Análisis: Anexo del TISA que se filtró sobre Comercio Electrónico por Burcu Kilic & Tamir Israel[1]

En el día de hoy, Wikileaks publicó un borrador actualizado del anexo sobre Comercio Electrónico del Acuerdo de Comercio de Servicios (TISA) que se propone. El TISA es un acuerdo comercial que están negociando actualmente 24 países (contando a la UE como uno solo), que se denominan a sí mismos "los Auténticos Buenos Amigos de los Servicios".

El anexo sobre comercio electrónico incluye medidas apoyadas por Estados Unidos sobre comercio electrónico, transferencia de tecnología, flujos transfronterizos de datos y neutralidad de las redes de telecomunicaciones, que ampliarían el alcance y las normas del Acuerdo General sobre el Comercio de Servicios (AGCS) de la Organización Mundial del Comercio.

El TISA pretende ser un "patrón oro" en materia de acuerdos comerciales al cual puedan sumarse otros países, que permita establecer nuevas normas que habrán de servir como aporte para otros acuerdos, y que eventualmente pueda incorporarse al AGCS para que sea aplicable a todos los miembros de la OMC.

Algunas disposiciones:

Artículo 2: Movimiento de información o flujos transfronterizos de información

Artículo 2: [CA/PE/EEUU proponen: Movimiento de la Información] [JP/MX/CH proponen: Flujos transfronterizos de información]

[Kr: En lo referente al artículo sobre el movimiento de información, Corea considera que todo movimiento de información que surja de las acciones de un proveedor de servicios debe estar basado en el "consentimiento informado". El consentimiento informado refiere a la idea de que las personas que proporcionen sus datos personales a los proveedores de servicios tengan protección y garantía plena en el marco de la ley en lo relativo al uso de sus datos personales que proporcionan a los proveedores de servicios. Esto se debería ver reflejado adecuadamente en la redacción del artículo.

HK: El movimiento de información debería aplicarse sin perjuicio del régimen nacional de protección de datos personales y debería estar basado en el consentimiento informado.]

1. [CA/TW/CO/JP/MX/EEUU proponen: Ninguna de las Partes puede prohibir que el proveedor de servicios de otra parte [CO/JP proponen: o los usuarios de estos proveedores] [CA/CO/JP/TW/EEUU proponen: transfiera, [acceda, procese o almacene] información, incluyendo datos personales, dentro o fuera del territorio de la Parte, si tal actividad se lleva a cabo en relación con la conducción del

[1] Burcu Kilic, Public Citizen y Tamir Israel, Canadian Internet Policy & Public Interest Clinic

negocio del proveedor del servicio.]

2. [EEUU propone: REFERENCIA a las instituciones financieras.]

3. [CH propone; CO se opone: Las Partes deben asumir medidas para proteger a los usuarios que se involucran en acciones de comercio electrónico contra las prácticas comerciales fraudulentas o engañosas.]

4. [CH propone; CO se opone: Las Partes deben mejorar su capacidad de aplicar leyes para garantizar que se cumplan las leyes y reglamentaciones aplicables relativas a la protección de datos y privacidad.]

5. [CH propone; CO/EEUU se oponen: Las Partes no deben prohibir que los proveedores extranjeros de comercio electrónico o los usuarios de dichos proveedores transfieran electrónicamente información a nivel interno o entre fronteras, tengan acceso a información disponible públicamente o tengan acceso a su propia información almacenada en el extranjero.]

Los países Parte están debatiendo el título de esta disposición: Canadá, Perú y Estados Unidos proponen "Movimiento de información" y Japón, México y China proponen "Flujos Transfronterizos de Información". Una de las posibles razones de este debate es que el término "Movimiento de información" (o "Flujo libre de información") suena mucho más solidario y relacionado con los derechos humanos. "Flujos transfronterizos de información" suena más relacionado con el comercio.

El articulo 2.1 propone que "Ningún país Parte puede prohibir la transferencia, acceso, procesamiento o almacenamiento de información (incluyendo información personal) fuera del territorio de la Parte si se realiza en relación con un negocio". Esta disposición facilita las transferencias y procesamientos transfronterizos de datos en todos los sectores de servicios, incluyendo los servicios financieros, sin limitaciones.

