Mercaderías sino a la Contratación Internacional en General.

Tanto la CCIM como los Principios UNIDROIT no preveían en su articulado las relaciones contractuales desarrolladas al interior del *Comercio Electrónico,* ni se cuestionan sobre el papel que juega la protección de la seguridad y de la privacidad en dicho ámbito. En la CCIM su art. 13 sólo amplía la expresión "por escrito" a la utilización de medios tales como el telegrama y el télex. En los Principios UNIDROIT de 1994, no hay una mención expresa de operaciones de *Comercio Electrónico*. Sin embargo, de la interpretación del art. 6.1.7 (modalidades pago), se puede comprender, como lo ha hecho la comisión

redactora de los Principios (UNIDROIT, 1994: 124), la posibilidad de realizar el pago de las obligaciones mediante el uso de medios electrónicos, tales como transferencia bancaria, uso de tarjetas de crédito, entre otros. Asimismo, del art. 1.9 de los Principios UNIDROIT puede entenderse que la manifestación de la intención de contratar se puede realizar a través de cualquier medio idóneo, incluyendo el teléfono, el telegrama, el fax y télex (UNIDROIT, 1994: 23). Peso a ello, ninguno de los dos instrumentos consagraban regulaciones sobre relaciones que pudiesen surgir del *Comercio Electrónico* como tal, especialmente en las relaciones surgidas a través de Websites o E-Mails. Por tanto, la cuestión para cada uno de los instrumentos era, básicamente, cómo adecuarse a las nuevas operaciones realizadas en el nuevo espacio virtual.

La respuesta a esta cuestión se encontró por vías distitnas. Mientras que la CNUDMI se encargó del diseño de una Ley Modelo de 1996, que se encargase directamente de las distintas materias del *Comercio Electrónico*, UNIDROIT se orientó hacía una reforma de los Principios de la Contratación Internacional, finalizada en el 2004.

Finalizada la elaboración de la CCIM y en espera de su entrada en vigencia, la CNUDMI inició en 1984 –en Viena- el estudio de las posibles influencias de las tecnologías de la información en la contratación internacional (GUTÍERREZ M., 2005, 6). Luego de doce años de estudio y de la realización de 30 sesiones de

trabajos –las últimas tuvieron lugar en Nueva York-, la CNUDMI publicó la Ley Modelo de Comercio Electrócnico, la cual tuvo como objetivos: a) servir como texto normativo ejemplar para los Estados, que permitiese la evaluación y modernización de algunos aspectos de su normatividad legal y la realización de prácticas contractuales, llevadas a cabo mediante la utilización de la informática y de otras técnicas de comunicación modernas (NACIONES UNIDAS, 1996: 68); b) proponer la eliminación progresiva de la obligatoriedad legal del papel y de la firma escrita (NACIONES UNIDAS, 1996: 71); c) ofrecer unos principios aplicables a la contratación internacional realizada por medios electrónicos (NACIONES UNIDAS, 1996: 72) y; d) armonizar las reglas básicas de intercambio electrónico de datos (NACIONES UNIDAS, 1996: 72 ss.). Lo interesante de la Ley Modelo de la CNUDMI consiste en que ella no adopta o asume ningún sistema informático ni programa para la realización de datos, sino, por el contrario, centra su ámbito de aplicación a un elemento básico y común a toda forma de comunicación en Red: el mensaje de datos. De esta forma, la Ley Modelo permite que los agentes comerciales utilicen cualquier medio electrónico que consideren idóneo para la ejecución de actividades pre –ofertas e invitatio ad oferendum- y contractuales. Asimismo, este ámbito de aplicación material permite que la Ley Modelo sea *flexible* y no tenga problemas de vigencia frente a nuevos avances tecnológicos. Sin embargo, la Ley Modelo CNUDMI no trata, de manera rigurosa algunos temas que son de especial interés en las tendencias regulatorias actuales, como son la seguridad y la privacidad en el flujo de información o de datos. Sólo el art. 7 Núm.

1 de la Ley Modelo CNUDMI establece un criterio sobre la certeza de la identidad de quien transmite un mensaje de datos. De acuerdo al art. 7. Núm. 1, se entederá que existe firma, cuando sea utilizado un método que; a) permita identificar a la persona y que la misma aprueba la información contenida en el mensaje de datos y; b) sea confiable.

La UNIDROIT, por su parte, estableció en 1994 que era necesaria la existencia de un monitoreo constante al funcionamiento de los Principios publicados en el mismo año. En 1997, se formó un grupo de trabajo a fin de revisar y diseñar la segunda edición de los Principios UNIDROIT (UNIDROIT, 2004, vii). En los trabajos preparatorios, se tuvo en cuenta los avances tecnológicos y las nuevas formas de contratación a través de medios informáticos propios del *Comercio Electrónico* (SIQUEIROS J., 2005: 131). Sin embargo, la reforma a los principios UNIDROIT no trae consigo la inclusión expresa de un Capítulo exclusivo sobre *Comercio Electrónico*[iv]. Agunos artículos, en cambio, fueron redactados de forma tal, que fuese posible entender que se adaptan a las circunstancias del *Comercio Electrónico*. El art. 1.2 (libertad de forma) expresa que la celebración del contrato puede ser probada a través de cualquier medio, permitiendo así el uso de E-Mails y comunicaciones vía Internet como medios probatorios idóneos para demostrar la existencia del contrato (UNIDROIT, 2004: 9). Igualmente, el art. 1.10 (1) de los Principios UNIDROIT 2004, permite que la notifiación, en caso de ser necesaria, se realice a través de cualquier medio idóneo, en el cual se encuentran

comprendidos los medios electrónicos (UNIDROIT, 2004: 29). El art. 2.1.1 establece que el contrato se perfecciona mediante la aceptación de la oferta o por la conducta de las partes que sea suficiente para manifestar un acuerdo. La redacción de este artículo es lo suficientemente amplia para comprender acciones propias del comercio electrónico, como el envío de E-Mails manifestando la aceptación, los *Clickwraps* o los sistemas automatizados (UNIDROIT, 2004: 36). En el art. 2.1.7, que regula el plazo de aceptación de la oferta, se consagra que las ofertas realizadas verbalmente deben ser aceptadas inmediatamente, a menos que de las circunstancias se determine otro plazo. Lo interesante, es que para UNIDROIT "oferta verbal" debe entender no en un sentido estricto –comunicación mediante voz-, sino como toda oferta realizada a través de comunicaciones de respuesta inmediata (UNIDROIT, 2004: 48). De esta forma, es posible aplicar en estos casos, el concepto de ofertas a las realizadas a través de *chat rooms* (UNIDROIT, 2004: 48), sistemas de comunicación como *skype*, *ichat* o *messenger*. Aunque estas normas incorporan algunas modificaciones para la celebración de contratos vía *Comercio Electrónico*, aquellas no incorporan reglas en materias como la seguridad y la privacidad.

Debe preguntarse, por tanto, quiénes son los encargados de proferir normas que regulen los criterios de seguridad y privacidad en el *Comercio Electrónico*. Si bien dos instrumentos de la Nueva Lex Mercatoria no consagran normas que regulen dichos criterios, no quiere decir que la misma no tenga normas que establezcan

reglas sobre la materia. La expresión de Nueva Lex Mercatoria se ve, para el caso de la seguridad y privacidad, manifestada en otro tipo de instrumentos, como lo son los códigos de ética o de conducta emitidos por agentes particulares, quienes trabajan habitualmente en el espacio virtual y conocen los problemas y riesgos que, en materia de seguridad y privacidad, pueden surgir. Estas códigos de conducta, a su vez, se ven complementados por normas de carácter internacional, regional y nacional que buscan un funcionamiento adecuado del *Comercio Electrónico*, no sólo desde la seguridad y la privacidad, sino también desde los temas de acceso a la Red. Estas normas serán presentadas en el siguiente punto (III).

