Ars Iuris Salmanticensis
ESTUDIOS
Vol. 10, 199-226
Junio 2022
eISSN: 2340-5155
doi: https://doi.org/10.14201/AIS2022101199226

Tecnología y derecho: una mirada al comercio electrónico, el cibercrimen y el *soft law*

Technology and Law: a Look at e-Commerce, Cybercrime and Soft Law

Leónidas Salvador TAPIA SÁNCHEZ
Universidad Americana (UAM)
Nicaragua
Doctorando en Derecho (1.ª edición) por la Universidad Americana UAM (Nicaragua) y la Universidad de Salamanca (España)
Asesor legal del Poder Judicial de Nicaragua
https://orcid.org/0000-0002-9711-720X
leotapia@uamv.edu.ni

Recibido: 29/09/2021

Aceptado: 26/03/2022

Resumen

El derecho internacional, el comercio electrónico y la tecnología justifican su relación porque en la Internet o el ciberespacio no existen fronteras terrestres, marítimas o aéreas. Internet, por ende, abarca una pluralidad de jurisdicciones. Dentro del

Abstract

International law, the e-commerce and technology justify their relationship because, in the specific case of the Internet or cyberspace, does not establish land, sea or air borders. The Internet, therefore, encompasses a plurality of jurisdictions. Within the development of technology,

desarrollo de la tecnología, igualmente se habla de nuevos conceptos como personalidad digital, persona digital (usuario), firma electrónica *(password)*, comercio electrónico *(e-commerce)*, ecosistema digital, ciberdelitos y un nuevo término denominado *soft law*. Hoy, la humanidad se relaciona e interactúa en un planeta virtual o ciberespacio o, mejor dicho, en un ecosistema digital, donde el comercio electrónico es un paradigma a tomar en cuenta. Esto colige que la disrupción digital tiene presencia en todos los continentes y casi todos los países del mundo.

Actualmente, podemos comunicarnos de un continente a otro, de un país a otro con solo tener acceso a Internet y a un dispositivo tecnológico *(smartphone*, *tablet, laptop)* y, para ello, no se necesita visa o pasaporte. Sin embargo, dicha cohesión también ha traído concomitantemente la proliferación de ciertas conductas que, a la luz del derecho, no son adecuadas o son ilegales, tal es el caso de los ciberdelitos, los cuales no conocen de fronteras terrestres, marítimas o de cualquier otra índole, ya que se realizan en un entorno digital o virtual. Probablemente, a futuro se crearán fronteras digitales las cuales hoy en día son un *noúmeno*, con el objetivo de combatir el cibercrimen, lo que generaría también delimitar jurisdicciones digitales y un tribunal ad hoc, instituciones que podrían crearse por medio de un tratado o plantearse desde la academia como forma de coadyuvar a que los Estados logren un consenso, que al final contribuya a combatir los delitos transfronterizos sin afectar el acceso a las TIC. El derecho, igualmente, debe evolucionar hacia el ciberderecho o el derecho digital, el cual dentro de sus ramas plantearía el derecho global digital internacional con el objetivo de crear un derecho originario contenido en tratados o convenios internacionales para regular y garantizar la seguridad jurídica, el tráfico de información, la información personal y la justicia en el actual mundo digital.

there are new concepts such as digital personality, digital person (user), electronic signature (password), electronic commerce (e-commerce), digital ecosystem, cybercrimes, and a new term called *Soft Law*. Today, humanity relates and interacts on a virtual planet or cyberspace or, rather, in a digital ecosystem, where e-commerce is a paradigm to be taken into account. This suggests that digital disruption has a presence on every continent and almost every country in the world.

Currently, we can communicate from one continent to another, from one country to another just by having access to the Internet and a technological device *(smartphone*, *tablet, laptop)*, and for this, no visa or passport is needed. However, this cohesion has also brought concomitantly the proliferation of certain behaviors that, in the light of the law, are not appropriate or are illegal, such is the case of cybercrimes which do not know of land, sea or any other borders, since they are carried out in a digital or virtual environment. Probably, in the future digital borders will be created which today are a *noumeno,* with the aim of combating cybercrime, which would also generate delimiting Digital Jurisdictions and an *ad hoc* Tribunal, institutions that could be created through a Treaty or, raised from the academy as a way to help States achieve a consensus, that in the end contributes to combating cross-border crime without affecting access to ICTs. The law must also evolve towards cyberlaw or digital law, which within its branches would raise the International Digital Global Law in order to create an Original Law contained in International Treaties or Conventions to regulate and guarantee legal certainty, information traffic, personal information and justice in the current digital world.

Therefore, the development of Information and Communication Technologies (ICT) is regard by many as the new industrial revolution, also called Revolution 4.0. This

Por consiguiente, el desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) es considerado por muchos como la nueva revolución industrial, también denominada Revolución 4.0. Esto ha venido evolucionando desde las últimas décadas del siglo XX y primeros veinte años del siglo XXI provocando un «boom digital» con el desarrollo de los programas informáticos y dispositivos celulares *(smartphones)*, alimentadas por el progreso de la inteligencia artificial.

Palabras clave: comercio electrónico; derecho internacional; soft law; hard law; transacciones on line; ecosistema digital; derecho digital; personalidad digital; cirberderecho; ciberdelito; cibernética; inteligencia artificial; seguridad jurídica; Derecho Informático; ingeniería social; tratados internacionales; convenios de cooperación; Convención sobre el Cibercrimen; datos personales; *Lex Mercatoria*; Lex Electrónica.

has been evolving since the last decades of the twentieth century and the first twenty years of the twenty-first century causing a «digital boom» with the development of computer programs and cellular devices *(smartphones)*, fueled by the progress of Artificial Intelligence.

Keywords: E-Commerce; Derecho International; Soft Law, Hard Law; Digital Ecosystem; Digital Law; Digital Personality; Cyberlaw; Cybercrime; Cybernetics; Artificial Intelligence; Legal Security; Computer Law; Social Engineering; International Treaties; Cooperation Conventions; Convention on Cybercrime; Personal facts; Merchant Law; Lex Electronics.

1. INTRODUCCIÓN

La Revolución 4.0 es el resultado de los procesos que se dan dentro de la sociedad de la información y las tecnologías de la información. Las transacciones comerciales tanto nacionales como internacionales y la competitividad entre personas naturales y/o jurídicas (empresas) que residen en diferentes naciones o Estados, cada uno con sendas legislaciones, son un ejemplo de ello y son una realidad. En la actualidad, no

es necesario abocarse a un lugar específico para comprar un bien o adquirir un servicio, basta con tener acceso a Internet, un *smartphone* y una aplicación descargada para luego hacer el pedido en línea, transacción que, como se mencionó antes, puede hacerse de un Estado o país a otro, o dentro del mismo país. Esto requiere que el comprador tenga una personalidad digital, ligada con sus cuentas bancarias (tarjeta de débito o crédito), entre otras variables, lo que genera el despliegue de un tendido tecnológico *sui generis*.

En cada Estado donde la transacción comercial tenga lugar debe o debería existir una política de protección de datos personales que garantice al comprador o ciberconsumidor que su información personal será utilizada solamente para el propósito para la cual fue otorgada, siendo esto el derecho a la autodeterminación informativa. Y tal derecho aplica o debería aplicar en todas las transacciones o actos de comercio que impliquen el almacenamiento, procesamiento y archivo de datos personales, sea el dato automatizado o no. Acá podríamos decir que estamos en presencia de la precitada Lex Electrónica, pero enfocada en los datos que son torales en el comercio nacional y/o internacional electrónico. Esto abarca otro estándar fundamental, el cual es la ciberseguridad ante las amenazas que rondan en el ciberespacio y presente en varias jurisdicciones, ya que trasciende los territorios propios de los países, regiones y continentes del planeta.

En este conglomerado de innovación digital, se encuentra lo atinente a redes neuronales artificiales, ya que las mismas son el alma de la inteligencia artificial que hoy en día existen y que, según el sitio *web* Aprende Machine Learning, en su artículo «Breve Historia de las Redes Neuronales Artificiales» (2018), el inicio de la denominada «neurona artificial» fue el Perceptron desarrollado en 1958 por el científico Frank Rosenblat, el cual sería «la unidad desde donde nacería y se potenciarían las redes neuronales artificiales».

> La Comisión Europea señala que el término «inteligencia artificial» (IA) se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción —con cierto grado de autonomía— con el fin de alcanzar objetivos específicos. (SARASÍBAR IRIARTE, 2019, pp. 379-380)

Y, por último, están los ciberdelitos que se realizan utilizando las TIC, Internet y, claro, la inteligencia artificial. Respecto a estos actos delictivos, se desprende que «son las conductas típicas, antijurídicas y culpables en la que se tiene a la Cibernética como instrumento o fin» (TÉLLEZ VALDÉZ, 1998, p. 113). Igualmente, es importante acotar que, por ejemplo, un usuario de la Banca en Línea, donde los datos personales son fundamentales, debe tomar en cuenta ciertas recomendaciones, tales como entrar de manera directa al URL cuando se accede al portal del banco para evitar ser redireccionado donde un *cracker*; se debe también verificar en la esquina superior izquierda de la interfaz que a las letras http les subsiga la letra «s», es decir: https. La letra «s» significa seguridad, amén del candado color verde que se encuentra a la izquierda de las letras antes mencionadas. Igualmente, hay que evitar realizar transacciones de Banca en

Línea en servidores públicos o redes abiertas (ciber-cafés, hoteles, restaurantes con Wi-Fi gratis, etc.). Hay que revisar periódicamente los estados de cuenta bancarios, entre otras variables (LEE, 2015). Con todo esto, tenemos suficientes insumos para desarrollar a lo largo del presente artículo una investigación teórica y descriptiva, basada en la relación que existe entre la tecnología y el derecho a través del análisis del comercio electrónico, la cibercriminalidad y el *soft law*.

