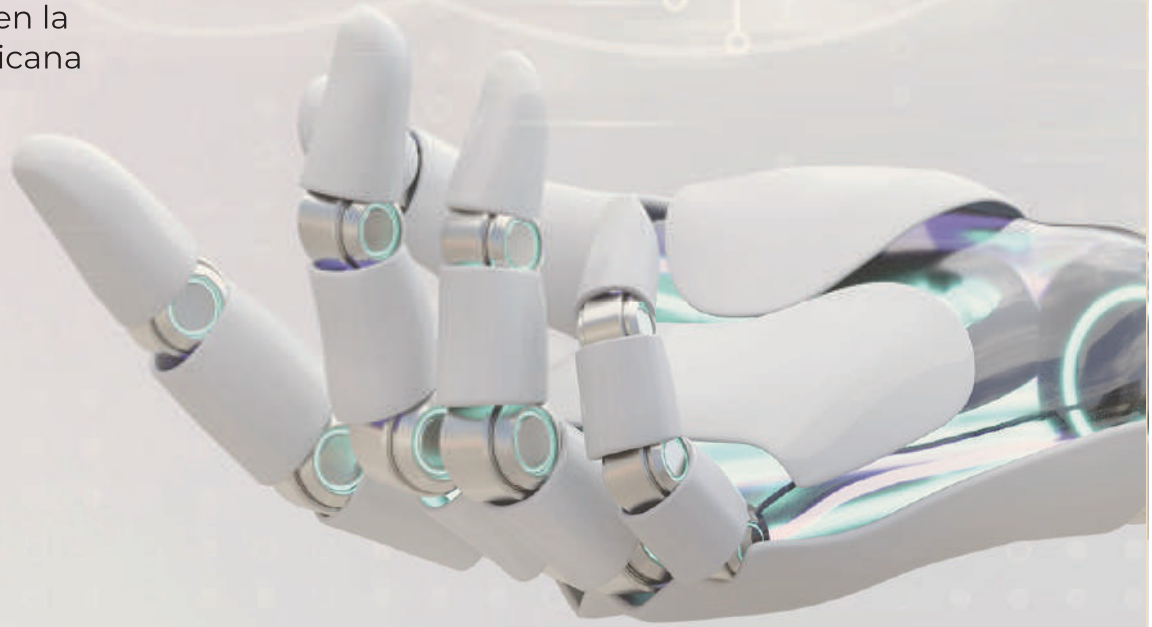
EL EFECTO BRUSELAS Y SU IMPACTO EN LA REGIÓN:
La regulación sobre economía digital

SIGÜENZA & CARRASCOSA
ANÁLISIS LEGAL Y DERECHO COMPARADO

- Bitcoin, moneda de curso legal
- Regulación del mercado electrónico transfronterizo en Centroamérica y El Caribe
- Insuficiencia de la regulación en materia de protección de datos y ciberseguridad en la República Dominicana



VOLUMEN
2023

CRÉDITOS

Dirección Editorial:
María Isabel Carrascosa Coll

Autores:
María Isabel Carrascosa Coll
Luis Ernesto Peña Jiménez
María Alejandra Barillas Gordillo
Victoria Fernanda Méndez Echeverría
Fátima Alejandra Aldana González

Diseño y diagramación:
The Corner Studio, S.A. | www.thecornerstudio.net

Impresión:
Digitalhouse, Innovaciones en papel S.A.

Imágenes y fotografías
Freepik | www.freepik.com

SUMARIO

NOTA EDITORIAL
Socios Fundadores 5

EL EFECTO BRUSELAS, LA REGULACIÓN EN MATERIA TECNOLÓGICA EN LA UNIÓN EUROPEA
Victoria Fernanda Méndez Echeverría 8

FICHAS TÉCNICAS SOBRE LAS NORMAS EN MATERIA TECNOLÓGICA EN LA UNIÓN EUROPEA
Victoria Fernanda Méndez Echeverría 11

REGULACIÓN DEL MERCADO ELECTRÓNICO TRASFRONTERIZO EN CENTROAMÉRICA Y EL CARIBE
Fátima Alejandra Aldana González 15

NORMAS DE PROTECCIÓN DE DATOS, INTELIGENCIA ARTIFICIAL Y CIBERSEGURIDAD: UN ANÁLISIS DE CENTROAMÉRICA Y REPÚBLICA DOMINICANA
Victoria Fernanda Méndez Echeverría 22

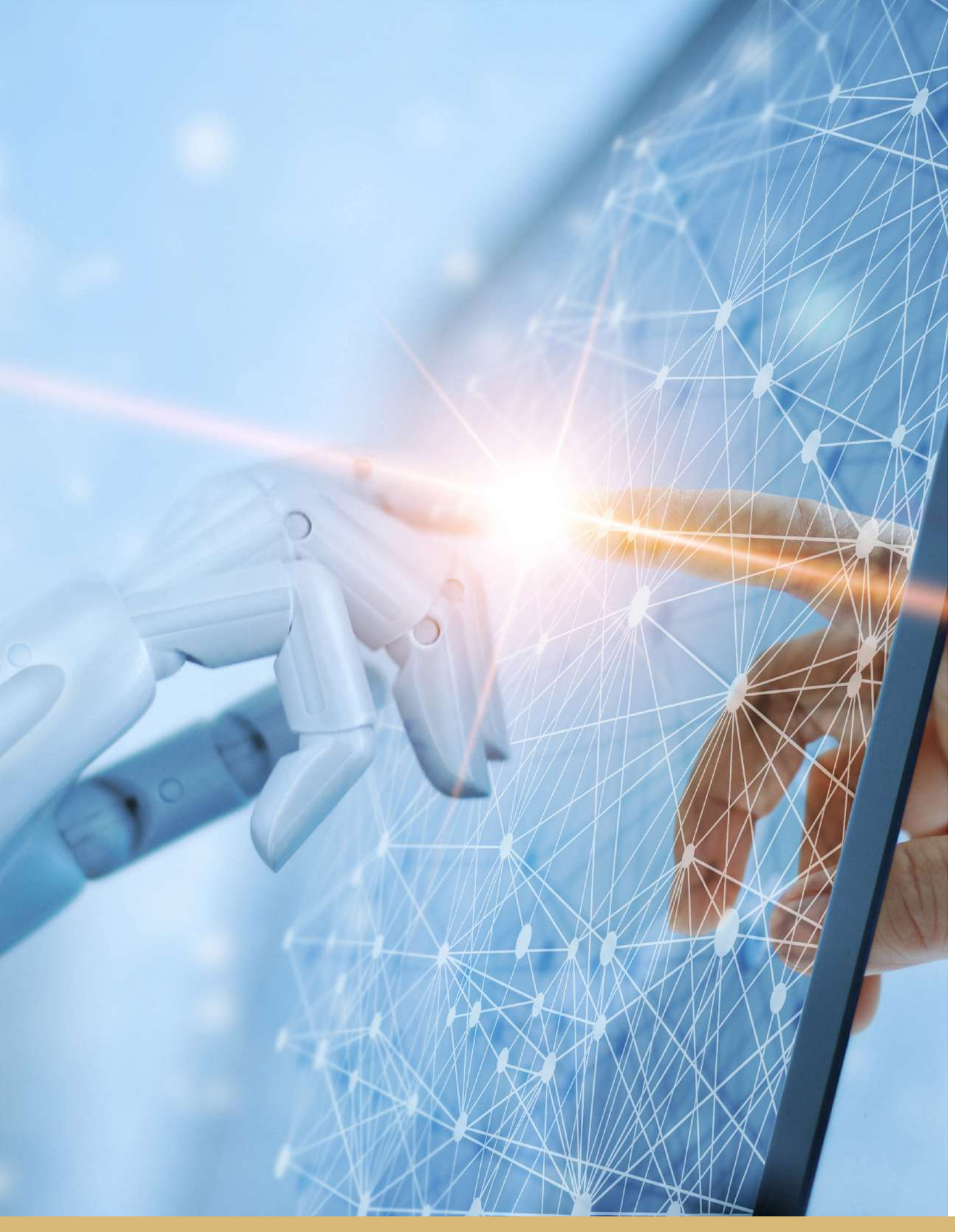
EL SALVADOR: A DOS AÑOS DE QUE BITCOIN SEA MONEDA DE CURSO LEGAL
María Alejandra Barillas Gordillo 29

BITCOIN, MONEDA DE CURSO LEGAL
María Isabel Carrascosa Coll 32

GUATEMALA: EL PROBLEMA DE LOS TRASPLANTES JURÍDICOS DESCONTEXTUALIZADOS
María Alejandra Barillas Gordillo 35

LA LEY DE DATOS EN COSTA RICA: PROTEGIENDO LA PRIVACIDAD EN LA ERA DIGITAL
Victoria Fernanda Méndez Echeverría 38

INSUFICIENCIA DE LA REGULACIÓN EN MATERIA DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD EN LA REPÚBLICA DOMINICANA
Luis Ernesto Peña Jiménez 41



NOTA EDITORIAL

En Sigüenza y Carrascosa creemos en la importancia de la discusión de ideas. Por eso, por segundo año consecutivo, trabajamos para nuestros clientes, a quienes consideramos nuestra inspiración, una revista que pretende plantear asuntos regulatorios que son tendencia en la región centroamericana y el Caribe.

Este es entonces un tributo al esfuerzo de las compañías que trabajan en la región y que nos hacen parte de sus proyectos. Es gracias a la confianza que ustedes depositan en nosotros que podemos observar de cerca la influencia que tienen sistemas jurídicos considerados prestigiosos en sistemas también llamados periféricos como los nuestros. En esta edición explicamos el "Efecto Bruselas" y su impacto en Guatemala y Centroamérica en materia de regulación de la economía digital. Pero también buscamos comprender la necesidad que existe en la región de regular la protección de datos, los ciberdelitos, el comercio electrónico o activos digitales por mencionar algunos, de forma armonizada y tomando en consideración las realidades económicas y culturales de cada país.

S&C es una firma boutique que busca mejorar la calidad legislativa, políticas públicas e instituciones en la región Centroamericana y el Caribe. Esperamos esta edición sea de utilidad.

César Leonel Sigüenza Blanco y María Isabel Carrascosa Coll
Socios Fundadores

SOBRE NUESTRO EQUIPO

Socios fundadores

María Isabel Carrascosa Coll:

Abogada y Notaria egresada de la Universidad Francisco Marroquín de Guatemala. Ganadora de las becas Carolina y Fullbright LLM. Cuenta con una maestría en Derecho Internacional y Comparado de la Universidad George Washington, EEUU. Tiene amplia experiencia en el sector de bebidas y alimentos, asuntos ambientales, contrataciones públicas, transparencia y sistemas judiciales. Es profesora de Sistemas Jurídicos Contemporáneos en la Universidad Francisco Marroquín.

César Leonel Sigüenza Blanco:

Abogado y Notario egresado de la Universidad Francisco Marroquín, con un Maestría en Política y Derecho Internacional. Profesor Universitario de Derecho Administrativo. Experto en negociación y diseño de políticas públicas. Ha liderado procesos de gestión de intereses para el sector financiero, que han manejado asuntos como: privacidad, secreto bancario, derecho de competencia, tarjetas de crédito, entre otros.

SOBRE NUESTRO EQUIPO

Luis Ernesto Peña Jiménez:

Abogado de la República Dominicana especializado en Derecho Público, con práctica concentrada en Compras Públicas, Derecho Político/Electoral y Constitucional. Graduado de la George Washington University Law School, Washington, D.C., Universidad Castilla-La Mancha, Albacete, España y de la Pontificia Universidad Católica Madre y Maestra, Santo Domingo, República Dominicana.

María Alejandra Barillas Gordillo:

Abogada y Notaria egresada de la Universidad Francisco Marroquín de Guatemala, en donde obtuvo el Premio de Luis Beltranena Sinibaldi de Derecho Administrativo. Se encuentra cursando una maestría de Asuntos Globales en la Universidad del Valle de Guatemala. Es encargada del departamento de Análisis y Monitoreo Legislativo y del departamento de Derecho Comparado y Diseño Legislativo y Reglamentario.

Victoria Fernanda Méndez Echeverría:

Abogada y Notaria egresada de la Universidad Francisco Marroquín de Guatemala, de donde fue acreedora de los premios: Luis Beltranena Sinibaldi de Derecho Administrativo; José Vicente Rodríguez de Derecho Civil y Premio del Decanato. Actualmente es encargada del departamento de Corporativo y Notariado y Asistente del Departamento de Derecho Comparado y Diseño Legislativo y Reglamentario.