III. Normas de protección de seguridad y privacidad en el comercio electrónico

Si bien los Principios UNIDROIT y la Ley Modelo CNUDMI de *Comercio Electrónico* incorporan reglas en las relaciones contractuales aplicadas al espacio virtual, ellas no regulan algunos temas que, pese a no ser objeto esencial del contrato, están vinculados a él y son, en la actualidad, de gran importancia. Estos temas son precisamente los de la seguridad y la privacidad. La seguridad implica, entre otros, que el uso de medios de pago, como las transacciones bancarias o uso de tarjetas, no corran el riesgo de ser observadas y manipuladas por terceros,

por ejemplo, mediante clonación de tarjeta o suplantación –*physing*-. La privacidad implica que los datos ofrecidos a la otra parte contratante sólo serán manejados por la misma, no pudiendo transferirlos a terceros o utilizados para otros asuntos que no sean el contrato mismo. Estos elementos no representaban mayor complicación en el *Comercio Electrónico* cuando funcionaba bajo la modalidad de sistema cerrado, pues todos los agentes se conocían y existía una certeza de quién manejaba la información y bajo cuáles condiciones. Con la entrada del sistema abierto de *Comercio Electrónico*la seguridad y la privacidad toman mayor fuerza, así como la discusión de quiénes y cómo debe regularse el funcionamiento de la Red a propósito los derechos. Asimismo, ha surgido una nueva discusión –no muy antigua- sobre la protección de otro elemento que, pese no estar directamente relacionado con el contrato mismo, si afecta un Derecho que antes era considerado de naturaleza privada y en la actualidad es entendido como un Derecho Fundamental. Dicho Derecho es la Propiedad Intelectual (ORDOÑEZ J., 2002: 31 ss.; GAMBOA R., 2005: 2).

La regulación protectora de estos derechos se ha desarrollado a través de distintas propuestas. Una primera propuesta, proveniente del sistema Estadounidense, establece, básicamente, que son los agentes del *Comercio Electrónico*, quienes deben establecer las reglas de protección de la seguridad, la privacidad y la Propiedad Intelectual. Dicha propuesta es conocida como *self regulation*. Sin embargo, esta propuesta ha sido sólo parcialmente aceptada, pues,

en consideración de otros Estados y de Organizaciones Internacionales, el *Comercio Electrónico* y sus distintos elementos no pueden ser objeto de regulación sólo parte de los particuales, sino que es necesaria una acción conjunta entre ellos y las instituciones públicas. La actuación de instituciones públicas, de carácter estatal, debe estar a su vez armonizada en el contexto internacional, a fin de evitar problemas como el de la jurisdicción aplicable y la disparidad normativa –derecho aplicable-. Estas dos propuestas –*self-regulation* e institución pública-, se manifiestan a través de cinco tipos de normas, cada una con características especiales: a) normas de *self regulation* o de agentes particulares, expresadas en códigos de conductas y protocolos de seguridad; b) normas de carácter internacional, proferidas por instutciones como la OCDE; c) normas de carácter regional proferidas por instituciones supranacionales, como la UE; d) normas híbridas, que se caracterizan por la formulación de normas marco, diseñadas por instituciones públicas y reglamentadas o ejecutadas por particulares y; e) normas estatales que generalmente son una incorporación de normas internacionales y regionales, o consisten en la incorporación de normas como los Principios UNIDROIT o las Leyes Modelo. En este punto sólo se tratarán los cuatro pimeros tipos de normas, mientras que el quinto será presentado en el siguiente punto (IV) a través del caso colombiano.

A. Normas *self regulation*

La primera forma de regulación del *Comercio Electrónico* de la seguridad y privacidad, se encuentra en normas diseñadas por los agentes del mercado, quienes participan directamente en el espacio virtual, denominadas *self regulation*. Los fundamentos de la *self-regulation* se centran en el conocimiento técnico de la Red y en la confianza de la autorregulación. Por una parte, la realización habitual de los contratos, bien sea de bienes o de servicios así como el conocimiento de los aspectos técnicos de los sistemas, permiten a los particulares conocer los posbiles riesgos en el flujo de información y, por tanto, determinar las medidas convenientes para evitar problemas como los *hackers*, envío indebido de información confidencial o personal a terceros, entre otros. Por otra parte, la formulación de normas por los mismos agentes, implica la existencia de una conciencia de la necesidad de confiar en el *Comercio Electrónico* y en los medios electrónicos que buscan las empresas y consumidores en el mismo. Dicha conciencia no sólo lleva a una formulación de normas, sino a un seguimiento estricto de las misas (LÓPEZ D. et al., 2010: 129).

Las normas de *self regulation* se manifiestan, generalmente, de dos formas: a) protocolos de seguridad y; b) códigos de conducta o de ética. Los protocolos de seguridad son normas diseñadas por algunas compañías dedicadas a la seguridad informática, las cuales se caracterizan por el estabelcimiento de parámetros

técnicos que permiten un uso adecuado de las redes y de los datos que en ellas circulan. Ejemplo de estos protocolos son *Common Name Resolution Protocol* (IETF, 2002), del Internet Engineering Task Force (FARREL, 2003: 288 ss.), el cual ofrece criterios sobre la utilización de nombres comunes –common names- para la identifiación de compañías, entidades y otros en la Web. Otro ejemplo es el Protocolo de seguridad Secure Socket Layer, de VeriSign –adjunto a la compañía Symantec- y cuyo objeto es brindar la realización de transacciones y comunicaciones de forma segura, mediante la utilización de servicios de cifrado y autenticación de *Websites*.

Los Códigos de Conducta o Ética, por su parte, son normas creadas bien sea por las empresas, o bien por terceros contratados por las mismas, que no consagran parámetros técnicos en sí, sino que establecen normas de conducta de los particulares en cuanto al manejo de datos, fortalecimiento de la confianza, entre otros. Los Códigos de Conducta o de Ética se entienden como el conjunto de buenas prácticas en materia pre-contractual, contractual y post-contractual, teniendo en cuenta los intereses de las personas que contratan con cada compañía, como consumidores, clientes comerciales u otros (LÓPEZ D. et al., 2010: 128). En el ámbito del *Comercio Electrónico*, los Códigos de Conducta o de Ética contienen, además, buenas prácticas en materia de publicidad interactiva, protección a menores de edad y protección de la privacidad y la seguridad (LÓPEZ D. et al., 2010: 128) de los clientes que contratan bienes o servicios con

las compañías creadoras de los Códigos de Conducta o Ética. Sin embargo, es necesario tener en cuenta que la finalidad misma de los Códigos de Conducta o Ética no son los consumidores o clientes en sí mismos, sino el mantenimiento y promoción de la *rentabilidad* (CASTAÑO C., 2003: 6 s.). Si se establecen Códigos de Conducta o Ética, se está informado a la competencia las reglas que rigen el comportamiento de un agente en el mercado y se da garantía de evitar un cambio repentino de las mismas (LÓPEZ D. et al., 2010: 128). Al mismo tiempo, se le informa a los clientes y consumidores cuáles serán los términos y condiciones que regirán el contrato, así como los mecanismos de reclamación en caso del no cumplimiento de dichos términos (LÓPEZ D. et al., 2010: 128). La publicidad de estas normas crea en los clientes en general una sensación de confianza en las compañías y, consecuentemente, un cierto grado de fidelidad hacia las mismas. Esta fidelidad permite que las compañías puedan contar con una realización segura de contratos a través del *Comercio Electrónico.*

B. Normas Internacionales

Las normas de *self-regulation* han sido consideradas por la doctrina y por la práctica como normas insuficientes en la regulación del *Comercio Electrónico*. Es necesario que dichas normas sean complementadas con normas de origen institucional, tendientes a garantizar derechos o libertades fundamentales. Pero,

es necesario tener presente que las normas institucionales no deben ser de carácter exclusivamente nacional, pues podrían surgir problemas de disparidad normativa y de jurisdicción competente. Por ello, es necesario que las normas sean de carácter internacional, es decir, que sean expedidas por instituciones internacionales que busquen la armonización o unificación de criterios. En relación con el *Comercio Electrónico*, las normas internacionales producidas hasta el momento pueden agruparse en dos grandes categorías: a) normas netamente internacionales y; b) normas híbridas.