2. DE LOS TRATADOS INTERNACIONALES Y SU RELACIÓN CON LAS TIC

2.1. *Un análisis doctrinario desde los derechos humanos y los tratados internacionales*

La Declaración Universal de los Derechos Humanos de 1948 reconoce el derecho a la vida, al trabajo, a la educación, a la dignidad, a la libertad, a la personalidad, a la igualdad, a ser juzgado con base a la ley, entre muchos otros. Antes de dicha Declaración, se exploraron y establecieron en la Edad Contemporánea los derechos alcanzados con la Revolución francesa (1789), como son la libertad, la igualdad y la fraternidad. Asimismo, se abolió el Antiguo Régimen y, con él, los estamentos medievales. Igualmente, a lo largo de la historia antigua y la Edad Media, ocurrieron cambios como los producidos dentro del Imperio romano con el Edicto de Milán (313 d. C.), que permitió la libertad de culto, especialmente del cristianismo, lo que avivó en su momento las relaciones comerciales. *Verbigracia*, Vera RAMÍREZ (2018) citando a BERGIER (1973) colige que en la época medieval la economía era preindustrial y precapitalista, donde las ferias de Ginebra se basaban en el intercambio a larga distancia de mercancías de lujo como la seda y las especias, como principal mercancía para traficar a distancia. Es decir, que en el Medioevo ya existía actividad comercial, sin embargo, esta se ceñía a pocos productos o mercancías. Más ilustrativo aún resulta lo que Vera RAMÍREZ (2018) expresa, respecto a la producción durante la Edad Media:

> La transformación sustancial en el modo de producción que llegará a través de los feudos significó el detrimento de la actividad comercial. Por tal razón, se comparte la idea de que el retroceso que implicó para la Edad Media la vuelta a un sistema basado en la actividad agrícola como lo sostienen Pirenne (1983) y Pounds (1987), va a ver compensada por la actividad comercial ejercida principalmente por el Imperio Romano de Oriente. (p. 6)
>
> En este punto, y basándonos en esas relaciones preindustriales de la Edad Media, es que podríamos hablar de la entrada en acción del Comercio y del Derecho Internacional. Tradicionalmente el Derecho Internacional General se ha dividido en dos grandes esferas: a. El derecho Internacional Público, y b. El Derecho Internacional Privado [...] (CLERC, 2013, p. 17)

En el derecho internacional privado, con base a lo expresado por CLERC (2013), se colige siguiente:

> Bajo las incumbencias caídas en la órbita del DIP, exceptuando al derecho penal, deben incluirse todas las disciplinas jurídicas y todas las controversias interpartes susceptibles de ser planteadas en sede judicial y siempre que una de ellas sea extranjera y en razón de concurrir allí ordenamientos y legislaciones diversas. (p. 19)

El derecho internacional público se presenta como una fuente de derechos, una cantera de los denominados derechos originarios que se crean mediante los tratados y que, a posteriori, tienen influencias en las legislaciones nacionales. Con base a ello, se coligen los denominados sistemas monistas y dualistas.

Al respecto, TREJO GARCÍA *et al*. (2006) establecen que los tratados internacionales regulan algunas materias que inciden en el Derecho nacional como es el comercio, los derechos humanos, las relaciones contractuales, el medio ambiente, etcétera. Los tratados se reputan como un ordenamiento para los aspectos comerciales y jurídicos en el campo del comercio, aspectos que en la Antigüedad y en la Edad Media no existían como tales. Ejemplo de ello es la Convención de Viena sobre el Derecho de los Tratados del 23 de mayo de 1969 y la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías de 1980 adoptada el 11 de abril de 1980 y que entró en vigor el 1 de enero de 1988, cuya finalidad fue prever un régimen moderno, uniforme y equitativo para los contratos de compraventa internacional de mercancías, por lo que contribuyó notablemente a dar seguridad jurídica a los intercambios comerciales y a reducir los gastos de las operaciones, entre otros tratados relacionados.

En la misma línea, TREJO GARCÍA *et al*. (2006) expresan:

> Se utilizan muchos nombres para designar a los tratados, aunque esto no es relevante desde el punto de vista jurídico, ya que la Convención de Viena señala «... cualquiera que sea su denominación». Esta multiplicidad de nombres se debe a que los tratados internacionales presentan entre sí características muy diversas según la materia a que se refieren [...]. (p. 1)

La misma autora discurre que el art. 38 del Estatuto de la Corte Internacional de Justicia, respecto a las controversias, deberá aplicar las convenciones internacionales, la costumbre internacional, los principios generales del derecho reconocidos por las naciones civilizadas, las decisiones judiciales y la doctrina.

La tesis dualista, TREJO GARCÍA *et al*. (2006) deducen en que en la misma se postulan dos órdenes jurídicos donde convergen el internacional y el interno, siendo diferentes en su esfera de acción y su carácter, pero aun así existen independientemente como dos sistemas jurídicos autónomos. La validez de uno no depende de la validez de otro.

De forma más atinada, TREJO GARCÍA *et al*. (2006) coligen:

> La teoría dualista o pluralista afirma que el Derecho Internacional y el Derecho Interno son dos ordenamientos jurídicos totalmente separados, independientes y autónomos, ya que sus fundamentos de validez y destinatarios son distintos. De este modo, las normas de Derecho Internacional son producidas mediante un procedimiento internacional y solamente obligan a comunidades soberanas, mientras que el Derecho Interno tiene su fundamento de creación y validez en la Constitución del Estado, que es el único ordenamiento que puede originar derechos y obligaciones para los individuos. (p. 14)

Por su parte, al referirnos a la teoría monista internacionalista, según TREJO GARCÍA *et al*. (2006), el derecho internacional es un orden jurídico jerárquicamente superior al derecho interno. Y en lo que respecta a la teoría monista nacionalista, según la misma autora, la primacía del derecho interno del Estado se basa en sostener que este es superior al derecho internacional. En este tema, para que las normas internacionales sean reconocidas por un Estado es necesario que la misma Constitución del Estado realice una incorporación de dichas normas internacionales o que se realice una adaptación de ellas a las estatales a través de los órganos competentes (TREJO GARCÍA *et al*., 2006).

Con la puesta en práctica de los precitados sistemas, donde se avalen principios rectores enfocados en el ciberespacio y comercio electrónico, es lógico encaminarse hacia la consolidación de una sociedad digital integral, la cual tendrá mayor connotación en los países desarrollados en sus inicios, pero que, poco a poco, se disgregará en el resto de los países democráticos y sociales de derecho.

Por ende, se reputa al ciberderecho como una nueva rama de la ciencia del Derecho. Según el sitio *web* Ródenas Abogados (s. f.), el ciberderecho es una rama que surge por el desarrollo del ciberespacio y la Internet, con el objetivo de establecer normas jurídicas que regulen a los cibernautas. Busca cómo adaptar las leyes tradicionales al espacio virtual.

Para BUSTAMANTE DONAS (s. f.), los derechos civiles y políticos de primera generación inciden sobre la expresión de libertad de los individuos y proceden de la tradición constitucionalista liberal, propios de la Declaración Universal de los Derechos Humanos de 1948 y los pactos internacionales de 1966, a saber: el de los Derechos Civiles y Políticos y el de los Derechos Económicos, Sociales y Culturales.

Los derechos de segunda generación son de naturaleza económica y social, e inciden sobre la expresión de igualdad de los individuos, exigiendo la intervención del Estado para garantizar un acceso igualitario a los derechos de primera generación. Por su parte los de tercera generación surgen en la segunda mitad del siglo XX, protegiendo los derechos de colectivos discriminados, grupos de edad, minorías étnicas o religiosas, países del Tercer Mundo, que se ven afectados por alguna de las múltiples manifestaciones que cobra la discriminación económico-social (BUSTAMANTE DONAS, s. f.)

Para BUSTAMANTE DONAS (s. f.), los derechos humanos de cuarta generación son los que se relacionan con la expansión del concepto de ciudadanía digital y conciernen con el libre acceso y uso de la información y conocimiento; con la lucha contra la exclusión digital y, por último, con la inteligencia colectiva que facilita la inserción de cada país a un mundo globalizado. Es decir, los derechos de cuarta generación son los que insertan o incluyen al ser humano en la sociedad digital, garantizándole sus derechos digitales (acceso a Internet, libertad de expresión, educación digitalizada, etcétera), y ello es, por lógica, la forma de garantizar una mejor subsistencia en el mundo globalizado porque cada vez más se hace necesario adecuarse a las nuevas tecnologías para estudiar, trabajar y convivir en la sociedad, entiéndase a esta última como la sociedad de la información.

2.2. *Supranacionalidad*

La supranacionalidad trae consigo relación con el derecho internacional, específicamente cuando nos referimos a comunidades de naciones como lo es, por antonomasia, la Unión Europea. RAMOS (2011), al respecto, discurre que dicho organismo comenzó con la Comunidad Europea del Carbón y el Acero en 1951; pasando a la Comunidad Europea de la Energía Atómica en 1957; hasta llegar al Acta Única Europea de 1986, camino que dio pauta al mercado único; luego con el tratado de Maastricht, que entra en vigor en 1993, se genera la unión monetaria, sin perjuicio del tratado de Ámsterdam que estableció en 1999 la unión política.

La palabra «supranacionalidad» tuvo su aplicación concreta cuando se creó la Comunidad Económica del Carbón y del Acero (CECA) por el Tratado de París en 1951. Efectivamente, el art. 92 punto 2 de dicho tratado, en la versión francesa, expresamente se refería al neologismo, al mencionar las facultades de la Alta Autoridad [...] (RAMOS, 2011, p. 8).

