

Comercio electrónico y el underground: Elementos para la gestión comercial de Costa Rica en la sociedad de la información

Luis Diego Salas Ocampo

Académico – investigador
Escuela de Relaciones Internacionales
Programa Innovación metodológica, participación estudiantil y gestión del conocimiento
Universidad Nacional de Costa Rica
luis.salas.ocampo@una.cr

Marly Yisette Alfaro Salas

Escuela de Informática
Subdirectora Programa de Gestión Financiera
Universidad Nacional de Costa Rica
marly.alfaro.salas@una.cr

RESUMEN

En este artículo da un panorama de las acciones globales desarrolladas para la evidenciación de las dinámicas de comercio electrónico y su gestión para la facilitación del comercio. Compara las acciones formales con la existencia de espacios de intercambio económico en la Deep y Dark Web. Evidencia que, a pesar de los avances en los cuadros normativos y operativos a nivel de la Organización Mundial de Comercio, existen prácticas como el Proteccionismo 4.0 que inciden en la generación de proteccionismo estatal.

Se constata que, para el caso de Costa Rica, pese a la existencia de una estrategia de Ciberseguridad, son muchos los nudos problemáticos para la gestión y vigilancia de la Deep y Dark Web a nivel de gestión país.

Se recomienda el desarrollo de una investigación en el campo que trascienda la línea académica que usualmente se tiende a privilegiar. Esto significa abrir nuevos espacios

de encuentro, donde sociedad civil organizada y no organizada puedan evidenciar los hallazgos que ocurren en esferas tan difusas y complejas para el desarrollo de comercio como lo es la Deep web.

PALABRAS CLAVE

Comercio electrónico – Proteccionismo – Ciberseguridad – Deep web – Organización Mundial del Comercio

SUMMARY

This article gives an overview of the global actions developed for the evidence of the dynamics of electronic commerce and its management for trade facilitation. Compare formal actions with the existence of economic exchange spaces in the Deep and Dark Web. Evidence that, despite the advances in the normative and operational tables at the World Trade Organization level, there are practices such as Protectionism 4.0 that affect the generation of state protectionism.

It is noted that, in the case of Costa Rica, despite the existence of a Cybersecurity strategy, there are many problematic nodes for the management and surveillance of the Deep and Dark Web at the country management level.

It is recommended to develop research in the field that transcends the academic line that usually tends to be privileged. This means opening new meeting spaces, where organized and unorganized civil society can demonstrate the findings that occur in areas as diffuse and complex for the development of commerce as is the Deep web.

KEYWORDS

Electronic commerce - Protectionism - Cybersecurity - Deep web - World Trade Organization

INTRODUCCIÓN

Desde 1998 la Organización Mundial de Comercio (OMC) estableció su declaración sobre comercio electrónico. Eso era esperable, tanto por la abundancia de oportunidades y posibilidades que se daban como consecuencia de la utilización frecuente de esta manera de hacer negocios. Según esta organización, los servicios representan el 60% de la producción y el empleo mundial, pero apenas el 20% del comercio total (OMC, 1998a). Según la OMC (2019) se entiende el comercio electrónico como la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos, incluido el desarrollo de arquitectura para la ejecución de estas actividades.

El marco normativo sobre el cual se rige este tipo de actividad es el Acuerdo General sobre Comercio y Servicios. Este se pone en vigor en 1995, como consecuencia de la Ronda de Uruguay, con el fin de extender el comercio multilateral al sector servicios, en similitud al GATT. De hecho, es tan importante el comercio electrónico, que se ha establecido una relación entre este con los cuatro modelos de suministro de servicios que este acuerdo regula:

- Servicios Transfronterizos (del territorio de un Miembro al territorio de cualquier otro Miembro)
- Consumo en el extranjero (en el territorio de un Miembro a un consumidor de servicios de cualquier otro Miembro)
- Presencia Comercial (por un proveedor de servicios de un Miembro mediante la presencia comercial en el territorio de cualquier otro Miembro)

- Presencia de personas físicas (por un proveedor de servicios de un Miembro mediante la presencia de personas físicas de un Miembro en el territorio de cualquier otro Miembro)

Estos cuatro modelos, se definen a partir de dos variables clave. La primera de ellas, la presencia territorial del proveedor y del consumidor del servicio. Este acuerdo no hace diferenciación en relación con el medio tecnológico de facilitación de los servicios.

De hecho, esto fue todo un proceso de discusión a lo interno de la Comisión del Consejo de Servicios de la OMC, sin embargo, dentro de sus consideraciones decidieron incluir además del servicio transfronterizo, los otros bajo el argumento, de que cualquiera de ellos, puede intervenir esta modalidad de comercio.

Solamente han quedado excluidos los referidos a los servicios suministrados en ejercicio de facultades gubernamentales, no suministrados en condiciones comerciales ni en competencia con uno o varios proveedores de servicios, y la mayor parte de los servicios de transporte aéreo.

En otras palabras, queda claro que, en todo proceso de prestación de servicios mediante comercio electrónico, los principios legales del Acuerdo General de Comercio de Servicios de la OMC serán vigentes, tanto a nivel de la prestación del mismo directamente, así como todos aquellos aspectos indirectos que lo regulan.

Un elemento que es especialmente interesante para comprender el alcance del comercio electrónico en los países tiene que ver con la relación existente entre el modelo o tipo de servicio y los compromisos nacionales de los estados miembros de la OMC.

Un compromiso nacional se entiende como la obligación de conceder el acceso a los mercados y el trato nacional a la actividad de servicios de que se trata con sujeción a los términos y las condiciones que se especifican en dicha Lista de compromisos. Al contraerlo, por tanto, el gobierno consolida el nivel especificado del acceso a los

mercados y el trato nacional y se compromete a no imponer ninguna medida nueva que restrinja el ingreso en el mercado o la prestación del servicio.

Los compromisos específicos tienen por ende un efecto similar al de una consolidación arancelaria: dan a los agentes económicos de otros países la garantía de que no se modificarán en detrimento de ellos las condiciones de entrada y operatividad en el mercado. Esos sólo podrán retirarse o modificarse previo acuerdo sobre los ajustes compensatorios pertinentes con los países afectados, y no cabrá retirada ni modificación alguna hasta tres años después de la entrada en vigor del Acuerdo. Se podrá sin embargo añadir o mejorar compromisos en cualquier momento. En el caso de Costa Rica, se presentan listas del año 1998 con respecto al sector financiero (OMC, 1998b).