Las normas netamente internacionales son aquellas que han sido creadas mediante tratados internacionales o a través de instituciones internacionales creadas por los mismos, en ejercicio de sus funciones, y se caracterizan por ser normas dirigidas a los Estados[v], a fin de establecer condiciones adecuadas para el funcionamiento del *Comercio Electrónico*. Ejemplo de estas normas son las proferidas por la ONU y por la OCDE. Las normas proferidas por la ONU son, básicamente, tres, de las cuales dos son de carácter general, es decir, no aplicables exlusivamente al *Comercio Electrónico*, y una de carácter concreto. Las normas de carácter general son el art. 12 de la Declaración Universal de Derechos Humanos, que consagra la prohibición de intervención arbitraria en la privacidad de las personas, y el art. 17 de la Convención de Derechos Civiles y Políticos, que establece el Derecho a no ser sujeto de intervención arbitraria en su privacidad, determinando que las personas gozan del Derecho a una protección legal frente a

dichas actuaciones. Con respecto al *Comercio Electrónico*, la ONU produjo la Guía sobre Archivos Digitalizados de Datos Personales de 1990. Esta guía está compuesta de dos apartados. En el primero, la ONU consagra los diez principios que deben orientar las políticas de regulación nacional de Datos Personales, mientras que en el segundo presenta, de modo general, la forma en que dichos principios deben ser aplicados.

La OCDE, por su parte, emitió en 1980, la Guía sobre Protección de la Privacidad y del Flujo Transfronterizo de Datos Personales, compuesto por cuatro partes. La Primera parte se orienta a definir los conceptos que orientan la Guía, es decir, "Controlador de Datos" –Data Controller-, "Datos Personales" –Personal Data- y "Flujo Transfronterizo de Datos" –Transborder Flows of Personal Data-. La segunda parte establece los ocho principios que deben orientar la actividad estatal en materia de regulación del flujo transfronterizo de datos personales. La tercera parte consagra los principios que rigen las relaciones entre los Estados miembros de la OCDE en cuanto al flujo transfronterizo de datos personales. La cuarta parte determina la forma de implementación nacional de los principios contenidos en las partes dos y tres, haciendo especial énfasis en los procedimientos legislativos y administrativos.

Las normas híbridas, a diferencia de las normas netamente internacionales, cuentan con una participación activa de los particualres, especialmente en la

ejecución de las políticas diseñadas o previstas en los instrumentos internacionales (FARRELL H., 2003: 278 ss.). Básicamente, las normas híbridas pueden entenderse como un acuerdo bi- o multilateral –varios Estados-, donde se establecen principios orientadores de las actividades en el *Comercio Electrónico*, pero su aplicación no se deja exclusivamente a los Estados miembros a través de sus órganos gubernamentales, sino que se permite que los particulares, a través de sus diversas formas de actuación, ejecuten y hagan efectivos dichos principios (FARRELL H., 2003: 287 ss.). Un ejemplo es el *Safe Harbor*, compuesto, en términos de FARRELL (2003: 287), de tres partes: a) los principios básicos; b) las preguntas frecuentes –Frequently Asked Questions FAQs- sobe la incorporación y aplicación de los principios y; c) los mecanismos de exigibilidad o coerción –enforcement mechanisms-, dimesnionados desde la actividad estatal y la actividad de autoregulación –cimentada en los Mecanismos Alternativos de Resolución de Conflictos o *Alternativ Disputs Resolution*, ADR-. Lo interesante del *Safe Harbor* como norma híbrida, es que representa el encuentro entre dos concepciones distintas en cuanto al papel regulador del Estado en las actividades del mercado[vi]. Por una parte, el modelo Estadounidense tiende a un mero establecimiento de las directrices generales del comportamiento de los agentes del mercado, especialmente del *Comercio Electrónico* a traves del *Framework for Global Electronic Commerce* de 1997, y permite un margen de acción alto a los particulares (FARRELL H., 2003: 288). La Unión Europa, por otra parte, basada en el Concepto de Estado Social de Derecho característico de sus Estados

Miembros, aboga por una intervención directa del Estado, no sólo en el establecimiento de directrices generales, sino en la formulación de normas concretas y de mecanismos de protección efectivos, los cuales están a cargo tanto de los Estados miembros como del mismo Bloque Regional (FARRELL H., 2003: 289).

Dicha diferencia produjo en la Unión Europea una especial preocupación sobre el flujo de datos personales en Estados Unidos, pues, en cosideración de aquella, éste no contaba con las garantías necesarias para la protección de datos personales y exigía a los Estados Unidos que cambiase su política legislativa para que, inspirada en guías como la de la OCDE, existiese un papel más activo en la protección de datos personales (FARRELL H., 2003: 291). Por su parte, Estados Unidos, en el período de negociaciones, buscó demostrar que, como Estado, contaba con las herramientas necesarias para ser considerado como seguro en el flujo de datos personales y buscó convencer que la participación de particulares en la regulación del *Comercio Electrónico* era idónea. Es por ello que el *Safe Harbor*, como producto final, permite que los particulares, bajo la dirección del Estado, pueda participar en la construcción y ejecución de normas reguladoras de *Comercio Electrónico.*

C. Normas Regionales

A diferencia de las normas internacionales, las normas regionales tienen como destinatarios los Estados miembros de un Bloque Regional. Asimismo, otra diferencia entre las normas internacionales y regionales se encuentra en el Derecho aplicable. Mientras en las normas internacionales se aplican las reglas del Derecho Internacional Público, las normas regionales se rigen por las normas de Derecho Comunitario, fundamentado, entre otros, en el principio de Cesión de Competencias.

Salvo estas diferencias, la función básica de las normas regionales es la misma que la función de las normas internacionales. Aquellas buscan la armonización de criterios estatales en la regulación del *Comercio Electrónico*. Un ejemplo de normas regionales se encuentra en la Unión Europea.

Como Bloque Regional, la Unión Europea ha proferido directivas que se han encaminado a regular algunos aspectos puntuales sobre el *Comercio Electrónico*, tales como protección al consumidor europeo en contratos a distancia –Directiva 97/7/CE-, procedimiento de información en materia de normas y reglamentaciones técnicas –Directiva 98/34/CE-, firma electrónica –Directiva 1999/93/CE-, acceso a la actividad de las entidades de dinero electrónico y su ejercicio –Directiva 2000/46/CE-, entre otras. Sin embargo, en el 2000, la Unión Europea profirió una

Directriva sobre determinados aspectos jurídicos de la sociedad de la información en particular sobre el *Comercio Electrónico* en el mercado interior, Directiva 2000/31/CE. La Directiva 2000/31/CE, además de buscar la armonización de las legilasciones de los Estados Miembros, cuenta con algunas características especiales, entre ellas: a) limitación del ámbito de aplicación de la Directiva, a fin de garantizar una armonización global a través de las normas internacionales; b) reconocimiento y protección de la contratación electrónica; c) promoción a la participación de los particulares a través del apoyo en el diseño de Códigos de Conducta o Ética.

De acuerdo a la Directiva 2000/31/CE, las disposiciones establecidas por la Unión Europea sólo tendrán un ámbito de aplicación restringido. Si bien uno de los objetivos esenciales son la promoción y fortalecimiento de un mercado interior así como garantizar el libre flujo de bienes y servicios en el mismo, las normas contenidas en la Directiva no se aplicarán en las relaciones internacionales, pues la Unión Europea es consciente de la dimensión global del *Comercio Electrónico* y, por tanto, de la necesidad de una coherencia entre las normas regionales y las internacionales. Ello implica, entonces, que las reglas contenidas en la Directiva 2000/31/CE se entenderán sin perjuicio de los resultados obtenidos en las discusiones jurídicas de las distitnas organizaciones internacionales, tales como la Organización Mundial de Comercio –OMC-, la OCDE y la CNUDMI.

El reconocimiento y protección de la contratación electrónica se encuentra consagrado en el art. 9 de la Directiva 2000/31/EC. En ésta, la Unión Europea establece como obligación a los Estados miembros del Bloque Regional garantizar el reconocimiento en los Ordenamientos Jurídicos de cada uno de ellos, la alternativa de la celebración de contratos por vía electrónica. Asimismo, el art. 9 de la Directiva 2000/31/EC establece la prohibición a los Estados miembros, de crear normas que entorpezcan la utilización de contratos por vía electrónica.

