

# EDI Joven

Revista Digital Distribución gratuita

AGOSTO 2020 | EDICIÓN 35



EDI JOVEN

Adonde vas vos?

ElDerecholInformatico.com



Vamos...



ELDERECHOINFORMATICO.COM

# ÍNDICE

<i>Editorial</i>	<b>5</b>
<i>El Habeas Data en Venezuela como única alternativa a la protección de datos personales - Mary Raquel Duque</i>	<b>7</b>
<i>Alerta PHISHING! Estás a un clic de morder el anzuelo - Maria José Quintana</i>	<b>13</b>
<i>La fake democracy y el proyecto de ley brasileño contra las fake news - Leonardo de Andrade Alberto</i>	<b>16</b>
<i>Los contratos eletrónicos: riesgos y conflictos en el derecho - Victor Aldair Mejia Molina</i>	<b>22</b>
<i>Derecho a la desconexión digital - Emilse María del Milagro Tabera Cabrera</i>	<b>27</b>
<i>Derecho al honor e inteligencia artificial - Darío Echeverría Muñoz. Msc, LL.M</i>	<b>31</b>
<i>Grooming, el día después - Vanina Kandyba</i>	<b>37</b>
<i>Grooming, un delito que crece día a día en pandemia - Yamila Arriaga / Aisha Loreley Quiroga</i>	<b>41</b>
<i>Hacia una estandarización de la firma electrónica en Latinoamerica - José Gallegos</i>	<b>45</b>
<i>Inteligencia artificial en el Derecho Internacional público y las relaciones internacionales - Maiger Dalay Urbina Romero</i>	<b>51</b>
<i>Las tecnologías de la información y comunicación y el pluralismo jurídico - Gardenia Revollo</i>	<b>57</b>
<i>Reconocimiento de las comunicaciones electrónicas y el comercio electrónico - Manolo Rivera</i>	<b>63</b>



LA RED

EL DERECHO INFORMATICO

UNA LLUVIA DE  
INFORMACIÓN EN  
TU VIDA





Guillermo M Zamora - Director

## REVISTA DIGITAL EDI

(Fundación con personería en trámite)

## DISTRIBUCIÓN GRATUITA

prohibida su venta o reproducción

## INFO DE CONTACTO

twitter: @elderechoinf

Instagram: @elderechoinformatico

youtube.com/c/elderechoinformatico

facebook.com/elderechoinformatico

Email: info@elderechoinformatico.com

dirección: 9 de Julio 585 Of 2

Trelew / Chubut / Argentina

# EDITORIAL

Una edición especial de la revista de La Red, en esta oportunidad, está conformada por artículos escritos en su totalidad por integrantes de la rama Joven de EDI.

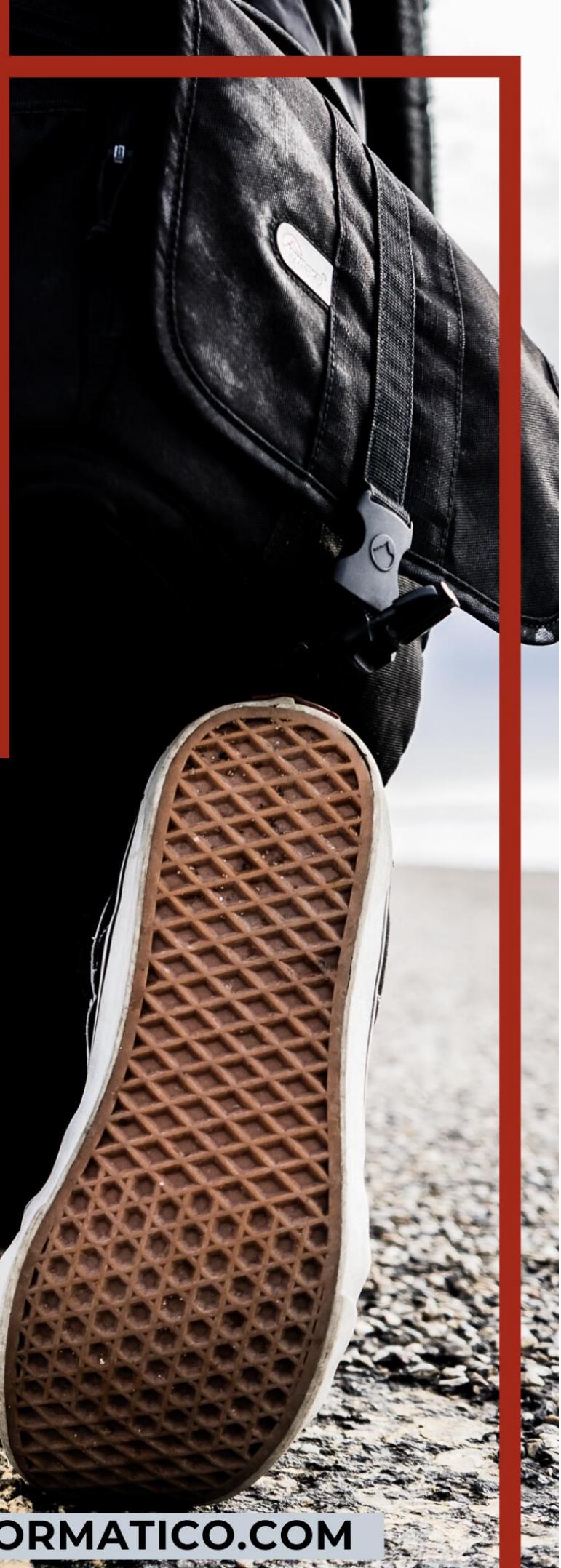
En tiempos donde no nos debe apenar decir que extrañamos los afectos, que deseamos poder vernos cara a cara y compartir los after de los congresos, este grupo de jóvenes promesas del derecho informático, se han propuesto hacer ruido y generar movimiento, no quedarse con las ganas de ir preparando su camino.-

El 22 y 23 de Septiembre estarán al frente del CONGRESO LOCALEMIA JOVEN DE DERECHO Y TECNOLOGÍA, mientras tanto coordinarán 3 campañas de concientización en el uso de tecnología, estarán promoviendo el conocimientos a través de programas para el canal de Youtube de EDI y Podcast donde estarán contándoles sus ideas, proyectos, y fundamentos.-

Desde EDI estamos lanzando en Octubre junto con la Universidad de Tachira (Venezuela) un curso de actualización de 11 módulos con docentes de toda Iberoamerica, luego se vendrán los Destacados y algunas ediciones especiales de esta Revista.-

Extraño los reencuentros, los abrazos y las risas en mi oido, mientras tanto, hagamos lo imposible por mantenernos en contacto, porque las pantallas son frias, pero no nuestros deseos.-

# VAMOS DEJANDO HUELLA



# El *Habeas Data* en Venezuela como única alternativa a la protección de datos personales

Autora: Mary Raquel Duque

Conocer quiénes tienen acceso a nuestra información personal es un tema incierto. En el mundo, hasta hace poco carecía de importancia determinar a quién entregamos nuestros datos personales; qué hacen con ellos y qué tan importante es para quien los obtiene y detenta.

La Constitución de la República Bolivariana de Venezuela (CRBV) en su artículo 28, indica que cada persona tiene derecho de acceder a su información



personal, solicitar rectificación, destrucción o actualización al tribunal competente; mostrando también y muy ampliamente, que podrá accederse "... a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas..."<sup>1</sup>.

El artículo 60 del mismo texto normativo, nos habla acerca de la protección de nuestra vida privada, de nuestra imagen y los límites que debe tener la informática para la garantía de estos derechos como el honor y la intimidad.

La Carta Magna Venezolana data del año 1999, han pasado desde entonces, dos décadas de avance tecnológico e informático, con cambios estructurales a nivel mundial y local. Luego del auge tecnológico diversos países de Latino América han promulgado leyes que regulan la nueva era de la información; sin embargo - y como posteriormente se ampliará - en este país no se avanzó demasiado en esta área.

Día a día interactuamos en distintas plataformas, aplicaciones,

<sup>1</sup> Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N° 36.860 de fecha 30 de diciembre de 1.999.

empresas, instituciones y proveemos nuestro documento de identidad, nuestro género, nuestra edad, pero no todos estamos en conocimiento de que esa información personal que suministramos tiene un valor económico, que, en la peor de las situaciones, puede representar un riesgo si cae en manos equivocadas.

Los datos personales no solo tienen información genérica sino también sensible, que puede afectar nuestra esfera más privada e íntima, siendo susceptibles a ser manipulados con fines comerciales, laborales o políticos.

Uno de los ejemplos más importantes de este suceso en Venezuela, fue la publicación de la denominada "lista Tascón", un hecho que vulneró los principios de intimidad y privacidad de la información. Los datos que contenía dicha lista eran de ciudadanos que solicitaban activar el referéndum revocatorio contra el fallecido presidente, Hugo Chávez, en el año 2003.

Esta petición que se realizó formalmente ante el Consejo Nacional Electoral (CNE), no obtuvo una respuesta favorable para los firmantes, pero dichas listas fueron publicadas por el entonces diputado, Luis Tascón, en la página web <https://listadetascon.com/><sup>2</sup>-que

posteriormente se amplificó con el software Maisanta y que actualmente se encuentra activa- obteniendo huella digital, nombres, apellidos, género, número de documento y dirección de los firmante.

En consecuencia, los altos dirigentes políticos y jefes de oficinas públicas ingresaban los datos de sus empleados y si estos aparecían en esta web, eran despedidos debido a su preferencia política, evidenciándose una discriminación notoria, gracias a la divulgación de información sensible, como lo es la ideología política.

Por consiguiente, cualquier persona podría ser víctima de discriminación y vulneración, al proveer datos sensibles, sin asegurarnos el cumplimiento del tratamiento de nuestros datos personales; debiendo existir una cierta cantidad de principios, bases y procedimiento que garanticen el derecho a su protección.

Ciertamente, la mayoría de las personas no conocen los posibles riesgos que existen al compartir los datos personales en Internet, muchos de nosotros no sabemos que todos los datos que compartimos son de nuestra propiedad y que tenemos derecho a pedir que no sean difundidos,

<sup>2</sup> En fecha 30/01/2004 El presidente Hugo Chávez, autorizo mediante misiva a Luis Tascón a retirar copias certificadas de las planillas

utilizadas durante el evento 2-A, ocurrido entre el 28/11/2003 y 01/12/2003.

cambiados o compartidos con terceros.

No sólo es la obtención sino también la importancia de la obligatoriedad de dar el consentimiento expreso para el uso de estos. Los datos personales como un conjunto sirven para localizarnos, identificarnos y contactarnos, poseen nuestros nombres, apellidos, teléfonos, correo electrónico, nacionalidad, sexo y documento de identidad, que hacen un conglomerado de información que nos define, adquiriendo así nuestras cualidades y nuestra identidad.

### **¿Qué derechos al día de hoy tienen los venezolanos sobre sus datos personales?**

En referencia a esto, se puede decir que, la única alternativa para la protección de los datos personales es la mencionada en el artículo 28 de la Constitución, que prevé lo que se conoce mundialmente como *Habeas Data*, una institución jurídica constitucional y que fue un hecho normativo que se implementó en la región en los años 2000, cuando la era digital no contaba con el auge que tiene en la actualidad. El *Habeas Data*, se recoge e implementa inspirado en la Declaración Universal de los Derechos Humanos, exigiéndose por parte de la Comisión Interamericana de DDHH que: todo ciudadano posee la garantía del acceso a la información sobre sí mismo, contenida en archivos públicos o privados, pudiendo acceder para eliminarla, actualizarla o suprimirla.

Entonces, el *Habeas Data* es el derecho que tienen los individuos a sus datos personales y a solicitar a los órganos jurisdiccionales la modificación, actualización o eliminación de estos. La figura conlleva en sí misma, un proceso engorroso, difícil de acceder y mantiene un número casi mínimo de acogida favorable por el justiciable.

Es importante mencionar que, esta figura constitucional no tiene por finalidad emitir una nulidad o exigir una indemnización, sino que se encuentra para que el Estado interfiera, pero no se obtiene un dictado de sanciones pecuniarias, ya que, el Amparo Constitucional es una vía extraordinaria para garantizar derechos.

De lo anteriormente mencionado, en cuanto a la amplitud que prolifera en el artículo 28 de la CRBV, no es del todo cierta, ya que, mediante el fallo nº 332 de fecha 14 de marzo de 2001 el Tribunal Supremo de Justicia (TSJ) en Sala Constitucional, sobre el caso INSACA, indicó expresamente que el acceso, rectificación o eliminación de los datos personales, no procede en si sobre “(...) cualquier tipo de información almacenada en la variedad de archivos y registros con

*los que cuenta nuestro país (...)"<sup>3</sup>* pues, infiere el máximo tribunal que, de la lectura del articulado, este no se aplicaría a expedientes personales de orden laboral, o a datos sueltos, o a diarios, sino aquellos que cuenten con registros oficiales sea de forma informática o no y, con codificaciones en series, es decir, solo aquellos datos que en sí, engloben un perfil completo del individuo, dejando de lado que, si tenemos varios datos, podría obtenerse una identificación del mismo, pues no se va a extender este derecho a los datos que sean para fines de estudio, estadístico, consumo propio para satisfacer necesidades espirituales o culturales, no formando parte del accionar por medio del *Habeas Data*.

Mediante el fallo N° 182 de fecha 08 de marzo del 2005<sup>4</sup>, el máximo tribunal se pronunció acerca de la diferencia entre el *Habeas Data* y un Amparo Constitucional, que a través del Amparo no se pueden constituir derechos, sino únicamente se busca restablecerlos, sin embargo, el *Habeas Data* no procederá cuando se hayan lesionado los derechos que contiene el artículo 28, ni cuando estos revistan una violación concreta.

Entendamos que las medidas jurisprudenciales tomadas, no son suficientes para delimitar y proveer

de procedimientos que permitan efectivamente proteger nuestros datos, para ejercer la acción de *Habeas Data*, necesitaría el interesado en los datos probar la existencia del registro que lo detenta, para poder el Juzgador emitir una orden judicial y solicitar la exhibición de esos archivos, parecería entenderse como un Derecho fácil de ejercer, sin embargo, esto no es así, ya que en los procesos de amparo se debe cumplir con formalismos tanto de fondo como de forma, y que no se traducen en requisitos simples, sino engorrosos y burocráticos, ya que, para el ejercicio de un amparo de este tipo, se debe cumplir con la Ley Orgánica de Amparo sobre Derechos y Garantías.

El Registro Civil, es un órgano que funge como banco público de hechos importantes como nuestro nacimiento, y con este una gran cantidad de información sensible que, como dijimos anteriormente, en manos equivocadas puede vulnerar nuestros derechos. El órgano rector del Registro Civil es el CNE, tal como lo indica en el artículo 19 de la Ley Orgánica de Registro Civil, pese a esto, comparten información como cooperadores: el Ministerio de Relaciones Interiores y de Justicia

<sup>3</sup>

<http://historico.tsj.gob.ve/decisiones/scon/Marzo/184-24310-2010-09-1109.html>

<sup>4</sup>

<http://www.tsj.gob.ve/es/web/tsj/decisiones#>

(SAREN)<sup>5</sup>, el Ministerio para la Salud y el Ministerio con competencia en los Pueblos y Comunidades Indígenas, es decir, el Estado venezolano es uno de los bancos de información pública más completos, ya que, en estas instituciones depositamos nuestra información. Obtienen datos personales ilimitados, pues los cooperadores tienen información sobre nuestras transacciones inmobiliarias, nuestra salud, entre otros datos que son sensibles.