En el caso de las exenciones; estas son entendidas como la autorización concedida por los Miembros de la OMC a un Miembro para que éste deje de cumplir los compromisos normales. Las exenciones tienen plazos, y su prórroga debe justificarse. En el caso de nuestro país en materia de servicios se tiene que; servicios a las empresas, publicidad, transporte y carga se establecen dentro de ellas. Estas tienen una duración definida y luego son estudiadas por los estados parte (OMC,1994).

También con relación a la transparencia, los miembros de la organización están obligados a publicar todas las medidas pertinentes de aplicación general que se refieran al Acuerdo General de Comercio de Servicios que afecten a su funcionamiento. Entre esas medidas estarían incluidas las que afectarían al suministro electrónico de servicios, y asimismo las adoptadas por instituciones no gubernamentales en el ejercicio de facultades delegadas.

Es claro entonces que como consecuencia de este tipo de movimientos que en el mundo vienen desde 1998, los escenarios de negociación internacional han tenido variaciones importantes. De igual manera, los escenarios de gestión de lo electrónico en los márgenes de maniobra de los estados.

Un aspecto que contribuirá de manera fundamental a estas acciones que se presentan en el marco del comercio internacional de servicios, particularmente el comercio electrónico, será la evolución del propio internet. Ya en 1998 internet contaba con un millón de usuarios, además se crea Google.

Mucha agua ha corrido desde la creación del internet y de la comercialización del mismo, hasta llegar a las tendencias de uso que se tienen hoy. Según la Universidad de Salamanca, citando el estudio de Hootsuite, sobre tendencias de lo digital para 2019:

- Actualmente hay 5,11 mil millones de usuarios móviles únicos en el mundo, 100 millones más (2 por ciento) en el último año.
- Hay 4,39 billones de usuarios de internet en 2019, un aumento de 366 millones (9 por ciento) en comparación con enero de 2018.
- Hay 3.48 mil millones de usuarios de redes sociales en 2019, con un total mundial de 288 millones (9 por ciento) desde el año pasado.
- En enero de 2019, 3.26 mil millones de personas utilizan las redes sociales en dispositivos móviles, con un crecimiento de 297 millones de usuarios nuevos, lo que representa un aumento anual de más del 10 por ciento.

Fuente: <https://universoabierto.org/2019/02/04/como-utiliza-la-gente-internet-los-dispositivos-moviles-los-medios-sociales/> consultado el 25 de marzo de 2019

En síntesis, es posible indicar que ante este crecimiento vertiginoso de usuarios y de formas para la gestión y regulación del comercio electrónico, es esperable, la necesidad de desarrollar mecanismos de promoción, posicionamiento y protección de las transacciones en el mundo bajo el modo de servicios.

También resulta claro que el escenario internacional ha sido transformado, no solamente por la aparición de distintas herramientas para la diversificación de las prácticas comerciales, sino porque actores de distintos referentes y que respondieron a

mecanismos diversos luego de la ruptura de la bipolaridad mundial, emergieron dando como consecuencia, un nuevo mercado de bienes y servicios que se mueve no en lo evidente, sino en lo profundo y cuyo espacio mediatizado, se ha convertido en la Deep web.

En este artículo se estarán considerando al menos dos movimientos. En primer lugar, las acciones que se han dado de cara a la evidenciación de las dinámicas de comercio electrónico en los espacios globales de gestión y facilitación del comercio. En segundo lugar, se considerarán algunos elementos específicos de otros espacios que si bien, no son evidenciados desde los espacios institucionales, si juegan un papel medular en los procesos de comercio global hoy mediante tecnología.

Los nuevos escenarios a nivel de negociación internacional producto del comercio electrónico

El nombre del juego es tecnologías de información y comunicación. Otros le han decidido poner Sociedad de la información. Desde 2003 y luego en 2005 con la Cumbre Mundial de la Sociedad de la información (Betancurt, 2004), se vio el potencial de las TICs tanto para colaborar con los Objetivos del desarrollo del Milenio y posteriormente con su sucesor como lo fue la Agenda 2030 sobre Desarrollo Sostenible y la firma en 2016 sobre el acuerdo de París sobre cambio climático.

El supuesto básico, es que existe como consecuencia de una disminución de las brechas digitales entre países desarrollados y no desarrollados, una posibilidad de incrementar el comercio. Para ello, un elemento sumamente importante tiene que ver con la necesidad de instrumentalización de los estados para garantizar un control o al menos un acercamiento a este fenómeno.

Ya desde 2016, A partir de la cumbre del G7, los eventos ministeriales de la OCDE y del G20, y hasta la Reunión Ministerial de la cumbre del G20 de 2017, la transformación digital ahora está firmemente arraigada en la agenda global (OCDE, 2017).

Existe un amplio reconocimiento al más alto nivel gubernamental en muchos países y entre los líderes mundiales de que la digitalización está transformando nuestras vidas. Además, se presenta una urgencia de llevar a cabo la transformación digital para lograr una prosperidad más inclusiva y sostenible. En general, los ministros coincidieron en que para desbloquear los beneficios de la transformación digital en curso es necesario abordar los desafíos creados por esta transformación, en particular para los empleos, las habilidades y la confianza.

También destacaron la urgencia de que los gobiernos sean proactivos y adopten un enfoque de formulación de políticas mediante el cual se invite a todas las partes interesadas a desarrollar e implementar un camino claro para dar forma a la transformación digital, con base en un enfoque de política plenamente integrado. Desde la declaración de Cancún de 2016 sobre economía digital, se indicaron algunos elementos medulares:

La apertura de Internet impulsa el desarrollo social, económico y cultural.

- Estimular la innovación digital en toda la economía es esencial.
- Existen muchas oportunidades para mejorar las redes y los servicios mediante la convergencia de diferentes tecnologías de comunicación.
- Es fundamental garantizar que tengamos los marcos adecuados para habilitar el Internet de las Cosas del mañana.
- La confianza del consumidor es un elemento clave para impulsar el crecimiento de la economía digital.

- Gestionar la seguridad digital y el riesgo de la privacidad es necesario para la prosperidad económica y social.
- Todas las partes interesadas tienen una función que desempeñar para facilitar nuevos mercados y nuevos empleos en la era digital.

