TRIBUNA LIBRE

EDICIÓN DIGITAL

EDICIÓN 8/1

OCTUBRE 2021



ALBAN BONILLA SANDÍ
TICS Y ENSEÑANZA DEL DERECHO, VENTAJAS, LÍMITES, RETOS

VILMA SÁNCHEZ DEL CASTILLO
ENTRE EL BACK TO BASICS Y LOS NUEVOS PARADIGMAS DE LA REVOLUCIÓN TECNOLÓGICA

JULIO CÓRDOBA ELIZONDO
REFLEXIONES SOBRE ALGUNAS AMENAZAS CONTRA EL BITCOIN

LEÓN WEINSTOK
FORMAS DE LEGITIMACIÓN DEL TRATAMIENTO DE DATOS PERSONALES

JUAN ESTEBAN DURANGO RAVE
ACREDITACIÓN DE LAS ACTUACIONES ELECTRÓNICAS PERSONALES: DE LA FIRMA ELECTRÓNICA A LA IDENTIDAD DIGITAL AUTO-SOBERANA

JOSÉ ADALID MEDRANO

EL DELITO DE VIOLACIÓN DE DATOS PERSONALES

ISSN: 2953-7339

EDICIÓN ESPECIAL DE
DERECHO INFORMÁTICO

ESCUELA LIBRE DE DERECHO
UNIVERSIDAD

TRIBUNA LIBRE

Tribuna Libre

Dr. Ricardo Guerrero Portilla
Director

Consejo Editorial

Licda. Andrea Gómez Ulloa
Dr. Albán Bonilla Sandí
MSc. Cristina Gómez Fonseca
Dr. Ricardo Guerrero Portilla
Lic. José Adalid Medrano

Tribuna Libre es una publicación sin fines de lucro, patrocinada por la Universidad Escuela Libre de Derecho, dedicada a la promoción y divulgación del libre pensamiento.

Revista Tribuna Libre. Vol. 8, No. 1 (1 - 209). Octubre - 2021. Primera Edición Digital

ISSN: 2953-7339

ESCUELA LIBRE DE DERECHO UNIVERSIDAD

EDICIÓN DIGITAL

CONTENIDOS

0 **Presentación**

1 **Alban Bonilla Sandí**
TICs y enseñanza del Derecho,
ventajas, límites, retos.

2 **Vilma Sánchez Del Castillo**
Entre el back to basics y los nuevos
paradigmas de la revolución tecnológica
Pensamientos para la reducción de la brecha
tecnologíca-jurídica y la estandarización de
las legislaciones: caso costarricense.

3 **Julio Córdoba Elizondo**
Reflexiones sobre algunas
amenazas contra el bitcoin.

4 **José Adalid Medrano**
El delito de violación de
datos personales.

5 **León weinstok**
Formas de legitimación del tratamiento
de datos personales.
(Basis for processing personal information)

6 **Juan Esteban Durango Rave**
Acreditación de las Actuaciones Electrónicas
Personales: de la Firma Electrónica a la
Identidad Digital Auto-Soberana.

PRESENTACIÓN

Con particular emoción, TRIBUNA LIBRE, revista de la Universidad Escuela Libre de Derecho viene hoy, treinta y dos años después de haber visto la luz por primera vez (1989), a presentar lo que correspondería al No 8 de su secuencia editorial, pero No 1 en su nueva y remozada versión digital.

Consideramos menester recordar algunos preceptos indicados en la presentación del primer número, pues creemos que ellos deben seguir inspirando y orientando esta nueva versión digital:

"TRIBUNA LIBRE logra ver la luz luego de un intenso trabajo, que ha implicado esfuerzo, sacrificio y mística de muchas personas,… quienes convencidas de que no puede haber formación integral de un futuro profesional sin investigación científica y sin posibilidad de manifestar con argumentos serios su pensamiento… Surge TRIBUNA LIBRE, haciéndole honor a las Tribunas Romanas, en donde se exponía el pensamiento de los grandes forjadores de la civilización, cuna de nuestro sistema jurídico; y al planteamiento filosófico que inspira nuestra Casa de Enseñanza, la cual es la libertad de pensamiento y expresión…. el único condicionamiento que pondrá TRIBUNA LIBRE al que desee que su pensamiento sea conocido a través de ella, es que su artículo sea serio y respetuoso del honor ajeno, … así como que haya criticidad y argumentación en el planteamiento…" (Guerrero Portilla, 1989, p.1).

Hoy TRIBUNA LIBRE, en su remozada versión digital, vuelve con entusiasmo y esperanza al Foro Nacional, con la firme y clara convicción de rescatar el acervo científico que la Universidad Escuela Libre de Derecho genera en las diferentes instancias del desarrollo académico de su carrera de Derecho, pues resulta un sinsentido intelectual dejar en nuestros anaqueles los resultados de la investigación científica realizada por docentes y discentes de los distintos grados académicos.

Al aprestarnos a celebrar el 45 aniversario de fundación de la Escuela Libre de Derecho y ante el advenimiento vertiginoso, a raíz de la pandemia del SARS COV 2, que sin avisar y de un día para otro, nos introdujo en la vorágine de la digitalización académica en todos sus niveles, TRIBUNA LIBRE vuelve con una edición monográfica referida esencialmente al Derecho Informático.

Sin embargo, es oportuno señalar que, a pesar de lo novedoso que pueda verse hoy el tratamiento de la temática relacionada jurídicamente con las Tics, aunque parezca mentira, para TRIBUNA LIBRE no es una materia del todo desconocida, por cuanto desde su primer número en 1989, cuando apenas empezábamos a tener las primeras relaciones con los ordenadores, que no eran más que unos procesadores de texto que se arrancaban con un disquete de 5 ¼ para instalarles el sistema operativo MS-DOS, así como el procesador de texto WordStar, cuyos comandos debían ser aprendidos de memoria por el usuario, o bien, poco después, el más amigable procesador de texto WordPerfect, soñado por los notarios de la época, la revista incorporó como su primer artículo "La Informática Jurídica … para repensar el Derecho", del catedrático Dr. don Juan Diego Castro Fernández (1989), donde con visión de futuro indicaba:

"De los cuatro mil cuatrocientos profesionales que se encuentran inscritos en el Colegio de Abogados, algunos cientos de ellos poseen equipo computacional y la Junta Directiva proyecta asesorar y financiar a los juristas para que adquieran microcomputadoras, y obviamente no serán las máquinas las que marquen las diferencias entre los abogados, las que generen el desempleo, pero dentro de muy pocos años, existirá una enorme brecha entre los informatizados y los otros. Así como la caligrafía era una virtud indispensable de los viejos abogados,

hoy ninguno de nosotros cuestiona la mecanografía como vehículo indispensable, para ejercer la abogacía y el notariado… y mañana, antes de que los relojes electrónicos marquen el año dos mil, los juristas que no sean capaces de operar una computadora, estarán en mucho mayor desventaja que los malos calígrafos que ejercieron, sin mayor gloria, la abogacía y el notariado, antes de que las máquinas nos prestaran su auxilio." (p.6).

Evidentemente, hoy no tenemos de los "otros" Abogados, pues resulta inconcebible e incomprensible, siquiera, imaginarnos un profesional de las Ciencias Jurídicas, que no tenga un conocimiento, por lo menos básico, del manejo de las tecnologías de la información y la comunicación. El maestro Castro Fernández (1989), en ese primer artículo de nuestra revista, para la exposición de sus ideas indicó: "Acogemos la clasificación en la que son ordenadas las tareas informático –jurídicas que se realizan hoy día y las finalidades a las cuales están dirigidas. Distinguiremos las siguientes categorías de la informática jurídica: Documental, De gestión, Decisoria y Analítica." (p.6). Temáticas todas de gran relevancia hoy, sin dejar de lado que la evolución de los tiempos nos ha traído los smartphones, la robótica, la inteligencia artificial y por supuesto, fundamental, la internet, entre otras, que han hecho que aquellas problemáticas incipientes hoy se hayan desplazado a temáticas que ni siquiera podíamos imaginar en aquellas épocas.

De igual manera, en los números tres y cuatro de 1990 y 1991, se publicó, en dos partes, un profuso artículo del profesor Dr .don Eric Alfredo Chirino Sánchez (1990), relacionado con una problemática de vital importancia el día de hoy que se denominó "Informática y Derecho a la Intimidad. Perspectivas de Política Criminal", donde el autor resaltaba que "… se ha dicho que la generalización del uso de los ordenadores comporta, principalmente, dos graves riesgos para el ciudadano: por un lado, desde la perspectiva del Estado, el control y el manejo de la información puede limitar la participación democrática del individuo (se incluyen aquí las hipótesis de acceso a la información las cuales se ven también limitadas). Desde la perspectiva del ciudadano, la creación de una imposibilidad física para proteger su esfera íntima." (p.36). Nos preguntaríamos hoy: ¿estas preocupaciones, en nuestra realidad, habrán cambiado o evolucionado mucho?

La relación de nuestra Universidad con esta materia, no sólo ha quedado supeditada a la publicación antes mencionada, sino que, también, durante diez años estuvimos vinculados internacionalmente con la Federación Iberoamericana de Derecho Informático (FIADI), participando en sus diversos congresos en España, Perú y México, al punto que se nos asignara para abril del año 2002 la realización del IX Congreso en Costa Rica, el cual efectivamente llevamos a cabo. Cuando aceptamos esta tarea externamos lo que consideramos hoy sigue vigente:
"Cuando la historia nos ha permitido, a todos nosotros, asistir a uno de sus momentos más extraordinarios y evolutivos, pues nos encontramos más que en una era de cambios, en un cambio de era, donde lo único permanente es el cambio, dado el desarrollo vertiginoso de las tecnologías, a nosotros los juristas nos corresponde la ineludible responsabilidad de buscarle soluciones normativas a los cuestionamientos e interrogantes,

que la era del ciberespacio, de los bits, y de las comunicaciones instantáneas nos presenta. Por lo menos, nuestra responsabilidad es no desmayar en la hoy más que nunca difícil, pero muy difícil labor de tratar de encontrarlas, pues la lucha cotidiana más que con relación a la evolución tecnológica es con relación al tiempo en que esa evolución se da.

Para nadie es un secreto que la informática, como medio tanto como objeto del derecho, ha atravesado transversalmente a éste y a sus ramas. Por ejemplo, el derecho civil con la sucesión electrónica, el derecho comercial con el comercio electrónico, ambos con el problema de la firma digital, el derecho penal con los delitos informáticos, el derecho procesal con los medios de prueba y aceleramiento de los procesos, el derecho administrativo con la telemática, el derecho fiscal con el problema de los tributos, el laboral con el teletrabajo y así innumerable cantidad de situaciones.

La doctrina deberá debatirse sobre la problemática de la superación o no del principio de territorialidad de los ordenamientos jurídicos y el concepto de soberanía, sobre el principio de igualdad en materia informática y los derechos humanos, así como el surgimiento y consolidación de nuevos principios como el de autorregulación y accesibilidad.

En fin, el espectro que nos presenta esta nueva era, esta nueva realidad, es virtualmente infinito, por lo que su problemática es virtualmente infinita y la búsqueda de soluciones normativas de carácter jurídico será, igualmente, virtualmente infinita. Lo único permanente es el cambio.

Así, esta nueva realidad nos pone a soñar con la ley modelo de comercio electrónico, de firma digital o de sitios de dominio. Frente a la evolución vertiginosa de la informática, la respuesta jurídica debe ser sencilla, transparente y expedita y tal vez lo más importante de fácil acceso a todos. Los tiempos del derecho solo para los iniciados y ungidos es muy posible que estén cerca de ser superados.

Podemos así ver que de cara a ocho congresos iberoamericanos de informática y derecho la labor apenas empieza y muy lejos, en lontananza de los tiempos, quizás se podrá divisar un momento de reposo jurídico." (Guerrero Portilla, 2000). Es claro, que la especialidad de la materia y el constante salto de la evolución tecnológica nos indica que el momento del "reposo jurídico" está cada vez más lejano, pues, a pesar de las décadas que ya han transcurrido y a las que nos hemos referido, pareciera, que la tarea apenas está empezando.

Conscientes de que la tarea apenas está empezando, la Universidad Escuela Libre de Derecho ha organizado un programa Académico de educación continua o ejecutiva de alto nivel, que corresponde a un certificado de "Especialización en Derecho Informático" pronto a iniciar, con la clara intención de ir contribuyendo, en el ámbito del Foro Nacional, al desarrollo de toda esta nueva rama del derecho que atraviesa transversalmente todo nuestro ordenamiento jurídico.

Por ello, este nuevo número de TRIBUNA LIBRE, el 8/1, está dedicado fundamentalmente al planteamiento de algunos de los temas relacionados con el Derecho Informático. Haciéndose aquí necesario dejar expresamente

manifestado nuestro agradecimiento imperecedero al profesor don José Adalid Medrano Melara, quién con su expertise, constancia y perseverancia ha apoyado todo este proyecto, el cual difícilmente hubiera visto la luz sin su concurso.

El profesor Medrano Melara presenta el artículo "El delito de violación de datos personales", donde se plantea que "La violación de datos personales es un tipo penal que tutela el derecho de autodeterminación informativa tanto de personas físicas como de las jurídicas y representa una serie de conductas que realizan los grupos cibercriminales para la comisión de distintos delitos tradicionales e informáticos. … La ciberdelincuencia se dirige a una modalidad de operación que afectará cada vez más bienes jurídicos de una manera acelerada y con gran impacto."

También es importante dejar constancia de agradecimiento a todas las personas que colaboran con sus artículos en la presente edición.

El profesor Julio Córdoba Elizondo nos aporta "Reflexiones sobre algunas amenazas contra el bitcoin (4 de mayo del 2021)", en el cual se sostiene que "Las monedas electrónicas y en especial el bitcoin son una tendencia económica global y objeto de estudio en foros académicos, de opinión y polémicas sobre la existencia de una moneda descentralizada, de respaldo civil, sin corporalidad ni emisión por parte de un banco central. La disrupción que significa en la economía mundial y en el campo tecnológico no está ajena a polémicas que podrían afectar su creciente aceptabilidad sino incluso la naturaleza funcional como medio de pago."

Por su parte, la profesora Vilma Sánchez del Castillo nos presenta "Entre el back to basics y los nuevos paradigmas de la revolución tecnológica. Pensamientos para la reducción de la brecha tecnológica-jurídica y la estandarización de las legislaciones: caso costarricense.", indicando que "El back to basics planteado, pretende concientizar a los operadores legales costarricenses de la necesidad de ajustarse al orden proveniente de los cimientos del Derecho Uniforme del Comercio Internacional, el cual, se debe acoplar con los avances del Derecho Comunitario en la materia, como punto de partida y marco de obligado anclaje para afrontar los retos del Comercio electrónico reloaded."

En el artículo la "Acreditación de las Actuaciones Electrónicas Personales: de la Firma Electrónica a la Identidad Digital Auto-Soberana", el profesor Juan Esteban Durango Rave plantea "… un estudio de la eficacia y validez jurídica de los métodos de acreditación electrónica conocidos para personas físicas y disponibles en la actualidad, así como la manera en que éstos pueden generar confianza entre las personas bajo un contexto digital."

Se indica que "… el derecho a la Autodeterminación Informativa le permite a cada persona decidir cómo desea que sean tratados sus datos personales. Sin embargo, al igual que casi todos los derechos, este no es un derecho irrestricto y tiene algunas limitaciones. Para ello, existen muchas bases que permiten justificar el tratamiento de datos personales las cuales incluyen aquellas que requieren la autorización expresa del interesado, así como las que encuentran su justificación de alguna otra forma.", afirmación, en materia tan sensible, que desarrolla el profesor León Weinstok en

su artículo "Formas de legitimación del tratamiento de datos personales (Basis for processing personal information)"

Finalmente, y no por ello menos importante y trascendente, mereciéndose resaltar, por cuanto fue uno de los profesores que contribuyó con el primer número de TRIBUNA LIBRE con su artículo denominado "Kant. Derecho y Moral", el Catedrático don Alban Bonilla Sandí contribuye con su reflexión "TICs y enseñanza del Derecho, ventajas, límites, retos.", donde plantea "… una reflexión sobre la tecnología y evolución que han tenido desde la Edad de Piedra hasta nuestros días, su uso en diferentes campos de la actividad humana, pero sobre todo en la educación, y particularmente en el campo del Derecho. La hipótesis básica es que la pandemia impuso la educación virtual y generó un cambio en la cultura pedagógica del sector educación, lo que facilitará la práctica de diferentes modalidades de educación en la post pandemia. Se analizan ventajas, desventajas y límites de la educación virtual, pero también se mencionan los peligros de la deshumanización, y llama la atención para no caer en la tecnocracia. El ser humano y no la máquina debe seguir siendo el centro del proceso."

Esperamos, de alguna manera, que esta nueva versión digital de TIBUNA LIBRE pueda servir para despertar, por lo menos, la curiosidad en nuestros lectores y, ojalá, más allá de esto, se desarrolle o despliegue la intención de profundizar en el análisis, estudio e investigación de la problemática que las TICs y los nuevos tiempos nos traen.

Septiembre del 2021.-
Dr. Ricardo Guerrero Portilla
Rector/ Director

Revista Tribuna Libre. Vol. 8, No. 1 (14 - 38). Octubre - 2021.
Primera Edición Digital

ALBAN BONILLA SANDÍ

Licenciado en Filosofía (UCR)
Doctor en Derecho (UELD)
42 años de docencia universitaria (UNA-UCR-UELD) en los campos de la Filosofía de la Educación, Filosofía del Derecho, Realidad Nacional, Ética Profesional, Derecho de Familia y Teoría General del Derecho. Ha sido Presidente Comisión Carrera Académica (UNA), Decano Facultad de Filosofía y Letras (UNA), Presidente fundador del Consejo de Facultades Humanísticas de Centroamérica (COFAHA), Director Académico Colegio de Abogados, Director Ejecutivo de SUPRICORI y Director Ejecutivo de UNIRE.

- albanbonilla.abogado@gmail.com

1



TIC's y enseñanza del Derecho, ventajas, límites, retos.

Alban Bonilla Sandí

Licenciado en Filosofía (UCR)
Doctor en Derecho (UELD)
42 años de docencia universitaria (UNA-UCR-UELD) en los campos de la Filosofía de la Educación, Filosofía del Derecho, Realidad Nacional, Ética Profesional, Derecho de Familia y Teoría General del Derecho.
Ha sido Presidente Comisión Carrera Académica (UNA), Decano Facultad de Filosofía y Letras (UNA), Presidente fundador del Consejo de Facultades Humanísticas de Centroamérica (COFAHA), Director Académico Colegio de Abogados, Director Ejecutivo de SUPRICORI y Director Ejecutivo de UNIRE.
Correo: albanbonilla.abogado@gmail.com

Resumen:

Este artículo está escrito a modo de ensayo, por lo que se prescinden de las formalidades de un artículo científico, pues constituye una reflexión coyuntural sobre el impacto de la pandemia SARS-CoV-2 en la virtualización de la enseñanza del Derecho. Incluye una reflexión sobre la tecnología y evolución que han tenido desde la Edad de Piedra hasta nuestros días, su uso en diferentes campos de la actividad humana, pero sobre todo en la educación, y particularmente en el campo del Derecho. La hipótesis básica es que la pandemia impuso la educación virtual y generó un cambio en la cultura pedagógica del sector educación, lo que facilitará la práctica de diferentes modalidades de educación en la post pandemia. Se analizan ventajas, desventajas y límites de la educación virtual, pero también se mencionan los peligros de la deshumanización, y llama la atención para no caer en la tecnocracia. El ser humano y no la máquina debe seguir siendo el centro del proceso.

Summary:

This article is written as an ESSAY, so the formalities of a scientific article are dispensed, as it constitutes a conjunctural reflection on the impact of the

SARS-CoV-2 pandemic on the virtualization of legal education. It includes a reflection on the technology and evolution that they have had from the Stone Age to the present day, its use in different fields of human activity, but above all in education, and particularly in the field of Law. The basic hypothesis is that the pandemic imposed virtual education and generated a change in the pedagogical culture of the education sector, which will facilitate the practice of different forms of education in the post-pandemic. Advantages, disadvantages and limits of virtual education are analyzed, but the dangers of dehumanization are also mentioned, and it draws attention to avoid falling into technocracy. The human being and not the machine must remain as the center of the process.

Palabras clave: cultura, tecnología, pandemia SARS-CoV-2, catalizador, educación virtual, ventajas, posibilidades, límites, peligros, tecnocracia, humanización, Derecho.

Keywords: culture, technology, SARS-CoV-2 pandemic, catalyst, virtual education, advantages, possibilities, limits, dangers, technocracy, humanization, Law.

Sumario:

1. **Antecedentes.**
2. **Educación y tecnología (TICs)**
3. **La pandemia como catalizador**
4. **Enseñanza virtual del Derecho**
5. **Ventajas, desventajas y límites.**

1. Antecedentes.

Desde el origen del hombre existe la educación. La especie humana no se rige por instinto, ni viene programada como las especies animales. La especie humana por su naturaleza requiere preparar la prole para sobrevivir y continuar la

línea ascendente de su desarrollo, sobre todo porque el homo sapiens como productor de cultura y símbolos, requiere ser formado para sobrevivir en las construcciones sociales que va diseñando.

Esta preparación es un proceso de reproducción sistémica y sistemática de las condiciones cambiantes en que se desenvuelve el ser humano, ya sea consciente o inconsciente, formal o informal, y ha adoptado las más diversas metodologías. La cultura se hereda y aprende. El ser humano no nace naturalmente culturizado, siempre ha debido ser culturizado. Ha sido culturizado por la familia, la comunidad, las instituciones religiosas que va construyendo. Los animales no producen cultura, por eso en ellos no hay procesos educativos destinados a reproducir su forma de vida. Aprenden por instinto. Si bien es cierto existen entre ellos ciertos procesos que algunos denominan educación, realmente de lo que se trata es de procesos de adecuación instintiva a la sobrevivencia, que no implican nuevas construcciones socioculturales, se quedan en la etapa de desarrollo de la especie.

El ser humano, en cambio, progresa constantemente y constantemente debe ampliar las perspectivas de culturización (educación) de su propia especie. Los seres humanos, desde que el ***Homo neanderthalensis*** fue superado por el ***Sapiens*** ha seguido una línea evolutiva ascendente sostenida (está por verse si sostenible) que ha implicado nuevas producciones culturales.

La cultura implica tecnología, en los primeros estadios de la humanidad, y ciencia en los posteriores. Todas las edades humanas han producido tecnología. Cultura es todo lo que el hombre hace y que se aparta de la naturaleza (no necesariamente la contradice). La producción de herramientas (desde el hacha de piedra hasta los superordenadores) siempre ha acompañado al ser humano, y, por eso requiere educar a las nuevas generaciones no solo para aprender las tecnologías que va produciendo y mantenerlas, sino también para superarlas.

Si bien es cierto la educación tiene diversas implicaciones y contenidos, pues no solo incluye la preparación con relación a las tecnologías imperantes, también incluye las normas de convivencia (valores, representaciones, tareas), y a lo largo de toda su historia ha sido así en todas las civilizaciones.

Haremos abstracción de la relación tecnología-educación que es lo que interesa en esta ponencia, no porque los otros aspectos no sean de interés, sino porque a esta relación se circunscribe el marco teórico que articulamos.

No solo se educa en tecnologías y ciencias (más las preindicadas normas de convivencia), también la educación misma usa y produce sus propias tecnologías, que son los instrumentos (en el sentido amplio del término) con los que se educa. Desde las tablas de arcilla hasta las herramientas virtuales (TICS) y las metodologías de enseñanza están en constante evolución, en función de los nuevos contextos que a su vez se ven afectados por las nuevas tecnologías. Pensemos cómo ha de haberse afectado la educación durante la peste negra medieval (1347-1353) con los medios tecnológicos a disposición en aquellos momentos. Pensemos ahora en qué hubiera sido de la educación con la pandemia SARS-CoV-2 si no dispusiéramos de los medios tecnológicos de que hoy día disponemos. Evidentemente la respuesta es que las nuevas TICS, han ofrecido alternativas, han acelerado transformaciones y seguramente impactarán permanentemente los procesos educativos avanzando hacia nuevas metodologías de enseñanza, para las cuales no estábamos preparados con anterioridad a la pandemia. Las herramientas condicionan las metodologías (en sus diferentes aspectos: educación, instrucción, didáctica, pedagogía), requieren respuestas creativas acordes con las exigencias.

Con estos antecedentes nos proponemos hacer una breve reflexión sobre TICS y enseñanza del Derecho, ventajas, límites y retos, como indica el epígrafe de este artículo.

2. Educación y tecnología (TICS)

Evidentemente las TICs están modificando los diferentes aspectos de nuestras vidas, la manera en cómo nos transportamos, nos comunicamos, nos curamos, nos divertimos, y hasta las formas de orar. Pero si hay alguna actividad humana que se ha visto impactada por los avances tecnológicos es precisamente la educación. Estos han dejado anacrónicos los sistemas educativos.

Nos limitamos a reflexionar sobre la educación como instituto formal, pues igualmente habría que reflexionar en otros espacios sobre el impacto de las TICs en la educación informal (familia, iglesia, comunidad, el mismo mercadeo), que igualmente, con o sin pesar, también se han visto macadas por las TICs.

No solo por las nuevas herramientas a disposición de los actores (docentes y discentes) que les otorgan nuevas posibilidades, sino que ellos mismos se han visto obligados a adquirir nuevas competencias, habilidades y destrezas, obligan a una actualización permanente, pues precisamente una de las características del desarrollo contemporáneo es la velocidad con que se remoza.

Esto significa que no solamente estamos modificando los instrumentos a nuestra disposición, sino que también y necesariamente estamos modificando la forma en que enseñamos y las maneras en que los discentes aprenden. Queda, desde luego la incógnita, sujeta a reflexiones de otra ocasión, si estas nuevas formas de enseñar y aprender son más eficientes, si producen personas críticas, creadoras e innovadoras, si están a buen recaudo los valores que los sistemas promueven, si esta sociedad del conocimiento que las nuevas tecnologías han hecho posible es para bien o para mal de nuestras sociedades, es decir, si solamente estamos mejorando los entornos económicos, pero deshumanizando las futuras generaciones. Esas incógnitas no son gratuitas.

Nos encontramos en una nueva era tecnológica, cuyo superdesarrollo continuo inició hace unos 50 años cuando los ordenadores se empezaron a popularizar. Incursionamos en la era de las supercarreteras de la información. La juventud actual puede ser fácilmente calificada de nativos digitales, que manejan cotidianamente las redes sociales, manejan procesadores de datos con soportes ofimáticos, les son familiares los dispositivos móviles como smartphones o tablets, pues con ellos no solo cumplen sus deberes escolares, sino que también se divierten y no se les ocurren buscar alternativas de diversión a pesar de que estas existen.

Para los docentes, sobre todo de generaciones anteriores, esto también forma parte de su paisaje, con la diferencia de que son digitales por adopción, pero las exigencias de actualización los obligan a incursionar en este mundo desconocido en la segunda mitad del siglo XX. En todas las profesiones siempre la actualización ha sido un imperativo de sobrevivencia, pero ahora esta exigencia se ha acelerado, con el ultimátum de que no reaccionar, es perecer.

Entonces no solo debe renovar sus equipos y herramientas sino las metodologías que se adecúen a ellas. No se trata de cambiar el pizarrón por una tablet o una laptop, debe emigrar hacia nuevas formas de enseñanza. Se trata de familiarizarse con las TICs, aprender a sacarles provecho, pero a la vez promoviendo el pensamiento divergente que permita a las nuevas generaciones encontrar respuestas a los nuevos retos, inexistentes y sin fórmulas de solución conocidas.

Tenemos un sistema educativo (y legal) pensado para otras realidades, que Robinson (2011) caracterizó que “se crearon en el pasado, en una época distinta para responder a retos diferentes”. Los sistemas crean a las personas, pues su entorno las condiciona. Los diferentes niveles educativos se han visto obligados a transitar aceleradamente, de una sociedad industrial, en el mejor de los casos, cuando no en una sociedad exportadora de materias primas como las nuestras, a

una era (sociedad y economía) del conocimiento. Los sistemas educativos estaban centrados en la memorización (estudiar para el examen), eran procesos de estandarización (educación enlatada), en el espíritu acrítico que garantizara la reproducción del sistema, y no en los emprendimientos e innovaciones. Desgraciadamente nuestra sociedad no ha evolucionado al mismo ritmo que otras en los requerimientos de la sociedad del conocimiento, y nos vemos arrastrados (fuerza de atracción tecnológica) por sociedades que privilegian la innovación, la investigación, pero sobre todo el patentamiento. Las patentes han sustituido las bayonetas. Tenemos que construir la sociedad del conocimiento, y en eso los abogados no podemos ser ajenos. Las transformaciones nos arrastran. Así como los docentes deben actualizarse, lo mismo las sociedades y sistemas, so pena de perecimiento.

Las universidades, incluimos a sus escuelas de Derecho, no solo deben ser capaces de transmitir conocimientos al viejo estilo, sino que deben partir de ambientes profesionales simulados en los que puedan experimentar los entornos en los cuales han de desenvolverse. Las clínicas jurídicas juegan este papel, pero igualmente hay que ofrecer otros escenarios de dedicación profesional en bufetes, juzgados, instituciones públicas, etc.

En este contexto es donde las TICs contribuyen, a modificar los modelos educativos. Cuando la educación era necesariamente presencial, el proceso se centraba en el docente (*magister dixit*), con las TICs, y a partir de la virtualización forzosa, aunque temporalmente, la educación virtual cuyo soporte son las TICs, el modelo educativo ha tenido que ir evolucionando hacia el discente, pues al no contar con la compulsión que significa la presencia docente, ha tenido que asumir mayores responsabilidades, convertirse en un actor, incluso proactivo. Ya la memoria no es el único instrumento (se volvió inútil, el discente dispone de la fuente en tiempo real, aún durante los exámenes), ni más deseable, de aprendizaje, pues el alumno dispone de la materia, de modo que las experiencias didácticas obligan al profesor a inducir al discente a enfrentarse a situaciones significativas (a buscar soluciones),

a adoptar decisiones, a reflexionar sobre la materia que se le ha dado (ahora es más importante hacer las preguntas correctas), al aprendizaje autónomo sobre la base de lecturas y foros, a distinguir los datos arbitrados de las fake news, en síntesis, el docente debe superar la educación bancaria (como decía Pablo Freire) en la cual el profesor depositaba en una cuenta corriente (el discente) un elenco de datos que el alumno repetía, aún sin entenderlos, para luego olvidarlos. De transmisor de conocimientos (instrucción propiamente dicha), las TICs apremian al docente a convertirse en un coordinador de experiencias, enseñando al alumno a "aprender a aprender" como diría Benedict Carey, a crear conocimiento, a aplicarlo, a construirlo en lugar de recibirlo construido. De nada sirve a un estudiante de derecho aprender de memoria una norma si es incapaz de aplicarla a casos concretos. Ya no pueden "copiar" pues disponen de los datos, ahora tienen que utilizarlos, investigar. Innovar, ser creativos y a la vez, aprender a la construcción del conocimiento colectivamente (después de todo hoy día con las redes la práctica profesional cada día es más colectiva), pues los discentes conforman sus propias redes grupales, que operan durante los trabajos asignados y durante los exámenes. Estos factores hay que tomarlos en cuenta, también en los nuevos paradigmas.

Desde luego los nuevos paradigmas educativos, por su propia naturaleza están, por un lado, aún en construcción, por otro lado, y por esto mismo las nuevas respuestas no necesariamente serán únicas ni univocas, sino que habrá diversidad: pero lo que sí parece plausible es que podrían encontrar tres elementos relacionados entre sí, puesto que son imprescindibles: tendremos las TICs como fuente de transmisión de conocimiento, como instrumento que permitirá converger actores, pero a la vez, las mismas TICs se constituyen en sí mismas como objeto de estudio.

Estos tres elementos los encontramos en mayor o menor medida en todos los campos de la actividad humana. Como veremos en el epígrafe 4. en el Derecho las consecuencias de las TICs han sido sustanciales, y han contribuido a hacer más fluido el tráfico jurídico.

En el campo educativo igualmente encontramos impactos. No solo han permitido nuevas modalidades educativas como la virtual (sincrónica y diacrónica), la bimodal, la presencial a distancia, sin que estas modalidades eliminen la presencialidad (momentáneamente interrumpida por el SARS-CoV-2 por la pandemia) sino que estas se han caracterizado por el acceso a nuevas fuentes, plataformas online, quizá ilimitadas, tanto en servicios de pago como las bibliotecas virtuales arbitradas (EBSCO-SPRINGER-CIBEROTECA por ejemplo) como a servicios gratuitos, que si bien es cierto hay que usarlos con cierta aprensión, un docente o discente entrenado puede sacarles provecho. Por otra parte, la interrelación docentes-discentes hace posible un contacto 24/7 (atemporal u ubicuo, pues no interesa cuando ni donde, pues el trabajo colaborativo puede ser geográficamente distante) y diferentes dinámicas como foros, comunidades virtuales que comparten archivos y acceden a diferentes fuentes, trabajos en grupo (igualmente sincrónicos y diacrónicos), socializando así la construcción del conocimiento. Igualmente han aparecido nuevas modalidades de evaluación, incluso con sistema de revisión en tiempo real inmediato y automático, o bien autoevaluación colectiva, evaluación de profesores y del servicio educativo. Todos los actores del proceso educativo se han adaptado (han tenido que) provocando nuevos desarrollos con nuevas velocidades.

Desde luego que el tercer elemento ha hecho que la huella de las nuevas tecnologías en el campo educativo ha provocado verdaderos campos de investigación, de debate, de congresos, foros, paneles, disciplinarios, interdisciplinarios y multidisciplinarios con relación a la informática educativa, la humanización-deshumanización de los sistemas educativos provocados por las TICs, y básicamente las TICs han revolucionado la gestión de información jurídicamente relevante, lo que abre un abanico de posibilidades anteriormente inexistentes. Desde luego que estas posibilidades también comportan retos y peligros.

Tampoco podemos caer en el tecnocentrismo, ni pensar como creía Augusto Comte que la sociedad evoluciona irremediablemente hacia un modelo sociocrático, en donde un Consejo de Científicos serían los que tomen las decisiones (según eso se eliminaría el modelo democrático) o una sociedad como la que previó George Orwell en su novela 1984, que hoy tiene posibilidades reales de conformarse, si es que no estamos cerca de estarlo. Las nuevas tecnologías tienen potencialidades y retos, hay que aprovecharlos, pero igualmente debemos ubicar las distorsiones que pueden producir.

Ureña (2021) nos llama la atención, en un reciente artículo, sobre los peligros de la digitalización:

> Vivimos en un mundo acelerado, complejo y «líquido» —como lo definió el sociólogo Zygmunt Bauman—, caracterizado además por una digitalización cada vez más extrema de la política, la economía y la vida cotidiana. Esta situación implica grandes riesgos para países, empresas y personas, puesto que la privacidad y la seguridad de todos queda a merced de la maldad informática.

Finalmente, en este apartado hay que señalar que por su propia naturaleza las TICs inciden de distinta manera en los diferentes campos de la vida humana (no los mencionaremos, pues nuestro tema es las TICs, educación y Derecho). El campo del Derecho lo veremos en el párrafo 4, en el campo educativo que es el que nos ocupa, incide de diferente manera dependiendo de la disciplina y de las diferentes materias. No nos vamos a referir a las enseñanza primaria y media, solo a la terciaria. En este nivel, la incidencia va a depender de la naturaleza de la disciplina, pues en carreras como Derecho, Filosofía o Lingüística o algunas STEM ligadas a ciencias formales o ciencias básicas (al menos parcialmente), por decir algunas, donde virtualidad integral es posible, pero hay carreras en donde la presencialidad es insustituible por los requerimientos de laboratorio o prácticas que demandan manipulaciones donde no son posibles las simulaciones. Prácticas en

las áreas de la salud, laboratorios de química, física, prácticas de campo en las diferentes ingenierías o campos clínicos, por citar ejemplos, no permiten la virtualidad, y la aplicación de TICs se refiere a las fuentes o los aspectos donde es posible y deseable. Desde luego que el acceso a fuentes, foros, lecciones, etc. en donde la capacidad de gestión de la información lo permite, sí es posible en cualquier área del conocimiento.

A esta caracterización endogámica hay que agregarle la que hace el experto de teoría universitaria, Rama (2020), sobre las posibilidades nuevas que ofrecen las TICs y sus posibles aplicaciones educativas como forma de libertad:

> Toda educación es un camino a la libertad ya que crea competencias que permiten mejorar las expectativas y posibilitar mejores desarrollos futuros. La educación siempre es en este sentido un espacio de libertad ya que además aumenta nuestra capacidad de analizar las realidades y comprender el entorno en el cual vivimos. La historia de la humanidad es un avance hacia la libertad de las personas y ello está asociado directamente al mejoramiento del conocimiento y de la formación de las personas. La educación a distancia es una forma superior de libertad ya que no está sujeta a nuestra movilidad o a determinados costos de traslado o de disposición de tiempo. Cuando más tenemos opciones de escogencia, tenemos mayor libertad. La educación presencial implica menos grados de libertad de la educación presencial.

En realidad, estamos en presencia de una democratización de la educación permitida por las nuevas TICs, democratización que no es plena aún por cuanto tenemos sectores poblacionales importantes cuya conectividad se sitúa en el campo de los debes. De ahí que las propuestas políticas que se formulen deben aprovechar las posibilidades de las nuevas TICs para que estos sectores accedan en igualdad de condiciones que el resto de la población a las ventajas de la conectividad. Esto es así, en cierta manera, pues si bien es cierto las TICs han puesto de relieve estas desigualdades, no las han creado, pues son preexistentes. Estas desigualdades no

son producto de las TICs sino de las condiciones económico sociales de los pueblos, de modo que el problema no reside en la cobija, el frío está en otro lado. La presión no está en el barómetro, sino que en el ambiente. Precisamente por eso es que hay que aprovechar las TICs como herramienta de democratización, pues ofrecen esa posibilidad y son una invitación a una política pública inclusiva que las aproveche. Al fin y al cabo, quizá Kant tenía razón: avanzamos hacia el reino de la libertad. Solo que no podemos esperar con los brazos cruzados hasta que esta llegue y se convierta en una realidad plena para todas las personas, pues la historia avanza haciendo.