Por su parte, PEREIRA COUTINHO (2012) nos expresa claramente que los intereses meramente estatales quedan relegados cuando la supranacionalidad entra en función y, al respecto, el mismo autor colige:

> Las instituciones supranacionales trascienden, en teoría, la referida lógica de coordinación —les corresponden intereses supraestatales cuyo preciso alcance es definido por ellas mismas—. En consecuencia, la toma de decisiones vinculantes en el ámbito de las instituciones supranacionales no depende del consentimiento continuamente expresado por parte de todos o de algunos de los Estados, y ello se refleja en la inexigencia de unanimidad (democrática u oligárquica) en los procedimientos decisorios. (p. 200)

2.3. *Las normas* ius cogens

El derecho internacional igualmente establece normas *ius cogens*, o aquellas que no admiten reforma una vez que se aprueban y ratifican, tal es el caso de la prohibición del genocidio, el uso de la fuerza y de la tortura, lo que, por lógico corolario, crea derechos universales cuya transgresión puede ocasionar crímenes de lesa humanidad o delitos universales propiamente dichos.

«Desde que en 1969, la Convención de Viena sobre el Derecho de los Tratados (CV69) aludiera en el art. 53 a las normas imperativas de derecho internacional general, se han escrito y dicho muchas cosas sobre estas» (QUISPE REMÓN, 2012, p. 144). Por otro lado, GUERRERO MAYORGA (2012) deduce que las normas *jus (ius) cogens* se pueden reputar como la libre determinación, la buena fe en las obligaciones contraídas, la abstención del uso de la fuerza o de amenazas contra la integridad territorial o la independencia política de cualquier Estado.

En el mismo sentido, QUISPE REMÓN (2012) expresa lo siguiente en referencia al precitado art. 53 de la Declaración de Viena sobre el Derecho de los Tratados:

> Lo que sí queda claro del art. 53 es que las normas imperativas no admiten acuerdo en contrario, salvo que exista otra de la misma naturaleza, en tanto que, como dice Mariño, se trata de un caso de nulidad absoluta ab initio que excluye toda divisibilidad de las disposiciones del tratado y respecto a la cual la aquiescencia (y la renuncia al derecho a alegarla) queda asimismo excluida. (p. 147)

Y en lo que respecta a la falta de codificación de las normas *ius cogens*, GUERRERO MAYORGA (2018) concuerda con lo dicho por QUISPE REMÓN (2012), ya que el art. 66 de la Convención de Viena sobre el Derecho de los Tratados en su literal a) establece jurisdicción obligatoria para controversias derivadas por el incumplimiento de normas *jus (ius) cogens*, pero sin determinar positivamente cuáles son estas.

> El Internacional no reposa en la voluntad del Estado, sino que hay en él normas que prevalecen incondicionalmente sobre ella. Un tratado contrario a tales normas sería nulo o terminaría. (Guerrero Mayorga, 2018, p. 4)

Hasta el momento, no se ha relacionado a las TIC con normas *ius cogens*, sin embargo, por la importancia que estas están adquiriendo con el paso de los años (las TIC), podría llegar a estipularse una norma *ius cogens* propia de las Tecnologías de la Información y las Comunicaciones, sobre todo si hacemos énfasis en el tema de la Lex Electrónica, ya que, según PEÑA VALENZUELA (s. f.), la deslocalización y la virtualidad son características dominantes en la era digital, donde la sociedad de la información es la que se basa en el uso cotidiano de tecnología. Es así que, básicamente, el mundo está interconectado a través de los medios electrónicos, telemáticos, digitales, etcétera, y esto ha ocasionado la proliferación del comercio electrónico, lo que conlleva, a su vez, la necesidad de creación y aplicación de una Lex Electrónica común *sui géneris* del y para el comercio electrónico.

En la aplicación de una Lex Electrónica, PEÑA VALENZUELA (s. f.) establece lo siguiente:

> La existencia del documento electrónico está definida por determinada configuración de los programas de ordenador que definen su creación, almacenamiento y transporte. El mensaje de datos se convierte en la categoría general que reúne a la información generada, almacenada y transportada por medios digitales. (p 104)

Los datos son el alma de la información almacenada en medios digitales y su procesamiento es indispensable para el tráfico internacional de mercancías, el cual ya se basa en la *Lex Mercatoria*, pero que, debido a la proliferación de las tecnologías de la información y las comunicaciones, también resulta necesaria una ley ajustada a estas transacciones digitales que se dan a través de Internet, y que sería la Lex Electrónica propiamente dicha, en tal sentido, PEÑA VALENZUELA (s. f.) colige lo siguiente:

> La contratación electrónica es una materia en constante evolución, a la par de avances tecnológicos relacionados con la presentación de productos y servicios en línea.
> La desmaterialización de documentos permite mayor agilidad en las transacciones internacionales y anticipa el crecimiento de los negocios jurídicos respecto de bienes intangibles que van a aumentar en la medida de que la sociedad de la información alcance su madurez. (p. 115)

Algo que debemos tomar en cuenta es que las normas *ius cogens* son de derecho internacional general, no regional, lo que implicaría una norma global. Respecto a ello, QUISPE REMÓN (2012) concluye lo siguiente:

> Como su propio nombre indica, son normas de Derecho Internacional General. Así, resulta importante en su determinación la repercusión para la comunidad internacional y no regional. En consecuencia su existencia genera obligaciones *erga omnes* y no se limita al ámbito regional. Es un derecho elemental por la naturaleza especial del objeto que protege, y por tanto se torna en una exigencia en el mundo. (p. 148)

Es así que el derecho internacional público o privado se relacionan con los procesos de mercado en todas sus esferas, incluyendo el comercio electrónico, en un momento donde la globalización tiene presencia y predominio, sin embargo, cabe hacer una especial diferencia entre esta última y el término «mundialización», para lo cual, CLERC (2013), citando a CHESNAIS (1994), infiere:

> En efecto, mientras la globalización quedaría restringida al ámbito estrictamente económico, financiero y tecnológico, la mundialización, en cambio, expresa una fase específica del proceso de internacionalización del capital y de su emplazamiento totalizado a escala mundial que, en este caso, no solo implica la expansión del comercio mundial, sino que incluye allí a los rediseños jurídicos, institucionales, normativos, legislativos y políticos que dicha expansión requiere. La mundialización, en el sentido descrito, y según la definición de Chesnais (1994), puede muy bien ser utilizada como la clave explicativa e interpretativa del proceso de refuncionalización al que está sujeto el DIP, siendo la llamada *Lex Mercatoria*, la expresión más acabada de aquella mundialización. (p. 21)

La mundialización no necesariamente está basada en aspectos de estricta expansión del comercio a nivel global, sino que se relaciona con la *Lex Mercatoria*, es decir, los usos y costumbres mercantiles y los rediseños jurídicos, normativos o legislativos que la globalización como tal requiere. Es, en lógica jurídica, una regulación a la globalización vista desde un enfoque más humano para que la misma tenga un sentir basado en este último.

3. DIPLOMACIA DIGITAL

3.1. *Nuevas manifestaciones diplomáticas: diplomacia digital y uso de las TIC*

El uso de las TIC crea mayor cohesión humana y/o social, e igualmente fortalece la relación de los Estados como sujetos de derecho internacional público, tanto a nivel regional como mundial. Ejemplo de ello es la *diplomacia digital*, la cual supone la conectividad nacional como internacional a través de Internet, donde la actividad o comentarios en redes sociales de un ciudadano, gobernante o algún diplomático/cónsul de un Estado pueden afectar los intereses y/o relaciones diplomáticas con otro Estado u otros Estados, sin perjuicio de afectar a su propia nación.

Respecto a este tema, BASSANTE (s. f.) expresa:

> Por Diplomacia Digital se puede entender la incorporación de las redes sociales virtuales en el ejercicio diplomático como herramienta fundamental para la consecución de objetivos de política exterior. Se hace cada vez más evidente que la adopción de la Diplomacia Digital ha dejado de ser una opción y, al contrario, resulta cada vez más claro que se trata de una necesidad. (p. 77)

Se colige que un comentario a través de *Twitter*, por ejemplo, podría ocasionar conflictos sociales, tanto internos como externos, al crear una crisis diplomática por el contenido del comentario en dicha red social, lo que indica el poder de llegada y acogida que estas nuevas tecnologías tienen. La tecnología, por ende, tiene presencia en todos los ámbitos, estructuras sociales, gubernamentales, políticas, nacionales e internacionales. Esto infiere que un jefe de Estado, presidente o primer ministro puede expresar su opinión mediante una red social y, debido a que el algoritmo es utilizado por personas de todos los círculos sociales, la repercusión pública de dicha opinión podría ser considerable. Respecto al tema de las redes sociales y la diplomacia, es importante el ejemplo que a continuación BASSANTE (s. f.) explica:

> Uno de los primeros registros sobre la utilización de redes sociales virtuales para comunicaciones entre diplomáticos de alto nivel se dio en 2011, cuando el Ministro de Relaciones Exteriores sueco descartó el uso de cables diplomáticos o llamadas telefónicas para comunicarse con una de sus contrapartes y prefirió, en cambio, usar Twitter. (pp. 80-81)

Entonces, los medios comunes que los agentes diplomáticos solían utilizar, como es el caso de los cables diplomáticos, hoy se sustituyen, en muchos casos, por los recursos que dan las nuevas tecnologías.