En 2017 en Ginebra la UNCTAD (Conferencia de Naciones Unidas sobre comercio y desarrollo) estableció la necesidad de conformar un grupo de expertos para la medición de este fenómeno en el marco de la economía digital.

Esto por cuando había identificado entre otras cosas, las ventas globales por internet de bienes y servicios alcanzaron US\$ 25,7 billones en el año 2016. De ese valor, el 90% fueron transacciones entre empresas (*business-to-business*, o B2B). Como consecuencia, las disposiciones sobre comercio electrónico y digital crecieron sustancialmente en el ámbito de los acuerdos regionales de comercio, con el objetivo de remover y evitar barreras al libre flujo de datos y contener el surgimiento del llamado "proteccionismo digital" (o sea, los intereses nacionales asociados a esta agenda), que se encuentra motivado por demandas específicas de las empresas que dominan la arena digital en sus países y globalmente.

Pese a los distintos esfuerzos para que estos modelos de comercio internacional pudiesen estar por encima de viejas prácticas, lo cierto del caso, es que ni han podido desaparecer prácticas que obstaculizan el comercio y más bien, se han "virtualizado", en el sentido de que estas restricciones han ganado nuevos espacios en la gestión de lo tecnológico.

El proteccionismo digital como manifestación de lo expuesto permite darse una idea del tamaño de las consecuencias de la tecnificación de estos mecanismos de gestión comercial:

Ilustración 1

Flujos de comercio, capital y datos en el mundo entre período comprendido entre 1980 y 2014

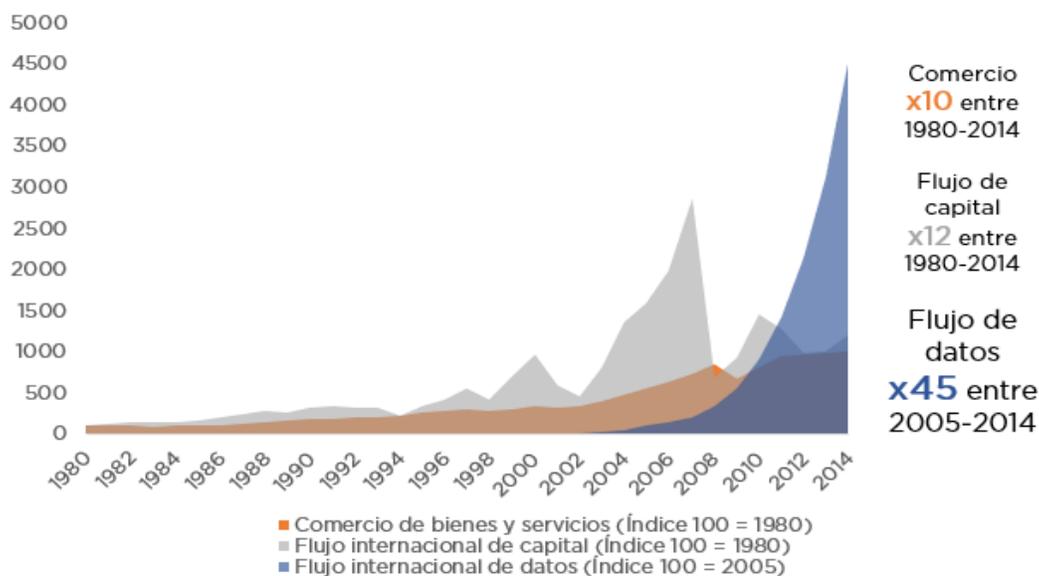


Ilustración 1 Fuente: INTAL-BID con base en UNCTAD, Mckinsey (2016) y James et al. (2014) * Nota: Flujo de comercio es el valor del comercio global de bienes y servicios; flujo de capital es el valor global de la salida bruta de capital (incluye IED, inversión de port

Como hace evidente la ilustración el flujo de datos tiene un comportamiento de crecimiento impresionante, mucho más grande que el de comercio y el de capital. Ahora bien, se genera como consecuencia también mecanismos de protección y restricción por parte de los estados a este flujo de datos, tal y como lo evidencia la siguiente ilustración:

Ilustración 2

Evolución de las restricciones a los flujos de datos en el mundo por región durante el período 1960-2017

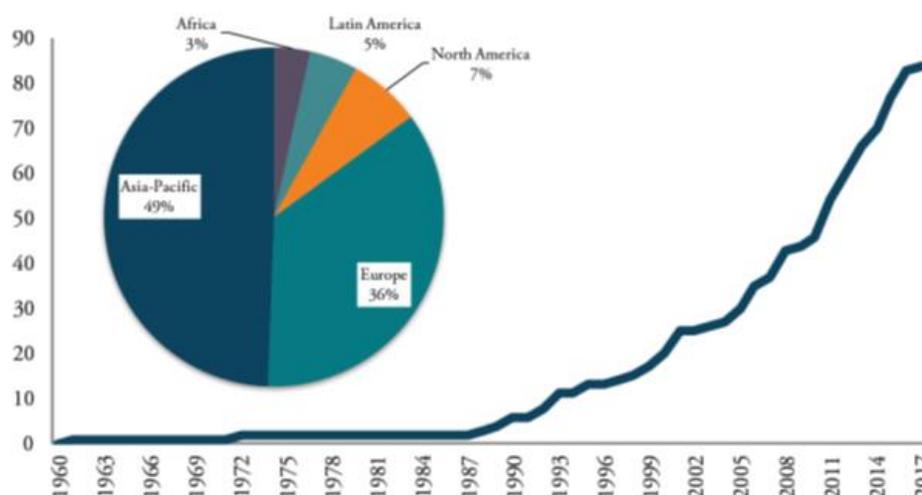


Ilustración 2 Banco Interamericano de Desarrollo.

<http://conexionintal.iadb.org/2018/05/30/ideas-1/> consultado el 28 de marzo de 2019

Son varias las medidas que los países han implementado para la restricción del flujo de datos. Usualmente estas van desde la obligatoriedad de que servidores se encuentran en el espacio geográfico de un país (Rusia), hasta el almacenamiento de los datos de proveedores de agencias gubernamentales en el entorno de los países (Alemania) (Slaughter and May, 2017).