3. La pandemia como catalizador

En el país predominaba la educación presencial hasta marzo del 2020. Las experiencias de otras modalidades de educación eran significativamente escazas.

Aún recordamos las experiencias de la Hemphill Schools que inició en Costa Rica la educación a distancia, cuando su sede estaba en Estados Unidos, y se dedicaba a formar fundamentalmente en carreras parauniversitarias. Sus estudiantes recibían del correo los sobres con las lecciones en áreas como la Mecánica Automotriz, Electricidad, Refrigeración, inglés, Radio y TV, Contabilidad.

La Hemphill Schools había sido fundada por Ralph Hempill en 1920 en Vancouver, Canadá, y de ahí extendió sus servicios de educación a distancia a USA y a América Latina.

No obstante, la educación universitaria a distancia se formalizó con la creación de la Universidad Estatal a Distancia, la UNED, fundada en 1977 como la primera universidad en Costa Rica y en América Latina que utiliza la modalidad a distancia, y continúa siendo la única universidad pública de Costa Rica que utiliza esta modalidad de educación. Esta universidad siguió el modelo español de educación a distancia. Desde luego ni la Hemphill Schools ni la UNED son pioneros

de la educación virtual, pues las condiciones tecnológicas de la época no lo permitían, pero si rompieron el marco de la presencialidad.

Conforme las TICs lo fueron permitiendo la educación virtual empezó a adquirir mayor relevancia, sin romper el marco presencial.

En las universidades privadas la que mayor ha incursionado en la educación virtual ha sido la Universidad San Marcos, originalmente fundada como presencial, pero que paulatinamente ha ido evolucionando a la virtualidad hasta el extremo de que hoy día su principal matrícula está constituida predominantemente por estudiantes de educación virtual. Otras universidades, tanto públicas como privadas, han incursionado tibiamente en esta modalidad, y sus carreras siguen estando aprobadas como presenciales.

Hay que reconocer que sus cultores han tenido que nadar contra corrientes culturales y prejuicios, pues en sus inicios, en la década de los setentas, tuvo que luchar para ganarse un espacio en el imaginario costarricense, en donde por inercia histórica el prestigio lo exhibían los modelos presenciales.

No cabe duda que este esquema lo rompió la pandemia de SARS-CoV-2 en marzo del 2020. Las medidas sanitarias de distanciamiento social, restricción vehicular, aforos restringidos, cuarentena y confinamiento impuestas por las autoridades sanitarias con fundamento en un principio básico de salud pública, obligó a las autoridades educativas de todos los niveles a decretar la educación virtual como medida de contingencia, y, en consecuencia, provisional.

Las universidades también tuvieron que adherirse a esta política pública. Tanto CONARE como CONESUP impulsaron políticas y medidas de contingencia para emigrar, al menos, a la educación presencial a distancia, es decir, educación virtual sincrónica. La pandemia nos cogió por sorpresa y nos obligó por sorpresa. Hay que reconocer que pocos estaban preparados para lo que se venía. La infraestructura, física y tecnológica estaba diseñada para la presencialidad, y el

personal docente no estaba familiarizado con las TICs ni preparado pedagógicamente para asumir el reto de educación virtual, pero la ausencia a alternativas obligó a todos a lanzarse a la experiencia. No solo hubo que actualizarse aceleradamente, sobre la marcha, sino que se necesitó cambiar una cultura: la cultura de la presencialidad resultó anacrónica de un momento a otro, sin ceremonias ni previo aviso.

Había que garantizar la continuidad del proceso educativo, había que evitar el “apagón educativo” al menos en el sector terciario. Había que adaptarse para seguir y sobrevivir, y sobre todo ante la incertidumbre de cuánto tiempo iba a durar la pandemia y las condiciones que produjeron la transformación repentina de la educación presencial en virtual.

Para las escuelas de Derecho esta transformación resultó igualmente inesperada, pero por la naturaleza de la disciplina, las posibilidades virtuales más bien abrieron nuevas entradas metodológicas.

La práctica es la madre de todas las enseñanzas. La ventaja de tomar el proceso de transformación (aún en progreso) sobre la marcha, fue que no hubo tiempo de pensar ni planear, ni de asumir miedos ni resquemores. Cuando no hay alternativas o te comprometes o sucumbes.

La experiencia enriqueció. Demostró que era posible la transformación, mostró las ventajas y desventajas de las diferentes modalidades. Si bien es cierto se trata de medidas provisionales, pero son medidas que abren puertas y animan cambios estructurales. Ojalá los órganos del Estado estén abiertos a los cambios, y permitan que las universidades puedan escoger las modalidades que más convengan a sus intereses educativos, y superen el síndrome de la presencialidad.

Los acontecimientos provocados por la pandemia lo que han hecho es abrir posibilidades, sin que eso signifique necesariamente que hay que echar la presencialidad al cubo de la historia. El mundo marcha hacia nuevas formas de

relacionarnos y comunicarnos, la educación también, pero este es un proceso dialéctico, es decir no se trata de desechar lo que ha servido por milenios, sino de incorporarlo a las nuevas realidades tecnológicas, por ejemplo, mediante método bimodales. Lo están haciendo los Tribunales con audiencias presenciales, virtuales y mixtas, es decir, se pasó de una única modalidad a tres modalidades. Las universidades sabrán adaptarse, y particularmente las escuelas de derecho, quizá a distintas velocidades y con distintas calidades.

4. Enseñanza virtual del Derecho

En el campo del derecho esto es particularmente cierto, puesto que los operadores jurídicos tienen como principal herramienta la palabra, y las TICs han impactado la profesión hasta el extremo de permitir el teletrabajo jurídico, las audiencias virtuales, los expedientes digitales, y su manipulación, las nuevas formas de notificación, contratación electrónica, teletrabajo, criminalidad informática, democracia electrónica, propiedad intelectual, tratamiento de datos personales, la administración electrónica ha permitido la comunicación en tiempo real, el acceso y clasificación de la información (NEXUS y SINALEVI por ejemplo), e igualmente esto ha facilitado las reuniones, negociaciones y audiencias, además se consolidado todo una nueva rama del Derecho, a saber: el Derecho Informático (consecuencias, regulaciones).

Si bien es cierto nuestras escuelas de Derecho fueron fogueadas todas en educación presencial, estuvieron prestas a los cambios tecnológicos que la pandemia impuso. Previo a la pandemia no existían en nuestro país experiencias de educación online en el campo del Derecho.

Hay que reconocer que la comunidad académica jurídica pertenece a un gremio más bien de perfiles tradicionalistas, tendente a mantener los esquemas pedagógicos al uso durante años, donde predominan la memorización y aplicación

mecánica de preceptos. Si bien es cierto hay algunos avances hacia la oralidad, metodologías clínicas y resolución de casos, aún falta por recorrer camino hacia metodologías activas y de investigación. Hay que orientarse hacia el constructivismo jurídico, y abandonar lo que queda de conductismo jurídico (simple transmisión de conocimientos jurídicos, lo que genera acriticidad) en la cultura docente de las escuelas de Derecho. Centrar el proceso en el discente para que no reciba pasivamente los conocimientos, sino que los construya por sí mismos, "aprendiendo a aprender", abandonar las clases magistrales (ese problema se genera en el hecho de que los profesores de Derecho no suelen tener formación pedagógica, no los preparan para ser docentes) y poner al discente en contacto con las fuentes, es algo que sería posible con las nuevas herramientas tecnológicas, a efecto de que nuestros graduados adquieran habilidades y destrezas para el ejercicio profesional como capacidad de análisis de discurso, capacidad investigativa y desarrollar una capacidad erística, pues el abogado debe saber discutir tanto en su expresión oral como escrita, debe ser un buen polemista.

Ciertamente la mayoría de las instituciones vinculadas a la comunidad jurídica empezaron a adoptar modelos de gestión virtual, digital, ante la evidencia de sus beneficios, la enseñanza del Derecho quedó anclada a la presencialidad, aun cuando había escuelas que tenían sus plataformas digitales, formaban a sus docentes en estas herramientas, los capacitaban en metodologías didácticas y pedagógicas acordes con la virtualidad, les costaba dar el paso. En el caso de las universidades privadas quizá porque el CONESUP no facilita la innovación.

La pandemia abrió posibilidades de avanzar hacia la enseñanza del derecho utilizando las TICs, y abandonar lo que algunos autores llaman "*analfabetismo iusdigital*". Camarillo y Barboza (2020) lo denominan como:

> "analfabeta iusdigital a la persona (independientemente de su rol social, como docente, estudiante o profesional de la abogacía) que sigue aprendiendo derecho sin utilizar o aplicar las TIC, ya sea por desconocerlas

> o por su resistencia a hacerlo, es decir, sin ponderar las innovaciones disruptivas que son distintas a las ordinarias y que permiten un aprendizaje expandido del derecho que escapa a los límites de la educación formal, a la temporalidad y al espacio. (p. 4)

Esos “cambios disruptivos” (Camarillo y Barboza, 2020) de la enseñanza del Derecho se presentan en este momento ante la posibilidad desalentadora de tener que volver a los pasos andados. Ya no hay motivos para resistir las TICs, pues los contextos han cambiado, la pandemia los cambió. Hemos convertido una crisis en una oportunidad, pues tanto docentes como discentes están mediados por la cultura digital.

Delgado y Oliver (2003) en su interesante trabajo: “Enseñanza del Derecho y tecnologías de la información y la comunicación” nos indican lo siguiente:

> Un campus virtual está constituido por dos metaestructuras: una física (formada por redes, servicios y recursos que soportan la información y las relaciones entre los miembros del campus) y otra virtual (formada, a su vez, por el conjunto de relaciones que establecen los miembros del campus entre sí y con la información que contiene). Por ello, para Zapata, el campus virtual tiene "naturaleza propia independientemente del lugar y del tiempo en que se sitúe cada uno de sus componentes". Así pues, el campus virtual estará allí donde concurran alguno de sus componentes (los individuos que lo componen, los participantes) y un punto de acceso a la información común (a "la red", entendiendo por red algo más amplio que Internet o que cualquiera de las redes y servicios digitales existentes).

Una de las plataformas que más ha contribuido durante la pandemia a promover los entornos virtuales en la enseñanza del Derecho ha sido la plataforma MOODLE diseñada precisamente para la educación online:

> Moodle y los entornos virtuales -en especial Second Life- ofrecen un servicio formativo interesante para los estudiantes y un medio útil en la enseñanza virtual universitaria, ya que además de potenciar la adquisición y transmisión de conocimientos, posibilita el aprendizaje a través de juegos de rol en los distintos ámbitos profesionales. En el Grado de Derecho es posible llevar a cabo una estrategia educativa mucho más participativa y adecuada para la adquisición de las competencias propias que deberán utilizar en su futura actividad profesional, tales como la resolución de casos prácticos o la redacción de escritos ejercitando la capacidad de argumentar o el manejo de bases de datos y sistemas informáticos para la búsqueda de información. Además, mediante el desarrollo de esta atractiva actividad, la simulación de juicios en Second Life, los estudiantes pueden interpretar las distintas identidades de los operadores jurídicos en un entorno inmersivo. (Monterroso y Escutia, 2011, p. 53).

También encontramos otras plataformas educativas como WebCT, FirstClass y Claroline, o bien el Microsoft Teams que es el que usa el Ministerio de Educación.

Sobre la enseñanza virtual del Derecho un aspecto que parece relevante es concluir que la pandemia nos obligó a movernos hacia la educación virtual, y estamos preparados para la pospandemia, cuando las nuevas normalidades nos ofrezcan posibilidades que la cultura prepandémica no nos ofrecía, y por cultura prepandémica no entiendo solamente la existencia de herramientas, que de todos modos ya existían antes de la pandemia, sino que entiendo una manera de pensar que ahora existe, una predisposición hacia nuevas metodologías pedagógicas que necesariamente requieren apoyos tecnológicos. Si pasada pandemia, aún en condiciones de endemia, logramos articular nuevas metodologías pedagógicas todo dependerá de factores ajenos a las TICs, que, aunque evolucionen rápidamente, ya existían antes de la pandemia, existen y seguirán existiendo, pues habiendo superado el "*analfabetismo iusdigital*" (cambio de paradigma cultural) no existe

justificación para no seguir avanzando en la educación virtual y combinarla con otras posibilidades, sin excluir como peste la presencialidad.

5. Ventajas, desventajas y límites.

Normalmente nos referimos a la educación virtual como metodología de la era de la información, que incorpora necesariamente las TICs como una herramienta que tiene ventajas y desventajas, y que necesariamente debe incidir en los modelos educativos, pues no se trata de sustituir los cuadernos de apuntes por laptop, ni pizarras por pantallas.

Los entornos virtuales en la enseñanza del Derecho evidentemente ofrecen ventajas, que han sido anunciadas por otros autores como Delgado y Oliver (2003), que reseñamos, como por ejemplo que los actores (docentes-discentes) conjugan vida familiar, profesional y académica, permiten la adquisición de conocimientos independientemente del tiempo y lugar donde residan los actores por romper la rigidez sincrónica, lo que permite estudiar en cualquier lugar y momento, salvo desde luego que se desestime el modelo diacrónico. El modelo sincrónico tiene menos ventajas que el diacrónico con relación a las condiciones que crea. Pero aun así estas metodologías apuntan hacia una democratización de la enseñanza, excepto en aquellos casos en que resulte precaria o inexistente la conectividad, pero no es culpa del modelo.

Además, el proceso es más individualizado pues el discente decide a dónde y cuándo estudiar, y la relación docente-discente también es más personalizada en la medida en que el docente está a disposición del discente a cualquier hora, resolviendo consultas en forma instantánea y continua, lo que le permite, por otra parte, darle seguimiento al progreso del discente. Hay que agregar que el modelo virtual permite combinar diversos recursos como vídeo conferencias, información multimedia, enlaces con bases de datos y bibliotecas digitales, foros diacrónicos,

etc. Igualmente, el sistema permite una mayor interacción con la creación de chats, con docentes-discentes, entre ellos mismos, tutorías virtuales y la conformación de comunidades virtuales.

Y algo que podría ser más psicológico que real es la posibilidad de acceder a fuentes de información casi infinitas. Si bien es cierto éstas existían antes de la pandemia, la educación presencial seguía privilegiando las fuentes impresas (libros-fotocopias). La pandemia ha puesto en evidencia la importancia y utilidad de las fuentes digitales, que no solo tienen menor costo, sino que también abren un abanico de información, además manipulable, lo que da posibilidad de tener más y mejores fuentes, sino que facilita la investigación.

Estas ventajas constituyen una preparación para un mundo profesional informatizado.

Desde luego que la educación virtual también tiene desventajas relativas. ¿Por qué relativas? Porque algunas de ellas dependen de factores externos al sistema como la personalidad del docente, del discente, o de la desigualdad de acceso a internet. Precisamente una de las desventajas es que el sistema exige tener acceso pleno a internet, que con frecuencia tiene fallas ya sea porque se cae el proveedor de señal o el proveedor eléctrico, por otro lado, todos los actores deben disponer de los mejores equipos y tecnología, con disposición de programas y formatos compatibles y acordes con la plataforma al uso; agreguemos que en la educación online el discente debe tener mayor autodisciplina, ya que no existe un profesor llamando la atención o pasando lista o vigilando exámenes memorísticos; agreguemos que con este tipo de educación interactuamos por medio de pantallas y dependiendo del manejo que haga el docente puede resultar despersonalizado, pues el contacto humano tiende a perderse, evidentemente hay menos socialización; asimismo al realizarse el proceso en entornos familiares éstos tienen distractores de los que carecen las aulas, lo que obliga al profesor a utilizar estrategias para mantener la atención cuando la educación es sincrónica;

finalmente hay que hacer un balance de costos, para todos: los docentes, los discentes y la institución, pues ciertamente el sistema permite economías, pero a su vez genera costos emergentes.

Todas estas desventajas son corregibles.

Evidentemente el sistema tiene más ventajas que desventajas.

La educación virtual también ofrece límites que no podemos ignorar como es la brecha digital que existe entre las diferentes clases sociales, sobre todo en los niveles preuniversitarios, pero aún en la enseñanza terciaria esta brecha existe ya sea por razones geográficas o sociales, lo que significa que la educación virtual es una posibilidad de democratización, pero también ofrece menos posibilidades a los sectores de ingresos bajos. El otro límite que conviene apuntar es que no toda la institución tiene la infraestructura tecnológica apropiada para ofrecer este tipo de educación ni cuenta siempre con los cuadros formados en educación virtual. Al mismo tiempo, tenemos noticia del "*apagón educativo*" en educación primaria y media pública provocado precisamente por este tipo de límites, no obstante, el **ESTADO DE LA EDUCACIÓN** aún no ha hecho un diagnóstico del impacto de la educación virtual en la calidad de la enseñanza universitaria.

Caballero (s.f.) nos trae un dato que posiblemente esté relacionado con los límites preindicados:

> Según The New York Times, el Waldorf School, donde asisten los hijos de directivos de grandes compañías tecnológicas en Silicon Valley, ofrece como gran atractivo una educación "casi libre de pantallas, con énfasis en el contacto humano."

Pareciera que los ejecutivos de Silicon Valley tienen claros los peligros de la tecnocracia y la importancia de la humanización de los procesos de enseñanza. La

tecnología, por más que facilite los procesos, nunca sustituirá al ser humano al que está llamada a servir, y en el campo del Derecho esto es particularmente cierto. El profesor Catala citado por German (2005), experto en Informática Jurídica de la Universidad de Montepellier, señala lo siguiente:

> En principio, ninguno de los investigadores comprometidos en este trabajo, ha llegado a la conclusión de que la computadora puede sustituir al hombre, o al libro de enseñanza jurídica. La informática Jurídica aparece como un complemento, sin duda admirable, pero accesorio de la enseñanza fundamental. Ella se dirige a los que poseen conocimientos básicos, colocándolos sobre la calidad y claridad de lo real, surgiéndoles aproximaciones, inesperadas, llevándolas a aplicaciones concretas. todo ello busca revivir la lección inicial del educador, pero no a ocupar su lugar, el trabajo en el terminal del computador suplanta el papel del monitor, antes de catedrático.

El peligro de la deshumanización hay que saber afrontarlo, el eje del sistema debe seguir siendo el discente y el docente, no la máquina. Ese es el gran reto.

Aparte de las ventajas, desventajas y límites propios de la educación virtual, tampoco está exenta de peligros como podría ser acceso a contenidos violentos o sexuales, acoso cibernético, obesidad, trastornos antisociales, retrasos del desarrollo y problemas de somnolencia asociados.

Sobre desventajas y límites habría que agregar que no solo son superables o controlables, sino que legítimamente habría que preguntarse si algunos de ellos no existen también en la educación presencial y no son exclusivos de la educación virtual.

Así las cosas, queda claro que la educación virtual en diferentes campos, pero particularmente en las escuelas de Derecho tiene evidentes ventajas que

merecen respaldo institucional, es decir, de las universidades. También existen desventajas, pero en su conjunto algunas son subsanables, otras no dependen propiamente del modelo sino de condiciones extratecnológicas, podríamos decir lo mismo de los límites. Por supuesto que hay ventajas que podrían ser perdidas si no les saca el provecho debido o no se abordan de manera adecuada. Pero de igual forma estas pérdidas no son inherentes al modelo, sino a sus operadores.

Tenemos un diagnóstico del "*apagón educativo*" en enseñanza primaria y media públicas en el reciente publicado informe del Estado de la Educación (ver por ejemplo la nota de Cerdas (2021) donde habla sobre docentes sin preparación para impartir clases virtuales), pero adolecemos de un diagnóstico con relación a la educación terciaria. Debemos reconocer que la educación terciaria se vio afectada en aspectos como laboratorios, pruebas de campo, etc., es decir, en aquellos aspectos que requerían presencialidad, también es cierto, que respondieron oportunamente a la virtualidad, con más o menos preparación en infraestructura tecnológica y preparación docente para la metodología virtual (técnica y pedagógicamente), pero igualmente empezaron los correctivos, pues las universidades, a diferencia de la educación preuniversitaria, tenía los recursos humanos para iniciar los correctivos y preparaciones. No hay que olvidar que estábamos (estamos) ante una emergencia y no se le pueden pedir resultados de procesos ordinarios a una situación extraordinaria. Quizá la excepción a esta regla lo fueran las universidades que tenían la metodología instalada de previo a la pandemia como la UNED, la USAM y en algunas universidades que tenían algunas carreras virtuales.

En el caso de las 24 escuelas de Derecho existentes el impacto de la pandemia en sus resultados se verá a mediano plazo con los resultados del examen de incorporación que hace el Colegio de Abogados, pero aun así, si se diera una variación en los resultados históricos de dicho examen habría que tomarlos a beneficio de inventario, pues mientras las universidades se vieron forzadas a emigrar hacia la educación virtual el Colegio sigue renuente a aplicar pruebas

virtuales, insiste en la presencialidad. Entonces, los resultados del examen lo que pueden reflejar, como hipótesis, sería el desfase entre ambas metodologías. Actualmente el Colegio aplica el examen presencial a graduados que han recibido su formación presencialmente, a mediano plazo aplicará el examen presencial a graduados virtuales. Eso podría reflejar distorsiones.

El balance general para la metodología virtual es positivo. Sus ventajas comparativas son evidentes, sus desventajas podrían controlarse y los límites superarse. El reto es no sucumbir a la tecnocracia y no permitir que la máquina domine al hombre.

Referencias y bibliografía

Caballero, C. (s.f.). *Los límites de la educación virtual*. Portafolio. Columnista.

Recuperado de https://www.portafolio.co/opinion/cesar-caballero-reinoso/los-limites-de-la-educacion-virtual-cesar-caballero-540465

Camarillo, H. y Barboza, C. (2020). El aprendizaje disruptivo y expandido del derecho. Profesión tradicional y cultura digital. *Sinéctica. Revista Electrónica de Educación*, (54), 1-16. https://sinectica.iteso.mx/index.php/SINECTICA/article/view/1023/1219

Cerdas, D. (24 de setiembre del 2021). *6 de cada 10 docentes del MEP sin preparación para impartir clases virtuales*. La Nación. Educación. Recuperado de https://www.nacion.com/el-pais/educacion/6-de-cada-10-docentes-del-mep-sin-preparacion-para/AP2GRRIL5BABBKDZEDLYPVEHR4/story/

Delgado, Ana M.ª; Oliver, Rafael (2003). *Enseñanza del Derecho y tecnologías de la información y la comunicación* [artículo en línea]. UOC. [Fecha de consulta:

26/09/2021].
http://www.uoc.edu/dt/20310/index.html

E. Punset, «El sistema educativo es anacrónico» [en línea], RTVE, *Redes*, 2011a

German, J. (24 de noviembre del 2005). *La informática como metodología para la enseñanza del Derecho*. Derecho Ecuador. Doctrinas. Recuperado de https://www.derechoecuador.com/la-informaacutetica-como-metodologiacutea-para-la-ensentildeanza-del-derecho

Monterroso, E. y Escutia, R. (2011). Enseñanza práctica en 3D: juicio virtual. *@tic. Revista d' Inovació Educativa*, (6), 46-54. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=3693961

Rama, C. (27 de setiembre del 2020). *"La educación virtual es la única forma plena para realizar el derecho a la educación"*. Misceláneas Educativas. Entrevistas. Recuperado de https://pedagogia.ubp.edu.ar/2020/09/24/la-educacion-virtual-es-la-unica-forma-plena-para-realizar-el-derecho-a-la-educacion/

Ureña, M. (23/09/2021). Soberanía digital o el santo grial del siglo XXI. *La Nación*, Columnistas. Recuperado de https://www.nacion.com/opinion/columnistas/soberania-digital-o-el-santo-grial-del-siglo-xxi/GAL6OUY4YZASNMPQIVOLOT5YEE/story/

VILMA SÁNCHEZ DEL CASTILLO

- Letrada de la Sala Constitucional
- Licenciada en Derecho por la Universidad de Costa Rica
- Doctora en Derecho Privado y de la Empresa. Universidad Carlos III de Madrid
- Experta en Derecho Uniforme, Derecho Comunitario y Comercio Electrónico
- Redactora de los Proyectos de Ley números 19.012 y 21.183
- vsdelcastillo@hotmail.com

2



Entre el *back to basics* y los nuevos paradigmas de la revolución tecnológica.
Pensamientos para la reducción de la brecha tecnológica-jurídica y la estandarización de las legislaciones: caso costarricense.

Vilma Sánchez Del Castillo
Letrada de la Sala Constitucional
Licenciada en Derecho por la Universidad de Costa Rica
Doctora en Derecho Privado y de la Empresa. Universidad Carlos III de Madrid
Experta en Derecho Uniforme, Derecho Comunitario y Comercio Electrónico
Redactora de los Proyectos de Ley números 19.012 y 21.183
vsdelcastillo@hotmail.com

Palabras clave: Comercio Electrónico, Derecho Uniforme del Comercio Internacional, Derecho Comunitario Europeo, comercio electrónico *reloaded*, mercados electrónicos, plataformas electrónicas, electronificación, uniformidad del derecho, servicios de la sociedad de la información, servicios de intermediación.
Key words: E-commerce, Uniform Law of International Trade, European Community Law, reloaded e-commerce, electronic markets, electronic platforms -e-marketplaces-, electronification, harmonization, information society services, intermediary services.

Resumen: La revolución tecnológica ya es un tema asentado a nivel práctico y, avanza cada vez con mayor velocidad dejando atrás las estructuras legales decimonónicamente dictadas para pautas tradicionales. El *back to basics* planteado, pretende concientizar a los operadores legales costarricenses de la necesidad de ajustarse al orden proveniente de los cimientos del Derecho Uniforme del Comercio Internacional, el cual, se debe acoplar con los avances del Derecho Comunitario en la materia, como punto

de partida y marco de obligado anclaje para afrontar los retos del Comercio electrónico *reloaded.*

Abstract: The technological Revolution is already a well-established matter at a practical level and advances every day at an increasing pace; it is overcoming old legal structures set up at the 19 Century on the basis of traditional perceptions. The aim of the proclaimed back to basics consists in the building among the Costa Rican legal and commercial operators of the feeling of needed adaptation to the new legal realities: the rules incardinated onto the Uniform Law of International Trade as adapted to the advances and enlargement of the European Community Law. These rules encompass the starting point and the necessary framework in order to deal with the challenge offered by the legal discipline of the reloaded e-commerce.

I. PARTICULARIDADES Y BONDADES DEL DERECHO UNIFORME. EL *BACK TO BASICS.*

Como fiel seguidora y creyente de las bondades y capacidades prácticas y atemporales del Derecho Uniforme del Comercio Internacional -DUCI-, sobre el cual, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional -CNUDMI/UNCITRAL- nos ilustra desde hace más de 50 años estimo, indefectiblemente, que para atender de manera acertada la compleja disciplina jurídica y práctica que reviste al Derecho del Comercio Electrónico y a su fiel asociada, la revolución tecnológica, de inicio, es fundamental dominar esta disciplina.

El Derecho Uniforme en esta rama queda zanjado por medio de la Ley Modelo de la CNUDMI/UNCITRAL de Comercio Electrónico, que data ya del año 1995 y, que pretende, más allá del alcance del Derecho Internacional Privado, con sus normas de conflicto y fijación de la jurisdicción competente para conocer de una determinada desavenencia de carácter internacional establecer, *a priori*, cuál va a ser el fundamento legal que va a regularizar una determinada situación, erigiendo un marco

normativo de carácter uniforme, cuya interpretación también, se pretenda homogénea.

Esta referencia obliga *per se* a las partes a ajustarse a una ordenación que impida o, al menos, minimice a futuro la proliferación de conflictos -muy comunes en virtud del carácter eminentemente internacional de las transacciones electrónicas-.

El DUCI marca su ámbito de acción bajo la tutela de algunas máximas, que aún hoy, tras la aparición de la Segunda Revolución o Generación Tecnológica de la Economía, una Cuarta Revolución Industrial, una *Digital Transformation* o, como voy a decirle, un comercio electrónico "*Reloaded"* -con la nube, el auge del *Blockchain*, el fenómeno de la inteligencia artificial, la 3D, la robótica y, la incesante aparición de aplicaciones y plataformas que pretenden facilitarnos o, incluso, alterarnos la vida- sienta ese *back to basics* al trazar las líneas de acción para el desenvolvimiento del actual Derecho del Comercio Electrónico. Es decir, pese al despertar tecnológico, el comercio electrónico requerirá forzosamente y, todavía, de su auxilio y entendimiento, para arribar a un buen puerto.

Las máximas a que hago referencia son las siguientes:

a. La equivalencia funcional.

Este ápice se levanta como la capacidad reivindicatoria que coloca en un mismo nivel de eficacia y eficiencia jurídica, al documento electrónico y al sentado en soporte de papel. De esa forma, a fin que las manifestaciones de voluntad y las de ciencia y conocimiento, tengan impacto y razón de existir no solo en la práctica, sino en el ámbito legal, no se negará validez ni fuerza jurídica a las comunicaciones por el simple hecho de encontrarse en soporte electrónico.

El Derecho, principalmente, el español, con el apoyo y la inteligencia del principal creador y precursor del DUCI en el mundo, el Catedrático de Derecho Mercantil, Rafael Illescas Ortiz, introdujo en el Proyecto de Ley de

Reforma al Código Mercantil español, la noción de electronificación, que viene a establecer lo que me gusta llamar, la madurez del Derecho del Comercio Electrónico y de esa equivalencia. Reza la propuesta ibérica lo siguiente: "*Electronificación: Toda declaración o acto referido a la formación, perfección, administración, cumplimiento y extinción de los contratos mercantiles podrá efectuarse mediante comunicación electrónica entre las partes y entre estas y los terceros, salvo disposición expresa legal en contrario. 1.- Siempre que la ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico. 2.- La utilización de medios electrónicos en los contratos mercantiles ni requiere el acuerdo previo entre partes*".

b. La inalteración del derecho preexistente de obligaciones y contratos.

El presente axioma ordena que no deviene necesario el dictado de toda una nueva forma de disciplina jurídica, pues, en razón de la equivalencia entre las nociones de derecho que tradicionalmente se ceñían sobre las transacciones manuales y, las electrónicas, lo indispensable sería emitir normas marco o reformas específicas, para acoplar la entrada de las nuevas tecnologías al mundo del papel.

Si bien esta guía es la que más resquemores ha despertado, tomando en consideración los ya muchos cambios que la revolución digital ha levantado no solo a nivel de nomenclatura, sino, en razón de sus posibilidades prácticas y legales, es menester seguirla tomando en cuenta, aun cuando, hoy día existan temas erigidos plenamente a nivel electrónico, que por su novedad y reciente aparición, no habían sido vislumbrados en el derecho tradicional.

c. La neutralidad tecnológica.

Es la tercera guía que quiero resaltar. Predica que en razón de las constantes creaciones tecnológicas -de ayer, de hoy y de mañana- no nos podemos enlazar con una sola de ellas. Es necesario, para mantener un orden normativo actualizado, aceptar desde las tecnologías pasadas, hasta las futuras, en un ámbito neutral, que se desenvuelva en una amplitud tal, que no requiera de constantes cambios.

d. La vis expansiva.

El DUCI, en la persona del Catedrático Rafael Illescas, sienta otro aforismo. La vis expansiva. Esta máxima lo que propone es hacernos caer en cuenta que la transformación digital no sólo se acomoda en la economía, en el comercio y, en las ramas civiles y mercantiles de lo jurídico, sino que, va a abarcar a todas las disciplinas, acogiendo en su seno con las modificaciones que se requieran, a la normalización propia del Derecho Público, del Penal, del Administrativo, del Constitucional, en fin, de la materia que se nos ocurra y, además de empapar a nuestra vida cotidiana, también lo hará en cualquier profesión imaginable.

A *grosso* modo, sus fundamentos guiarán también el destino de todo lo que nos rodea, siendo que más allá de la acostumbrada mención a la *Internet of Things*, ya debemos pensar en la *Internet of Everything*.

e. Finalmente, al menos para lo que a este artículo concierne, tenemos la buena fe, como principio que proviene del derecho preexistente y, del cual, me reservaré algunos comentarios para el desenlace de este escrito.

En pleno contubernio con los principios referidos, también existen elementos objetivos y subjetivos nacidos del DUCI, que complementarán y darán forma al Derecho del Comercio Electrónico. Ellos son las nociones de: iniciador, destinatario e, intermediario, todos de un mensaje de datos y; la Internet y los sistemas de información, a los que ahora se pueden ir

agregando otros elementos, como lo podrían ser, el *blockchain*, la inteligencia artificial y, la robótica, por ejemplo.

Además, el DUCI aclara nociones tan importantes hoy día, como lo son lo que debe entenderse por escrito, firma, original, lo concerniente a la admisibilidad y fuerza probatoria de los mensajes de datos y las comunicaciones electrónicas, la conservación de los mensajes de datos, la formación y validez de los contratos, el reconocimiento por las partes de los mensajes de datos, la atribución de los mensajes de datos, el acuse de recibo y, el tiempo y lugar del envío y la recepción de un mensaje de datos. Lo dicho, solo para esbozar el contenido de la Ley Modelo de Comercio Electrónico, pero dejando abierto para su consideración que esta disciplina se encarga de dilucidar muchos más ámbitos y apartados, que no creo conveniente traer a colación acá, dada la dimensión de este estudio.

En consecuencia y, en relación con la primera parte de este escrito, nótese que en el título de este pequeño artículo aludo al *back to basics*, es decir, a la concientización de la importancia de los fundamentos del DUCI en el comercio electrónico para poder comprender, de manera cabal, la disrupción en que nos posiciona el mundo moderno.

Y es que para comprender el funcionamiento del comercio electrónico *reloaded*, resulta necesario, dominar el Derecho de la Contratación Electrónica en sus más elementales cimientos.

II. LOS NUEVOS PARADIGMAS DE LA REVOLUCIÓN DIGITAL. EN BUSCA DE LA REDUCCIÓN DE BRECHAS.

"*Las olas tecnológicas vienen más frecuentes y cambiantes, pero la empresa promedio de América latina es un surfeador demasiado propenso a trastabillar o, peor aún, dejar pasar las mejores oportunidades del lucirse en el mar de competidores globales*"

INCAE, Costa Rica

Uno de los más volátiles recursos con que cuenta la humanidad hoy día, es la tecnología, con lo cual, es imposible pensar que con solo el DUCI proclamado en la Ley Modelo de Comercio Electrónico, vaya a ser suficiente para atenderla plenamente. La aparición de sistemas como el *blockchain* y la inteligencia artificial -por mencionar solo dos-, nos provocan aún más cuestionamientos acerca de la forma en que debe erigirse este Derecho y, nos reta a implementar y complementar nuestros ordenamientos jurídicos.

Nosotros, los abogados, como curiosos/expertos/apasionados/estudiosos del derecho que rige a las tecnologías de la información, dando seguimiento a los propios prodigios que inventan y crean las tecnologías en sí, debemos cuestionarnos algo crucial: ¿en dónde estamos y hacia dónde vamos?. Esa labor no es baladí, pues, debe contener una pizca del pasado y del presente, sin dejar de tomar en consideración a las futuras creaciones tecnológicas de las que es posible, en este momento, no tengamos ni idea.

Es bien sabido que los Estados y sus organizaciones internas para normalizar o ponerse de acuerdo en algo, tienen que ajustarse a intrincados procesos burocráticos que, de más está decir, frenan el avance oportuno de la creación de cuerpos jurídicos legales que regulen, en lo que se estime necesario, el auge tecnológico; a ello, se suma que la legalidad, ni por asomo, puede transitar a la misma velocidad que lo hace la tecnología.

Los servicios de la sociedad de la información y sus respectivas plataformas, se vuelven cada vez más sofisticados y demandantes y, plantean desafíos y situaciones que nos conducen a un obligado replanteamiento de los dogmas legales y de los mapas jurídicos que hemos seguido durante tantos años y, que creíamos inescrutables.

Tan es así que, en el marco de la responsabilidad de los prestadores de servicios de la sociedad de la información que desde el año 2000 contempla la normativa comunitaria según el texto de la Directiva 2000/31, relativa a determinados aspectos jurídicos de los Servicios de la Sociedad de la Información y, desde el 2002, la Ley 34/2002 de España, de Servicios

de la Sociedad de la Información y de Comercio Electrónico, a 20 años de su vigencia, se está pensando incluir una reforma que se dirige a incluir a los prestadores de servicios de intermediación en un rol más activo dentro de sus funciones, a fin que no solo se vean compelidos a eliminar los contenidos que alojen provenientes de iniciadores que utilicen sus servicios hasta que se percaten de su ilicitud o de su ilegalidad, o bien, en el momento en que las autoridades administrativas y jurisdiccionales se los impongan; sino que la nueva tendencia rompedora de paradigmas, busca que estos participantes electrónicos concursen de manera proactiva y, se vean inducidos a implementar mecanismos para revisar de manera constante, tanto los contenidos que alojan en sus plataformas, como los datos que por su intermedio transiten.

Ese paso ya es casi una realidad y, los esfuerzos ya están dando frutos y fueron plasmados en los siguientes textos[1]: 1) Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de Servicios Digitales) y por el que se modifica la Directiva 2000/31, y; 2) Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales)[2]. Lo dicho, como seguimiento de una de las más recientes reformas comunitarias destinadas a la implementación ágil y segura de los servicios de intermediación en línea, el Reglamento 2019/1150 del Parlamento Europeo y del Consejo

[1] Estamos en presencia de dos documentos en suma ambiciosos que, de aprobarse, serían la máxima reforma a aplicar en 20 años a las normas dirigidas a regular los mercados electrónicos. Es una acción sin precedentes que busca, entre otras cosas, uniformar el derecho, modernizarlo, adaptarlo a las nuevas exigencias tecnológicas y, combatir la presencia de contenido ilegal o perjudicial, a través de la imposición de flamantes responsabilidades, obligaciones y sanciones a los intermediarios, todo en procura de la defensa de los derechos fundamentales en línea y de fortalecer la transparencia de los servicios y la diligencia debida de los operadores.

[2] En esta línea normativa, no puedo dejar de mencionar el más reciente proyecto de la Unión Europea, que pretende someter el mundo de la inteligencia artificial, a través de la “Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules artificial intelligence”.

sobre el fomento de la equidad y transparencia para los usuarios profesionales de servicios de intermediación en línea[3].