Estos derechos tan importantes en la actualidad no han sido desarrollados, teniendo como opción la jurisprudencia, quien se ha encargado en algunos casos de regular estos derechos por medio de un *Habeas Data*, dictando un procedimiento propio a pesar de esto no garantiza lo primordial, que es el tratamiento de estos datos, su

procesamiento y al castigo con sanciones y repercusiones monetarias, que puedan persuadir de no caer en reincidencia de la violación de estos derechos a los datos personales.

Venezuela, carece de un anclaje normativo que suponga una rectoría formal en la regulación de los datos personales, que proteja la información personal y cuide la intimidad de los sujetos. En las distintas leyes promulgadas, no ha sido imperante legislar pensando en la necesidad de articular en esta materia, evitando a toda costa el tratamiento de los datos y su libre circulación, siendo importante mencionar que, los datos personales no solo circulan a nivel nacional, sino que también se da la venta y transferencia internacional de información.



<sup>5</sup> Ley Orgánica del Registro Civil. Publicado en Gaceta Oficial Número 39.264 de fecha martes 15 de septiembre de 2.009.



CONVERSATORIOS DE  
LA RED

# CHARLANDO CON LOS QUE SABEN

[ELDERECHOINFORMATICO.COM](http://ELDERECHOINFORMATICO.COM)

[YOUTUBE.COM/USER/ELDERECHOINFORMATICO](https://YOUTUBE.COM/USER/ELDERECHOINFORMATICO)

# ALERTA PHISHING! ESTÁS A UN CLIC DE MORDER EL ANZUELO <sup>6</sup>

Autora: María José Quintana

Dentro de los ciberdelitos que se han incrementado más del 80% este último tiempo, la modalidad de phishing es sin duda la vedette de las estrategias de ingeniería social. Es que con la cuarentena y el Aislamiento Social Preventivo y Obligatorio, muchas más personas frecuentan las pantallas de los dispositivos electrónicos y se aventuran en el mundo ciber, sin siquiera sospechar los riesgos que corren, o hasta qué punto se exponen. Se han vuelto presa fácil de quienes están al acecho de información sensible.

La modalidad más común: llega un mensaje de WhatsApp con una increíble oferta que no puedes



rechazar (a quién no le ha pasado?). Algunas veces la excusa es que un gran *mall* regala compras a los primeros cien que se inscriban en un sitio web; otras, una compañía de cosméticos francesa está obsequiando kits de maquillaje... todo eso y mucho más. Sólo con hacer clic en el pequeño link de abajo, llenando un simple formulario. *“Yo pruebo, qué puedo perder?”*

Luego lo más probable es que la víctima quiera compartir esa “gran oportunidad”, con alguno de sus contactos. Suponiendo que te llegó por casualidad y para tener un buen gesto para que alguien más se beneficie, lo reenvía a varios... ahí se viraliza. Esa es otra de las estrategias del atacante: hacer un mensaje atractivo para que los receptores lo comparten rápidamente con muchas personas o grupos, incrementando la posibilidad de que alguien pique el anzuelo.

Lo que muchos no suponen, es que al hacer clic en ese pequeño link bajo la tentadora promesa, han “mordido el anzuelo” de algún ciber delincuente. Porque cuando ingresan en esos sitios que suplantan la identidad de renombradas empresas multinacionales o instituciones

<sup>6</sup> Por María José Quintana Dourado, Abogada, Argentina.

gubernamentales, empiezan a dejar tu **ciber rastro** para quienes anhelan sus datos.

Tras hacer clic normalmente llegan a un formulario que le solicita datos: nombre, apellido, documento, domicilio; correo electrónico, teléfono. Ahí ya está entregando información sensible y valiosa a un grupo de desconocidos, y lo peor es que no hay percepción de riesgo.

La mayoría de las veces que he recibido alguno de estos mensajes trato de alertar al remitente sobre el phishing, diciéndole que no haga clic, que no reenvíe, etc., y la mayoría no lo toman a bien: se sienten ofendidos y dicen cosas como “*perdona, que tont@ he sido*” o “*una vez que quiero regalarte algo me retas*”, lo cual me sorprende bastante, pues no se los ha concientizado aún acerca del valor de sus datos, y del riesgo que supone su entrega.

Como es ampliamente reconocido, la conducta en el mundo cibernético es más imprudente que en el medio físico: tomamos las decisiones más rápido y sin analizar demasiado los riesgos y consecuencias a los que nos estamos exponiendo.



Pensemos por un momento que pasa si te intercepta un desconocido en la calle, y de pronto te solicita muchos datos, se los darías sin dudar o indagarías primero quién es y para qué los necesita?. En cambio, en los casos de phishing como en las ofertas de regalos y promociones, las personas que ingresan al link, no analizan aquello.

Con motivo de la cuarentena, las personas nos volcamos al ciberespacio y ahora todos pasamos muchas más horas pegados a las pantallas, para tareas que antes se hacían “personalmente”. Frente a esto, el Estado debe implementar políticas a través de las instituciones, a fin de no dejar desprotegida a la gran masa de consumidores de redes sociales y aplicaciones de mensajería, que no cuenten con los conocimientos ni el manejo de las herramientas para poder detectar la veracidad de una página. Y claramente este deber de información y educación se extiende

a los servidores de internet, como prestadores del servicio. Estos actores sociales emitiendo una serie de consejos de seguridad y buenas prácticas pueden hacer mucho por los cibernautas.

Muchas veces los ciberdelincuentes usan la metodología del phishing suplantando la identidad de una empresa reconocida, y así se hacen directamente de los números de cuenta y claves de sus víctimas, para cometer fraudes y robarles sus cuentas.

Otras el phishing es usado como un acto preparatorio de otro delito, como puede ser el de estafa, por ejemplo. Formando parte de mecanismos de obtención de datos como la ingeniería social, práctica que consiste en obtener información importante, sensible e íntima de las personas, para luego usarlas en su contra o manipularlas, finalmente para obtener un beneficio económico.

Así cuantos más datos obtenga quien pretenda cometer una estafa, más verosímil sonará al teléfono. El siguiente paso será contactar a la víctima, mayormente de manera telefónica, para pedirle sus datos. Pero el que está al otro lado del teléfono sabe mucho sobre la víctima ya, y entonces el nivel de sospecha se reduce, y el argumento se vuelve más creíble.

Esta metodología cada vez se sofistica más y aprovecha la variedad de personas a las que pueden llegar, sobre todo las

personas mayores, recientemente integradas al uso de las redes y aplicaciones de mensajería, que tienden a ser mucho más crédulas con la información que circula en la red.

Esta nueva forma de delinquir, no es exclusiva de ningún grupo etario o social, sino todo lo contrario, es transversal y puede tocarnos a cualquiera de nosotros, directa o indirectamente. Por eso cuanto más solidarios y pacientes seamos en alertar y colaborar haciendo docencia al respecto, estaremos contribuyendo a mejorar la información que usuarios de la “*Red de Redes*” manejan, protegiéndolos y protegiéndonos también.

## LA FAKE DEMOCRACY Y EL PROYECTO DE LEY BRASILEÑO CONTRA LAS FAKE NEWS

**Autor:** *Leonardo de Andrade Alberto*



La consolidación de Internet, entre los años 2006 y 2015, a partir de los sitios de relación y de intercambio de contenidos (redes sociales) como fotos, videos y textos instantáneos (GOMES, 2018), ha representado una (r)evolución en las relaciones interpersonales, debido a la compresión del tiempo-espacio, es decir, relaciones sin barreras territoriales y temporales.

Este proceso de transformación de las relaciones es llamado por el sociólogo polaco, Zygmunt Bauman, “modernidad líquida”, es decir, la capacidad de relacionarse de manera fluida y en constante cambio, siendo el cambio solamente algo constante en esta sociedad.

El impacto que Internet y las redes sociales han tenido en la sociedad ha transformado no sólo las relaciones interpersonales, sino también el concepto mismo del Estado y su régimen político.

La referencia a la repercusión en el concepto de Estado está vinculada precisamente al elemento territorial, es decir, al proceso de desterritorialización que sufre el Estado por la complementación del espacio material con el espacio inmaterial, lo que da lugar al espacio digital virtual o ciberespacio.

Sin embargo, el impacto en el (algunos) régimen estatal está vinculado a la democracia, ya que internet ha democratizado el acceso, por ejemplo, a los contenidos educativos y los contactos virtuales

que se realizan, la mayoría de las veces, a través de las redes sociales.

Aunque las redes sociales desempeñan un papel importante en la democratización de los contenidos, también representan una posible amenaza para el Estado y las instituciones democráticas por los discursos ilegítimos con tono de legitimidad, así como por la difusión de noticias falsas. Estos ejemplos traen la idea de construir una falsa democracia (*fake democracy*) por medio de herramientas creadas para ser democráticas.

En este sentido, la *fake democracy* es el término que caracteriza a una sociedad que vive en torno a una falsa libertad de expresión e información, que impide al usuario formar su propia política y/o social basada en hechos reales.

Las *fake news*, un elemento de la *fake democracy* que se explota aquí, se utiliza con el propósito principal de la desinformación, es decir, se utiliza para engañar al usuario sobre una determinada situación, persona o grupo de personas. Este objetivo puede observarse durante la pandemia de Covid-19, donde hay numerosas "noticias" compartidas que distorsionan la verdad sobre la enfermedad, como que habría sido creada en un laboratorio por China, que hay un remedio eficaz contra la enfermedad o incluso que una vacuna que está en fase de prueba contiene un microchip para controlar a los seres humanos mediante la tecnología 5G (ejemplos de noticias falsas que circulan en las redes sociales en el Brasil).

La difusión de noticias falsas, que se produce de forma exponencial, es un fenómeno de extrema importancia capaz de impactar en la democracia de los Estados y de movilizar a la población en favor de una verdad falsa, por lo que la Organización de las Naciones Unidas (ONU) y la Organización para la Educación, la Ciencia y la Cultura (UNESCO) han clasificado el momento actual de la pandemia Covid-19 como un escenario de "infodemia" debido a la cantidad de noticias falsas que circulan en los sitios web y las redes sociales.

El Secretario General de la ONU dijo que "a medida que la pandemia se extiende, también da lugar a una segunda pandemia de desinformación, desde consejos malsanos hasta feroces teorías de conspiración" (ONU, 2020).

En el mismo sentido, el director general de la UNESCO dijo "esta ola de desinformación [...] está exacerbando la pandemia y poniendo vidas en riesgo" (ONU, 2020).

En este sentido, a través de la actual pandemia de desinformación, es posible ver con mayor énfasis el impacto de las *fake news* en el escenario de la modernidad líquida.

Así, a fin de limitar la divulgación de noticias falsas con potencial de daño, el Senado Federal brasileño propuso el proyecto de ley (PL) nº 2.630/2020 que establece la "Ley brasileña de Libertad, Responsabilidad y Transparencia en Internet", más conocida como "PL das *Fake News*".

Sin embargo, a pesar del noble objetivo del proyecto de ley con el deseo de combatir las noticias falsas, el texto propuesto presenta disposiciones que violan los derechos fundamentales garantizados por la legislación brasileña y decididos por el Tribunal Supremo Federal.

Según una nota técnica elaborada y publicada por el Instituto de Tecnología y Sociedad de Rio (ITS), el PL no tiene una redacción futurista, es decir, su texto se refiere a las tecnologías existentes hoy en día y no observa su evolución, porque “en lugar de proponer un texto que podría ser exhaustivo y acompañar el desarrollo de la tecnología, los proyectos congelan el desarrollo de las *apps* tal como están en 2020” (ITS, 2020).

Además de estancarse la evolución de la tecnología, el PL haría del Brasil un territorio con reglas únicas con el potencial de hacer inviables las *apps* en el país, y “el brasileño podría convertirse en un usuario de Internet de tercera clase con acceso a menos productos y servicios” (ITS, 2020).

Otro punto importante que hay que destacar se refiere al potencial de PL para vigilar la Internet, porque en su texto exige a los proveedores que vigilen “[...] sus plataformas para saber quién está difundiendo información errónea” (ITS, 2020).

El Data Privacy Brasil también ha producido y publicado una nota técnica que trata de los derechos fundamentales afectados por el PL de *Fake News*, como el no

reconocimiento de un derecho autónomo a la protección de datos personales, así como la contradicción como jurisprudencia brasileña, porque “el proyecto no adopta un concepto de privacidad del siglo XX, conectado en el Tribunal Supremo Federal de un derecho autónomo a la protección de los datos personales que difiere del derecho a la intimidad” (DATA PRIVACY BRASIL, 2020).

Además, otro problema se refiere a la celeridad del proyecto de ley ante la legislatura federal brasileña, que discute sin la debida atención un texto de impacto directo en las relaciones brasileñas, porque “un texto tan ambicioso, que trata de una cuestión vital para la democracia brasileña, no debería ser votado apresuradamente y sin las debidas consultas públicas. El Brasil es conocido internacionalmente por abrir el proceso de creación del Marco Civil de Internet a todas las partes interesadas, inaugurando en 2009 una nueva forma de construir leyes y políticas en la red. Aprobar el texto actual de manera apresurada y en su estado actual - lleno de errores de redacción e inexactitudes conceptuales – enviaría un mensaje muy negativo sobre la forma en que el Congreso ve la participación de la sociedad en el proceso legislativo” (ITS, 2020).

Ante los problemas expuestos, así como otros innumerables que presenta el PL das *Fake News*, las Naciones Unidas y la Comisión Interamericana de Derechos Humanos presentaron un informe al gobierno brasileño

señalando el conflicto de el PL con tratados internacionales como la Convención Americana de Derechos Humanos de 1969, así como la amplitud y generalidad del texto capaz de afectar el libre acceso a Internet en Brasil (TRINDADE, 2020).

Así pues, en vista de lo anterior, es posible observar que, aunque es necesario luchar contra las *fake news*, el proyecto de ley actualmente en curso en el Brasil no impedirá ni limitará la aparición de uno de los elementos que caracterizan a la *fake democracy* – las *fake news* –, sino que colocará al país bajo un régimen que limita los derechos fundamentales digitales en oposición a los tratados internacionales y las propias leyes brasileñas.

## REFERENCIAS

BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro: Zahar, 2001.

DATA PRIVACY BRASIL. **Nota técnica sobre o projeto de lei 2630/2020**. 2020. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2020/06/Nota-T%C3%A9cnica-PL-2630-1.pdf>

GOMES, Wilson. **A democracia no mundo digital**: história, problemas e temas. São Paulo: Edições Sesc SP, 2018.