Fátima Alejandra Aldana González:

Licenciada en Ciencias Jurídicas y Sociales egresada de la Universidad Rafael Landívar de Guatemala. Es encargada del Monitoreo Constitucional y la elaboración de análisis de asuntos sometidos a jurisdicción constitucional, así como de la centralización de los servicios de Análisis y Monitoreo Legislativos Regionales.

EL EFECTO BRUSELAS, LA REGULACIÓN EN MATERIA TECNOLÓGICA EN LA UNIÓN EUROPEA

Victoria Fernanda Méndez Echeverría

La transformación digital está más cerca de lo que creemos. Los avances tecnológicos han cambiado la forma en que el ser humano interactúa y obtiene información. **A pesar de que la era digital ofrece soluciones y hace más eficiente el actuar del hombre, también origina retos nunca antes vistos.** La revolución tecnológica ha ocurrido en dos etapas. La primera de ellas se dio con la creación de las Tecnologías de Información y Comunicación (TICS), que permiten obtener información sin cambiar la forma en que se hacen las cosas. (Carrillo, 2019).

La segunda de ellas está actualmente ocurriendo. Esta etapa incluye a la inteligencia artificial, el metaverso, la realidad inmersiva, la realidad aumentada, entre otros. Estas tecnologías permiten que ciertas actividades ya no sean realizadas de manera directa por el hombre. Por este motivo la Unión Europea, siendo pionera en la materia, ha considerado que el marco normativo existente es inadecuado a los avances tecnológicos y ha propuesto redefinirlo a través de la creación de normas específicas (Ballel, 2018).

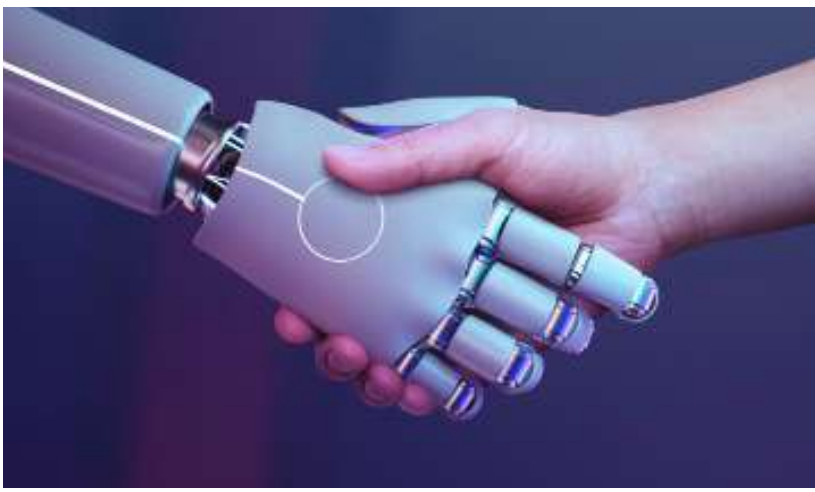
Con esta revolución normativa la Unión Europea tiene como objetivo ocasionar el **"Efecto Bruselas"**. **El efecto Bruselas se refiere a la influencia regulatoria y política que ejerce la ciudad de Bruselas, como capital de Europa, en el mundo.** La importancia que ha adquirido el Parlamento Europeo y la normativa que el mismo ha promulgado en los últimos años, ha convertido en Bruselas un lugar importante para creadores de políticas públicas así como para cabilderos y empresas (Bradford, 2019).

El efecto Bruselas es real. La Unión Europea se ha convertido en un actor influyente en la formulación de normas clave en el mundo. **Muchas de las políticas públicas desarrolladas por la UE sobre comercio, protección del medio ambiente y derechos humanos han sido adoptadas por otros países.** Por ejemplo, la Convención sobre la Diversidad Biológica, el Acuerdo de París, la Política Agrícola Común, el Reglamento UE 1169/2011 sobre etiquetado de alimentos, entre otras. Asimismo ha establecido estándares rigurosos sobre protección al consumidor, privacidad de datos y seguridad alimentaria, logrando así que otros países se ajusten a ellos, para acceder a su mercado. También ha desarrollado relaciones estratégicas con actores internacionales que le han permitido promover sus valores en la agenda global e influir en la formulación de políticas públicas (Bradford, 2019). Por lo tanto, es evidente que la capacidad de persuadir a otros países y regiones ha ocasionado que la Unión Europea se convierta en un líder regulatorio a nivel mundial.

A pesar de que el efecto Bruselas permite un avance en la integración normativa a nivel mundial y en la creación de estándares altos de cumplimiento, también presenta complicaciones. Este fenómeno ha ocasionado una centralización de poder en la Unión Europea, lo que puede limitar las capacidades de los países para tomar decisiones autónomas en áreas clave.
Por ejemplo, en el sector ambiental, alimenticio, laboral, energético, entre otros. Asimismo, puede desalentar la inversión y creación de empleo dentro de la UE, ya que no todos los comercios tienen protocolos alineados a los altos y rigurosos estándares que caracterizan a la Unión Europea. Por lo tanto, su implementación impondría cargas adicionales a las empresas y comercios, tales como la readecuación de sus protocolos de cumplimiento, la obtención de ciertas certificaciones, entre otros, que dichas empresas no estarían dispuestas a cumplir o no tendrían las capacidades económicas y tecnológicas para hacerlo (Elisabeth Christen, Birgit Meyer, Harald Oberhofer, Julian Hinz, Katrin Kamin, Joschka Wanner, 2022).

De igual manera puede afectar económicamente a los países con economías menos desarrolladas, quienes deberán cumplir y adecuarse a estos nuevos parámetros para poder seguir negociando con la Unión Europea. Finalmente puede ocasionar la creación de políticas públicas inaplicables o demasiado costosas de cumplir, si los países que están ajustando sus normas internas a los protocolos de la UE no los adecúan al contexto social, político, económico y cultural de su propio país.

La Unión Europea ha desempeñado un papel importante en la promoción y regulación de la era digital. Para hacerle frente a los avances tecnológicos, ha promovido directivas y normas que regulan temas como: la protección al consumidor y libre competencia digital, la inteligencia artificial, los criptoactivos, la protección de datos, la ciberseguridad, entre otros. **Estas normas son novedosas y han establecido a Europa como pionera en el tema. Muchas de ellas, al ser aprobadas, serán las primeras en existir en el mundo.**



En el contexto del Efecto Bruselas, se espera que este tipo de políticas públicas comiencen a ser promovidas y aplicadas fuera de la Unión Europea. Este será el primer paso para lograr una armonización digital a nivel mundial. Ahora bien, **es importante que los países que ajusten sus normativas internas a los parámetros de la UE realicen un esfuerzo por identificar las diferencias tecnológicas y económicas que existen entre ésta y su país. Esto permitirá crear políticas públicas aplicables y adecuadas a la problemática nacional y evitará la creación de normas imposibles de cumplir.**

A pesar que la UE se encuentra muy avanzada en el mundo digital, todavía enfrenta grandes desafíos. El primero de ellos es la brecha digital que existe a lo interno entre ciertos países de la UE. Esto genera desigualdad y limita el potencial de la economía digital (Cuervo, 2005). Esta brecha se marca aún más cuando se compara a Europa con países con menor grado de desarrollo. El segundo de ellos consiste en la protección efectiva de datos. A pesar que la UE está en proceso de crear una Ley de Datos digital, no se sabe si dicha norma podrá prever todos los escenarios que se presenten a futuro (Castilla, 2018).

El tercero de ellos es la escasez de habilidades digitales en la UE. Esto obliga a invertir en capacitaciones y educación digital (Castilla, 2018). Finalmente, la ciberseguridad. A pesar que la UE se encuentra aprobando una norma de ciberseguridad, los malwares y los mecanismos para violar la seguridad digital seguirán evolucionando (Nieva, 2016). **Cabe mencionar que estas problemáticas también se transferirán a los países que se adecúen a los protocolos de la UE. Es más, estos retos serán solo la punta del iceberg, ya que dichos países también deberán preocuparse por tener un contexto digital, político y económico que les haga posible cumplir con esos estándares tan rigurosos.**

En conclusión, con la aprobación de estas normas la Unión Europea se volverá líder regulatorio mundial y parámetro mínimo de cumplimiento de ciberseguridad, protección de datos, inteligencia artificial, etc. Esto significa que, con mayor brevedad de la esperada, se estarán promoviendo normas similares en todo el mundo. En este sentido, **es necesario comenzar a generar protocolos, con el objetivo de poder cumplir de una manera más eficiente y menos costosa, en términos de tiempo, con las obligaciones que de estas normas se derivan.** Para la elaboración de estos protocolos deberá tomarse en cuenta que: i) el contexto social, económico, político y cultural de cada país es distinto. Por lo tanto, los estándares de cumplimiento deberán adecuarse a la realidad social nacional; ii) el giro económico y funcionamiento de cada empresa es distinto. Por lo tanto, los protocolos deben realizarse de manera personalizada y iii) será necesario revisar y actualizar los protocolos a medida que los estándares se modifiquen. Por lo tanto, los protocolos no serán estáticos.

REFERENCIAS

Ballel, T. R. (2018). Una regulación Europea para las plataformas electrónicas: propuesta en curso y alternativas. En A. Madrid, *Derecho mercantil y tecnología* (págs. 427-452). España: Editorial Arazandi, S.A.U.

Bradford, A. (2019). *The Brussels Effect: how the European Union Rules the world.* Oxford: 25-66.

Carrillo, M. R. (2019). El modelo de neutralidad de la red en la Unión Europea: alcance y contenido. *Revista de Derecho Comunitario Europeo*, 449-488.

Castilla, C. (2018). Evolución y perspectivas de la brecha digital en la Unión Europea. *Revista ComHumanitas*.

Cuervo, M. R. (2005). Una aproximación a la brecha digital. El caso de la Unión Europea. *Boletín Económico ICE*.

Elisabeth Christen, Birgit Meyer, Harald Oberhofer, Julian Hinz, Katrin Kamin, Joschka Wanner. (2022). The Brussels Effect 2.0 How the EU sets global standards with its trade policy. 79.

FICHAS TÉCNICAS SOBRE LAS NORMAS EN MATERIA TECNOLÓGICA EN LA UNIÓN EUROPEA

Victoria Fernanda Méndez Echeverría

Victoria Fernanda Méndez Echeverría

PROTECCIÓN AL CONSUMIDOR Y LA LIBRE COMPETENCIA DIGITAL EN LA UNIÓN EUROPEA:

Reglamento (UE) 2022/1925 sobre mercados disputables y equitativos en el sector digital - Reglamento de Mercados Digitales	• Aprobada el 18 de julio del 2022. Entró en vigor el 2 de mayo del 2023. • **Objetivo:** evitar que las grandes plataformas en línea (guardianes de acceso) se aprovechen de su posición dominante y afecten el principio de igualdad de condiciones. • **Sujetos obligados:** guardianes de acceso (grandes plataformas en línea), tales como: Alphabet, Amazon, Apple, ByteDance, Meta y Microsoft. • **Prohibiciones y beneficios:** i) se prohíben las prácticas desleales de las grandes plataformas y ii) se promueve el aumento de oferta para el consumidor • **Repercusiones en la Industria:** Limita la cuota de mercado que tienen las grandes plataformas en línea y permite que las empresas tecnológicas emergentes puedan competir de forma más accesible.
Reglamento (UE) 2022/2065 de Servicios Digitales	• Aprobado el 4 de octubre del 2022. Entrará en vigor el 17 de febrero del 2024. • **Objetivo:** proteger a los usuarios y aumentar la transparencia en el intercambio de bienes y servicios digitales. • **Sujetos obligados:** todas las empresas que tienen un rol de intermediarios en línea. Es decir, todos aquellos que conectan a los usuarios con productos o servicios en la Unión Europea. • **Obligaciones impuestas a intermediarios:** a) informar a los usuarios las condiciones generales de la plataforma; b) no utilizar datos personales o sensibles para personalizar publicidad y c) no utilizar interfases engañosas. • **Repercusiones en la Industria:** Las empresas que intercambien bienes y servicios de manera electrónica deberán invertir en sistemas de vigilancia y en el desarrollo de mecanismos para evitar que la interfaz sea engañosa.