Un argumento de fondo que suele darse tiene que ver con la necesidad de proteger a los competidores nacionales de sus competidores internacionales. Como consecuencia de esto, se dan restricciones de acceso a los sitios web de compañías competidoras internacionales, el pedir requisitos para la operación en los países que son disuasivos de iniciar operaciones de tipo tecnológico en el país o bien el desarrollo de discursos y reglamentos que tengan como base la seguridad nacional., De hecho en casos extremos se indica la necesidad de que para acceso a ciertos mercados las compañías deban revelar el código de sus soluciones en software por ejemplo. Diversas economías en desarrollo como China, Indonesia, Bulgaria, Irán, Polonia, Rumania, Corea del Sur y Vietnam implementaron medidas de este tipo para proteger industrias digitales nacientes e impulsar el desarrollo tecnológico asociado a la economía digital (Cory, 2017).

En América Latina, países como Argentina, Perú, Brasil, Colombia han generado un conjunto de medidas que van desde la protección de los datos personales y restricciones en la transferencia de los mismos, hasta requisitos de localización de servidores (Ferracane, 2017).

Es particularmente interesante el comportamiento que han tenido varios países asiáticos a las iniciativas de la OMC para la reducción de bloqueos de páginas tales como Google, Facebook y Amazon y otras restricciones comerciales. Esto se ha evidenciado en la negativa de China, India, Indonesia y Vietnam a la participación de este tipo de acuerdos.

Resulta claro que la economía global ha cambiado y que las prácticas más concretas en el marco de ello también. El Banco Mundial ha utilizado el concepto Globalización 4.0 para dar cuenta del fenómeno (Mckinsey, 2016).

Entre los principales cambios que se logran apreciar existe un giro importante en lo que tiene que ver con los flujos que alimentan los procesos de globalización. Mientras que clásicamente el capital y el trabajo en el inicio de estos procesos habían sido los insumos más importantes, al iniciar la globalización 4.0 esto se transforma en un movimiento superior de flujos de conocimiento. Esto implica que la infraestructura digital como elemento medular del proceso logístico adquiere una mayor relevancia. La consecuencia directa de ello, es un cambio importante en la difusión de las ideas y el acceso a los contenidos. Por un lado, las ideas adquieren una dimensión global al igual que sus usos. Por otro lado, los contenidos gratuitos y también pagados aumentan en calidad y también existe un crecimiento exponencial de los contenidos basura, elemento que implica un importante costo en términos de gestionar los datos con los cuales se toman decisiones.

Resulta claro que esta forma de hacer negocios y comercio internacional, no es el futuro, ya es el presente y en este sentido, es fundamental poder leer a Costa Rica en el marco de esta Sociedad de la Información.

Es por ello, que resulta medular leer el país desde sus avances en materia de normativa al menos en lo referido a comercio electrónico.

Costa Rica en la Sociedad de la Información desde el Comercio Electrónico

Este país ha venido generando un conjunto de movimientos bilaterales mediante la figura de tratados donde el tema de comercio electrónico y particularmente lo vinculado a tecnologías de información ha tomado forma en seis tipos particulares de medidas:

1. Normas sobre el libre comercio de los productos digitales (capítulos de comercio electrónico).
2. Normas de propiedad intelectual para la protección de los derechos de autor de los desarrolladores de programas de software y productos digitales.
3. Normas relativas a servicios vinculados a las TIC.
4. Normas sobre inversión, que aplican tanto para las inversiones de productos físicos (hardware) como para las áreas vinculadas al software y otros productos digitales.
5. Normas sobre compras públicas vinculadas a las TIC
6. Normas que estimulan el uso de las TIC para facilitar el comercio.

Fuente: Gil Calderón, M. (2012). Primer Congreso Nacional de Información para el Desarrollo: “Costa Rica hacia la sociedad de la información de todos para todos”: Informe final mesas de trabajo. *E-Ciencias de la Información*, 2(2).

La ilustración permite visualizar dentro de los TLC suscritos con Costa Rica, los niveles de acercamiento del tema de TICs dentro de su conformación

Tabla 1

Capítulos de los Tratados de Libre Comercio de Costa Rica donde se ubican normas que inciden en las TICs

que inciden en las TIC						
TLC	Comercio Electrónico	Propiedad Intelectual	Servicios	Inversiones	Compras Públicas	Facilitación de Comercio
México	--	X	X	X	X	X
Chile	--	--	X	X	X	X
R. Dominicana	--	X	X	X	X	X
Canadá	(1)	--	X	X	--	X
CARICOM	--	--	X	X	X	--
Panamá	--	X	X	X	X	X
Estados Unidos	X	X	X	X	X	X
China	--	X	X	X	--	X
Singapur	X	X	X	X	X	X

1. No hay un capítulo específico en el TLC. Suscribieron una Declaración Conjunta.

2. El programa de desgravación arancelaria inició el 1 de marzo de 2006 para todos los países, aunque no lo hubieran puesto en vigor según lo estipulado en el Anexo 3.3: inciso 4 del TLC.

Fuente: Elaboración propia con datos del Ministerio de Comercio Exterior de Costa Rica. PROSIC, Febrero 2011.

Ilustración 3Fuente: Gil Calderón, M. (2012). Primer Congreso Nacional de Información para el Desarrollo: “Costa Rica hacia la sociedad de la información de todos para todos”: Informe final mesas de trabajo. E-Ciencias de la Información, 2(2).

Como puede visualizarse resultan constantes los elementos relacionados con otros elementos de comercio y no necesariamente los referidos a comercio electrónico. Ahora bien, esto cobra un especial interés cuando se visualiza claramente que existen condiciones de acceso a internet importantes en este país.