ITS. **Nota técnica sobre os Projetos de Lei nº 2927/2020 (Câmara) e nº**

**2630/2020 (Senado)**. 2020. Disponível em: <https://itsrio.org/wp-content/uploads/2020/06/Nota-T%C3%A9cnica-ITS-PLs-contra-fake-news.pdf>

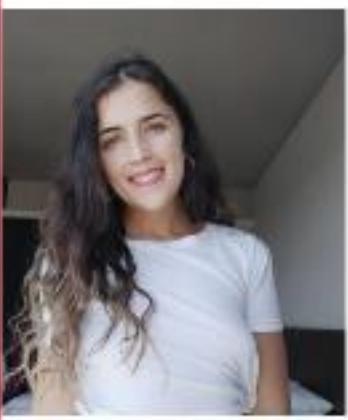
ONU. **No dia da liberdade de imprensa, ONU pede apoio a trabalhadores da mídia em meio à pandemia**. 2020. Disponível em: <https://nacoesunidas.org/no-dia-da-liberdade-de-imprensa-onu-pede-apoio-a-trabalhadores-da-midia-em-meio-a-pandemia/>

TRINDADE, Rodrigo. **PL das fake news é arbitrário e amplo demais, diz relatório da ONU e OEA**. **TILT**. 2020. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/07/21/relatores-especiais-de-onu-e-oea-pedem-que-planalto-revise-pl-das-fake-news.htm>

# EDI JOVEN AQUÍ ESTÁN - ELLOS SON



# EDI JOVEN AQUÍ ESTÁN - ELLOS SON



*Autor Victor Aldair Mejia Molina.*

Sumario: ¿Cuál es la importancia jurídica de los contratos electrónicos como instrumento y como objeto de estudio? en virtud de que ha

contratos electrónicos, para garantizar que el régimen jurídico aplicable al proceso contractual no impida la concertación de los contratos por vía electrónica, es por ello, que en 1996 la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) aprobó la Ley Modelo de Comercio

## LOS CONTRATOS ELECTRÓNICOS: RIESGOS Y CONFLICTOS EN EL DERECHO

propiciado una ascendente comercialización de los bienes y servicios, mediante figuras jurídicas como lo son los contratos informáticos de compraventa, derivados del derecho civil, revisten una serie de caracteres específicos muy marcados que dificultan una adecuada negociación y la problemática de legislar en materia nacional la tipología de estos contratos.

La contratación electrónica nace de los acuerdos efectuados en la red electrónica, actualmente la única legislación puramente aplicable a este es de la Comisión sobre Comercio Electrónico de la Unión Europea del 8 de junio del 2000, donde se convoca a los países miembros a conceder la validez a los

Electrónico, las cuales han sido piedra angular para el desarrollo jurídico de la materia informática en nuestro país.

Un contrato electrónico puede ser definido de distintas maneras, sin embargo, no se ha planteado en los códigos el concepto concreto de contrato electrónico y es necesaria la construcción de una definición. Cornejo Certucha considera que el contrato es “Un acto jurídico bilateral que se constituye por el acuerdo de voluntades de dos o más personas por medios electrónicos que permite otorgar validez, a los actos jurídicos celebrados entre las partes y que produce ciertas consecuencias de

Derecho".(2004, p.554)<sup>7</sup> Derivado el Código Civil Federal en su artículo 1824-Bis, establece que para que exista un contrato electrónico debe ser cumplido mediante la utilización de medios electrónicos, ópticos u otra tecnología, siempre que sea íntegro en su información, ¿Por qué es un problema? Se ha categorizado como problema por la problemática para los elementos que generan la validez de los contratos al no existir una legislación aplicable genera un problema, es por ello que se ha detonando la promulgación de normas para legalizar la práctica de los contratos y los diversos negocios jurídicos efectuados a través de esta novedosa herramienta electrónica, considerando que México solo cuenta con reformas y adhesiones al Código Civil Federal como al de los estados, las cuales, se centran en el reconocimiento de la celebración de actos jurídicos a través de medios electrónicos, donde se le da valor probatorio a la información contenida en dichos medios.

En el campo del derecho existen distintas materias que se dedican a ciertos actos por su jurisdicción, en el ámbito de los contratos electrónicos tenemos distintas disciplinas de aplicación como lo son: el derecho civil, derecho informático y el derecho mercantil, cada rama regula una parte fundamental para la celebración de actos por dichos medios, además, tenemos que definir cada una de las ramas para

revisar el alcance de los contratos celebrados en dichas materias.

En primer lugar, se considera al Código Civil por que le ataña la materia de contratación, es así que podemos encontrar en su legislación diversos tipos de contratos (Compraventa, permuta, mutuo, donación, comodato, etc.) incluyendo los que se perfeccionan por los medios que le ataña al presente artículo, sin embargo, no existe un apartado específico donde establezca los contratos que pueden ser perfeccionados por medios electrónicos, el código civil establece en su artículo 7.31 bis del Código Civil para el Estado de México menciona que cualquier convenio o contrato que se encuentre regulado en dicho instrumento podrá realizarse a través de dichos medios y constar en documentos electrónicos, ahora bien, cada contrato tiene una formalidad que debe seguirse en el caso de la Compraventa de bien inmueble que la venta debe estar en escritura pública, y en el caso de bien mueble, que en caso de exceder tres mil veces el salario mínimo debe realizarse ante fedatario público.

En concreto, cada contrato establecido en dicho instrumento jurídico tiene formalidades que hacen que sea válido dicho contrato, al no tener un capítulo establecido para regular dichas formalidades o una jurisprudencia que establezca

<sup>7</sup> CORNEJO CERTUCHA, Francisco M. Contrato, en Enciclopedia Jurídica Mexicana, Tomo II 2da

Edición, Editorial Porrúa, México, 2004, pág. 554

como debe ser la forma de los acuerdos electrónicos para que sean viables de su aplicación, y en caso de controversia sean viables para un juicio.

En segundo lugar, tenemos al Derecho Mercantil en el cual se regula los actos de comercio, con la finalidad de que estos actos de comercio generen una especulación comercial derivado de esta obtengan un lucro, como es el comercio electrónico, las compraventas de bienes o mercaderías.

En efecto el comercio electrónico se encuentra regulado en el Título Segundo del Código de Comercio, también con la firma de tratados internacionales México tiene suscrita la Convención de las Naciones Unidas sobre Contratos de Compraventa Internacional de Mercaderías donde regula la formación del contrato que también puede ser por medios electrónicos y asegura los riesgos que puedan devenir de dicha contratación, así mismo, el ordenamiento jurídico mexicano tiene una Ley de Firma electrónica avanzada, la cual regula el uso de la firma electrónica para los actos previstos en la ley, como veremos más adelante es uno de los elementos para prevenir riesgos en la contratación.

Finalmente, el derecho informático, que es también una base fundamental para la celebración de dichos actos, aunque tiene que ver más con contratos sobre bienes informáticos, teniendo en cuenta que existen diversas plataformas que ofrecen servicios de música o algún

otro servicio, es regulado por el derecho informático dichos softwares y las licencias de uso que se le brindan a los usuarios como usuarios del servicio que están prestando, para ilustrar esto planteamos el caso de Spotify como proveedor de servicios de música:

Spotify como empresa no celebra directamente un contrato de uso del servicio de música con cada usuario, este servicio cuenta con dos variables, la primera "Spotify Free" el cual ofrece el beneficio de utilizar el servicio de música gratuita bajo ciertas condiciones, en segundo lugar "Spotify Premium" este servicio ofrece lo mismo que el primero, solo que con otros beneficios que un usuario gratuito no tendría, este servicio se paga por medio de tarjeta de crédito o débito, ahora bien, cuando se paga por dicho servicio se aceptan "**Términos y Condiciones**" sin embargo, mucha gente no lee estos términos, al leerlos podemos ver que el primer párrafo establece "Los términos y condiciones de uso son importantes y afectan sus derechos legales" lo que equivale decir que dichos términos harían la base de un contrato que posteriormente estará especificado en los apartados consecuentes de los términos y condiciones. A pesar de eso contiene la el domicilio y nombre de la empresa, el objeto del contrato, establece la capacidad de los usuarios para celebrar contratos y en caso de ser *menores, bajo consentimiento del padre o tutor*, los derechos y obligaciones que tienen las partes, por lo según expuesto en

el artículo 7.8 del código civil vigente en el Estado de México se le da validez a dichos términos como un acto jurídico, a su vez el mismo contrato establece la vigencia, la jurisdicción de los tribunales según el país de origen del usuario, así como la jurisdicción y leyes que regirán el arbitraje en primera instancia, para concluir con dicho ejemplo, entendemos que los términos y condiciones de cualquier plataforma que brinde un servicio pueden hacer las bases de un contrato, y encontramos la importancia de la celebración de contratos por medios electrónicos y una vía electrónica.

Por lo que se refiere a los riesgos y elementos de prevención de la contratación por medios electrónicos, Téllez Valdés establece como riesgos en la contratación electrónica de entre otros el fraude o desfalco que comúnmente se da por tarjeta de crédito, el robo y modificación de programas, además la falta de comprobaciones mediata y que no existe certeza jurídica por el desconocimiento de la identidad e incapacidad jurídica de la persona para celebrar dichos actos, sin embargo, cada contrato y cada acto celebrado tendría sus riesgos al realizarse y en ciertas ocasiones dichos actos no tienen riesgos ya que existe una certeza jurídica y una responsabilidad inmediata de la persona, al contrario se llegasen a existir dichos riesgos en un contrato no existe ordenamiento jurídico que lo regule o imponga una sanción.

A partir de los riesgos y el desconocimiento de un

ordenamiento jurídico que regule dichos actos, podemos establecer que antes de realizar un acto por medios electrónicos revisar que tenga los siguientes elementos de prevención, así como lo es una oferta detallada donde se establezcan todos los medios por los que se puede llegar a un arreglo en caso de una problemática, indicar domicilios de las partes, que no exista desconocimiento del acto que se está realizando, que esta oferta contenga una firma electrónica que como ya se estableció en puntos más arriba, nos ayudara a tener una seguridad de saber con quién estamos celebrando dicho acto y que tiene toda personalidad jurídica establecida por las leyes de su país, en consecuencia, que exista un soporte electrónico o un tercero de confianza que valide dicho acto celebrado esto es que se tenga validado en documentos electrónicos (correos, páginas de internet, recibos), por ultimo una legislación aplicable.

En el caso de una legislación aplicable se establece como propuesta por todo lo anterior, el realizar una legislación, adicionar capítulos o artículos a dichas leyes con el fin de regular de manera específica lo relativo a los contratos electrónicos. El derecho moderno debe crear mayores acuerdos a nivel internacional, para la una mejor solución y unificación de un derecho de contratación electrónica para así realizar adiciones a los códigos civiles y mercantiles e informar a la población de cómo prevenir riesgos

al momento de generar un acto por medios electrónicos, para generar certeza y seguridad jurídica a los mismos.



*Victor Aldair Mejia: Licenciado en Derecho Internacional por la Universidad Autónoma del Estado de México. Profesor de Informática, bachillerato, mentor académico y Secretario General del UAPCIMUN.*



**Autora: Ab. Emilse María del Milagro Tabera Cabrera.**

oportunidad para adoptar esta nueva modalidad de trabajo.



## DERECHO A LA DESCONEXIÓN DIGITAL

La llegada del COVID-19 junto al aislamiento social y preventivo, trajo consigo un nuevo paradigma laboral. El Teletrabajo parece haber llegado para quedarse. Sin embargo, da la impresión de que aún queda mucho por andar.

El trabajo de manera remota y a través de medios tecnológicos, requiere una estrategia planificada, una nueva cultura laboral, así como personas líderes que estén preparadas para enfrentar este nuevo desafío.

En cambio, lo que se dio ante la Pandemia por el Coronavirus, fue algo intempestivo y carente de una estrategia diseñada y planificada. Por un lado, la ventaja es que esta circunstancia, acelera y adelanta el futuro. Por otro, la desventaja, es que hay todo un proceso de maduración que no se dio a cabo y que podría complicar esta gran

Lo cierto es que el Teletrabajo parece haber ganado muchos adeptos. Junto a la expansión de la modalidad se ha reactualizado el debate en torno a la necesidad de establecer horarios precisos para el cumplimiento de tareas ante la multiplicidad de vías de comunicación que se pueden llegar a emplear para tal fin.

En otras palabras, el derecho a la denominada **desconexión digital**, promete ser la manera de garantizar el reposo y los momentos de ocio necesarios para cualquier persona. Esto nos invita a preguntarnos, ¿Qué es el Derecho a la desconexión digital?

A través de la legislación, países como España, Chile y Argentina han aprobado este derecho a la desconexión digital. Como su nombre lo anticipa, garantiza al trabajador y a la trabajadora, la libertad de no permanecer conectado digitalmente a su trabajo una vez finalizado su

horario. Esto podría traducirse en el derecho de cada empleado y empleada a no contestar comunicaciones, llamadas, emails, mensajes, WhatsApp, etc., de trabajo fuera de su jornada laboral.

Este derecho implica, por lo tanto, que quien trabaja bajo la modalidad de teletrabajo tiene derecho a no ser contactada y a desconectarse de los dispositivos digitales y/o tecnologías de la información y comunicación, fuera de su jornada laboral y durante los períodos de licencias, quedando claro que no podrá ser sancionada por hacer uso de este derecho.

El empleador no podrá exigir a la persona que trabaja la realización de tareas, ni remitirle comunicaciones, por ningún medio, fuera de la jornada laboral establecida.

El período señalado, debería comenzar en el mismo momento en el que el personal finaliza su jornada laboral y extenderse hasta el inicio de la siguiente. La sola conciencia de la existencia de pendientes puede afectar la tranquilidad del trabajador o la trabajadora.

De no respetarse esta pausa podría producirse una situación común a miles de trabajadores durante esta cuarentena: un aumento de las horas laborales y un completo desdibujamiento de los límites entre el espacio de privacidad y la actividad laboral.

Para ello, es necesario que se articulen mecanismos a fin de llevar a cabo la delimitación de la jornada laboral para garantizarle al trabajador el respeto de sus derechos. La regulación de esta facultad deberá buscar satisfacer no solo la prevención de nuevos riesgos laborales, sino, con especial atención, la importancia de establecer y mantener los límites entre la esfera laboral - profesional y la esfera personal – familiar.

Por todo esto, en este momento de teletrabajo mayoritario, las empresas deben elaborar políticas internas de desconexión digital para sus trabajadores y trabajadoras, incluidos los puestos directivos. En estas políticas internas las empresas podrán concretar las modalidades de ejercicio del derecho a la desconexión y deberán poner en marcha acciones de formación y de sensibilización sobre un uso razonable de los dispositivos digitales.