En lo que atañe al proyecto normativo relativo a un mercado único de servicios digitales, se comienza con una ávida reflexión: "*Desde que se adoptó la Directiva 2000/31/CE1 (la «Directiva sobre el comercio electrónico»), han aparecido nuevos e innovadores servicios (digitales) de la sociedad de la información que han transformado la vida cotidiana de los ciudadanos de la Unión y cambiado sus formas de comunicarse, conectarse, consumir y hacer negocios. Dichos servicios han contribuido en gran medida a las transformaciones sociales y económicas que se han producido en la Unión y en el mundo entero. Al mismo tiempo, esos servicios se han convertido en una fuente de nuevos riesgos y desafíos, tanto para la sociedad en su conjunto como para las personas que hacen uso de ellos. Los servicios digitales pueden coadyuvar al cumplimiento de los Objetivos de Desarrollo Sostenible al contribuir a la sostenibilidad económica, social y medioambiental. La crisis del coronavirus ha demostrado la importancia que tienen las tecnologías digitales en todos los aspectos de la vida moderna. Ha puesto claramente de relieve que nuestra economía y nuestra sociedad dependen de los servicios digitales, así como las ventajas y los riesgos que se derivan del actual marco de funcionamiento de dichos servicios* (…) *Considerando lo siguiente: (1) Los servicios de la sociedad de la información y especialmente los servicios intermediarios se han convertido en una parte importante de la economía de la Unión y de la vida cotidiana de sus ciudadanos. Veinte años después de la adopción del marco jurídico vigente aplicable a dichos servicios establecido en la Directiva 2000/31/CE del Parlamento Europeo y del*

[3] En su considerando primero, esa norma sienta que: "*Los servicios de intermediación en línea son factores esenciales para el emprendimiento y los nuevos modelos de negocio, el comercio y la innovación que, a su vez, también pueden potenciar el bienestar de los consumidores y cada vez se emplean más tanto en el sector privado como en el público. Facilitan el acceso a nuevos mercados y oportunidades comerciales de modo que permiten a las empresas aprovechar las ventajas del mercado interior. Permiten a los consumidores de la Unión obtener provecho de dichas ventajas, en concreto al ampliar la gama de bienes y servicios y al contribuir a la oferta de precios competitivos en línea, pero también plantean desafíos a los que hay que hacer frente si se quiere garantizar la seguridad jurídica*".

Consejo, han aparecido nuevos e innovadores modelos de negocio y servicios, como las redes sociales y los mercados en línea, que han permitido a los usuarios profesionales y a los consumidores comunicar información y acceder a ella, y efectuar transacciones de formas novedosas. La mayoría de los ciudadanos de la Unión utiliza ahora este tipo de servicios a diario. Sin embargo, la transformación digital y el creciente uso de tales servicios también entraña nuevos riesgos y desafíos, tanto para los usuarios a título individual como para la sociedad en su conjunto".

Incluso, en sus prospectivos considerandos, evocó la importancia de la armonización de las legislaciones, según se colige del siguiente párrafo: *"(4) Por tanto, a fin de salvaguardar y mejorar el funcionamiento del mercado interior, debe adoptarse un conjunto específico de normas uniformes, eficaces y proporcionadas de obligado cumplimiento en el ámbito de la Unión. En el presente Reglamento se establecen las condiciones para que aparezcan servicios digitales innovadores y se expandan en el mercado interior. Es necesario aproximar las disposiciones reglamentarias nacionales en el ámbito de la Unión en relación con los requisitos aplicables a los prestadores de servicios intermediarios a fin de evitar la fragmentación del mercado interior y ponerla fin, y garantizar la seguridad jurídica, de modo que se reduzca la incertidumbre para los desarrolladores y se fomente la interoperabilidad. Si se aplican requisitos tecnológicamente neutros, la innovación no debería verse obstaculizada sino estimulada*".

De la lectura de las anteriores citas, se vislumbra: 1) la innegable necesidad de armonizar el Derecho en esta disciplina, y; 2) que resulta menester compatibilizar las normas existentes, con las demandas del mercado digital moderno y sus nuevos participantes.

Sé que este foro está dirigido principalmente al caso costarricense y, tal vez, a América Latina. Pero lo que ha de quedar claro es que en estas materias, no existen fronteras, lo que provoca que la disparidad de culturas, legislaciones y, puntos de vista, prevalezcan. A nivel europeo y, a lo que a España concierne, con el soporte que brinda la Unión Europea y la cantidad

de Estados que colaboran en el pensamiento normativo que rige y, regirá a futuro, los mercados electrónicos, llegamos a un vértice indiscutible. La calidad de sus normas, tanto las transpuestas como las que entren directamente a regir en su ordenamiento interno como leyes europeas -caso de los Reglamentos Comunitarios-, aparte de ser uniformes, son por mucho superiores a las que surgen en América Latina.

A eso, se suma que la aplicación de la normativa comunitaria gozará de una riqueza interpretativa jurídica innegable, al provenir de las distintas jurisdicciones que engrosan los países miembros del entorno comunitario y, de la existencia de Tribunales Europeos.

De ahí que, sería conveniente que países como los nuestros para progresar y estrechar las brechas que nos separan del continente europeo, tomáramos nota de la experiencia del DUCI, lo compatibilizáramos con las propuestas y normas comunitarias -incluyo en este apartado la experiencia de potencias como los Estados Unidos de Norteamérica-, con el cometido de acceder de manera adecuada y segura al mercado internacional electrónico. ¿Para qué?, para reducir la brecha normativa y tecnológica que nos separa y, permitir que los operadores legales establecidos en Costa Rica ingresen a esos mercados extranjeros de manera competitiva y en respeto de la legalidad que nos imponen.

Lo recomendado tiene, incluso, una incidencia práctica, que no solo abarca el harto conocido espectro “alargado” de aplicación del Reglamento (EU) 2016/679, relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, que conmina hasta a los prestadores de servicios no establecidos en el entorno comunitario. Las flamantes propuestas también lo hacen sin tapujo alguno, lo que demuestra el fuerte escrutinio al que están sometidos los prestadores

de servicios de la sociedad de la información -en todas sus modalidades- de nuestras latitudes[4]. Esto es solo el principio.

III. PODRÍA EL DERECHO DIRIGIRSE A UNA ENCRUCIJADA Y CAER EN UN FIN APOCALÍPTICO EN EL ÁMBITO DE LA ELECTRÓNICA? RECOMENDACIONES.

Desde el momento en que las transacciones electrónicas no respetan las fronteras de las naciones, pulula la disparidad de las legislaciones y de las idiosincrasias nacionales, las tecnologías avanzan de forma imparable y a veces impredecible, crece el desconocimiento de los operadores legales hacia sitios práctica y jurídicamente inexplorados, aumenten los vacíos y las lagunas legales, nos encontremos ayunos de mecanismos internacionales capaces de satisfacer las exigencias de la Cuarta Revolución Industrial y, residamos en un mundo donde el Derecho Internacional Privado ya no se prevé como una solución viable o suficiente, deviene necesario crear un nuevo trazado que nos conduzca a la mejor solución posible.

De ahí que, ante el "vaticinio" de un futuro un tanto apocalíptico para nuestra economía y sus homólogas latinoamericanas y, lo mismo para su mundo normativo, propongo una serie de soluciones que, estimo, podrían favorecernos.

---

[4] Además de extender el ámbito de aplicación a los prestadores e intermediaries no domiciliados en la Unión Europea, se crean nuevas figuras e intervinientes. Para su conocimiento, el Proyecto de Reglamento relativo a un mercado único de servicios digitales, en su primer precepto, de aprobarse, dirá: "*Artículo 1 Objeto y ámbito de aplicación .1. El presente Reglamento establece normas armonizadas sobre la prestación de servicios intermediarios en el mercado interior. En particular, establece: a) un marco para la exención condicionada de responsabilidad de los prestadores de servicios intermediarios; b) normas sobre obligaciones específicas de diligencia debida adaptadas a determinadas categorías específicas de prestadores de servicios intermediarios; c) normas sobre aplicación y ejecución del presente Reglamento, por ejemplo, en relación con la cooperación y coordinación entre autoridades competentes. 2. El presente Reglamento tiene los siguientes fines: a) contribuir al correcto funcionamiento del mercado interior de servicios intermediarios; b)* ***establecer unas normas uniformes para crear un entorno en línea seguro, predecible y confiable****, en el que los derechos fundamentales consagrados en la Carta estén efectivamente protegidos.* ***3. El presente Reglamento se aplicará a los servicios intermediarios prestados a destinatarios del servicio que tengan su lugar de establecimiento o residencia en la Unión, con independencia del lugar de establecimiento de los prestadores de dichos servicios.*** *4. El presente Reglamento no se aplicará a ningún servicio que no sea un servicio intermediario ni a ningún requisito que se imponga al respecto de un servicio de esa índole, con independencia de si el servicio se presta mediante el uso de un servicio intermediario*" (el resaltado es nuestro). Juzguen ustedes mismos.

Las recomendaciones a este respecto, serían las siguientes:

a. La uniformidad y homogeneidad de las legislaciones. Mi mundo ideal.

"*Las incompatibilidades jurídicas y técnicas son las dos causas principales de dificultades en la utilización transfronteriza de los métodos de firma y autenticación electrónicas, en particular cuando su finalidad es sustituir una firma legalmente válida. Las incompatibilidades técnicas son las que afectan a la interoperatividad de los sistemas de autenticación. Las incompatibilidades jurídicas pueden surgir cuando las leyes de los diferentes ordenamientos estipulan diferentes requisitos en cuanto a la utilización y la validez de los métodos de firma y autenticación electrónicas* (…) *El riesgo que distintos países adopten criterios legislativos diferentes en relación con las firmas electrónicas exige disposiciones legislativas uniformes que establezcan las normas básicas de lo que constituye en esencia un fenómeno internacional, en el que es fundamental la armonía jurídica y la interoperabilidad técnica*".

Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas. CNUDMI/UNCITRAL, 2009.

Uno de los objetivos a perseguir es lograr que en el mundo se maneje un lenguaje común, de talante electrónico, donde la nomenclatura sea de uso general y de conocimiento de sus operadores. También, que lo tocante a las ordenanzas sobre protección y tratamiento de los datos de carácter personal, terceros de confianza, servicios intermediarios, derechos y deberes de los cuales gocen las partes que participen en las transacciones electrónicas, derecho de consumo, derechos humanos como prerrogativas de cuarta o quinta generación -sin ánimo de ser excluyente en mis menciones-, se estandaricen.

Esa precisamente ha sido la meta del DUCI desde hace más de 50 años. Misión cuyo valor no puede ser negado ni desconocido, pues, a través de convenciones internacionales, leyes modelo y guías jurídicas, que han favorecido la incorporación de sus atestados a los órdenes internos de gran cantidad de naciones, no ha hecho más que beneficiarnos y abastecer a muchos países en vías de desarrollo, de órdenes jurídicos de avanzada.

Pensemos esto. Si todos habláramos y entendiéramos un lenguaje común -entiéndase uniforme-, en un tema donde la nota preponderante es y, siempre será, su carácter internacional y el rompimiento de fronteras, no dudo que viviríamos en un sistema más organizado, menos complejo, complaciente y, con pocos o limitados conflictos, dudas y resquemores. En este espacio quimérico que propongo, ya ni siquiera sería necesario el Derecho Internacional Privado.

Voy más allá. Noten ustedes que en este universo de la homogeneidad, no estoy proponiendo necesariamente que los países y las naciones nos unamos en un Estado supranacional, para nada. Simplemente, creo que el mundo debería marchar en esta materia bajo un mismo norte, en el que los países más desarrollados y avanzados colaboren con los que nos encontramos en vías de desarrollo, para que esa brecha digital y legal que nos separa, desaparezca o, al menos, se reduzca.

Pero bueno, esta solución de equidad no se encuentra alejada de la realidad. Ya la Unión Europea la ha puesto en práctica y, ha funcionado. Es acá donde resaltan las Directivas comunitarias y los Reglamentos europeos -y las flamantes propuestas- traídos a colación en este pequeño ensayo. Además, el mundo de la autorregulación y de los códigos de conducta, grandes aliados en el tema de la electrónica, han sido de gran soporte.

b. Reglas varias.

Hace al menos 20 años uno que otro visionario, como en su momento lo fue Santiago Muñoz Machado, habló de tres posibilidades

regulatorias enrumbadas al sistema de información conocido con el nombre de Internet, la red de redes.

La primera, proponía que este ámbito debía permanecer inescrutado, sometido a su natural desenvolvimiento en un ambiente de libertad plena y, de libre circulación de ideas y mensajes.

La segunda, se decantaba por normar algunos extremos que se previeran de interés, a fin de brindar un flujo adecuado y continuo entre la prestación de servicios y, la protección de los usuarios de la red.

Por último, la tercera propuesta, sugería la necesidad de crear un régimen jurídico extremo, que contuviera cualquier posibilidad de abuso en el uso de las tecnologías de la información.

Con el paso de los años y, con los cambios y quebrantos sufridos por el principio de inalteración del derecho preexistente, podemos decir que ya tenemos un panorama un poco más prístino, que ha ido evolucionando en un vaivén de prueba y error que ha provocado la reforma, derogación, evolución y, cuestionamiento de muchas de las reglas primigenias vertidas para este ámbito[5]. Con esa base ya impuesta, será más sencillo determinar los parámetros que podrían o, deberían, ser incorporados en nuestro sistema normativo.

Pasando a otra idea, hay que tener mucho cuidado con la doble regulación, es decir, con la expedición de reglas contenidas en varios cuerpos legales que, al final de cuentas, pretendan normar lo mismo de manera diferente. Este tema se ha presentado como una constante en nuestra legislación.

Otra circunstancia a tomar en cuenta es que con la expedición de este tipo de ordenaciones debemos, en lo posible, brindar un cierto estatus de libertad al desenvolvimiento tecnológico, en la plataforma que se presente -principio de neutralidad tecnológica-.

[5] En el actual punto no quiero dejar de mencionar que la única disciplina que ha permanecido incólume en el tiempo, con apenas alguna variación o modernización, lo ha sido la del DUCI; lo que no es otra cosa que prueba fiel de su calidad y consistencia.

Asimismo, en el caso de países que en la actualidad no gocen de marcos legales suficientes en esta disciplina -como lo es el nuestro-, recomiendo acogerse a las prédicas del DUCI, mismas que han sido, con éxito, sometidas a prueba por más de 25 años, superando con creces las expectativas que imagino, pudieron haber vaticinado sus creadores -acá incluyo a la Ley Modelo de Documentos Electrónicos Transmisibles de la CNUDMI/UNCITRAL de 2017-.[19]

No omito pronunciarme también en esta línea, sobre la imperativa necesidad de apuntalar nuestros esfuerzos regulatorios, basándonos en la normativa ya vigente y en las nuevas propuestas de índole comunitario.

c. Valorar la capacidad de los mecanismos de autorregulación.

Los códigos de conducta devienen herramientas básicas en la sostenibilidad y desarrollo de los servicios de la sociedad de la información, en especial, en un mundo donde las plataformas y los mercados a los que pertenezcamos –piénsese en las plataformas en línea, como los mercados y las redes sociales- nos convierten, a nosotros, los seres humanos, en habitantes de una comunidad virtual que, si bien debe respetar el orden público y las normas dispositivas de los Derechos internos, se rigen por sus propias reglas y, hasta contienen sus propios mecanismos de solución de controversias.

d. La confianza: a propósito de la buena fe, como fiel expresión del principio sobre inalteración del derecho preexistente obligaciones y contratos.

Finalmente, quisiera agregar estos pensamientos que la modernidad nos conduce a transitar por caminos que antes no habíamos considerado. En este punto quiero retomar el principio del DUCI que predica la buena fe.

La buena fe, proviene nada más y nada menos que del principio de inalteración del derecho preexistente y, en los tiempos que corren, ha

adquirido una transcendencia impactante que nos reta a nosotros, a todos, como usuarios de las tecnologías de la información, a dejarnos caer en manos de las bondades y beneficios del entorno digital.

Les comento. Hace casi 10 años -este vórtice no se ha resuelto-, surgían una gran cantidad de dudas e inconsistencias en la utilización de las firmas electrónicas, a raíz de la disparidad de ordenaciones jurídicas y los problemas en el reconocimiento de las rúbricas electrónicas extranjeras, a tal punto que la CNUDMI/UNCITRAL publicó un excelso y revelador texto titulado "Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas", del cual, se extrajo una cita textual para ilustrar uno de los acápites previos.

Dentro de uno de sus apartados, se hizo referencia a la confianza y, en ese sentido se estatuyó lo que de seguido se transcribe: "*Aunque una firma manuscrita es una forma habitual de "autenticación" y sirve para documentos de transacción que cambian de manos entre partes conocidas, en muchas situaciones comerciales y administrativas una firma es sin embargo relativamente insegura. La persona que confía en el documento no suele disponer de los nombres de las personas autorizadas a firmar ni de especímenes de sus firmas a efectos de comparación. Esta situación es especialmente cierta en el caso de muchos documentos en los que se confía en países extranjeros en operaciones comerciales internacionales. Incluso cuando existe un espécimen de la firma autorizada con fines de comparación, tan solo un perito podrá detectar una falsificación bien hecha. Cuando se tramita un gran número de documentos, a veces ni siquiera se comparan las firmas, salvo cuando se trata de operaciones muy importantes. La confianza es uno de los elementos básicos de las relaciones comerciales internacionales*".

De nuevo, la sapiencia de la CNUDMI/UNCITRAL salta a la vista. La electrónica, a parte de sus implicaciones y evocación de la distancia entre las partes que la utilizan, muchas veces brinda más seguridad a las

transacciones que se gestan por su intermedio, que sus homólogas del papel.

La práctica y el paso del tiempo, llevaron a la Unión Europea a dictar el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo 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.

Dicho entramado, en suma técnico y complejo, crea la disciplina jurídica que va a girar sobre los prestadores de servicios de confianza, los sellos electrónicos y de tiempo y, las firmas electrónicas.

Sin embargo, se debe tener presente que de manera paralela a iniciativas como la mencionada, la tecnología nos está conduciendo a otros rumbos y, acá menciono la idea esbozada por la profesora Teresa Rodríguez de las Heras Ballell. Pese a que es inevitable requerir la intervención de los terceros de confianza, ahora, convivimos en ecosistemas que predican que los propios participantes de la electrónica, es decir, los servicios intermediarios, se involucren y coadyuven en la generación de la confianza, sin necesidad, muchas veces, de acudir al auxilio de esos otros prestadores de servicios de confianza. Este hecho magnifica el principio de buena fe.

IV. A MANERA DE CONCLUSIÓN.

Las posibilidades que la vida nos da en este siglo, son infinitas y, debido al auge electrónico, difíciles de predecir.

En mi criterio, lejos de mostrar miedo y limitar nuestro actuar virtual, debemos disfrutar de los regalos que la modernidad nos facilita, desplegándonos como lo hacemos siempre y, en el mundo real, con cautela.

Resulta aconsejable que los legisladores, gobernantes y los actores comerciales, abran sus mentes y faciliten la inserción de normas nacionales

basadas en el DUCI y en las reglas internacionales testadas a través de los años, para evitar caer en una separación que en algún punto, fortalezca y haga crecer aún más, la brecha digital-jurídica que ya separa el ordenamiento jurídico costarricense, de otras normalizaciones.

Desde mi experiencia, puedo decir que la regulación y expedición de una Ley Marco sobre Comercio Electrónico, conteniendo las menciones al DUCI y a normalizaciones de avanzada, como la comunitaria y la española, es lo ideal.

Pienso entonces, cómo es posible que a estas alturas, muchos se estén cuestionando la inserción a nuestro marco regulatorio de aspectos legales propios de la primera generación de la economía digital -sean, los fundamentos básicos del DUCI-, cuando ya los retos nos están llevando a otras dimensiones.

En este punto de constante inflexión cuestionémonos todos, sobre todo, la realidad que nos abarca y, dirijamos nuestros esfuerzos a renovar de manera decidida el ordenamiento costarricense. Plaguemos nuestro derecho de DUCI y, remocémoslo con las prescripciones del Derecho Comunitario que se requieran.

Les aseguro que con esta simple receta, nuestro país logrará postularse como un referente a nivel regional -sino internacional-, en lo que a la normativización de los mercados digitales atañe.

V. REFERENCIAS BIBLIOGRAFICAS.

Ley Modelo de la CNUDMI/UNCITRAL de Comercio Electrónico. (1996).

Proyecto de Ley de Reforma al Código Mercantil español (2014).

Reglamento 2019/1150 del Parlamento Europeo y del Consejo sobre el fomento de la equidad y transparencia para los usuarios profesionales de servicios de intermediación en línea

CNUDMI/UNCITRAL, 2009

Ley Modelo de Documentos Electrónicos Transmisibles de la CNUDMI/UNCITRAL (2017)

Reglamento (UE) 910/2014. Parlamento Europeo y del Consejo (2014)

JULIO CÓRDOBA ELIZONDO

- Licenciado en psicología por la Universidad Autónoma de Centro América
- Licenciado en Derecho por la Universidad Fidélitas Especialista en neuromarketing del Instituto Tecnológico de Costa Rica.
- Abogado litigante y consultor en derecho penal e informático, asesor psicológico en procesos legales. Conferencista en criptodivisas y derecho de las nuevas tecnologías.
- Miembro fundador de la Comisión de Derecho Informático y de la Comisión de Innovación Regulatoria del Colegio de Abogados y Abogadas de Costa Rica.
- julio@bufetecordoba.com

3



Reflexiones sobre algunas amenazas contra el bitcoin
(4 de mayo del 2021)

Julio Córdoba Elizondo
Licenciado en psicología por la Universidad Autónoma de Centro América
Licenciado en Derecho por la Universidad Fidélitas
Especialista en neuromarketing del Instituto Tecnológico de Costa Rica.
Abogado litigante y consultor en derecho penal e informático, asesor psicológico en procesos legales. Conferencista en criptodivisas y derecho de las nuevas tecnologías. Miembro fundador de la Comisión de Derecho Informático y de la Comisión de Innovación Regulatoria del Colegio de Abogados y Abogadas de Costa Rica.
julio@bufetecordoba.com

Resumen: Las monedas electrónicas y en especial el bitcoin son una tendencia económica global y objeto de estudio en foros académicos, de opinión y polémicas sobre la existencia de una moneda descentralizada, de respaldo civil, sin corporalidad ni emisión por parte de un banco central. La disrupción que significa en la economía mundial y en el campo tecnológico no está ajena a polémicas que podrían afectar su creciente aceptabilidad sino incluso la naturaleza funcional como medio de pago. Su coexistencia con monedas alternativas, situaciones delincuenciales, demanda energética, contaminación de la cadena de bloques y emisión de moneda digital soberana por parte de las naciones genera retos que de no ser superados podrían terminar minimizando o acabando la criptoeconomía.

Palabras clave: bitcoin, monedas electrónicas, blockchain, economía, delito, crimen, medio ambiente.

Abstract: Electronic currencies and especially bitcoin are a global economic trend and object of study in academic forums, opinion and controversies about the existence of a decentralized currency, with civil support, without corporeality or issuance by a central bank. The disruption that it means in the world economy and in the technological field are not immune to controversies that could affect its acceptability but even its functional nature as a means of payment. Its coexistence with alternative currencies, criminal situations, energy demand, contamination of the blockchain and issuance of sovereign electronic currency by nations generates challenges that, if not overcome, could end up minimizing or ending the crypto economy.

Keywords: bitcoin, electronic currencies, blockchain, economy, crime, crime, environment.

Introducción. Qué es la criptoeconomía.

Desde que iniciamos la vida el dinero se transforma en una cotidianidad que simplemente aceptamos sin racionalizar, simplemente se transforma en parte de las experiencias cuando vemos a nuestros padres laborar para generar ingresos, con esos ingresos se realizan pagos, con esos pagos se adquieren los alimentos y servicios para la vida familiar.

Cuando ingresamos al sistema educativo se nos entrega dinero para hacer la compra de merienda en el recreo, nos profundizamos sin concientizar que reconocemos su alcance finito respecto a nuestros deseos por lo que tenemos que administrarlo con economía.

En ese proceso de crecimiento nos damos cuenta que no todas las personas tienen los mismos bienes y capacidad de pago, correlacionando así la actividad profesional o comercial respecto a lo más rentable y lo menos rentable, llevándonos entonces al final de la secundaria a tomar decisiones para la vida, muchas veces desde las necesidad y oportunidades relacionadas también con el dinero, eligiendo una opción de formación según su costo respecto a lo que tenemos la expectativa de ganar, es decir -sin caer en reduccionismos materialistas-, la elección vocacional tiene una arista económica la cual es ganar lo suficiente para vivir puesto que solo una persona privilegiada con la virtud del ingreso garantizada por fuentes no laborales podría elegir su carrera universitaria desde la perspectiva de no generar dinero.

Todo lo anterior gira alrededor de monedas y billetes, esas que acuñan nuestros gobiernos mediante la banca central y que proveen a la sociedad del circulante para pagar lo comprado, cobrar lo vendido y realizar donaciones u obsequios.

En alguna medida damos por sentado que el sistema económico siempre fue así y, quizás, siempre será así pero la construcción sociojurídica de lo que consideramos dinero es una evolución histórica de siglos (Córdoba, 2014).

Este sistema centralizado de emisión monetaria, de respaldo estatal -es decir, por los gobiernos- tuvo un fuerte cuestionamiento con repercusiones económicas globales en el año 2009 con el texto o manifiesto de un usuario o colectivo no identificado (aún) llamado Satoshi Nakamoto intitulado “Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario” en el que propone un sistema económico global descentralizado, sin la participación de los gobiernos ni la banca tradicional, basado en la confianza de los usuarios del sistema, generado y respaldado en la fuerza computacional que aportan los participantes.

Este sistema económico tecnológico ha llegado a constituir la moneda que más alto cotiza en el planeta, sin respaldo estatal, corporalidad (como las monedas y billetes) ni manipulación por parte de operadores políticos.

Como toda innovación, y en este caso de características revolucionarias, surgen industrias colaterales, en el caso puntual podemos citar -pero sin limitarnos a- la educación en el tema, el *trading* o especulación con la compra y venta, la minería o proceso de generación de criptodivisas y las casas de cambio.

Al momento de redactar este artículo el bitcoin bordea sus máximos históricos y diversas especulaciones auguran mayores ascensos o estrepitosas caídas, sin embargo dada la notoriedad del tema, los cuestionamientos y las diferentes posturas gubernamentales, incluso con una corrección de precio a la baja difícilmente el sistema será abandonado o inutilizado, puesto que históricamente ya ha sobrevivido a severas caídas en el precio respecto a la moneda de referencia que es el dólar.

No obstante lo anterior, sobre este auge de innovación, educación y comercio, el sistema tiene naturalmente sus críticas, algunas de ellas muy fundamentadas y que conllevan una reflexión para la toma de decisiones, especialmente de quienes tienen inversiones en criptomonedas y quienes desarrollan emprendimientos relacionados, temas de los cuales nos referiremos de seguido.

Criptopercances por inversiones inciertas

Es inherente a la motivación humana la búsqueda de prosperidad, riquezas y aun fama. La historia muestra cómo desde la antigüedad la expansión territorial y dominio de otros pueblos daba prestigio al soberano, también los esfuerzos de aventureros por “descubrir” territorios no señalados en los mapas y colonizarlos,

así como el busca fortuna en lugares “sin ley” como la fiebre del oro en el siglo XIX en el viejo oeste estadounidense o en nuestro país con la mina Crucitas cuyos coligalleros la explotan con mucha tranquilidad, de forma constante, próspera e ilegal.

Las monedas electrónicas son por mucho un atractivo por su alta volatilidad y las historias de “criptomillonarios”, personas que compraron la divisa digital a precios de centavo y luego transformaron su patrimonio cuando esta se elevó de forma súbita.

Todo esto atrae personas curtidas en inversión que estudian la materia, se asesoran y toman decisiones altamente racionalizadas, así como entusiastas que en poca comprensión pero sí mucha sensación terminan realizando una apuesta emocional sin fundamento intelectual que termina generando pérdidas dinerarias o severos golpes patrimoniales por incomprensión de la volatilidad, tecnología y capacidad de análisis de la moneda en la cual se está invirtiendo.

Esta situación lleva a que estas historias se compartan con recelo y muchos tengan desconfianza en las monedas electrónicas, puesto que conocen la historia de personas que perdieron y mucho.

Esquemas piramidales.

Aunque el Código Penal tipifica la estafa (numeral 216) y la Ley Orgánica del Banco Central de Costa Rica establece que solo entidades autorizadas pueden realizar intermediación financiera y quien la realice sin autorización se expone a pena de prisión de hasta seis años (artículos 116 y 157 respectivamente), han cundido advenedizos que valiéndose de ser figuras públicas promueven la “inversión en criptodivisas” como si fuera la olla de oro al final del arcoíris.

De ahí estas personas con trayectorias provenientes del mundo del fútbol, modelaje o humor, antes de la pandemia realizaban giras al interior del país reuniendo multitudes en salones comunales para hablarles de las virtudes de invertir en sus productos financieros, ofreciendo rendimientos excepcionalmente altos e invitándolos a traer a sus amigos y parientes al negocio… a cambio de una cuota mensual, de la cual pueden recibir una comisión.

Por lógica una persona que haya encontrado (por estudio, iluminación repentina o adquisición) la fórmula para las riquezas en mercados financieros se dedicaría a estar haciendo millones y billones con sus inversiones, empero el caso criollo es que este valioso tiempo es dedicado al reclutamiento de nuevos miembros para que participen en los placeres de este exclusivo mundo digno de magnates petroleros de Medio Oriente.

Esta situación tiene más similitud, la cual debería ser profundamente investigada por el Ministerio Público, con la reconocida estafa ponzi o esquema piramidal que con una inversión legítima.

Como lo desarrolla Jiménez (2019) el ardid de la estafa piramidal consiste en hacer creer a las personas que necesitan invertir dinero en un producto que no existe a cambio de alto retorno, sin embargo si se dan ganancias estas proceden de intereses generados y reclutamiento de nuevos individuos.

En pocas palabras, muchas personas invirtiendo en un producto que no existe o no entienden bajo la promesa de grandes sumas de dinero como retorno, todo gracias a la bondad de una persona famosa y amable generadora de confianza.

Esta práctica, que a la fecha parece impune, deteriora la aceptabilidad social de las monedas electrónicas (confianza necesaria para que funcione como dinero) porque resta credibilidad, debilitando el movimiento supranacional que pretende normalizar las monedas no gubernamentales basadas en capacidad computacional para el intercambio económico.

Monedas electrónicas falsas o de poco futuro, esquemas ponzi y otras estafas

En la actualidad hay más de 8400 monedas electrónicas (Castro, 2021), no obstante muchas de estas no llegan a ver una luz y son catalogadas con el malsonante de *shitcoins*.

En el apartado de “Diccionario Blockchain” Gutiérrez, Gutiérrez y Jaén (2018) definen el *altcoin* como “cualquier moneda criptográfica que no sea bitcoin y tenga su propia Blockchain” (p. 73) y la *shitcoin* como “moneda sin valor potencial o uso, altcoin de nivel bajo” (p.74).

Lo anterior no quiere decir que toda *altcoin* sea una *shitcoin* pero sí la gran mayoría de las altcoins y otras monedas electrónicas centralizadas podrían ser *shitcoin*.

“De hecho, entre las aproximadamente 5.000 criptomonedas que existen en la actualidad, hay cientos de ejemplos en los que los proyectos han fallado por varias razones. También hay docenas de monedas alternativas sospechosas de convertirse en shitcoin. Proyectos como Useless Token (token inútil), OneCoin y Siacoin Classic, son imposibles de cambiar por dinero real, así que tenga cuidado” señala la periodista especializada en monedas electrónicas Marianella Vanci (2020).

Dada la severidad o riesgo que presenta esta situación, hemos propuesto en reiteradas conferencias desde años atrás (Córdoba, 2018) un camino lógico para acercarnos para formar opinión sobre una moneda electrónica específica, ya que como se indicó estas sobreabundan como árboles en un parque nacional.

En primer lugar es necesario que evaluemos si la moneda electrónica que se nos presenta tiene un léxico propio de multinivel.

Sobre lo anterior hacemos un paréntesis para eliminar de forma preventiva todo rastro descalificante sobre los multiniveles. Paes, citado por Reyes (2019) indica sobre el multinivel que “es una de las formas de negocio de más rápido crecimiento en los últimos años en casi todo el mundo. Para la mayoría de los entendidos que estudian tendencias de mercado, el Multinivel es una opción para los negocios familiares y para las grandes empresas una alternativa de reducir la distancia entre los proveedores de productos o servicios y el consumidor final”, es decir se trata de un sistema que mueve productos o servicios donde el grueso del dinero no se genera por afiliaciones sino por el consumo y / o venta del producto.

Aclarado el punto es llamativo que algunas monedas electrónicas centralizadas (sobre esto nos referiremos más adelante) se coloquen en el mercado mediante léxicos de multinivel ya que es profundamente peligroso.

Para ingresar a esto primero tenemos que abordar “la salida al mercado” de la moneda.
En la criptopedia del portal Criptonoticias se define el ICO como “una Oferta Inicial de Monedas o ICO (Initial Coin Offering, del inglés), es un mecanismo de financiamiento que permite a un proyecto o empresa recaudar capital en

criptomonedas con alta liquidez, como Bitcoin o Ethereum, y monedas fíat, como dólar o euro, a través de la venta multitudinaria de un criptoactivo nuevo. Es un caso de uso del crowdfunding, el cual es un método de financiar un proyecto o empresa mediante la recaudación de muchas pequeñas cantidades de dinero desde un gran número de personas, típicamente por Internet. El término puede ser análogo con «venta masiva» o crowdsale."

Es importante estar atento a ciertos esquemas en que la moneda es vendida mediante un sistema de referidos, es decir, que para participar se otorguen beneficios si se lleva a otros personas para que las compren ya que la lógica de la venta es, como verdad de perogrullo, que se vendan y no el formar una red piramidal de personas beneficiarias con la colocación de más monedas.

Una moneda electrónica ofertada al público en estos términos debe llevar al menos a una alerta sobre la legitimidad del producto que se está comprando: para comprar monedas no debería ser necesario llevar referidos (esto aplica para comprar cualquier bien o servicio).

Cómo segundo punto se debe destacar si el sistema es centralizado o descentralizado. Recordemos que en el sistema de bloques del bitcoin toda la red de computadoras participantes hace que el sistema sea descentralizado.

De hecho como bien lo explica Navarro (2017) "las redes blockchain son altamente escalables, descentralizadas y peer-to-peer. Es así que, la integridad está basada en un mecanismo de consenso, en vez de una infraestructura basada en la confianza sobre un organismo central, como sería un banco u otra entidad financiera. La red P2P evita que un único participante o grupo controlen el sistema completo. Todos los integrantes de una red se adhieren, a los mismos protocolos, ya sean individuos, organizaciones o actores estatales. Las

transacciones son irreversibles, por lo que una vez realizadas no pueden anularse, modificarse o revertirse.”

Es decir, lo valioso del movimiento iniciado por Nakamoto tiene intrínseco un pensamiento donde el poder computacional transfiere el gobierno económico del sistema bancario tradicional y de confianza legal -inicialmente de los Estados- a la población civil, por lo que llegar a invertir en una moneda electrónica centralizada es simplemente cambiar la banca central del dinero fiducario por un mecanismo análogo: es quedar en las mismas.

En tercer punto es usual escuchar la pregunta si es seguro invertir en criptodivisas, lo cual se puede contestar con otra pregunta “¿El dinero que piensa invertir lo necesita o puede darse el lujo de perderlo?”, si la respuesta es que no, la persona haría mejor ingresando esos recursos en una inversión tradicional o cubriendo una necesidad personal.

Las historias de “criptomillonarios” tienen amplia difusión, no obstante la historia de los grandes perdedores rara vez se publica. Con solo apreciar las fluctuaciones históricas del bitcoin, en cada uno de sus movimientos, hubo ganadores y perdedores, siendo popularizados únicamente los primeros.

Siendo que el bitcoin es la moneda arquetipo de este sistema computacional, la más estudiada, la de mayor difusión y no exenta de controversias, el aventurarse a invertir en otras monedas electrónicas “porque son nuevas” y “crecerán como la espuma” pueden ser las mismas premisas emotivo-intelectuales con que se participa en loterías.

Como cuarto punto, aparejado a las mismas especies explayadas respecto a los multiniveles, también es importante mencionar que también existe la “oferta” de

entregar el dinero a un tercero para que lo invierta en monedas electrónicas, puntualmente para que haga “trading”, o sea el especular con la compra y venta de monedas electrónicas.

Esta “inversión” es en sí un desafío jurídico y lógico. Sobre lo legal ya se mencionó con anterioridad que en Costa Rica no se puede captar dinero del público para realizar intermediación financiera sin estar debidamente autorizado. En segundo punto -y más lógico y protagónico quizás- es el hecho que una persona que sabe cómo hacer dinero con los mercados financieros hace, valga la redundancia, dinero en los mercados financieros y carece de toda lógica que descuide sus riquezas y libertad para engrandecer la de otros puesto que, como juicio de derivación, siendo una persona rica no tiene necesidad de ganar comisiones sobre ganancias de dinero ajeno.

Basta decir que si una persona entrega sus ahorros para que sean invertidos de esta forma y no puede explicar cómo se va a generar el dinero, simplemente va expuesto a un mal final por manejar sus finanzas desde la irresponsabilidad del azar.

¿Burbuja?. Finalmente, de forma válida, hay quienes preguntan si las pasiones de las monedas electrónicas y en especial el bitcoin, corresponden a una burbuja.

Astray (2019) explica que “Las burbujas se caracterizan por la inestabilidad, por etapas de fuerte crecimiento (“vacas gordas”) seguidas de grandes depresiones (o “vacas flacas”), que en ningún caso se ven compensadas por los beneficios obtenidos durante el crecimiento (González, 2014). Lo que generan estos momentos de crecimiento o expansión económica en el proceso de creación de una burbuja, es que los inversores estén dispuestos a aceptar mayores riesgos.

Tanto particulares como empresas comienzan a financiarse con fondos de carácter especulativo, de manera que, ante cualquier imprevisto, no pueden hacer frente a sus deudas. Minsky (1992) afirma que, “ante la inexistencia de dificultades económicas, se genera una economía expansiva en la que las posiciones cortoplacistas, el riesgo, las innovaciones financieras o la deuda, lo son todo. En este sentido, cuánto mayor sea el período expansivo de la economía, mayores son los desequilibrios del sistema”.