Por último, el art. 16 núm. 1º lit. a) de la Directiva 2000/31/EC establece como obligación para la Unión Europea –a través de la Comisión- y para los Estados miembros, el fomentar la elaboración de Códigos de Conducta a nivel comunitario a través de asociaciones y organizaciones comerciales, a fin de dar cumplimiento efectivo a las reglas establecidas en la Directiva. Sin embargo, ésta no sólo faculta a los comerciantes para la elaboración de Códigos de Conducta, sino que en el mismo art. 16 núm. 1º lit. a) faculta a las asociaciones u organizaciones de consumidores elaborar Códigos de Conducta para la correcta aplicación de la Directiva 2000/31/CE. Con esta norma se complementa el ámbito de aplicación de la Directiva 2000/31/EC, pues no sólo hay un reconocimiento limitado de la aplicación territorial de la misma, a fin de reconocer la aplicación de normas internacionales, sino que, a su vez, permite la participación de normas *self-regulation*, construyendo así un espacio de convergencia normativa, que garantiza una regulación armónica del funcionamiento del *Comercio Electrónico*, al combinar

los conocimientos propios de los agentes que participan en el mismo –*self regulation*-, la protección de intereses estatales y regionales –*normas regionales*- y las tendencias armonizadoras de las organizaciones internacionales –*normas internacionales netas e híbridas*-.

IV. Recepción de normas de comercio electrónico en Colombia

En Colombia existen dos formas de incorporación normativa. Por un lado, en virtud de la Autonomía Privada de la Voluntad –material y conflictual- y de la Costumbre Mercantil –nacional e internacional-, las normas de *Comercio Electrónico* pueden ingresar a través de la práctica habitual de los comerciantes o *Business Community* mediante la elaboración de Códigos de Conducta o Ética, establecimiento de cláusulas compromisorias o a través de Costumbres. Por otro lado, el Estado puede también, incorporar normas de *Comercio Electrónico* a través de los procedimientos Legislativo –promulgación de Leyes-, Administrativo –Decretos Reglamentarios, Resoluciones y Circulares- y Judicial –utilización de Fuentes de Derecho en la resolución de conflictos judiciales-. Asimismo, es necesario tener en cuenta que Colombia hace parte de Procesos de Integración Regional a distintos niveles –Zonas de Libre Comercio, Zonas Aduaneras-, especialmente en la Comunidad Andina de Naciones, cuyas normas derivadas tienen efectos directos e inmediatos sobre el Ordenamiento Jurídico nacional. Por

tanto se describirá cuáles de las normas mencionadas anteriormente se han incorporado y cómo ha sido su incorporación, a partir de la actuación de los particulares y del Estado.

A. Incorporación de normas a través de particulares (*selfregulation)*

Aunque en el ámbito del *Comercio Electrónico* los particulares pueden manifestar la producción de normas de *self-regulation* a través de Costumbres y Cláusulas compromisorias, en este punto se observarán únicamente los Códigos de Conducta o Ética. Asimismo, teniendo en cuenta que existen diversos tipos de empresas –Alimentos, Agricultura, Transporte, otros-, sólo se presentarán cuatro Códigos de Conducta o Ética, relacionados con empresas bancarias y aseguradoras. Los Códigos de Conducta o Ética corresponden a las entidades GRUPO EMPRESARIAL BOLIVAR, BANCOLOMBIA, BBVA y LIBERTY SEGUROS S.A. Aunque estos códigos presentan diferencias considerables en cuanto a su construcción y organización, poseen algunos elementos en común, entre ellos: a) los destinatarios de las normas contenidas en los Códigos son directivos y empleados de cada una de las compañías; b) los temas contenidos en los Códigos de Conducta o Ética se centran, básicamente, en las relaciones empleados-compañía y empleados-cliente; c) todos los Códigos cuentan con un conjunto de principios orientadores y; d) en materia de *Comercio Electrónico*, las

reglas se encaminan a la protección de la seguridad y privacidad de datos personales y al flujo de los mismos.

En cuanto a las diferencias entre cada uno de los Códigos de Conducta o Ética de las compañías mencionadas anteriormente, se puede establecer una doble clasificación, teniendo en cuenta el nivel de estructuración –primer grupo- y el nivel precisión en la formulación de las reglas de comportamiento –segundo grupo-. En el primer grupo –estructuración- los Códigos de Conducta pueden ser clasificados como normas de estructuración sencilla o básica, Códigos de Conducta o Ética de estructuración semicompleja y Códigos de Conducta o Ética de estructuración compleja. Código de Conducta o Ética de estructuración sencilla sería el Código de Ética diseñado por GRUPO EMPRESARIAL BOLIVAR; Código de Conducta o Ética de estructuración semicompleja sería el Código de Conducta del Grupo BBVA y; Códigos de Conducta o Ética de estructuración compleja serían el Código de Ética del Grupo BANCOLOMBIA y el Código de Conducta y Ética del Negocio Internacional del Grupo LIBERTY Mutual. En el Segundo Grupo –precisión en formulación-, los Códigos de Conducta o Ética pueden ser clasificados como Códigos de Conducta o Ética de formulación abierta –formulaciones generales- y Códigos de Conducta o Ética de formulación precisa o detalla. Códigos de Conducta o Ética de Formulación abierta sería el Código de Ética de GRUPO EMPRESARIAL BOLIVAR y el Código de Conducta del Grupo BBVA, mientras que Códigos de Conducta o Ética de formulación precisa o detallada serían el

Código de Ética del Grupo BANCOLOMBIA y el Código de Conducta y Ética del Negocio Internacional del Grupo LIBERTY Mutual.

Clase/Código	**BOLIVAR**	**BANCOLOMBIA**	**BBVA**	**LIBERTY**
ESTRUCTURA				
Sencilla	X			
Semicompleja			X	
Compleja		X		X
PRECISIÓN				
Abierta	X		X	
Detallada		X		X

El Código de Ética del Grupo Empresarial Bolivar es el más sencillo y con una redacción más abierta de los cuatro Códigos de Conducta o Ética. Está compuesto de tres partes: a) Declaración ética de conductas deseables e inaceptables; b) Declración de responsabilidades y compromisos y carta de compromiso. En materia de *Comercio Electrónico,* el apartado de Dlecaración ética consagra una conducta deseable y una conducta indeseable, ésta última encaminada a la protección de información. La conducta deseable No. 10 del apartado apartado Declaración ética, consagra como regla el uso de axclusivo de software con licencias de protección de la Propiedad Intelectual y Derecho de uso y explotación (GRUPO EMPRESARIAL BOLIVAR, 2001: 9). La conducta inaceptable No. 7 del apartado Declaración ética prohibe la divulgación de información (datos) de clientes, intermediarios y proveedores, así como información sobre la infraestructura tecnológica (GRUPO EMPRESARIAL BOLIVAR, 2001: 12). Sin embargo, el Código de ética del Grupo Empresarial Bolivar no establece

definiciones o delimitaciones sobre el concepto información o datos –entre otros- ni tampoco consagra las posibles acciones a las que puede recurrir un cliente o la misma entidad en caso de incumplimiento de alguno de los compromisos o reglas contenido en el Código de ética.

El Código de Conducta del Grupo BBVA cuenta con una estructura más compleja que el Código de Ética del Grupo Empresarial Bolivar, pero su formulación de reglas es similar, es decir, contiene redacciones de tipo amplio y no entra en precisiones o delimitaciones de los conceptos que manejan. Asimismo, el Código de Conducta del Grupo BBVA tampoco cuenta con un apartado que consagre posbiles acciones que puedan usar los clientes o la misma entidad en caso de infracción de las reglas contenidas en el Código de Conducta. El Código de Conducta del BBVA está compuesto de seis apartados: a) ámbito de aplicación (2); b) valores éticos (3); c) integridad relacional (4); d) integridad en los mercados (5); e) integridad personal (6) e; f) integridad organizativa. En el apartado 4 –integridad relacional- y en relación con la regulación del *Comercio Electrónico*, el Código de Conducta del BBVA desarrolla el tema de confidencialidad en tres puntos. El primer punto (4.6) consagra como uno de los elementos esenciales de la confianza del cliente la apropiada salvaguardia de la información así como uso adecuado uso (GRUPO BBVA, 2011: 15). En virtud de este elemento el segundo punto (4.7) el Código de Conducta del Grupo BBVA determina que la información no pública manejada por la entidad goza del carácter de confidencial y por tanto,

se adoptan medidas para garantizar la seguridad informática de los sistemas donde se almacena información contractual y transaccional de sus clientes (4.7.1), así como para dar cumplimiento a las exigencias legales en materia de protección de datos de carácter personal (4.7.2) (GRUPO BBVA, 2011: 15). Por último, el Código de Conducta del Grupo BBVA consagra la responsabilidad de sus empleados en el uso adecuado de la información a la cual tengan acceso (4.8) (GRUPO BBVA, 2011: 15).