Dra Emile Tabera

Asimismo, otro tema central a tener en cuenta es la disparidad de género, tornando imprescindible que



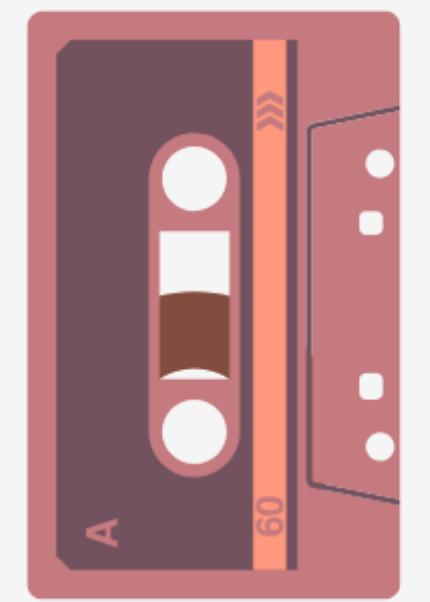
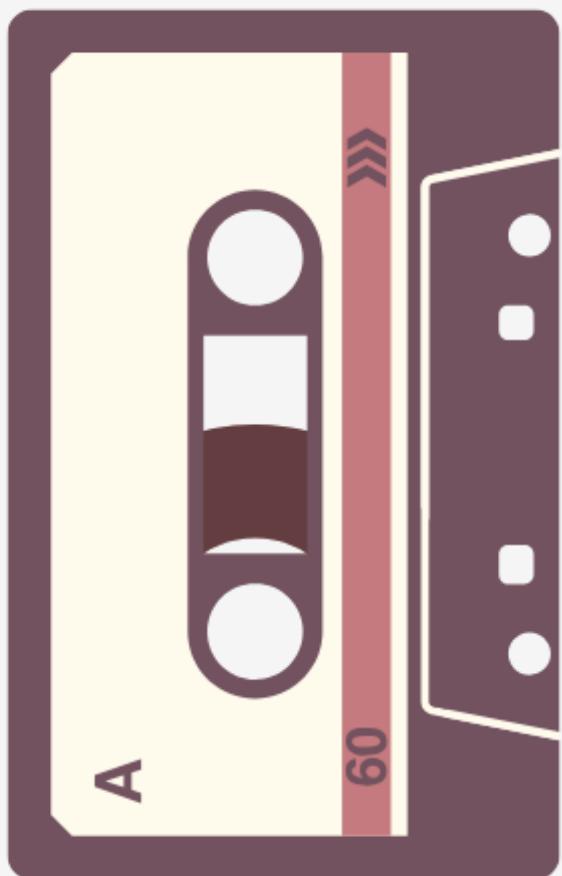
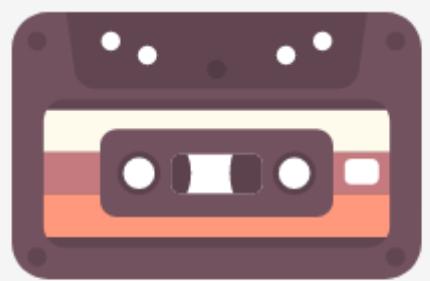
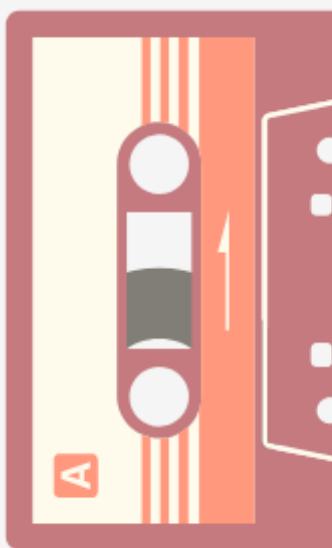
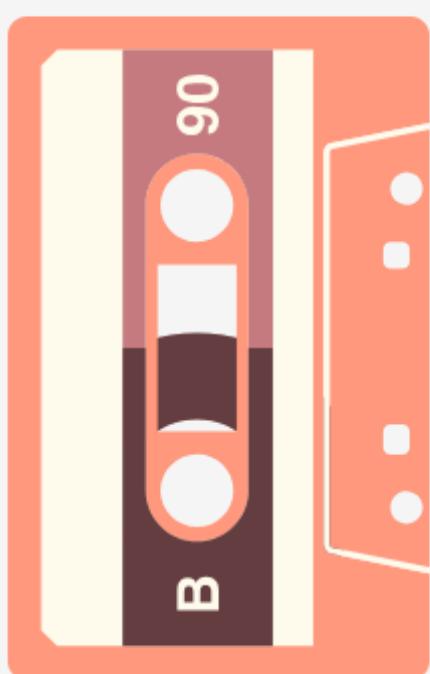
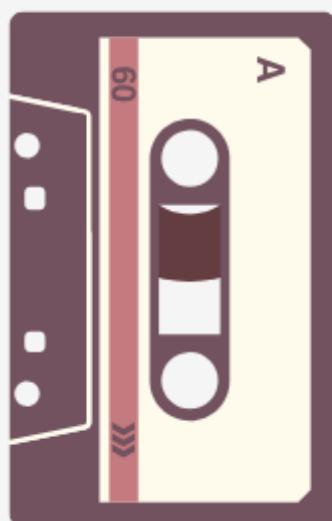
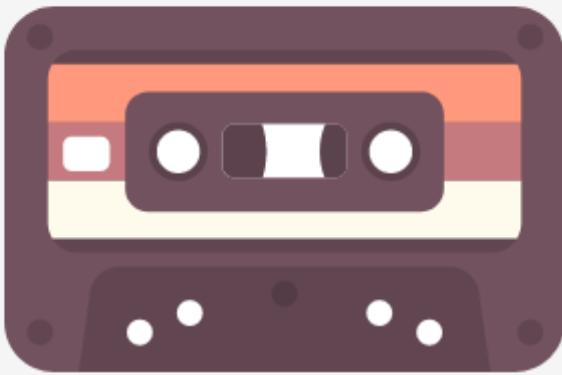
las políticas internas por parte de los empleadores no perjudiquen a las mujeres, quienes son las que más cargan con tareas de cuidado y del hogar y pueden necesitar de mayor flexibilidad respecto a las horas en el trabajo y las horas de conexión en su hogar.

Dada esta nueva realidad que vivimos, el ejercicio del derecho a la desconexión no puede ni debe residir en una responsabilidad individual. Para hacer frente a esta problemática, que se profundiza en el escenario del teletrabajo generalizado producto de la emergencia sanitaria actual, es vital que el enfoque sea colectivo y que imponga a los Estados y al sector empresario el esfuerzo por cuidar a los trabajadores y no exponerle al grave riesgo del estrés por el uso de dispositivos digitales.

Es dable a destacar, que para asegurar los momentos de ocio y recreación también será indispensable que todas las personas contribuyamos a tomar conciencia de los efectos y riesgos asociados a la hiperconectividad, aplicando una ética del descanso tan fuerte como la ética del trabajo.

La dinámica de la pandemia y de los procesos de aislamiento social hicieron que la hiperconectividad sea hoy lo cotidiano, atravesando a toda la sociedad y a la cultura de forma innegable. En el contexto laboral, la llegada del Teletrabajo como una alternativa al trabajo presencial, evidencio las bondades de esta modalidad, mostrando, en muchos casos, ser incluso más eficiente. La urgencia de la situación sanitaria dificultó la transición armónica, gradual y equilibrada a esta nueva forma de trabajo. Sin embargo, se ha visto de manera positiva al Teletrabajo, que permite una cultura laboral más flexible. En base a la experiencia y la regulación de este, seguramente caminaremos hacia un nuevo escenario donde el Teletrabajo será parte de nuestra cotidianidad.

#DerechosDigitales  
#DerechoalaDesconexiónDigital  
#DesconexiónDigital #Teletrabajo



---

**LA RED EDI**  
**INFORMACIÓN QUE SUENA BIEN**

---

**Autor: Ab. Darío Echeverría Muñoz. Msc, LL.M**

El aprendizaje automático (machine learning), es una rama de la inteligencia artificial que consiste en modelos algorítmicos de asimilación cuya información recabada por esta, busca determinar una respuesta concreta en lugar de utilizar el elemento humano para llevarla a cabo, su insumo principal son los datos de los cuales se alimenta para realizar los distintos procesos que corresponden a dicho aprendizaje.

La inteligencia artificial ha evolucionado de tal manera que, en sus diversos procesos, facilitan las labores diarias en distintos ámbitos profesionales, se subdivide en tres categorías:

- **Aprendizaje supervisado:** se utiliza para realizar predicciones cuya base recae en circunstancias del pasado, y estos modelos se utilizan para entrenarlos y mejorar su eficacia, exactitud y eficiencia. Un ejemplo de los procesos utilizados hoy en



día en este tipo de aprendizaje es el procesamiento de lenguaje natural (natural language processing - NLP)

A breves rasgos, el procesamiento de lenguaje natural es un proceso de inteligencia artificial, encargado de estudiar la interacción entre computadoras y el lenguaje de los seres humanos, mediante la formulación e investigación de mecanismos eficaces a nivel tecnológico para lograr una efectiva comunicación con la información procesada, por ejemplo, la herramienta de inteligencia artificial conocida

## DERECHO AL HONOR E INTELIGENCIA ARTIFICIAL

como *prometea* que tiene como fin resolver casos jurídicos y dictar sentencias.

- **Aprendizaje no supervisado:** se utilizan para clasificar y estructurar datos cuyos modelos deben ser entrenados para mejorar su eficiencia y exactitud. Un ejemplo de estos procesos es la reducción de dimensionalidad (dimensión reduction), cuyas técnicas pretenden la reducción del número de dimensiones del espacio analizado, determinado por el conjunto de variables explicativas.

Por lo general se utiliza para clasificar la generalidad de datos para almacenarlos en un entorno específico que sirva para determinar un análisis concreto de la información recabada, por ejemplo, la identidad de una persona en base a distintos fotogramas existentes que analizan información como sus expresiones o características únicas gestuales utilizados para el reconocimiento de personas desparecidas o buscadas por sospecha de delitos.

- **Aprendizaje reforzado:** son modelos de aprendizaje automático que asimilan la información recabada en base a cometer errores, se utiliza un mecanismo de “recompensa” o “penalidad”, este método se lo utiliza en el área de los

videojuegos para determinar la dificultad y mecanismos a utilizarse, o en el campo jurídico se usa para realizar diversas simulaciones en sus distintos ámbitos para reflexionar de la prueba y error aplicado en la experiencia del caso.

El Derecho tampoco está libre de evolucionar en el aspecto informático, en la actualidad existen propuestas para el desarrollo de inteligencia artificial que tenga la capacidad de resolver problemas jurídicos con la mayor celeridad y tutela que requieren los ciudadanos en lo que a sus derechos se refiere, sin embargo, legalmente estos métodos de aprendizaje no podrían actuar de forma independiente completamente, ya que tendrían sus limitaciones para actuar ¿Hasta qué punto se garantiza el derecho al honor, honra y buena reputación como derecho fundamental que tiene el ciudadano a su favor?

Para ello es necesario citar el Art. 12 de la Declaración Universal de los Derechos Humanos emitida por la Asamblea de las Naciones Unidas:<sup>8</sup>

«*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*»

<sup>8</sup> (Naciones Unidas, 1948)

Que tiene concordancia con lo prescrito en el Art. 11 de la Convención Americana de Derechos Humanos:<sup>9</sup>

**«Artículo 11. Protección de la Honra y de la Dignidad**

1. *Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.*

2. *Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.*

3. *Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.»*

Con la evolución de la sociedad es conveniente ampliar estos criterios para abarcar otras esferas. Respecto al derecho de honor, honra y buena reputación, existen nuevas alternativas de perjuicio gracias a las nuevas tecnologías y a la publicidad masiva de la información, que requieren mecanismos adecuados de protección, porque si bien la inteligencia artificial abarca una extensiva cantidad de datos personales, hay detrás un elemento humano que programa los algoritmos para su desenvolvimiento, y si existe un sesgo ya sea de tipo racial, ideológico, religioso, etc; no se garantizaría eficazmente su

aplicación provocando su indefensión.

Un ejemplo en la actualidad de este problema sucedió en febrero de 2013, Eric Loomis fue capturado bajo sospecha de estar involucrado en un tiroteo ocurrido en la pequeña ciudad de La Crosse, este aceptó que conducía el vehículo donde huyeron las personas que participaron en el intercambio de disparos, pero la corte lo sentenció a seis años de prisión.<sup>10</sup>

Sin embargo, al utilizar un análisis de inteligencia artificial conocido como COMPAS (Correctional Offender Management Profiling for Alternative Sanctions, en español traducido como Administración de Perfiles de Criminales para Sanciones Alternativas del Sistema de Prisiones de Estados Unidos) la corte notó que Loomis había sido identificado como "un individuo de alto riesgo para la comunidad.

El programa en principio, mediante sus algoritmos permite cotejar toda la información posible sobre el acusado, y esto ayude al sistema judicial para tomar decisiones más objetivas, sin embargo, surgen cuestiones subjetivas, por ejemplo, el cuestionario no pregunta sobre la etnia del acusado.

A decir de esto, la Corte Suprema de Wisconsin también advirtió que COMPAS podría darles

<sup>9</sup> (Corte Interamericana de Derechos Humanos - Comisión Nacional de los Derechos Humanos - Organización de los Estados Americanos, 2018)

<sup>10</sup> (Maybin, 2016)

a las minorías étnicas puntajes de riesgo desproporcionado, esto debido a las actuales tensiones con los que se desenvuelve la policía en sus actuaciones, que en la mayoría de los casos han demostrado discriminación y el desigual trato basado en aspectos raciales socavando su derecho al honor y dañando su buena reputación.

Además, el derecho al honor es derivativo de otros derechos y se encuentra ligado a los mismos, como es el caso del derecho a la libertad de expresión, que, si bien brinda la potestad a las personas de opinar libremente respecto de cualquier tema, situación o persona, no puede exceder al nivel de atentar contra la dignidad de las personas y causar perjuicios a su imagen, con el pretexto de invocar su planteamiento sin escrúpulo alguno. La afirmación es recogida por Soto Gama (2010, p. 99), quien afirma:

«La limitación a este derecho supone la prohibición de la publicación y emisión de injurias en contra de cualquier persona y por cualquier medio. Las limitaciones también inciden sobre las informaciones difamatorias y el correspondiente delito de difamación. En ocasiones, este delito es el instrumento de que se valen los funcionarios públicos para acallar críticas u ocultar conductas ilícitas».<sup>11</sup>

La jurisprudencia en materia de derechos humanos no se queda atrás, en el caso *Memoli vs. Argentina*, El juez Diego García

Sayán en su voto concurrente señaló:<sup>12</sup>

«12. Lo importante es que en el proceso de protección y garantía del derecho a la honra, se resuelva cualquier controversia o contencioso derivado de lo que podría considerarse un ejercicio abusivo del derecho a la libertad de expresión de manera que ambos bienes jurídicos queden adecuadamente protegidos por un adecuado ejercicio de ponderación. Como es evidente, en caso de conflicto corresponde y corresponderá a la judicatura procesarlo y resolverlo en la búsqueda de una armonía entre la libertad de expresión y otros derechos fundamentales. En ese ejercicio de la ponderación se puede procesar y resolver adecuadamente conflictos de derechos como los que se presentan en casos como éste. Esto significa, en esencia, que se ponderan las circunstancias del caso en conflicto, no para concluir en la “preferencia” de un derecho sobre el otro, sino para resolver en torno a los aspectos concretos del derecho o derechos invocados de tal forma que queden debidamente delimitados para el caso específico de manera que ambos puedan ser protegidos.»

Por este motivo es importante delimitar los derechos individuales, ya que estos terminan donde inicia el derecho colectivo. Además, en cuanto al reconocimiento y aplicación de estos derechos, no existe distinción alguna ya que todas las personas son iguales ante la ley sin importar su religión, etnia,

<sup>11</sup> (Echeverría Muñoz, 2020)

<sup>12</sup> (Caso Mémoli vs. Argentina, 2013)

pensamiento, inclinaciones sexuales, ideología política entre otros.

Por lo tanto, para que los sistemas de inteligencia artificial apliquen en debida forma sus funciones, las personas que los programen deben garantizar que la información procesada no tenga sesgo alguno que deje en indefensión a las personas en cuanto a sus derechos se refiere y así evitar cualquier violación a los mismos para lo cual, es necesario formular las siguientes recomendaciones:

- Derecho de las personas a conocer para qué se utilizan sus datos, el tiempo que son conservados, cómo elaboran sus perfiles y qué tipo de decisiones automatizadas están programadas en los sistemas de

inteligencia artificial utilizados para su tratamiento.

- Responsabilidad de quienes utilizan la información y sus finalidades.
- Derecho a la rectificación y suspensión por uso equivocado o doloso de la información garantizando su honor, honra y buena reputación.
- Derecho de oposición al tratamiento de la información almacenada salvo que exista un interés legítimo debidamente justificado.



Presenta  
CICLO  
NUEVA  
CULTURA  
LEGAL

**Martes 20 hs**

Vivo por  
Instagram.