Ilustración 3

Uso del Internet en América Latina según Ecommerce Foundation para el período 2015-2017

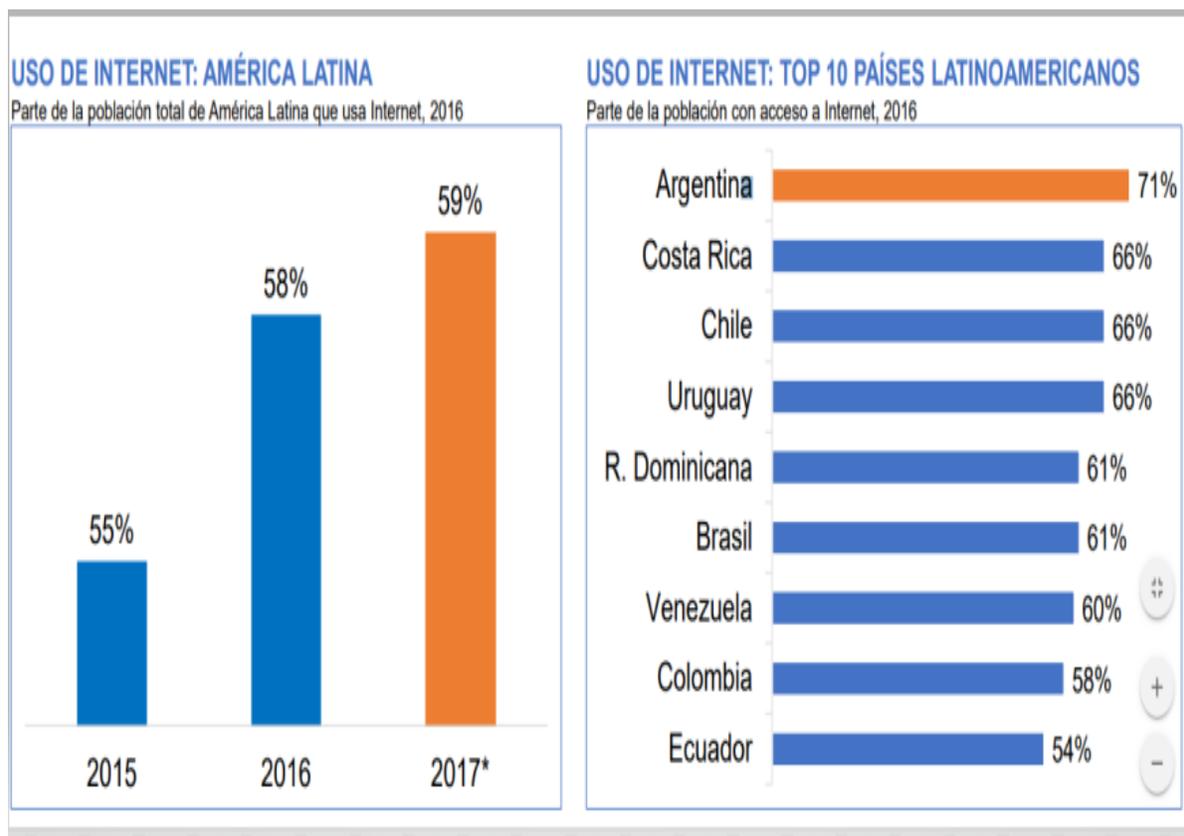


Ilustración 4 Fuente: Ecommerce Foundation. Informe sobre comercio electrónico en América Latina para el año 2018. ecommercefoundation.org/reports. Consultado 28 de marzo de 2019

Pese a tener la infraestructura y la arquitectura idónea, Costa Rica aún tiene un conjunto de aspectos culturales relacionados a los tipos de uso del internet y en particular al tema

de la confianza en las transacciones que hacen que pese a contar con los dispositivos tecnológicos idóneos, su nivel de participación de comercio electrónico en cuanto a compras, sea discreto.

Ilustración 4

Comportamiento de compra mediante comercio electrónico de los países de América Latina

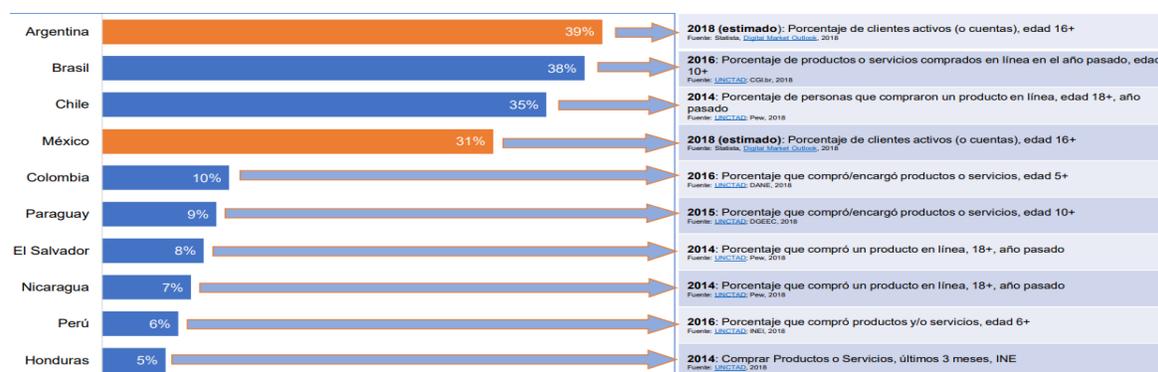


Ilustración 5 Fuente: UNCTAD, 2018

Lo más interesante del asunto es que si tiene un movimiento importante en este momento en el país que ha venido generando un conjunto de legislación relacionada en la materia y que apunta fundamentalmente a poder aumentar los niveles de confianza del consumidor con respecto a la modalidad.

Algunas de las más importantes son:

- Estrategia de Ciberseguridad de Costa Rica Ministerio de Ciencia y Tecnología 2017
- Reforma a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor (Capítulo de Promoción al Consumidor en el contexto del comercio electrónico)

- Se trabajan tres ámbitos medulares Publicidad que genera una lista de información obligatoria que debe brindarse en la página o sitio web sobre la empresa o persona que ofrecen los productos de forma electrónica, así como sobre la transacción que se realiza. Por otro lado, debe dejar claro su estrategia de funcionamiento en cuando a promociones y desarrollar un elemento de reclamaciones dentro de su página web.
- Se regulan las ventas en línea: En caso de no indicar el plazo de entrega del producto o servicio, se asumirá que el mismo debe ser entregado dentro de las 24 horas siguientes posteriores a la compra. Además, la forma en la cual los consumidores aceptan un contrato electrónico debe ser expresa e informada.
- En este sentido, no es posible tener casillas preseleccionadas o que la decisión de compra se realice sin haber tenido acceso a toda la información necesaria y obligatoria para la compra. Además, una vez realizada la venta, es obligatorio enviarle al consumidor un comprobante de la transacción realizada.
- Manejo de información: Para el envío de comunicaciones electrónicas de parte del comercio a sus clientes se debe tener el consentimiento previo de los consumidores. La información debe tratarse de forma confidencial y en total apego de lo estipulado en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales y la Ley General de Telecomunicaciones; debe contar con medios seguros (e informarlos a los consumidores) para realizar la transacción y los pagos que involucre, así como con una entidad certificadora del manejo de la información.
- Ley de certificados, firmas digitales y documentos electrónicos
- Ley de Protección de la persona frente a sus datos

Es posible que muchos actores, se encuentran esperando el despegue de las dinámicas de comercio electrónico y el tema de la seguridad financiera y jurídica para ello resulta

fundamental. El tema de fondo, entonces tiene que ver con la pregunta ¿Deberían temer los consumidores de realizar transacciones por este medio?