A diferencia de los Códigos de Ética y de Conducta del Grupo Empresarial Bolívar y del Grupo BBVA, el Código de Ética del Grupo Bancolombia se caraceriza por tener una estructura más compleja y una delimitación mayor en cuanto a los términos utilizados en el mismo. Igualmente, incluye temas tales como el régimen sancionatorio en caso de incumplimiento de las reglas establecidas en el Código, la conformación de un Comité de Ética y el control y prevención de lavado de activos y de financiación del terrorismo. Este Código está compuesto de siete partes: a) destinatarios del Código de Ética; b) disposiciones generales; c) disposiciones particulares; d) control interno y prevención de actos incorrectos y prevención de lavado de activos y de la financiación del terrorismo; e) régimen sancionatorio; f) comité de ética y; g) canales de información y actuación del comité de ética. En materia de *Comercio Electrónico*, el Código de Ética del Grupo Bancolombia consagra dos reglas en dos apartados distintos. En el apartado de disposiciones particulares establece la obligación, en virtud del concepto

información privilegiada, de realizar operaciones en provecho propio o de un tercero mediante la utilización de información confidencial de clientes y de la compañía, así como de suministrar información a un tercero que éste no tenga derecho a recibir (GRUPO BANCOLOMBIA, 2011: 3). En el apartado de control y prevención de actos incorrectos, el Código de Ética del Grupo Bancolombia consagra un conjunto de actos incorrectos, entre los cuales se encuentra el *abuso tecnológico*. Por abuso tecnológico entiende el acceso no autorizado a sistemas de cómputo, violación de licencias de software, implantación de virus y actos de sabotaje tales como acceso o divulgación no autorizado de datos electrónicos, uso indebido de la red, destrucción y distorción de información clave para el banco, y fraude por computador en todas sus manifestaciones (GRUPO BANCOLOMBIA, 2011: 9).

Por último, el Código de Conducta y Ética del Negocio Internacional del Grupo Liberty Mutual, es el más avanzado. Además de contar con una estructura compleja y formulaciones detalladas –como el Código de Ética del Grupo Bancolombia-, este Código incorpora un apartado especial sobre armonización de las normas creadas por el grupo con las normas legales nacionales e internacionales (GRUPO LIBERTY MUTUAL, 2011: 13 ss.), mediante el establecimiento de la obligación del cumplimiento de leyes nacionales en materia de monopolios, sistemas financieros y otras, así como la prohibición de obstrucción de la justicia. El Código está compuesto de nueve apartados: a)

principios; b) introducción; c) conflicto de interés; d) cómo manejar información; e) prácticas laborales; f) uso indebido de los recursos corporativos; g) cumplimiento con leyes gubernamentales, reglas y regulaciones; h) prevención y control de lavado de activos y financiación del terrorismo; i) divulgación de violaciones del Código de Conducta y Ética del Negocio y preocupaciones en relación con la integridad financiera sin retaliaciones. En materia de *Comercio Electrónico*, el Código de Conducta y Ética del Grupo Liberty Mutual establece dos reglas sobre el manejo de información y manejo de sistemas. Sobre el manejo de información, el apartado cuatro establece la responsabilidades que tiene el empleado o miembro del Grupo Liberty sobre el manejo de la información de la compañía; para ello hace una diferenciación entre información pública, información interna, información confidencial e información restringida, y consagra estándares distintos sobre el manejo de cada una de las modalidades de información (GRUPO LIBERY MUTUAL, 2011: 8 s.). Por otra parte, el mismo apartado cuatro consagra la prohibición de uso de indebido de software y la obligación de uso de programas con licencia (GRUPO LIBERTY MUTUAL, 2011: 10).

B. Incorporación de normas a través del Estado

Si bien puede hablarse de la aplicación de normas de *self regulation* en Colombia a través de la aplicación de Códigos de Conducta o Ética de ciertas compañías, es

necesario tener en cuenta que dicha regulación no es suficiente, sino que se requiere, también, la participación del Estado colombiano. Éste actua básicamente de dos formas: a) a través de la recepción de normas provenientes de Procesos de Integración Regional, como la Comunidad Andina o Tratadas de Libre Comercio o; b) a través de la producción de normas estatales –legislativas, ejecutivas o judiciales- que pueden tener origen en el Estado mismo o en normas internacionales. Estas últimas implicarían una recepción de disposiciones de organizaciones tales como la CNUDMI, la OCDE, la OMC, entre otros.

1. Recepción de normas regionales

El Estado Colombiano ha participado desde 1969, en el Proceso de Integración conocido como Comunidad Andina de Naciones (CAN). A través del Acuerdo de Cartagena, se han cedido competencias a Instituciones Supranacionales como el Consejo Andino de Ministros de Relaciones Exteriores, la Comisión de la Comunidad Andina y la Secretaría General, a fin de proferir normas armonizadoras que cumplan –en materia de *Comercio Electrónico*- metas como una liberación del comercio interregional avanzado –art. 3 inc. 1º lit. d) Acuerdo de Cartagena- y la liberación del comercio intrarregional de servicios –art. 3 inc. 1º lit. h) Acuerdo de Cartagena-, así como ejecutar programas de promoción del desarrollo científico y tecnológico –art. 3 inc. 2º lit. a) Acuerdo de Cartagena-.

Desde su fundación hasta la fecha, la CAN no ha regulado aun el tema de *Comercio Electrónico*. Por el contrario, ha permitido que los Estados, de forma aislada, regulen las distintas relaciones y factores que puedan surgir en el espacio virtual (GUTÍERREZ M., 2008). Esto ha producido que Bolivia, Colombia, Ecuador y Perú regulen el *Comercio Electrónico* a través de leyes nacionales que, pese a estar influidas por la Ley Modelo CNUDMI sobre *Comercio Electrónico*, tratan los diversos aspectos sobre el tema de modo distinto, especialmente en lo que tiene que ver con mensajes de datos, firmas electrónicas y entidades de certificación(GUTÍERREZ, 2008).

Sin embargo, Colombia no participa exclusivamente en la CAN. Desde la Constitución de 1991 hasta hoy, Colombia ha celebrado Tratados de Libre Comercio con distintos países, entre los que conforman Triángulo Centroamericano (CORTE CONSTITUCIONAL, SENTENCIA C-446 de 2009) y con Estados Unidos. En el Tratado de Libre Comercio con los países del Tríangulo Centroamericano –Salvador, Guatemala y Honduras-, el capítulo 14 establece las reglas básicas del funcionamiento del *Comercio Electrónico*. De este capítulo es de resaltar el art. 14.7 del Tratado de Libre Comercio –autenticación y certificados digitales-, el cual establece la prohibición de adopción o mantenimiento de medidas legales sobre autenticación electrónica que impida a las partes un reconocimiento de las transacciones electrónicas en instancias judiciales o administrativas. Por su parte, el Tratado de Libre Comercio con

Estados Unidos, el Capítulo 15 regula aspectos fundamentales del *Comercio Electrónico*. En especial, el art. 15.6 del Tratado de Libre Comercio establece la prohibición de adoptar o mantener disposiciones legales sobre autenticación que prohiba a las partes en una transacción electrónica determinar en forma mutua los métodos apropiados para dicha transacción o impedir a las partes el reconocimiento de las transacciones electrónicas ante instancias judiciales o administrativas.