En la historia de las burbujas como la de los tulipanes, la Gran Depresión, la de las punto com y la inmobiliaria, tienen por igual característica que no existe homogeneidad de criterios sobre si es una burbuja o no y por unanimidad es burbuja hasta que estalla, siendo así que el decir que las monedas electrónicas son una burbuja tiene argumentos a favor y en contra, por lo que simplemente se debe tener presente la premisa que, tanto en monedas electrónicas “duras” como en otras novedosas, lo más saludable es invertir dinero no vital para las necesidades personales.

El riesgo ambiental

Las naciones han ratificado acuerdos para enfrentar el reto del calentamiento global. En el artículo primero de la Convención Marco de Naciones Unidas sobre el Cambio Climático (ONU), Ley 7414, se definen los conceptos relacionados con el cambio climático “el cual se entiende (como) un cambio de clima atribuido directa o indirectamente a la actividad humana que altera la composición de la atmósfera mundial y que se suma a la variabilidad natural del clima observada durante períodos de tiempo comparables” y ”Por "emisiones" se entiende la liberación de gases de efecto invernadero o sus precursores en la atmósfera en un área y un período de tiempo especificado. 5.- Por "gases de efecto

invernadero" se entiende aquellos componentes gaseosos de la atmósfera, tanto naturales como antropógenos, que absorben y reemiten radiación infrarroja".

Un reporte de Infobae especifica que "Un informe de Citigroup Inc. divulgado el pasado 13 de abril reportó que Bitcoin consume 66 veces más electricidad que en 2015 y que las emisiones de carbono asociadas a esta minería probablemente se enfrentarán a un escrutinio cada vez mayor" y agrega que en 2019 por cada dólar de valor creado por en la minería bitcoin se producía 49 centavos de daños a la salud y medio ambiente en los Estados Unidos, y es que el consumo eléctrico anual global en minería supera a Holanda.

Es un hecho indiscutible que la minería no está siendo apreciada como una experiencia ecológica y una de las voces más calificadas de la humanidad en preservación del medio ambiente ha realizado su señalamiento al respecto: Bil Gates.

El sitio web La Información (2021) alertó sobre esto "Una de las razones por las que Gates no es partidario de esta moneda virtual es puramente medioambiental. Lo que ocurre es que para "minar" la criptomoneda, se utilizan enormes servidores que no paran de trabajar, algo que consume ingentes cantidades de energía. Más electricidad, incluso, que Finlandia, Suiza o Argentina, según un análisis del Centro de Finanzas Alternativas de la Universidad de Cambridge. Recordemos, que Bill Gates siempre ha sido uno de los mayores impulsores de la lucha contra el cambio climático."

Y es que esto es un problema que no se está logrando enfrentar puesto que a mayor exposición de las oportunidades de negocios más personas especulan con cripto e invierten en minería, lo cual aumenta la demanda energética.

Palacios, Vela y TaraZona (2015) explican cómo la minería empezó a cobrar protagonismo en la demanda energética de la criptoeconomía: “En sus inicios, un bitcoin se compraba por 25 centavos en un intercambio, y un minero con solo la CPU de un ordenador podía minar una cantidad considerable de nuevos bitcoins en un día. Con el paso del tiempo la creación de bitcoins ha aumentado su complejidad [103], lo que significa que los mineros necesitan constantemente la potencia de procesamiento más avanzada para competir, siendo indispensable las computadoras diseñadas exclusivamente para la minería. Como consecuencia han surgido las siguientes tecnologías para hacer minería, cada una de ellas más rápida y eficiente que la anterior: CPU, GPU, FPGA y la que actualmente se utiliza: la plataforma de circuito integrado de aplicación específica (ASIC), diseñada particularmente para ejecutar la operación de hash [104]. De este modo, Taylor describe en detalle la evolución de los hardware anteriormente mencionados para la minería Bitcoin” (p. 116).

Entre más capacidad computacional se posee más posibilidades hay de participar en el sistema de recompensas por minar cripto. Este 30 de abril de 2021 el portal dedicado a las criptomonedas, Criptonoticias, informó sobre las preocupaciones del gobierno chino al respecto: “Las autoridades de Pekín, capital de China, se encuentran realizando investigaciones para conocer más sobre el impacto de las granjas de minería de criptomonedas sobre el consumo energético.”

Y si bien, sería plausible que los grandes emprendimientos en granjas de cripto utilicen energías limpias, es complicado porque a mayor crecimiento del mercado mayor es la demanda para garantizar la transparencia del sistema económico de la red peer to peer global del bitcoin, como lo explica Segesdi (2019) “Este sistema de validación de transacciones es una de las principales críticas dirigidas a Bitcoin y sus clones (criptomonedas similares) por el impacto

en el medio ambiente, ya que la articulación en la Cadena de Bloques genera cálculos que consumen enormes cantidades de energía utilizada solo para validar las transacciones del sistema.” (p. 6)

En este escenario si autoridades gubernamentales y activistas unen esfuerzos contra el cambio climático enfocándose en los efectos colaterales de la minería, podría afectar tanto la cotización de las criptomonedas y, en caso extremo, arriesgar el sistema mismo en caso de ejecutarse directrices tendientes a la regulación, desestimulación e incitación a la proscripción.

La contaminación del blockchain con contenido ilegal

Como se ha mencionado con anterioridad, la particularidad de un blockchain robusto con el de bitcoin u otras monedas electrónicas descentralizadas es que su contenido no es corregible una vez consumado el bloque: “La llamada “cadena de bloques” (blockchain, en inglés) es un protocolo criptográfico, usado inicialmente para crear la divisa Bitcoin. En síntesis, se basa en integrar ficheros informáticos, relacionados matricialmente por identificadores o códigos (por ejemplo, alfanuméricos), según combinaciones generadas con algoritmos, en múltiples ordenadores y de forma idéntica en todos. Lo cual, cuando un número suficiente de usuarios participa en el sistema, permite la perfecta, irreversible y sincrónica identificación del contenido incorporado a aquellos ficheros.” (Íbañes, 2018, p.1)

Esta característica de irreversible es sin duda una virtud, empero vale el cuestionamiento sobre qué pasaría si una persona incluye en la cadena de bloques información indeseable como secretos, apología de delitos, imágenes privadas en venganza contra otra persona, manifiestos racistas, homofóbicos o

xenofóbicos o, pornografía infantil, para citar solo algunas gravedades. La contestación no es amable porque ya ocurrió.

La compañía de seguridad McAfee (2018) en su publicación sobre riesgos al blockchain estableció que “(…) en un libro de contabilidad de blockchain no solo se puede registrar dinero. Bitcoin permite almacenar en sus transacciones una pequeña cantidad de información adicional. Los investigadores han encontrado documentos filtrados, datos arbitrarios e incluso pornografía almacenada y recuperable en el libro de contabilidad de Bitcoin. Algunos libros de contabilidad están diseñados para almacenar programas enteros que pueden ejecutar los participantes del blockchain. Ether, la segunda criptomoneda en popularidad, hace esto con un "smart contract" (contrato inteligente). En esa implementación, el código, o contrato, se carga en el libro de contabilidad” (p. 5)

Sin duda esta situación supera cualquier reserva política, ambiental o ideológica, sino que aparte de lo inaceptable de la acción puede exponer a personas que participan en el ecosistema de bloques a almacenar esta información del libro contable en su registro informático, con eventuales consecuencias penales puesto que la tenencia de algún material como lo es el de pornografía infantil es castigado y perseguido internacionalmente gracias a el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y utilización de niños en la pornografía, que corresponde a la Ley Nº 8172, y además nuestro Código Penal sanciona la fabricación, producción o reproducción de pornografía infantil (artículo 173), la tenencia de pornografía infantil (artículo 173 bis), la difusión de pornografía infantil (artículo 174) y la pornografía virtual y pseudopornografía infantil (artículo 174 bis).

Esta situación puede generar la tormenta perfecta para el ecosistema de la criptoeconomía porque contaminada la información, contaminado todo el

sistema con uno de los delitos más pluriofensivos contra la dignidad humana que es atentar de esta forma contra la niñez.

Las repercusiones sobre esto son difíciles de dimensionar y podría motivar la desestimulación completa de participar en el sistema, la persecución de los participantes o decisiones drásticas de gobiernos para tomar medidas en nombre del cumplimiento de la legalidad penal.

Criptomonedas gubernamentales ¿Un retroceso?

La profundización del sistema económico propuesto por Nakamoto y deriva en una sociedad más horizontal; ácrata, de ahí su funcionamiento civil, su búsqueda de confianza en la capacidad computacional y el respaldo originado por los participantes del sistema sin soberanía de gobierno alguno.

Wim Dierckxsens y Walter Formento (2018) lo explican con detalle “Bitcoin se caracteriza por ser una red descentralizada que no está respaldada por ningún gobierno o banco central y cada transacción requiere algún trabajo para registrarlo en la historia de todas las transacciones y que tiene cierto costo. Tal trabajo que es realizado para impedir que un mismo Bitcoin sea utilizado varias veces. En cada transacción, los registros digitales – resúmenes criptográficos- se agrupan en bloques, vinculándose posteriormente de manera cronológica en una cadena de complejos algoritmos matemáticos, proceso llamado hashing. Este proceso es llevado adelante por numerosas computadoras o nodos distribuidos en distintas partes del globo, que corroboran la validez de la respuesta, dotando a cada bloque de una exclusiva firma digital,manteniendo los datos seguro” (p. 2)

China, como sociedad y potencia, es la segunda economía mundial y está construyendo una hegemonía diplomática, tecnológica, logística y financiera, de ahí que su propuesta de crear su propia moneda electrónica es por mucho la más llamativa para los fines de este artículo.

Como bien explica Víctor Ventura (2021), desde el manifiesto de Nakamoto a la propuesta de Pekín hay diferencias propias del agua y aceite: "El principal objetivo del creador del bitcoin, Satoshi Nakamoto, era crear una moneda anónima, sin nadie que controle ni supervise las operaciones, para apoyar una visión libertaria de la economía. Utilizando mecanismos similares, el Gobierno de China está preparando todo lo contrario: el 'eYuan', una criptomoneda controlada por el Banco Central que permita a las autoridades del país conocer todas las transacciones de todos sus ciudadanos, minuto a minuto. Y sus pruebas ya avanzan en varias ciudades."

China tiene una modalidad política que podríamos llamar capitalismo vigilante o totalitarismo capitalista, en el cual la tecnología tiene una fuerte función de control en la vida ciudadana.

China, con sus grandes bases de datos agregadas, controla el comportamiento social mediante un sistema de créditos que premia o castiga con base a la conducta de la persona en el mundo digital o analógico, por lo que personas que sean sancionadas no podrán utilizar el avión o el tren (Aribau, 2018, p.7).

Todo esto conlleva a un choque en la lógica de la filosofía de la criptoeconomía, "Nidia Osimani señala que en 2014, el Banco Popular de China comenzó a experimentar en la producción de su propia moneda digital similar al Bitcoin, para ser utilizada en intercambios comerciales más allá de sus fronteras, que redujera de manera drástica los costos de las transacciones. Se buscaba

garantizar, además, un sistema seguro de registración y transferencia contra la evasión tributaria y el lavado de dinero. Finalizando 2016, ya realizó su primer ensayo, siendo ésta la primera criptomoneda respaldada por un Banco Central en todo el mundo, basada en tecnología blockchain. La cripto-moneda emitida por el Banco Central de China Constituirá una moneda controlada exclusivamente por la autoridad monetaria de ese país y por ninguna otra entidad financiera. La eventualidad de la tecnología Blockchain y el dinero digital como medio de intercambio en la nueva Ruta de la Seda, reemplazaría nada más y nada menos que al dólar" (Dierckxsens y Formento, 2018).

¿Cuál es el inconveniente? Que no hay diferencia entre utilizar el dinero emitido por el banco central en términos tradicionales (monedas y billetes) que uno, con el barniz del discurso cripto, que incluso dará mayor trazabilidad a la conducta de la persona invadiendo esferas inimaginables de sus hábitos de consumo.

Pero esto no es una cuestión exclusivamente china, "Una encuesta reciente del Banco de Pagos Internacionales ha revelado que hasta el 80% de todos los bancos centrales han considerado emitir sus propias monedas digitales. La Reserva Federal, el Banco Central Europeo (BCE), el Banco de Inglaterra y las autoridades monetarias de Rusia e India también han iniciado el proceso de desarrollo de sus propias criptomonedas. Pero China ha tomado la delantera al resto de países creando el yuan digital. El Banco Popular de China ha distribuido más de 100 millones de yuanes digitales hasta ahora", explica Fortuño (2021) en el Blog Salmón.

Como vemos occidente no se queda atrás y Europa promete respetar la privacidad con el euro digital, para lo cual realizó una consulta pública cuyos resultados fueron comunicados al público el pasado 14 de abril: "El Banco Central Europeo (BCE) ha publicado hoy un análisis exhaustivo de su consulta

pública sobre un euro digital. El análisis confirma, en general, nuestras conclusiones iniciales: lo que más esperan los ciudadanos y los profesionales de una moneda digital de este tipo es privacidad (43 %), seguida de seguridad (18 %) y la posibilidad de pagar en toda la zona del euro (11 %), sin costes adicionales (9 %) y sin conexión a Internet (8 %)", reza el comunicado.

Si bien el euro digital no es una criptodivisa ni es descentralizada, al igual que la china, lo que hará es relacionar al usuario directamente con la banca central centralizando la información de las transacciones (Nieves, 2021), con un fuerte componente en el compromiso de privacidad.

Si bien no es negable la tradición europea por la protección de datos personales y Derechos Humanos, este tipo de moneda no es más que una evolución del tradicional dinero fiduciario, con la novedad de la disminución de la participación de los agentes comerciales como bancos y proveedores de tarjetas de crédito, con una propuesta que sí otorgaría mayor confianza en cuanto al mencionado compromiso de respeto por la intimidad del usuario en sus operaciones financieras.

Sin embargo, a pesar de los buenos ojos que genera un euro digital, la inminente emisión de criptomonedas soberanas centralizadas no es más que la continuidad del monopolio en la emisión monetaria desarrollada desde hace poco más de un siglo con el surgimiento de la banca central (Córdoba, 2014), y por ende en un retroceso o un camino totalmente diferente al valor de la descentralización basado en potencia computacional en el blockchain.

CONCLUSIONES

De toda la revolución tecnológica disfrutada durante poco más de una década, afirmar que la criptoeconomía llegó para quedarse es una idea aceptable pero tampoco es descabellado sentir preocupación por la posibilidad que no logre superar sus retos, de los cuales hemos apenas abordado algunos en este artículo.

Si bien no todos son igual de protagónicos, consideramos que la pureza del blockchain es vulnerabilidad de mayor riesgo y cuya atención es más urgente por los problemas que podría generar a la dignidad de terceros, especialmente niños, en segundo lugar la necesidad de construir alternativas energéticas que garanticen una minería amigable con el ambiente, limpia y una mayor participación de las autoridades respecto a las delincuencias tradicionales (como la estafa e intermediación financiera ilegal) que cunden alrededor de las monedas electrónicas.

Respecto a nuestra preocupación por la desnaturalización del sistema por la emisión de monedas electrónicas por parte de Estados soberanos, la decisión será ideológica en el fuero de las convicciones de quienes las adopten o rechacen, sin embargo la aceptación masiva sí podría marcar el inicio del final para la tradición descentralizada de respaldo civil.

Finalmente, si el sistema no lograra sobrevivir a mediano o largo plazo y quedamos anclados a monedas tradicionales o digitales emitidas por gobiernos, el impulso de la tecnología blockchain como disrupción tecnológica apenas inicia y posiblemente sea cada día más utilizado para generar confianza en las relaciones comerciales de una sociedad más transparente.

BIBLIOGRAFÍA

Córdoba, J. (2014). *Análisis jurídico, en particular de la normativa penal vigente, sobre la comisión de delitos tradicionales o informáticos cuyo fin sea la obtención de un beneficio patrimonial antijurídico por medio de moneda electrónica sin respaldo de banca central, mención especial bitcoin, del año 2001 al 2013*. Trabajo final de licenciatura en derecho. Universidad Fidélitas, Costa Rica.

Nakamoto, S. (2009). *Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario*. Recuperado 28 de abril de 2021, de elbitcoin.org website: https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

Reyes, D. *Sistemas de contrato comercial multinivel y sistemas piramidales de defraudación. Contrastes.* Tesis de Licenciatura en Derecho, Facultad de Derecho. Universidad de Costa Rica. San José, Costa Rica. 2019.

Gutiérrez, P. *et al* (2018). *Banca Comercial tradicional y los nuevos actores del mercado, Fintech, analizando el pasado, presente y diferentes estimaciones sobre el futuro del sector.* Trabajo de Fin de Máster Universitario en Instituciones y Mercados Financieros. CUNEF Universidad, España. Recuperado de: https://biblioteca.cunef.edu/files/documentos/TFM_MUIMF_2018-11.pdf

Castro, J. (2021). ¿Cuántas criptomonedas existen en el mundo además del Bitcoin?. Recuperado 29 de abril de 2021, de La República website: https://www.larepublica.net/noticia/cuantas-criptomonedas-existen-el-mundo-ademas-del-bitcoin

Vanci, M. (2020). *Altcoin o shitcoin ¿qué fue primero en las criptomonedas?. Recuperado 29 de abril de 2021,* de Criptonoticias website: https://www.larepublica.net/noticia/cuantas-criptomonedas-existen-el-mundo-ademas-del-bitcoin

Córdoba, J. (2018). *Conferencia sobre monedas electrónicas en el Simposio Internacional de Derecho Informático.* Recuperado 29 de abril de 2021, de Colegio de Abogados y Abogadas de Costa Rica website: https://www.youtube.com/watch?v=jyU3a7kdvsU

Cripnoticias (sf). *Qué son las Ofertas Iniciales de Monedas (ICO).* Recuperado 29 de abril de 2021, de Criptonoticias website: https://www.criptonoticias.com/criptopedia/que-son-ofertas-iniciales-criptomonedas-ico-tokens-ethereum/

Navarro, B. (2017) *Blockchain y sus aplicaciones.* Recuperado el 29 de abril de 2021, de JeuAzarru website: http://jeuazarru.com/wp-content/uploads/2017/11/Blockchain.pdf

Astray, M. C. (2019). *Bitcoin¿ Oportunidad del siglo o burbuja especulativa?*. Trabajo Trabajo de Grado en Derecho. Universidad Pontificia de Comillas, España. Recuperado el 29 de abril de 2020 de Universidad Pontificia de Comillas, website: : https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/27752/TFG-%20Astray%20RodrAguez%2c%20MarAa%20Cristina.pdf?sequence=1&isAllowed=y

Segesdi, L. (2019). *Monedas sociales. Aproximaciones a algunas experiencias con diversas tecnologías y motivaciones, desde el papel a las criptomonedas para la promoción de mercados de proximidad y generación de comunidad*. Recuperado el 30 de abril de Academia, website: https://d1wqtxts1xzle7.cloudfront.net/60625113/Monedas_sociales._aproximaciones_a_algunas_experiencias_con_diversas_tecnologias20190917-105009-

rw1uxt.pdf?1568740746=&response-content-disposition=inline%3B+filename%3DMonedas_sociales_aproximaciones_a_alguna.pdf&Expires=1619830401&Signature=RjYRG-GoOcq2NeDV~BY5xmU9OiwVA~A1ZlQvdi0vVySjfTkr-x~meBXH5r8TnH0~qsKz7kHhDoxVm7UG5qlQZ0c8X-b~piP37cXAUwNhWghUnVwXrZ2-1nGVmUK39wBlKJDz7EeQ3kPzjG5LLeL6GxQ0KpZgKXI2mhL8joI~-eZYqYWI~WAgRJ1jGYP8BO0vpEBBeZxIxPrGEDrxIxBHKSJWeiBxxa8xCc43zKp1LVc11elBOAq2-my7~tbjz84T4pU1qtZXP0-qf4nYcdb5EARGhKTZnVA~XbGyBrwi5VWVw5r1rB6Z~yyVHPoW~tEln-B3qKkHcKav52fzYB~xDw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Clementín, F. (2021). *Capital china pone el ojo en las granjas de minería de bitcoin por su consumo eléctrico*. Recuperado el 30 de abril de 2021 de Criptonoticias, website https://www.criptonoticias.com/mineria/capital-china-pone-ojo-granjas-mineria-bitcoin-consumo-electrico/

Infobae (2021) *La criptominería consume más energía eléctrica que Holanda y cada vez preocupan más sus altas emisiones de carbono*. Recuperado el 30 de abril de 2021 de Infobae, website. https://www.infobae.com/america/medio-ambiente/2021/04/22/la-criptomineria-consume-mas-energia-electrica-que-holanda-y-cada-vez-preocupan-mas-sus-altas-emisiones-de-carbono/

Cárdenas, Z. J. P., Avellaneda, M. A. V., & Bermúdez, G. M. T. (2015). *Bitcoin como alternativa transversal de intercambio monetario en la economía digital*. Universidad Distrital Francisco José de Caldas, Bogotá, recuperado el 30 de abril de 2021, website https://revistas.udistrital.edu.co/index.php/REDES/article/view/8617/10531

La Información. (2021). *La crítica de Bill Gates a las inversiones en Bitcoin: «Deberías tener cuidado»*. Recuperado el 30 de abril de 2021 de La Información, website https://www.lainformacion.com/management/critica-bill-gates-bitcoin-inversiones/2830723/

Dierckxsens, W., & Formento, W. (2018). *El bitcoin en la geopolítica*. Recuperado el 30 de abril de 2021 del Departamento Ecuménico de Investigaciones, Chile, website http://www.deicr.org/IMG/pdf/el_bitcoin_en_la_geopolitica_wim_walter_20_de_enero.pdf

Ventura, V. (2021, 18 febrero). *El «anti-bitcoin»: China avanza en las pruebas del «eYuan», una criptomoneda para aumentar el control sobre los ciudadanos*. Recuperado el 30 de abril de 2021, de El Economista, website https://www.eleconomista.es/divisas/noticias/11058557/02/21/El-antibitcoin-China-avanza-en-las-pruebas-del-eYuan-una-criptomoneda-para-aumentar-el-control-sobre-los-ciudadanos.html

Fortuño, M. (2021). Las criptomonedas como algo más que inversión: China planea su uso generalizado. Recuperado el 30 de abril de 2021 de El Blog Salmón, website https://www.elblogsalmon.com/productos-financieros/criptomonedas-como-algo-que-inversion-china-planea-su-uso-generalizado

McFarland, C., Hux, T., Wuehler, E., & Campbell, S. (2018,). Informe sobre amenazas contra blockchain. Recuperado el 30 de abril de 2021 de McAfee, website https://www.mcafee.com/enterprise/es-es/assets/reports/rp-blockchain-security-risks.pdf

Ibáñez Jiménez, J. W. (2016). *Blockchain,¿ el nuevo notario?.* Recuperado el 30 de abril de 2021 de La Universidad Pontificia de Comillas, España, website https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/14564/Blockchain_el_nuevo_notario.pdf?s

Aribau, Ó. (2018). *Las TIC y la cibersoberanía en China: la base del presidente Xi Jinping para perfeccionar el control social maoísta*. Recuperado el 1º de mayo de 2021 de la Universidad Oberta de Cataluña, España, website http://openaccess.uoc.edu/webapps/o2/bitstream/10609/83827/6/oaribauTFM0618memoria.pdf

European Central Bank. (2021, 14 abril). *El BCE publica los resultados de la consulta pública sobre un euro digital*. Recuperado el 2 de mayo del Banco Central Europeo, Alemania, website 2021https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414%7Eca3013c852.es.html

Nieves, V. (2020). ¿Qué es el euro digital y por qué quiere introducirlo ahora el BCE?. Recuperado el 2 de mayo de 2021 El Economista, website https://www.eleconomista.es/economia/noticias/10838221/10/20/Que-es-el-euro-digital-y-por-que-quiere-introducirlo-ahora-el-BCE.html

JOSÉ ADALID MEDRANO

- Abogado especialista en derecho informático
- Conferencista internacional, consultor y capacitador sobre ciberdelincuencia y protección de datos personales.
- Coordinador de la Comisión de Innovación regulatoria.
- Miembro fundador de la Comisión de Derecho Informático del Colegio de Abogados y Abogadas.
- Miembro de la comisión de asuntos jurídicos de la ONG internacional sobre ciberseguridad, Fundación Capa Ocho, con sede en Argentina.
- adalid@ciberjuristas.com

4



José Adalid Medrano

Abogado especialista en derecho informático
Conferencista internacional, consultor y capacitador sobre ciberdelincuencia y protección de datos personales.
Coordinador de la Comisión de Innovación regulatoria.
Miembro fundador de la Comisión de Derecho Informático del Colegio de Abogados y Abogadas.
Miembro de la comisión de asuntos jurídicos de la ONG internacional sobre ciberseguridad, Fundación Capa Ocho**,** con sede en Argentina.
Correo: adalid@ciberjuristas.com

El delito de violación de datos personales.

RESUMEN:

La violación de datos personales es un tipo penal que tutela el derecho de autodeterminación informativa tanto de personas físicas como de las jurídicas y representa una serie de conductas que realizan los grupos cibercriminales para la comisión de distintos delitos tradicionales e informáticos.

La ciberdelincuencia se dirige a una modalidad de operación que afectará cada vez más bienes jurídicos de una manera acelerada y con gran impacto.

En la presente investigación se ha encontrado que España, Ecuador, Colombia y Costa Rica tutelan de forma expresa el derecho de autodeterminación informativa en sus códigos penales.

Palabras clave: delitos informáticos, ciberdelitos, datos personales, violación de datos personales, autodeterminación informativa, protección de datos personales, ciberdelincuencia, cibercrimen.

ABSTRACT:

The violation of personal data is a type of crime that protects the right to informational self-determination of natural and legal persons and represents a series of conducts carried out by cybercriminal groups for the commission of different traditional and computer crimes.

Cybercrime is aimed at a way of operation that will increasingly affect almost every legal assets in an accelerated manner and with great impact.

This research has found that Spain, Ecuador, Colombia and Costa Rica expressly protect the right to informational self-determination in their criminal codes.

Keywords: computer crime, cybercrime, personal data, personal data breach, informational self-determination, personal data protection, cybercrime.

I. Introducción.

La sociedad costarricense del siglo XXI se encuentra en una transición entre el uso intensivo de la tecnología propiciado por la constante reducción de la brecha digital -acelerada por la pandemia Covid-19- y la cada vez más cercana ubicuidad tecnológica a la que nos dirige la cuarta revolución industrial, en donde el concepto de privacidad, construido con base a paradigmas de siglos pasados, está siendo desafiado por la constante recopilación de datos personales.

Con el uso intensivo de medios sociales y el aumento de sensores y cámaras de vigilancia -inclusive con reconocimiento facial- que rastrean el paso por las vías físicas y electrónicas de los usuarios, muchas personas se cuestionan si ya hemos renunciado a la privacidad, en favor del crecimiento económico y tecnológico, o si todavía hay tiempo de cambiar el camino.

La duda es importante porque las empresas tecnológicas e inclusive los gobiernos dependen, cada vez más, de la recopilación y análisis de los datos de los ciudadanos para un mejor ejercicio de sus actividades. El problema deriva en que con este tipo de vigilancia se generan cantidades ingentes de

información, que sin una regulación y controles adecuados puede debilitar los cimientos de cualquier democracia.

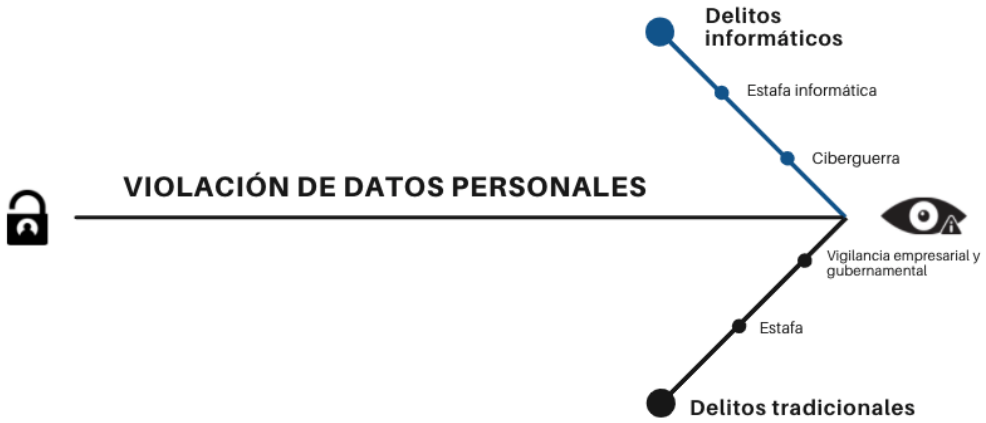


FIgura 1. La violación de datos personales favorece la comisión de distintos tipos de delitos. [Elaboración propia]

Casos recientes, a nivel nacional e internacional, como UPAD y Cambridge Analytica, generan interesantes debates regulatorios sobre cuál es la mejor manera de combatir la violación de la privacidad y en dónde debemos establecer los límites de protección, tomando en cuenta que estas acciones contra los datos personales potencia la comisión de otros delitos.

En Costa Rica, desde el año 2012[1] sancionamos penalmente la violación de los datos personales, mientras en Estados Unidos -que es el país donde residen la mayoría de empresas tecnológicas cuyos servicios usamos- el comercio de los

1 Delito de violación de datos personales, incluido en el Código Penal costarricense a través de la Ley № 9048.

datos personales de los consumidores, inclusive sin su consentimiento[2], es una práctica permitida. A pesar de lo anterior, estamos lejos de ser una autoridad en esta materia, ya que a pesar de la estricta regulación, es claro el comercio ilegal de datos personales en nuestro país se hace a vista y paciencia de todos, lo que alimenta el cibercrimen organizado local de estafas informáticas y tradicionales.

Como parte del análisis que debe realizarse de manera frecuente sobre normativa que involucre las TIC en la presente investigación analizaremos el tipo penal costarricense, así como su regulación en el derecho comparado, con el fin de analizar si requiere reformas y propuestas de *lege ferenda.*

II. La ciberdelincuencia costarricense.

La ciberdelincuencia es la actividad delictiva que tiene como eje central la utilización de medios electrónicos con el objetivo de vulnerar bienes jurídicos tutelados penalmente. En la lucha contra la ciberdelincuencia se debe tener presente que nos encontramos ante un fenómeno transfronterizo de elevada complejidad, donde los grupos criminales no son homogéneos y se dedican a diferentes acciones delictivas que impactan a la sociedad de distintas maneras, por lo que es imperativo crear una estrategia nacional que permita establecer un norte a las autoridades.

Lo anterior es necesario, ya que el nivel de impunidad con el que operan las bandas locales de estafadores cibernéticos es tan grande que requiere que en

2 En los Estados Unidos el comercio de datos personales por parte de “data brokers” es parte de la dinámica del desarrollo comercial de las empresas tecnológicas quienes utilizan esta información como objeto de comercio el cual tiene un valor. A los usuarios se les permite “optar por que sus datos no se vendan a terceros, pero no les permite elegir el que sus datos se recopilen y usen en primer lugar” (Dean, 2020)

la sociedad costarricense cada parte asuma su responsabilidad y colabore para detener este flagelo que erosiona la confianza en el sistema financiero nacional, al mismo tiempo que genera un gran daño en la ciudadanía. Lo más grave de la situación es que mientras estamos siendo derrotados por los cibercriminales locales, la ciberdelincuencia internacional no solo atenta contra empresas, organizaciones o individuos, sino que también dirige sus ojos hacia los gobiernos. Los ataques contra distintas naciones son parte de una estrategia delictiva de muchos gobiernos atacantes, quienes utilizan el ciberespacio para espiar a sus rivales y/o desestabilizarles, por lo que la capacidad de daño que tienen las acciones delictivas informáticas son ilimitadas.

Sin importar el área de acción de las bandas criminales o su ubicación geográfica, todas se alimentan de la información de carácter personal, ya sea para crear perfiles de sus víctimas para ataques posteriores o para utilizarla de forma directa en contra de estas, por lo que toda política criminal que busque mitigar el impacto de la ciberdelincuencia debe sancionar penalmente diferentes acciones informáticas que buscan violar la privacidad ciudadana.

Los datos personales de los costarricenses no solo son violentados por grupos organizados, o ciberdelincuentes especializados, sino que también por personas con pocos conocimientos en informática, pero que se encuentran en sus grupos sociales más cercanos, por lo que es habitual que en esos espacios - como el hogar, trabajo o inclusive en un comercio de confianza - se comentan delitos informáticos, sin que la víctima tenga la menor sospecha.

Con el fin de combatir la ciberdelincuencia nuestro país ha promulgado distintas leyes con el fin de sancionar penalmente los delitos informáticos, las cuales han venido a robustecer el derecho penal sustantivo, al contener tipos penales novedosos que sancionan las acciones digitales ilícitas más utilizadas por los

ciberdelincuentes modernos. Lo anterior, aunque le permite a las autoridades judiciales saltar el obstáculo de la atipicidad -motor de la impunidad- no les resulta suficiente ya que no se les ha dotado de normas procesales y herramientas aptas para los retos que conllevan los entornos digitales y de una capacitación robusta que les permita enfrentar este flagelo de la mejor manera.

a. Delitos informáticos.

La informática ha generado una transformación sin precedentes en la humanidad, marcada por una 'Ley de Moore'[3] que funge como un derrotero de crecimiento exponencial que se ha venido cumpliendo en las últimas décadas, llevando a la sociedad a experimentar cambios de forma continua, sin descanso y sin un espacio para una profundo debate regulatorio sobre cómo debería el derecho intervenir.

En ese sentido, al estudiar la ciberdelincuencia, es importante tomar en cuenta que el medio electrónico es un agente óptimo, potente y pluriofensivo de bienes jurídicos, con resultados que son difíciles de prever a nivel legislativo, por lo que históricamente muchas de las conductas cometidas por medios informáticos han resultado atípicas, lo que ha generado una necesidad urgente de sancionar penalmente conductas novedosas que tutelan bienes jurídicos vinculados con la informática, en un proceso circular que va de la mano con el desarrollo tecnológico.

A finales del siglo pasado, era todavía común el debate sobre si era necesario incluir en el Código Penal los delitos informáticos, porque algunos autores

[3] Se conoce como Ley de Moore a la predicción que hizo Gordon Moore, cofundador de Intel, en 1965 respecto del aumento de la cantidad de transistores en los procesadores. En aquel entonces dijo que el número se duplicaría cada año. Luego, en 1975, redefinió este concepto y explicó que este aumento ocurriría cada dos años. (Jaimovich, 2019)

sostenían que simplemente eran nuevas formas de lesionar bienes jurídicos tradicionales, por lo que no había necesidad de tener legislación especial. Lo anterior se afirmaba sin tomar en cuenta el principio de legalidad, la prohibición de la interpretación analógica y la regla de interpretación restrictiva que rigen en materia penal, por lo que aunque este debate se encuentra superado, lo cierto es que sigue vigente que la comunidad jurídica debe mejorar en la comprensión de las acciones delictivas informáticas, que son la base de las operaciones de la ciberdelincuencia, la cual tiene un impacto transversal en todos los sectores de la sociedad.

El aumento de la calidad del debate regulatorio vinculado con esta materia permitirá avanzar hacia la construcción de una política criminal eficiente y moderna, que en respeto del principio de mínima intervención penal, permita combatir este flagelo sin poner en riesgo las bases de un Estado democrático de derecho.

Es importante tomar en cuenta que toda nueva regulación vinculada con las TIC, principalmente la relacionada con la función punitiva estatal, puede no solo servir para la protección de derechos fundamentales, sino que también para lesionarlos. Lo anterior, ya que como músculos que permiten el ejercicio de derechos fundamentales, los medios electrónicos al regularse, pueden potenciarse o atrofiarse, por lo que hay que tener precisión quirúrgica al diseñar legislación relacionada con la informática, para no generar un impacto negativo en el desarrollo democrático y/o económico que se encuentra estrechamente vinculado con el de índole tecnológico.

b. Primeras reformas sobre delitos informáticos.

En Costa Rica, en el mes de agosto de 1999 se promulgaron dos leyes que incluían en nuestro ordenamiento jurídico a los delitos informáticos, una como reforma al Código Penal sobre la pornografía infantil[4] y otra vinculada con la protección de los sistemas de información y bases de datos tributarias. Como dato anecdótico, de lo que son los cambios culturales entre la Costa Rica de este siglo y finales del anterior, es que solo dos años antes que se decidiera sancionar penalmente la difusión de la pornografía infantil en el país, el diario La Nación incluyó una noticia que vertía una crítica camuflada de un ciudadano estadounidense hacia la decisión de un juez de retirar de circulación, en Oklahoma, la película *El Tambor Escarlata* que contenía escenas de un menor de edad sosteniendo relaciones sexuales orales con una joven:

"Nadie discute que la pornografía infantil es condenable, pero no podemos dejar las decisiones culturales a gente que pondría una hoja de higuera en una estatua de Miguel Angel", consideró Michael Salem, abogado de la Asociación de EE.UU. para las Libertades Civiles" (La Nación, 1997).

En aquellos tiempos nos conectábamos a internet principalmente por un modem que utilizaba la línea telefónica como medio de conexión, por lo que descargar cualquier contenido se hacía eterno y caro. En aquel tiempo RACSA, aprovechando su monopolio nos cobraba "$30 por 30 horas de uso más un dólar por cada hora adicional" (La Nación, 1999), mientras en Estados Unidos ya se cobraba tarifa plana. Por lo anterior, era claro que en aquellos tiempos la velocidad de propagación de contenidos era menor, por lo que todavía no había conciencia del daño que podría generar la compartición masiva de un contenido audiovisual, ya que su consumo se hacía principalmente en VHS -que alquilábamos en un videoclub- y no como en el presente a través de Netflix,

[4] La ley №7899 del 3 de agosto de 1999, incluyó en nuestro Código Penal los delitos de fabricación y difusión de material pornográfico infantil, acciones que no son necesariamente deben desarrollarse por medios informáticos.

Youtube, Tik Tok o distintos medios sociales, donde en pocas horas se pueden alcanzar millones de reproducciones.