El underground

Hasta ahora se ha mencionado el comportamiento del comercio electrónico frente a las estructuras globales en el marco de los servicios y además de la manera en la que se evidencian en la firma de acuerdos bilaterales de comercio de Costa Rica con otras naciones. Igualmente se ha visto cómo se presentan una serie de instrumentos jurídicos que tratan de promover confianza y en esta medida aumentar las transacciones.

No obstante, existe otro mundo de la tecnología el mundo de la Deep Web y el de la Dark Web. En estos igualmente ocurren transacciones de servicios. Es donde los motores de búsqueda no indexan la información de internet. Sólo determinados usuarios, aquellos con contraseñas o códigos especiales, pueden hacerlo. En otras palabras, particularmente la Deep Web no es ni ilegal ni peligrosa, es simplemente de acceso restringido. Esto significa que para poder acceder a ella son otros los navegadores que se utilizan. Sin embargo, ni son de uso común y mucho menos se presentan habitualmente las condiciones para que la gente se capacite en el manejo de ellas. Algunos de estos son Tor, Anonimus Netword, i2p, freenet.

Estos tienen un elemento fundamental que es que avanzan mucho más rápido en la generación de condiciones de inter operatividad. Se entiende esta como la habilidad de organizaciones y sistemas dispares y diversos para interactuar con objetivos consensuados y comunes y con la finalidad de obtener beneficios mutuos. La interacción implica que las organizaciones involucradas compartan información y conocimiento a través de sus procesos de negocio, mediante el intercambio de datos entre sus respectivos sistemas de tecnología de la información y las comunicaciones.

En palabras mucho más sencillas, esto significa que la velocidad de procesamiento de la información y la limpieza de la misma de datos identificadores son de suma utilidad para la realización de transacciones. Esto genera evidentemente condiciones desigualdad para el movimiento de la información y los datos a lo largo del mundo, es más a lo largo de la red.

En el caso de la Deep web esta se configura por niveles que tienen un conjunto de diferencias medulares en lo referido al conjunto de prácticas y el tipo de información que se puede acceder. Aunque existen algunas diferencias entre la cantidad de niveles, usualmente las tendencias apuntan a la existencia de cinco o seis de ellos.

Tabla 2

Estructura de la Deep web

Nivel	Características
1	Páginas comunes de acceso público
2	Resultados de búsqueda que han sido suprimidos que no pueden ser accedidos mediante navegadores comunes
3	Utilización de información de otros sin consentimiento mediante la utilización de softwares hospedados en nubes
4	Sitios donde se maneja el comercio y el tráfico humano y explotación sexual comercial
5	Tráfico de órganos, niños y esclavitud

6

Venta de armas, drogas y asesinatos por encargo

Ilustración 6 Fuente: Elaboración propia con base en <https://www.deepdotweb.com/> y <https://www.pandasecurity.com/spain/mediacenter/seguridad/tor-y-deepweb-todos-los-secretos/> consultados el 14 de agosto de 2019.

Uno de los problemas técnicos más importantes que solían existir en estos niveles era el medio de pago para el ejercicio de estas transacciones, pero esto ha sido solventado con el desarrollo de las criptomonedas.

De hecho, en el año 2017 indica que estas no pueden ser consideradas como medio de pago ya que rigen los principios de La Ley Orgánica del Banco Central, en sus artículos del 42 al 51, establece el colón como la unidad monetaria de la República de Costa Rica. Asimismo, la Ley designa al Banco Central como único emisor de los billetes y monedas en circulación y establece el poder liberatorio ilimitado del colón para liquidar toda clase de obligaciones pecuniarias, tanto públicas como privadas (Banco Central de Costa Rica, 2017)

Por lo anterior, el bitcoin y otras criptomonedas similares no cuentan con el respaldo del Banco Central de Costa Rica. De igual manera, al no ser emitidas por un banco central extranjero no pueden ser consideradas como moneda o divisa extranjera bajo el régimen cambiario, razón por la cual no están cubiertas por la seguridad que ofrece la intermediación cambiaria ni la libre convertibilidad de la moneda, consagradas en los artículos 48 y 49 de la Ley Orgánica del Banco Central.

Resulta relativamente claro que no es infundada o producto de la casualidad la desconfianza natural que puede tener el costarricense con respecto al comercio electrónico. De hecho, el Ministerio de Ciencia y Tecnología ha sacado recientemente una campaña para responder al ciber crimen desde la perspectiva de las operaciones en línea.

Esta responde a la Estrategia Nacional de Ciber seguridad (Ministerio de Ciencia y Tecnología, 2017).

Llaman la atención en esta estrategia un conjunto de elementos importantes de evidenciar. La primera es que indica que el documento fue construido por distintos sectores que participaron en las mesas de consulta organizadas durante el 2015, sin embargo, no se evidencia la naturaleza de los mismos. El segundo aspecto interesante es que pese a que como reconoce la estrategia desde 2012 existe el Centro de Respuestas a Incidentes de Seguridad Informática, generado por el Este centro fue constituido mediante el Decreto Ejecutivo Nº 37052-MICIT del 09 de marzo de 2012, en este documento de estrategia no se visualizan datos de ningún tipo sobre delincuencia informática y líneas de actuación de los mismos ni tampoco nada relacionado con fondos desarrollados para el trabajo gubernamental a nivel de respuesta organizada de la Deep y la Dark Web.

Como tercer elemento importante llama la atención que esta estrategia genera un comité consultivo que de soporte técnico y además de gestión a la misma, sin embargo, en la conformación existen dos ausentes en extremo importantes. En primer lugar, no esta representado el Colegio de Profesionales en Informática, lo cual es un error importante. El otro gran ausente es la Comunidad de Software Libre de Costa Rica. Ambos quizá tienen un conocimiento importante relacionado con lo que podría ser la Deep y la Dark Web.