LA INTELIGENCIA ARTIFICIAL EN LA UNIÓN EUROPEA:

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen las normas armonizadas en materia de inteligencia artificial- Ley de Inteligencia Artificial	• No está vigente. Los negociadores del Parlamento y del Consejo alcanzaron un acuerdo provisional. El Parlamento y el Consejo votarán sobre su adopción en el 2024 y surtirá efectos hasta el 2025. • **Objetivo:** garantizar que los sistemas de Inteligencia Artificial introducidos a la Unión Europea sean seguros. • **Sujetos obligados:** todos aquellos que utilicen IA en la prestación de servicios o negociación de bienes. • **Sistemas prohibidos:** son todos aquellos que causan una amenaza física o psicológica en las personas. Estos sistemas no son permitidos. • **Sistemas de alto riesgo:** son todos aquellos que pertenecen al ámbito educativo, de empleo y gestión, aplicación de la ley, gestión de migración, control de fronteras, identificación biométrica, entre otros. Estos sistemas son permitidos siempre y cuando cuenten con un mecanismo de gestión de riesgos. • **Repercusiones en la Industria:** Las empresas que utilicen la IA para brindar servicios deberán invertir en capacitaciones, manuales y protocolos de uso y buen desarrollo del sistema, para evitar responsabilidades monetarias.
Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos	• No está vigente. Se encuentra en debates en el Consejo de la Unión Europea. • **Objetivo:** Propone que el sistema de IA sea considerado un producto y que la falla sea el defecto. Bajo este sistema el fabricante del producto, es decir, el desarrollador, es el responsable por el funcionamiento indebido de la IA. • **Repercusiones en la Industria:** Obliga al desarrollador del sistema de IA a ser más precavido en su elaboración, para evitar repercusiones monetarias. Asimismo, protege a los usuarios de la IA que se ven afectados por su uso.
Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial	• No está vigente. Se encuentra en debates en el Consejo de la Unión Europea. • **Objetivo:** responsabilizar al desarrollador de la IA por los daños derivados de las fallas en el diseño del sistema o al operador de la IA por los daños derivados del mal uso, falta de supervisión o exposición a datos no adecuados. • **Repercusiones en la industria:** Obliga al desarrollador y al operador del sistema de IA a ser más precavidos en su elaboración y uso, para evitar repercusiones monetarias. También protege a los usuarios afectados por la IA.

LOS CRIPTOACTIVOS EN LA UNIÓN EUROPEA:

Reglamento (UE) 2023/114 relativo a los mercados de criptoactivos	• Aprobado el 31 de mayo del 2023. Entrará en vigor a mediados del 2024. • **Objetivo:** regular la emisión, oferta al público y negociación de los criptoactivos, para proteger a los usuarios y titulares de estafas y crisis. • **Obligaciones impuestas a los proveedores de criptomonedas:** i) contratar pólizas de seguro para hacer frente a sus obligaciones con los usuarios; ii) habilitar procedimientos claros de reclamaciones para sus clientes y iii) hacer públicas las características del proyecto, previo a ofrecer una moneda digital. • **Con relación al blanqueo de capitales:** obliga al emisor de criptoactivos a implementar procedimientos internos para evitar estos delitos. • **Repercusiones en la industria:** Obliga a los emisores de criptoactivos a implementar protocolos para evitar el blanqueo de dinero y proteger la inversión del titular del criptoactivo. Asimismo, protege al titular de los criptoactivos y hace más factible el uso de criptomonedas para realizar transacciones económicamente relevantes.

PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA:

Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas armonizadas para un acceso justo a los datos y su utilización - Ley de datos.	• No está vigente. El acto está sujeto a aprobación formal y una vez adoptado entrará en vigor 20 días después de su publicación en el Diario Oficial. • **Objetivo:** establecer normas sobre quién puede acceder a qué datos y para qué fines pueden utilizarse. • **Sujetos obligados:** todos los involucrados en la cadena de transmisión de datos. • **Obligaciones impuestas a los fabricantes de productos o servicios:** informar al usuario del uso que se le darán a los datos, si éstos serán cedidos y el mecanismo para que sean compartidos con un tercero. • **Obligaciones impuestas a los terceros que reciben datos:** utilizar los datos para los fines acordados, no ceder los datos sin autorización y no utilizar los datos para elaborar perfiles de personas físicas. • **Acuerdos abusivos o unilaterales:** los acuerdos sobre el acceso a los datos impuestos de manera unilateral o abusivos no son vinculantes. En este sentido, la entidad que obtiene los datos no podría comercializarlos ni utilizarlos en su favor de manera legal o lícita. • **Repercusiones en la industria:** Las entidades que obtienen datos de manera electrónica deberán generar protocolos de cumplimiento y transparencia.

REGULACIÓN DEL MERCADO ELECTRÓNICO TRANSFRONTERIZO EN CENTROAMÉRICA Y EL CARIBE

Fátima Alejandra Aldana González

La sociedad ha experimentado una notoria transformación digital en los últimos años. Esto ha provocado un crecimiento acelerado del comercio electrónico, que se presenta como una oportunidad valiosa para expandir la oferta de productos y servicios hacia nuevos mercados. **El comercio electrónico ha revolucionado la manera en que se presentan y se consumen bienes y servicios, desempeñando un papel importante en el impulso del crecimiento económico.**

Esta forma de comercialización se ha impulsado con el desarrollo de distintas tecnologías de la información y la comunicación, que promueven el ecosistema ideal para desarrollar un canal de compras electrónicas para los consumidores.

El comercio electrónico abarca, no solo la adquisición de bienes y servicios, sino también otras actividades como transacciones comerciales y los procesos internos utilizados por los proveedores para respaldar sus operaciones (Schneider, 2013).

En este contexto, **es importante que el engranaje legislativo se adapte y busque nuevas formas de interactuar con los actores del comercio electrónico, tanto proveedores como consumidores del comercio. Sin embargo, regular el comercio electrónico implica superar una serie de desafíos legales, fiscales, logísticos y tecnológicos.** La cooperación internacional y la adopción de estándares comunes son esenciales para abordar estos desafíos de manera efectiva y fomentar un entorno comercial electrónico seguro y eficiente.

Uno de los retos asociados con la regulación del comercio electrónico radica en el ámbito territorial de la aplicación de las normativas. A diferencia del comercio convencional, donde la aplicabilidad de las normas puede determinarse de acuerdo con el espacio físico donde se adquieren productos o servicios, se prestan servicios, se encuentran los bienes o la nacionalidad de los contratantes, el comercio electrónico presenta una dinámica más compleja.

Las empresas que operan en el comercio electrónico extienden su alcance más allá de las fronteras tradicionales, lo que dificulta la **delimitación territorial** para la aplicación de regulaciones específicas. Una vez que los negocios empezaron a operar en línea se ha hecho notorio que las medidas tradicionales para identificar el ámbito territorial de aplicación de una norma no resultan efectivas para normar esta actividad.

Otro de los retos asociados con la regulación del comercio electrónico es la protección al consumidor. Garantizar estándares uniformes, por medio de la legislación, para la seguridad de los productos, la privacidad de los datos y la resolución de conflictos puede ser complicado debido a las diferencias en las leyes y la implementación de estas normativas.

La primera complicación surge en la determinación de los alcances de las disposiciones en materia de protección al consumidor. Esto debido a que desde la definición de "consumidor" existen distintas perspectivas. Algunas de estas definiciones son laxas y, por lo tanto, amplían el ámbito de aplicación; otras son restrictivas y limitan los alcances de este tipo de disposiciones. En cuanto a la regulación del comercio electrónico, a pesar de que existe una tendencia a dar una definición más restrictiva, definiendo como consumidor a aquel sujeto que contrata para uso o consumo de su entorno personal o familiar; no hay unificación en el contenido del concepto de consumidor, lo que dificulta identificar los alcances de la normativa (Barral Viñals, 2004). En la región estos obstáculos han sido abordados de diferente forma en la legislación o se han planteado distintos enfoques en las iniciativas que se han presentado en los poderes legislativos.

A continuación, haremos un repaso de cómo se concibe en cada país.

COSTA RICA

Actualmente Costa Rica no cuenta con una legislación que regule de forma expresa el comercio electrónico. Sin embargo, a la fecha se han presentado y tramitado las siguientes iniciativas de ley:

- Expediente 16.081 – Ley de Comercio Electrónico. El proyecto fue presentado el 29 de noviembre de 2005 y fue dictaminado de forma negativa por la comisión en noviembre de 2009. Los diputados consideraron, al dictaminar la iniciativa, que era necesario delimitar de manera adecuada su ámbito de aplicación. A pesar de que la iniciativa no sobrevivió a su trámite en la comisión fue el primer antecedente de este tipo de iniciativas en la Asamblea Legislativa.

- Expediente 19.012 – Ley de Servicios de la Sociedad de la Información (Ley de Comercio Electrónico). Esta iniciativa es el segundo intento de regular el Comercio Electrónico en Costa Rica y fue presentada el 19 de junio de 2014. La iniciativa no alcanzó a ser dictaminada por la comisión y fue archivada por vencimiento del periodo cuatrienal.[1]

- Expediente 21.183 – Ley del Mercado y del Comercio Electrónico. El tercer intento de regular esta actividad comercial fue presentado el 12 de diciembre de 2018. Sin embargo, el 18 de noviembre de 2020, la comisión a cargo de estudiar la iniciativa acordó emitir dictamen desfavorable, por lo que la iniciativa no prosperó en su trámite legislativo. Lamentablemente el dictamen de la iniciativa no cuenta con un análisis sobre los motivos que tuvo la comisión para dictaminar la iniciativa.

- Expediente 23.184 – Gobernanza de los Servicios Digitales y el Comercio Electrónico. Es la iniciativa más reciente en este ámbito. Fue presentada el 21 de junio de 2022, por lo que aún se encuentra vigente en su trámite en la Asamblea Legislativa por los próximos 3 años. Sin embargo, la iniciativa no ha tenido movimiento desde el mes de septiembre de 2022, fecha en la que se asignó a estudio de la comisión de Tecnología y Educación.

    - La iniciativa indica que se deriva, entre otras fuentes de derecho, de leyes modelo de origen internacional, por lo que para su interpretación debe tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación. La iniciativa hace referencia a la necesidad de contar con regulación armonizada para regular el comercio electrónico (Artículo 2 Iniciativa 23.184 – Gobernanza de los servicios digitales y el comercio electrónico).

    - A su vez, la iniciativa procura delimitar su ámbito de aplicación a: i) los prestadores de servicios establecidos de Costa Rica y ii) los prestadores de servicios en otros estados cuando éstos sean ofrecidos a través de un establecimiento permanente en Costa Rica. Se entiende que un prestador de servicios se encuentra establecido en Costa Rica cuando su residencia o domicilio social se encuentra en territorio costarricense (Artículo 9 Iniciativa 23.184 – Gobernanza de los servicios digitales y el comercio electrónico).

    - De forma expresa la iniciativa regula que todo comerciante que no cuente con un establecimiento en Costa Rica y que realice comercio electrónico en el país se deberá regular conforme al Derecho Internacional Privado (electrónico).

    - En cuanto a la definición de consumidor, la iniciativa hace relación a la definición de consumidor que utiliza la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, Ley N° 7472. Esta normativa aplica la definición más amplia de consumidor.

[1] Dentro de la regulación en Costa Rica, las iniciativas de ley tienen una temporalidad de 4 años. Por lo que, transcurrido este plazo, sin que la iniciativa se haya aprobado y sin extensión aprobada por el pleno de la Asamblea Legislativa, las iniciativas se archivan.

A pesar de que a nivel legislativo en Costa Rica no hay regulación vigente que norme la actividad del Comercio Electrónico, existen disposiciones aplicables a esta actividad en el Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, Ley N° 7472.

En octubre 2017 el Ministerio de Economía, Industria y Comercio aprobó reformas al reglamento e incluyó el Capítulo X – Sobre la protección al Consumidor en el Contexto del Comercio Electrónico.

En el reglamento no se resuelve o aborda de ninguna forma la problemática de la territorialidad de la normativa. En cuanto a los alcances en las disposiciones de protección al consumidor, el reglamento no ofrece ninguna definición sobre qué se entiende por "consumidor". Sin embargo, en la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor Ley N° 7472, se implementa una definición amplia de "consumidor", regulando que se entiende como consumidor a toda persona física o entidad de hecho o de derecho, que, como destinatario final, adquiere, disfruta o utiliza los bienes o los servicios, o bien, recibe información o propuestas para ello. También se considera consumidor al pequeño industrial o al artesano (...) que adquiera productos terminados o insumos para integrarlos en los procesos para producir, transformar, comercializar o prestar servicios a terceros (Artículo 2 Ley N° 7472.).