3.2. *Transacciones internacionales: identidad digital*

Las transacciones comerciales internacionales y la competitividad entre personas naturales y/o jurídicas (empresas) que residen en diferentes naciones o Estados, cada uno con sendas legislaciones, son una realidad. En la actualidad, no es necesario ir a la tienda a comprar un par de zapatos, basta con tener acceso a Internet, un smartphone y una aplicación descargada para luego hacer el pedido en línea, transacción que puede hacerse de un Estado o país a otro, o dentro del mismo país. Esto requiere que el comprador tenga una identidad digital y, dentro de ella, tenga datos personales que lo acrediten y relacionen con sus cuentas bancarias (tarjeta de débito o crédito), entre otras variables, lo que genera el despliegue de un tendido tecnológico propio o *sui géneris* de la actual sociedad de la información, siendo en conclusión el mensaje de datos el alma de la transacción electrónica.

Respecto a las características y propiedades de la identidad digital, la *web* del Gobierno de Canarias (s. f.) expresa que «La identidad digital es lo que somos para otros en la Red o, mejor dicho, lo que la Red dice que somos a los demás. No está definida a priori y se va conformando con nuestra participación, directa o inferida, en las diferentes comunidades y servicios de Internet». Igualmente, el mismo sitio *web* colige que nuestras acciones u omisiones en la red constituyen parte de nuestra identidad digital, así como las imágenes u otros datos que nos identifican.

La identidad digital se construye con la actividad que un usuario o usuaria tiene en la Red, es decir, se erige desde y por la Red, por lo tanto, sin Red no podríamos tener identidad digital por lo que, por lógico corolario, dicha identidad solo podría alegarse desde la Red o en el ciberespacio. No tenemos identidad digital por defecto, sino hasta que la construimos en la Red, y, con ello, los elementos de dicha identidad como el domicilio y demás datos para identificarnos serían también digitales. Por ende, debemos tener claro que a la misma están ligados un nombre, una dirección, un estado civil, un número de tarjeta de crédito, un DNI, entre otros factores que son propios de los datos personales, que, al fin de cuentas, deben estar protegidos por el Estado o por las normas del programa o aplicación que se usa, lo que podría reputarse como *soft law*, el cual analizaremos más adelante.

En cada Estado donde la transacción comercial tenga lugar debe existir una política de protección de datos personales que garantice al comprador o ciberconsumidor que su información personal será utilizada solamente para el propósito para el cual fue otorgada, y así evitar ser víctima de actos de ingeniería social. Y esto opera en todas las transacciones o actos de comercio que impliquen el almacenamiento, procesamiento y archivo de datos personales, sea el dato automatizado o no. Acá podríamos

decir que estamos en presencia de la precitada Lex Electrónica, pero enfocada en los datos que son torales en el comercio nacional y/o internacional electrónico. En tal efecto, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de España en su art. 2, numeral 1.º dice: «Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero».

En el control jurisprudencial de la protección de datos personales en España, es importante aludir a la *Sentencia de Casación del Tribunal Suprema Español (TS) de la Sala de lo Contencioso Administrativo n.º 815/2020, del 18 de junio*, la cual nació de un proceso contencioso-administrativo donde hubo una desestimatoria de Recurso promovido por la empresa DIRECCION001 contra resolución de la directora de la Agencia Española de Protección de Datos en fecha 11 de julio de 2017, por lo que se le impuso a la demandante una multa de 7500.00 euros por infracción del artículo 6.1 de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de carácter personal. En la precitada sentencia, se discutió en qué circunstancias (o con qué alcance) la voz de una persona puede considerarse como un dato de carácter personal, con arreglo al artículo 3 LOPD en relación con el artículo 5 RLOPD —actualmente artículo 4.1 del Reglamento General (UE)—. Al final, en su considerando sexto, el TS concluyó que «la grabación de la voz asociada a otros datos como el número de teléfono o su puesta a disposición de otras personas que pueden identificar a quién pertenece ha de considerarse un dato de carácter personal sujeto a la normativa de protección del tratamiento automatizado de los mismos».

Queda pendiente el análisis de la incidencia de estos ordenamientos jurídicos y/o jurisprudencia, como la precitada sentencia del TS respecto al mundo digital, especialmente en lo referente a los datos personales, es decir, si el derecho como tal entrará con mayor fuerza en las transacciones, procesos y demás actos que se dan dentro del ciberespacio, y donde los precitados datos son fundamentales para la identificación de las partes contratantes por la ausencia física de ellas, la virtualidad per se, los diferentes usos horarios, entre otros factores. Allende de esto, no debemos olvidar que las aplicaciones o *apps* tienen en su funcionamiento políticas y manuales los cuales el usuario debe «aceptar» para poder acceder a ellas, muchas veces desconociendo lo que esto implica.

A futuro y apartando la «ciencia ficción», la inteligencia artificial va a estar tan desarrollada que podrá establecer un gobierno digital, controlado por *bots* o robots, que no necesariamente reciban órdenes nada más, sino que tengan la capacidad de darlas y tomar decisiones en una sociedad donde los organismos serán digitales, *verbigracia*; un parlamento conformado por robots con inteligencia artificial, que sea capaz de emitir un decreto o ley en el ciberespacio, que afecte a las personas que transan en él mediante el comercio electrónico. Podría inclusive que, a futuro, si no está ocurriendo ya, la realidad corpórea de las personas naturales será por defecto al nacer, pero como

entrarán en un mundo virtual, su vida se desarrollaría primordialmente de manera digital (estudios, convivencia, relaciones sociales, jubilación, vejez, etc.). Es decir, la mayoría de los actos que son necesarios para el desarrollo social e interacción humanos serán digitalizados, aunque no sea viable el hecho de sustituir la ingesta de alimentos u oxígeno, que son aspectos básicos para vivir, por un programa o chip que satisfaga en el cerebro u organismo dichas necesidades básicas, por lo menos no en este momento.

4. ECONOMÍA DIGITAL, CIBERCRIMEN, CIBERSEGURIDAD Y LA PLURALIDAD DE JURISDICCIONES

4.1. *Economía digital*

Al hablar de tráfico de información, que va relacionado también al tráfico de mercancías y/o servicios y de dinero a través de las TIC, hablamos de economía digital, es decir, la que comprende transacciones que se realizan por medio de Internet a través de un medio electrónico.

La Ley Modelo de la CNUDMI (Comisión de la Naciones Unidas para el Derecho Mercantil Internacional) sobre comercio electrónico (1996) estableció como objeto la posibilidad de facilitar el comercio por medios electrónicos a través de reglas internacionales aceptables que traten de suprimir las cortapisas jurídicas en el campo de comercio electrónico.

Según el sitio *web* DocuSign (2021), «La economía digital es un modelo de mercado reciente que tiene presencia en casi todos los países y nos permite comunicarnos, consumir contenido y realizar transacciones comerciales pasando las barreras territoriales y temporales que comúnmente conocíamos».

La economía digital consta de varios factores: 1. La extraterritorialidad; 2. Uso *sine qua non* de las TIC, medios electrónicos e Internet; 3. Comercio internacional, y 4. globalización.

Esto incluye un aspecto fundamental, el cual es la ciberseguridad ante las amenazas que rondan en el ciberespacio, el cual abarca una pluralidad de jurisdicciones, ya que trasciende los territorios jurisdiccionales de los países, regiones y continentes del planeta.

Por ende, nos referimos a la *Lex Mercatoria*, y al respecto CALDERÓN MARENCO (2018), colige:

> La compraventa de mercaderías es hoy en día el acto de comercio por excelencia tanto nacional e internacional, por lo que su regulación es propia de los sistemas jurídicos nacionales, empero, en el ámbito exterior se ha debatido acerca de las nuevas formas jurídicas que pretenden regularla a través de instrumentos de Derecho paralelos a los instrumentos tradicionales creados por el Estado. (p. 2)

Siguiendo la línea de CALDERÓN MARENCO (2018), en el plano internacional es normal elegir el derecho a aplicar por parte de los contratantes, a lo que la doctrina denomina *autonomía conflictual*, figurándose como la salida de los conflictos tradicionales y entendiéndose que es la capacidad que tienen las partes de elegir la norma o ley más aplicable o que mejor convenga en su relación jurídica.

En tal sentido, CALDERÓN MARENCO (2018) expresa siguiente:

> De modo que las partes tienen derecho a elegir en su negocio jurídico normas de Derecho positivo nacional e internacional, o bien, una ley uniforme o todos aquellos instrumentos internacionales que hayan sido incorporados al Derecho nacional, o ya sea, la *Lex Mercatoria* (usos y costumbres). (p. 3)

Por su parte, RODRÍGUEZ FERNÁNDEZ (2012) expresa que el comercio global se enfrenta a normas locales, lo que pareciese que el comerciante del mundo moderno se presenta como un sujeto extraño al derecho positivo, porque sus actividades están fuera de la normativa estatal.

El problema estriba en un conflicto de costumbres y usos *(Lex Mercatoria)* con los ordenamientos jurídicos positivos. Desde la Edad Media, los comerciantes no se sujetaban a ordenamientos jurídicos porque se carecía de ellos. Hay que recordar que antes de la codificación contemporánea que comenzó en 1804 con el Código Napoleónico, dichas costumbres de alguna manera permanecieron en el inconsciente colectivo de los habitantes de los burgos, costumbres que a posteriori de la Revolución francesa y el Estado liberal, continuaron teniendo efectos en el comercio, como ocurre en la actualidad, y que en su momento fueron también fortalecidas con la eclosión de las Revoluciones Industriales. Al respecto, ESCUDERO (2009) se basa en el término crecimiento económico y lo conceptualiza como el aumento de la producción de bienes y servicios. Y es, efectivamente, el precitado crecimiento económico que en su momento histórico influyó en la Revolución Industrial del siglo XVIII, sin perjuicio de las subsiguientes.