En el año 2001, a través del proyecto de ley №8148, se adicionaron al Código Penal 3 tipos penales informáticos:

a) 196 bis. Violación de las comunicaciones electrónicas. Penas de seis meses a dos años.
b) 217 bis. Fraude informático. Penas de uno a diez años.
c) 229 Bis. Alteración de datos y sabotaje informático. Penas de uno a cuatro años.

De acuerdo con Chinchilla (2002) en su libro Delitos Informáticos, esta reforma vino motivada por un proyecto que presentó la Procuraduría General de la República, el cual fue determinante para incorporar las novedosas tres figuras penales y señala que lamentablemente quedó fuera el hurto agravado mediante la utilización de tarjetas magnéticas o perforadas. En otras palabras, esta reforma, aunque novedosa para la época, quedó debiendo.

c. Definición de delito informático.

Debido al avance que han tenido en la última década los delitos informáticos, su naturaleza pluriofensiva de bienes jurídicos y la diversidad de los sujetos involucrados, la labor de definirle es altamente compleja. En esta tarea, no se puede caer en el error de usar definiciones tan restringidas que limiten el objeto de estudio, ni tan amplias que pierdan todo sentido práctico.

1. Delitos informáticos en *stricto sensu*

En sentido restringido, nos permitimos definirlo como toda aquella acción delictiva informática dirigida a vulnerar la confidencialidad, integridad, disponibilidad y/o normal funcionamiento de los sistemas informáticos, así como toda aquella dirigida contra la autodeterminación informativa y la identidad en medios electrónicos.

Esta es una definición de índole purista, al incluir únicamente los tipos penales informáticos que cuentan con verbos rectores de naturaleza informática, y que nacieron con el fin de tutelar bienes jurídicos relacionados con la tecnología.

Se es consciente que este concepto deja por fuera a todas aquellas acciones donde el medio informático es solo la herramienta a través de la cual se realiza un delito tradicional, sin embargo, su utilidad conceptual reside en la necesidad de un análisis jurídico de la ola de nuevos tipos de delincuencia que aparecieron con la creciente adopción de la informática por parte de la población.

2. Delitos informáticos en *lato sensu*

Parece claro que el enfoque restrictivo permite el estudio del núcleo de las acciones que suelen desplegarse por parte de los grupos delictivos, con el fin de conseguir sus diversos objetivos criminales, pero la naturaleza híbrida y pluriofensiva de las ciberdelincuencia organizada moderna, cuyo marco de acción es tan amplio que genera un impacto en los principales intereses de la sociedad del Siglo XXI, lo que hace imperativo adoptar una definición que no restrinja el estudio de este fenómeno cambiente y resiliente.

Por ende, en sentido amplio nos permitimos definir al delito informático como toda aquella acción delictiva que se desarrolla especialmente por medios informáticos. Este concepto, nos permite incorporar el estudio de ciertas

modalidades de delitos tradicionales, en las cuales el elemento informático es protagónico y que son parte de la ciberdelincuencia moderna.

Una modalidad delictiva que nos permite ilustrar lo anterior, es la 'sextorsión', en la cual los ciberdelincuentes por medio de la seducción, usualmente a través de la utilización de identidades falsas[5], establecen comunicaciones de contenido sexual o erótico con sus víctimas, para obtener fotografías o videos íntimos, con el fin último de amenazarles con la difusión del material íntimo sino le pagan un monto económico. En este caso nos encontramos ante una modalidad de extorsión simple que:

a) Se despliega principalmente en el ciberespacio.
b) Involucra el tratamiento ilegal de datos personales.
c) Amenaza de/y/o difusión de documentos electrónicos de índole privada.
d) Es una figura explotada por el cibercrimen organizado[6].

Por otro lado, el *ransomware*[7] es una modalidad de extorsión calificada, la cual es potenciada por la tecnología y que está siendo utilizada de forma

5 Una identidad falsa es toda aquella utilizada con fines fraudulentos o de engaño, al no corresponder con la identidad real del individuo.

6 "Cientos de miles de hombres de todo el mundo caen víctimas cada año de un crimen en internet llamado "sextorsión". Primero los hombres son atraídos y tentados a participar en chats sexualmente explícitos con cámara web, y después son chantajeados: o pagan o hacen públicos los videos. Los extorsionistas son grupos organizados que operan desde diferentes países, como Filipinas. (BBC Mundo, 2014)

7 Definición del programa informático malicioso tipo 'ransomware': El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos (Instituto Nacional de Ciberseguridad, 2017, p. 31)

agresiva[8] por grupos cibercriminales, la cual consiste en la utilización de un programa informático malicioso con el fin de 'secuestrar'[9] la información contenida en un ordenador, como medio de presión para obtener un lucro a cambio de devolverle el acceso a la víctima de su información. Adicionalmente, algunos grupos recurren a la modalidad de doble extorsión, que consiste en extraer bases de datos personales de clientes y/o información confidencial de sus víctimas, antes de cifrarla[10], incrementando así la presión extorsiva, ya que si el cliente no cumple las demandas de los extorsionistas[11] -que suele pedirse a través de criptomoneda[12]- los delincuentes no solo no brindarán las claves, para descifrar la información, sino también publicarán las bases de datos con información sensible, generando un daño grave tanto a la reputación de la empresa, como a la privacidad de ciudadanos.

---

[8] Si se compara con los datos de 2019, los ataques de ransomware a nivel global crecieron un 485% en 2020, según el análisis que ha hecho Bitdefender de la la evolución de las ciberamenazas más importantes. (IT Digital Security, 2021)

[9] Los delincuentes lo que realizan es un cifrado de la información, para que no esté disponible para el titular, salvo que pague el rescate. Podríamos decir que la información se encuentra "secuestrada" en el propio equipo de la víctima.

[10] Los delincuentes cifran la información con fines delictivos, sin embargo, es una operación que puede realizarse con fines de proteger la privacidad de la información. El concepto de cifrado o algoritmos de cifrado es el siguiente:

Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida. Existen dos tipos de cifrado atendiendo a las características de las claves de cifrado, estos son el cifrado simétrico y cifrado asimétrico. (Instituto Nacional de Ciberseguridad, 2017, p. 31)

11 En nuestro país, el caso más emblemático que se ha dado de ransomware es el caso del Banco de Costa Rica, en donde el grupo cibercriminal Maze amenazó con publicar la base de datos con información de los clientes del banco sino se realizaba el pago que ellos pedían. Los delincuentes cumplieron parcialmente su amenaza y publicaron alguna de la información prometida, lo que deja dudas sobre si, en primer lugar, la tenían completa.

[12] La criptomoneda o criptodivisa es un tipo de moneda digital que utiliza la criptografía para proporcionar un sistema de pagos seguro. Estas técnicas de cifrado sirven para regular la generación de unidades monetarias y verificar la transferencia de fondos. No necesitan de un banco central u otra institución que las controle. Las criptomonedas son un tipo de moneda digital, que son aquellas que no existen de forma física, pero que sirven como moneda de intercambio, permitiendo transacciones instantáneas a través de Internet y sin importar las fronteras. (Criptomoneda - qué es, definición y concepto , 2017)

Por lo anterior, no podríamos imaginarnos estudiar los delitos informáticos sin incluir estas nuevas modalidades delictivas. Como puede verse, nos dirigímos a un momento donde un gran porcentaje de delitos que se encuentra en el Código Penal podrían tener una modalidad informática, que sin duda podría estudiarse dentro de lo que conocemos como delincuencia informática.

El lector podría sorprenderse con que, en las próximas décadas, lo que los ciberdelincuentes ataquen, ya no solo sean los sistemas informáticos como los conocemos ahora, sino que también a los seres humanos cuyo sistema incorpote elementos informáticos, como algún chip[13] que potencie su rendimiento. Un ataque informático de esta índole podría atentar de forma directa contra la vida[14], los sentidos y/o alguna función biológica del ser humano (e inclusive de animales), de forma permanente o temporal, lo que cambiará la percepción que tendrá la sociedad sobre la ciberdelincuencia[15].

Por lo anterior, con el avance hacia el transhumanismo[16] de darse un debate regulatorio sano sobre la tutela penal especial en esta materia, la cual podría inclusive resultar extensiva a animales, que con ayuda de la tecnología puedan

[13] La definición de chip es "Pequeña pieza de material semiconductor que contiene múltiples circuitos integrados con los que se realizan numerosas funciones en computadoras y dispositivos electrónicos. (RAE, 2021)

[14] Aunque se pueda ver como un análisis de ciencia ficción lo cierto es que dispositivos médicos como los marcapasos están siendo ya objetivo por parte de los ciberdelincuentes. En este sentido un reportaje de la ABC nos alerta:
"Para los pacientes con desfibiriladores implantables, es posible que los hackers interrumpan las comunicaciones inalámbricas, lo que inhibe el valor de la telemonitorización y permite que el sistema no detecte ningún evento clínicamente relevante. La sobredetección puede inhibir la estimulación o dar lugar a descargas inapropiadas o potencialmente mortales." (ABC, 2018)

[15] En este sentido, en nuestro Código Penal, en el artículo 232 que sanciona la instalación y propagación de programas informáticos maliciosos, contiene un agravante en el caso que se ataque un sistema informático de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.

[16] "El transhumano es el ser humano mejorado física, cognitiva, moral o emocionalmente por medio de la tecnología" (Ethic, 2017).

comunicarse de forma fluida con nosotros. El anterior, sin lugar a dudas, es un tema controversial que nos saca de la zona de confort y cuyo análisis requiere de profesionales en derecho que comprendan el entorno tecnológico y el científico.

d. Características de los delitos informáticos.

Para Chinchilla (2002), estos delitos poseen peculiaridades que les hacen de alguna manera *sui generis*, por una parte, en cuanto a su forma de comisión y, por otra, respecto a su detección. El autor cita 3 siguientes características de los delitos informáticos, que consideramos vigentes hasta la actualidad:

a) Rapidez (en tiempo) y acercamiento (en espacio): las acciones delictivas a través de medios informáticos permiten una rapidez sin precedentes y pueden inclusive realizarse desde lugares a miles de kilómetros de distancia del lugar donde se producen los efectos. Lo que es particularmente peligroso, en la actualidad, cuando se atacan infraestructuras críticas de las naciones y cuyo riesgo aumentará con la implementación de las redes 5G.

b) Facilidad para encubrir el hecho: Los delincuentes pueden hacer parecer que su procedencia es de un lugar distinto al real o pueden programar rutinas que dificulten la detección de sus acciones. Adicionalmente, podríamos agregar que actualmente el anonimato forma parte de las ventajas con las que cuenta el ciberdelincuente, por lo que resulta dificil vincular sus acciones con su identidad real.

c) Facilidad de borrar las pruebas: aunque similar a la anterior, en casos donde la actividad delictiva ha cesado, la facilidad con la que se pueden borrar

las pruebas representa un reto enorme para las fuerzas del orden.

e. El Sujeto activo

Con la reducción de la brecha digital y el amplio catálogo de acciones delictivas que se encuentran en nuestro Código Penal nos permite concluir que cualquiera puede ser un ciberdelincuente y víctima de un delito informático.

A pesar de la afirmación anterior, para fines de comprensión, sin pretender abarcar todos los tipos de actores que hay, se puede limitar a los sujetos activos en dos categorías no excluyentes:

a) **Caza-vulnerabilidades:** este tipo agente se encuentra en constante búsqueda de errores en los sistemas informáticos que puedan facilitarle la comisión de actos delictivos. Al encontrar vulnerabilidades, puede venderlas y/o crear herramientas que automaticen su explotación, con las cuales pueden lucrar o ponerlas a disposición del público de forma gratuita[17].

   Este tipo de delincuente es especializado, puede trabajar de forma individual, para un Estado atacante o cualquier otro tipo de organización criminal.

b) **Usuarios de herramientas:** ya sean herramientas tecnológicas dirigidas especialmente para la comisión de actividades delictivas o que son abusadas para distintos fines. En esta clase de categoría encontramos a todo usuario que, aunque no contara con conocimientos especializados

[17] Importante destacar que hay *hackers* éticos que también se dedican a detectar vulnerabilidades y las reportan de forma responsable a los desarrolladores.

sobre informática, puede utilizar estas herramientas que automatizan la comisión de los abusos informáticos.

f. Delitos informáticos contra la privacidad.

Como hemos comentado, este tipo de delitos tienen una naturaleza pluriofensiva de bienes jurídicos y es difícil imaginar acciones desplegadas por la ciberdelincuencia, en la actualidad, que no lesionen de forma directa o indirecta la privacidad de sus víctimas, como lo es el caso de la compra y venta de bases de datos personales.

A manera de ejemplo, en las estafas informáticas que se dan de forma tan frecuente en Costa Rica, como *conditio sine qua non* para iniciar con el 'vishing'[18] el estafador debe haber obtenido, de cualquier vía, alguna base de datos con información de sus víctimas. De la misma manera, cuando obtiene las credenciales necesarias para ingresar en la cuenta de la víctima para realizar las transfreencias ilegales, el actor logra acceder información sensible de su víctima porque en la banca electrónica se encuentran todos los datos de hábitos de consumo del cliente del sistema financiero[19].

IV. El delito de violación de datos personales. (Artículo 196 bis)

[18] Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta. (INCIBE, 2017). Cuando la misma se realiza a través de la utilización de llamadas utilizando la voz, se denomina '**vishing'.**

[19] Estos datos se reconocen como sensibles en nuestra legislación de protección de datos personales, al ser de carácter socioeconómico.

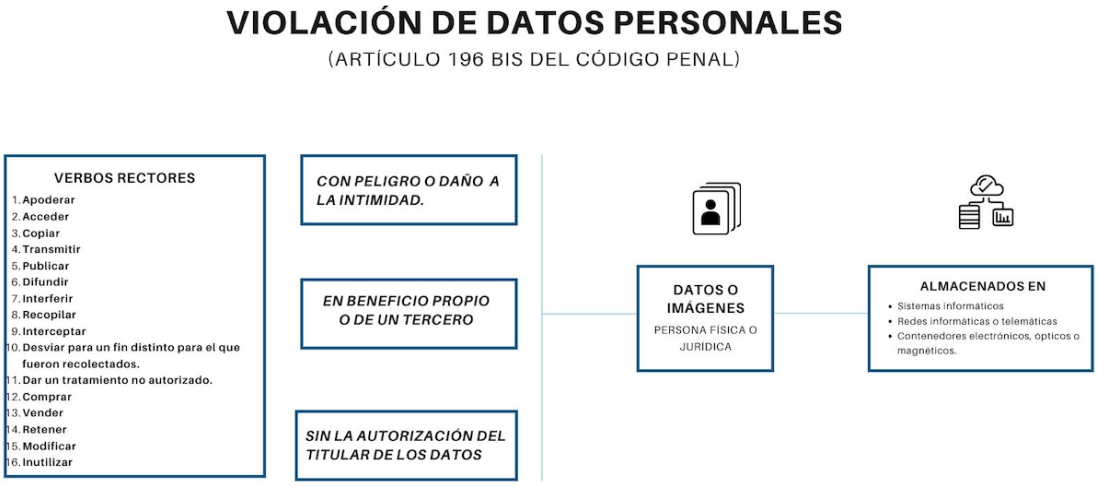


Figura 2. Elaboración propia

En la reforma al Código Penal de la sección VIII, denominada *Delitos Informáticos y Conexos*, del título VII, a través de la ley № 9048, se incorporó la violación de datos personales, cuyo fin es proteger a los datos personales de su tráfico ilegal.

Este comercio ilegal de datos es piedra angular de distintas acciones delictivas del cibercrimen, por lo que los ataques informáticos más frecuentes, a nivel mundial, están vinculados de forma directa o indirecta con el abuso de los datos personales, ya sean estos perpetrados por organizaciones criminales, individuos o Estados atacantes[20]. Debido a esto, el legislador costarricense, de manera acertada, incorpora este tipo penal inspirado en el Código Penal colombiano, que el año 2009, en su artículo 269F incluyó el delito de violación de datos personales con elementos bastante similares al nuestro, lo que para ambas naciones es un paso importante hacia el fortalecimiento de la protección de los

[20] El Estado atacante es toda aquella nación que forma parte de la llamada 'ciberguerra', realizando ataques a otras naciones con fines políticos o de información.

datos de los habitantes:

El artículo 196 bis del Código Penal costarricense en su primer párrafo reza:

> "Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores, electrónicos, ópticos o magnéticos."

El tipo penal puede sanciona cualquier tratamiento no autorizado por el titular que cumpla con los siguientes elementos:

1. En beneficio propio o de un tercero.
2. Con peligro o daño a la intimidad.
3. Datos, de persona física o jurídica, almacenados en sistemas informáticos**.**
4. Sin autorización del titular de los datos.

Bien jurídico tutelado.

La autodeterminación informativa sobre los datos electrónicos.

De acuerdo a la ley № 8968 y a diversas resoluciones de la Sala Constitucional, la autodeterminación informativa es un derecho fundamental derivado del derecho a la privacidad, que tiene toda persona sobre el flujo de informaciones

que conciernen a su persona, de acuerdo a las garantías y excepciones que contiene el ordenamiento jurídico, con el fin de evitar que se propicien acciones discriminatorias.

Es importante destacar que este tipo penal protege únicamente al dato personal que se encuentra alojado en soportes electrónicos, por lo que toda conducta ilegal realizada sobre datos en soportes físicos no es sancionable penalmente a través de este tipo penal. Aunque es discutible el porqué no se extendió la tutela penal a todos los datos, sin hacer distinción en cuanto al soporte en el que se encuentra almacenado, lo cierto es que la informática aumenta el riesgo y la potencia con la que se puede lesionar un bien jurídico, por lo que no puede negarse que la decisión o preocupación del legislador se encuentra fundamentada.

Por lo anterior, no resulta sorprendente, que el desarrollo de la informática generó en el continente europeo una serie de reformas vinculadas con este derecho que han influido de forma importante en nuestro país.

La primera ola de reformas legales surgió en el campo de la protección a la intimidad en los años setenta del siglo XX. Las nuevas tecnologías brindaban la posibilidad de formas de procesamiento, almacenamiento y transmisión de datos inexistentes hasta aquel momento. Datos relativos a las personas aparentemente insignificantes, sin comportar un riesgo a la intimidad personal en caso de encontrarse en manos de otros distintos a su titular, se convertían en una información valiosísima después de ser agrupados, tratados en forma conjunta, interrelacionados y analizados mediante los modernos medios tecnológicos. (Davara, 2017, p.47)

En ese sentido, la Constitución Española de 1978 reconoce el riesgo de la informática sobre la intimidad personal y otros derechos, por lo que ordena que mediante la ley esta debe limitarse, a través de su artículo 18.4 que reza de la siguiente manera:

La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. (Constitución de España, 1978)

En línea similar, veinte años después y de manera visionaria, la Sala Constitucional costarricense decide reconocer lo que llama el nuevo derecho de la intimidad en la sociedad informatizada.

Lo que hoy conocemos como "sociedad informatizada" plantea nuevos retos al concepto clásico del derecho a la intimidad. En la década de los ochenta y noventa, en nuestro país, la libertad individual, la personal y la colectiva, estaban relativamente lejos de la influencia de la tecnología. Así por ejemplo, el ciudadano no se cuestionaba con qué fin le eran solicitados sus datos personales, quienes tienen acceso a ellos con cual objeto. Consecuentemente, el derecho a la protección de la persona frente al procesamiento de sus datos personales es una cuestión que se deja sólo a la academia. Es pronto también para cuestionarse si la manipulación de los datos personales puede vaciar el contenido esencial de algunos de los derechos fundamentales. Menos aún se concibe que el desarrollo informativo pueda implicar alguna forma de violencia. En la actualidad, la doctrina nacional y extranjera, admite que la manipulación de la información posibilita el control sobre el ciudadano como una alternativa real y efectiva. De tal manera que los derechos individuales de los ciudadanos puedan quedar prácticamente sin contenido efectivo. Así ocurre, cuando se

desarrollan perfiles de las personas utilizando información aislada y aparentemente inofensiva.

La informática, no sólo representa uno de los más grandes avances del presente siglo, sino que pone en evidencia las posibilidades de inspección de la vida interior de las personas, desde este punto de vista, la personalidad de los ciudadanos y su fuero interno cada vez se hacen más trasparentes. Esta situación hace necesario que los derechos fundamentales amplíen también su esfera de protección. La esfera privada ya no e reduce al domicilio o a las comunicaciones, sino que es factible preguntarse si es comprensible incluir "la protección de la información" para **reconocerle al ciudadano una tutela a la intimidad que implique la posibilidad de controlar la información que lo pueda afectar. Lo expuesto, significa que el tratamiento electrónico de datos, como un presupuesto del desarrollo de nuestra actual sociedad democrática debe llevarse a cabo afianzando los derechos y garantías democráticas del ciudadano** (arts. 24, 22, 123, 2824, 3025, 3326 y 4127 de la Constitución). Es obvio, que el acceso a la información es un poderoso instrumento de progreso individual, y para el ejercicio de los derechos políticos y sociales. Pero también debe reconocerse que el progreso no significa que los ciudadanos deban quedar en situación de desventaja frente al Estado o a los particulares. El nuevo derecho a la intimidad, debe ponderar los intereses en conflicto, entre el legítimo interés de la sociedad a desarrollarse utilizando la información, como la también necesidad de tutelar a la persona frente al uso arbitrario de sus datos personales. **La tutela a la intimidad implica, la posibilidad real y efectiva para el ciudadano de saber cuáles datos suyos están siendo tratados, con qué fines, por cuáles personas, bajo qué circunstancias, para que pueda ejercer el control correspondiente sobre la información que se distribuye y que lo afecta** (arts. 24 de la

Constitución y 13 inciso 1, de la Convención Americana de Derechos Humanos)."[21] (Sala Constitucional, Resolución Nº 01345 - 1998).

Los datos personales en entornos informáticos.

La Sala Constitucional en su jurisprudencia ha manifestado que "la garantía del derecho fundamental no depende de la titularidad del medio sino que es independiente de la titularidad del soporte" (Sala Constitucional, N° 2005-15063), principio que es de alto interés en materia de derechos digitales, como el caso del derecho de protección de datos personales objeto de la presente investigación, donde el titular tiene el derecho de control sobre sus datos, sin importar cuál es el soporte en el que se encuentren alojados. En esa línea, desde que nacemos la ley y nuestros representantes legales dan licencia a terceros para el tratamiento de nuestros datos personales, labor la cual pueden realizar en entornos digitales ajenos a nuestro control, en apego a los fines para los que fueron recopilados y para los tratamientos que se encuentren debidamente autorizados.

Este tratamiento en entornos que no son de nuestra propiedad aumentan los riesgos de lesionar la privacidad y generar acciones discriminatorias, las cuales en casos de bases de datos públicas pueden darse de manera masiva[22].

La violación de datos personales (artículo 196 bis, CP) tutela los datos que se encuentren en:

[21] Las negritas contenidas en esta resolución no corresponden a su original.
[22] En Costa Rica se ha vuelto práctica común fisgonear la vida de otros ingresando al Registro Civil para conocer sobre las relaciones familiares que el Tribunal Supremo de Elecciones ha decidido que son de acceso irrestricto.

a) Contenedores electrónicos, ópticos o magnéticos: el legislador cuando realizó la reforma al Código Penal contenida en la ley № 9048 sobre delitos informáticos, decidió adoptar el concepto de contenedor como sinónimo de soporte[23] para este y otros tipos penales informáticos. No estamos de acuerdo con esta imprecisión, ya que a los materiales que contienen información no se les conoce a nivel técnico como contenedores y esto podría generar que conductas donde los datos violados se encuentren en dispositivos aislados de almacenamiento no puedan ser sancionadas penalmente por atípicas.

El concepto técnico y más preciso para referirse a los materiales que permiten el almacenamiento de información es el de soporte[24], los cuales pueden contar con capacidad de almacenamiento en formato electrónico[25]. Los soportes de información pueden ser magnéticos, ópticos, magneto-óptico, telemáticos, de estado sólido, biológicos[26], entre otros.

Sistema informático: "todo dispositivo[27] aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan en ejecución de un programa" (Convenio sobre la Ciberdelincuencia, artículo 1 inciso a)). Importante destacar, que todo sistema informático requiere de un soporte de almacenamiento para funcionar, ya que esto es parte de sus funciones.

---

[23] Este concepto fue el utilizado en el artículo 196 bis del Código Penal, llamado Violación de comunicaciones electrónicas, el cual fue incluido por la ley N° 8148 (2001) y fue reformada por la ley N° 9048 (2012).

[24] **Soporte**: Material en cuya superficie se registra información, como el papel, la cinta de video o el disco compacto. (RAE, 2021)

[26] Para soluciontar los problemas de memoria, Microsoft tiene previsto tener un sistema de almacenamiento de datos en ADN funcionando en unos pocos años. Microsoft tiene previsto tener un sistema de almacenamiento de datos en ADN funcionando en unos pocos años. Así lo han asegurado arquitectos informáticos de la compañía en MIT Technology Review, donde afirman que están desarrollando un dispositivo que reemplaza las unidades magnéticas por unidades biológicas para guardar información digital. (Arteaga, 2017)

[27] **Dispositivo**: Aparato, o elementos de un sistema, conectados para poder ser reconocidos por el sistema operativo cumpliendo determinadas reglas de configuración. (González, 2018, p.16).

Red informática: Conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos con la finalidad de compartir información y recursos en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el coste general de estas acciones. (González, 2018, p.50).

Sobre datos digitalizados.

El tipo penal requiere que al momento de realizar la acción contenida en el verbo típico se aplique sobre datos que se encuentren almacenados en sistemas informáticos o contenedores informáticos, por lo que si un dato se encuentra en soporte de papel y se digitaliza, este adquiere tutela penal al almacenarse en un sistema informático, aunque la acción de digitalización la realice el delincuente. A manera de ejemplo, si una persona compra bases de datos en papel y las digitaliza para difundirlas por internet, la difusión sí podría ser sancionada penalmente, más no la digitalización, la cual es un tratamiento no autorizado, el cual podría denunciarse ante Prodhab[28].

El sujeto pasivo.

La ley de protección de la persona frente al tratamiento de sus datos personales, reconoce el derecho de autodeterminación informativa únicamente a personas físicas, sin embargo, la Sala Constitucional que desarrolló este derecho a finales del siglo pasado, cobijó a las personas jurídicas, de similar manera que el Código Penal en el año 2012, con la inclusión del tipo penal bajo estudio. Por lo anterior,

[28] Sería una falta grave, de acuerdo al artículo 3, inciso a) de la Ley № 8968.

el sujeto pasivo en esta clase de delitos puede ser tanto una persona física como una jurídica.

En ese sentido la Sala Constitucional, al definir el derecho de autodeterminación informativa, manifiesta:

En este caso, también estamos ante una lesión **al derecho a la autodeterminación informativa** de la parte tutelada, el cual fue definido por este Tribunal en su sentencia número 4847-99, como el **" derecho fundamental de toda persona física o jurídica a conocer lo que conste sobre ella, sus bienes o derechos en cualquier registro o archivo, de toda naturaleza, incluso mecánica, electrónica o informatizada, sea pública o privada; así como la finalidad a que esa información se destine y a que sea empleada únicamente para dicho fin, el cual dependerá de la naturaleza del registro en cuestión.** Da derecho también a que la información sea rectificada, actualizada, complementada o suprimida, cuando la misma sea incorrecta o inexacta, o esté siendo empleada para fin distinto del que legítimamente puede cumplir.". (Sala Constitucional, Resolución Nº 14676 - 2020)

Es importante subrayar que los datos de las personas jurídicas están contenidos en los repositorios que almacenan y distribuyen los ciberdelincuentes con fines delictivos, al ser información de alto valor para sus operaciones criminales, por lo que la tutela penal de los datos personales de persona jurídica es relevante y tiene sentido desde la perspectiva de la política criminal en contra de la ciberdelincuencia.

En España, de igual manera, se permite tutelar penalmente los datos reservados de carácter personal de una persona jurídica, ya que extiende la

protección del capítulo *Del descubrimiento y revelación de secretos a las personas jurídicas:*

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código. (Código Penal de España de 1995, artículo 200)

Concepto de dato personal.

La ley № 8968 define al dato personal como “cualquier dato relativo a una persona física identificada o identificable” (Ley de la protección de la persona frente al tratamiento de sus datos personales, artículo 3, inciso a.)

Por otro lado, el concepto de dato personal de persona jurídica no lo encontramos en nuestro ordenamiento jurídico, sin embargo la Sala Constitucional nos da luz sobre este concepto en su jurisprudencia, al definirle de igual manera que el de persona física:

> III.- El objeto de protección del hábeas data y los principios básicos para la protección de datos. Objeto de protección del hábeas data son los "datos de carácter personal", es decir, **cualquier información relativa a una persona física o jurídica identificada o identificable.** El grado de protección de los datos dependerá de la naturaleza de los mismos, así, debe el Estado procurar que los datos íntimos (también llamados "sensibles") de las personas no sean siquiera accedidos sin su expreso consentimiento. (Sala Constitucional, Resolución Nº 08996 – 2002)

Verbos rectores.

El tipo penal incluye los siguientes verbos rectores o acciones que se pueden ejercer sobre el dato de una persona física o jurídica, cuyas acciones deberán entenderse en un contexto informático y ejercidas sobre un dato personal:

a) **Apoderar**: Acción a través de la cual un usuario toma posesión de la información de carácter personal de otro[29].
b) **Acceder**: Acción informática a través de la cual el agente tiene acceso al dato personal[30]. Un ejemplo de esta acción es cuando una persona ingresa a una base de datos electrónicas y ejecuta un comando para acceder al dato.
c) **Copiar**: Acción de duplicar un dato[31].
d) **Transmitir**: trasladar o transferir un dato de un lugar a otro[32].
e) **Publicar**: Incorporar al acceso público un contenido en un entorno digital (RAE, 2021)
f) **Difundir**: Propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas (RAE, 2021). De acuerdo al reglamento de la ley №8968, se define distribución, difusión de la siguiente manera: "Cualquier forma en la que se repartan o publiquen datos personales, a un tercero" (Reglamento N° 37554-JP, 2016)

[29] **Apoderar**: "Hacerse dueño de algo, ocuparlo, ponerlo bajo su poder". (RAE, 2021)
[30] **Acceder**: "Tener acceso a algo, especialmente a una situación, condición o grado superiores, o llegar a alcanzarlos. (RAE, 2021)

[31] **Copiar**. La Real Academia Española no contiene una definición precisa y aplicable para el campo de la informática, por lo que ante una consulta del diccionario Merriam-Webster (2021) que contiene una definición para la informática la cual podemos traducir cómo "hacer una copia o duplicado de… un documento o archivo de computadora" (Merriam Webster, 2021). De acuerdo a la RAE, duplicar es: "Repetir exactamente algo, hacer una copia de ello"

32 **Transmitir**:

1. Trasladar, transferir.
2. Dicho de una emisora de radio o de televisión: Difundir noticias, programas de música, espectáculos, (RAE, 2021)

g) por cualquier medio siempre que medie un fin de comercializar el dato o medie el lucro con la base de datos.

h) **Interferir**:
dicho de una señal: Introducirse en la recepción de otra y perturbarla. (RAE, 2021)

i) **Recopilar**: recoger datos personales con un fin[33].

j) **Interceptar:** apoderarse de datos contenidos en una comunicación[34] antes de que lleguen a su destino final[35].

k) **Desviar[36] para un fin distinto para el que fueron recolectados:** los datos personales deben recopilarse para fines específicos, que fueron autorizados por el titular o una ley facultativa, que no pueden ser variados por el responsable de la base de datos de manera unilateral.

l) **Dar un tratamiento no autorizado:** cada una de las acciones que se realicen sobre un dato deben estar debidamente autorizados por el titular o por ley. De acuerdo al reglamento de la ley №8968, se define como tratamiento: "Cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión,distribución o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros." (Reglamento N° 37554-JP, 2016)

m) **Comprar:** obtener el dato por un precio.

---

[33] **Recopilar**: Juntar en compendio, recoger o unir diversas cosas, especialmente escritos literarios. (RAE, 2021)

[34] **Comunicación**: Transmisión de señales mediante un código común al emisor y al receptor. (RAE, 2021)

[3535] **Interceptar**: Apoderarse de algo antes de que llegue a su destino. (RAE, 2021)

[36] **Desviar**: Apartar o alejar a alguien o algo del camino que seguía. (RAE, 2021)

n) **Vender**: Traspasar a alguien por el precio convenido la propiedad de lo que se posee. (RAE, 2021).
o) **Retener**: Impedir que algo salga, se mueva, se elimine o desaparezca. (RAE, 2021).
p) **Modificar**:
Transformar o cambiar algo mudando alguna de sus características. (RAE, 2021).
q) **Inutilizar:** hacer inútil, vano o nulo algo. (RAE, 2021).

El beneficio propio o de un tercero.

El elemento del beneficio es *conditio sine qua non* en este delito y precisamente es uno de los elementos que lo diferencian de de la violación de datos personales administrativa, que la persona puede denunciar ante la Prodhab. De acuerdo a la Real Academia Española (2020), podemos definir al beneficio de la siguiente manera:

1. Bien que se hace o se recibe.
2. Utilidad (provecho): a su vez la utilidad la define como "Provecho, conveniencia, interés o fruto que se saca de algo" .

Como puede extraerse de la definición, la violación de datos personales debe generarle beneficio, provecho[37] o utilidad al agente, o a un tercero. Sin pretender presentar una lista taxativa, los beneficios, no excluyentes entre sí, que pueden presentarse son los siguientes:

[37] Como puede verse más adelante el legislador colombiano adoptó el término provecho en el tipo penal de violación de datos personales.

a) **Comerciales**: para fines de mercadeo o conexos.

b) **Electorales**: los datos pueden ser utilizados de forma interna para generar análisis y tomar decisiones de carácter político, pero también podrían usarse para enviar comunicaciones masivas no solicitadas.

c) **Delictivos**: la información de carácter personal suele ser utilizada para crear perfiles de personas con la cual pueden realizar distintas actividades de carácter delictivo, como por ejemplo, para iniciar ataques de ingeniería social para realizar estafas informáticas.

d) **Económicos**: en este caso el beneficio es directo y de contenido económico.

e) **Laboral**: aunque de naturaleza similar a la anterior, en estos casos la persona podría obtener alguna ventaja para obtener o permanecer en un puesto debido a la acción sobre el dato.

Como puede verse, no necesariamente el beneficio debe ser de índole patrimonial, pero sí debe ser tangible y/o susceptible de ser acreditado en una investigación penal, ya que cuando el operador jurídico realice el juicio de tipicidad debe cerciorarse de que la conducta sujeta a su análisis se realice en beneficio propio o de un tercero, así como los otros elementos contenidos en la descripción típica.

El tráfico de datos personales es una conducta donde el dato es objeto comercial, el cual se transfiere a cambio de una contraprestación, la cual no necesariamente tiene contenido patrimonial. Debido a lo anterior, se puede concluir que cuando se trafican datos personales existe una persona que obtiene

un beneficio con esta acción y que esta dinámica genera un mercado ilegal de información personal y lesiona de forma sistemática la privacidad de los ciudadanos; lo que justifica la decisión del legislador de sancionarlo penalmente, al incorporar el delito de violación de datos personales en el artículo 196 bis del Código Penal. Lo anterior, en armonía con la ley de protección de la persona frente al tratamiento de sus datos personales, por lo que cuando en distintas acciones ilegales que lesionan el derecho de autodeterminación informativa, no está presente el beneficio, el ciudadano pueda siempre acudir a otras vías de resolución de este conflicto social, como lo puede ser la vía administrativa o la constitucional.

A pesar de que los tipos de beneficio que permite el tipo penal son *numerus apertus*, es importante ser claro que, de ninguna manera, el beneficio puede extenderse inclusive al sentimiento de satisfacción que puede sentir una persona al publicar de forma vengativa un dato personal de índole sexual o erótico, como en los casos de "porno-venganza"[38]. Si una autoridad judicial hiciera uso de este criterio, no solo generaría una profunda inseguridad jurídica, sino que la misma resultaría violatoria de la regla de interpretación restrictiva, la prohibición de la interpretación analógica y del principio de legalidad, que rigen en materia penal y procesal penal[39].

Desafortunadamente, la formula del beneficio puede resultar insuficiente para combatir la publicación masiva de bases de datos personales por parte de la

[38] Esta conducta, cuando se trata de documentos privados encuadra en el artículo 196 del Código Penal en su párrafo segundo

[39] Inclusive si el lector quisiera hacer un ejercicio futurista, se adelantara cien años, y se imaginara que un fiscal solicite el acceso a los recuerdos del imputado contenidos en soportes biológicos, la solicitud no sería de recibo porque de acuerdo al artículo 36 de la Constitución Política nadie está obligado a declarar contra sí mismo, por lo que la extracción, no consentida, de un recuerdo sería a todas luces una declaración obligada y por ende inconstitucional.

ciberdelincuencia donde no se busca un beneficio, sino simplemente realizar un daño a la privacidad colectiva, lo que es una modalidad de lo que se conoce como “doxing”[40] y que cuando se dirige a individuos de forma individual suele realizarse como parte de un acoso cibernético[41].

Agravantes.

En el delito de violación de datos personales, las penas serán de dos a cuatro años de prisión cuando las conductas descritas:

a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que **en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos:** en este caso no solo se sanciona de manera más grave a las personas que con mayores conocimientos de informática y/o por la confianza inherente a su cargo realizan la conducta delictiva, sino que también a toda persona que debido al acceso que ha tenido al sistema debido a sus funciones decide violar los datos del titular.

b) La información vulnerada corresponda a un menor de edad o incapaz: El legislador decidió proteger los datos de los menores, sin que implique

[40] El “doxing” anglicismo que abrevia el concepto de exponer documentos: Consiste en revelar información identificadora de una persona en línea, como su nombre real, dirección particular, lugar de trabajo, teléfono, datos financieros y otra información personal. Luego, esta información se divulga al público sin el permiso de la víctima.