Dentro de las disposiciones contenidas en el reglamento del Ministerio de Economía, Industria y Comercio, destaca una disposición que obliga a los comerciantes a abstenerse de realizar suscripciones automáticas a los usuarios. Esta práctica es común en las plataformas de streaming digitales, las cuales ofrecen un periodo de servicio gratuito. Al vencimiento de este periodo, se realiza la suscripción automática del usuario si este no cancela su cuenta antes del vencimiento de este periodo.

REPÚBLICA DOMINICANA

República Dominicana sí cuenta con un marco regulatorio vigente que regula el Comercio Electrónico, siendo este la Ley N° 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales.

Dicha ley hace referencia a la necesidad de tener en cuenta las recomendaciones de organismos multilaterales para su interpretación. Al igual que la iniciativa en Costa Rica, esta ley declara la necesidad de promover uniformidad en la regulación de esta actividad.

La ley no ofrece ninguna solución específica a la problemática sobre el ámbito de aplicación ni cuenta con un apartado especial para regular la protección del consumidor en el mercado electrónico.

EL SALVADOR

En El Salvador, se encuentra vigente el decreto N° 463 – Ley de Comercio Electrónico. Para resolver la problemática de la territorialidad, la ley determina de manera precisa quiénes son sujetos obligados. En este sentido, los limita a todas aquellas personas naturales o jurídicas, públicas o privadas establecidas en El Salvador que hagan transacciones comerciales utilizando la tecnología o por medio de redes de comunicación interconectadas. Además, de forma expresa manifiesta que cuando el proveedor de bienes se encuentre establecidos fuera del territorio, su actividad estará sujeta a lo que regulen convenios o tratados internacionales (Artículo 3 Ley de Comercio Electrónico Decreto N° 463).

La ley no cuenta con regulación específica para la protección al consumidor. Sin embargo, sí brinda una definición de usuario implementando una definición amplia indicando que se entenderá como usuario a toda persona, natural o jurídica, que por medios electrónicos contrate bienes o servicios, o reciba oferta de los mismos (Artículo 6 Ley de Comercio Electrónico Decreto N° 463).

GUATEMALA

Actualmente, Guatemala no cuenta con ninguna norma vigente que regule de forma específica el Comercio Electrónico. El primer paso que tomó este país fue la aprobación del Decreto 47-2008- Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas. Dentro de este cuerpo normativo, se incluyen disposiciones generales que podrían aplicarse al Comercio Electrónico. En coincidencia con el resto de los países, esta ley reconoce la necesidad de contar con regulación armonizada (Artículo 3, Decreto 47-2008- Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas).

Además, se encuentra en trámite la iniciativa 6029 – Ley para promover y facilitar el comercio electrónico transfronterizo, presentada en 2022 por los diputados Enrique Montano, Lázaro Zamora y Álvaro Arzú. A través de este proyecto se proponen reformas concretas a leyes tributarias, para otorgar claridad sobre las normas fiscales aplicables a las transacciones electrónicas.

La iniciativa, a diferencia de la norma vigente y de las iniciativas en los otros países, se enfoca en regular los negocios jurídicos que utilizan medios electrónicos entre proveedores y consumidores de bienes y servicios prestados desde el territorio nacional de Guatemala al extranjero. Asimismo, limita su ámbito de aplicación a todos los actos, negocios jurídicos o contratos lucrativos que se originen desde el territorio nacional por medios extranjeros al extranjero, y contiene una serie de reformas en materia tributaria para regular las cargas tributarias de este tipo de negociaciones.

Por lo que tampoco ofrece regulación en materia de protección al consumidor.

En cuanto a su estatus legislativo, la iniciativa cuenta con dictamen favorable de la comisión. Sin embargo, no se ha incluido en agenda para ser discutida en primer debate. Asimismo, con relación a la expectativa de que esta iniciativa avance en su trámite legislativo, es importante tomar en cuenta que en 2024 inicia una nueva legislatura y que solo uno de los ponentes fue reelecto para la legislatura 2024-2028. A pesar de lo anterior, la aprobación de esta sería de suma importancia para Guatemala porque precisamente evita el problema de dispersión normativa y adoptaríamos un set de normas armonizadas.

Cabe mencionar que en esta materia, a nivel internacional, rige la Convención de las Naciones Unidas sobre la utilización de las Comunicaciones Electrónicas en los Contratos Internacionales. Dicho convenio tiene como objetivo facilitar la utilización de las comunicaciones electrónicas en el comercio internacional, garantizando que los contratos concretados electrónicamente y las comunicaciones intercambiadas por medios electrónicos tengan la misma validez y sean igualmente ejecutables que los contratos y las comunicaciones tradicionales sobre papel.

Esta Convención, a su vez, se basa en instrumentos redactados anteriormente por la Comisión, en particular, en la Ley Modelo de la CNUDMI sobre Comercio Electrónico y en la Ley Modelo de la CNUDMI sobre las firmas electrónicas. Estos textos legislativos son de suma importancia ya que establecen principios claves sobre comercio electrónico tales como: la no discriminación, la neutralidad respecto de los medios técnicos y la equivalencia funcional. Guatemala, a la fecha, no ha ratificado la Convención, por lo que no es aplicable en territorio nacional. Ahora bien, es importante que la región centroamericana enfoque sus esfuerzos para ratificarla, ya que ésta es una norma internacional creada por expertos que facilita y hace más eficientes las transacciones electrónicas.

HONDURAS

En Honduras se encuentra vigente el Decreto 149-2024 -Ley sobre Comercio Electrónico. En concordancia con el resto de los países, la legislación de Honduras reconoce la necesidad de promover uniformidad en la regulación de esta materia.

La Ley no establece ningún mecanismo específico que permita entrever el ámbito territorial de su aplicación. Es decir, no limita su aplicación a los negocios que tengan un establecimiento en Honduras o a que la entrega de los bienes y el suministro de servicios se ejecuten dentro de dicho territorio. entrega de los bienes y suministro de servicios se ejecute dentro del territorio.

A su vez, en cuanto a la protección del consumidor, la ley da preeminencia a las disposiciones contenidas en las leyes vigentes en materia de protección al consumidor. En resumen, la transformación digital ha impulsado de forma rápida el crecimiento del comercio electrónico. Esta evolución ha sido respaldada por avances tecnológicos que crean un entorno propicio para el desarrollo del comercio electrónico. Sin embargo, la regulación de esta actividad se enfrenta a distintos desafíos, como la complejidad territorial y las normas de protección al consumidor.

A nivel legislativo, diferentes países de la región han abordado la regulación del comercio electrónico de manera dispar, lo que es un grave problema Lo más adecuado sería reconocer la importancia de contar con regulación armonizada y uniforme para facilitar el comercio electrónico. Costa Rica, por ejemplo, ha presentado diversas iniciativas, aunque ninguna ha prosperado hasta el momento. La última propuesta busca armonizar la regulación con leyes modelo internacionales y delimitar su ámbito de aplicación. En República Dominicana, existe una ley vigente, pero no ofrece disposiciones especiales a protección al consumidor. El Salvador y Honduras cuentan con legislaciones en vigor, que dan preeminencia a las leyes de protección al consumidor existentes. Guatemala, por su parte, se encuentra en proceso de legislar sobre el comercio electrónico, con una iniciativa que busca regular los negocios jurídicos transfronterizos. Sin embargo, aún no se ha discutido en el pleno del congreso.

Estos diferentes enfoques reflejan la complejidad y la diversidad de los desafíos que enfrenta la regulación del comercio electrónico en la región. **En este contexto, la cooperación internacional y la adopción de estándares comunes son cruciales para superar estos desafíos y promover un entorno seguro y eficiente para el comercio electrónico.**

REFERENCIAS

Barral Viñals, L. (2004). La regul@ción del comercio electrónico: (ed.). *Dykinson*, 59. electrónico, A. 1.–G. (n.d.).

Schneider, G. (2013). *Comercio electrónico:* (10 ed.). México: Cenegage Learning.

NORMAS DE PROTECCIÓN DE DATOS, INTELIGENCIA ARTIFICIAL Y CIBERSEGURIDAD: UN ANÁLISIS DE CENTROAMÉRICA Y REPÚBLICA DOMINICANA

Victoria Fernanda Méndez Echeverría

En la era digital, la regulación de la inteligencia artificial, la protección de datos y la ciberseguridad se han convertido en prioridades regulatorias. **Debido a la influencia regulatoria que tiene la Unión Europea en el mundo, estas áreas han adquirido relevancia en Centroamérica y República Dominicana, dando lugar a trasplantes de leyes y reglamentos.**

En Centroamérica varios países tienen normas vigentes o han presentado iniciativas de ley sobre protección de datos. Costa Rica cuenta con una ley vigente denominada Ley 8969- Ley para la Protección de la Persona frente al tratamiento de sus datos personales, aprobada en el 2011. Dicha ley tuvo como objetivo adecuar las normas costarricenses a los mayores estándares internacionales de protección de datos de la época, específicamente a la Directiva Europea de Protección de Datos de 1995 (Mok, 2010).

Ahora bien, las nuevas crisis tecnológicas y los avances legislativos han hecho que la Ley 8969 se quede corta. En este sentido, dentro de la Asamblea Legislativa de Costa Rica se encuentra en proceso de aprobación una nueva iniciativa de protección de datos personales denominada Iniciativa 23.097- Iniciativa de ley de protección de datos personales. Este proyecto, a la fecha, ha sido discutido en primer debate y ha sido actualizado a través de mociones de fondo. Tiene como objetivo adecuar las normas costarricenses al Reglamento General de Protección de Datos Personales (GDPR por sus siglas en inglés) de la Unión Europea (Exposición de Motivos Iniciativa de Ley 23.097).

Cabe mencionar que la posibilidad de avance de la Iniciativa 23.097 es alta, ya que su aprobación le permitirá a Costa Rica: i) ser un atractivo para la inversión digital proveniente de Europa y ii) adecuar su normativa interna y dar pleno cumplimiento a las directrices específicas de la OCDE en esta materia[2]. Ahora bien, cabe resaltar que **la Unión Europea siempre va un paso adelante: actualmente se está discutiendo una Ley de datos digitales. Por lo tanto, a pesar de que la aprobación de dicha iniciativa constituye un esfuerzo válido por parte del país centroamericano, su esquema jurídico que regula la protección de datos en el país no estará adecuado a los nuevos avances tecnológicos, por lo que sus relaciones pueden verse comprometidas.**

Por otra parte, en Guatemala no existe una norma vigente que regule este tema. Ahora bien, dentro del Congreso se encuentran presentadas tres iniciativas de ley. La primera de ellas es la Iniciativa 5921- Ley de Protección de Datos Personales presentada por los diputados Aníbal Estuardo Samayoa Alvarado y Douglas Rivero Mérida el 9 de junio del 2021. Esta norma determina los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales, considerando su interrelación con la vida y demás derechos de los ciudadanos. Actualmente el proyecto se encuentra pendiente de ser aprobado en los tres debates, ser aprobado por artículos y redacción final. El último movimiento legislativo fue en diciembre del 2021, cuando la Comisión de Educación emitió dictamen favorable.

La segunda de ellas es la Iniciativa 6105- Ley de Protección de Datos presentada por el diputado José Alejandro de León Maldonado el 24 de junio del 2022. Tiene como objetivo regular la protección y manejo de datos personales. Actualmente el proyecto se encuentra pendiente de ser aprobado en los tres debates, ser aprobado por artículos y redacción final. El último movimiento legislativo fue en abril de este año, cuando la Comisión de Transparencia y Probidad emitió dictamen favorable.

La tercera de ellas es la Iniciativa 6103- Ley Integral de Protección de Datos Personales en Poder de Terceros presentada por los diputados Hugo Ottoniel Rodríguez Chinchilla, José Alberto Rivera Nájera y Oscar Stuardo Chinchilla el 23 de junio del 2022. Tiene como objetivo garantizar la protección y tratamiento de los datos personales en poder de terceros. Actualmente el proyecto se encuentra pendiente de ser aprobado en tercer debate, ser aprobado por artículos y redacción final. El último movimiento legislativo fue en febrero de este año, cuando la iniciativa fue aprobada por el Pleno en segundo debate.