Haciendo un breve análisis de la situación económica del antes y después de la primera Revolución Industrial, ESCUDERO (2009) expresa:

> Durante la Edad Moderna, los países europeos estaban poco poblados, y la esperanza de vida de sus habitantes no superaba los 30 años. Más del 75 por 100 de la población trabajaba en la agricultura, porque, como los campesinos tenían una baja productividad, se requería mucha mano de obra para producir los alimentos necesarios para alimentar a la población. Las ciudades eran pequeñas, y en ellas los artesanos también tenían una baja productividad. El comercio no era voluminoso y se realizaba con carros tirados por animales o con barcos de vela. Al ser baja la productividad, la renta por persona era pequeña, y la gran mayoría de la población consumía poco [...]. (p. 14)

El comercio ha evolucionado a parajes que en los siglos XVIII y XIX se consideraban utópicos. Y el punto de inflexión son efectivamente las TIC. Muchas actividades comerciales se basan en un comercio eminentemente electrónico *peer to peer* e igualmente

aplica en transacciones B2B *(Business to Business)*, B2C *(Business to Consumer)* o C2C *(Consumer to Consumer)*, donde las nuevas tecnologías son el medio y lalnternet el camino o la ruta donde transitan los mensajes de datos. Esto obviamente ha generado una eclosión sin precedentes en el comercio mundial, que irónicamente con la pandemia del COVID-19 se fortaleció por los aspectos del distanciamiento social, más no un distanciamiento digital. Por ello, el corolario es que, a mayor distanciamiento social, mayor es el acercamiento digital. Y de esto, los gobiernos son conscientes.

En tal línea, RODRÍGUEZ FERNÁNDEZ (2012) nos dice:

> Es por ello que la comunidad internacional de comerciantes, también denominada *societas mercatorum*, se ha encargado de la elaboración y reconocimiento de un conjunto de normas que devienen de sus mismos usos y prácticas mercantiles, y que por siglos se ha denominado *Lex Mercatoria*. En las últimas décadas ha tomado fuerza la hipótesis de que la existencia de una sociedad o grupo social integrado por aquellos que hacen parte o interactúan en los mercados nacionales, regionales e internacionales *(societas mercatorum),* le otorga a sus miembros la potestad para regular sus actividades. (p. 6)

4.2. *Comercio electrónico, cibercrimen e ingeniería social*

Según la *web* de la Organización para la Cooperación y el Desarrollo Económicos, OCDE (2020), desde mediados de la década de los noventa, el comercio electrónico ha despuntado. Dicho organismo y el Gobierno de Canadá, en 1998, organizaron de manera conjunta una Conferencia Ministerial sobre Comercio Electrónico en Ottawa, donde se convocó a líderes de gobiernos nacionales, directores de las principales organizaciones internacionales, líderes de la industria y representantes de los grupos de interés social, laboral y del consumidor, para debatir el desarrollo del comercio electrónico mundial. En dicha Conferencia se reconoció por parte de los participantes que el comercio electrónico es una forma radicalmente nueva para realizar transacciones comerciales. Luego, en la Conferencia Ministerial de la OCDE sobre la Política de Economía Digital celebrada en Cancún en 2016, los ministros declararon que «estimularían y ayudarían a reducir los obstáculos al comercio electrónico».

Posteriormente, en diciembre de 2017, la Organización Mundial del Comercio, el Foro Económico Mundial y la Plataforma Electrónica de Comercio Mundial pusieron en marcha conjuntamente la Iniciativa de promoción del comercio electrónico en beneficio de los consumidores, pequeñas y medianas empresas. Lo analizado nos ilustra sobre la importancia que esta novedosa actividad ha tenido y tiene en el desarrollo económico global.

Según la *web* de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, UNCTAD por sus siglas en inglés (2021), las restricciones en varios países debido a la pandemia del COVID-19 provocaron un aumento del comercio electrónico de las ventas minoristas, el cual pasó del 16 % al 19 % en 2020 con base en su informe del 3 de mayo de 2021. Según el mismo sitio *web*, «las ventas mundiales de comercio

electrónico alcanzaron los 26,7 mil millones de dólares a nivel global en 2019, un aumento del 4 % con respecto a 2018, según las últimas estimaciones disponibles. La cifra incluye las ventas de empresa a empresa (B2B) y de empresa a consumidor (B2C) y equivale al 30 % del producto interior bruto (PIB) mundial de 2019». Lo anterior demuestra la importancia que tiene en la actualidad la actividad comercial en línea; las cantidades inmensas de dinero que por ella circulan, y, por supuesto, la necesidad de una regulación adecuada que siga fomentando el comercio electrónico, pero con seguridad y justicia para los consumidores y/o ciberconsumidores.

Las transacciones comerciales internacionales en línea, realizadas entre diferentes países, son comercio internacional electrónico o digital. Esto ocasiona o puede ocasionar actos ilícitos contra las personas naturales o jurídicas que utilizan este tipo de procesos, y es en este punto donde los ciberdelitos, o los actos típicos y antijurídicos realizados con la ayuda de dispositivos, programas e Internet, pueden cometerse y lesionar el patrimonio. Los ciberdelitos son realizados de una forma avanzada y estratégica por los denominados *crackers (black hat hackers)*, quienes en su misión aplican técnicas de *ingeniería social* porque a través de tal actividad es que los cibercriminales *(crackers)*, o también denominados ingenieros sociales, identifican vulnerabilidades tanto en los sistemas como en las personas que los utilizan, lo que nos lleva a deducir que todo aquel que navegue en Internet de alguna manera está expuesto a ser víctima de un ciberdelito, siempre y cuando el acto esté tipificado como tal. Dicho riesgo está en cualquier punto donde se realice la transacción electrónica, sea en el servidor del comprador, del vendedor o en otro punto del *iter* digital, porque el ingeniero social, *verbigracia*, puede entrar a la red del comprador haciéndose pasar por el vendedor y creyendo el primero que la transacción en dinero la hará a favor del último, lo que no es así y, por ende ,se ocasionaría un daño patrimonial. Otra variable es que el *cracker* o delincuente informático se puede encontrar en un país determinado y la víctima en otro, lo que nos lleva a una *pluralidad de jurisdicciones* que dificulta o puede dificultar la investigación y captura del ciberdelincuente, para lo cual, el derecho internacional tendría que entrar en acción con el objetivo de elaborar un Convenio Global de Cooperación Común en Materia de Investigación de Ciberdelitos, que brinde a cada país suscriptor los lineamientos adecuados para este tipo de investigación criminal-digital, y donde los países más ricos coadyuven a los países con menos recursos económicos. Lo antes mencionado es sin perjuicio del Convenio de Budapest (2001), su Protocolo, y otros convenios regionales en la materia.

Según el sitio *web* Kaspersky Lab. (s. f.), atendiendo el rol de los ingenieros sociales en la cibercriminalidad, la *ingeniería social* es:

> [...] un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados. [...] debido a la velocidad a la que avanza la tecnología, numerosos consumidores y trabajadores no son conscientes del valor real de los datos personales y no saben con certeza cuál es la mejor manera de proteger esta información.

Con la ingeniería social se pueden realizar actos que afecten a los sistemas, a los procesos y a los usuarios, y parte del poder de los ingenieros sociales radica en la falta de conocimiento o imprudencia por parte de los usuarios de Internet en lo que respecta a la ciberseguridad, *verbigracia*, aceptar en redes sociales amistades de usuarios desconocidos, contestar correos electrónicos catalogados como *spam* y que pueden llevar consigo un *ransomware* (programa que secuestra la información guardada en el disco duro de la computadora o computadoras), ser víctima de estafa telefónica por parte de un *phreaker*, entre otros, lo que representa una vulnerabilidad que da pauta a la comisión de ciberdelitos. En este punto, resulta más peligroso el factor concerniente a la ubicación territorial del ciberdelincuente, quien, como se mencionó antes, puede estar en un país con jurisdicción diferente al de la víctima.

Relacionando la ingeniería social con delitos electrónicos o ciberdelitos transfronterizos, entonces hablaríamos de ingeniería social transnacional. Asimismo, la tipicidad propiamente dicha y la jurisdicción penal encuentran cortapisas. *Verbigracia*, un ciberdelincuente que se encuentre en X país realiza actos de *phishing* (dirigido a varias personas naturales o jurídicas), o *spear phishing* (dirigido a una persona natural o jurídica en particular) y la o las víctimas de este ciberdelito se encuentran o residen en otros países. En este proceso, se pueden plantear muchas hipótesis, poniendo a un lado los principios de la *Lex Mercatoria* o cualquier uso y costumbre mercantil, entre las cuales estarían: a. tomando en cuenta la acción dentro de la teoría del delito, sería competente la jurisdicción del país donde el cibercriminal realiza el acto, siempre y cuando se tipifique dicha acción en el Estado donde se inicia; b. tomando en cuenta el resultado, la jurisdicción competente sería la de las víctimas, es decir, la jurisdicción del lugar donde se dio el resultado, siempre y cuando exista tipicidad; c. si en ningún país existiere una ley que castigue (tipifique) los ciberdelitos, podría aplicarse la del país donde la aplicación utilizada para cometer el acto tiene su domicilio, sede o servidor central. o d. podrían aplicarse normas de *soft law* establecidas en las políticas de privacidad o de protección de datos de cualquiera de los países involucrados (de la víctima, autor o de la aplicación).