**IG: @estudiovizcaychipi - youtube.com/c/elderechoinformatico**





CONGRESO VIRTUAL

# "LOCADEMIA (JOVEN) DE DERECHO Y TECNOLOGÍA"



ELDERECHOINFORMATICO

22 Y 23 DE SEPTIEMBRE

[YOUTUBE.COM/USER/ELDERECHOINFORMATICO](https://www.youtube.com/user/ELDERECHOINFORMATICO)

## Grooming

## El día después

suele derivar el tráfico y la pornografía infantil .

**Autora: Vanina Kandyba**

Vivimos en tiempos donde la sociedad cambia constantemente, el ser humano a lo largo de su ciclo psico-evolutivo ha ido adaptándose a las circunstancias, el uso de las Tics fue creando nuevos universos, el poder comunicarnos, descargar información, trajo consigo algo más, algo que mueve millones de dólares, veremos a lo largo del presente texto algunos aspectos, ya sea en su parte jurídica, humanística y/o psicológica.

La Convención sobre los Derechos del niño ha sido receptado por naciones de todo el mundo, se ha tomado algunos aspectos de la misma, por lo que haremos un análisis un tanto llamativo para muchos, atrevido para otros, pero en definitiva se apunta a poder aplicar ciertas sentencias, olvidándonos de la vulneración de estos derechos, un ejemplo es en los casos de Grooming, modalidad delictiva que aparece con estas nuevas tecnologías donde los menores son captados por groomers, configurando ello un delito del cual

En Argentina tenemos la ley que data del año 2013 n° 26.904 que incorpora el art.131 del Código Penal, por el cual se castiga con seis meses a cuatro años de prisión a quien por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos contacte a un menor con el propósito de cometer cualquier delito contra su integridad sexual. Dentro del supuesto no se contempla al infanticidio para la suma de delitos, es decir siempre se sanciona el delito máximo, no obstante a criterio propio considero que deberían sumarse ambos tipos penales para alcanzar la pena máxima; No podemos dejar de pensar que a todo esto, cuando termina el proceso judicial, en la mayoría de las oportunidades la víctima no tiene el seguimiento y contención por parte del Estado, circunstancia que según los derechos del niño debería producirse.

Ya sea por falta de profesionales o recursos que el estado debería contar para estos casos, existen muchos organismos trabajando

estas temáticas, pero ¿hasta qué punto estas leyes contemplan la real necesidad del infante? Son Normas que tienen en cuenta las realidades de la generalidad de los menores? Por poner solo un ejemplo, cuanto más declara un infante más vulnerable se torna su psiquis.

Cabe destacar que estos pequeños hechos pueden definir el



Autora: Vanina Kandyba

futuro del menor al transformarse en un adulto. Es una realidad que a nivel mundial existe la problemática delictiva a través de redes sociales, y en épocas de aislamiento preventivo, las estadísticas muestran que 1 de cada 3 niños o adolescentes ha sufrido una situación incómoda en la web (fuente: Argentina.gob.ar). Teniendo el incremento del uso de las redes sociales y el tiempo de navegación online de los menores, es oportuno incrementar medidas que permitan la prevención de delitos como el grooming y conductas como el

sexting, que dañan a la víctima y a todo su entorno familiar y afectivo, en todo el mundo las cifras han aumentado entre un 30 % y un 40%.

Muchos de nosotros hemos pensado cual será la situación de diversos casos una vez pasada la condena o descubierto el ataque, personalmente suelo reflexionar ¿que será que ocurrió con esta víctima?, ¿afloraran las circunstancias que tuvo que pasar? ¿Incidirá en su psicodesarrollo? ¿Será que influyó en su sociabilidad? ¿Se encontrará vulnerable aún? ¿Qué será de sus miedos, su dolor oculto? Nuestro cerebro, en algunas ocasiones reprime el trauma, o hace olvidar ese hecho tan doloroso, pero en otras permite que afloren nuevamente, y no siempre es con buenas consecuencias, por ello

es necesario reaprender, reconstruirse.

A nivel mundial las estadísticas son devastadoras con respecto al suicidio adolescente, y la realidad es que una enorme mayoría de esos suicidios, se da por los acosos sufridos por redes sociales, desde mi personal punto de vista, creo que hace falta más educación, más empatía, más respeto, los estados deberían hacer especial hincapié en todo esto, el ser humano se convierte en un ser pequeño e indefenso ante ese enemigo invisible que lo avasalla.

Muchas veces los Niños, Niñas y Adolescentes terminan siendo víctimas especies de huérfanos digitales, donde para un adulto es más simple darle un dispositivo, o niñera virtual como me gusta llamarlo para que no den problemas, para que no causen molestias, que no ensucien, que queden quietos, ahora bien, ¿que responsabilidad jurídica tiene ese adulto? ¿Acaso es lo mismo que dejarlo deambular solo en las calles? Entiendo que si se los deja expuestos a un mundo donde los ciberdelincuentes buscan captarlos, dicho esto cabe preguntarnos ¿Cómo regulan los estados las leyes para tratar de erradicar este gran problema al que hacemos frente?

No obstante la existencia de control parental, o sobre los contenidos, hay que decir que los ciberdelincuentes siempre encuentran la manera de infiltrarse y/o filtrar contenidos a juegos diseñados para niños, recordemos el caso de roblox, donde un avatar fue violado, con toda la escena gráfica. Si es real que no hubo acceso carnal pero el trauma que se puede generar es el mismo. Si bien esta compañía afirmó estar trabajando sobre las cuestiones de seguridad para que esto no vuelva a suceder,

La tecnología es maravillosa y muy útil, pero hay que aprender a usarla, para cuidar a quienes amamos, como podrán apreciar este texto posee muchas preguntas, pues la idea es que podamos realizar una introspección, pensemos y nos preguntemos qué podemos hacer como sociedad para cuidar a nuestros niños niñas y adolescentes, como colaborar para su protección y que sus derechos se cumplan, que tengan la contención necesaria no solo para un proceso judicial, sino para el proceso de desarrollo y construcción que deben enfrentarse luego de ser captados.

Debemos procurar que aquellos menores pasibles de un ataque tengan acompañamiento después de una sentencia, se debe fomentar y pelear para que cada víctima siga con acompañamiento continuo, allí realmente se marcará la diferencia en un antes y después. Pensemos que no es solo meter a alguien a la cárcel cuando se logra comprobar que cometió algún tipo de delito relativo a la integridad de los niños niña y adolescentes, sino tratar de que los estados también cumplan al pie de la letra los convenios establecidos para proteger, acompañar y asegurar un pleno desarrollo en diferentes áreas.



# INTERACTUEMOS DERECHO TECNOLOGÍA Y CIENCIA



# GROOMING, UN DELITO QUE CRECE DÍA A DÍA EN PANDEMIA.

Autoras: Yamila Arriaga - Aisha Loreley Quiroga



**Yamila Arriaga**

Diversos estudios han demostrado que los niños, niñas y adolescentes transcurren cantidad de horas frente a dispositivos electrónicos, y no es sorpresa para nadie que ellos, llamados la Generación de la Tecnología, aprendan a utilizarlos y a navegar por el mundo de internet a temprana edad.

Sumado a ello y a la explosión que ha devenido hace unos años de las muy utilizadas y adictivas Redes

Sociales, como ser, Facebook, Instagram, Tik Tok, Twitter, Whatapp, han revolucionado la manera de interactuar unos con otros, de expresarnos y de comunicarnos entre sí.

Si bien, se les atribuye innumerables beneficios a dichas plataformas, a saber, comunicación instantánea, oportunidades laborales, información, entretenimiento, conocimiento compartido, el poder denunciar socialmente, etc, también se les asigna un buen grado de peligrosidad para aquellos que desconocen o son desatentos al momento de configurarlas.

Ello es así, ya que, en la emoción, ansiedad y velocidad de la interconectividad, hace que muchas



**Aisha Loreley Quiroga**

veces no nos detengamos a leer los famosos términos y condiciones, como tampoco resguardar nuestros datos al configurar nuestra privacidad en las aplicaciones, sin saber qué información personal dejamos al descubierto para que otros se aprovechen de ello.

Más aún cuando son niños o niñas los que están frente a estos dispositivos, que si bien como expresamos, es evidente que manejan mejor la tecnología que un adulto, muchas veces son vulnerables y víctimas de las amenazas que se encuentran del otro lado de la pantalla.

Ello se ve reflejado en el delito de Grooming, el cual ocurre cuando un adulto contacta a un menor de edad (que por lo general la franja es de 8 a 13 años), a través de Internet (redes sociales) y mediante la manipulación o el engaño, muchas veces ocultando la condición de adulto y / o haciéndose pasar por un menor con el fin de entablar una "amistad", logran que el niño o niña realicen acciones de índole sexual, a través de envío de fotografías o videos.

En Argentina, un caso que tuvo auge en este sentido es el de un joven, mayor de edad, que, en agosto de 2010, se contactó con una adolescente de 14 años y, tras reiteradas conversaciones, logró concretar un encuentro en el que el hombre abusó sexualmente de él. Este, como muchos otros casos similares, sentaron precedente sobre delitos cometidos en uso de la

web, para que en noviembre de 2013 se sancionara la Ley 26.904 referida al delito de Grooming en Argentina.

Estudios psicológicos han demostrado que lo que pasa en Internet tiene un impacto real en nuestras vidas por lo que es sumamente necesario que un menor pueda confiarle a un adulto responsable si hay algo que lo inquiete o perturbe, ya que es moneda corriente la creación y contacto a menores a través de perfiles falsos.

Si bien, las denuncias sobre Grooming han aumentado exponencialmente, profundizándose por el hecho de tener que estar más horas en casa a causa del Covid19, circunstancia que nos toca atravesar como sociedad a nivel Mundial, el fin último que buscan los atacantes se corresponde a conseguir imágenes privadas ya sea para su propia satisfacción, ser distribuirlas en redes de pedofilia; utilizarlas para extorsionarlos o llevar adelante un encuentro físico donde cometer abuso sexual.

Según un estudio en Argentina es alarmante la estadística que demuestra que seis de cada diez menores habla con desconocidos en Internet, creando un lazo de confianza totalmente irreal, siendo el mismo a través de cualquier medio digital que permita la interacción entre dos o más personas, no solo redes sociales, sino también a través de correo electrónico, mensajes de texto, sitios web de chats, videojuegos, entre otros.

De acuerdo a lo manifestado por expertos en la materia, el proceso de esta problemática tendría cuatro etapas, siendo la primera de ellas, el CONTACTO que se produce entre el victimario con la víctima, generando esa confianza ut-supra mencionada. En segundo lugar, se destaca la CONSTRUCCIÓN DEL VINCULO, donde el primero busca mediante preguntas típicas, como ser: ¿Con quién vive, y cuantas veces se queda solo/a en su casa?, ¿Qué edad tiene?, ¿A qué colegio va, y a qué horario?, ¿A qué se dedican los padres, y con quién se queda cuando trabajan?

Ello es así, ya que el ciberdelincuente va buscando un espacio seguro para contactarse con el menor sin ser interrumpido. También, suele ser habitual que el Groomer se haga amigo de los amigos del menor para profundizar la confianza entre ellos y conocerlo mejor. Seguidamente se presenta la tercera etapa a la que llamamos OBTENCIÓN DE IMÁGENES, en la cual el abusador comienza a solicitar fotografías o videos a ese niño/a o adolescente con contenido sexual. Pero cuando la víctima quiere salir del “juego”, aparece la figura del ACOSO, siendo esta la última etapa, donde el adulto amenaza al menor con hacer públicas esas imágenes a sus padres y en contraprestación, este último por miedo, continúa cumpliendo las órdenes de su abusador.

Es fundamental y necesario reconocer que allí, donde no hay cuidado, se abre el espacio para que

delincuentes y abusadores encuentren el modo de llegar a los niños. Si bien la responsabilidad primaria es de los padres, todos los adultos deben hacer primar los derechos de los menores y estar alerta sobre ciertos síntomas que ellos pueden manifestar, como ser, cambios en su comportamiento, dolores de estómago, cabeza, cansancio, dificultades en las relaciones familiares, alejamiento de su círculo de amigos, hermetismo, ausencia de ganas de ir al colegio o salir, depresión, ansiedad, etc.

Por lo que desde La RED EDI, insistimos en el aprendizaje de estas temáticas y llevamos adelante campañas de concientización e información tanto para niños, niñas, adolescentes, adultos, padres y docentes, a fin de que estén instruidos sobre la materia y puedan brindar a sus hijos o alumnos, una respuesta inmediata y eficaz ante un pedido de ayuda, preservando la infancia y combatiendo así esta amenaza que se presenta en la vida digital, que cada día va en aumento.

# INFORMÁTICA FORENSE EN GUATEMALA

Un análisis a profundidad sobre los avances y el futuro de las investigaciones digitales y del computo forense en nuestro País.

COMIENZA EL 30  
DE SEPTIEMBRE

JOSE R. LEONETT



\* Abogado, con Maestría en Derecho



Comercial y Civil, Fedatario juramentado con especialidad en Informática en Perú, Bachiller en Ingeniería de Sistemas, especialista en Derecho Digital y Nuevas Tecnologías, docente y capacitador en temas de derecho informático y transformación digital.

## INTRODUCCIÓN

El año 2020 va a ser recordado como el año de la pandemia y de la cuarentena, a nivel mundial, de esto no cabe duda, pero también y como consecuencia de esta cuarentena forzada, también se recordará en el futuro, que una serie de procesos, actividades y labores cotidianas, se han visto forzadas a realizarse de manera digital, lo cual ha llevado a acelerar el proceso de transformación digital que se venía implementando en las diversas organizaciones de Latinoamérica, algunas con más avance que otras, pero en las organizaciones gubernamentales que son las que rigen y administran el sistema económico y legal de una nación, es donde debería darse este cambio con mayor importancia.

El presente artículo comentara brevemente sobre una problemática con la cual se ha topado este proceso de cambio hacia lo digital: **la aplicación de la firma electrónica y como lograr una adecuada identificación digital**, ya que si bien es cierto que en diversos países, ya se han implementado diversas propuestas de firma electrónica para la población en general, estas muchas veces no han logrado el objetivo para el cual fueron implementadas, y en ocasiones han tenido una débil adecuación y difusión, no teniendo la eficacia deseada.

Pero más allá de las soluciones aisladas desarrolladas por cada país, también se ha encontrado una problemática adicional, ya que estas soluciones son justamente eso: aisladas e independientes, realizadas de manera separada por cada país, sin tomar en cuenta una realidad común latinoamericana: que entre los diversos países se realiza diversas operaciones comerciales tanto de manera presencial como electrónica; contando también que hay una alta circulación y tránsito de personas entre estos países, por lo cual tener soluciones de firma electrónica independientes y aisladas una de otra, no permite que haya una eficiente interoperabilidad y comunicación entre los diversos organismos y países que actúan en estas operaciones comerciales e interactúan de diversas maneras.

Por lo cual se analizara brevemente esta situación, ya que con la aceleración de la mencionada

transformación digital, debido a la cuarentena, se ha puesto de manifiesto las dificultades que tiene la aplicación de la firma electrónica en los diversos países de la región sudamericana y como es su interacción entre estos.