Cabe mencionar que la iniciativa 6103 toma como referencia al Reglamento General de Protección de Datos de la Unión Europea, el cual es uno de los modelos más estrictos sobre el tratamiento de datos personales e impone una serie de obligaciones que han sido incluso complicadas y confusas de cumplir para países de Europa.

De las tres iniciativas presentadas, la 6103 es la que tiene más posibilidad de

[2] Costa Rica acaba de adherirse a la OCDE. Se convirtió en el 38 miembro de la organización el 25 de mayo del 2021.

avance, ya que: i) es la única iniciativa que tuvo movimiento legislativo este año y ii) es la única iniciativa que se encuentra aprobada en segundo debate. Por lo tanto, está a dos pasos[3] de convertirse en ley, para después ser enviada al Ejecutivo para su sanción y promulgación.

Ahora bien, **en El Salvador no existe una norma vigente que regule la Protección de Datos, pero sí una Ley que regula el Historial Crediticio de las personas**. Dicha Ley se denomina Decreto Número 695– Ley de regulación de los servicios de información sobre el historial crediticio de las personas y tiene como objetivo garantizar el buen manejo de los datos crediticios de las personas[4]. Esta Ley aplica específicamente a los agentes económicos, personas naturales y personas jurídicas o privadas que manejen o tengan acceso a datos sobre el historial de crédito de las personas[5].

Dicha norma incluye disposiciones que pueden ser dañinas o peligrosas para el sector crediticio. Por ejemplo, la eliminación de los datos negativos del historial crediticio del consumidor luego de un plazo de tres años y la eliminación de los datos negativos del historial crediticio del consumidor luego de un año, si éste cancela su crédito. Este tipo de disposiciones que reconocen un amplio derecho al olvido, pueden reducir la calidad de las evaluaciones crediticias que se hacen.

Continuando con Honduras, resalta que, al igual que en Guatemala, no existe una norma vigente que regule este tema. No obstante, desde el año 2015 fue presentado al hemiciclo legislativo un proyecto de Ley de Protección de Datos Personales impulsado por el entonces vicepresidente del Congreso Nacional, el diputado Antonio Rivera Callejas. Dicha iniciativa se basó en el anteproyecto redactado por el Instituto Nacional de Acceso a la Información Pública y la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) en el 2013. Con su aprobación, Honduras esperaba adecuar su normativa interna a los mayores estándares internacionales de protección de datos de la época, específicamente a la Directiva Europea de Protección de Datos de 1995.

Actualmente el proyecto sigue en proceso de debate en el hemiciclo legislativo. El último debate se llevó a cabo en abril del 2018. Sin embargo, solo se han aprobado 19 de los 97 artículos que contiene el proyecto (Tomé, 2019). Cabe mencionar que su posibilidad de avance es baja, ya que lleva desde el 2018 sin movimiento. Asimismo, que **la norma es un poco desactualizada, ya que desde su presentación en el hemiciclo legislativo, la Unión Europea ha aprobado nuevas normativas sobre protección de datos.**

En República Dominicana, a diferencia de Guatemala y Honduras, existe una ley de protección de datos denominada Ley 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos y otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, la cual fue aprobada en el 2013. Esta

[3] Aprobación en tercer debate, aprobación por artículos y redacción final.
[4] Artículo 1 Decreto Número 695– Ley de regulación de los servicios de información sobre el historial crediticio de las personas.
[5] Artículo 2 Decreto Número 695– Ley de regulación de los servicios de información sobre el historial crediticio de las personas.

ley aplica a todos los datos de carácter personal registrados en cualquier banco de datos y a toda modalidad de uso posterior en el ámbito público o privado[6]. Ahora bien, no aplica para: i) el uso doméstico de datos personales; ii) el uso de datos personales de personas fallecidas; iii) los datos relacionados a personas jurídicas y personas físicas que presten servicios y iv) los registros llevados por organismos de investigación[7]. Cabe mencionar que, **a pesar de que dicha norma incorpora el principio de consentimiento del afectado, permite que la recolección y cesión de datos de acceso público, listas para fines mercadológicos y los datos obtenidos de una relación contractual se realice sin el consentimiento del afectado. Esto es beneficioso, ya que hace más eficiente y flexible el sistema, al no sobre regular datos que son de dominio público o que no contienen datos sensibles.**

Los avances legislativos recientes en materia de datos han hecho que la Ley 172-13 se quede corta. En este sentido, dentro del Senado de la República Dominicana, desde el año 2021, se encuentra en proceso de aprobación la Iniciativa 00486-2021-PLO-SE que tiene como objetivo modificar ciertos artículos de la Ley 172-13. Las reformas se enfocan principalmente en: i) limitar la capacidad de los organismos penales y de investigación de obtener y utilizar datos personales sin necesidad del consentimiento del titular; ii) limitar la capacidad de las fuerzas armadas, de seguridad y organismos policiales o de inteligencia para tener archivos de datos personales no sujetos a la ley y iii) hacer las sanciones más proporcionales y congruentes con el resto del texto de la Ley 172-13.

El último movimiento legislativo de la Iniciativa 0048-2021-PLO-SE fue en el 2021 con su asignación a la Comisión de Justicia y Derechos Humanos. Su posibilidad de avance es media, ya que lleva sin movimiento desde el 2021.

Con relación a la ciberseguridad, en Centroamérica y República Dominicana se han establecido estrategias y planes de acción para fortalecerla. Guatemala no cuenta con una norma vigente en esta materia[8]. No obstante, este año fue presentada en el Congreso la Iniciativa 6236- Reformas

[6]Artículo 2 Ley 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos y otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados.

[7]Artículo 4 Ley 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos y otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados y Sentencia TC-0484-16.

al Código Penal para tipificar delitos informáticos impulsada por los diputados José Alberto Rivera Nájera y Oscar Stuardo Chinchilla Guzmán. Este proyecto tiene como objetivo reformar el Código Penal para incluir a los delitos cibernéticos como un tipo delictivo. Algunos de los delitos cibernéticos que se incluyen son: i) engaño informático con fines sexuales; ii) acceso ilícito al uso de tecnologías de la información y las comunicaciones; iii) acceso ilícito a datos con información protegida, iv) intercepción ilícita de datos informáticos; v) ataque a la integridad de los datos; vi) falsificación informática; vii) fraude informático; viii) apropiación de identidad ajena, entre otros.

Actualmente el proyecto se encuentra pendiente de ser aprobado en los tres debates, ser aprobado por artículos y redacción final. El último movimiento legislativo fue en junio de este año, cuando fue enviada a la Comisión de Reformas al Sector Justicia.

En El Salvador los delitos cibernéticos están regulados en la Ley de Delitos Informáticos y Conexos, la cual fue aprobada en el 2016. Tiene como objetivo proteger a las personas de los delitos cometidos por las tecnologías de la información y comunicación. Dicha norma fue reformada en el año 2022 a través del decreto número 236, el cual fue aprobado por la Asamblea Legislativa a finales del 2021 y sancionado y publicado por el Presidente en el 2022.

La reforma tuvo como objetivo: i) incluir qué significan los términos "código malicioso" y "virus informático"; ii) agregar delitos informáticos relacionados a niños, niñas, adolescentes o personas con discapacidad y iii) agregar delitos informáticos relacionados con el contenido de los datos. Es importante mencionar que **en El Salvador, a diferencia de Guatemala, se creó una norma específica para regular la ciberdelincuencia. Por lo tanto, la Ley de Delitos Informáticos y Conexos es ley especial y en caso de conflicto entre normas, prevalecería sobre cualquier norma general, incluso sobre el mismo Código Penal.**

Costa Rica, al igual que Guatemala, no tiene una norma de ciberdelincuencia vigente. No obstante, dentro de la Asamblea Legislativa de Costa Rica se encuentra presentada la Iniciativa 23.292 Ley de Ciberseguridad de Costa Rica, que tiene como objetivo regular el resguardo y la protección de la seguridad cibernética de las infraestructuras tecnológicas críticas del país en las instituciones del Gobierno Central, Descentralizadas y Semiautónomas. A diferencia de la iniciativa de ley de Guatemala y la ley vigente de El Salvador, la Iniciativa 23.292 se limita a regular los delitos cibernéticos

[8] En el año 2022 el Congreso aprobó la iniciativa 5601- Ley de Prevención y Protección contra la ciberdelincuencia, a través del Decreto 39-2022. Ahora bien, ésta fue archivada 20 días después de su aprobación, por lo que no llegó al Ejecutivo ni entró en vigencia en territorio nacional.

que puedan perjudicar la infraestructura tecnológica de las instituciones del país. Por lo tanto, es una norma más concreta.

Su último movimiento legislativo fue en diciembre del 2023, cuando regresó a la Comisión de Tecnología y Educación por mociones de fondo. Cabe mencionar que esta norma tiene una probabilidad de avance grande, ya que **Costa Rica se caracteriza por cumplir con parámetros y estándares promulgados por la Unión Europea, siendo uno de ellos la protección contra los delitos cibernéticos.**

En República Dominicana la ciberseguridad se ha promovido a través de distintos instrumentos. En el año 2007 se aprobó la Ley 53-07 sobre crímenes y delitos de Alta Tecnología. Dicha norma tiene como objetivo prevenir y sancionar los delitos cometidos contra las tecnologías de información y comunicación. Esta norma incluye delitos relacionados con los datos y la confidencialidad, tales como: la clonación de dispositivos de acceso, el uso de datos por acceso ilícito, daño o alteración de datos, sabotaje, intercepción de datos, entre otros. Asimismo delitos relacionados con las personas, tales como: la difamación, estafa, chantaje, robo mediante uso de la tecnología, entre otros.

Luego, en el 2018, mediante el Decreto 230-18 se creó la Estrategia Nacional de Ciberseguridad 2018-2021, la cual proponía crear un marco regulatorio para fortalecer la gestión de la ciberseguridad. Para cumplir con dichos fines, en el año 2021 se presentó en el Senado la Iniciativa 00636-2021-PLO-SE que tiene como objetivo fortalecer el marco normativo para la gestión de la seguridad cibernética de las tecnologías de la Administración Pública y de las infraestructuras críticas en la República Dominicana. Su último movimiento legislativo fue en marzo del 2023, cuando fue aprobada en segundo debate por el Senado y presentada en la Cámara de Diputados.

Dicho proyecto, al igual que iniciativa costarricense, se enfoca principalmente en proteger las tecnologías de las instituciones gubernamentales, por lo que es más precisa. Asimismo, se fundamenta en los principios incluidos en el Llamado de París del 12 de noviembre del 2018 para la Confianza y la Seguridad del Ciberespacio y en la Resolución de la Asamblea General de las Naciones Unidas A/70/174 del 22 de julio de 2015 sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. Su posibilidad de avance es media, ya que su último movimiento legislativo es reciente. Asimismo, porque ya fue aprobada en una de las instancias legislativas.

Cabe mencionar que **en Centroamérica y República Dominicana no existen regulaciones específicas para el uso de la Inteligencia Artificial. A pesar de ello, en virtud de la influencia regulatoria que tiene la Unión Europea en el mundo, no falta mucho para que esta área adquiera relevancia en la región, dando lugar a trasplantes de leyes y reglamentos.**

En conclusión, en Centroamérica y el Caribe la protección de datos, la inteligencia artificial y la ciberseguridad están adquiriendo mayor importancia en el contexto digital. Aunque existen diferencias en las normativas y enfoques adoptados por los países de la región, el reconocimiento de la necesidad de abordar estos aspectos es común. Cabe mencionar que, para evitar estas diferencias, **sería interesante que los países de Centroamérica y el Caribe exploraran la posibilidad de promover marcos normativos homogéneos, a través de un Reglamento Técnico Centroamericano, un Reglamento aplicable en la Región o un Tratado Internacional en esta materia.**

REFERENCIAS

Amir Mohammed, Fasil Muddeen, Lincoln Marine, Craig J. Ramlal. (2023). The Exigency for Resilient and Cyber-Secure Critical Infrastructure in the Caribbean. *The West Indian Journal of Engineering*, 35-49.

CEPAL. (2020). *Elementos principales del informe sobre el estado de la jurisdicción de internet en América Latina y el Caribe.* Naciones Unidas, Santiago: Naciones Unidas.

Data Protection Laws of the world. (2023, noviembre 29). Retrieved from https://www.dlapiperdataprotection.com/index.html?t=law&c=BB#:~:text=The%20Data%20Protection%20Act%20(the,relation%20to%20their%20personal%20data.