La discusión dogmática parte de la jurisdicción, es decir, el país que se arrogaría la investigación, persecución, captura y castigo del o los cibercriminales. Con base en las hipótesis mencionadas, debemos tomar en cuenta el principio *Lex Loci Delicti Commissi*, o Ley del Lugar de Comisión del Delito, por el cual sería la jurisdicción del país donde el ciberdelincuente realizó el envío de los archivos maliciosos *(malwares)* con el objetivo de cometer el delito de *phishing* mencionado, lo que se relaciona con el otro axioma denominado *Locus Regit Actum* (la ley del lugar rige el acto), sin embargo, a las víctimas no se les garantizaría un proceso justo porque, de ser el caso, tendrían que viajar al país donde se juzgará al cibercriminal/ingeniero social. Sin embargo, también se le podría garantizar el acceso a la justicia a través de un ciberjuicio realizado de forma sincrónica por Internet donde los testigos, peritos y demás sujetos procesales tengan acceso a participar vía *on-line*, pero subyugándose a la jurisdicción del juez, que igualmente podría ser un ciberjuez, del lugar donde el ciberdelincuente cometió el

acto, quien dictaría sentencia y graduaría la pena con base a la ley vernácula o, de ser el caso, la ley comunitaria. En fin, podrían aplicarse muchas otras hipótesis debido a la pluralidad de jurisdicciones, dejando claro que este tipo de actos son o serían muy difíciles de perseguir, no así imposibles.

5. REGULACIÓN DE LA TECNOLOGÍA EN LA SOCIEDAD DE LA INFORMACIÓN

5.1. *Convención de Budapest*

El Convenio de Budapest o «Convenio sobre la ciberdelincuencia» del Consejo de Europa es, hasta hoy, el acuerdo internacional de mayor extensión en el tema de la cibercriminalidad per se, cuyo propósito es desarrollar el combate contra el cibercrimen a través de la armonización de la legislación en dicha coyuntura transnacional. Según el sitio *web* Wikipedia, el Convenio y su Informe Explicativo fueron aprobados por el Comité de Ministros de Europa en su reunión número 109 en fecha 8 de noviembre del año 2001. Luego, el 23 de noviembre del 2001, se abrió a firma, y entró en vigor el 1 de julio del año 2004. Posteriormente, el 1 de marzo del año 2006, entró en vigor el Protocolo Adicional a la Convención sobre el Delito Cibernético, cuyo objetivo es penalizar actos xenófobos y racistas cometidos a través de sistemas informáticos.

Dentro de los Principios que dicho Convenio establece en su Preámbulo, podemos mencionar:

> [...] los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas; [...] el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por dichas redes; [...] la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia [...]; [...] la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal; [...] el Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad, y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el Convenio [...].

5.2. *El ciberdelito: una discusión entre el hard y el* soft law

Los delitos cibernéticos son «actitudes ilícitas que se tiene a la cibernética como instrumento o fin». Igualmente «son las conductas típicas, antijurídicas y culpables en las que se tiene a la Cibernética como instrumento o fin» (TÉLLEZ VALDÉZ, 1998, p. 113).

Los ciberdelitos se cometen por medio de Internet con la ayuda de dispositivos electrónicos y generalmente afectan el patrimonio o el honor de las víctimas. En tal sentido, el ciberderecho es la rama que amarra la tecnología y el derecho donde este último tendría la potestad de regular el uso y manejo de las redes sociales, allende de las normas *soft law* que rigen las propias redes sociales. Por ende, el *soft law* se refiere a las reglas de conducta que no tienen una fuerza vinculante, sin embargo, tienen efectos prácticos (PASTORE, 2014).

Siguiendo la misma línea, PASTORE (2014) expresa lo siguiente:

El soft law hace referencia a una serie de fenómenos relacionados a la positivización jurídica y a las prácticas interpretativas en el ámbito del derecho internacional, derecho de la UE y derecho nacional. El soft law desempeña distintas funciones que coexisten con el sistema de hard law. El soft law juega un papel en el ordenamiento jurídico que muestra la gradual diferenciación de su normatividad. (p. 75)

En conclusión, el *soft* y el *hard law* más que repelerse deben como un *joint venture* emprender un camino donde el uno apoye al otro, debido a la eclosión de actos y procesos que dentro del ciberespacio se dan y que de manera concomitante traen consigo una serie de conceptos que antes no se utilizaban, y, por ende, se desconocían y carecían de una regulación ad hoc.

5.3. *Relación entre tecnología y derecho*

La relación entre tecnología y derecho busca cómo establecer una metodología para regular la tecnología, sin perjuicio de auxiliarse de ella. En temas anteriores, se establecieron marcos conceptuales sobre las normas *soft law* que, en detrimento o falta de normas *hard law*, regulan las redes sociales y el andamiaje tecnológico, lo que no quiere decir que el Estado como tal no tenga la facultad de establecer, a través de leyes especiales u ordinarias, preceptos jurídicos que se encaminen a regular u ordenar el uso de las redes sociales en la prevención de los ciberdelitos. El derecho internacional, a través de tratados (allende de los existentes), puede establecer principios con carácter intergubernamental o supranacional basados en el ciberderecho y la informática jurídica, donde se desarrolle un criterio jurídico que delimite una frontera digital o una jurisdicción digital con el objetivo de establecer un tribunal uniforme para los países suscriptores, con la competencia para conocer de ciberdelitos o delitos transfronterizos cometidos por cibercriminales/*crackers*/ingenieros sociales. Dicho tribunal tendría su sede en el país con mejor desarrollo en aspectos de tecnología y sus jueces serían especialistas en cibercrimen y/o ciberderecho. Es la propuesta de creación de un tribunal de justicia que posea la competencia para conocer ciberdelitos y sus efectos análogos, lo que puede ser viable. El tribunal podría ser regional, sin perjuicio de que por ulteriores protocolos adquiera mayor competencia. Igualmente podría crearse un tribunal supranacional en comunidades de naciones como las existentes en la Unión Europea. O convocar a la realización de un convenio global que, incluso, declare como

norma *ius cogens* lo referente a la seguridad en el comercio electrónico a través de Internet y uso de las TIC, como antes se mencionó.

6. EL *SOFT LAW*: FUNDAMENTOS Y APLICACIÓN

6.1. *El* soft law: *una regulación no vinculante*

Las normas de *soft law* relacionadas con la regulación *sui géneris* de las redes sociales y demás tecnologías deben coexistir con el *hard law* o conjunto de leyes que conforman los ordenamientos jurídicos, de lo contrario se podría ocasionar un conflicto entre ambos sistemas, siempre tomando en cuenta que la potestad del Estado está por encima de cualquier norma de *soft law.* Asimismo, las normas de *soft law* establecen las políticas internas de las redes sociales como forma de autorregulación debido a que los Estados han, hasta cierto punto, permitido esta «anarquía digital», lo que ha dejado en situación de atipicidad ciertos actos que afectan bienes jurídicos protegidos. *Verbigracia*: el *grooming*, el *phishing*, el *carding*, entre otros, no están tipificados como ciberdelitos en muchas legislaciones latinoamericanas, incluso anglosajonas.

Sin embargo, el uso del *soft law* se reputa de carácter funcional con normas destinadas a regular determinados sectores, es decir, viene a ser un instrumento regulatorio alterno debido a la ausencia de regulaciones provenientes de las propias Constituciones o del derecho positivo (PASTORE, 2014)

De algo hay que estar seguros: las amenazas/delitos como se conocen (robo con fuerza en las cosas, con intimidación, hurto simple o agravado, entre otros) hoy han evolucionado a través de la tecnología a robo, hurto o estafas cibernéticas/electrónicas, y se les ha designado *phishing, carding, vishing*, lo que nos indica que, a futuro, nos enfrentaremos a mayores amenazas *sui géneris* y más peligrosas, lo que impulsará a los gobiernos a crear leyes/normas más fuertes que las combatan, siendo esto uno de los principales retos en la era digital, sin perjuicio de la unión de los Estados, de forma regional o mundial inclusive, en la lucha contra la cibercriminalidad.

En Nicaragua, por ejemplo, desde la puesta en marcha de leyes como la Ley 787 o Ley de Protección de Datos Personales (2012), se crearon instituciones que, en la vía administrativa, garantizan al administrado la justa recopilación y manejo de sus datos; sin embargo, aún dichas instituciones materialmente no funcionan, por lo que la Sala Constitucional de la Corte Suprema de Justicia ha dicho que tiene competencia para conocer situaciones conexas a través del Recurso de Hábeas Data, actualmente vigente en Nicaragua por medio de la Ley de Justicia Constitucional (2018), enfocado en proteger la autodeterminación informativa. Igualmente, Nicaragua ostenta de una Ley de Ciberdelitos, Ley 1042, aprobada el 27 de octubre del 2020, en la cual se establecen una serie de delitos cibernéticos los cuales se enfocan en la protección del principio de la autodeterminación informativa, entre otros. El país está irrumpiendo

en la materia, lo cual es loable para su ordenamiento jurídico, y a futuro se espera que ratifique la Convención de Budapest, sin perjuicio de los demás Convenios de Cooperación que ha ratificado a través de la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB), tal es el caso del Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia, del 28 de mayo del 2014, entre otros.

Y respecto a la Ley Especial de Ciberdelitos, SÁNCHEZ (2020) expresa que «A diferencia de las experiencias regionales [...] Nicaragua carece de un marco jurídico que fortalezca la capacidad y aptitud de los órganos policiales, fiscalías y poder judicial, para la correcta implementación de esta normativa especializada, tal como lo recomienda el Convenio de Budapest [...]».

6.2. *El Estado liberal: la transformación de la Administración Pública*

Los Estados, desde las Administraciones Públicas, están dando pasos hacia una Administración digital, en la cual los usuarios interactúan con *chatbots*, con programas informáticos o algoritmos, lo cual ha tenido su inyección financiera por parte de organismos de cooperación o de países desarrollados, como en el caso de Nicaragua en la modernización del sistema de registros públicos, por ejemplo, y en otros países de la región centroamericana. Igualmente, este desarrollo digital en la Administración Pública interna ha ocasionado que los Estados se cohesionen o relacionen más, lo que puede facilitar los convenios o tratados de cooperación en materia del combate directo al ciberdelito o regulación del comercio electrónico.