Finalmente, la estrategia carece de estadísticas policiales que indiquen a la comunidad nacional, sobre la importancia de las incidencias de crimen informático en los campos de delitos cibernéticos en general (datos personales, fraude electrónico, phishing, pharming, interrupción de comunicaciones), elementos relacionados con el Código de la Niñez y la Adolescencia (Pornografía infantil, captación de personas menores de edad con fines de explotación mediante pseudo pornografía, pornografía virtual, posesión de material pornográfico, etc.) entre otras áreas.

No obstante, el propio Organismo de Investigación Judicial del país ha venido reconociendo desde 2015 la importancia de este tipo de delitos y la dinámica comercial que se genera en torno a esta dimensión underground. Solamente por mencionar un caso, en ese año el entonces Director de ese organismo señaló la experiencia del empresario canadiense Ryan Craig Piercy Bate, que había sido secuestrado. En este momento, su liberación tuvo un costo de \$500 mil (€250 millones aproximadamente) y los pagos se hicieron con transacciones en bitcoins en la Deep Web, que posteriormente, según investigaciones, llegaron hasta países europeos como Rumania (Diario Extra, 2017).

En otras palabras, existen las condiciones y particularmente las plataformas para que un conjunto importante de volumen de comercio electrónico potencialmente ilegal se desarrolle a nivel país y dentro de la estrategia país de Ciberseguridad esta relación no se haya completamente clara ni evidente.

Esto llama la atención porque basta con solamente realizar el ejercicio técnico de visualización de las posibilidades para el intercambio económico mediante la Deep web, para saber el amplio tamaño del mercado y sus posibilidades reales de generación de dinero.

De acuerdo con Diario Bitcoin (2019) existen al menos las siguientes plataformas claramente detectadas:

1.- *Dream* que opera desde 2013 y tiene más de 63.000 productos digitales, 87.000 medicamentos y muchos otros listados de artículos lícitos e ilícitos. Se puede utilizar como medio de pago saldos Bitcoin (*BTC*) y Bitcoin Cash (*BCH*) como medio de pago. También cuenta con servicios de mensajería encriptada.

2.- *Wallstreet Market* Admite el uso de cuentas multifirma y el inicio de sesión *PGP*. Cuenta con un gran catálogo de artículos ilícitos (falsificaciones, joyas, malwares y armamento). Se puede pagar mediante saldos Bitcoin y Monero.

3.-*Point*: Es el tercer mercado clandestino más popular en la actualidad. El catálogo de productos se divide en drogas falsificaciones y medicamentos de difícil acceso. Se puede pagar con saldos Bitcoin, Bitcoin Cash y Ethereum (ETH), así como otras monedas menos populares. Comerciantes y compradores pueden establecer ubicaciones secretas de entrega.

4.-*Cannabis Growers & Merchants Co-op, CGMC* Cuenta con proveedores de Estados Unidos, Reino Unido; Europa y Canadá. Acepta pagos con saldos Bitcoin y Litecoin (LTC).

5.- *Berlusconi Market* Vende drogas, joyas, bienes digitales y muchos otros artículos ilegales. Acepta pagos Bitcoin, Litecoin y Monero. También vende muchas armas, en ocasiones de grueso calibre tales como AK-47, pistolas Glock 17 y 26, explosivos y equipos de destrucción masiva.

6.- *Cannazon* Vende gran variedad de productos de marihuana.

Es posible que la ausencia de desarrollo en la estrategia de Ciberseguridad costarricense tenga relación con la dificultad con contabilizar la dinámica de comercio electrónico que se mueve desde ahí, pero las tendencias internacionales apuntan a señalar lo visto de manera general por muchas fuentes que cada vez más y de forma vertiginosa, están popularizando el tema de la Deep y la dark web en los escenarios más conocidos de la internet.

A manera de conclusión

Queda claro que la normativa de comercio de servicios expresada en el Acuerdo General sobre Comercio y Servicios aplica al Comercio Electrónico. Esta normativa expresa una preocupación y acción de entes competentes y globales en materia de potenciar el comercio electrónico como medio para reducir las brechas entre economías. También se ha podido constatar que en la Sociedad de la Información se participa de forma desigual pese a los elementos normativos.

Otro de los aspectos que ha sido interesante determinar es que los países tienen una competencia entre ellos por el flujo de los datos donde se protegen por el cambio que introduce estos en los propios procesos de globalización. Resulta evidente que la información es el nuevo motor del capitalismo avanzado y si se controlan los datos se controla la estrategia. Esto introduce una paradoja que se comprende cuando se visualiza que los volúmenes de comercio electrónico son medulares para el crecimiento y el desarrollo, por tanto, las empresas tienen muchas posibilidades de incidencia en la agenda política. De ahí que la idea de que los gobiernos no intervienen en los flujos de comercio o al menos no deberían obstaculizarlo según la OMC, queda en este campo, en una perspectiva retórica.

Se ha podido evidenciar la existencia en la web una dimensión underground que genera tanto o más dinero que las operaciones lícitas.

Resulta sencillo visualizar que el comercio electrónico no es el futuro es el presente en el marco del comercio de servicios. En esta línea el comercio multilateral deberá seguir construyendo mecanismos para controlar el proteccionismo digital. El trabajo en Costa Rica para el desarrollo de confianza debe tocar el núcleo duro de las prácticas culturales y trabajar de forma profunda los elementos de Ciberseguridad, más allá de una estrategia que solamente vincula a ciertos sectores.

La ruta de Costa Rica en materia de comercio electrónico es realmente importante y permite establecer un conjunto de elementos para potenciar. En primer lugar, es fundamental la investigación estructurada en esta materia.

Esta investigación para que sea de utilidad tiene que trascender la línea academicista que usualmente se tiende a privilegiar. Esto significa abrir nuevos espacios de encuentro, donde sociedad civil organizada y no organizada puedan evidenciar los hallazgos que ocurren en esferas tan difusas y complejas para el desarrollo de comercio como lo es la Deep web.

A la par eventualmente podría desarrollarse un conjunto de acciones a la par del Ministerio de Ciencia y Tecnología y de otras instancias que permitan el desarrollo de un área de investigación de inteligencia de negocios y seguridad de transacciones sobre la base de las prácticas de consumo de sectores de población concretos.