Data Protection Laws of the World: Trinidad y Tobago. (2023). *DLA PIPER*.

Exposición de Motivos Iniciativa de Ley 23.097. (n.d.).

Mok, D. S. (2010). Privacidad y Protección de datos: un análisis de legislación comparada. *Revista electrónica de Historia, 38.*

Osorio, J. (2023). HACIA UNA GOBERNANZA DE LA INTELIGENCIA ARTIFICIAL EN LA REGIÓN CENTROAMERICANA. *EKTENOS/ ISSN: L 2710-7485, 60-83.*

Quiñones, E. O. (2022). *Prospectiva y planificación en la era de la inteligencia artificial en América Latina y el Caribe.* Huancayo: Fondo Editorial.

Tomé, E. (2019). Estudio Centroamericano de Protección de Datos, Honduras. *Instituto Panameño de Derecho y Nuevas Tecnologías, 22.*

EL SALVADOR: A DOS AÑOS DE QUE BITCOIN SEA MONEDA DE CURSO LEGAL

María Alejandra Barillas Gordillo

El 7 de septiembre de 2021 marcó un hito en la historia económica de El Salvador, cuando se convirtió en el primer país en adoptar el Bitcoin como moneda de curso legal. Ahora, dos años después de esta decisión sin precedentes, es pertinente realizar un análisis postlegislativo para evaluar los impactos y desafíos que esta medida trajo consigo y los efectos que la misma ha tenido en la región.

La Ley Bitcoin, Decreto Legislativo no. 57, fue aprobada por la Asamblea Legislativa. Esto posicionó el Bitcoin como moneda de curso legal junto al dólar estadounidense en El Salvador. Esta ley fue impulsada por el presidente Nayib Bukele, quien argumentó que la adopción de Bitcoin podría mejorar la inclusión financiera y fomentar la inversión extranjera en el país, convirtiéndolo en un país líder en el mercado de monedas digitales (Hartley).

El impacto económico de la ley en el país fue significativo. Por un lado, se observó un aumento en la adopción de Bitcoin dentro del país, con la apertura de cajeros automáticos y la aceptación de Bitcoin como forma de pago en diversos comercios, aunque al principio hubo renuencia a hacerlo por la falta de entendimiento de cómo funcionaba. **Como era de esperarse, el desafío más grande que se enfrentó fue la volatilidad del precio de Bitcoin y la falta de infraestructura financiera para respaldar adecuadamente esta nueva forma de transacción.** Este riesgo se trató de reducir creando un fideicomiso por 150 millones de dólares para conversión de bitcoin, el que sería administrado por el Banco de Desarrollo de El Salvador, el cual quedó plasmado en la Ley de Creación del Fideicomiso Bitcoin, Decreto Legislativo no. 137.

El marco jurídico inicial de Bitcoin en el país vecino incluía: el Reglamento de la Ley Bitcoin; las Normas Técnicas para Facilitar la Participación de las Entidades Financieras en el Ecosistema Bitcoin; los Lineamientos para la autorización del funcionamiento de la Plataforma tecnológica de servicios con Bitcoin y dólares y, en materia de ciberdelitos, las reformas a la Ley de Delitos Informáticos y Conexos relativas al fraude informático mediante transacciones en Bitcoin y otras criptomonedas. **A pesar de la existencia de estas normas, resalta que la falta de claridad en los marcos legales y algunas lagunas legislativas generaron incertidumbre para los actores económicos y para los ciudadanos.**

La preocupación por el uso de Bitcoin en actividades ilícitas y su potencial para facilitar el lavado de dinero requirió una respuesta regulatoria más sólida por parte del gobierno. El Salvador no cumplía con las recomendaciones emitidas por el GAFI sobre la supervisión o monitoreo, sanción a proveedores de servicios de activos virtuales (PSAV) (GAFILAT, 2023). Por lo que, en los años subsiguientes, se complementó el marco jurídico primario con: la Guía para Proveedores de Servicios de Activos Virtuales sobre Cumplimiento de Obligaciones en Materia de Lavado de Activos y Contra el Financiamiento del Terrorismo; la Creación de la Oficina Nacional del Bitcoin, y la Ley de Emisión de Activos Digitales, Decreto Legislativo no. 643, aprobada por la Asamblea este año (GAFILAT, Recomendación 15. Nuevas tecnologías, 2023).

Uno de los principales argumentos a favor de la adopción de Bitcoin fue su potencial para fomentar la inclusión financiera en El Salvador. Sin embargo, dos años después, persisten desafíos significativos en este aspecto. **La falta de educación financiera y la limitada infraestructura tecnológica han dificultado la participación de sectores vulnerables de la población en el ecosistema Bitcoin.**

La adopción del Bitcoin como moneda de curso legal ha sido criticada por el Fondo Monetario Internacional quien en el reporte de 2022 estableció que: *"... hay grandes riesgos asociados al uso de Bitcoin para la estabilidad financiera, la integridad financiera y la protección del consumidor, así como las posibles contingencias fiscales"*. En este sentido, instaron a las autoridades a limitar el alcance de la ley Bitcoin eliminando su calidad de moneda de curso legal. Algunos directores también manifestaron su preocupación sobre los riesgos asociados a la emisión de bonos respaldados por Bitcoin (Elnagar, 2022).

A pesar de los desafíos y las críticas que ha enfrentado la adopción de Bitcoin en El Salvador, es importante destacar que la experiencia del país puede servir como lección para otros Estados interesados en explorar la adopción de criptomonedas como moneda de curso legal (Daniel Cooper y Nina Kruglikova, 2022). Unos meses después de la adopción del Bitcoin en El Salvador, la República Centroafricana aprobó una ley similar pero fue reformada un año después eliminando la obligatoriedad del uso de la misma (Vanci, 2023).

En 2022, la Asamblea de Paraguay aprobó la Ley de la minería, comercialización, intermediación, intercambio, transferencia, custodia y administración de criptoactivos o instrumentos que permitan el control sobre criptoactivos, sin embargo el Ejecutivo vetó la ley y la misma quedó archivada (Herrera, 2022) (Comunicación, 2022).

Las lecciones aprendidas de El Salvador podrían ayudar a desarrollar marcos regulatorios más sólidos y a abordar los desafíos inherentes a esta innovación financiera. En definitiva, **El Salvador ha sentado las bases a nivel regional para una mayor exploración de las criptomonedas en el ámbito legal, económico y regulatorio.**

REFERENCIAS

Comunicación, D. d. (2022, diciembre 5). Archivan proyecto de ley que regula comercialización y administración de criptomonedas.

Daniel Cooper y Nina Kruglikova. (2022). Strike Mission: El Salvador, Blockchain Technology, and Sustainable Development. *Multistakeholder Forum on Science, Technology and Innovation for the SDGs, 3*.

Elnagar, R. (2022, enero 25). El Directorio Ejecutivo del FMI concluye la Consulta del Artículo IV con El Salvador correspondiente a 2021. *Fondo Monetario Internacional*.

GAFILAT. (2023). *Guía para la Regulación ALA/CFT de Activos Virtuales y Proveedores de Servicios de Activos Virtuales en la Región del GAFILAT*. Retrieved from https://gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/guias-17/4580-guia-para-la-regulacion-alacft-av-psav/file

GAFILAT. (2023, diciembre 7). *Recomendación 15. Nuevas tecnologías.* Retrieved from https://www.cfatf-gafic.org/index.php/es/documentos/gafi40-recomendaciones/421-fatf-recomendacion-15-nuevas-tecnologias

Hartley, J. (n.d.). Pre-Analysis plan for “The El Salvador Bitcoin Monetary Experiment”. . *Standford University.*

Herrera, J. (2022, diciembre 6). Ley Bitcoin de Paraguay es archivada y la regulación queda «en el aire». *Criptonoticias.*

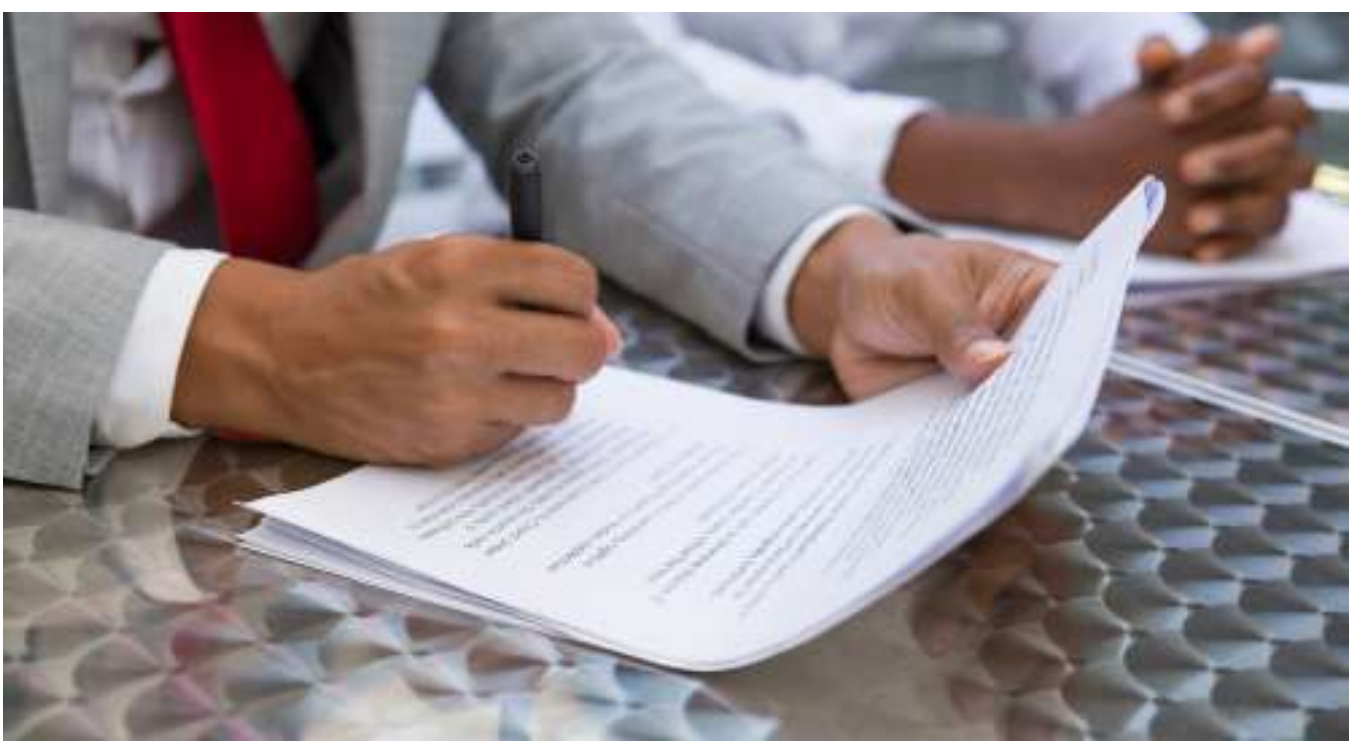
Vanci, M. (2023, marzo 23). República Centroafricana cambia su Ley Bitcoin y abandona la ruta señalada por El Salvador. *Criptonoticias*.

BITCOIN, MONEDA DE CURSO LEGAL

María Isabel Carrascosa Coll

La moneda de curso legal (o *legal tender*) se define como el dinero que es legalmente válido para el pago de deudas y que debe ser aceptado para ese fin cuando se ofrece (Merriam-Webster, 2023). En este sentido, **al convertirse Bitcoin en moneda de curso legal en El Salvador, este país no sólo reconoció su libre circulación en el país, sino también su poder liberatorio para el pago de cualquier obligación, especialmente para el pago de impuestos** (Goldberg, 2009) (Tello, 2023)**. Esto no solo tuvo efectos para El Salvador sino para el resto del mundo.** En este artículo examinaremos el efecto en Guatemala y en Estados Unidos.

Las divisas son reconocidas a nivel global como las monedas extranjeras que han sido reconocidas en otros países y tienen poder liberatorio para el pago de deudas. Antes de que El Salvador le diera status de moneda de curso legal, los bancos centrales argumentaban que el Bitcoin no era divisa pues ningún país la reconocía como dinero legal (Monzón, 2016).