En lo que respecta a los cambios que está experimentando la Administración Pública, el doctor Luciano PAREJO (2012) colige:

> Esta transformación del Estado nacional clásico «hacia afuera» ha ido acompañada de un conjunto de complejos procesos en el orden interno. Pero sin olvidar que ello no impide el paralelo desarrollo, lento pero progresivo, de normas y regulaciones transnacionales o derivadas de una específica cooperación regulatoria internacional, particularmente en campos como los de la seguridad, asistencia a países en desarrollo, protección ambiental, sistema financiero, telecomunicaciones, comercio de productos y servicios, propiedad intelectual, relaciones laborales, migración e, incluso y con carácter general, el cumplimiento mismo de las Leyes. Y con tal desarrollo, el surgimiento del que comienza a denominarse Derecho administrativo global o internacional, el cual, por sus consecuencias en los Derechos administrativos de factura nacional o supranacional, comienza a ser objeto de atención y estudio. (p. 31)

Sin embargo, hoy en día hasta cierto punto, las normas *soft law* se asemejan a las de *hard law*, por la inmensa cantidad de procesos que existen derivados del comercio internacional, de las tecnologías de la información y de Internet. «En efecto, cada vez es más complicado distinguir la línea que separa el *hard*, del *soft law*, sobre todo

porque es extraño encontrar a los instrumentos de ésta última clase, en forma aislada» (PULIDOS RIVEROS, 2018, p. 227).

Igualmente, PULIDO RIVEROS (2018) expresa:

> Para el Derecho Privado, es tanta la importancia de ese tipo de instrumentos de soft law, que aludiendo a los Principios de UNIDROIT, a los Principios del Derecho Contractual Europeo —PDEC o PECL—, al Draft Common Frame of Reference (DCFR), a los Trust Principles, a la Insurance Initiative, y a los Principles of European Tort Law, Magnus (2012) expresa que esos cuerpos normativos se han influenciado, dándose justo como huevos, puestos uno después de otro, y cada uno comprende una codificación comprensiva en su respectivo campo. (p. 233)

SARASÍBAR IRIARTE (2019), por su parte, refiriéndose a dicha interacción y a la necesidad de que el derecho regule los aspectos de inteligencia artificial, nos expresa lo siguiente:

> El interés del jurista se genera por la entrada de los robots en ambientes cotidianos y por la variedad de relaciones que de ellos se derivan. Esto va a suponer una nueva revolución y el legislador debe reflexionar sobre estas cuestiones y las consecuencias que de la coexistencia robots-humanos se derivan. Y evidentemente, la regulación no debe obstaculizar la innovación, pero también es evidente que el Derecho tiene que intervenir para regular esta nueva realidad. Habrá que buscar el equilibrio, como en todo. (p. 382)

Y para terminar, refiriéndonos al precitado *soft law*, fundamental a lo largo del presente artículo de investigación, según CALDERÓN MARENCO (2017), la *Lex Mercatoria* y el *soft law* han salido a relucir como alternativa al tradicional derecho duro o *Hard Law*. «Con el paso del tiempo el Derecho suave *(Soft Law)* ha ido adquiriendo mayor protagonismo en el escenario jurídico internacional, posicionándose como un instrumento del que gozan las partes para regular sus transacciones internacionales, aunque carezca de efectos vinculantes» (CALDERÓN MARENCO, 2017, p. 3). Por su parte, PULIDOS RIVERA (2018), citando a ARRUBLA PAUCAR (2005, p. 60), dice: «El derecho comercial es un derecho de tráfico económico y lo que le ofrece al empresario, y a la vida económica, son los instrumentos para que la comercialización pueda desplegarse; [...] evitando en lo posible, el menor número de conflictos entre las personas [...]»

Más allá, refiriéndose al *soft law*, en su aplicación material en el campo de los conflictos atinentes al comercio internacional, sin perjuicio de otras actividades de derecho privado, PULIDOS RIVERA (2018) comenta que el *soft law* encuentra su máximo apoyo en el arbitraje. Y, en tal línea, CALDERÓN MARENCO (2018) expresa que la *Lex Mercatoria* y el *soft law* gozan de gran preferencia entre los comerciantes por la libertad y la flexibilidad que otorgan por la oportunidad de elegir un derecho distinto al de las legislaciones nacionales.

Finalmente, lo que se busca es la convivencia social armónica y la paz, desde y en la sociedad de la información, la cual ha evolucionado de la interacción personal hacia la interacción digital en un mundo virtual denominado ciberespacio donde, de una u otra manera, todos y todas deberíamos tener nuestro lugar, sin exclusión.

7. CONCLUSIONES

1. La tecnología se relaciona con el derecho porque la primera ha cohesionado a la humanidad, permitiendo que las personas interactúen a mayores escalas, y en dichos procesos suceden o pueden suceder conflictos. NO existen en la actualidad fronteras digitales en el ciberespacio, por ende, el mismo es holístico y global. El Estado liberal, desde 1789, evolucionó desde la Edad Contemporánea hacia un punto donde hoy podría reputarse como Estado digital o digitalizado por el crecimiento del uso de las TIC dentro de la Administración Pública, sin perjuicio del avance de la diplomacia digital. Los ciberdelitos son riesgos para quienes navegan en Internet, sin distingo de ninguna clase, y la atipicidad de los mismos en ciertos países puede conducir a impunidad y afectación del patrimonio de los comerciantes y/o consumidores dentro del comercio electrónico, sin perjuicio de afectar otros bienes jurídicos protegidos.
2. El derecho internacional público, a través de convenios como el de Budapest (2001), entre otros, ha puesto en marcha principios básicos en la lucha contra el cibercrimen. Sin embargo, la pluralidad jurisdiccional internacional se puede considerar una cortapisa en la lucha contra el cibercrimen, debido a que un ciberdelito, más allá de la teoría propia del delito, puede realizarse desde un lugar lejano al cual se encuentra la víctima, y la investigación, detección y detención/arresto de un cibercriminal es más difícil debido a la falta de presencia física del autor en el momento de la comisión y/o resultado. Personas naturales y/o jurídicas, incluyendo al mismo Estado, son susceptibles de ser víctimas de acciones/actos ilícitos en el ciberespacio porque en Internet navegan miles de millones de usuarios, y los cibercriminales pueden utilizar una identidad digital falsa para engañar y afectar a cualquier cibernauta o ciberconsumidor, en el actual mercado electrónico/digital. Es, aplicando equivalencia funcional desde un delito común, un acto típico y antijurídico entre ausentes.
3. No tenemos identidad digital por defecto, sino que la construimos en la Red. Por ello, de nosotros mismos depende, en gran parte, la seguridad que tengamos al navegar por el ciberespacio, sea en una red social, correo electrónico, o realizando una transacción comercial o comercio electrónico per se a través de mensajes de datos.
4. El ciberderecho puede establecer como una de sus ramas el derecho digital internacional con el cual, desde un punto de vista teleológico, se podrían instituir jurisdicciones digitales.
5. La tecnología está presente en casi todo el planeta, aun en países en vías de desarrollo en la actual sociedad de la información, lo que intuye que vamos hacia una ciberdemocracia, donde nos gobernarán robots y no necesariamente personas físicas o naturales. Esto implicaría un desarrollo tal de la inteligencia artificial donde los robots no serían los que reciban órdenes, sino quienes las den.

6. La ingeniería social es el conjunto de actos realizados por personas denominados *crackers* o *black hat hackers* o ingenieros sociales, quienes cometen los ciberdelitos vernáculos o transfronterizos utilizando primordialmente la tecnología y luego la persuasión.
7. Aceptar las denominadas *cookies* al entrar a navegar en un sitio *web* obliga al usuario a ceder parte de su derecho a la autodeterminación informativa para que este sitio *web* procese sus datos (correo electrónico) con fines publicitarios y de marketing.
8. Las redes o programas informáticos que son los que tienen y procesan datos personales, tienden a «evolucionar» hasta el punto de traficar con dichos datos sin el consentimiento expreso del titular violentando la autodeterminación informativa.
9. Aplicando la teoría de la evolución, *estamos pasando de la selección natural a la selección digital*, donde los más vulnerables, es decir, aquellos que desconozcan cómo vivir e interactuar en el ciberespacio, serán los mayores afectados o, simplemente, no podrán sobrevivir en el mismo. En este punto, hablamos también de analfabetismo digital.
10. Se puede elaborar un Convenio Global de Cooperación Común en Materia de Investigación de Ciberdelitos y de Comercio Electrónico, donde los países más ricos coadyuven a los países con menos recursos económicos en la lucha contra el cibercrimen y el fortalecimiento de la protección de las transacciones electrónicas.
11. El *soft law* desde el derecho comunitario, por ejemplo, puede coadyuvar a establecer directrices justas para todos los países de las regiones en el ámbito de las TIC, y la regulación de las mismas a través del derecho digital/ciberderecho, lo que a futuro ayude a las naciones a crear leyes apropiadas y más modernas que regulen la institución jurídica que se investiga.
12. La pandemia del COVID-19 fortaleció los aspectos del distanciamiento social, y evolucionó el acercamiento digital vigorizando el cibertrabajo o teletrabajo, la ciberenseñanza o educación a distancia, la cibercomunicación, entre otros. Por ello, el corolario es que, a mayor distanciamiento social, mayor es el acercamiento digital.

8. BIBLIOGRAFÍA

BASSANTE, D. s. f.: «Diplomacia Digital. Las relaciones internacionales en tiempos de Twitter y Facebook», https://www.afese.com/img/revistas/revista59/diplodig.pdf [28 marzo 2022].