2. Normas Nacionales

Aunque en el ámbito nacional ya existían algunas normas relacionadas con el *Comercio Electrónico*, especialmente en temas como factura electrónica y el uso de medios electrónicos en conferencias (REMOLINA, 2006: 338 ss.), se puede hablar de una ley concreta sobre el espacio virtual sólo con la entrada en vigor de la ley 527 de 1999, sobre *Comercio Electrónico*, la cual trae consigo, de acuerdo a RINCÓN C. (2007: 384 ss.), la incorporación de elementos de la seguridad en el espacio virtual, tales como el uso de firmas digitales y las entidades de certificación. Esta ley, siguiendo la tendencia de los países suramericanos, no crea un régimen original como tal, sino que adapta la Ley Modelo CNUDMI sobre *Comercio Electrónico* y complementa algunos apartados (GUTÍERREZ M., 2005: 10 ss.; ORDOÑEZ J., 2002: 24 ss.). Dos elementos esenciales de la Ley 527 de 1999, que son asumidos sin modificación alguna de la Ley Modelo CNUDMI , son

los criterios de *internacionalidad* y *neutralidad*. El criterio de internacionalidad (GUTÍERREZ, 2005: 12; REMOLINA 2005: 344 s.), consagrado en el art. 3 inc. 1º de la Ley 527 de 1999, establece que las normas contenidas en la Ley deben ser intepretadas teniendo en cuenta su origen internacional y la necesidad de promover la uniformidad de aplicación. Asimismo, el art. 3 inc. 2º de la Ley 527 de 1999 consagra, en caso de no existir norma en la Ley, que las cuestiones deben resolverse conforme a los principios que orientan la Ley. Aunque la Ley 527 de 1999 no consagra un apartado de principios como tal, si tiene en cuenta que la misma es una adaptación de la Ley Modelo CNUDMI –internacionalidad-, que la finalidad de aquella es la aplicación uniforme y que el artí. 3º de la Ley Modelo CNUDMI es el mismo art. 3 de la Ley 527 de 1999 sin modificación alguna, podría afirmarse que los principios orientadores son aquellos que soportaron la formulación de la Ley Modelo CNUDMI, es decir, son los establecidos por un órgano internacional y no por el Estado mismo. La neutralidad (GUTÍERREZ, 2005: 14; RAVASSA G., 2004: 510; REMOLINA, 2005: 346 s.), consagrada en los arts. 1 y 5 de la Ley 527 de 1999, establece que el Estado colombiano no se inclina por un sistema en particular, sino que, por el contrario, determina como ámbito de aplicación el mensaje de datos –art. 1 Ley 527 de 1999-, soporte de cualquier sistema y reconoce, a su vez, efectos jurídicos al mismo –art. 4 Ley 527 de 1999-, siguiendo así los mismos criterios que la Ley Modelo CNUDMI sobre *Comercio Electrócnico*-.

Sin embargo, una modificación esencial que realiza el Legisador colombiano al adaptar la Ley Modelo CNUDMI sobre *Comercio Electrónico*, es la incorporación de un capítulo no previsto en la misma. Este nuevo capítulo versa sobre las firmas digitales y las entidades de certificación. A fin de garantizar unos estándares de seguridad, la Ley 527 de 1999 sólo permite la utilización de firmas digitales, una modalidad avanzada de firma electrónica, en Colombia[vii]. La firma digital, de acuerdo al art. 2 lit. c) de la Ley 527 de 1999, es entendida como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación. Esta firma, a su vez, conforme al art. 28 par. único de la ley 527 de 1999, cuenta cinco requisitos: a) que la firma sea utilizada únicamente por una persona; b) que sea susceptible de ser verificada; c) estar bajo el control exclusivo de la persona que la usa; d) estar ligada a la información o mensaje, de forma tal que si la información o el mensaje son cambiados, la firma se invalida y; e) estar sujeta a las reglas del Gobierno nacional.

En virtud del art. 28 par. único núm. 5º, el Gobierno nacional mediante Decreto Reglamentario 1747 de 2000, reguló el aspecto de la seguridad en las firmas digitales a través de las entidades de certificación, las cuales, pueden ser de carácter abierto o cerrado. Sin embargo, el art. 15º núm. 1º del Decreto 1747 de

2000, establece que sólo las firmas digitales cuenten con un certificado digital emitido por una entidad de certificación abierta autorizada por la Superintendencia de Industria y Comercio[viii], cumpliendo con los requisitos establecidos en el art. 28 de la Ley 527 de 1999. Ello no significa que las firmas que usen certificados proferidos por entidades de certificación cerrada no tengan efecto jurídico alguno pues, de acuerdo al art. 4º del Decreto 1747 de 2000, los certificados emitidos por entidades de certificación cerrada tendrán efectos *inter partes*.

Jurisprudencialmente, la Ley 527 de 1999, ha sido estudiada tanto por la Corte Constitucional como por la Corte Suprema de Justicia. Los análisis de la Corte Constitucional han tenido como objeto principal determinar la constitucionalidad de algunos apartados de la Ley 527 de 1999, mientras que la jurisprudencia de la Corte Suprema de Justicia, a través de su *obiter dicta*, se ha manifestado de forma tangencial con respecto a algunos aspectos de la misma Ley. La Corte Constitucional ha estudiado, a través de sus Sentencias de Constitucionalidad C-662 de 2000 y C-831 de 2001, la calidad de las entidades de certificación –si son o no equivalentes a los notarios- y el factor de equivalencia funcional de los mensajes de datos. En la Sentencia C-662 de 2000 es necesario resaltar algunos aspectos relacionados sobre el tema de regulación del comercio electrónico, los cuales son retomados por la misma Corte en la Sentencia C-831 de 2001. Para ésta, es claro que el avance de las tecnologías de la información cuestiona la vigencia de los ordenamientos jurídicos nacionales, pues ellos no preveían

aspectos relacionados como la Internet y por tanto, dichos desarrollos han planteado un resto en la actualización de los regímenes jurídicos nacionales e internacionales, a fin de poder responder a las transformaciones y exigencias planteadas por la globalización que han tenido lugar en la organización social, económica y empresarial en el ámbito mundial, regional, nacional, local, social y personal (CORTE CONSTITUCIONAL, Sentencia C- 662 de 2000). En virtud de esta necesidad de actualización normativa, la Corte Constitucional reconoce la labor de la CNUDMI en cuanto al diseño de una Ley Modelo sobre *Comercio Electrónico* pero, a su vez, reconoce que no es el único contexto de la Ley 527 de 1999, sino que también es parte del trabajo de una Comisión Redactora liderada por el Ministerio de Justicia –actualmente del Interior y de Justicia-, con la colaboración los Ministerios de Comercio Exterior, Transporte y Desarrollo y con la participación del sector público y privado (CORTE CONSTITUCIONAL, Sentencia C- 662 de 2000). Por tanto, pese a que la Ley 527 de 1999 tiene su origen en un proyecto de armonización por parte de la CNUDMI, contiene también elementos propios al Estado colombiano.

Por su parte, la Corte Suprema de Justicia, Sala de Casación Civil, ha reconocido el *Comercio Electrónico* como un escenario que acentúa ciertas situaciones así como el papel del mensaje de datos en la contratación moderna. Al estudiar el daño y la exposición del sujeto al mismo como elemento esencial del Contrato de Seguro, la Corte Suprema de Justicia, Sala de Casación Civil, reconoce el

incremento de la posibilidad de daño a través del *riesgo de desarrollo*, entendido como aquel riesgo vinculado a los avances científicos y tecnológicos, las comunicaciones, el uso de la Internet, las bases de datos y el comercio electrónico (CORTE SUPREMA DE JUSTICIA, 2008: 31). En caso de llegar ser efectivo el daño, es decir, de ocurrir un siniestro, la Corte Suprema de Justicia, Sala de Casación Civil, ha reconocido que la prueba de ocurrencia del mismo puede efectuarse a través de distintos medios, en especial de mensajes de datos –ley 527 de 1999 y arts. 95 y ss. de la Ley 270 de 1996-, pues el los arts. 1077 y 1080 del Código de Comercio, permiten acreditar la ocurrencia del siniestro mediante todo medio probatorio lícito, idóneo, conducente, eficaz y con aptitud (CORTE SUPREMA DE JUSTITICA, 2008: 41), permitiendo así el uso de mensajes de datos, reconocidos por el ordenamiento jurídico nacional.

V. Síntesis y algunas cuestiones

El Comercio Electrónico es un escenario virtual que permite la realización de transacciones comerciales. Este escenario, a diferencia de lo que se podría llamar el comercio en espacio físico, cuenta con unas características especiales, a saber, virtualidad, no vectorialidad e internacionalidad. Estas características hacen que las relaciones comerciales en el Comercio Electrónico no se puedan regular con las normas tradicionales del Derecho Internacional Privado, el cual ha sido

diseñando con criterios geográficos determinados. Ello ha implicado, a su vez, que algunas normas de la Nueva Lex Mercatoria, como las leyes modelo de la CNUDMI y los Principios UNIDROIT hayan sufrido algunas modificaciones, a fin de poder ser aptas para su aplicaciones en contrataciones o relaciones comerciales electrónicas.