## PALABRAS CLAVES

Identidad digital, Firma electrónica, Firma digital, Identidad digital, Equivalencia funcional

## TERMINOS COMUNES APLICADOS ENTRE LOS DIVERSOS PAISES USUARIOS

En esta sección se ha querido colocar algunos conceptos comunes a todas las propuestas de firma electrónica de cada país ya que, en términos generales, lo que se busca es lo mismo: la identificación de la persona y su posible manifestación de voluntad, estos conceptos serian:

### 1. EQUIVALENCIA FUNCIONAL

En este caso podemos hacer referencia a lo señalado por la **Ley Modelo UNCITRAL sobre Comercio Electrónico**, que indica en su artículo 5:

*“No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos”*

Y siguiendo esa línea se puede definir a la **Equivalencia Funcional** como la propiedad de otorgarle el mismo valor probatorio y la misma calidad jurídica que tiene un medio físico o tradicional, a los realizados por medios electrónicos, siendo principalmente las

firmas electrónicas los que tienen este atributo de equivalencia funcional.

## 2.-FIRMA ELECTRÓNICA

Son varios los conceptos de Firma electrónica que se pueden señalar, para hacer una definición, podemos entenderla como aquellos recursos basados en medios electrónicos con la intención precisa de autenticarse y demostrar la identidad, dependiendo del caso, también podría darse la intención de hacer una manifestación de la voluntad.

## 3.-FIRMA DIGITAL

La firma digital puede ser considerada como un tipo de firma electrónica que utiliza una técnica de criptografía asimétrica.

## 4. NEUTRALIDAD TECNOLÓGICA

Mediante este principio se establece que las normas y leyes no pueden obligar el uso de una tecnología en particular, pero este es considerado solo un principio, el cual muchas veces no se toma en cuenta, y depende de los gobiernos su aplicación.

## 5. INTEGRIDAD Y NO REPUDIO

Características que se puede aplicar a la firma electrónica que consisten en la seguridad de que el documento electrónico está completo y no ha sido modificado. Siendo el “no repudio”, aquella por la cual el que firmo el documento no puede negar su firma de dicho documento.

## 6. IDENTIFICACION Y AUTENTIFICACION

Son las principales características que se buscan lograr cuando se gestiona y

trabaja con documentos electrónicos, por lo cual con las soluciones de Firma Electrónica y Digital se busca lograr una adecuada **identificación y autenticación** de la persona usuaria

## RIESGOS POSIBLES y PROBLEMAS QUE SE BUSCA SOLUCIONAR

Aquí se han determinado algunos problemas comunes a todos los países que se quieren eliminar, se les mencionara brevemente:

### 1. SUPLANTACIÓN

Cuando se trata de comercio e interacción usando canales informáticos, el riesgo de que la persona que dice ser quien realiza determinada transacción, pueda ser un suplantador o un falsificador es mayor, por lo que es importante tener un mecanismo idóneo de identificación.

### 2. ALTERACIÓN

Como se sabrá tratándose de documentos electrónicos es mas factible su alteración o modificación que tratándose de medios físicos, pudiendo cambiarse lo consignado en un documento originado electrónicamente, por lo cual se requiere un medio que permita tener plena certeza de la inalterabilidad del documento

### 3. RECHAZO O REPUDIO

Se trata de la posibilidad de que el firmante de determinado documento rechace su propia firma, igualmente se requiere de un mecanismo que no permita este tipo de situaciones.

### 5. FECHA CIERTA

El concepto de fecha cierta es muy usado en derecho, pero tratándose de medios electrónicos se requiere de un mecanismo el cual no pueda ser alterado y modificado, y es aquí donde la firma digital ha resultado una solución alternativa para determinar una fecha base.

Estos son algunos de los riesgos y problemáticas más comunes que existen en las diversas operaciones comerciales que se realizan a menudo, pero cuando se trata de comercio electrónico estos riesgos pueden ser mayores, tomando en cuenta que durante la cuarentena ha habido una mayor difusión de dichas transacciones, ha tomado mayor importancia la necesidad de recurrir a estos recursos tecnológicos para lograr en alguna forma la seguridad jurídica.

#### SITUACION ACTUAL Y PROBLEMÁTICA DE LA FIRMA ELECTRÓNICA Y DIGITAL Y EN LATINOAMERICA

Hay que tomar en cuenta la situación dispersa que se tiene en Latinoamérica, ya que si bien es cierto que algunos de los países de la región han adoptado la ley modelo de la UNCITRAL en su estructura, este modelo ha sido adecuado a las necesidades y posibilidades de cada país.

Como se verá más adelante cada país ha optado por proponer un modelo diferente de aplicación de la firma electrónica, pese a esto se podría decir que hay puntos en común, uno de

ellos es que los países que han aplicado la implementación de firma electrónica tiene actualmente, una ley en materia de validez jurídica y probatoria respecto de los documentos que utilizan firma electrónica, también se aprecia, que hay una regulación en materia de comercio electrónico, entre otras regulaciones que sirven de apoyo a todo lo que son transacciones por medios digitales.

Otro de los puntos en común es que estos países han optado por reconocer a través de criterios de **equivalencia funcional** la eficacia jurídica de las firmas electrónicas y digitales propuestas en su propia normativa, lo cual ya representa un punto de partida del cual se puede establecer semejanzas.

En resumen se ve que si existen puntos en común y similitudes pero, pese a esto, no resulta ser suficiente para lograr un adecuado y eficiente flujo comercial y personal, principalmente debido a lo separada que se encuentra la normativa de un país con respecto al otro, siendo que las soluciones tecnológicas son casi iguales pero no terminan de hablar el mismo lenguaje legal, ósea no tiene una norma común a todos los países.

Haciendo un resumen muy sintético de como aplican los distintos países de Latinoamérica la Firma Electrónica, podemos apreciar las siguientes clases de firma usada:

**1.- Firma Electrónica**

**2.- Firma Electrónica avanzada**

**3.- Firma Digital**

Teniendo que una mayor seguridad y la validez reconocida se da, partiendo desde la Firma Electrónica hasta la Firma Digital, siendo más *flexible* la Firma Electrónica y siendo más rígida o estricta la Firma Digital.

Pero en este punto hay que notar que no todos los países tienen estas tres categorías de Firma aplicada en medios digitales, siendo muy diversos y dispares, existiendo en unos la Firma digital y en otros no, lo mismo con la Firma Electrónica avanzada, lo cual no permite un adecuado reconocimiento por parte de los países de una alternativa de Firma Electrónica común a todos estos países usuarios.

He aquí la problemática, ya que si bien es cierto existe por parte de los países miembros el reconocimiento del **La Ley Modelo UNCITRAL sobre Comercio Electrónico**; en materia de Firma Electrónica no hay un documento o manual supranacional, el cual todos reconozcan y que permita una estandarización de estas herramientas digitales usadas.

También hay que tomar en cuenta la problemática respecto del uso y la aplicación común que cada país ha tenido y ha visto por conveniente aplicar en su legislación para proponer las diversas formas de Firma Electrónica en sus países, y que aparentemente debería ser igual en todos los países ya que son modelos legales y económicos similares, con algunas excepciones, pero todas estas variaciones deben ser analizadas en una investigación profunda, en donde se debe llegar a un consenso.

## COMPARATIVA CON OTROS MODELOS: LA UNION EUROPEA

En la Unión Europea la situación es distinta ya que existe el Reglamento (UE) Nº 910/2014 del Parlamento Europea y del Consejo de 23 de julio de 2014, el cual trata sobre la Identificación Electrónica y los servicios de confianza para las transacciones electrónicas realizados por los países que forman parte de este grupo, y es en este documento donde se regulan los distintos conceptos de firma electrónica avanzada, simple y cualificada, siendo de plena aplicación en todos los Estados Miembros de la Unión Europea, además regulando lo relativo a las entidades que prestan los servicios como Prestadores de Servicios de Confianza.

## CONCLUSIONES Y RECOMENDACIONES

-Se debe realizar un estudio e investigación a nivel regional (Latinoamerica en su conjunto) de cómo se aplica actualmente las diversas opciones de Firma Electrónica en cada uno de los casos determinados, y como se aplica en cada país, para así poder identificar situaciones similares que darían la posibilidad de homologar el requerimiento de firma electrónica dependiendo del caso, por ejemplo no es lo mismo requerir la Firma Electrónica en su forma básica para realizar actos entre privados, que requerir la Firma Digital para presentar documentos ante una Entidad del Gobierno, es aquí donde se debe analizar la necesidad de su uso en

cada situación concreta, para poder identificar aplicaciones similares.

- Se debe tener en cuenta que el uso de una Firma electrónica o Digital estandarizada e igual entre los países de Latinoamérica, lograría la interoperabilidad entre estos países, lo cual nos dotaría de transparencia, simplificación de procedimientos, y un mejor flujo en el comercio tanto físico como electrónico a nivel región Latinoamérica e inclusive a nivel mundial.

- Cuando se realice un estudio de una posible estandarización de la Firma Electrónica, también se debe tomar en cuenta una política de accesibilidad a estas propuestas ofrecidas por los gobiernos, ya que muchas de las deficiencias actuales en la aplicación de las firmas electrónicas en cada país, son debido al poco alcance y conocimiento que tienen los ciudadanos de estas, debiendo ser estas soluciones lo más amigables, accesibles y económicas posibles.

Esperemos que a la larga todas estas investigaciones y estudios que se realizan y se realizaran sobre estos avances tecnológicos, lleguen a ser de utilidad práctica, no debiendo quedar solo en la teoría y en meras propuestas, sino que deben ser la base para que haya un cambio en la realidad y soluciones para las carencias y deficiencias existentes, y para que haya un común acuerdo entre todos los países usuarios de esta tecnología y así se logre el beneficio de la población latinoamericana en su conjunto.

## BIBLIOGRAFIA

AENOR (2007): UNE-ISO/IEC 27001:2007 – Tecnología de la información – Técnica de seguridad – Sistemas de Gestión de la Seguridad de la Información (SGSI) –Requisitos, Asociación Española de Normalización y Certificación, Madrid.

BOIX PALOP, A. (2010): "Previsiones en materia de neutralidad tecnológica y acceso a los servicios de la Administración", en COTINO HUESO, L. y VALERO TORRIJOS, J.(Coords.): Administración electrónica: la Ley/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del egobierno en España, Tirant lo Blanch, Valencia.

ESPINOZA CÉSPEDES, J.F. (2000), Contratación electrónica, medidas de seguridad y derecho informático, Lima, RAO

ORTEGA DÍAZ, J.F. (2008): La firma y el contrato de certificación electrónicos, Aranzadi, Cizur Menor.

PÉREZ PEREIRA, M. (2009): Firma electrónica: contratos y responsabilidad civil, Aranzadi, Cizur Menor.

PIÑAR MAÑAS, J.L. (2011): "Revolución tecnológica y nueva administración"

REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

## INTELIGENCIA ARTIFICIAL EN EL DERECHO INTERNACIONAL PÚBLICO Y LAS RELACIONES INTERNACIONALES: ¿PELÍCULAS DE “MARVEL” O REALIDAD?

**Autor:** *Maiger Dalay Urbina Romero\**

Las dinámicas actuales cada vez más siguen un curso tan acelerado, cambiante, ambivalente y complejo que los adjetivos para caracterizarla sencillamente se podrían quedar cortos, incluso si decidiéramos traer a escena las más refinadas figuras literarias de épocas pasadas y presentes.

Particularmente, ningún área del saber está exenta de la abundante información que se requiere manejar para seguir el ritmo de las situaciones que se generan cotidianamente y que, con sus aciertos y desaciertos, suben el nivel de discusión hacia campos multidisciplinarios. Ya no basta el manejo teórico de conceptos, antecedentes y lenguajes propios de la disciplina en la que se decide hacer vida, pues la interconexión nos lleva a construir puentes eficientes en procura de disminuir las brechas entre el deber ser (no solo normativo sino ideacional) y el ser que constituye la realidad en la que vivimos.



A tales efectos, frente a los nuevos retos que encarna la tecnología transversalizada en un mundo globalizado y entendiendo que la idea de mundo puede ser casi cualquier cosa que concentre diversidad de elementos, actores y variables, en las presentes líneas se harán unas muy breves aproximaciones respecto a la

inteligencia artificial aplicada actualmente en el Derecho Internacional Público y las Relaciones Internacionales, utilizando algunas analogías con el mundo cinematográfico, específicamente el universo *Marvel*<sup>13</sup>, en tanto que:

el cine tiene un destacado potencial educativo y formativo inherente (...) en la que los conceptos teóricos abstractos se convierten en situaciones prácticas concretas y se recrean supuestos –ficticios o reales– sobre los que proyectar y a los cuales que aplicar las competencias profesionales adquiridas mediante los estudios universitarios<sup>14</sup>.

En otros términos, aprovechando el contexto donde las personas consumimos múltiples servicios de entretenimiento masivo (Netflix, Youtube, entre otros) desde la comodidad de nuestro hogar, ya sea de forma voluntaria o quasi obligatoria (en el caso de la conocida pandemia del Covid-19), es por lo que buscamos potenciar “la

Abogado Magna Cum Laude, UCV. Licenciado Magna Cum Laude en Estudios Internacionales, UCV. Profesor de Teoría de las Relaciones Internacionales, UCV. Cursante de la Maestría en Derecho Internacional Privado y Comparado, UCV. Miembro del Consejo Directivo del Instituto Venezolano de Derecho y Tecnología.

<sup>13</sup> Ficción construida a partir de las historietas estadounidenses desarrolladas por la empresa Marvel

*experiencia vital*<sup>15</sup> de todos los involucrados en estas dos áreas, donde, como puede presumirse, la notable presencia del Estado-Nación en el eje de las mismas, representa una de las razones por las que aun cuesta encontrar muchos análisis dirigidos a la aplicación de la tecnología en los sacramentales espacios del bien común o los intereses nacionales.

Por demás, de forma meramente enunciativa, revelaremos algunos avances de inteligencia artificial (IA) para abrir la caja de pandora de una realidad algo incipiente en áreas tan tradicionales como las de la óptica ius-internacionalista pública. No se trata de esfuerzos heroicos, pero estamos convencidos que la inteligencia artificial incontrovertiblemente tiene manifiestas intenciones de perdurar en el tiempo con más de 14.605.000 posibilidades. *End Game* apenas comienza.

## I. ALGUNAS PRECISIONES CONCEPTUALES PREVIAS

Para manejar una línea de pensamiento clara, entenderemos que, a pesar de no existir criterio

Worldwide Inc fundada en 1939 y que sirve de sustento a las películas de superhéroes producidas por la franquicia de Marvel Studios.

<sup>14</sup> Ana Gemma, López Martón & José Anonio Perea Uncela, *El cine y el derecho internacional: materiales para la docencia*, Universidad El Bosque – Universidad Complutense de Madrid, 2014, p. 10.

<sup>15</sup> Ana Gemma, López Martón & José Anonio Perea Uncela, *El cine y el derecho...*ob. cit., p. 19.

pacífico en cuanto a todos sus elementos, lo cierto es que de manera muy simplificada, la IA es aquella donde los sistemas piensan y/o actúan de forma racional.<sup>16</sup>

Por su parte, el Derecho Internacional Público vendría a suponer un conjunto de normas y principios heterogéneos “*tanto por la índole de los sujetos que son sus destinatarios, como por la forma de su creación y el fin mismo que se propone*”<sup>17</sup>, a partir de los cuales se regulan las relaciones entre los actores políticos y sujetos de derecho que forman parte de la dinámica de la sociedad internacional. Características que se suman a la ausencia de jerarquía entre sus fuentes que “*deriva en la estructura descentralizada del Derecho Internacional...*”<sup>18</sup> e impulsa el desarrollo de áreas diversas en su seno tales como el Derecho Internacional Humanitario (DIH), Derecho Internacional de los Derechos Humanos (DIDH), Derecho Diplomático y Consular (DDC), Derecho Penal Internacional (DPI), Derecho Internacional de los Refugiados, Derecho Ambiental, entre otros tantos.