Si bien la práctica de revelar información personal sin el consentimiento del sujeto en cuestión existe desde antes del nacimiento del Internet, el término doxing surgió primero en el mundo de los hackers en la década de 1990, en el que el anonimato se consideraba sagrado. Las disputas entre los hackers rivales a veces provocaban que alguien decidiera “exponer docs” sobre otra persona, quien hasta ese momento solo era conocida por su nombre de usuario o alias. “Docs” se convirtió en “dox” y, finalmente, en su propio verbo (es decir, sin el prefijo “exponer”) (Kaspersky, 2021)

[41] Como se analizará más adelante el Código Penal de 1995 de España sanciona las acciones que se realizan en perjuicio del titular, a diferencia del costarricense que requiere un beneficio.

necesariamente un mayor daño o que afecten una categoría de datos personales.

c) Las conductas afecten datos que revelen la ideología, la religión, las creencias la salud, el origen racial, la preferencia o la vida sexual de una persona: en este caso nos encontramos ante los datos que en nuestro ordenamiento jurídico se conocen como datos sensibles pero presentados en una lista taxativa que da mayor seguridad jurídica en su aplicación.

Aclaraciones sobre la aplicación del tipo penal.

La reforma № 9135 que vino a reformar el Código Penal, tan solo un año después de la reforma № 9048, se realizó en un contexto de señalamientos de "Ley mordaza", los cuales nos parecen fueron infundados, pero es cierto que permitieron corregir algunos de los errores graves que contenía la reforma, más por razones de índole político, no todos pudieron corregirse.

Debido a esto, con enorme influencia de medios de comunicación, en lo que podría considerarse una mala técnica legislativa se incorporaron, a nuestro criterio de manera innecesaria, "aclaraciones" sobre qué no configura este delito[42] en los siguientes casos:

1**. No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley:** en estos casos nos encontramos ante situaciones donde

[42] Aun en los casos donde la conducta que el legislador aclara que no es delito, de acuerdo con la descripción típica del tipo no sería delito.

no existiría violación de la privacidad y se contaría con facultad legal para realizar la publicación. Lo que es cierto es que este tipo de aclaraciones trajeron tranquilidad a la prensa nacional y eso es de gran valor en una democracia.

2. **Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley:** nuevamente**,** si un tratamiento se hace conforme a la ley no contendría todos los elementos para que sea considerado delito, al no ser típico, antijurídico ni culpable.

Caso nacional

Acceso ilegal a datos de Keylor Navas.

En el Poder Judicial se presentó un caso de un acceso ilegal de datos personales confidenciales, los cuales estaban almacenados en su sistema interno para investigaciones judiciales. Este acceso fue realizado por parte de funcionarios, en donde aparentemente el fin que tenían, era el de satisfacer su curiosidad sobre la vida personal del deportista que jugaba en el Real Madrid, aprovechando el acceso con el que contaban en la Plataforma de Información Policial (PIP).

Por los motivos legales expuestos anteriormente, no podríamos concluir que la satisfacción de su deseo de fisgonear, pueda interpretarse como una utilidad que obtuvieron de su acción ilegal, ya que esa sería una interpretación extensiva y analógica[43].

En esa misma línea, la causa fue desestimada, como lo reportó el diario electrónico de La Nación:

El Juzgado Penal del Segundo Circuito Judicial de San José desestimó la causa penal abierta contra 25 funcionarios judiciales que, en el 2014, accedieron a información privada del portero costarricense Keylor Navas en una base de datos policial, la cual es de acceso restringido.

La desestimación fue solicitada por la Fiscalía Adjunta de Probidad, Transparencia y Anticorrupción, la cual argumentó que los hechos investigados "no configuraron una conducta delictiva tipificada en nuestra legislación", lo que se conoce, técnicamente, como atipicidad (Artavia, S. 2020).

Derecho comparado.

España.

El Código Penal de España de 1995 decidió tutelar penalmente los datos reservados de carácter personal en el título X que contiene los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.

En el numeral 197.1, parte del capítulo I, correspondiente al *Descubrimiento y revelación de secretos*, sanciona penalmente la violación de correspondencia y documentos privados de manera similar al artículo 196 de nuestro Código Penal[44], con penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

[44] 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será

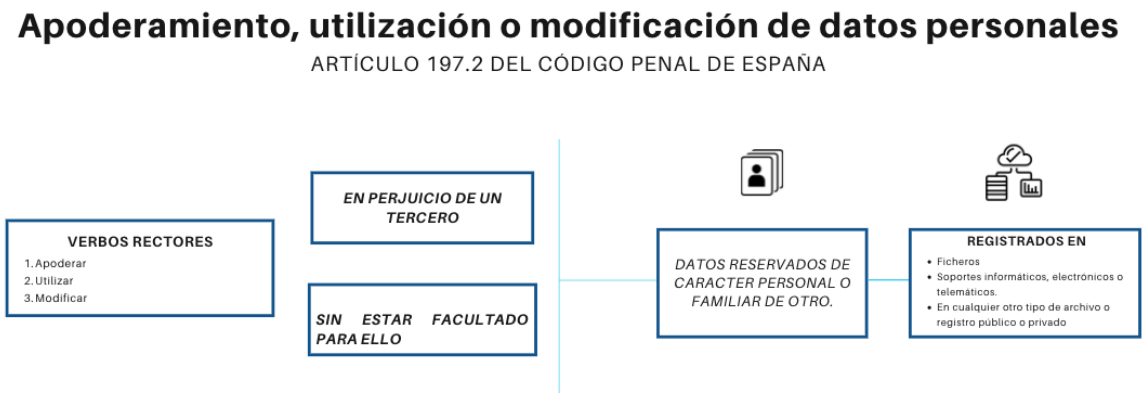


FIgura 3. (ARTÍCULO 197.2 del Código Penal de España [Elaboración propia]

Por otro lado, en el numeral 197.2, sanciona el apoderamiento, utilización o modificación de datos personales, el cual cuenta con similar naturaleza al de violación de datos personales costarricense:

> 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. (Código Penal de España, artículo 197.2)

Debido al objeto de estudio de la presente investigación, procederemos a analizar los de elementos de este tipo penal:

a) Sin estar autorizado: nos parece adecuado ya que es un concepto más amplio que incluye tantos tratamientos realizados con el consentimiento

castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. (Código Penal de España, Artículo 197.1)

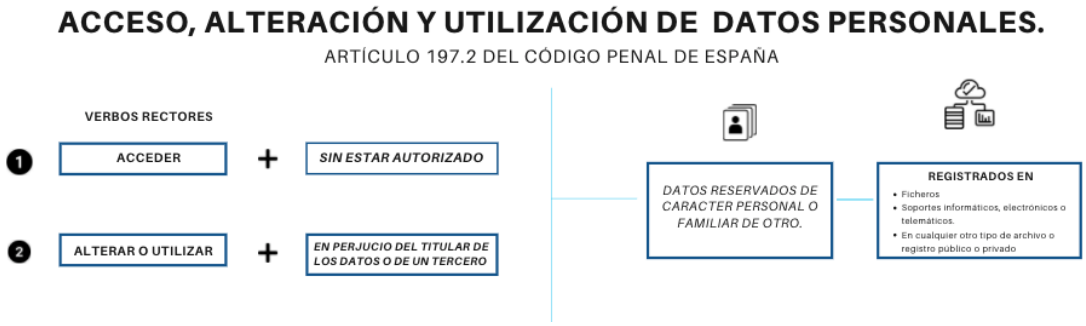
expreso, por autorización de carácter legal e inclusive contractual.

b) Verbos rectores: apoderamiento, utilizar y modificar: si bien es cierto la cantidad de verbos rectores es inferior en cantidad a los contenidos en la violación de datos personales costarricense, lo cierto es que el verbo “utilizar” es lo suficiente amplio como para poder extenderse a varios de los verbos que están contenidos en el nuestro.

c) En perjuicio de un tercero: Este elemento es de menor complejidad probatoria, que el contenido en nuestra legislación, ya que acreditar la lesión a la privacidad resulta más sencilla en el proceso judicial que acreditar el beneficio.

Sin embargo, con respecto al sujeto pasivo, indicar que es un “tercero”, resulta un término impreciso el cual se presta para confusión con respecto a si el daño debe ser para el titular u otro individuo, ya que el mismo tipo penal hace la diferenciación en cuanto al acceso y la alteración en perjuicio de tercero o del titular.

d) Datos reservados de carácter personal o familiar de otro: han de ser informaciones cuyo conocimiento está limitado a personas autorizadas o, lo que es lo mismo, han de ser datos no disponibles sin autorización y que incidan en la esfera personal o familiar. (Gómez, 2020, p. 341)



Este artículo sanciona, con las mismas penas, el acceso no autorizado a los datos reservados de carácter personal, cuando el agente realiza la acción sin contar con la autoridad para realizarlo.

De la misma manera, la alteración y utilización de los datos, en perjuicio del titular se sanciona con la misma pena, lo que a diferencia del tipo penal costarricense permite perseguir penalmente tratamientos de datos personales que, aunque se utilicen en perjuicio del titular no le genera al agente, o a un tercero, un beneficio.

Para la difusión, revelación o cesión de datos y/o secretos el Código Penal español lo regula de la siguiente manera:

> Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.
>
> Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior. (Código Penal de España, Artículo 197.3)

a) Verbos rectores: difusión, revelación cesión

b)Datos o hechos descubiertos o las imágenes captadas: en los casos donde aparte de las acciones contenidas en los tipos penales anteriores el agente las difunda, revela o ceda la conducta se subsumiría en este tipo penal.

De manera acertada el legislador español decide aumentar la pena cuando la acción que realiza el agente es de difusión, ya que coincidimos con que el daño a la privacidad de la persona es mayor.

Agravantes.

El legislador español del Código Penal de 1995, aumenta las penas cuando las acciones se realizan por personal que brinda soporte al sistema informático[45], lo que en el año 2012 fue incorporado de la misma manera por el legislador costarricense.

De manera interesante, cuando los datos se difundan[46] o medie lucro, el legislador español tiene previsto que las penas aumenten, lo que sería más cercano con el delito de violación de datos personales costarricense[47].

Colombia

La República de Colombia mediante la Ley 1273 del 5 de enero del 2009, reforma su Código Penal que incluye dos nuevos bienes jurídicos al incluir el

[45] 4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. (Código Penal de España, Artículo 197.4)

[46] Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior. (Código Penal de España, Artículo 197.5)

[47] Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años. (Código Penal de España, Artículo 197.6)

“Título VII BIS” denominado "De la Protección de la información y de los datos", con el cual incorpora la violación de datos personales, entre otros delitos informáticos:

a) **Artículo 269A: Acceso abusivo a un sistema informático.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

   Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor

b) **Artículo 269C: Interceptación de datos informáticos.** Pena de prisión 36 a 72 meses.
c) **Artículo 269D: Daño Informático.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

d) **Artículo 269E: Uso de software malicioso:** Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

e) **Artículo 269F: Violación de datos personales.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

f) **Artículo 269G: Suplantación de sitios web para capturar datos personales.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1000

salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena más grave.

g) **Artículo 269I: Hurto por medios informáticos y semejantes**. Pena de 3 a 8 años de prisión.

h) **Artículo 269J: Transferencia no consentida de activos.** Pena de prisión de 48 a 120 meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes.

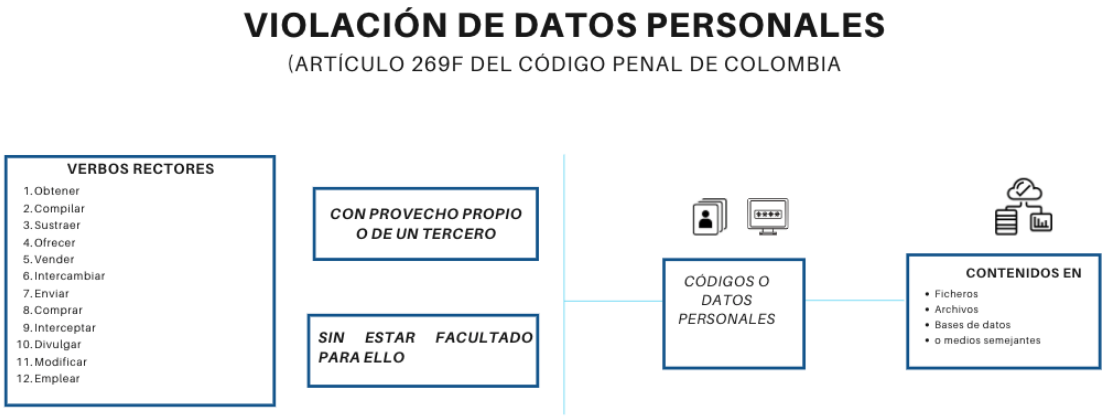


FIgura 4. Artículo 269F del Código Penal de Colombia. [Elaboración propia]

La formula elegida por el legislador colombiano para el delito de violación de datos personales, contenida en el artículo 269F del Código Penal colombiano es la siguiente:

“El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá

en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

A continuación analizaremos los elementos del tipo penal:

a) Sin estar facultado para ello: este elemento pareciera mucho más amplio y acertado que el elegido por el legislador costarricense, debido a que un responsable de una base de datos podría estar facultado por una ley para realizar un tratamiento y no necesariamente contar con el consentimiento del titular, como lo establece como requisito el 196 bis de nuestro Código Penal.

b) Con provecho propio o de un tercero: el beneficio y el provecho son sinónimos por lo que este elemento no presenta mayor diferencia con respecto al tipo local.

c) Verbos rectores: obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear.

d) Códigos personales: tomando en cuenta que por información personal solo debe entenderse aquella que permite identificar o hacer identificable a un individuo, la incorporación de la protección a las contraseñas o códigos personales, aunque nos parece impreciso, favorece la lucha contra el comercio de contraseñas en los mercados negros.

e) Ficheros, bases de datos o medios semejantes: El legislador colombiano no límita la tutela del dato de acuerdo a su soporte.

Ecuador

El Código Penal ecuatoriano en su numero 178, denominado *Violación de intimidad*, incorporado en el año 2014, se tutelan los datos personales, así como las comunicaciones de acciones violatorias a la intimidad.

> Artículo 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.
>
> No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley. (UNODC, 2021)

Los elementos del tipo penal son los siguientes:

a) Sin contar con el consentimiento o la autorización legal: de igual manera que el legislador colombiano, este elemento resulta más preciso.

b) Verbos rectores: acceder, interceptar, examinar, retener, grabar, reproducir, difundir o publicar: si bien es cierto vemos que muchos de los verbos son similares al tipo penal nuestro, al incorporar distintos bienes jurídicos y acciones en un mismo penal hace que su aplicación sea más amplia. En este sentido, se puede ver como conductas que se aplicarían en distintos tipos penales en nuestro Código Penal, en el caso de Ecuador encuadrarían en este tipo penal.

c) Intereses protegidos: datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio.

d) **No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley:** nos parece un elemento incongruente que deja en desprotección, con respecto a su privacidad, a una de las partes intervinientes en la comunicación. Por otro lado, en casos de información pública no existiría lesión del bien jurídico.

En el año 2021, en una reciente reforma que elimina el párrafo segundo del tipo penal, se ha generado una gran controversia debido a que restringe las situaciones en las que se puede realizar una grabación, lo que ha despertado malestar nacional ya que cree que la misma es para proteger políticos.

En ese sentido Mae Montaño, legisladora proponente, indica que esta norma estaba orientada a combatir y prevenir la violencia sexual digital. Sin embargo, indica que “el aprovechamiento y oportunismo politiquero” hicieron una ley para “proteger a los políticos autoritarios, abusivos y corruptos“. (González, 2021)

Es importante reiterar que toda reforma sobre las TIC requiere un importante debate regulatorio que incorpore a todas las partes interesadas para evitar este tipo de controversias que no son sanas para ninguna democracia.

Conclusiones

La aceleración en la transformación digital que se está presentando en la sociedad costarricense, potencia la recopilación de los datos personales de los habitantes, los cuales corren el riesgo de ser capturados por la ciberdelincuencia, lo que requiere que se persiga de forma más activa a los actos delictivos que atenten contra el derecho de autodeterminación informativa.

Para cumplir lo anterior es necesaria una Estrategia Nacional de Lucha Contra la Ciberdelincuencia que sirva como derrotero de las autoridades en este campo, desde contar con un programa establecido de capacitación, herramientas tecnológicas y procesales que favorezcan la investigación de delitos cometidos por medios informáticos.

El tipo penal de violación de datos personales requiere una reforma que incorpore el concepto soporte informático en vez del de contenedor el cual resulta impreciso y limita la protección de datos que se almacenen en dispositivos aislados de almacenamiento.

Como propuesta de *lege ferenda* se debe reformar el Código Penal, en tipo penal independiente al de estudio, con el fin de sancionar de manera especial la violación de bases de datos electrónicas que afecten datos de múltiples personas y/o se difundan datos personales sensibles y confidenciales, aunque en las conductas no se realicen en beneficio propio, o de un tercero, pero sí en perjuicio de los titulares, de manera similar a la elegida por el legislador Español del Código Penal de 1995.

Bibliografía

Acceder, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/acceder

Apoderar, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/apoderar

Artavia S. (7 de Junio de 2020). Juzgado desestima causa penal sobre violación de datos de Keylor Navas. Recuperado el 27 de abril del 2021 de https://www.nacion.com/el-pais/politica/juzgado-desestima-causa-penal-sobre-violacion-de/DCRBN6NJGVHTLHAYRZR5SUB25M/story/

Arteaga, S. (30 de Junio de 2017). Microsoft implementará el almacenamiento de datos en ADN en 2020. Recuperado el 26 de abril del 2021 de https://computerhoy.com/noticias/hardware/microsoft-implementara-almacenamiento-datos-adn-2020-62994

Artículo 178 (2014) UNODC, Sherloc. Recuperado el 8 de mayo del 2021 de https://sherloc.unodc.org/cld/en/legislation/ecu/codigo_organico_penal/libro_primero/articulo_178/articulo_178.html

Beneficio, Definición. Real Academia Española. Recuperado el 27 de abril del 2021 de https://dle.rae.es/beneficio

Criptomoneda - Qué es, definición y concepto. (26 de setiembre de 2017). Economypedia. Recuperado 25 de abril, 2021, de https://economipedia.com/definiciones/criptomoneda.html

Chip, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/chip

Chinchilla, D (21 de febrero de 2020.). Alvarado crea oficina para obtener datos confidenciales de los ticos. Recuperado el 26 de abril del 2021 de https://computerhoy.com/noticias/hardware/microsoft-implementara-almacenamiento-datos-adn-2020-62994

Comunicación, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/comunicaci%C3%B3n

Contenedores y la nube: una forma más sencilla de implementar cargas de trabajo (2021). Intel. Recuperado el 26 de abril del 2021 de https://www.intel.es/content/www/es/es/cloud-computing/containers.html

Cuidado, los marcapasos también pueden hackearse (21 de febrero del 2018). ABC. Recuperado el 26 de abril del 2021 de https://www.abc.es/salud/tecnologia-salud/abci-cuidado-marcapasos-tambien-pueden-hackearse-201802211613_noticia.html

Dávara, E y Dávara L (2017). Delitos Informáticos. Thomson Reuters Aranzandi

Dean, S. (1 de enero de 2020), Es 2020 y usted tiene nuevos derechos de privacidad en línea. Pero es posible que deba mostrar una identificación. Recuperado el 23 de abril del 2021 de https://www.latimes.com/espanol/california/articulo/2020-01-01/es-2020-y-usted-tiene-nuevos-derechos-de-privacidad-en-linea-pero-es-posible-que-deba-mostrar-una-identificacion

Doxing, Definición y explicación. Recuperado el 28 de abril del 2021 de https://latam.kaspersky.com/resource-center/definitions/what-is-doxing

Gómez, A. (2011). Enciclopedia de la Seguridad Informática. Alfaomega, Ra-Ma.

González S (2 de enero de 2018). Glosario de terminología TIC. Abogacía Española, Consejo General.

González, M. (8 de Mayo de 2021). Protección de la intimidad o censura: polémica por reformas al COIP. Recuperado el 8 de mayo del 2021 de https://www.primicias.ec/noticias/politica/proteccion-intimidad-censura-reformas-coip/

Glosario de Términos de Ciberseguridad: Una Guía de Aproximación Para El Empresario. (2017). Instituto Nacional de Ciberseguridad.

Interceptar, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/interceptar

Interferir, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/interferir

Jaimovich, D. (25 de setiembre, 2019). *Qué es la Ley de Moore y cómo marcó el ritmo de la evolución digital*. Infobae. Recuperado 25 de abril, 2021, de https://www.infobae.com/america/tecno/2019/09/25/que-es-la-ley-de-moore-y-como-marco-el-ritmo-de-la-evolucion-digital/

Luna, N (1 de Marzo de 2018). ¿Qué es B2B y B2C en marketing? Recuperado el 27 de abril del 2021 de https://www.entrepreneur.com/article/308985

Los ataques de ransomware se disparan en todo el mundo (7 de abril del 2021). IT Digital Security. Recuperado el 26 de abril del 2021 de https://www.itdigitalsecurity.es/actualidad/2021/04/los-ataques-de-ransomware-se-disparan-en-todo-el-mundo

Modificar, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/modificar

Monopolio en Internet. (18 de agosto de 1999).). La Nación. Recuperada el 25 de abril de 2021. https://www.nacion.com/opinion/monopolio-en-internet/RWEXHLY3YVGYXAI5MVSV7CHBJ4/story/

Peñas, E. (13 de febrero, 2017). Ethic. Recuperado el 26 de abril del 2021 de https://ethic.es/2017/11/transhumanismo-antonio-dieguez/

Publicar, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/publicar

Resultó ser obscena. (2 de julio de 1997). La Nación. Recuperada el 25 de abril de 2021. https://www.nacion.com/archivo/resulto-ser-obscena/SPNHX2KPPBFUPBEWGGREF6534A/story/

Recopilar, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/recopilar

Retener, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/retener

Sandí, C. C (2002). *Delitos informáticos*. Editorial Investigaciones Jurídicas S.A.

Sextorsión, el chantaje por internet que deja indefensos a cientos de miles de hombres. BBC Mundo. (22 de diciembre de 2014) Recuperado el 26 de abril del 2021 de https://www.bbc.com/mundo/noticias/2014/12/141222_tecnologia_sextorsion_chantaje_internet_sexo_extorsion_ig

Soporte, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/soporte

Transmitir, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de https://dle.rae.es/transmitir

LEÓN WEINSTOK

- Experto en Protección de datos y privacidad y director en el Bufete BLP en las áreas de Protección de Datos, Propiedad Intelectual y Protección del Consumidor.
- Master en derecho de la empresa de la Universidad Católica de Chile
- Licenciado en Derecho en la Universidad de Costa Rica.
- Asesor de empresas nacionales y transnacionales en la implementación de los procedimientos y documentación necesaria para el manejo de datos
- Representación en a defensa ante la Agencia de Protección de Datos (PRODHAB) de Costa Rica
- Director de empresas en los pasos que deben tomar en caso de que sufran algún incidente de seguridad con sus datos.
- lweinstok@blplegal.com

5



Formas de legitimación del tratamiento de datos personales (Basis for processing personal information)

León Weinstok
Experto en Protección de datos y privacidad.
Master en derecho de la empresa de la Universidad Católica de Chile.
Licenciado en Derecho en la Universidad de Costa Rica.
Director en el Bufete BLP en las áreas de Protección de Datos, Propiedad Intelectual y Protección del Consumidor.
lweinstok@blplegal.com

I. RESUMEN

En síntesis, el derecho a la Autodeterminación Informativa le permite a cada persona decidir cómo desea que sean tratados sus datos personales. Sin embargo, al igual que casi todos los derechos, este no es un derecho irrestricto y tiene algunas limitaciones. Para ello, existen muchas bases que permiten justificar el tratamiento de datos personales las cuales incluyen aquellas que requieren la autorización expresa del interesado, así como las que encuentran su justificación de alguna otra forma.

Palabras clave: Autodeterminación Informativa, Datos Personales, Consentimiento Informado, Bases de legitimación, Privacidad

II. ABSTRACT

In summary, the right for self-determination allows to every individual to decide what information about himself should be communicated to others and under what circumstances. As such, this is not an unrestricted right and may be limited.

Thus, there are different basis for processing the information which include those that demand the authorization from the data subject and those that justify this processing in any other reason.

Keywords: Informational Self-Determination, Personal Data, Informed Consent, Lawful processing, Privacy.

III. INTRODUCCIÓN

El tratamiento de Datos Personales, entendidos estos como "*cualquier dato relativo a una persona física identificada o identificable*"[1] conlleva muchas etapas. Dentro de estas etapas se encuentran entre otras, la recopilación de la información, su tratamiento, respaldo, así como respuesta a los derechos de los interesados. En el presente artículo, se pretende tener una noción clara del concepto de autodeterminación informativa siendo este el principal derecho que se pretende proteger y a partir de este desarrollar las bases con las cuales los responsables de las bases de datos pueden realizar un tratamiento válido de los datos personales de los interesados.

IV. AUTODETERMINACIÓN INFORMATIVA

Para comprender de forma adecuada las distintas bases de legitimación para el tratamiento de datos personales, es importante conocer el derecho medular de la protección de datos personales, es decir, la autodeterminación informativa.
Si bien se considera que internacionalmente este derecho nace en el Tribunal Constitucional Federal Alemán, esta protección quedaba englobada, según el decir de la sentencia, en el artículo 2, párrafo primero, de la Ley Fundamental de Bonn de 1949. De igual forma en nuestro país, el surgimiento de este derecho

[1] Artículo 3 de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales

fue similar. Si bien el artículo 24 de la Constitución Política de 1949, garantiza entre otros, los derechos fundamentales a la intimidad, la inviolabilidad de los documentos privados, el secreto de las comunicaciones y el derecho a la autodeterminación informativa es hasta la creación de la Sala Constitucional donde se desarrolla este concepto específicamente mediante la figura del Habeas Data.

Estos derechos se basan en la dignidad de la persona y su ejercicio supone la autodeterminación consciente y responsable de la propia vida. Es decir, la autodeterminación informativa, lejos de ser un "nuevo" derecho fundamental corresponde a la transformación del derecho a la privacidad e intimidad a raíz principalmente de los avances tecnológicos y la información.

En este sentido, la autodeterminación informativa incluye el derecho fundamental de las personas a decidir sobre quién, cuándo y bajo cuáles circunstancias otras personas tienen acceso a sus datos, así como el derecho a conocer la información que conste sobre ella en las bases de datos y el derecho a que esta información sea rectificada, actualizada, complementada o suprimida, cuando sea incorrecta. Para un mejor entendimiento sobre este concepto, el mismo ha sido definido como:

> "*El derecho a la autodeterminación informativa es un derecho fundamental que habilita a la persona para decidir, por sí sola, sobre la difusión y utilización de sus datos personales con un fin determinado y con independencia del tipo de soporte (físico o electrónico) en el que se encuentren los datos personales.*
>
> *La expresión "autodeterminación informativa" tuvo su origen en la sentencia del Tribunal Constitucional alemán del 15 de diciembre de 1983 y hace referencia a un derecho auto nomo que se entrelaza con el derecho humano a la protección de datos personales, que se relaciona estrechamente con los de intimidad y privacidad y cuyo*

objeto es otorgar protección al individuo frente a la obtención, almacenamiento, utilización y transmisión de sus datos personales, al otorgarle la facultad para decidir sobre su difusión y uso con un fin determinado.

Desde una acepción genérica, el término "autodeterminación" significa "determinar por sí mismo", que se puede traducir como la capacidad de decidir por uno mismo, y en relación con el tratamiento de los datos personales esta expresión se vincula con la facultad del titular de los datos para decidir sobre el uso que se da a su información y tener control sobre la misma."[2]

Como se mencionó, este derecho ha sido reconocido por nuestro país e incluso previo a la promulgación de la Ley de Protección de la Persona frente al tratamiento de sus Datos Personales, la Sala Constitucional en el voto N° 754-2002, de las 13:00 del 25 de enero de 2002, además de reconocer este derecho, se pronunció en específicamente en relación a los grados de protección propios de cada forma de tratamiento de datos personales:

"*En la actualidad, debido a la facilidad y fluidez con que las informaciones son obtenidas, almacenadas, transportadas e intercambiadas, fenómeno en apariencia irreversible y que por el contrario tiende a acentuarse a cada momento, se hace necesario ampliar la protección estatal a límites ubicados mucho más allá de lo tradicional, en diferentes niveles de tutela. Así, <u>debe el Estado procurar que los datos íntimos (también llamados "sensibles") de las personas no sean siquiera accedidos sin su expreso consentimiento</u>. Trátase de informaciones que no conciernen más que a su titular y a*

[2] Davara, I, Barco, G y Cervantes, A (2019). Diccionario de Protección de Datos Personales. Conceptos Fundamentales (Primera Edición). México: INAI

quienes éste quiera participar de ellos, tales como su orientación ideológica, fe religiosa, preferencias sexuales, etc., es decir, aquellos aspectos propios de su personalidad, y que como tales escapan del dominio público, integrando parte de su intimidad del mismo modo que su domicilio y sus comunicaciones escritas, electrónicas, etc. En un segundo nivel de restricción se encuentran las informaciones que, aun formando parte de registros públicos o privados no ostentan el carácter de "públicas", ya que –salvo unas pocas excepciones- interesan solo a su titular, pero no a la generalidad de los usuarios del registro. Ejemplo de este último tipo son los archivos médicos de los individuos, así como los datos estrictamente personales que deban ser aportados a los diversos tipos de expedientes administrativos. En estos casos, si bien el acceso a los datos no está prohibido, sí se encuentra restringido a la Administración y a quienes ostenten un interés directo en dicha información. En un grado menos restrictivo de protección se encuentran los datos que, aun siendo privados, no forman parte del fuero íntimo de la persona, sino que revelan datos de eventual interés para determinados sectores, en especial el comercio. Tal es el caso de los hábitos de consumo de las personas (al menos de aquellos que no quepan dentro del concepto de "datos sensibles"). En estos supuestos, el simple acceso a tales datos no necesariamente requiere la aprobación del titular de los mismos ni constituye una violación a su intimidad, como tampoco su almacenamiento y difusión. No obstante, la forma cómo tales informaciones sean acopiadas y empleadas sí reviste interés para el Derecho, pues la misma deberá ser realizada de forma tal que se garantice la integridad, veracidad, exactitud y empleo adecuado de los datos. Finalmente, se encuentran los datos que, aun siendo personales, revisten un marcado interés público, tales como los que

se refieren al comportamiento crediticio de las personas; no son de dominio público los montos y fuentes del endeudamiento de cada individuo, pero sí lo son sus acciones como deudor, la probidad con que haya honrado sus obligaciones y la existencia de antecedentes de incumplimiento crediticio, datos de gran relevancia para asegurar la normalidad del mercado de capitales y evitar el aumento desmedido en los intereses por riesgo. Con respecto a estos datos, también caben las mismas reglas de recolección, almacenamiento y empleo referidos a los anteriores, es decir, la veracidad, integridad, exactitud y uso conforme. El respeto de las anteriores reglas limita, pero no impide a las agencias –públicas y privadas- de recolección y almacenamiento de datos, cumplir con sus funciones, pero sí asegura que el individuo, sujeto más vulnerable del proceso informático, no sea desprotegido ante el poder inmenso que la media adquiere día con día." (El subrayado es propio)

Adicionalmente, muchos tratados y convenios internacionales de los cuales Costa Rica es parte, incluyen este derecho. De esta forma, tanto la Declaración Universal de los Derechos Humanos de 1948 (artículo 12), el Pacto Internacional de Derechos Civiles y Políticos de 1966 (artículo 17) y la Convención Americana de 1969 (artículo 11), contemplan el derecho a la intimidad personal y familiar que como se mencionó, son derechos de los cuales deriva la autodeterminación informativa.

Con base en lo anterior, resulta claro que en Costa Rica se encuentra debidamente consagrado en todos los niveles del bloque de legalidad, el derecho a la autodeterminación informativa y de esta forma, el tratamiento de los datos personales requiere una especial atención.

V. BASES DE LEGITIMACIÓN

Para poder realizar un tratamiento legítimo de los datos personales, es necesario tener un respaldo o motivo que justifique la licitud del tratamiento. En este sentido, en Costa Rica el Consentimiento Informado ha sido el principal medio para justificar dicho tratamiento. Si bien el consentimiento es necesario para muchas cosas, esto podría considerarse inadecuado al ser en muchos casos imposible su obtención. En virtud de lo anterior, se han desarrollado otras herramientas para justificar el tratamiento de datos personales, teniendo como principal marco normativo en realizar este desarrollo el Reglamento General de Protección de Datos de la Unión Europea. Es así que estas formas permiten ajustarse de mejor forma al flujo real de los datos.

Para lo anterior, resulta imperioso conocer las particularidades de cada base de legitimación a fin de conocer los beneficios y limitaciones de cada una.

a. Consentimiento Informado

El consentimiento es una materia extremadamente delicada y compleja de regular, ya que resulta muy difícil encontrar un equilibrio entre la prestación de un consentimiento verdaderamente informado y libre cuando éste se conjuga con los deberes que debe cumplir el responsable y que le son razonablemente exigibles. Para mayor claridad, el Consentimiento Informado es definido en el Reglamento General de Protección de Datos de la Unión Europea como "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*". Asimismo, el Reglamento a la Ley de Datos lo define como "*Toda manifestación de voluntad expresa, libre, inequívoca, informada y específica que se otorgue por escrito o en medio digital para un fin determinado, mediante la cual el titular de los datos personales o su representante, consienta el tratamiento de sus datos*

personales. Si el consentimiento se otorga en el marco de un contrato para otros fines, dicho contrato deberá contar con una cláusula específica e independiente sobre consentimiento del tratamiento de datos personales." Como podemos notar, estas definiciones son similares entre si y a su vez consistentes en muchos los ordenamientos. En esta línea, con mayor amplitud el considerando 32 del Reglamento General de Protección de Datos indica lo siguiente:

> "*El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta*."

Es de esta forma como queda claro que el Consentimiento Informado es un documento o herramienta formal que tiene muchos requisitos tanto de forma como de fondo. Asimismo, tiene como sus principales requisitos el hecho que

sea expreso, libre, inequívoco e informado. De esta forma, en relación al deber de ser expreso, esto implica que debe darse una actitud activa por parte del interesado a fin de garantizar que se dio una manifestación de voluntad de forma inequívoca. Asimismo, esta declaración debe presentarse de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo, especialmente cuando se trate de un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento de datos personales[3]. Es así como no se puede esperar una actitud pasiva del interesado y por el contrato, debe darse una actitud pasiva en el cual no se entienda que por omisión fue otorgado o se presuma otorgado el consentimiento.

Asimismo, para que el mismo sea específico esto conlleva a que cuando el consentimiento expreso se refiere de forma concreta, explícita y lícita a una o varias finalidades determinadas que justifiquen el tratamiento de los datos personales. Este requisito se cumple cuando la solicitud del consentimiento va relacionada con las finalidades concretas del tratamiento que se informan en el aviso de privacidad. Es decir, con base en esta característica, el consentimiento se debe solicitar para tratar los datos personales para finalidades específicas, no en lo general.[4]

Adicionalmente, para que el mismo sea informado, debe darse una descripción de los tratamientos que se vayan a hacer en el marco del correspondiente contrato debe basarse en un lenguaje claro y sencillo. Ello debería requerir el uso de un texto de fácil comprensión, con el objetivo de que los afectados puedan entender fácilmente los tratamientos que se darán como consecuencia de su aceptación del correspondiente consentimiento. Asimismo, el consentimiento informado no tiene únicamente regulaciones de forma como las mencionadas del lenguaje y forma de aceptación. Incluso la Ley de Datos

[3] Sentencia del 11 de noviembre del 2020 del caso C-61/19 del Tribunal de Justicia de la Unión Europea (Sala Segunda)

[4] INAI. (2016, junio). Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, p. 18. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

incluye una lista taxativa de información que se debe cumplir a fin de cumplir con este requisito. En este sentido, el artículo 5 de la Ley de Datos incluye las siguientes obligaciones de informar:

> **"a)** De la existencia de una base de datos de carácter personal.
>
> **b)** De los fines que se persiguen con la recolección de estos datos.
>
> **c)** De los destinatarios de la información, así como de quiénes podrán consultarla.
>
> **d)** Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos.
>
> **e)** Del tratamiento que se dará a los datos solicitados.
>
> **f)** De las consecuencias de la negativa a suministrar los datos.
>
> **g)** De la posibilidad de ejercer los derechos que le asisten.
>
> **h)** De la identidad y dirección del responsable de la base de datos."

Por último, en relación a los requisitos para que el consentimiento sea libre, este debe entenderse como aquel que es otorgado sin que medie algún tipo de error, presión mala fe, violencia o similar que de alguna forma pudiese afectar la libre voluntad del interesado.

Como se puede notar, el Consentimiento Informado resulta ser un mecanismo importante (no el único) para recopilar datos personales. Incluso, países como Costa Rica en la Ley de Datos le dan a este un rol protagónico al señalar en el artículo 5 que "Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo." Es decir, salvo las 3 excepciones mencionadas en dicho artículo (cuando exista orden fundada de un juez o acuerdo de una comisión de la

Asamblea Legislativa; se trate de datos personales de acceso irrestricto o bien, los datos deban ser entregados por mandato legal), el Consentimiento informado es necesario para cualquier tipo de recolección de datos personales. Esta obligación o uso exclusivo del Consentimiento Informado, deja de lado muchas otras formas que deberían considerarse como bases para legitimar el tratamiento de datos personales y que en la Ley de Datos actual de Costa Rica se echan de menos.

b. Tratamiento necesario para la ejecución de un contrato

Otra forma para legitimar el tratamiento de datos personales es cuando dicho tratamiento es necesario para la ejecución de un contrato. En este sentido, el inciso b) del artículo 6 del Reglamento General de Protección de Datos indica que el tratamiento será lícito cuando "el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales".

Esta posibilidad aplica en aquellos casos en que el titular es parte de un contrato o bien desea realizar los pasos previos para la formalización de un contrato. Uno de los casos más evidentes resulta cuando el titular adquiere un producto o servicio del encargado del tratamiento y para la entrega del producto o servicio el encargado de tratamiento necesita procesar o realizar tratamiento de datos personales del titular.

No obstante lo anterior, esta es una justificación que si bien puede ser sumamente práctica y dinámica, debe ser utilizada únicamente en aquellos casos en que resulta necesario y esencial el tratamiento de dicha información y el uso de la misma debe limitarse única y exclusivamente a cumplir con dicho fin.