BRYSON J. s. f.: «La última década y el futuro del impacto de la IA en la sociedad», https://www.bbvaopenmind.com/articulos/la-ultima-decada-y-el-futuro-del-impacto-de-la-ia-en-la-sociedad/ [15 julio 2021].

BUSTAMANTE DONAS, J. s. f.: «La cuarta generación de derechos humanos en las redes digitales». *Telos*, https://telos.fundaciontelefonica.com/archivo/numero085/la-cuarta-generacion-de-derechos-humanos-en-las-redes-digitales/ [10 septiembre 2021].

CALDERÓN MARENCO, E. 2017: *Los incoterms como instrumento de derecho suave (soft law)*. Universidad Centroamericana (UCA). Nicaragua.

CALDERÓN MARENCO, E. 2018: *Lex Mercatoria como Derecho Aplicable a la Compraventa Internacional de Mercaderías en el Derecho Positivo Nicaragüense*. Tesis doctoral. Nicaragua: Universidad Centroamericana (UCA).

CLERC, C. 2013: «El Derecho Internacional Privado y los procesos globalizadores». *Revista Prolegómenos. Derechos y Valores*, 2013, 16: 32, 15-30. Colombia.

ESCUDERO, A. 2009: «La Revolución Industrial: una nueva era». *Grupo Anaya S.A.* ISBN: 978-84-667-8675-1, https://adultosmayores.unr.edu.ar/wp-content/uploads/2020/04/Antonio-Escudero.pdf [12 septiembre 2021].

GUERRERO MAYORGA, O. 2018: «El Jus Cogens la Grand Norm del Derecho Internacional». *Revista de Derecho de la Facultad de Ciencias Jurídicas y Sociales*, 2018, vol. 2. UNAN-León.

LEE, D. 2015: *Manual de Seguridad para Prevención de Delitos*. México: Grupo Paladin, S. A. de C. V.

MARONGIU, D. 2018: «Inteligencia artificial y administración pública». En . R. Torres Carlos, A. Garrido Juncal, J. M.ª Miranda Boto y C. García Novoa (dirs.): 4.ª Revolución Industrial: Impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital. ed. Thomson.

PAREJO ALFONSO, L. 2012: Lecciones de Derecho Administrativo. 5.ª ed. Valencia, España: Tirant lo Blanch.

PASTORE, B. 2014: «Soft Law y las Teorías de las Fuentes del Derecho». *Soft Power*, enero-junio, 2014, 1(1). Università degli Studi di Ferrara.

PEÑA VALENZUELA, D. s. f.: «Lex Electrónica: ¿mito o realidad? Perspectiva desde la contratación por medios electrónicos». *Revista de la Propiedad Inmaterial*, https://revistas.uexternado.edu.co/index.php/propin/article/view/1152/1093 [30 agosto 2021].

PEREIRA COUTINHO, L. 2012: «El Desarrollo de la Supranacionalidad. Algunos apuntes». *ReDCE*, año 9, julio-diciembre 2012, 18: 199-2013.

PULIDO RIVEROS J. 2018: «El 'Soft Law' en el Derecho Privado: Sostén a la Teoría de la nueva *'Lex Mercatoria'*». *Revista Misión Jurídica*, enero-junio de 2018, 11(14): 223-259. DOI: https://doi.org/10.25058/1794600X.917 [10 agosto 2021].

QUEVEDO GONZÁLEZ, J. 2017: *Investigación y prueba del ciberdelito. Programa de Doctorado en Derecho y Ciencia Política. Línea de Investigación: Derecho Procesal*. Universitat de Barcelona.

QUISPE REMÓN, F. 2012: «Las normas de ius cogens: ausencia de catálogo». *Anuario Español de Derecho Internacional*, 2012, 28: 143-183. ISSN 0212-074.

RAMOS, R. 2011: «La Supranacionalidad en la Unión Europea. Comparación con el Proceso Centro Americano de Integración». *La Revista de Derecho*, 2011, 32. DOI: https://doi.org/10.5377/lrd.v32i0.1249 [9 septiembre 2021].

RODRÍGUEZ GARCÍA, J. A y MORENO REBATO, M, 2018: «¡El futuro ya está aquí! Derecho e Inteligencia artificial». *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2018, 48.

RODRÍGUEZ FERNÁNDEZ, M. 2012: «Reconocimiento de la *lex mercatoria* como normativa propia y apropiada para el comercio internacional». *REVIST@ e-Mercatoria*, julio-diciembre 2012, 11(2).

SÁNCHEZ, S. 2020: «Nicaragua y su iniciativa de ciberdelitos», https://www.ipandetec.org/2020/10/08/nicaragua-ciberseguridad-ley/ [29 agosto 2021].

SARASÍBAR IRIARTE, M. 2019: «La Cuarta Revolución Industrial: el Derecho Administrativo ante la inteligencia artificial». *Revista Universidad Pública de Navarra*, 2019, 115: 377-401.

TÉLLEZ VALDÉS, J. 1998: «Delitos Cibernéticos». *Revista Iberoamericana de Derecho Informático*, 1998, 27-29: 113-122.

TÉLLEZ VALDÉS, J. 2008: Derecho Informático. 4.ª ed. México: Mcgraw-Hill.

TREJO GARCÍA, E. *et al*. 2006: «Sistema de Recepción de los Tratados Internacionales en el Derecho Mexicano». *Dirección General de Bibliotecas. Servicio de Investigación y Análisis. Cámara de Diputados, Estados Unidos Mexicanos*, http://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-07-06.pdf [4 septiembre 2021].

VERA RAMÍREZ, H. 2018: «Apuntes sobre el comercio exterior y la moneda durante la época del emperador Justiniano!. *Revista Tiempo y Economía. Universidad de Bogotá Jorge Tadeo Lozado*, 2018, 5(1). Colombia.

Convenios internacionales

Consejo de Europa. 2001: *Convenio sobre la Ciberdelincuencia.* Budapest, 23 de noviembre de 2001, https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf [25 julio 2021].

Consejo de Europa. 2003: *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*. Estrasburgo, 28 de enero de 2003, https://www.plataformaong.org/conferencia/wpcontent/uploads/2014/10/Protocolo_adicional_convencion_cibercrimen.pdf [28 julio 2021].

Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB). 2014: *Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia*. Madrid, 28 de mayo del 2014, https://www.segib.org/paises-iberoamericanos-firman-en-madrid-convenio-y-recomendacion-sobre-ciberdelincuencia/ [2 agosto 2021].

Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) con su nuevo artículo 5 bis aprobado en 1998. Fecha de adopción: 12 de junio de 1996 (el artículo 5 bis suplementario fue adoptado en 1998), https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_commerce [22 septiembre 2021]

Webgrafía

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD). 2021: *El comercio electrónico mundial alcanza los 26,7 mil millones de dólares mientras COVID-19 impulsa las ventas en línea*, https://unctad.org/es/news/el-comercio-electronico-mundial-alcanza-los-267-mil-millones-de-dolares-mientras-covid-19 [25 septiembre 2021]

DocuSign. 2021, 28 de enero:) *Economía digital: ventajas y desventajas*, https://www.docusign.mx/blog/economia-digital [17 septiembre 2021]

Gobierno de las Canarias. s. f.: *Identidad digital. La identidad digital en la sociedad de la información*, https://www3.gobiernodecanarias.org/medusa/ecoescuela/ate/ciudadania-y-seguridad-tic/identidad-digital/ [25 septiembre 2021].

Historia de las Redes Neuronales, desde 1950 a 2018, 2018, https://www.aprendemachinelearning.com/breve-historia-de-las-redes-neuronales-artificiales/ [3 junio 2021].

Informática y derecho: Revista Iberoamericana de derecho informático, 27-29, https://dialnet.unirioja.es/servlet/articulo?codigo=248139 [25 mayo 2021].

Kaspersky Lab. s. f.: *Consejos para protegerse contra el cibercrimen*, https://latam.kaspersky.com/resource-center/threats/what-is-cybercrime [18 septiembre 2021].

Organización para la Cooperación y el Desarrollo Económicos (OCDE). 2019: *Panorama del comercio electrónico Políticas, Tendencias y Modelos de Negocio*, https://doi.org/10.1787/23561431-en [23 septiembre 2021].

Real Academia Española. s. f.: «Autonomía conflictual». En *Diccionario Panhispánico del Español Jurídico*, https://dpej.rae.es/lema/autonom%C3%ADa-de-la-voluntad-conflictual [14 septiembre 2021].

Ródenas Abogados. s. f.: *Qué es el Ciberderecho*, https://www.rodenasabogados.com/ciberderecho/ [22 septiembre 2021].

Legislación

España. Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 6 de diciembre de 2018, n.º. 294, https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673&tn=2&p=20210527

Asamblea Nacional. (2012). Ley n.º 787. Ley de Protección de Datos Personales. Aprobada el 21 de marzo del 2012. *La Gaceta* del 29 de marzo del 2012. n.º. 61. Nicaragua.

Asamblea Naciona.l (2018). Ley 983. Ley de Justicia Constitucional. Aprobada el 11 de diciembre de 2018. *La Gaceta* del 20 de diciembre de 2018, n.º 247. Nicaragua.

Asamblea Nacional. (2020). Ley 1042. Ley Especial de Ciberdelitos. Aprobada el 27 de octubre del 2020. *La Gaceta* del 30 de octubre del 2020, n.º. 201. Nicaragua.

Jurisprudencia

Sentencia del Tribunal Supremo 815/2020 (Sala de lo Contencioso Administrativo Sección 3.ª) de 18 de junio del 2020. (Recurso 1074/2019). Recuperado de: https://www.poderjudicial.es/search/