A pesar de que El Salvador considera Bitcoin como moneda de curso legal, Guatemala no lo reconoce como divisa. A finales de la década de los noventas, en Guatemala se emitieron varias leyes que buscaron hacer una modernización financiera. Este proceso de reforma integral implicó un cambio en la concepción del papel de la banca central y en la orientación de la regulación financiera. Derivado de esto se emitieron las siguientes leyes: Ley Orgánica del Banco de Guatemala, decreto 12-2002,; Ley Monetaria, decreto 17-2002; Ley de Bancos y Grupos Financieros, decreto 19 - 2002 y Ley de Supervisión Financiera, decreto 18-2002, cuya vigencia inició el 1 de junio de 2002. Estas normas, junto con la Ley de Libre Negociación de Divisas, decreto 04-2000, que cobró vigencia casi un año antes, constituyen un cuerpo integral de regulación financiera que concede al sistema de banca central el deber de ejercer la vigilancia sobre la circulación de la moneda, pero que también permite la libertad de las personas para negociar con divisas, asumiendo ellas los riesgos que pueden derivar de esto. Previo a este paso de modernización financiera, la libre circulación de divisas en el país estaba restringida. En Guatemala además de la libre negociación de divisas, las transacciones por la convertibilidad de éstas están exentas de impuestos. **Nuestra ley considera a las divisas como monedas extranjeras, reconociéndole a las dos poder liberatorio de obligaciones siempre que sea un acuerdo voluntario entre las partes y ambas se responsabilicen de las pérdidas o riesgos que esto implique.**

Y es precisamente en esa línea de argumento que se debería de cuestionar el status de Bitcoin en Guatemala. ¿Es una divisa porque el país vecino la reconoció en ley como moneda de curso legal? ¿Tendría que dársele el mismo tratamiento legal que tienen los euros, los dólares o los yenes? Si el tratamiento que el Estado le diera fuera de divisa, cuando se negocie con Bitcoin las únicas obligadas a reconocerla como medio de pago válido son las partes del contrato. . Ahora bien, también debería poder reconocerse judicialmente una compraventa hecha con Bitcoin válidamente y así consecuentemente registrar un bien inmueble adquirido en Bitcoin, como se reconocen las compraventas de bienes inmuebles en dólares. Esto de ninguna forma implica que el Bitcoin se convierta en el país en una moneda de curso legal con poder liberatorio impuesto u obligado pues esto corresponde únicamente al Quetzal, pero si implica que puede circular libremente cuando existe voluntad de las partes.

Por su parte, el Banco de Guatemala en una publicación llamada Las Monedas Criptográficas en Guatemala: análisis técnico y jurídico, publicada en 2016 explicó lo siguiente sobre el Bitcoin:

"En Guatemala también podría asociarse a Bitcoin y similares con una divisa, en internet es común evidenciar la asociación de Bitcoin con una divisa, especialmente en medios de comunicación periodística. ***Se entiende que una divisa es la moneda de curso legal de un estado, Bitcoin no pertenece a ningún estado y no ha sido adoptada como moneda oficial o de curso legal por***

ningún país. *Sería difícil pensar que un estado con un sistema de banca central adopte una moneda criptográfica descentralizada y global, que no puede ser controlada, como moneda oficial. Sin embargo, algunos países empiezan a considerar la creación de una moneda criptográfica emitida y controlada por el banco central" (resaltado propio)* (Monzón, 2016).

En ese entonces, Bitcoin no había sido reconocido como moneda de curso legal en ningún país, argumento sobre el cual descansaba la postura del Banguat.

Algunos años después, ya con el desarrollo de las monedas criptográficas más avanzado, la Superintendencia de Bancos justo antes (en febrero 2021) de que El Salvador emitiera la Ley Bitcoin (8 de junio 2021) emitió un comunicado informando que las monedas virtuales no se consideraban divisas y que las plataformas transaccionales o personas, quesededicanalaventaycomercialización de monedas virtuales en Guatemala, no se encuentran bajo la vigilancia ni inspección de la Superintendencia de Bancos (Guatemala, 2021).

Finalmente, **cabe resaltar que a diciembre de 2023, no existe en el Congreso de la República ninguna iniciativa de ley que aclare la situación de las criptomonedas en el país. Tampoco ha habido una respuesta a nivel regulatorio del problema jurídico que en este texto se plantea con respecto del Bitcoin**, sobre todo tomando en cuenta que nuestro país vecino y socio comercial ya lleva más de dos años reconociéndola como moneda de curso legal.

REFERENCIAS

Goldberg, D. (2009). *Legal tender No 2009-04.* Leibniz Information Centre for Economics.

Guatemala, S. d. (2021). Comunicado de Prensa. *Superintendencia de Bancos de Guatemala*, 1.

Merriam-Webster. (2023, diciembre 8). *Merriam-Webster*. Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/legal%20tender

Monzón, D. A. (2016). *Las monedas criptográficas en Guatemala (análisis técnico y jurídico).* Guatemala: Banco de Guatemala.

Tello, M. P. (2023, diciembre 8). *Criptomonedas: su tributación, un análisis comparado.* Retrieved from https://derecho.udd.cl/actualidad-juridica/files/2021/01/AJ39_113.pdf

GUATEMALA: EL PROBLEMA DE LOS TRASPLANTES JURÍDICOS DESCONTEXTUALIZADOS

María Alejandra Barillas Gordillo

El mundo se encuentra en un constante intercambio de ideas. Este intercambio no sólo se refiere a información, noticias o contenido, sino también a experiencias jurídicas. La experiencia jurídica que un país o región ha tenido se transfiere a otro, a través de lo que técnicamente se conoce como "trasplante jurídico". Este proceso implica la adopción de normas y principios legales de otros sistemas jurídicos con el fin de encontrar una solución a un problema regulatorio desatendido y mejorar y modernizar el marco legal de un país.

En el caso de Guatemala se ha observado una preocupante tendencia hacia la adopción de trasplantes jurídicos descontextualizados, lo que plantea desafíos significativos en términos de eficacia y adecuación a la realidad guatemalteca.

El trasplante jurídico es una práctica común en el derecho comparado, que implica importar ideas y soluciones legales de otros sistemas jurídicos. Con esto se busca aprovechar las mejores prácticas y experiencias de otros países para fortalecer el sistema legal propio. Sin embargo, es importante destacar que para que los trasplantes jurídicos tengan una mayor probabilidad de éxito, requieren un análisis cuidadoso del contexto social, cultural, político y económico en el que se insertarán.

Todos estos contextos, sobre los cuales se construye la cultura jurídica de un país, son un elemento fundamental que se debe considerar previo a adoptar trasplantes jurídicos. Las normas y principios legales deben ser adaptados y ajustados para que sean coherentes con la realidad y las necesidades del sistema legal guatemalteco. **Ignorar el contexto puede llevar a la creación de leyes que no son aplicables, resultan ineficientes o incluso generan efectos contraproducentes.**

El derecho comparado desempeña un papel fundamental en la adopción de trasplantes jurídicos adecuados, pues estos estudios permiten identificar y comprender las similitudes y diferencias entre los sistemas legales, así como evaluar la viabilidad y pertinencia de las normas propuestas. Esto implica realizar análisis exhaustivos, por lo que es esencial fomentar la investigación jurídica nacional y fortalecer las capacidades internas de los entes reguladores para que estos puedan plantear soluciones mejor contextualizadas.

Un ejemplo de esto, que se vio durante el 2023, es la discusión de una ley de protección de datos personales para Guatemala en el Congreso de la República. **En Guatemala, la protección de datos personales debería ser**

un tema de creciente importancia debido a los avances tecnológicos y la creciente digitalización de la sociedad, sin embargo existe poca educación sobre la protección de datos personales en poder de privados y un sentir social que circunscribe la protección de datos a situaciones como la existencia de listas negras que, aprovechándose del vacío legal, comercializan datos personales sin garantías para sus titulares. Por lo mismo, la implementación de una ley de protección de datos efectiva es fundamental para salvaguardar la privacidad y los derechos de los guatemaltecos, sin que esto llegue a tener efectos contraproducentes en su economía o acceso al crédito.

Es claro que en otras latitudes ya existe regulación eficiente sobre protección de datos, que incluso trata la información financiera y crediticia de una persona de forma distinta, pues existe una razón legítima para limitar ciertos derechos respecto de estos o regularlos diferente. **Por lo mismo, sabemos que Guatemala no necesita inventar un nuevo modelo regulatorio, pero si necesita estudiar los modelos existentes y trasplantar uno que se adecúe a su contexto social y económico.**

Es importante considerar que el modelo regulatorio de la Unión Europea (UE), como el Reglamento General de Protección de Datos (GDPR) es un referente a nivel mundial de estándares en materia de privacidad y protección de datos personales. Sin embargo, este puede no ser adecuado para ser adoptado en su totalidad por Guatemala. **Existen varias razones por las cuales el modelo regulatorio de la UE no sería fácilmente aplicable a Guatemala. Entre ellas se debe tener en cuenta que Guatemala tiene realidades socioeconómicas y culturales diferentes a las de los países europeos. El modelo europeo se basa en una economía más desarrollada y, sobre todo, en una infraestructura tecnológica más avanzada.**

Otro punto importante a considerar es la capacidad institucional y el marco legal existente en Guatemala. En nuestro país no existe todavía regulación específica para ningún tipo de dato, fuera de lo que establece sobre el habeas data la Ley de Acceso a la Información Pública y la Constitución, lo cual implica que no tenemos normativa específica que por ejemplo, trate de forma distinta los datos financieros o crediticios de las personas[11], una excepción que es común en los modelos regulatorios existentes sobre protección de datos. **La adopción directa del modelo regulatorio de la UE, que si incluye esta excepción, requeriría entonces cambios significativos en las estructuras gubernamentales y legales del país que aún no existen, lo que podría generar dificultades en términos de implementación y cumplimiento.** A esto habría que sumarle la falta de recursos y experiencia en términos de aplicación y supervisión que representan un reto adicional.

Por lo mismo, en lugar de adoptar el modelo regulatorio de la UE en su totalidad, Guatemala podría beneficiarse de un enfoque adaptado a sus necesidades específicas. Hay que tomar en cuenta que la UE no logró consolidar su regulación sobre datos de la nada, sino fue un proceso de evolución gradual que

[11] La Corte de Constitucionalidad mediante fallos ha introducido al ordenamiento jurídico ciertas normas y garantías que deben respetarse en cuanto a la protección de datos. Ver expediente 3552 – 2014 de la CC.

inició en 1995 con su primer reglamento sobre datos, el cual fue reformado en 2016 con base en la experiencia y nuevas tecnologías surgidas. **Esto evidencia que para desarrollar una legislación de protección de datos, si bien sirve de base un modelo regulatorio garantista de los derechos de los ciudadanos a la privacidad, también hay que tener en cuenta las características propias del país receptor del trasplante, para que este sea el resultado de un análisis exhaustivo de nuestro entorno legal, económico y cultural y pueda ser exitoso.**

REFERENCIAS

Albrecht, J. P. (2016). How the GDPR will change the world. Eur. Data Prot. L. Rev., 2, 287.

Besson, S. (2012). Comparative law and legal change: The impact of comparative law on the legal development in transition countries. East European Politics and Societies, 26(1), 7-28.

Watson, A. (2014). Legal transplants and European private law. Oxford University Press.

Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. ACM Transactions on Management Information Systems (TMIS), 12(1), 1-20.

Zimmermann, R., & Visser, D. P. (Eds.). (2018). Comparative law and private international law. Oxford University Press.

LA LEY DE DATOS EN COSTA RICA: PROTEGIENDO LA PRIVACIDAD EN LA ERA DIGITAL

Victoria Fernanda Méndez Echeverría

En la era digital, la obtención y el manejo adecuado de la información personal es esencial. El uso de las Tecnologías de la Información y la Comunicación ha permitido que los datos personales se obtengan y transmitan con mayor facilidad. En muchas ocasiones, esta información es utilizada para fines distintos a los que originalmente fueron recabados. Con el creciente avance de la tecnología y la digitalización de la información, es fundamental contar con marcos legales sólidos que protejan la privacidad de las personas (Barrantes, 2019).

Costa Rica fue el primer país centroamericano en contar con una Ley de Protección de Datos Personales[12]. Esta proactividad del país centroamericano fue motivada por distintos factores: la necesidad de proteger la privacidad de las personas; el deseo de armonizar las normas internas con los estándares internacionales en materia de protección de datos, específicamente con la Directiva Europea de Protección de Datos; la necesidad de proteger los derechos de privacidad, autodeterminación y el control sobre datos personales de la persona y el deseo de fomentar la confianza del uso de servicios digitales (Mok, 2010).