Banco Central de Costa Rica (2017) Posición con respecto al uso de criptomonedas como medio de pago. Disponible en:

BIBLIOGRAFÍA

https://www.bccr.fi.cr/seccion-noticias/Noticia/Posicion_bccr_criptomonedas.aspx

Banco Interamericano de Desarrollo (2018). Proteccionismo 4.0: de la guerra comercial a la guerra por los datos. Disponible en: <http://conexionintal.iadb.org/2018/05/30/ideas-1/>

Betancourt, V (2004). La Cumbre Mundial sobre la Sociedad de la Información, Proceso y Temas debatidos. Asociación para el progreso de las telecomunicaciones. Disponible en:

https://www.apc.org/sites/default/files/wsis_process_ES.pdf

Calderón, M. (2012). Primer Congreso Nacional de Información para el Desarrollo: “Costa Rica hacia la sociedad de la información de todos para todos”: Informe final mesas de trabajo. E-Ciencias de la Información, 2(2).

Conferencia de Naciones Unidas sobre Comercio y Desarrollo. (2018). Grupo de Trabajo sobre la Medición del Comercio Electrónico y la Economía Digital. Ginebra, Suiza, 20/04/2018. Disponible en:

https://unctad.org/meetings/es/SessionalDocuments/tdb_ed2d3_es.pdf

Cory (2017). “Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?”. Information Technology & Innovation Foundation, Mayo 2017. Disponible en:

<https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>

Diario Bitcoin (2019). 6 mercados de la Dark Web que aceptan pagos con criptomonedas. Consultado 14 de agosto de 2019. Disponible en:

<https://www.diariobitcoin.com/index.php/2019/02/05/6-mercados-de-la-dark-web-que-aceptan-pagos-con-criptomonedas/>

Diario Extra (2017). Web profunda vulnera C.R. con raptos, drogas y armas OIJ e ICD luchan por atacar plataforma. San José, Costa Rica, agosto de 2017. Consultado el 14 de agosto de 2019. Disponible en:

diarioextra.com/Noticia/detalle/334836/web-profunda-vulnera-cr--con-raptos,-drogas-y-armas

Ecommerce Foundation (2018). Informe sobre comercio electrónico en América Latina para el año 2018. Disponible en:

ecommercefoundation.org/reports.

Ferracane (2017). "Restrictions on Cross-Border data flows: a taxonomy". European Centre for International Political Economy, Working Paper n. 1/2017. Disponible en:

<https://papers.ssrn.com/abstract=3089956>

James et al. (2014). "Cross-border capital flows since the global financial crisis". Reserve Bank of Australia, Bulletin, Junio de 2014. Disponible en:

<https://www.rba.gov.au/publications/bulletin/2014/jun/pdf/bu-0614-8.pdf>

Mckinsey (2016). "Digital globalization: The new era of global flows". Mckinsey Global Institute, marzo 2016. Disponible en:

<https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>

Ministerio de Ciencia y Tecnología de Costa Rica (2017) Estrategia Nacional de Ciberseguridad de Costa Rica. Ministerio de Ciencia y Tecnología, San José, Costa Rica. Consultado el 14 de agosto de 2019. Disponible en:

http://www.conicit.go.cr/biblioteca/publicaciones/publica_cyt/Estrategia-Nacional-Ciberseguridad-CR-19-10-17.pdf

OCDE (2017). Perspectivas de la OCDE sobre la Economía Digital 2017. Asociación Mexicana de Internet, México, Distrito Federal. Disponible en: <https://www.oecd.org/publications/perspectivas-de-la-ocde-sobre-la-economia-digital-2017-9789264302211-es.htm>

Organización Mundial del Comercio (1994). Lista de Exenciones del artículo II sobre el Acuerdo General de Comercio de Servicios, Costa Rica. 15/04/1994. Disponible en:

[https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=\(@Symbol=%20gats/el/*\)%20and%20\(\(%20@Title=%20costa%20rica%20\)%20or%20\(@CountryConcerned=%20costa%20rica\)\)&Language=SPANISH&Context=FomerScriptedSearch&languageUIChanged=true#](https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(@Symbol=%20gats/el/*)%20and%20((%20@Title=%20costa%20rica%20)%20or%20(@CountryConcerned=%20costa%20rica))&Language=SPANISH&Context=FomerScriptedSearch&languageUIChanged=true#)

Organización Mundial de Comercio. (1998). Declaración Mundial sobre comercio electrónico. 12/04/2019, de Organización Mundial de Comercio. Disponible en: [javascript:linkdoldoc\('WT/MIN98/DEC2.pdf', ''\)](javascript:linkdoldoc('WT/MIN98/DEC2.pdf', ''))

Organización Mundial del Comercio. (1998). Programa de Trabajo sobre Comercio Electrónico. 14/04/2019, de Consejo del Comercio de Servicios Sitio web: [javascript:linkdoldoc\('WT/L/274.pdf', ''\)](javascript:linkdoldoc('WT/L/274.pdf', ''))

Organización Mundial de Comercio (1998). Lista de Compromisos específicos en servicios para Costa Rica, suplemento 1. 24/02/1998. Disponible en: [https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=\(@Symbol=%20gats/sc/*\)%20and%20\(\(%20@Title=%20costa%20rica%20\)%20or%20\(@CountryConcerned=%20costa%20rica\)\)&Language=SPANISH&Context=FomerScriptedSearch&languageUIChanged=true#](https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(@Symbol=%20gats/sc/*)%20and%20((%20@Title=%20costa%20rica%20)%20or%20(@CountryConcerned=%20costa%20rica))&Language=SPANISH&Context=FomerScriptedSearch&languageUIChanged=true#)

Organización Mundial de Comercio (2019). Entender la OMC: Cuestiones transversales y cuestiones nuevas. Comercio Electrónico. 24/03/2019. Disponible en:

https://www.wto.org/spanish/thewto_s/whatis_s/tif_s/bey4_s.htm

Slaughter and May (2017). “Data protection – or protectionism by the back door?”.

Slaughter and May, Julio 2017. Disponible en:

<https://www.slaughterandmay.com/media/2536461/data-protection-or-protectionism-by-the-back-door.pdf>

Universidad de Salamanca (2019). Blog Universo Abierto. Cómo utiliza la gente el internet, los dispositivos móviles y los medios sociales. Salamanca, España, 04/02/2019. Disponible en:

<https://universoabierto.org/2019/02/04/como-utiliza-la-gente-internet-los-dispositivos-moviles-los-medios-sociales/>