<sup>16</sup> Nina, Wormer, *Los sistemas expertos en las relaciones internacionales: aplicación a la clasificación de conflictos violentos*, Universidad Complutense de Madrid, Madrid, 2019, p. 27.

<sup>17</sup> Fermín, Toro Jiménez, *Derecho Internacional Público*. Volumen I, UCAB, Caracas, 2004, p. 16.

<sup>18</sup> Manuel Diez de Velasco citado por Adalberto, Urbina, Derecho Internacional de los Refugiados: aspectos

En cuanto a las relaciones internacionales, siguiendo un concepto lato de Celestino del Arenal, serían aquellas “*...entre individuos y colectividades humanas que configuran y afectan a la sociedad internacional en cuanto a tal*”<sup>19</sup>; de allí que estaríamos ante un análisis de la dinámica de los grupos de poder y de variables económicas, culturales, comerciales, sociales y otras tantas que, interdisciplinariamente, aluden a la esencia de dicha sociedad.

Por ende, lejos de estar hablando de áreas entendidas como compartimientos estancos, estamos abordando sectores del saber que intentaremos demostrar cómo convergen en la inteligencia artificial.

## II. DOS EJEMPLOS DE “IA” EN EL ÁMBITO INTERNACIONAL

### A. ¿Ultrón en los terrenos del DIH y DIDH?

Hablar de Ultrón<sup>20</sup> dentro del referido universo cinematográfico Marvel, representa lo que se conoce como sistemas de armas autónomas o lo que es lo mismo AW (autonomous weapons). Al respecto, tal como indica la doctrina son

conceptuales universales y regionales, UCV-UCAB-SJR, Caracas, 2012, p. 28.

<sup>19</sup> Celestino del Arenal, *Introducción a las relaciones internacionales*, Tecnos, España, 2003, p. 424.

<sup>20</sup> En la película Avengers: Age of Ultron, se trataría de un sistema de inteligencia artificial programada por los personajes de Anthony Stark (Iron Man) y Bruce Banner (Hulk) con la exclusiva misión del mantenimiento de la paz, tanto a nivel interno como a nivel de amenazas externas para el planeta Tierra.

*“capaces de llevar a cabo una misión con intervención humana limitada o aún sin ella. Dependiendo del grado de implicación de la actividad humana, pueden ser semiautónomas o plenamente autónomas. Además, varía su letalidad...”<sup>21</sup>.*

Lejos de ser ficción, algunos familiares contemporáneos de Ultrón que moverían las bases del *ius ad bellum* serían el “...Sistema Phalanx, el C-RAM o el Northrop Grumman X-47 B de los Estados Unidos; el Harpy de Israel, el Taranis del Reino Unido o los robots Samsung Techwin en la zona desmilitarizada que separa a las dos Coreas”<sup>22</sup>

Ahora bien, reiteradamente se viene sosteniendo que sistemas como estos no respetarían, entre otros, el principio de distinción, el principio de no discriminación y el principio de proporcionalidad del DIH, en tanto que no sabrían identificar quien sería un no combatiente civil digno de protección, combatientes heridos o interpretar situaciones de rendición, ni tampoco serían capaces de decidir

<sup>21</sup> Daniela, Quelhas citada por Cesáreo Gutiérrez, Espada & María José, Cervell Hortal, “Sistemas de Armas Autónomas, Drones y Derecho Internacional” en: Revista del Instituto Español de Estudios Estratégicos, N° 2, 2013, p. 29.

<sup>22</sup> Cesáreo Gutiérrez, Espada & María José, Cervell Hortal, “Sistemas de Armas...”, ob. cit., p. 34.

<sup>23</sup> Ibídem, p. 35

<sup>24</sup> Ibídem, p. 37.

<sup>25</sup> Leonel, Gorriín Mérida, “Breve comentario sobre el desafío que para el DIH representan las armas

en qué situaciones el daño probable causado a civiles sería excesivo en relación con la ventaja militar, de conformidad con los artículos 51.5.b y 57.2 del Protocolo I de 1977 de los Convenios de Ginebra relativos a los conflictos armados<sup>23</sup>.

Por si fuera poco, su uso compromete la discusión sobre la responsabilidad individual de los mandos militares a la luz de los Convenios de Ginebra<sup>24</sup>, cambiaría la idea de teatro de operaciones, ya que “...también abarca el espacio de donde se ordenan las acciones que deben cumplir las armas autónomas”<sup>25</sup> y aviva el debate sobre el artículo 36 del citado Protocolo de 1977<sup>26</sup> por cuanto amplia en exceso el rango temporal y especial de la guerra. Tal como sucede en la película, recordemos que Ultrón no hace distinciones en búsqueda de su enemigo e incluso desarrolla un viraje en su acción propia que, si bien es algo de lo que adolecen los actuales sistemas de armas autónomas, no es menos cierto que revela la posibilidad que una “Legión

autónomas” en: Centro de Estudios de Derecho Internacional Humanitario, Cuba, 2016, p.1.

<sup>26</sup> Textualmente reza: “cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante”.

de Hierro”<sup>27</sup> cauce destrozos generalizados que vulneren las garantías a la vida o se puedan convertir en ejecutores de una suerte de genocidio controlado desde algún Estado frente a poblaciones particulares, en absoluto desconocimiento al DIDH y consecuencialmente al DPI.

Las posibles ventajas de tipo técnico, económico, político, militar y emocional que puede brindar el perfeccionamiento de los sensores, data y reglas de probabilidad introducidas en la programación de estas armas robotizadas al modo Ultrón, aun pierden estrepitosamente la batalla contra los elementos de humanidad que dotan de racionalidad a la ciencia jurídica y que, cambiando lo cambiante, son incorporados por “Visión”<sup>28</sup> en dicho universo cinematográfico.

### B. ¿F.R.I.D.A.Y como asesora de analistas internacionales?

El sistema ficticio que ayuda incansablemente a Tony Stark (Iron Man) y que fuera conocido como Female Replacement Intelligent Digital Assistant Youth (F.R.I.D.A.Y) equivale a hablar de los Sistemas Expertos (SE), los cuales simulan el razonamiento de especialistas humanos en determinadas áreas del saber,

siguiendo un proceso de inferencias cuya mayor o menor complejidad, le permite aportar soluciones con base a un cumulo de hechos o informaciones previas<sup>29</sup>.

Históricamente, se comenzaron a poner en práctica en la ciencia social internacional hacia finales de los años 80 del siglo XX, pero lo que se programó en modelos computacionales de Alker y Christensen, en el modelo Tanaka, o en el de Caldugh, en cuanto a los procesos de paz de Naciones Unidas, el comportamiento de China en crisis internacionales o para predecir relaciones bilaterales entre dos países en situación de crisis o conflicto<sup>30</sup>, respectivamente, constituyen parte de la aplicación primigenia de un SE. Todo ello, con miras a coadyuvar con el trabajo de decisores que debían ponderar los escenarios de acción internacional sin dejar de escatimar la dimensión política, jurídica y ética de los mismos.

Justo en ese punto, la comparación con F.R.I.D.A.Y es pertinente porque, por ejemplo, fue usada dando consejos para optimizar el combate durante el enfrentamiento entre los superhéroes conocidos como los Vengadores. A su vez, colaboró configurando diferentes posibilidades de viajes en el tiempo

<sup>27</sup> Drones que, por momentos, se transforman en soldados automáticos influenciados por Ultrón en el universo Marvel.

<sup>28</sup> Androide que en el desarrollo del film derrota a Ultrón y, por definición, posee ciertas cualidades humanas.

<sup>29</sup> Nina, Wormer, *Los sistemas expertos en...* ob. cit., p. 43.

<sup>30</sup> Ibídem, p. 6.

dentro del reino cuántico, como mecanismo de solución ante la desaparición de la mitad del universo que ocurre dentro de la saga ficticia. En este mismo sentido, por cierto, destacaría el sistema de Inferencia de Prioridades de Políticas para el Desarrollo Sostenible (IPP) aplicado hoy por hoy en México, Uruguay o Colombia junto al PNUD y el Alan Turing Institute de Londres, con modelos probabilísticos que determinan qué deberían priorizar los gobiernos, anticipando los efectos de inversiones tendientes a garantizar los ODS<sup>31</sup>.

### III. A modo de colofón

Si comparamos las profusas discusiones prácticas sobre IA en áreas como el Derecho de Patentes, Derecho Penal, Derecho Internacional Privado o el Derecho Financiero, pareciera que el Derecho Internacional Público está quedando a deber. Sin embargo, paradójicamente, desde estos espacios donde hace vida el relacionamiento internacional, es donde se están gestando regulaciones conciencizadas y debates como el del Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial de la Comisión Europea o los de la Convención sobre Ciertas Armas Convencionales (CCW). Asimismo, tenemos el estudio comparado de la

Universidad de Harvard publicado en enero del presente año, con el fin de verificar coincidencias jurídicas a lo largo del orbe. En definitiva, todos estos son esfuerzos que nos hacen pensar en una suerte de “Acuerdos de Sokovia”<sup>32</sup> en clave contemporánea.

<sup>31</sup> Ver: <https://www.technologyreview.es/s/12294/la-onu-trabaja-en-un-simulador-de-ia-para-acelerar-el-logro-de-los-ods#:~:text=El%20software%2C%20denominado%20inferencia%20de,en%20vez%20de%20en%20otro.>

<sup>32</sup> Documento del universo Marvel donde se limitaban algunos usos tecnológicos, al tiempo que debían registrarse los mutantes y súper humanos.

Autora:  
Gardenia Revollo

# LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN Y EL PLURALISMO JURÍDICO

## I. INTRODUCCIÓN

América Latina estas últimas décadas ha ido desarrollando el concepto de pluralismo jurídico e interculturalidad, por citar como ejemplo, Bolivia y Colombia a través de sus últimas reformas constitucionales del año 2009 y 1991 respectivamente, reconocieron el pluralismo como parte de su ordenamiento jurídico.

El pluralismo jurídico es la antítesis del monismo jurídico, mientras la mayoría de los países cuentan con un solo ordenamiento jurídico que rige en todo su territorio y se basa en el positivismo jurídico; la idea del pluralismo jurídico es adoptar dentro de un Estado de derecho, diversos sistemas y prácticas jurídicas de igual jerarquía (Ariza, 2015, p.170) reconociendo la interculturalidad de sus habitantes. Al respecto, el parágrafo II del artículo 179 de la Constitución Política del Estado de Bolivia, señala: “*La jurisdicción ordinaria y la jurisdicción indígena originario campesina gozaran de igual jerarquía*”.

Al mismo tiempo que estas ideas van desarrollándose e implementándose a través del movimiento neoconstitucionalista, se podría decir que a la par o que incluso a una mayor velocidad y potencia, se están



implementando en los sistemas jurídicos el uso de tecnologías de información y comunicación (en adelante TIC) y el gobierno electrónico.

Este breve escrito, pretende reflexionar sobre estos hechos y si es posible la coexistencia de pluralismos jurídicos y el uso de TIC en la administración de justicia, tomando como objeto de análisis al país latinoamericano Bolivia.

## II. EL PLURALISMO JURÍDICO EN BOLIVIA

La última reforma de la Constitución Política del Estado de Bolivia (en adelante CPE) en su artículo 1 declara: *“Bolivia se constituye en un Estado Unitario Social de Derecho Plurinacional Comunitario, libre, independientes, soberano, democrático, intercultural, descentralizado y con autonomías. Bolivia se funda en la pluralidad y el pluralismo político, económico, jurídico, cultural y lingüístico, dentro del proceso integrador del país”*.

Este Estado de Derecho reconoce dos tipos de sistemas jurídicos dentro de su territorio, la justicia ordinaria y la justicia indígena originario campesina (en adelante IOC). Esta última consiste en aplicar principios, valores culturales, normas y procedimientos propios de los miembros de una nación o pueblo indígena originario campesino; Bolivia reconoce en su CPE 37 naciones y pueblos indígenas originarios campesinos.

Entonces el poder estatal central no sería la única y exclusiva fuente de Derecho, garantizándose una sociedad intercultural. Es así que, cuando asuntos jurídicos correspondientes a la jurisdicción IOC llegan a los más altos Tribunales

<sup>33</sup> CIDH, Tercer Informe sobre la Situación de los Derechos Humanos en Paraguay. Doc. OEA/Ser./L/VII.110, Doc. 52, 9 de marzo de 2001, Capítulo IX, párr. 12. CIDH, Segundo

de Justicia de Bolivia, que son el Tribunal Supremo y el Tribunal Constitucional, los magistrados deben cambiar de chip mental y fallar conforme los usos y costumbres de estas naciones, para lo cual se auxilian de estudios culturales antropológicos elaborados por la Unidad de Descolonización del Tribunal Constitucional, que les permite conocer la pluralidad de valores y estilos de vida de cada pueblo IOC.

Estas medidas que opta Bolivia, están en concordancia con lo establecido por el Convenio 169 de la Organización Internacional del Trabajo (OIT) que, para la Corte Interamericana de Derechos Humanos (CIDH), es el instrumento internacional de derechos humanos más relevantes para los derechos indígenas<sup>33</sup>. La CIDH y la Corte Interamericana también señalan que se debe tomar en consideración la identidad cultural para efectos de asegurar a los pueblos indígenas una protección efectiva que tome en cuenta sus particularidades propias, sus características económicas y sociales, así como su situación de especial vulnerabilidad, su derecho

Informe sobre la Situación de los Derechos Humanos en el Perú. Doc. OEA/Ser.L/V/II.106, Doc. 59 rev., 2 de junio de 2000, Capítulo X, párr. 7

consuetudinario, valores, usos y costumbres.<sup>34</sup>

Lo anteriormente expuesto es un ideal al que se pretende alcanzar, la realidad es mucho más compleja, debemos partir de que el pluralismo jurídico nace del mismo positivismo jurídico y; el positivismo jurídico es aquella doctrina que reconoce valor solamente a las normas de derecho positivo y, el derecho positivo es el conjunto de normas jurídicas vigentes de un Estado emanadas por autoridad competente y de carácter coercitivo. Estamos ante una paradoja cuando nos basamos del derecho positivo para aplicar un derecho consuetudinario.

Para entender mejor esta paradoja, un ejemplo en Bolivia es la Ley de Deslinde Jurisdiccional (Ley N° 073), que al regularizar el ejercicio de la jurisdicción IOC termina sometiendo a la misma, en razón de competencia material a la jurisdicción ordinaria, y a su vez también está sometida a la jerarquía constitucional y de los derechos humanos. No olvidemos que los derechos humanos son principios universales que pueden tener un enfoque diferencial respecto a las cosmovisiones y valores plurales (Attard, 2016, p.7).

Podemos inferir, que el pluralismo jurídico es una corriente que continua en desarrollo, aún está gateando esforzándose por dar sus primeros pasos firmes y poder correr, pero sus piernas son

endeble y tiene muchos obstáculos más por delante. Por otro lado, tenemos las tecnologías de información y comunicación que son un fenómeno que crece y corre a nivel global, su impacto es de carácter transversal en distintas áreas de la vida, incluyendo la legal y sus diferentes corrientes. Veamos:

### III. TIC en Bolivia

El derecho a las telecomunicaciones es un derecho fundamental reconocido en la CPE de Bolivia, partiendo de esta norma suprema, se cuenta con diferentes textos normativos que introducen a la sociedad herramientas técnico legales que son las tecnologías TIC para el desarrollo de las actividades del día a día. Entre ellas, la ciudadanía digital, la firma digital, buzones electrónicos de notificación, banca digital, teletrabajo; que se traducen en un crecimiento constante del Gobierno Electrónico y cultura digital.