Por ello, una de las cuestiones ha sido, desde el surgimiento del Comercio Electrónico hasta la actualidad, quiénes deben establecer las normas que regulen las relaciones comerciales en el espacio virtual y bajo cuáles criterios deben ser diseñadas las normas, teniendo en cuenta que no sólo está en juego la celebración y ejecución adecuada de un contrato, sino la protección de ciertos derechos, como la dignidad, la seguridad, la privacidad, entre otros. Una respuesta a la cual se ha llegado es propender por una regulación conjunta que cuente con la participación agentes privados, organizaciones internacionales, bloques regionales y el Estado. Los particulares actúan a través de las normas conocidas como normas de *self regulation* las cuales, si bien no cuentan con un mismo nivel de técnica legislativa que los Estados, crean normas que regulan el comportamiento de los agentes del mercado en sus relaciones internas como en sus relaciones con clientes. Las normas de organizaciones internacionales, como las producidas por Naciones Unidas o la OCDE, se encaminan principalmente a establecer un marco común de comportamiento de todos los agentes del mercado que actúen en el espacio virtual, ofreciendo así unas garantías comunes para el

comercio internacional. Las normas emitidas por organizaciones internacionales constan, básicamente, de dos apartados, el primero encaminado a establecer unos principios generales de actuación en el Comercio Electrónico y el segundo establece unos lineamientos a los Estados para incorporar adecuadamente dichos principios en los ordenamientos jurídicos nacionales, a fin de evitar aplicaciones diversas en cada uno de ellos. Las normas regionales establecen, al igual que las normas de organizaciones internacionales, criterios generales que deben ser incorporados por los Estados, sin embargo, su ámbito de aplicación es más restringido, pues sólo se encamina a los Estados miembros de un proceso de integración concreto, a fin de garantizar el cumplimiento de metas tales como el funcionamiento de un mercado interior. Existen también, algunas normas que no son de creación exclusiva de organizaciones internacionales o bloques regionales, sino que son acuerdos entre Estados y Bloques Regionales. Ejemplo de este tipo de normas es el *safe harbor*, norma de creación conjunta entre Estados Unidos y la Unión Europea, a fin de establecer estándares de seguridad uniformes en el manejo de datos privados. El Estado, finalmente, es el encargado de incorporar las normas internacionales y regionales, así como permitir la producción de normas por parte de los particulares.

En Colombia, el Comercio Electrónico cuenta con la existencia de regulación internacional, de *self regulation* y legislación nacional. Desde el ámbito regional, no ha existido una regulación por parte de la Comunidad Andina de Naciones, sin

embargo, se han formulado algunas reglas en ciertos Tratados de Libre Comercio –con Estados Unidos y el Triángulo Centroamericano-. En cuanto a normas de *self regulation*, puede hablarse de la existencia de Códigos de Conducta o de Ética, que consagran reglas de comportamiento de los agentes comerciales. Estas reglas establecen pautas de comportamiento de las empresas al interior de las mismas y en relación con sus clientes. Desde la actuación estatal propiamente dicha, Colombia cuenta con la Ley 527 de 1999, la cual incorpora al ordenamiento jurídico colombiano la Ley Modelo CNUDMI de Comercio Electrónico y adiciona, a su vez, normas para garantizar la seguridad en el manejo de firmas digitales, mediante la creación de entidades de certificación abierta y cerrada que, si bien no ofrecen una garantía real a la privacidad de los datos, garantiza la seguridad de las transacciones mercantiles, mediante el uso de certificados respaldados por entidades de confianza.

Sin embargo, la existencia de una pluralidad de normas con distintos agentes ofrece algunas cuestiones. Por una parte, debe cuestionarse si las distintas normas de Comercio Electrónico existentes cuentan con un elemento sistematizador de las mismas, de tal forma que se pueda hablar una aplicación uniforme de ellas, evitando así aplicaciones distintas que afecten el funcionamiento normal de las transacciones internacionales. Asimismo, debe cuestionarse si las normas que regulan el Comercio Electrónico, al momento de su creación y entrada en vigencia, tienen un reconocimiento de los Derechos

Humanos, así como herramientas efectivas de protección, especialmente en materias de protección de privacidad, seguridad. Dichas cuestiones serán analizadas posteriormente. El reconocimiento de los Derechos Humanos permitiría que ciertas entidades eviten el abuso y negociación de datos privados que corresponden a personas que han negociado o tenido contacto con ellas.

Asimismo, surge como cuestión el cómo debe regularse, desde el comercio electrónico, el manejo de bases de datos privadas que recolectan, organizan y distribuyen información tanto de consumidores como de comerciantes. Al presentar la existencia de normas que regulen la seguridad y privacidad de datos, especialmente en Colombia, puede percatarse que, mientras que los Códigos de Ética o de Conducta establecen principios que restringen o regulan la actividad de entidades financieras en cuanto a transmisión de datos, la ley 527 de 1999 no prevé norma alguna que regule el tema de bases de datos, la recolección, organización de información de particulares. Una posible respuesta puede darse desde la protección de Derechos Fundamentales. En Colombia, la Constitución de 1991 en su art. 15 consagra como Derecho Fundamental el Hábeas Data y otorga al legislador la facultad para regularla. Sin embargo, de acuerdo a la misma Constitución de 1991, los Derechos Fundamentales que permiten regulación, sólo pueden ser objeto de la misma a través de Ley Estatutaria. La Ley de Comercio Electrónico, como ley de incorporación de un instrumento de nueva lex mercatoria, no fue tramitada como Ley Estatutaria sino como Ley Ordinaria y por tanto, la

posibilidad de incorporar la regulación de un Derecho Fundamental implicaría la inconstitucionalidad de la misma. Por ello, es necesario el análisis de una segunda Ley, conocida como Ley de Hábeas Data (1266 de 2008), la cual regula el manejo de datos por parte de Bases de Datos, sus límites y las sanciones en caso de afectación negativa del Derecho Fundamental. Dicho análisis de la Ley se hará en un escrito posterior.

Bibliografía

_____ (2001), U.S.-EU "Safe Harbor" Data Privacy Arrangement, en The American Journal of International Law, Vol. 95, No. 1, Págs. 156 y ss.

ALJURE S. (2002), Antonio, Derecho Electrónico y Lex Mercatoria, en Revista Juris Consulta, No. 6, Cámara de Comercio de Bogotá.

CASTAÑO GÓMEZ DEL V., César (2003), Nueva Visión de la Ética Empresarial: Informes y Códigos Éticos, en Anales de Mecánica y Electricidad, Enero-Febrero.

FARRELL, Henry (2003), Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement, en International Organization Review, Vol. 57, No. 2.

GAMBOA B., Rafaél H. (2005), P2P: La nueva Amenaza a la Propiedad Intelectual en la Red, en Comercio Electrónico, Ed. Universidad de los Andez y Ed. Legis, 1ª Ed., Bogotá.

GARCÍA O., Berta M. (2009), Nuevos Desafíos para la Intervención Social: La Protección de los Consumidores en el Mercado Electrónico, en Revista e Estudios Empresariales-Segunda Época, No. 1.

GÓMEZ S., Luis Miguel (2002), Aspectos Tributarios del Comercio Electrónico, en Revista Juris Consulta, Cámara de Comercio de Bogotá, No. 6.

GUTÍERREZ G., María C. (2005), Consideraciones sobre el Tratamiento Jurídico del Comercio Electrónico, en Comercio Electrónico, Ed. Universidad de los Andes y Ed. Legis, 1ª Ed., Bogotá.

GUTÍERREZ, María Clara (2008), Desarrollo en la Regulación del Comercio Electrónico en los Países de la Región Andina, en Revista Alfa-Redi, No. 128, Agosto, versión digital. Recuperado el 08.04.2011 de http://www.alfa-redi.org/rdi-articulo.shtml?x=10731.

HERDEGEN, Matthias (2008), Internationales Wirtschaftsrecht, Verlag C.H. Beck, 7. Auflage, München.

KOBRIN, Stephen J. (2001), Territoriality and the Governance of Cyberspace, en Journal of International Business Studies, Vol. 32, No. 4.

LÓPEZ J. David, MARTÍNEZ L., Francisco J. (2010), Los Códigos de Conducta como Solución frente a la Falta de Seguridad en Materia de Comercio Electrónico, en Revista Ciencias Económicas, Vol. 28, No. 1.

MUÑOZ L., José E. (2009), Internet Conflict of Laws: a Space of Opportunities for ODR, en International Law Review, No. 14, Universidad Javeriana, Enero-Junio.

NACIONES UNIDAS (1996), Ley Modelo CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al Derecho Interno, Nueva York, 1996.