Asimismo, tal y como lo ha señalado la Agencia Española de Protección de Datos, cuando se utilice esta base de legitimación, es necesario informar de

dicha circunstancia a los titulares. Es decir, independientemente de que dicha circunstancia no debe ser expresamente aceptada por los interesados, esta debe ser debidamente informada. En este sentido ha señalado esta agencia que "*Cuando el tratamiento sea necesario para la ejecución de algún contrato (mercantil, laboral, administrativo,…) en el que el interesado sea parte, o para la aplicación de medidas precontractuales, se hará constar una referencia al contrato o tipo de contrato de que se trate, con el detalle suficiente para que no quepa ninguna ambigüedad sobre lo que se refiere*"[5]

c. Tratamiento necesario para el cumplimiento de una obligación legal

Esta es una base de legitimación es importante tomar en cuenta que esta hace referencia a una obligación en la cual el responsable de la base de datos tiene una obligación legal de cumplir con dicha obligación. En Costa Rica ejemplos de esto son las obligaciones incluidas en la "Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo" o bien la información que se debe enviar a la Caja Costarricense del Seguro Social o bien, para el cumplimiento de obligaciones tributarias. Sin embargo, esta justificación no es aplicable cuando la obligación nace de una obligación contractual dado que en dicho caso aplicaría la base para el tratamiento anterior.

Esta base de tratamiento de cierta forma se encuentra regulada en la Ley de Datos al señalar en el artículo 5 como una excepción al tratamiento cuando estos datos deban ser entregados "*por disposición constitucional o legal*". Sin embargo, en lugar de ser una excepción a la obligación del Consentimiento Informado, esta debería ser una base de legitimación independiente. Es decir, tal y como fue supra indicado, no es recomendable que el Consentimiento

[5] "Guía para el cumplimiento del deber de informar", Agencia Española de Protección de Datos. Disponible en: https://www.aepd.es/es/documento/guia-modelo-clausula-informativa.pdf-0

Informado sea la regla general para el tratamiento de datos personales sino que, las distintas justificaciones existentes deben estar al mismo nivel que el consentimiento informado al momento de justificar el tratamiento de datos personales.

Sobre este aspecto, merece un importante interés lo mencionado en el considerando 45 del Reglamento General de Protección de Datos de la Unión Europea en el cual se deja claro que esta justificación es aplicable cuando dicha obligación es hecha por países de la Unión Europea. En este sentido, tratamientos de datos que les sea aplicable este reglamento requerirían otra base de justificación cuando tengan que entregar los datos personales por obligación legal en un país que no pertenezca a la Unión.

d. Tratamiento basado en la protección de datos es necesaria para proteger el interés vital del interesado

Esta justificación hace referencia a circunstancias de vida o muerte de las personas. Es decir, cuando este es necesario para la sobrevivencia de una persona. De esta forma, el mismo sería aplicable en situaciones de emergencia como puede ser que el interesado o titular está inconsciente o imposibilitado de otorgar el consentimiento. En este sentido, el considerando 46 del Reglamento General de Protección de Datos señala lo siguiente en relación a esta base de legitimación del tratamiento:

> "*El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos*

importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano."

e. *Tratamiento basado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*

Podría ser una tarea compleja enlistar las circunstancias en las cuales esta base de legitimación podría ser utilizada. Esto dato que si bien resulta claro que se podría solicitar información para cumplir con un interés público o el ejercicio de un poder público, son las leyes locales las que deben definir cuando esta circunstancia podrá servir de base para el tratamiento de datos personales.

Sobre esta base de tratamiento, el Reglamento General de Protección de Datos de la Unión Europea, en el artículo 21 ha señalado que los titulares en cualquier momento podrán oponerse al tratamiento de datos personales con base en esta justificación. En caso de que esto ocurra, señala este artículo que "*El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones."*

La Ley de Datos recoge esta justificación, sin embargo, la misma se incluye en el artículo 8 como una excepción a la autodeterminación informativa y no como una justificación de tratamiento como debería ser toda vez que, estas razones no podrían desaplicar el derecho mencionado sino, ser únicamente una justificación para el tratamiento de datos personales.

VI. CONCLUSIÓN

El tratamiento de datos personales es sin duda necesario para el correcto funcionamiento de la sociedad en este sentido, más allá de prohibir la recopilación de los datos personales se debe abogar por el balance adecuado entre el respeto a la autodeterminación informativa y un manejo de datos personales que no imponga trabas innecesarias (o imposibles de cumplir) en su tratamiento.

Es por lo anterior que más allá de tener al consentimiento informado como regla general para el manejo de datos personales tal y como ocurre con la Ley de Datos, lo necesario es incluir diversas razones o justificaciones que se puedan utilizar para el tratamiento de datos personales y así lograr el balance necesario.

En consecuencia, resulta importante que el uso que se haga de los datos personales se ajuste a la justificación con la cual fueron recopilados. De lo contrario, se estaría incumpliendo con otros principios como podría ser la adecuación al fin, uso de datos personales sin la debida justificación, entre otros.

VII. REFERENCIAS BIBLIOGRAFICAS

Constitución Política de Costa Rica. 7 de noviembre de 1949.

Davara, I, Barco, G y Cervantes, A (2019). Diccionario de Protección de Datos Personales. Conceptos Fundamentales (Primera Edición). México: INAI.

Guía para el cumplimiento del deber de informar", Agencia Española de Protección de Datos. Disponible en: https://www.aepd.es/es/documento/guia-modelo-clausula-informativa.pdf-0

INAI. (2016). Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, p. 18. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. Ley Nº 8968. 7 de julio del 2011

Reglamento de actuación de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales en el Poder Judicial. Ley N° 8968. 11 de agosto de 2014

Reglamento General de Protección de Datos de la Unión Europea. 2018/1725.

Sala Constitucional en el voto N° 754- 2002, de las 13:00 del 25 de enero de 2002.

Tribunal de Justicia de la Unión Europea. Sentencia del 11 de noviembre del 2020 del caso C-61/19.

JUAN ESTEBAN DURANGO RAVE

- Licenciado en Derecho de la Universidad Latinoamericana de Ciencia y Tecnología.
- Máster en Ciberderecho por la Universidad Católica de Murcia España.
- Asesor legal en Derecho Digital en la firma GoLegal
- jdurango@golegalcr.com

6



Acreditación de las Actuaciones Electrónicas Personales: de la Firma Electrónica a la Identidad Digital Auto-Soberana

Juan Esteban Durango Rave
Licenciado en Derecho de la Universidad Latinoamericana de Ciencia y Tecnología.
Máster en Ciberderecho por la Universidad Católica de Murcia España.
Asesor legal en Derecho Digital en la firma GoLegal
jdurango@golegalcr.com

Resumen

Un usuario promedio se expone a diario a cientos de interacciones recíprocas a través de entornos digitales, no solo con otras personas, sino también con plataformas digitales que prestan diversos servicios. Lo anterior representa retos que surgen de la forma en que dichos participantes acreditan sus actuaciones electrónicas, mecanismo que será fundamental para determinar la confianza entre las partes. Es aquí donde convergen en un solo ecosistema la necesidad de identificarse y manifestar el consentimiento a través de firmas electrónicas, criptografía, tecnología fiable, sistemas informáticos de autenticación y la identidad digital, todo bajo las reglas de la legalidad que otorga el ordenamiento jurídico. Lo que este texto plantea es un estudio de la eficacia y validez jurídica de los métodos de acreditación electrónica conocidos para personas físicas y disponibles en la actualidad, así como la manera en que éstos pueden generar confianza entre las personas bajo un contexto digital.

Palabras clave: firma electrónica, firma digital, certificado digital, criptografía, tecnología de llave pública, acreditación electrónica, autenticación, identidad digital, identidad digital auto-soberana.

SUMARIO

Introducción – I. FIRMA ELECTRÓNICA – a.- Antecedentes de la firma – b.- La Firma Electrónica – II. FIRMA DIGITAL Y FIRMA DIGITAL CERTIFICADA – III. IDENTIDAD DIGITAL – a.- Identidad Digital Auto-Soberana – IV. CONCLUSIONES – Referencias bibliográficas.

ACCREDITATION OF PERSONAL ELECTRONIC ACTIONS: FROM ELECTRONIC SIGNATURE TO SELF-SOVEREIGN DIGITAL IDENTITY

Abstract

An average user is exposed daily to hundreds of reciprocal interactions through digital environments, not only with other people, but also with digital platforms that provide various services. The foregoing represents challenges that arise from the way in which participants certify their electronic actions, a mechanism that will be essential to determine trust between the parties. In this digital ecosystem converge needs to identify and express consent through electronic signatures, cryptography, reliable technology, computerized authentication systems and digital identity, all under the rules of legality granted by the legal system. What this text raises is a study of the efficacy and legal validity of the electronic accreditation methods known to individuals and currently available, as well as the way in which they can generate trust between people in a digital context.

Keywords: electronic signature, digital signature, digital certificate, cryptography, public key technology, electronic accreditation, authentication, digital identity, self-sovereign digital identity.

INTRODUCCIÓN

Las acreditaciones electrónicas son mecanismos facilitadores de confianza en los actuales entornos digitales, en la actualidad los más conocidos para personas físicas son las firmas electrónicas, firmas digitales, los certificados digitales y la autenticación de la identidad digital, la cual[151] con el ingreso de la Identidad Digital Auto-Soberana, promete un cambio revolucionario a la manera en que las personas gestionarán su identidad digital en el futuro.

Estos métodos de acreditaciones requieren el análisis de sus complejidades técnicas a la luz de lo dispuesto no solo por las leyes locales, sino por el Derecho Internacional, en el entendido que el mundo digital es un fenómeno local y global, por lo tanto, la doctrina y la regulación internacional, juegan un papel preponderante para realizar el análisis de estos instrumentos legales.

Nos adentramos en el estudio de una materia no muy explorada por el jurista, en parte por el desconocimiento de la terminología y los conceptos técnicos que envuelve su abordaje, por lo que será la ambición de este de este texto ser claro en el desarrollo de sus ideas logrando hacerse entender por la mayor cantidad de lectores.

Proponemos por lo tanto, el abordaje desde el concepto tradicional e histórico de la firma manuscrita, hasta llegar a los mecanismos que prometen ser en el futuro, los idóneos para la gestión de las acreditaciones electrónicas, como es el caso de la Identidad Digital Auto-Soberana.

I. FIRMA ELECTRÓNICA

a.- Antecedentes de la firma

La firma como elemento de identificación y manifestación de la voluntad tiene su origen en el uso de troqueles, anillos o sellos, los cuales fueron utilizados por personas o reinos para identificarse, dejando su marca única en objetos,

superficies o documentos oficiales[1]. Siglos más tarde, dichas prácticas dieron paso a la utilización de sello y firma manuscrita en el mismo acto, ésta última al ser realizada por la persona siempre de la misma manera se le conoció con el nombre de rúbrica[2], un signo único e ilegible la mayoría de las veces y que a través de la historia moderna ha sido utilizada por las personas para firmar documentos.

Desde entonces, la firma manuscrita, firma ológrafa[3] o autógrafa, es decir, aquella escrita a mano por su mismo autor, ha sido el principal instrumento utilizado por las personas para identificarse o manifestar su consentimiento relativo al contenido de un documento en formato físico. La Real Academia Española [RAE] (s.f.) en una de sus acepciones define la firma como el "rasgo o conjunto de rasgos, realizados siempre de la misma manera, que identifican a una persona y sustituyen a su nombre y apellidos para aprobar o dar autenticidad a un documento" (definición 2). De acuerdo con estas definiciones, es frecuente encontrar en nuestro ordenamiento el término de rúbrica como sinónimo de firma.

La firma se puede entender como un signo asociado a una persona y que la vincula con un acto específico, tal como lo expresa el autor colombiano Peña (2015) quien señala que la firma es el signo "por el cual el individuo se expresa mediante un acto físico en el que manuscribe sus iniciales o nombres y apellidos en las actividades de la vida cotidiana, en sus relaciones personales,

---

[1] "Los sellos empezaron teniendo forma circular o de disco y después cilíndrica, siendo originalmente de piedra y posteriormente de otros materiales entre los que el lapislázuli era muy apreciado; estaban grabados en su superficie con imágenes de dioses o con símbolos de poder. Con ellos se imprimía sobre la arcilla fresca o se sellaban puertas o tinajas. Es un objeto personal que identifica a su poseedor, de ahí que se utilizara por los que de una u otra manera ostentaba algún poder" (Robles, 2015, p. 39).

2 "Rasgo o conjunto de rasgos, realizados siempre de la misma manera, que suele ponerse en la firma después del nombre y que a veces la sustituye" (Real Academia Española, s.f.,definición 1).

[3] También hológrafa.

económicas y desde luego jurídicas". De ahí que el mismo autor llame este tipo de firma como *firma-signo*[4], siendo el instrumento que identifica al firmante y a la vez otorga certeza no solo de la firma sobre el documento, sino que además permite asociar la voluntad del firmante respecto del contenido del documento, por lo tanto, bajo estas características, la *firma-signo* goza de plena validez jurídica.

Es innegable por lo tanto, la trascendencia jurídica que alcanza la firma manuscrita por ser el instrumento idóneo a través del cual el firmante manifiesta su voluntad con respecto al contenido de un documento, no solo vinculándose jurídicamente con lo que expresa, sino además como bien señala Peña (2015) obligándose frente a terceros bajo ciertas circunstancias. A lo anterior podría agregarse otros propósitos de la firma y es cuando ésta se consigna en un documento por el hecho de que la persona quiera dejar constancia que estuvo en un lugar, un día y una fecha determinada, tal es el caso cuando en algunas instituciones académicas los docentes solicitan la firma manuscrita a los alumnos para dejar prueba de su asistencia a clase, también al ingresar en algunos edificios, el encargado de la seguridad exige la firma a todas las personas que ingresan a las instalaciones.

Si bien en la normativa costarricense no existe una definición jurídica de firma, el Tribunal Primero Civil (2009) desarrolló el concepto destacando que la firma es lo que permite crear un nexo entre el documento y la persona, ésta puede ser una rúbrica (no ser legible) y su función primordial es servir como instrumento no solo de la autenticidad del documento, sino también de la manifestación de

[4] La *firma-signo* es un concepto propuesto por Peña (2015) para representar la unión inescindible entre un sujeto y su representación.

voluntad del firmante[5]. Según lo anterior, es aceptable afirmar que la firma debe reunir las siguientes características: hecha a mano por su propio autor, vinculación y atribución del firmante con la aceptación del contenido del documento; identificar al autor de la firma a través de rasgos y patrones únicos atribuibles a esa persona (datos biométricos) y ser perdurable o longeva (integra).

b.- La Firma Electrónica

El desarrollo doctrinal de la firma electrónica se origina en el Derecho Mercantil Internacional, de manera precisa en los trabajos realizados por la Comisión de las Naciones para el Derecho Mercantil Internacional (CNUDMI), quienes desde la década de los años noventa observaron la importancia de las crecientes transacciones internacionales por medio del comercio electrónico, por lo cual desde entonces, la Asamblea General de la ONU ha procedido a la redacción y publicación de leyes modelo.

Las Leyes Modelo de la CNUDMI son disposiciones que persiguen la adopción de su texto en los países miembro y que al momento de elaborar las leyes internas, se inspiren en sus preceptos para lograr armonizar la regulación de los Estados en materia de comercio electrónico, mejorando no solo las relaciones económicas entre países con sistemas jurídicos diferentes, sino permitiendo a las empresas y ciudadanos de cada país participar con seguridad jurídica en un

---

[5] "*La firma es el lazo que une al firmante con el documento en que se pone, el nexo entre la persona y el documento. Para establecer ese lazo, la firma no necesita ni ser nominal ni ser legible; esto es, no requiere expresar de manera legible el nombre del firmante. La función primordial de la firma no es la identificación del firmante, sino la de ser el instrumento de su declaración de voluntad, que exige esa actuación personal del firmante en la que declara que aquello es un documento y no un simple borrador, además de que el firmante asume como propias las manifestaciones, declaraciones o acuerdos que contiene*". (Tribunal Primero Civil, 2009, Considerando III).

entorno global donde cada día más prevalecen las comunicaciones electrónicas (CNUDMI, 1996, pág. 80).

Con dicho propósito, la CNUDMI a través de la Asamblea General de la ONU aprueba diferentes Leyes Modelo en materia de Comercio Electrónico: en 1996 la Ley Modelo de la CNUDMI sobre Comercio Electrónico (LMCCE), años más tarde en el 2001, publica la Ley Modelo de la CNUDMI sobre Firmas Electrónicas (LMCFE) y en el año 2017, la Asamblea General aprueba la resolución para la publicación de la Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos (LMCDTE).

En la LMCCE, la CNUDMI (1996) plantea un nuevo criterio denominado “criterio de equivalencia funcional”, el cual se basa en analizar los principales objetivos y funciones de los requisitos impuestos a los actos escritos sobre papel y de esta forma determinar cómo cumplir estos objetivos y funciones bajo las técnicas y parámetros del Comercio Electrónico (pág. 20). Diversos ordenamientos en la actualidad han establecido la equivalencia funcional como un principio jurídico pilar en materia de Comercio Electrónico y Firma Electrónica. Desde la doctrina se ha desarrollado este concepto, de manera concreta Illescas Ortiz (como se citó en Torres, 2012) afirma que:

> La función jurídica que en toda su extensión cumple la instrumentación escrita y autógrafa – o eventualmente su expresión oral – respecto de cualquier acto jurídico, la cumple igualmente su instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, dimensión, alcance y finalidad del acto así instrumentado. La equivalencia funcional, en suma, implica aplicar a los mensajes de datos electrónicos una pauta de no discriminación respecto a las declaraciones de voluntad o ciencia manual, o gestualmente efectuadas por el mismo sujeto (pág. 7).

En consecuencia, no se impondrán requisitos legales más exigentes a los actos electrónicos que los ya establecidos a los actos escritos, físicos o presenciales, de tal manera que no se le negarán o restrinjan efectos jurídicos a un acto electrónico por el mero hecho de serlo, entendiéndose de manera equivalente los actos, documentos o comunicaciones en formato físico, como aquellos en formato electrónico. En este sentido, en la Ley Modelo sobre Comercio Electrónico, la CNUDMI (1996) para desarrollar el criterio de equivalencia funcional, consideró atribuir a la firma sobre papel las siguientes funciones: identificar a una persona; dar certeza de su participación en el acto de firmar; y asociar a esa persona con el contenido del documento. Por lo anterior, la CNUDMI señala que la adopción del principio de equivalencia funcional no deberá dar lugar a la imposición de normas de seguridad más estrictas a los usuarios en el marco del comercio electrónico, que los requisitos ya aplicables a la documentación consignada en papel (pág. 28).

En materia de firmas electrónicas, la CNUDMI (2001) a través de la LMCFE recomienda que los Estados al momento de incorporar esta Ley Modelo en su derecho interno, deberán tener en cuenta sus principios básicos: equivalencia funcional, neutralidad tecnológica, no discriminación entre las firmas electrónicas nacionales y extranjeras, la autonomía de las partes y el origen internacional de la Ley Modelo.

La neutralidad tecnológica es de igual forma un principio jurídico promovido y adoptado a nivel global, así la OCDE (2007) señaló que los países miembros apoyan el uso de firmas electrónicas como equivalentes a las firmas manuscritas y abogan por la neutralidad tecnológica en su uso. En lo relativo al comercio electrónico, este principio se define según Ibáñez y Rincón (como se citó en Torres, 2012) como aquel que propende que las normas del comercio electrónico puedan abarcar las tecnologías que propiciaron su reglamentación, junto con las tecnologías que se están desarrollando y están por desarrollarse (pág. 134). En

el mismo sentido, Madrid Parra (como se citó en Torres, 2012) afirmo que en cumplimiento de este principio, “el legislador dictará normas cuya aplicación no suponga una adopción por una determinada tecnología” (pág. 135).

Desde la perspectiva del Derecho Administrativo, la neutralidad tecnológica se le impone al Estado como una garantía hacia al administrado en la prestación de servicios y acceso a la información, así como una garantía de imparcialidad en la contratación administrativa. De acuerdo con la Procuraduría General de la República (2004) el Estado debe establecer un marco jurídico favorable a la competencia. Dicho régimen estaría basado en el principio de “neutralidad tecnológica”, lo que permitiría la propagación de las tecnologías de la información y la comunicación y un acceso más asequible a estas. De igual forma aclara la PGR, la “neutralidad tecnológica” entrañaría que el Estado no puede tomar decisiones que tiendan a favorecer la utilización de una determinada tecnología por encima de otra.

Desde el punto de vista normativo, el principio de neutralidad tecnológica se regula en el artículo 3, inciso h de la Ley de Telecomunicaciones No. 8642 como parte de sus principios rectores y en general ordena que es la posibilidad que tienen los operadores de redes y proveedores de servicios de telecomunicaciones para escoger las tecnologías por utilizar, siempre que estas dispongan de estándares comunes y garantizados (Asamblea Legislativa de La República de Costa Rica, 2008).

En Costa Rica, el legislador se inspiró en estos principios[6] para regular lo relativo a documentos electrónicos y firmas digitales a través de la “Ley de Certificados, Firmas Digitales y Documentos Electrónicos No. 8454”, al establecer en el artículo 2 los principios de: regulación legal mínima, autonomía de la voluntad de los particulares para reglar sus relaciones e igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas. Así mismo, el artículo 3 establece el reconocimiento de la equivalencia funcional a toda manifestación con carácter representativo o declarativo transmitida por un medio electrónico o informático, imponiendo igualdad jurídica a los documentos o comunicaciones electrónicas o físicas. Mientras que el artículo 4 ordena que los documentos electrónicos tendrán fuerza probatoria en las mismas condiciones que los documentos físicos.

Si bien la ley 8454 adopta los principios de la LMCFE, carece en su normativa de una definición y desarrollo jurídico del concepto de firma electrónica, al contrario de otros ordenamientos como el de México, Colombia, Panamá o Europa, siendo que en nuestro país el legislador al regular lo relativo a firma electrónica, ha decidido utilizar el término Firma Digital, alejándose de la terminología utilizada no solo por la LMCFE, sino del concepto que en la actualidad prevalece en el Derecho internacional, lo cual es el concepto de firma electrónica.

Para desarrollar el concepto de firma electrónica, se recogerá lo normado en el ordenamiento costarricense, la jurisprudencia, así como lo erigido por el Derecho comparado y los preceptos de la LMCFE, en el entendido que la LMCFE son

---

[6] De acuerdo con la CNUDMI, Costa Rica figura como uno de los países que se ha inspirado y ha incorporado en su ordenamiento local la Ley Modelo sobre Firmas Electrónicas y sus principios: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures/status

recomendaciones para la incorporación en los ordenamientos jurídicos internos, por lo tanto, no es limitante recoger sus principios y normas para interpretar los vacíos que pueda tener nuestra legislación en el tema.

En su artículo 2 inciso a), la LMCFE (2001) define firma electrónica como:

> Los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos (pág. 1).

Acotado a lo anterior, la LMCFE reconoce que la finalidad de los mecanismos de firma electrónica es desarrollar medios técnicos que ofrezcan características de las firmas manuscritas en entornos electrónicos.

En Costa Rica, si bien el concepto de firma electrónica no se incluye en la Ley 8454, sí existe normativa desde la década de los noventa que ya regulaba este instrumento, tal es el caso de la Ley General de Aduanas de 1995, en la cual La Asamblea Legislativa de La República de Costa Rica (1995) define firma electrónica como el “Resultado de obtener, mediante mecanismos o dispositivos, un patrón, que biunívocamente se asocie a una persona física o jurídica y a su voluntad de firmar” (Art. 266, inciso 11), así mismo en sus artículos del 103 al 106, se equipara el código de usuario y la clave de acceso confidencial asignada a los funcionarios aduaneros, con la firma electrónica y a su vez a ésta con la firma autógrafa, así el artículo 103 en su segundo párrafo ordena que “Las firmas autógrafas que la Dirección General de Aduanas requiera podrán ser sustituidas por contraseñas o signos adecuados, como la firma electrónica, para la sustanciación de las actuaciones administrativas que se realicen por medios informáticos”. De igual forma el artículo 105 en su segundo párrafo que establece

que “Para todos los efectos legales, la clave de acceso confidencial y/o firma electrónica equivale a la firma autógrafa de los funcionarios, auxiliares y demás usuarios”.

De forma semejante, La Corte Suprema de Justicia (2013) en el Reglamento sobre Expediente Judicial Electrónico ante el Poder Judicial, en su artículo 2, establece como requisitos para la validez de las piezas procesales la firma digital, electrónica y holográfica, pudiendo ser dicha firma: la firma digital certificada; firma electrónica mediante registro como usuario en el Poder Judicial; y la firma holográfica mediante dispositivo o capturador de firmas utilizado por despachos y fiscalías electrónicas. Ejemplo de lo anterior se puede apreciar en las sentencias firmadas por los Jueces y Magistrados de la Corte Suprema de Justicia, quienes estampan una firma electrónica holográfica en sus resoluciones judiciales.

La jurisprudencia ha ampliado los criterios del artículo 2 del Reglamento supra al considerar una comunicación firmada electrónicamente como aquella enviada a través del correo electrónico del usuario inscrito ante el sistema de gestión del Poder Judicial, la Sala Tercera (2019) en resolución afirmó que:

> es posible concluir entonces que pese a la ausencia de la firma, en caso de que el documento se remita desde una cuenta de correo electrónico validada por la institución se consideraría válido para todos los efectos, en el tanto, se entendería firmado electrónicamente (Considerando III).

Por otra parte y acudiendo a la doctrina internacional, el autor Alamillo Domingo (2019) manifiesta que la firma electrónica es “un artefacto técnico que va a ser reconocido jurídicamente en función de una serie de propiedades que lo hacen relevante como fuente de prueba electrónica, al objeto de atribuir un documento a una persona y, en su caso, también identificar a dicha persona” (pág. 335).

Para mayor amplitud en la definición del concepto en el marco del derecho comparado, estas son algunas definiciones adoptadas en las regulaciones extranjeras:

1.- Argentina

La Ley 25.506 de Firma Digital del 2001, en el artículo 5 denomina firma electrónica "al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales ser considerado firma digital. En caso de ser desconoce la firma electrónica corresponde a quien la invoca acreditar su validez" (Honorable Congreso de la Nación Argentina, 2001).

2.- Colombia

La Ley 527 de 1999 regula lo relativo a firma electrónica en el artículo 7, señalando que:

> Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si: a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación; b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.
>
> Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma. (Congreso de Colombia, 1999).

Consiente de la importancia de la firma electrónica como un instrumento de seguridad jurídica necesario para la realización de negocios en el marco del comercio electrónico, La Presidencia de La República emite el Decreto 2364 del año 2012, en el cual se reglamenta el artículo 7 de la Ley 527 de 1999, por lo que en el artículo 3 se establecen los criterios y métodos técnicos que pueden ser considerados como firma electrónica, tales como: “códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente” (Presidencia de La República, art. 3).

3.- Estados Unidos

La UETA Act (The Uniform Electronic Transactions Act) y la E-Sign Act (Electronic Signatures in Global and National Commerce Act) son las dos leyes que regulan la firma electrónica en Estados Unidos. La UETA fue promulgada en 1999 y ha sido a su vez incorporada por 49 Estados, este marco normativo establece la equivalencia legal de los registros electrónicos con los documentos en papel firmados manualmente, así mismo la E-Sign del año 2000, es una ley federal que busca facilitar el uso de registros electrónicos y firmas entre Estados y en el Comercio Internacional. Ambas leyes coinciden en señalar que la firma electrónica es un sonido electrónico, símbolo o proceso adjunto o lógicamente asociado a un registro (E-Sign incluye “contrato”) y ejecutado o adoptado por una persona con la intención de firmar (UETA Sección 2 inciso 7, E-Sign Sección 106 inciso 5).

4.- Unión Europea:

Por su parte, la Unión Europea a través del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de junio de 2014 (Reglamento eIDAS), regula lo referente a identificación electrónica, servicios de confianza y transacciones electrónicas dentro de la comunidad europea, estableciendo un marco de confianza y seguridad jurídica no solo para los más de 500 millones de ciudadanos que la conforman, sino para todo aquel que realiza transacciones electrónicas en este mercado. De acuerdo con el artículo 3, inciso 10, se entiende por firma electrónica "los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar. (Parlamento Europeo y el Consejo, 2014).

5.- México:

La definición de firma electrónica en México se incluye en el Código de Comercio y se inspira de manera clara en los preceptos de La Ley Modelo de la CNUDMI sobre Firmas Electrónicas, en ese sentido, el artículo 89 consagra que firma electrónica son:

> Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio (Cámara de Diputados, Código de Comercio, 1889).

6.- Panamá

La Ley 51 de 2008 panameña que regula los documentos electrónicos y las firmas electrónicas, inicialmente definió firma electrónica como el "conjunto de sonidos, símbolos o datos vinculados con un documento electrónico, que ha sido

adoptado o utilizado por una persona con la intención precisa de identificarse y aceptar o adherirse al contenido de un documento electrónico" (Art. 2 inciso 20), pero luego, a través de la Ley 82 de 9 noviembre de 2012 se modifica dicha definición, por lo que a partir de esa reforma, el artículo 2, inciso 20 de la Ley 51 de 2008 define firma electrónica como el "Método técnico para identificar a una persona y para indicar que esa persona aprueba la información que figura en un mensaje de datos o documento electrónico" (Asamblea Nacional, Ley 82 de 2012, Art. 7).

7.- Perú

El ordenamiento jurídico de Perú, regula la firma electrónica en la Ley 27269 Ley de Firmas y Certificados Digitales, dicho marco normativo entiende por firma electrónica "cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita" (Art. 1 párr. 2). Así mismo su ámbito de aplicación aplica a las firmas electrónicas añadidas o asociadas lógicamente a un mensaje de datos y que puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos (El Congreso de la República, 2000).

Visto lo anterior, se destaca la amplia adopción a nivel jurídico del concepto de firma electrónica en las diversas jurisdicciones revisadas, las cuales han adoptado o al menos seguido los preceptos y definiciones de la Ley Modelo Sobre Firmas Electrónicas, de manera que ordenamientos como el de Argentina, Estados Unidos, Europa, México, Panamá y Perú, permiten interpretar de sus redacciones que la firma electrónica es un mecanismo a través del cual se consignan, vinculan, adjuntan, integran, añaden, anejan o asocian datos electrónicos a un mensaje de datos (documento electrónico) y que éstos datos a su vez deben permitir identificar y vincular al firmante con el contenido del

documento y el mismo acto. Si bien las definiciones del ordenamiento colombiano no incluyen las acepciones aquí descritas, si contempla criterios técnicos más precisos acerca de los mecanismos que pueden ser considerados como firma electrónica: códigos, contraseñas, datos biométricos, o claves criptográficas privadas.

La firma electrónica es un procedimiento que está subordinado a la tecnología, debe ser no solo un mecanismo seguro que aporte la mayor cantidad de evidencias digitales para garantizar la veracidad del acto, sino además confiable para garantizar la identificación del firmante y la integridad del documento. En la firma electrónica prevalece el procedimiento técnico respecto al signo de la firma manuscrita y los métodos deben generar confianza en busca de la validez y eficacia probatoria, de manera acertada Peña (2015) llama a este instrumento *firma-método*.

La firma digital al ser un método ejecutado a través de un procedimiento digital y que a su vez permite reunir los criterios y requisitos de firma electrónica aquí estudiados, se considera en definitiva un tipo de firma electrónica, una especie de ésta. Es por lo anterior, que los preceptos y principios que rigen la firma digital en el ordenamiento costarricense a través de la Ley No 8454, son extrapolables y de aplicación al uso e implementación de cualquier otra firma electrónica. De esta forma y atendiendo a la normativa nacional e internacional repasada, a los principios de equivalencia funcional, neutralidad tecnológica y autonomía de las partes, así como también a los preceptos de las Leyes Modelos, se entiende que en el ordenamiento costarricense una firma electrónica podrá ser entre otras:

- El nombre de usuario y su clave de acceso confidencial a un sistema informático.

- La clave de un solo uso OTP (*One Time Password*) para ingresar a un sistema informático o para ejecutar cualquier acto con consecuencias jurídicas.
- El PIN de una tarjeta de débito.
- La firma agregada al final de un correo electrónico.
- Un correo electrónico.
- Marcar una casilla en el navegador (*Clic-Wrap*) o la navegación dentro de un sitio web (*Browser-Wrap*).
- La firma autógrafa estampada con lápiz óptico o con el dedo sobre un dispositivo electrónico.
- Los datos biométricos del firmante adjuntos a un documento electrónico: huella digital, reconocimiento facial, un video, un sel-fie, un audio.
- Las firmas electrónicas emitidas al amparo de un certificado suministrado por un ente certificador o servicio de confianza.
- La Firma Digital.

Ante los diferentes tipos de firma electrónica que los mecanismos tecnológicos pueden ofrecer, es fundamental señalar bajo que criterios técnicos y jurídicos tendrán mayor validez legal y solidez probatoria la firma electrónica, es decir que ofrezca la necesaria confianza y fiabilidad para dar certeza de la identidad de la persona y la integridad del documento. La Ley Modelo sobre Firma Electrónica expresa los requisitos y características de lo que se considera una firma electrónica fiable, en el artículo 3 la CNUDMI (2001) considera una firma fiable si: a) los datos de creación de la firma corresponden exclusivamente al firmante; b) los datos de creación de la firma estaban al momento de firmar, bajo el control exclusivo del firmante; c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma (integridad de la firma); y d) es posible detectar cualquier alteración de la información hecha después de firmar (integridad del documento).

Lo anterior es lo que la doctrina internacional considera como una firma electrónica fiable y en diversas jurisdicciones se ha regulado llamándola firma electrónica avanzada, tal es el caso del Reglamento eIDAS el cual considera como tal a la firma electrónica que cumple ciertos requisitos: estar vinculada al firmante de manera única, que permita la identificación del firmante, ser creada utilizando datos de creación con alto nivel de confianza y bajo control exclusivo del firmante y estar vinculada con los datos firmados de tal modo que una ulterior modificación de los datos sea detectable.

Similar definición ofrece el Código de Comercio Mexicano en el artículo 97, al establecer que una firma electrónica avanzada debe reunir las siguientes características: i) que los datos de creación de la firma correspondan exclusivamente al firmante; ii) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante; iii) poder detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y garantizar la integridad del mensaje de datos, es decir la no alteración del documento electrónico. Similares criterios consagra el Decreto 2364 de 2012 de Colombia, para considerar una firma electrónica confiable.

En Costa Rica no se hace mención dentro del ordenamiento al término firma electrónica avanzada, fiable o confiable. Sin embargo, las definiciones anteriores tanto la recogida por la Ley Modelo sobre Firmas Electrónicas como las de los diferentes ordenamientos jurídicos extranjeros, se asemejan de manera clara con los criterios plasmados en la definición de firma digital de nuestra Ley 8454. El artículo 8 en su primer párrafo expresa que firma digital es cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico. Por consiguiente, cuando hablamos de firma digital en nuestro ordenamiento estamos haciendo referencia

a una firma fiable o firma electrónica avanzada según la terminología en la materia aceptada mayoritariamente en el Derecho comparado.

De manera práctica y desde una perspectiva técnica ¿qué requiere una firma electrónica para ser fiable, avanzada o firma digital de acuerdo a nuestro ordenamiento? Existen en la actualidad múltiples plataformas que a través del uso de software y hardware ofrecen la posibilidad de realizar firmas electrónicas, éstas según las características técnicas podrán ser firmas electrónicas simples o avanzadas. Un caso para citar es el de una firma manuscrita o rúbrica plasmada con pluma digital o con el dedo sobre un dispositivo electrónico, dicho acto electrónico tendrá que valorarse a la luz del principio de equivalencia funcional y no podrá negársele efectividad jurídica, por ser este acto equivalente al de una persona que realiza la firma con pluma de tinta sobre un documento de papel.

Lo anterior es un ejemplo de firma electrónica simple, la cuál podría garantizar la identidad de la persona si durante la firma, un tercero verifico su rúbrica con la impresa en su documento de identidad, o bien si la realizó frente a terceros que han validado su identidad, es el caso de los repartidores de mercancías que para formalizar la entrega del producto o servicio, solicitan al receptor firmar sobre una tableta electrónica o sobre el teléfono móvil el cual contiene una aplicación para tal efecto, otro ejemplo es cuando en algunos bancos o empresas comerciales para recoger el consentimiento de los usuarios o clientes, solicitan la firma manuscrita sobre algún dispositivo electrónico, ya sea una tableta o un dispositivo con tecnología Wacom.

Si los casos descritos arriba el firmante negará la firma, dicha rúbrica podría ser cotejada y analizada en un peritaje informático. La eficacia de este peritaje dependerá en gran medida de las funcionalidades técnicas de la plataforma electrónica utilizada para la captura de la firma, ya que ésta podría recoger

rasgos personalísimos del firmante como lo son los datos biométricos, por ejemplo, la fuerza ejercida durante la realización de los trazos. Esta información sería confiable a la luz de los resultados obtenidos por el perito para comprobar la autenticidad de la firma. De modo similar sucede cuando una firma realizada con pluma sobre papel es repudiada por el firmante, ésta deberá ser analizada por un perito calígrafo quien realizará una prueba caligráfica para dar certeza sobre su autenticidad.

Sin embargo, para ser firma electrónica avanzada o firma digital (regulación costarricense) en el método anterior se está omitiendo el mecanismo que garantice la integridad y no alteración ulterior tanto de los datos como del propio documento electrónico, requisito pilar para considerar una firma fiable. La integridad es definida por el Reglamento 33018[7] como la propiedad de un documento electrónico que denota que su contenido y características de identificación han permanecido inalterables desde el momento de su emisión (Ministerio de Ciencia y Tecnología, 2006, art. 2.27). Por consiguiente, algunos mecanismos conocidos para garantizar la integridad del documento podrían ser, correr una función *hash* sobre el documento una vez firmado electrónicamente o estampar un sello de tiempo electrónico sobre todo el documento electrónico.

La función *hash* también se conoce como función resumen y es el resultado de obtener una versión reducida (resumida) de un mensaje de datos (Alamillo, 2018), esta versión resumida es una cadena de dígitos (*hash*) o digesto, obtenidos a partir del resultado de correr un algoritmo sobre el documento electrónico, es una huella digital única, por lo tanto, si ese documento electrónico origen es alterado en un solo *bit*, al volver a correr el algoritmo sobre el mismo documento el *hash* obtenido será diferente al primero, lo cual probará que el

[7] Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos No 33018.

documento ha sido modificado y ha perdido su integridad. Este mecanismo es utilizado por la informática forense para garantizar la cadena de custodia de las evidencias digitales, el *hash* obtenido al momento de recopilar la evidencia tendrá que ser el mismo *hash* al momento de presentarla ante el juzgador, si estos no coinciden querrá decir que la evidencia ha sido alterada.