La Ley de Datos Personales, como su nombre lo dice, tiene como objetivo proteger todos aquellos datos que se clasifican como "personales". Para lograr este cometido, incluye principios como el de "consentimiento informado", el cual obliga al receptor de datos a informarle al emisor de la existencia de una base de datos y los fines que se persiguen con la recolección de datos (Artículo 5- Ley 8968). Asimismo, obliga al titular de la base de datos a verificar que los datos almacenados sean verídicos, exactos, adecuados y estén actualizados, por lo que el receptor de datos no podrá almacenarlos por más de 10 años (Artículo 6- Ley 8968). También le otorga al emisor de los datos el derecho de acceder, rectificar y suprimir los datos que se tienen de su persona (Artículo 7- Ley 8968, 2023). Cabe mencionar que la norma regula sanciones pecuniarias para todos aquellos que incumplan sus deberes, las cuales van desde 5 salarios base hasta 15-30 salarios base y la suspensión para el funcionamiento de 1-6 meses (Artículo 28- Ley 8968).

Si bien la ley de datos en Costa Rica ha sido un paso importante en la protección de la privacidad y los derechos de los ciudadanos en el entorno digital, también tiene ciertas carencias. La primera de ellas consiste en que la ley no es del todo clara. Un ejemplo de ello es la falta de precisión

[12] Ley 8969- Ley para la Protección de la Persona frente al tratamiento de sus datos personales. Aprobada en el 2011.

en la definición de "datos personales". La norma los describe como: "*cualquier dato relativo a una persona física identificada o identificable*" (Artículo 2 Ley 8968). En este sentido, dentro de este concepto podrían caber datos efectivamente personales, así como datos que no son propiamente de carácter personal. Por lo tanto, esta ausencia de claridad puede ocasionar interpretaciones ambiguas y dificultades en la aplicación de la ley.

La segunda de ellas consiste en que no existen procedimientos claros y predefinidos para que los titulares de los datos soliciten su rectificación o supresión. Si bien es cierto que estos derechos están reconocidos en la ley, dicha norma y su reglamento no indican un procedimiento específico para realizar este tipo de reclamaciones. Al contrario, permiten al receptor de la información determinar el procedimiento interno para realizarlas (Artículo 32 Decreto Ejecutivo 37554, Reglamento de la ley 8968).

La última de ellas consiste en que **la aplicación de esta norma genera grandes desafíos monetarios y tecnológicos para las empresas y más aún para aquellas que son pequeñas o tienen recursos limitados.** El cumplimiento de la ley obliga a las entidades a invertir recursos en la elaboración de protocolos y mecanismos internos de manejo y obtención de datos. Esta brecha se vuelve más relevante cuando se comprende que, además de invertir en los protocolos y mecanismos, las entidades pueden ser multadas e incluso suspendidas por el fallo o uso inadecuado de sus protocolos. Por consiguiente, es importante la proporcionalidad en la imposición de sanciones y la aplicación de la ley.

Las nuevas crisis tecnológicas y los avances legislativos en materia de protección de datos en el mundo han hecho que la Ley de Datos vigente se quede corta. En este sentido, dentro de la Asamblea Legislativa de Costa Rica se encuentra en proceso de aprobación una nueva Iniciativa de Ley de Protección de Datos Personales[13].

Con la aprobación de esta ley Costa Rica adecuará sus normas a los más altos estándares en la protección de datos, específicamente al Reglamento General de Protección de Datos Personales (RGPDP). Asimismo, será un atractivo para la inversión digital proveniente de Europa, al ser un puerto seguro para las transferencias internacionales de datos. Finalmente, tras su reciente ingreso a la OCDE[14], podrá adecuar su normativa interna y darle pleno cumplimiento a las directrices específicas que dicho organismo tiene en esta materia (Exposición de Motivos Iniciativa de Ley 23.097).

[13] Iniciativa 23.097- Iniciativa de ley de protección de datos personales.
[14] Se convirtió en el 38 miembro de la organización el 25 de mayo del 2021.

Ahora bien, a pesar que estos esfuerzos son válidos, dentro de la Unión Europea actualmente se está aprobando una Ley de datos digitales. Por lo tanto, a pesar de que esta iniciativa de ley se apruebe y quede vigente en Costa Rica, el esquema jurídico que regula la protección de datos en el país no estará adecuado a los nuevos avances tecnológicos en la UE, por lo que sus relaciones comerciales pueden verse comprometidas o afectadas.

Cabe mencionar que los datos financieros, a diferencia de los personales, no se encuentran protegidos por estas normativas. En general, los datos personales están protegidos por normas de privacidad que requieren del consentimiento informado del titular de los datos para su recopilación y uso. Ahora bien, esto no aplica a los datos financieros, ya que muchas veces el procesamiento de este tipo de información es necesario para la ejecución de un contrato o para cumplir con una obligación legal. En este sentido, esta necesidad legítima de proteger los derechos de terceras personas permite darles un tratamiento distinto.

En conclusión, Costa Rica está altamente influenciada por la Unión Europea. La ley de protección de datos vigente y la iniciativa de ley 23.097 se fundamentaron en parámetros establecidos por la UE en protección de datos. **Este es un ejemplo claro del efecto Bruselas y el poder de influencia de la UE en Centroamérica. Ahora bien, es importante mencionar que este deseo por cumplir parámetros internacionales es riesgoso si éstos no se adecúan al contexto social, político, económico y cultural del país al que se están aplicando.** En este sentido, es importante que, en la lucha por promover normas y acoplarse a la era digital, los países analicen qué parámetros son prácticamente posibles de cumplir y cuáles no. Incluir protocolos o parámetros no adecuados puede ocasionar la inaplicabilidad de las normas o la aplicación arbitraria de las mismas. Esto genera un riesgo para la industria, ya que puede generar obligaciones económicas o tecnológicamente difíciles de cumplir.

REFERENCIAS

Barrantes, V. R. (2019). Realidad sobre la privacidad de datos personales en Costa Rica. *e-ciencias de la información*, 13.

Exposición de Motivos Iniciativa de Ley 23.097. (n.d.).

Mok, D. S. (2010). Privacidad y Protección de datos: un análisis de legislación comparada. *Revista electrónica de Historia*, 38.

Ley 8968. (n.d.). Retrieved from http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989

INSUFICIENCIA DE LA REGULACIÓN EN MATERIA DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD EN LA REPÚBLICA DOMINICANA

Luis Ernesto Peña Jiménez

La proliferación del mundo digital ha traído muchas ventajas a la vida en sociedad, pero también muchos retos. El principal: la protección en la interacción personal y el uso de los datos que en esos intercambios se dan. Bajo ese contexto, la necesidad de protección y regulación de escenarios para evitar el abuso abundan, y las maneras de burlar dichas regulaciones avanzan con el mismo ímpetu con el que evolucionan las tecnologías que soportan la interacción digital.

La República Dominicana no ha sido ajena a dicha realidad, y por eso desde muy temprano se ha dotado de las legislaciones necesarias para enfrentarla. Hoy en día, se pueden mencionar la Ley General de Telecomunicaciones No. 153-98; Ley General de Libre Acceso a la Información Pública No. 200-04; la Ley No. 126-02 sobre el Comercio Electrónico, Documentos y Firmas Digitales y la más reciente, la Ley No. 172-14 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados.

De hecho, **el reconocimiento de la importancia de la regulación en la materia viene refrendada por jurisprudencia constante de nuestro Tribunal Constitucional, el cual ha considerado que el derecho a la autodeterminación informativa y protección de datos constituye un derecho fundamental** derivado del derecho a la intimidad de conformidad

[15] TC/0044/17 del 31 de enero de 2017.

con el artículo 44 de la Constitución dominicana de 2015.

Así lo ha contemplado en varias ocasiones, cuando ha dispuesto que "*el derecho a la autodeterminación informativa está contemplado en el artículo 44.2 de la Constitución de la República. Este derecho puede ser conceptualizado como la facultad que corresponde a toda persona para ejercer un control sobre los datos e informaciones personales que le conciernen y que reposan en registros públicos o privados, pudiendo exigir su rectificación, suspensión, actualización y confidencialidad en los casos que corresponda conforme al a normativa jurídica. (...) Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal (Sentencia No. 00300-2010-PHD/TC, del 111 de mayo de dos mil diez del Tribunal Constitucional de Perú)*[15] , el cual en lo relativo al derecho a la protección de datos personales, "*se apoya en los derechos fundamentales a la dignidad humana y a la privacidad. Se reconoce al ciudadano su derecho a estar informado para consentir expresamente la entrega y uso de sus datos personales.*"[16]

Viendo el estado de las cosas, **¿podemos concluir que legislación de aproximadamente 20 y 10 años de antigüedad, sirven para responder a la realidad de las interacciones digitales hoy día?** Sobre la base de que cada día estas interacciones son más sofisticadas, y dan lugar a negocios e industrias nuevas, así como también nuevas ventanas para fraudes y delitos en operaciones financieras, y así un sin número de vulnerabilidades para la sociedad, entendemos que no.

Otros dentro de la doctrina local opinan igual, aunque por razones diferentes. En efecto, LIZ FERNÁNDEZ considera que la Ley No. 172-13 "*no ofrece una protección integral de los datos personales de los ciudadanos, ya que se enfoca especialmente en el tratamiento de datos personales por parte de las Sociedades de Información Crediticia. La protección de datos personales implica que se establezcan reglas aplicables al tratamiento de datos realizado por cualquier entidad pública o privada con estándares adecuados de protección y con un catálogo robusto de derechos para los usuarios. En el país no existe ninguna normativa que regule el tratamiento de datos personales de manera integral para todas las actividades públicas y privadas. Tampoco existe una autoridad administrativa de supervisión en materia de protección de datos personales con facultad normativa y a la cual se le reconozca poder sancionador", bajo ese tenor, abunda que "la evolución legislativa internacional, especialmente influenciada por la entrada en vigor* ***del Reglamento General sobre Protección de Datos Personales de la Unión Europea ("GDPR", por sus siglas en inglés) en el año 2018****, genera un conjunto de obligaciones para las entidades que realicen el tratamiento de datos personales y confiere elevados estándares de protección a los usuarios. Una de las particularidades de esta norma es que, bajo ciertas condiciones, su ámbito de aplicación puede extenderse fuera de la Unión Europea*" (Fernández, 2023) (énfasis nuestro).

[16] TC/0042/12 del 21 de septiembre de 2012.

Existen actualmente varios proyectos de ley que reposan en el Congreso Nacional (Proyecto de Ley sobre gestión de la ciberseguridad; Proyecto de Ley General de la Tecnología de la Información y Telecomunicaciones y Proyecto de ley que crea el Sistema Nacional de Inteligencia). A pesar que estas iniciativas tienen distintos enfoques y ramas, todas están ligadas al uso y protección de datos. Sin embargo, ninguna de ellas busca necesariamente actualizar o fortalecer las legislaciones existentes, que a nuestro entender hoy en día resultan insuficientes.

En tal virtud, **estamos en un momento ideal para utilizar las mejores prácticas internacionales así como la experiencia comparada que nos presenta un paradigma global que busca alimentar legislaciones de distintas jurisdicciones con un efecto jurídico de polinización cruzada en materia de protección de datos personales** como el que busca provocar el Reglamento General sobre Protección de Datos Personales de la Unión Europea, y a partir de este actualizar toda nuestra carpeta de legislación en la materia. **Ahora bien, dicha experiencia debe ser necesariamente filtrada, diluida y adaptada a la realidad nacional, que igualmente tiene circunstancias particulares**, de manera que no suceda lo que en otras jurisdicciones ha pasado donde se habla de "trasplantes jurídicos", o lo que sectores de la doctrina local han denominado como una "indigestión legal".

REFERENCIAS

LIZ FERNÁNDEZ, Annabelle. "¿Debemos reformar la Ley Núm. 172-13 de Protección de Datos Personales en la República Dominicana?" Accesible en https://www.iomg.edu.do/post/debemos-reformar-la-ley-n%C3%BAm-172-13-de-protecci%C3%B3n-de-datos-personales-en-la-rep%C3%BAblica-dominicana

Sentencia del Tribunal Constitucional de la República Dominicana No. TC/0044/17 del 31 de enero de 2017.

Sentencia del Tribunal Constitucional de la República Dominicana No. TC/0042/12 del 21 de septiembre de 2012.

SIGÜENZA & CARRASCOSA

ANÁLISIS LEGAL Y DERECHO COMPARADO