Actualmente el país cuenta con un plan de implementación de Gobierno Electrónico (2017-2025), partiendo de 3 ejes: 1) Soberanía tecnológica en base a una infraestructura de telecomunicaciones; 2) Gobierno eficiente, consiste en lograr mayor eficiencia en la gestión pública a través de la reingeniería de procesos y procedimientos para eliminar la burocratización y; 3) Gobierno abierto y participativo, consiste en consolidar y dinamizar distintos

<sup>34</sup> 1 Corte IDH. Caso Comunidad Indígena Yakye Axa Vs. Paraguay. Fondo, Reparaciones y Costas.

Sentencia de 17 de junio de 2005. Serie C No. 125, párr. 63

aspectos de la vida social a través del acceso de datos abiertos e información, para un mayor participación y control social.<sup>35</sup>

#### IV. TIC, ¿AMENAZA O VENTAJA PARA EL PLURALISMO JURÍDICO?

Para responder esta pregunta, es necesario comenzar con los efectos del gobierno electrónico, como se expuso, la misión es alcanzar una soberanía tecnológica, un gobierno eficiente, abierto y participativo; desde otra perspectiva un gobierno con mayor control sobre su territorio y principalmente con mayor información de sus habitantes.

Esta información crea una Big Data de un país, la misma que puede ser usada para mejorar procesos y procedimientos a través de la inteligencia artificial (IA), por ejemplo, en la administración de justicia.

Actualmente, países como EEUU, Estonia, China, Argentina y otros más, implementan la IA para tomar decisiones judiciales, otros países como Colombia y Brasil están en vías de implementarla.

Esta situación ha generado varias críticas en favor y en contra, entre las positivas esta la disminución de la carga procesal, la celeridad en los procesos, la transparencia en las decisiones y seguridad jurídica; entre las negativas tenemos

observaciones al algoritmo relacionadas a la retroalimentación al software, la frecuencia de análisis de defectos y errores que pueda tener el sistema, la pérdida de control social por la complejidad de entendimiento que requiere el software y que detrás de ese algoritmo que tomara estas decisiones está igual el ser humano, puede que ya no sea un juez directamente, sino un matemático y/o científico de datos.

Esto nos lleva, a una cuestión de perspectiva donde pueden materializarse dos hipótesis, una positiva que planteé que el uso de TIC a través del Big Data e IA en el sistema de administración de justicia, delimitará de una manera más clara los límites entre la jurisdicción ordinaria y la jurisdicción IOC, en la que se fortalezca el pluralismo jurídico a través de órganos de administración de justicia propios y exclusivos acorde a los usos y costumbres de la comunidad, dejando para la justicia ordinaria el uso de IA. Otra negativa, en la que el Big Data y la IA sean de aplicación a todo el sistema de justicia y debido a que se basa en datos, números, estadísticas y probabilidades, no exista lugar para la excepción, traduciéndose en un sistema discriminatorio contra la interculturalidad y cosmovisiones distintas y minoritarias.

#### BIBLIOGRAFÍA.

<sup>35</sup> [2025 Gobierno Electrónico Plan de Implementación](#)

- Ariza Santamaría Rosembert. (2015) El pluralismo jurídico en América Latina y la nueva fase del colonialismo jurídico en los estados constitucionales. *Insurgencia*. 1.
- Attard Bellido María Elena. (2016) Repensando los diálogos interjurisdiccionales desde el Abya Yala: La construcción plural de los derechos en un contexto multinivel. *Documentos de Trabajo SLADI*. 10
- O'neil Cathy. (2016) Armas de destrucción matemática. Como el big data incrementa la desigualdad y amenaza la democracia. Editorial orhi.
- <https://www.ambito.com/negocios/inteligencia-artificial/puede-la-mejorar-la-justicia-n5076798>
- CPE Constitución Política del Estado Plurinacional de Bolivia, 2009. Bolivia
- Ley N° 073 de Deslinde Jurisdiccional, 2010. Bolivia



**#MIS DATOS  
SOY YO**

La privacidad de las personas contagiadas con coronavirus es algo en lo que debemos pensar.

No divulgemos fotos de familiares y de amigos enfermos.

EDI

en preparación

## Colección «elderechoinformático.com»



11 volúmenes

Guillermo M. Zamora dirección

- 1 — La prueba informática
- 2 — Negocios jurídicos en tiempos de Internet
- 3 — Delitos informáticos
- 4 — Propiedad intelectual en la era de la información
- 5 — Gobierno digital y gobierno abierto
- 6 — Datos personales, su protección
- 7 — ODR, Resolución de Disputas Online
- 8 — Firma digital
- 9 — Régimen jurídico de nombres de dominio
- 10 — Teletrabajo
- 11 — Aspectos jurídicos del *cloud computing*

Novedad

## Código Civil y Comercial de la Nación analizado, comparado y concordado



Alberto J. Bueres dirección

2 tomos | Artículos 1 - 2671

Análisis complementario de las principales normas que inciden  
en el «Derecho del trabajo» al cuidado de Juan J. Formaro

Contiene: Cuadro comparativo de normas. Índice alfabético de voces

• **Tomo 1. Arts. 1 a 1429.** Autores: Juan M. Aparicio – Jorge O. Azpiri – Eduardo Barreira Delfino – Jorge Berbère Delgado – Rodolfo Borghi – Martín Calleja – Marcelo Camerini – Carlos A. Carranza Casares – Rubén Compagnucci de Caso – Leandro Cossari – Cecilia Danesi – Paula Feldman – Diego Fissore – Juan J. Formaro – Marcelo J. Hersalis – Germán Hiralde Vega – Nicolás Kitainik – Alejandro Laje – Sabrina Luini – Ramón Massot – Luz Pagano – Hernán Pagés – Alfredo Popritkin – Laura Ragoni – Lucas Ramírez Bosco – Carlos E. Tambussi.

• **Tomo 2. Arts. 1430 a 2671.** Autores: Liliana Abreut de Begher – Beatriz Areán – Jorge O. Azpiri – Eduardo Barreira Delfino – María I. Benavente – Gabriela Boquin – Roque Caivano – Carlos Calvo Costa – Marcelo Camerini – Juan Casas – Federico Causse Rubén Compagnucci de Caso – Leandro Cossari – Nelson Cossari – José Fajre – Eduardo N. Farinati – Juan J. Formaro – Andrés Fraga – Alberto Gabás – Lidia Garrido Cordobera – Marcelo J. Hersalis – Gabriela Iturbide – Jorge Juliá – Alejandro Laje – Ricardo Nissen – Martín Paolantonio – Christian R. Pettis – Lucas Ramírez Bosco – Javier Rosembrock Lambois – Luciana Scotti – Gabriel Ventura – Luis M. Vives.

Por la situación actual que se vive a nivel mundial, muchas empresas han tenido que innovar, y utilizar las TIC's, para seguir funcionando; aunque algunas personas consideran que las comunicaciones electrónicas y el e-Commerce, son modelos o herramientas que iniciaron hace unos años atrás, la realidad es otra.

Los primeros indicios de

Aunque EDI fue pionera, existen otros sucesos que marcaron el desarrollo de las Comunicaciones Electrónicas y el e-Commerce, por mencionar algunas se encuentran:

- 1979 Michael Aldrich es considerado el inventor del e-Commerce tras conectar por primera vez una Tv, un ordenador y un teléfono para vender productos de

## RECONOCIMIENTO DE LAS COMUNICACIONES ELECTRÓNICAS Y EL COMERCIO ELECTRÓNICO (PERSPECTIVA LEGAL)

Autor Manolo Rivera

Comunicación Electrónica y Comercio Electrónico, se remonta en los años de 1960, con el Intercambio Electrónico de Datos (EDI), el cual consiste en una forma estandarizada y estructurada de comunicación electrónica, que han permitido realizar operaciones comerciales haciéndolas más eficientes, y minimizando las transacciones en papel, por su parte la Organización de Naciones Unidas, desarrollo EDIFACT (Interchange for Administration, Commerce and Transport), el cual es un conjunto de reglas de sintaxis para el intercambio de mensajes entre diferentes países, relacionados al comercio de bienes y servicios.

supermercado.

- 1995 Presidential Bank en Estados Unidos, primer banco online reconocido.
- 1998 Fundación de Google y PayPal (considerada la primera Fintech). Ritmoteca para realizar descargas de música.
- 2012 las ventas por e-commerce alcanzan el primer trillón de dólares.
- 2020 Netflix reporta 193 millones de suscriptores e ingresos superiores a los seis mil millones, seguido de Amazon Prime con 150 millones de suscriptores, y Disney + con 60.5 millones (sin tomar en cuenta Hulu y

ESPN que forman parte de Disney).

En Guatemala, el 23 de septiembre de 2008, fue emitida la “Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas” Decreto 47-2008, la cual tiene por objeto:

1. El Reconocimiento legal, de todos aquellos actos o contratos que se realicen entre particulares y/o instituciones públicas, de forma local o internacional, utilizando “Comunicaciones Electrónicas”, dándole validez y fuerza obligatoria entre las partes.
2. Darle valor jurídico a la firma electrónica avanzada.

### **Antecedentes:**

En los Estados Unidos en 1996, se puso de manifiesto por primera vez la creación de un marco legal, que reconociera la validez legal de las Comunicaciones Electrónicas, la consecuencia de estas acciones conllevo a la incorporación de la iniciativa al Código de Comercio Uniforme (Uniform Commercial Code); en 1997 se aprobó la Ley Modelo de Comercio Electrónico, que ha servido de base para otros países, entre ellos Colombia, Chile, y argentina; mientras que la Unión Europea, inicio con un marco jurídico comunitario para la firma electrónica por medio de la Directiva 1999/93 (derogada actualmente por UE N. 910/2014)

Las bases para la creación de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas de Guatemala fueron la ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil sobre las firmas electrónicas (2001), y la Ley de Comercio Electrónico de Colombia (Ley No. 527), principalmente tiene muchas coincidencias con la ley colombiana; el ámbito de aplicación de las tres leyes es la misma.

### **Aspectos legales para tomar en cuenta**

Es común que los comerciantes emitan sus declaraciones de voluntad de forma verbal o escrita, y dependerá de cada acto o contrato en particular, de las formalidades y requisitos para su validez.

Las personas compran y venden productos sin necesidad de un contrato escrito en papel, o prestan servicios de mensajería, asesoría legal, médica, o jardinería, sin contar con un contrato escrito en papel y firmado para su validez.

El código civil guatemalteco establece en su artículo 1574, que las declaraciones de voluntad pueden realizarse verbalmente, y establece el contrato por teléfono en el artículo 1524 (verbalmente a través de un medio electrónico); inclusive, en materia laboral el código de trabajo permite los contratos verbales en su artículo 27; y por medio del acuerdo ministerial 324-2019 del Ministerio de Trabajo son aceptados los contratos digitales

que cuenten con firma electrónica avanzada.

Mientras tanto el Código de Comercio de Guatemala en su artículo 671 establece que los contratos para su validez no están sujetos a formalidades especiales, y cualquiera que sea la forma en que se celebren las partes quedan obligadas (siempre existen excepciones a la regla, ej. Solemnidad de la sociedad).

Es redundante decir, que el derecho laboral es poco formalista, y el derecho civil es conocido por su formalidad. Mientras que el derecho mercantil se caracteriza por ser poco formalista, dinámico e internacional, es por ello la extrema movilidad de los contratos mercantiles, que en muchos caso hacen suprimir todo requisito de forma para su validez, y desaparecen requisitos como el de escritura; si estos requisitos de forma del derecho civil, hubieran sido trasladados al derecho mercantil, hubieran distorsionado los contratos de comercio, y ahora con las nuevas tecnologías nacen nuevas formas para contratar y obligarse.

### Documento y Documentación

Es por ello importante diferenciar entre el documento, y la documentación, la primera es una declaración de voluntad encaminada a producir efectos jurídicos, es específicamente el acto o contrato, por ejemplo, una compraventa, testamento, letra de cambio, etc. y la segunda, es el soporte material o

inmaterial en donde consta el acto o contrato, por ejemplo, papel (documento privado, protocolo, etc.), bits (documento electrónico, grabación, etc.).

### Las ventajas del Reconocimiento de las Comunicaciones Electrónicas

- Agilizar procesos institucionales, los cuales cada año se vuelven más burocráticos.
- Disminuir costos para las entidades públicas y privadas.
- Mayor alcance de la oferta, nuevos mercados.
- Celebrar contratos a distancia.
- Dar seguridad jurídica a los documentos que lleven firma electrónica avanzada.
- Incentivar el comercio electrónico, dando seguridad jurídica a las partes de los actos o contratos que se realizan, principalmente si cuentan con firma electrónica avanzada.

### Desventajas

- Ciberdelitos.
- Protección de datos.
- Protección al consumidor.
- Impuestos.
- Seguridad de bienes y servicios (tener seguridad que lo que se compró, es lo que se recibe).

## Elemento Real de las Comunicaciones Electrónicas:

La comunicación electrónica, es toda comunicación que las partes realizan por medio de mensaje de datos.

Mensaje de datos: Es cualquier información (Contrato, aviso, documento, fotografía, audio, etc.), enviada, recibida o archivada por medios electrónicos, magnéticos ópticos, pudiendo ser fax, correo electrónico, Instagram, Facebook.

Esto se refiere, por ejemplo, a que dos personas podrían realizar un contrato a través de WhatsApp, en donde una persona se obliga a prestar un servicio, y la otra persona se compromete a realizar un pago por recibir el servicio, y estas declaraciones de voluntad, tienen la misma validez y fuerza obligatoria, como si lo hubieran escrito en un papel.

(Es de tomar en cuenta, que el elemento real de cada acto o contrato se sujetara a su norma aplicable específica).

## Elemento personal de las Comunicaciones Electrónicas:

Iniciador: Es la parte que, a título personal, o en nombre de otro (autorizado), envía un mensaje de datos, sin actuar como intermediario.

Intermediario: Es la parte que, actuando por cuenta de otra, envíe, recibe o archive un mensaje de datos.

Destinatario: Es la parte designada por el iniciador, para recibir el

mensaje de datos, sin actuar como intermediario.

## Elemento Formal:

Las consecuencias jurídicas de las Comunicaciones Electrónicas se regirán conforme a la norma específica aplicable, del acto o negocio jurídico que se realice; tomando en cuenta también tiempo y lugar de envío, y recepción de la comunicación electrónica.

El reconocimiento de las Comunicaciones electrónicas nos permite construir nuevos modelos de negocios, teniendo presencia en nuevos mercados, y si esto va acompañado de la utilización de las nuevas tecnologías, como una **firma electrónica avanzada**, **VPN**, y **Blockchain** le estaremos dando mas seguridad y certeza jurídica a los actos y contratos para que no sean modificados ni alterados con facilidad.



Manolo Rivera 

[I.manolorivera@gmail.com](mailto:I.manolorivera@gmail.com)

---

ELDERECHOINFORMATICO.COM  
ESTAMOS  
DONDE QUERÉS VOS

---

• S O M O S , L A R E D •

\\EL CENTRO DE FORMACIÓN E  
INFORMACIÓN MÁS GRANDE DE  
IBEROAMERICA\\