NICOLAIDIS, Kalypso (2005); SHAFFER, Gregory, Transnational Mutual Recognition Regimens: Governance without Global Government, en Law and Contemporany Problems Review, Vol. 68, No. 3/4.

ORDOÑEZ, Jaime A. (2002), Aspectos Comerciales y Regulatorios de Comercio Electrónico en el Siglo XXI, en Revista Juris Consulta, Cámara de Comercio de Bogotá, No. 6.

RAVASSA M., Gerardo J. (2004), Derecho Mercantil Internacional: Principios y Normas, Ed. Doctrina y Ley LTDA., 2ª Ed., Bogotá.

REMOLINA A., Nelsón (2005), Aspectos Legales del Comercio Electrónico, la Contratación y la Empresa Electrónica, en Revista de Derecho, Comunicaciones y Nuevas Tecnologías, Universidad de los Andes.

REMÓN P., Jesús (2002), Jurisdicción y Comercio Electrónico (Una Reflexión al Hilo del Proyecto de Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico y del Reglamento (CEE) 44/2001), en Revista Actualidad Jurídica Uría & Menéndez, No. 2º/2002.

RINCÓN C., Erick (2007), Aspectos jurídicos de los mecanismos de seguridad en entornos electrónicos, y análisis de un caso exitoso dentro de la industria, en CÁMARA DE COMERCIO DE BOGOTÁ, Escritos contemporáneos de derecho de los negocios, Uniempresarial/CCB, Bogotá, Colombia.

SIQUEIROS, José L., Los Nuevos Principios de UNIDROIT sobre Contratos Comerciales Internacionales, en Revista de Derecho Privado, Nueva Época, año IV, No. 11, mayo-agosto 2005.

UMAÑA CH., Andrés F. (2006), Contratación electrónica internacional, en RINCÓN C., Erick, Contratación electrónica, Universidad del Rosario, Bogotá, Colombia.

UNIDROIT, Principios UNIDROIT sobre los Contratos Comerciales Internacionales, 2ª Ed., Roma, 2004.

[i] GUTÍERREZ G., María C. (2005), Consideraciones sobre el Tratamiento Jurídico del Comercio Electrónico, en Comercio Electrónico, Ed. Universidad de los Andes y Ed. Legis, 1ª Ed., Bogotá Pág. 2; MUÑOZ L., José E. (2009), Internet Conflict of Laws: a Space of Opportunities for ODR, en International Law Review, No. 14, Universidad Javeriana, Enero-Junio, Pág. 167; RAVASSA M., Gerardo J. (2004), Derecho Mercantil Internacional: Principios y Normas, Ed. Doctrina y Ley LTDA., 2ª Ed., Bogotá, Págs. 506 y s.; REMOLINA A., Nelsón (2005), Aspectos Legales del Comercio Electrónico, la Contratación y la Empresa Electrónica, en Revista de Derecho, Comunicaciones y Nuevas Tecnologías, Universidad de los Andes, Pág. 331. Asimismo, la legislación colombiana ha asumido esta definición al establecer en su art. 2º lit. b) de la Ley 527 de 1999 que por *Comercio Electrónico* se entienden las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar.

[ii] FARRELL, Henry (2003), Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement, en International Organization Review, Vol. 57, No. 2, Pág. 277; GÓMEZ S., Luis Miguel (2002), Aspectos Tributarios del Comercio Electrónico, en Revista Juris Consulta, Cámara de Comercio de Bogotá, No. 6, Págs.103 y s.; GARCÍA O., Berta M. (2009), Nuevos Desafíos para la Intervención Social: La Protección de los Consumidores en el Mercado Electrónico, en Revista e Estudios Empresariales-Segunda Época, No. 1, Pág. 79; HERDEGEN, Matthias (2008), Internationales Wirtschaftsrecht, Verlag C.H. Beck, 7. Auflage, München, Pág. 38; KOBRIN, Stephen J., Op. Cit. Pág. 88; ORDOÑEZ, Jaime A. (2002), Aspectos Comerciales y Regulatorios de Comercio Electrónico en el Siglo XXI, en Revista Juris Consulta, Cámara de Comercio de Bogotá, No. 6, Pág. 16

[iii] La CNUDMI es el órgano jurídico de las Naciones Unidas en el ámbito del derecho mercantil internacional, de composición universal y dedicado a la reforma de la legislación mercantil a nivel mundial durante más de 40 años. La función de la CNUDMI consiste en modernizar y armonizar las reglas del comercio internacional. Para una mayor información sobre la CNUDMI, se recomienda ver http://www.uncitral.org/uncitral/es/about_us.html.

[iv] Básicamente, los nuevos capítulos incluidos en la Reforma de los Principios UNIDROIT de 2004 hacen referencia a temas tales como el apoderamiento de representantes, contratos a favor de terceros, cesión de créditos, transferencia de obligaciones, cesión de contratos y prescripción. Para un estudio sobre las reformas incluidas en los Principios UNIDROIT, véase UNIDROIT (2004) , Principios UNIDROIT sobre los Contratos Comerciales Internacionales, 2ª ed., Roma.

[v] Ejemplo de ellos son los textos guías –*primers*- y guías diseñadas por la OCDE, las cuales están dirigidas a las instituciones encargadas del diseño de políticas públicas. Particularmente, se puede destacar OCDE, *primer Working Party on Information Security and Privacy: The Role of Digital Identity Management in th Internet Economy: a Primer for Policy Makers*, 2009, Pág. 4. Asimismo, las Naciones Unidas establece, en el art. 17 Núm. 2º de la Convención de Derecho Civiles y Políticos, que toda persona tiene el Derecho a una

protección legal –estatal- contra toda interferencia injusta en su privacidad. Esta norma es uno de los fundamentos esenciales de la protección de datos en Internet y en el *Comercio Electrónico.*

[vi] El Safe Harbor Arrangement consiste básicamente en el debate de dos ordenamientos jurídicos sobre el manejo de datos en la red. Con el desarrollo de las tecnologías de la información, avanzaron también el la recepción de información de clientes como su posible negociación con otras compañías. La Unión Europea, a través de varias Directivas, como la 2000/31/CE, estableció normas de protección de datos privados y, a su vez, consagró criterios sobre el flujo de datos personales en países terceros. Estos criterios restringen considerablemente la acción de particulares en cuanto a la regulación del flujo de información o de datos personales. Dicha restricción entra en conflicto con los criterios establecidos en las políticas de Estados Unidos, para quien sólo es necesario la formulación de unas políticas generales y un amplio márgen de regulacción de los particualres. Sobre el encuentro de estos criterios y la construcción de un acuerdo entre Estados Unidos y la Unión Europea, véase FARRELL (2003: 277 ss.); HERDEGEN M. (2008: 39) KOBRIN (2001: 699 s.); _____ (2001), U.S.-EU "Safe Harbor" Data Privacy Arrangement, en The American Journal of International Law, Vol. 95, No. 1, Págs. 156 y ss.; NICOLAIDIS, Kalypso (2005); SHAFFER, Gregory, Transnational Mutual Recognition Regimens: Governance without Global Government, en Law and Contemporany Problems Review, Vol. 68, No. 3/4, Pág. 279.

[vii] Esta disposición se separa así de los criterios normativos de otras disposiciones. Por ejemplo, la Unión Europea, en la Directiva 1999/93/CE, permite y regula tanto la firma electrónica simple –art. 2 núm. 1º Directiva 1999/93/CE- y la firma electrónica avanzada –art. 2 núm. 2º Directiva 1999/93/CE-, que sería el equivalente a la firma digital consagrada en los arts. 2 lit. c) y 28 de la Ley 527 de 1999. Asimismo, la legislación colombiana se separa también de los criterios establecidos por las legislaciones de otros países surameticanos como Ecuador, Bolivia y Venezuela, quienes adoptan el uso de firmas electrónicas. Sobre éste último tema, véase GUTÍERREZ M. (2008) http://www.alfa-redi.org/rdi-articulo.shtml?x=10731.

[viii] La Superintendencia de Industria y Comercio, mediante Circular Única No. 10 de 2001, ha establecido en su Capítulo VIII las reglas sobre autorización y funcionamiento de las entidades de certificación tanto cerradas como abiertas. Esta circular ha sido modificada por los siguientes actos de la Superintendencia de Industria y Comercio: Resolución 36904 de 2001, Resolución 3493 de 20002, Circular 2 de 2002, Circular 19 de 2002 y Circular 23 de 2002.