Por otra parte, el sello de tiempo electrónico es un método conformado por “datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante” (Parlamento Europeo, Reglamento eIDAS, art. 3 inciso 33). Un sello de tiempo por lo tanto permite relacionar un conjunto de datos electrónicos con un tiempo específico, estableciendo certeza de que ese mensaje de datos existía en la fecha y hora que el sello fue estampado en el documento. En consecuencia, si el documento electrónico que ha sido estampado con el sello de tiempo es modificado, el sello de tiempo electrónico se destruye y el mensaje de datos o documento electrónica perderá su integridad.

Por lo tanto, si las partes acuerdan de manera previa manifestar el consentimiento a través de una firma manuscrita realizada sobre un dispositivo electrónico que capture los datos biométricos del firmante, que reúna además otras evidencias digitales que permitan identificar unívocamente al usuario: correo electrónico personal, sms, *one time password*, huella digital, intercambio de claves de acceso, y que de igual forma agregué un *hash* o un sello de tiempo electrónico sobre el documento una vez impuesta la firma, satisface los requisitos de integridad, identificación y vinculación jurídica exigida por el artículo 8 primer párrafo de la Ley 8454, pudiendo considerarse firma digital y atribuírsele el valor equivalente consagrado en el artículo 9 de la misma ley y en consecuencia tener el mismo valor y eficacia probatoria de su equivalente funcional firmado en manuscrito.

En resumen, no hay impedimento legal para utilizar firmas electrónicas en nuestro ordenamiento, a la luz de los principios de equivalencia funcional, neutralidad tecnológica y autonomía de las partes. De igual forma se podrá entender como firma electrónica avanzada, aquella que cumpla con los criterios exigibles de una firma fiable según la Ley Modelo sobre Firma Electrónica, o las características de la firma digital establecidas por el artículo 8 de nuestra Ley 8454.

II. FIRMA DIGITAL Y FIRMA DIGITAL CERTIFICADA

La firma digital desde un punto de vista técnico se asocia a un mecanismo numérico y matemático, de manera concreta a infraestructura de llave pública (tecnología PKI), por tal razón en diferentes ordenamientos lo han regulado desde esta perspectiva, así por ejemplo en Colombia la Ley 527 de 1999, define firma digital como un valor numérico que se adhiere a un mensaje de datos y que utiliza un procedimiento matemático para vincular al iniciador del mensaje (…) (art. 1.c), igualmente en Perú la Ley de Firmas y Certificados Digitales del año 2000, establece que la firma digital utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único (…) (art. 3); Argentina en su Ley de Firma Digital No 25.506 del 2011, expresa que por firma digital se entiende el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante (…) (art. 2).

En Costa Rica mientras tanto, ni en la Ley 8454 ni el Reglamento 33018[8] de manera expresa se atribuye a la firma digital un método asociado a un mecanismo numérico o matemático, decantándose más el legislador por otorgarle a la firma digital la definición de firma electrónica avanzada ya analizada anteriormente, esto se deduce al considerar en el artículo 8 de la Ley,

[8] Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos No 33018.

que los datos electrónicos de la firma se adjuntan al documento electrónico a través de un proceso lógico y no matemático o criptográfico. De acuerdo con lo anterior, es factible considerar que el legislador de manera un poco confusa definió firma digital acercándose más al significado de firma electrónica fiable, en vez del significado técnico de firma digital como instrumento asociado a un mecanismo matemático. Una redacción más armoniosa con la doctrina dominante hubiera sido llamar a la firma digital, firma electrónica avanzada.

Por otra parte, no debe confundirse firma digital con firma digitalizada, la cual se considera es una firma electrónica con muy poco valor probatorio y por lo tanto de escaza eficacia jurídica. La firma digitalizada es la que agrega una imagen de una firma manuscrita a un documento electrónico, o la firma manuscrita estampada en un documento físico y luego escaneada (digitalizada). Bajo estos supuestos, dicha firma no logrará cumplir con los requisitos mínimos de atribución e identificación que debe reunir una firma electrónica, mucho menos con los requisitos de una firma electrónica avanzada. Por lo tanto, no se recomienda su utilización, este criterio ha sido además manifestado por La Sala Tercera de la Corte (2008) al afirmar que la rúbrica debe interpretarse en un sentido amplio y no perderse de vista que de acuerdo con los avances tecnológicos, la firma hológrafa ha evolucionado a la firma digital, concepto que no equivale a la digitalización de la signatura (escaneo) (Resolución Nº 00941 - 2008).

Continuando con el análisis de la firma digital desde una óptica técnica, Alamillo (2019) acota que el algoritmo de firma digital se basa en una cifra asimétrica, formada por una clave pública y otra privada, que permite “firmar” documentos con la clave privada y verificar la firma digital con la clave pública. Criptográficamente, firmar digitalmente es generar un dato matemático asociado al objeto digital (pág. 40). Es por esta razón que la infraestructura de llave pública se considera uno de los mecanismos mas seguros para firmar electrónica

o digitalmente un documento, ya que este método permite verificar el emisor del mensaje de datos y la integridad del documento.

Sin embargo, Peña (2015) sostiene que la firma digital *per se* no genera confiabilidad técnica completa respecto del autor o emisor del mensaje de datos, sino únicamente respecto del mensaje. Para este último fin es necesario que la ley establezca una presunción, de manera que es el certificado digital emitido por una autoridad certificadora, el instrumento a través del cual se atribuye esta presunción legal a la firma digital, denominándola Firma Digital Certificada.

Dicho lo anterior, se entenderá por certificado todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma (CNUDMI, 2001, art. 2.b). El Reglamento eIDAS por su parte, define que el certificado de firma electrónica es una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona; mientras que el certificado cualificado de firma electrónica es un certificado que ha sido expedido por un prestador cualificado de servicios de confianza (Art. 3, incisos 14 y 15).

La Ley de Certificados, Firmas Digitales y Documentos Electrónicos No 8454, en el artículo 11 señala que un certificado digital es un mecanismo electrónico o digital mediante el que se puede garantizar, confirmar o validar técnicamente: a) la vinculación jurídica entre un documento, una firma digital y una persona; b) la integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada; c) la autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras.

Por consiguiente, la diferencia entre firma digital y firma digital certificada la otorga el certificado digital que ampara a esta última, dicho certificado emplea

criptografía de clave pública y clave privada y deberá ser emitido por una autoridad certificadora autorizada por la Dirección de Certificadores de Firma Digital (DCFD) una dependencia del Ministerio de Ciencia, Tecnología y Telecomunicaciones, que se encarga de la administración y supervisión del sistema de certificación digital. La autoridad certificadora deberá cumplir con lo establecido en la Sección II de la Ley, lo dispuesto en el Reglamento, así como los requerimientos técnicos de la Política de Certificados para la jerarquía nacional de certificadores registrados, entro otros requisitos. En la actualidad es el Banco Central de Costa Rica, el único emisor de certificados digitales autorizado y reconocido por la DCFD, siendo el servicio de confianza exclusivo en el país para la emisión de certificados digitales.

La Firma Digital Certificada es emitida por un tercero de confianza autorizado (Autoridad Certificadora del SINPE del Banco Central de Costa Rica). Para emitir un certificado al solicitante, los emisores quien a su vez son oficinas autorizadas para emitir certificados de la Autoridad Certificadora del SINPE, deberán validar de manera presencial la identidad del solicitante del certificado digital, una vez esta persona ha pagado los costos de solicitud de la firma y ha cumplido con el resto de requisitos, el emisor emite y entrega al solicitante una tarjeta que contiene un chip con los certificados digitales (un certificado de firma y un certificado de identificación), así como la llave pública y privada de los certificados, un dispositivo físico para insertar la tarjeta y un PIN, dichos elementos conforman lo que se conoce como la Firma Digital Certificada. Posteriormente la persona titular del certificado deberá instalar en su equipo de cómputo el firmador (software de la firma), para poder utilizar la tarjeta y el dispositivo de la Firma Digital Certificada, de esta forma, podrá estar listo para firmar documentos electrónicos y autenticarse en portales bancarios o de instituciones públicas.

Respecto a su fuerza probatoria, solamente a la Firma Digital Certificada (FDC) se le atribuye presunción de autoría y responsabilidad (artículo 10 de la La Ley 8454), es decir que, salvo prueba en contrario, todo documento electrónico asociado a una FDC se presumirá, de la autoría y responsabilidad del titular del correspondiente certificado digital. Quien firme utilizando una FDC no podrá negar su consentimiento respecto a lo firmado y no podrá repudiar la firma, por lo cual tendrá la carga de la prueba si niega la autenticidad de ésta y tendrá que demostrar su invalidez.

De igual manera, el Reglamento No. 33018, señala la diferencia entre los efectos legales de los certificados digitales emitidos en el país por un certificador autorizado versus las firmas y certificados emitidos por otros certificadores, ya sea dentro o fuera del país, el artículo 10 le otorga pleno efecto legal frente a terceros y al Estado, a los certificados digitales expedidos por certificadores registrados ante la Dirección de Certificadores de Firma Digital.

Sin embargo, en el segundo párrafo de la norma, se establece que las firmas y certificados emitidos dentro o fuera del país que no pertenezcan a un certificador registrado ante la DCFD, no surtirán efectos por sí solos, pero podrán ser empleados como elemento de convicción complementario para establecer la existencia y alcances de un determinado acto o negocio.

Se entiende entonces, que la presunción legal no ocurre con la firma digital, que al no estar amparada en un certificado digital emitido por la autoridad certificadora, obliga a que la carga de la prueba sea para quien pretende demostrar la veracidad y validez de dicha firma. A la luz de lo dicho en el artículo 10 del Reglamento, del principio de equivalencia, neutralidad tecnológica y de autonomía de las partes, si la firma digital contiene un certificado digital emitido por otro certificador (local o extranjero) y el cual también emplea criptografía de clave pública, deberá ser aceptado éste por la autoridad judicial correspondiente

para que a través de un peritaje y otras evidencias digitales, se pueda llegar a la convicción de que el mecanismo técnico permite con certeza determinar de que la firma es auténtica y por lo tanto válida, en consecuencia, no se le podrá negar efectos jurídicos *ad portas* a un documento firmado con una firma digital certificada no emitida por la autoridad certificadora costarricense.

Tal caso se ha evidenciado en resoluciones de algunos Tribunales Civiles que han rechazado el cobro de títulos valores firmados con firmas electrónicas avanzadas (firma digital) y amparadas en certificados digitales de proveedores extranjeros, así en la resolución 0024-2019 del Tribunal de Apelación Civil y Trabajo de Alajuela (2019) el juzgador manifestó:

> En el asunto que nos ocupa, no hay pruebas de que S.L. se encuentre autorizada y registrada ante la Dirección de Certificadores de Firma Digital. En consecuencia, al documento aportado con la demanda no se le pueden atribuir los efectos propios de una firma digital certificada. A lo sumo, se le podría tener como un documento probatorio complementario, en los términos señalados en el párrafo segundo del artículo 10 del reglamento indicado. No obstante, el documento base de un proceso monitorio dinerario debe valerse por sí mismo; no siendo factible, al menos en esta vía privilegiada, que se le complemente con fuentes de prueba adicionales.

En el anterior caso, el juzgador rechaza de previo los efectos jurídicos de la firma al no estar amparada en un certificado emitido por autoridad certificadora nacional, sin entrar a valorar a través de un peritaje informático las características técnicas de la firma, procedimiento que podría demostrar o no la autoría, autenticidad e integridad de la firma y el documento electrónico. Entiende el Tribunal que el único método válido para firmar títulos valores es una Firma Digital Certificada, pero no hay ninguna norma en nuestro ordenamiento que así

lo ordene, sería el equivalente a exigir que la firma de un título valor tenga que venir autenticada por notario. Así mismo, de ser así como lo interpreta el Tribunal, personas que no pueden optar por un certificado digital, como lo son las personas extranjeras[9], o costarricenses que no residan en el país y por lo tanto no tienen acceso a una oficina de un emisor de certificados, tendrían un impedimento legal para firmar títulos valores en formato electrónico.

Lo que consagra la Ley 8454 en su artículo 9 es que la firma digital tiene valor equivalente y eficacia probatoria en las mismas condiciones que una firma manuscrita, por lo tanto, si la parte interesada demuestra que la firma electrónica estampada en el pagaré goza de integridad, identifica al deudor y lo vincula jurídicamente con el documento electrónico, dicha firma es equivalente a una firma manuscrita. Lo contrario sería negar no solo los preceptos del artículo 9 (valor equivalente), sino además impedir a la aplicación de los principios de equivalencia funcional, neutralidad tecnológica y autonomía de las partes.

En suma, la Ley Modelo sobre Firmas Electrónicas establece la no discriminación de las firmas electrónicas extranjeras, es decir, que el lugar de origen en sí no debe ser en ningún caso un factor para determinar si puede reconocerse la capacidad de los certificados extranjeros o las firmas electrónicas para tener eficacia jurídica en un ordenamiento jurídico, ya que la determinación de si un certificado o una firma electrónica pueden tener eficacia jurídica, y hasta qué punto pueden tenerla, no debe depender del lugar en que se haya emitido el certificado o la firma electrónica sino de su fiabilidad técnica (2001, pág. 43).

[9] De acuerdo con las Política de Certificados para la jerarquía nacional de certificadores registrados el documento de identidad, la cédula de residencia o la cédula jurídica (Anexo A).

Finalmente, la presunción legal de la Firma Digital Certificada solo es aplicable en las vías jurisdiccionales costarricenses, si dicha firma es utilizada para actos que tengan eficacia fuera de nuestra jurisdicción, será en ese ordenamiento jurídico que deberá demostrar su validez legal ante la autoridad judicial de acuerdo con los preceptos legales de ese país.

III. IDENTIDAD DIGITAL

En la actualidad gran cantidad de personas interactúan la mayoría de su tiempo en un entorno predominantemente digital, durante sus interacciones personales, sociales, educativas, culturales y económicas convergen con otras personas y sistemas informáticos a través del ciberespacio[10]. La gestión de la identidad en el entorno digital se convierte por lo tanto en piedra angular para la generación de confianza durante dichas interacciones, de lo contrario, las personas tendrían vedado acceder a recursos e información que requieren para la ejecución de sus actividades diarias: envío y recibo de correos electrónicos, realizar transacciones bancarias en línea, charlar en línea con colegas y familiares, interactuar en sus redes sociales, realizar trámites en portales de la administración pública, etc.

Se requiere por ende una identidad digital con un mínimo de fiabilidad que garantice en gran medida, que la persona es quien dice ser y es titular de los atributos que la identifican.

En el mundo de la identidad digital una información adjunta a la identidad de alguien o algo se denomina atributo de identidad (EU Blockchain Observatory Forum [EU BOF], 2019, pág. 12). El reto será entonces determinar cuáles serán esos atributos válidos considerando en principio que la identidad no es estática,

[10] Ciberespacio: Ámbito virtual creado por medios informáticos. RAE, Consultado Abril 28 de 2021. Recuperado de https://dle.rae.es/ciberespacio?m=form

es dinámica y es una colección de atributos individuales que describen una entidad y determinan las transacciones en las que esa entidad puede participar. Si bien la cantidad de atributos puede ser infinito, se pueden clasificar en tres grupos: i) atributos inherentes; ii) atributos acumulados; y iii) atributos asignados. Los primeros refieren a los atributos intrínsecos a la persona: edad, rasgos físicos, datos biométricos; los segundos son los atributos que son acumulados durante el tiempo: salud, preferencias y comportamientos, estudios; y los atributos asignados son aquellos que reflejan las relaciones que la persona mantiene con otros organismos: número de identificación nacional, correo electrónico, número de licencia (World Economic Forum, 2016, pág. 41).

La identidad digital para Peña (2015) sobresale cada vez más como el valor fundamental para el siglo XXI como atributo de la persona digital que participa, interactúa, consume y ejerce sus derechos al acceso a la información, a la comunicación, a la libre expresión y al desarrollo libre de la personalidad y de actividades comerciales y sociales relevantes.

Se entiende por lo tanto identidad digital como un conjunto finito de atributos que permite a una entidad ser identificado como única y probar su identidad frente a terceros electrónicamente, siendo factible que nuestra persona digital se componga a su vez de varias identidades digitales, las cuales podrán usar unos u otros atributos de acuerdo con el contexto (Allende, 2020, pág, 12). Cuando pensamos en la identidad digital, por lo tanto, se necesita ver no como una sola cosa, sino más bien como la suma total de todos los atributos que existen sobre la persona en el ámbito digital, una constante colección creciente y en evolución de puntos de datos (EU Blockchain Observatory Forum, 2019, pág. 12).

En otro orden de ideas, la identidad digital de acuerdo con Barros, Gómez, Pareja y Pedak (2017) puede clasificarse en:

i. Identidad digital legal: es la que requiere estar vinculada a la identidad legal de una persona física o jurídica. Es necesaria, por ejemplo, para realizar transacciones con el gobierno o con instituciones financieras reguladas.
ii. Identidad digital simple: es aquella que no requiere estar vinculada a una identidad legal física. Se utiliza, por ejemplo, para conectarse a redes sociales (pág. 7).

En Costa Rica es válido considerar que la identidad digital legal se gestiona a través del certificado digital de identificación emitido por la autoridad certificadora, la cual luego de un proceso de verificación y registro presencial (cara a cara) de la persona, procede el emisor a entregar el certificado al solicitante, para que ésta se identifique con plena presunción legal ante las instituciones públicas o privadas en el entorno digital. De esta forma se garantizará el no repudio de las actuaciones electrónicas del ciudadano en los entornos que acepten el certificado digital como medio de autenticación.

La identidad digital puede tener validez en un determinado dominio, para Barros et al (2017) puede ser válida únicamente para interactuar con una institución, empresa o en una red social determinada o puede, en cambio, tener un reconocimiento más general (por ejemplo, en un Estado). Esto implica que una persona física puede tener más de una identidad digital a través de múltiples dominios, y utilizar cada una para una función o contexto diferentes. Lo que no puedes suceder es que dos personas físicas tengan la misma identidad digital legal (pág. 7).

La gestión de los sistemas de identidad digital combinan procesos y tecnologías que potencian el uso de los datos identificatorios de las personas, y requiere: i) un modelo de gobernanza y un modelo de negocio; ii) un marco legal apropiado y actualizado; iii) la simplificación y estandarización de procesos y sistemas; iv)

el establecimiento de mecanismos de interoperabilidad que faciliten la coordinación entre los diferentes organismos, y v) la promoción y coordinación del ecosistema de uso de la identidad (Barros et al., 2017, Pág. 6). Dentro del marco legal apropiado se deberá considerar el tipo de identidad digital (legal o simple) a gestionar para determinar la forma de atribuir el vínculo jurídico, ya sea éste a través de la presunción legal otorgada por el ordenamiento a los certificados digitales de identificación o a través de un contrato privado (términos y condiciones, condiciones de uso, contrato de adhesión) que permitan atribuir efectos legales a las actuaciones electrónicas de la identidad digital simple dentro de ese dominio específico.

Como parte de la gestión de la identidad digital, es fundamental el proceso de autenticación, según la norma internacional ISO7IEC 2382:2015 (como se citó en Alamillo, 2019, pág. 57), la autenticación es el acto de verificar la identidad alegada por una entidad, por lo que se entiende que este mecanismo de verificación permitirá atribuir efectos legales a las actuaciones electrónicas de una persona física.

De acuerdo con el artículo 2 inciso 1 del Reglamento de Firma Digital, la autenticación para verificar la identidad de una persona puede ser de dos tipos: i) durante el proceso de registro donde se evalúan las credenciales de la entidad (persona), como evidencia de que realmente es quien dice ser; ii) durante el uso de la identidad, es el acto de comparar electrónicamente las credenciales y la identidad enviada (Ej., código de usuario y contraseña, certificado digital, etc.) con valores previamente almacenados para comprobar la identidad.

Según la Guía de Identidad Digital del NIST, el paradigma clásico de los sistemas de autenticación identifica tres factores como los pilares de la autenticación: i) algo que la persona sabe (contraseñas, usuarios); ii) algo que la persona tiene (tarjeta de identificación o una clave criptográfica); iii) algo que la persona es

(datos biométricos). La solidez del sistema por lo tanto, estará determinado en gran medida por la cantidad de factores a incorporar, entre más factores utilice el sistema más robusto y confiable será (Grass, Garcia y Fenton, 2017, pág. 12).

En los mecanismos de autenticación predominante, es el agente verificador quien debe comprobar las credenciales de la entidad (usuario) y validar su identidad, es decir, debe haber existido un proceso de autenticación previo de la persona para lograr acceder a los servicios del verificador, esto lo convierte en el proveedor de la identidad y del servicio a la vez. Pero desde la perspectiva actual, en la que un usuario promedio interactúa con decenas de plataformas digitales las cuales a su vez recopilan atributos de la persona de acuerdo con la naturaleza de las funcionalidades ofrecidas, los riesgos emergen y amenazan la privacidad y los datos personales de la persona usuaria, además de exponerla a potenciales suplantaciones de identidad al existir la posibilidad de que alguien pueda robar los datos personales almacenados en los diferentes sistemas de información. Sumado a lo anterior, es una tarea caótica para el usuario la gestión de múltiples identidades digitales para satisfacer los requerimientos de cada plataforma digital.

Cabe destacar además que a consecuencia de la dependencia de las personas de los servicios digitales, el uso masivo de la población global de algunos servicios en la web como las redes sociales alcanza en la actualidad la cifra de cuatro mil doscientos millones de usuarios activos[11], lo cual facilita a terceros autenticar a sus usuarios a través de los mecanismos de estas plataformas predominantes, esto es lo que se conoce como delegación de autenticación.

[11] Cifras según el portal Statista a mayo 3 de 2021: https://www.statista.com/statistics/617136/digital-population-worldwide/

:

Alamillo (2018) señala que con la delegación de autenticación, nos encontramos ante la autenticación como servicio prestado por terceros; esto es, la identificación y autenticación por proveedores de credenciales, también denominados proveedores de identidad digital (pág. 68).

Un ejemplo de lo anterior son los servicios que encontramos en la web que nos permiten acceder a sus funcionalidades utilizando el servicio de autenticación de Google, Facebook o Linkedin entre otros. Consciente las plataformas que miles de millones de usuarios cuentan con identidad digital en estos servicios líderes de Internet, lo más práctico es crear un mecanismo que permita al usuario autenticarse en su sistema utilizando las credenciales ya creadas en otro sistema. Lo que aquí sucede es que la nueva plataforma va a confiar en la identificación que haya realizado el usuario en las plataformas mencionadas, así como en las medidas de seguridad para autenticación, seguramente porque, tras un análisis de riesgos, habrá llegado a la conclusión que resulta más seguro delegar el proceso que implementarlo (Alamillo, 2018, pág. 73).

a.- Identidad Digital Auto-Soberana

Con el desarrollo durante la última década de las tecnologías de registro distribuido (*Distributed Ledger Technology – DLT*), ha sobresalido el concepto de Identidad Digital Auto-Soberana, una identidad descentralizada en la que los atributos de identificación ya no estarán en control de un verificador central, sino en control de la misma entidad.

En el paradigma de la identidad centralizada que se analizó anteriormente, la identidad de una persona es proporcionada por alguna entidad externa, el verificador, y en el caso de la autenticación delegada, un tercero es el encargado de gestionar el mecanismo. En el paradigma de identidad descentralizada, el objetivo es poner al usuario en el centro del marco y así eliminar la necesidad de que terceros emitan y administren la identidad (EU BOF, 2019, pág. 12).

De manera muy resumida, las tecnologías *DLT* o *Blockchain* se caracterizan por estar basadas en criptografía de clave pública lo cual garantiza seguridad e integridad de la información, además crean registros inmutables y públicos que se puedes gestionar de forma descentralizada. Por tal razón, las funcionalidades y características de *Blockchain*, permiten que sea la tecnología idónea para operar el mecanismo de Identidad Digital Auto-Soberana.

Una aproximación a la definición de Identidad Auto-Soberana (IAS) la ofrece Sovrin (como se citó en Allende, 2020) al señalar que la "identidad auto-soberana (IAS) es un término utilizado para describir el movimiento digital que reconoce que un individuo debe poseer y controlar su identidad sin la intervención de las autoridades administrativas. La IAS permite a las personas interactuar en el mundo digital con la misma libertad y capacidad de confianza que en el mundo físico" (pág. 27). Así en el mundo de la identidad descentralizada, los usuarios crean sus propias identidades digitales. Por lo general, esto comienza con un usuario que crea su propio identificador o identificadores únicos y luego adjunta información a ese identificador de una manera que permite demostrar su autenticidad (EU BOF, 2019, pág. 13).

Según Allen (como se citó en Alamillo, 2019), las identidades auto-soberanas deben atender a los siguientes principios: existencia de la identidad de una persona independientemente de administradores o proveedores de identidad; control por la persona de sus identidades digitales; acceso completo por las personas a sus datos; transparencia de los sistemas y algoritmos; persistencia de las identidades digitales (las identidades deben ser longevas, duraderas); portabilidad de las identidades digitales; interoperabilidad de las identidades digitales; cumplimiento de la economía de datos; y protección de los derechos de la persona.

La idea general de la identidad auto-soberana se basa en repositorios personales portables en los que podemos almacenar y administrar todas nuestras claves privadas, nuestros autenticadores y nuestros tokens y credenciales digitales de manera segura y confiable. Estos repositorios se conocen como billeteras digitales (Allende, 2020, pág. 28).

Un caso de uso típico sería que un usuario obtuviera credenciales de su colegio profesional, por ejemplo, del Colegio de Abogados y Abogadas de Costa Rica, esta institución emitiría una credencial que certificaría que dicha persona es un profesional agremiado a su Colegio y que esta habilitado para ejercer la profesión, esta certificación se registraría en una *Blockchain* y sería accesible solamente por las personas a las que el Abogado o Abogada decida compartir esa credencial, por lo tanto, si la persona profesional en Derecho requiere demostrar en el Poder Judicial que está autorizado para ejercer la abogacía, solo tendrá que compartir con la institución a través de una billetera digital el acceso a sus credenciales. Gracias a diversas técnicas criptográficas, como las firmas digitales, es posible obtener prueba sólida de que la credencial es genuina (es decir, emitido realmente por la autoridad designada y no manipulado desde entonces) y que la persona que presenta esa credencial es la persona referida (EU BOF, 2019, pág. 13).

Desde un punto de vista más técnico, la IAS se basa en un tipo de identificador denominado DID, que no es más que una URL (identificador universal uniforme de recursos), similar a la dirección de un sitio web, esta URL relaciona un sujeto con un documento de identificación descentralizada, de esta forma, a través de un DID se puede acceder a los contenidos de dicho DID para obtener los atributos de la persona (Alamillo, 2019, pág 77 y 78).

En la actualidad la IAS es un instrumento en desarrollo y que aún le falta consolidarse como un mecanismo masivo de identificación, pero que de acuerdo

con sus características promete regresarle a la persona la soberanía sobre sus identidades digitales, ofreciendo un método seguro para el resguardo y la gestión de sus datos personales. Sin embargo a nivel jurídico existen limitaciones, ya que los marcos normativos sobre protección de datos personales y sistemas de identificación están basados en relaciones de usuario-proveedor (Chomczyk, 2020), es decir, un tercero es el encargado de guardar las credenciales del usuario, prestar el servicio y a su vez ofrecer el mecanismo de autenticación, siendo un reto desde ya analizar las implicaciones legales de la IAS en el entendido que bajo este marco de trabajo, las credenciales del usuario son gestionadas por el mismo a través de una plataforma descentralizada como Blockchain.

IV. CONCLUSIONES

Aunque nuestro ordenamiento jurídico no contemple en la ley especial de Firma Digital el concepto de firma electrónica, no es limitante la utilización de este mecanismo como un instrumento de acreditación electrónica, todo dependerá de la fiabilidad y seguridad brindada por la tecnología utilizada para generar la firma. Dicha fiabilidad estará dada por la capacidad del método tecnológico de poder identificar al firmante y garantizar a su vez la integridad de la firma y el documento electrónico.

A la luz de los principios de equivalencia funcional, neutralidad tecnológica y autonomía de las partes, no podrá el juzgador imponer mayores exigencias a la firma electrónica con respecto a las firmas manuscritas realizadas sobre formato papel. No se le podrá negar efectos jurídicos de previo a una firma electrónica, sin antes valorar la fiabilidad de la tecnología utilizada para determinar la identificación del firmante, así como la integridad y autenticidad del documento, lo anterior se logrará a través de un peritaje informático de la firma estampada y las evidencias digitales generadas.

Para mayor seguridad jurídica a las transacciones en el marco del comercio electrónico, se sugiere incluir una definición de firma electrónica dentro del cuerpo normativo de la Ley 8454, lo cual fortalecería los principios de autonomía de las partes, equivalencia funcional y neutralidad tecnológica, asimismo impulsaría las actividades comerciales por estos medios y homologaría nuestra normativa con la regulación internacional predominante en esta materia, este último elemento muy necesario en un mundo digital donde predominan las transacciones transfronterizas no presenciales.

Una firma digital en nuestro ordenamiento es equivalente a la firma electrónica avanzada consagrada en la mayoría de los ordenamientos jurídicos que se han inspirado en las Leyes Modelo de la CNUDMI, dicha firma deberá cumplir tres requisitos para ser fiable: permitir identificar al firmante, vincularlo jurídicamente con el acto de la firma y verificar la integridad (no alteración) del documento electrónico firmado. De otra parte, la firma digital certificada es una firma digital generada a través de un método matemático criptográfico, amparada por un certificado digital emitido por la autoridad certificadora y que goza de plena presunción legal. En suma, la firma digital y la firma digital certificada son dos instrumentos diferentes, por lo tanto, si una norma establece como válido el uso de firma digital para determinado acto, se deberá entender que acepta cualquiera de los dos tipos de firma, tal es el caso del reformado artículo 460 del Código de Comercio que le otorga a la factura electrónica el título de ejecutividad siempre y cuando cuente con firma digital, lo cual se aprecia como correcto pues de esta forma se cumple con el valor equivalente consagrado en el artículo 9 de la Ley 8454, el cual reconoce el mismo valor y eficacia probatoria a los documentos firmados con firma digital que a los firmados en manuscrito.

Por sus características y su enfoque centrado en la persona, la Identidad Digital Auto-Soberana promete convertirse en el mecanismo de identificación más seguro y fiable para las acreditaciones electrónicas, no solo por las garantías

que ofrece a la protección de los datos personales de los ciudadanos, sino por la interoperabilidad y alcance que ofrece como un mecanismo de identificación universal. Es un tema que en la actualidad todavía se desarrolla jurídicamente, pero que en los próximos años veremos un incremento en su utilización y por ende surge la necesidad de comenzar a realizar los análisis jurídicos pertinentes.

REFERENCIAS BIBLIOGRÁFICAS

Alamillo Domingo, Ignacio. (2019). *Identificación, Firma y otras Pruebas Electrónicas. La regulación jurídico-administrativa de la acreditación de las transacciones electrónicas*. Editorial Aranzadi, Pamplona: España.

Allende L. (2020). Identidad Digital Auto-soberana El futuro de la identidad digital: auto-soberanía, billeteras digitales y blockchain. BID, BID LAB & LACCHAIN. Recuperado el 3 de mayo de 2021, de: https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf

Asamblea Legislativa de La República de Costa Rica. 2005. *Ley de Certificados, Firmas Digitales y Documentos Electrónicos No 8454*. Recuperado de Sinalevi: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=55666

Asamblea Legislativa de La República de Costa Rica. 1995. *Ley General de Aduanas N° 7557*. Recuperado el 28 de abril de 2021, de Sinalevi: http://www.pgrweb.go.cr/SCIJ/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=25886

Asamblea Legislativa de La República de Costa Rica. 2008. *Ley General de Telecomunicaciones No 8642*. Recuperado el 28 de abril de 2021, de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=63431

Asamblea Nacional. (2008). *Ley 51 de 22 de Julio de 2008 Que define y regula los documentos electrónicos y las firmas electrónicas y la prestación de*

servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico. Panamá. Recuperado de: https://www.firmaelectronica.gob.pa/documentos/Ley_51-Firma_electronicas_almacenamiento_tecnologico_y_comercio_electronico.pdf

Asamblea Nacional. (2012). *Ley 82 de 9 de noviembre de 2012 Que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modifica la Ley 51 de 2008 y adopta otras disposiciones*. Panamá. Recuperado el 28 de abril de 2021, de: https://www.firmaelectronica.gob.pa/documentos/Ley_82-Que_modifica_la_Ley_51_de_2008.pdf

Barros, A., Gómez, C., Pareja, A., Pedak, M. (2017). *La Gestión de la Identidad y su impacto en la economía digital*. Banco Interamericano de Desarrollo (BID). Recuperado el 30 de abril de 2021, de: https://publications.iadb.org/publications/spanish/document/La-gesti%C3%B3n-de-la-identidad-y-su-impacto-en-la-econom%C3%ADa-digital.pdf

Cámara de Diputados del H. Congreso de la Unión. (1889). *Código de Comercio*. México. Recuperado el 28 de abril de 2021, de: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_de_Comercio.pdf

Congreso de Colombia. (1999). *Ley 527 de 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de*

certificación y se dictan otras disposiciones. Diario Oficial No 43.673 de 21 de agosto de 1999. Recuperado el 28 de abril de 2021, de: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Congreso de la República. (2000). *Ley No 27269 Ley de Firmas y Certificados Digitales*. Perú. Recuperado el 28 de abril de 2021, de: https://cdn.www.gob.pe/uploads/document/file/356833/NORMA_1887_LEY_27269_Modificada_por_LEY_27310.pdf

CNUDMI. (1996). *Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno*. New York. Recuperado el 25 de abril de 2021, de: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf

CNUDMI. (2017). *Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos*. New York. Recuperado el 25 de abril de 2021, de: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/mletr_ebook_s.pdf

CNUDMI. (2001). *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno*. New York. Recuperado el 25 de abril de 2021, de: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/ml-elecsig-s.pdf

Congress of the United States of America. (2000). ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT. Estados Unidos. Recuperado el 28 de abril de 2021, de:

https://www.govinfo.gov/content/pkg/PLAW-106publ229/html/PLAW-106publ229.htm

Chomczyk, Andrés. (2020). Regulación de blockhain e identidad digital en América Latina El futuro de la identidad digital. BID, BID LAB, DIDI, AB, LACCHAIN. Recuperado el 3 de mayo de 2021, de: https://publications.iadb.org/publications/spanish/document/Regulacion-de-blockchain-e-identidad-digital-en-America-Latina-El-futuro-de-la-identidad-digital.pdf

Departamento de Certificadores de Firma Digital Dirección de Gobernanza Digital Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2018). *Política de Certificados para la jerarquía nacional de certificadores registrados, versión 1.2 de 21 de Febrero 2018*.

EU Blockchain Observatory Forum. (2019). *Blockchain and digital identity*. Recuperado el 3 de mayo de 2021, de: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

Grassi, Paul A., Garcia, Michael E., Fenton, James L. (2017). Digital Idendity Guidelines. NIST Special Publication 800-63-3. NIST National Institute of Standards and Technology, U.S Department of Commerce. Recuperado de: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

Honorable Congreso de la Nación de Argentina. (2001*). Ley 25.506 de 2001 Ley Ley de Firma Digital*. Promulgada de Hecho: Diciembre 11 de 2001. Recuperado el 27 de abril de 2021, de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/texact.htm

Ministerio de Ciencia y Tecnología. (2006). *Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos Nº 33018*. San José Costa Rica. Recuperado el 20 de abril de 2021, de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=56884

OECD. (2007). *Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication*. OECD Committee for Information, Computer and Communications Policy (ICCP). Recuperado el 25 de abril de 2021, de https://www.oecd.org/sti/ieconomy/38921342.pdf

PARLAMENTO Y CONSEJO EUROPEO. (2014). *REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo 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*. Recuperado el 25 de abril de 2021, de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32014R0910

Peña Valenzuela, Daniel. (2015). *De la firma manuscrita a las firmas electrónica y digital: Derecho internacional de los negocios*. Tomo V. Universidad Externado. Edición de Kindle.

Presidencia de la República de Colombia. (2012). *Decreto 2364 de 2012 Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones*. Colombia. Recuperado el 22 de abril de 2021, de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50583#2364

Procuraduría General de la República. 2004. *Sobre el Principio de Neutralidad Tecnológica en las Compras Públicas, OJ-083-204*. San José.

Real Academia Española. (s.f.). Firma. En *Diccionario de la lengua española*. Recuperado el 10 de abril de 2021, de https://dle.rae.es/firma?m=form

Real Academia Española. (s.f.). Rúbrica. En *Diccionario de la lengua española*. Recuperado el 10 de abril de 2021, de https://dle.rae.es/r%C3%BAbrica

Robles Llorente, Miguel A. (2015). *La escritura y la firma manuscrita como elementos coadyuvantes de la seguridad documental*. (Tesis de Doctorado). Universidad Autónoma de Barcelona. Recuperado el 28 de marzo de 2021, de https://www.tesisenred.net/bitstream/handle/10803/315287/marl.pdf?sequence=1;La

Sala Tercera de la Corte Suprema de Justicia. (2019). *Resolución Nº 229-2019, de las 12:00 horas del 22 de febrero de 2019*. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0006-910187

Torres Torres, Ana Y. (2012). *Principios Fundamentales del Comercio Electrónico y su desarrollo legislativo en Colombia y Latinoamérica. Universidad de Los Andes*. Editorial Temis. Bogotá, Colombia.

Tribunal Primero Civil. (2009). *Resolución N° 2009-00293 de las ocho horas cinco minutos del diecisiete de abril de dos mil nueve*, San José, Costa Rica.

Uniform Law Comission. (1999). *UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)*. Estados Unidos. Recuperado el 25 de abril de 2021, de: https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFil

e.ashx?DocumentFileKey=2c38eebd-69af-aafc-ddc3-b3d292bf805a&forceDialog=0

TRIBUNA LIBRE

EDICIÓN DIGITAL

Edición 8/1, Octubre 2021
Costa Rica

ESCUELA LIBRE DE DERECHO
UNIVERSIDAD