Las leyes de protección de datos existen para equilibrar el derecho a la privacidad de las personas con la capacidad de las empresas de utilizar datos para los objetivos de su negocio. Esta disposición les da gran libertad a las empresas sobre cómo utilizar los datos (incluyendo datos personales) sin estar sujetos a restricciones. Los gobiernos probablemente no puedan garantizar que los datos se procesen de forma justa y con arreglo a las leyes, o que se obtengan sólo con fines específicos y legales. Ya que no habrá control sobre los datos, no será posible comprobar si los datos se mantienen más tiempo del necesario, o con qué objetivo se procesan. No queda claro qué sucedería en caso de procesamiento no autorizado o ilegal, o una pérdida accidental, destrucción o daño de los datos personales. Esta disposición permite la transferencia transfronteriza de datos a un país o territorio sin que antes se verifique si el país mantiene un nivel adecuado de protección de los derechos y libertades individuales.

Corea quiere que las transferencias transfronterizas de datos de los proveedores de servicios estén basadas en el "consentimiento informado". El consentimiento informado rige sobre determinados tipos de comunicaciones entre proveedores de servicios y usuarios acerca del uso de su información personal.

La disposición que propone Suiza establece la transferencia transfronteriza de información dentro de redes internas o atravesando fronteras.

Artículo 3: Protección del consumidor por Internet

Artículo 3: Protección del consumidor por Internet

[CH prefiere utilizar el término "comercio electrónico" en lugar de "actividades comerciales por Internet".]

1. [AU/CA/CL/TW/CO/UE/HK/IS/IL/JP/KR/LI/MX/NZ/NO/PA/PE proponen: Las Partes reconocen la importancia de mantener y adoptar medidas transparentes y efectivas para proteger al consumidor contra actividades comerciales fraudulentas y engañosas] [CO/JP/MX proponen; además de medidas que faciliten el desarrollo de la confianza de los consumidores] cuando se involucran en actividades de comercio electrónico.]

2. [AU/CA/CL/TW/CO/UE/HK/IS/IL/JP/KR/LI/MX/NZ/NO/PA/PE proponen: Con este fin, cada Parte adoptará o mantendrá leyes de protección del consumidor para prohibir actividades comerciales fraudulentas y engañosas que [puedan perjudicar] [perjudiquen o perjudiquen potencialmente] a los consumidores involucrados en [CO propone: comercio electrónico] [AU/CL/JP/CR/NZ/PE proponen: actividades comerciales por Internet.]

3. [CO propone: En el marco de los términos y condiciones no discriminatorios, cada Parte otorgará a los consumidores involucrados en actividades de comercio electrónico con sus propios proveedores de servicios, acceso a los mecanismos de defensa del consumidor existentes proporcionados por sus autoridades nacionales de defensa del consumidor respectivas.]

4. [AU/CL/CO/JP/MX/NZ/PE proponen: Las Partes] [AU/CL/JP/MX/NZ/PE proponen: reconocen la importancia de] [CO propone: deben aspirar a la promoción de] la cooperación entre sus agencias nacionales de defensa del consumidor respectivas u otros organismos relevantes en materia de las actividades relacionadas con el comercio electrónico [AU/CL/NZ/PE proponen: transfronterizo] para mejorar el [bienestar] [MX propone: la confianza] de los consumidores.

5. [CO/MX proponen: Las partes deberán, de acuerdo con sus leyes y reglamentaciones, permitir a las personas que determinen mutuamente los métodos apropiados para solucionar las controversias que surjan de sus transacciones de comercio electrónico. Tales métodos pueden incluir, de modo no taxativo, mecanismos de solución de controversias por Internet.]

El inciso 5 del artículo 3 plantea inquietudes específicas relativas a una característica común e importante de muchas leyes de protección del consumidor. Este inciso les prohíbe a los

gobiernos interferir con los intentos individuales de "determinar mutuamente los métodos apropiados para resolver controversias que surjan a partir de transacciones de comercio electrónico, incluyendo, mecanismos de solución de controversias por Internet". Varios marcos de protección del consumidor han prohibido el uso de cláusulas de solución de controversias en contratos entre consumidores. El motivo de tal reglamentación es que dichas cláusulas son impuestas a menudo unilateralmente en contratos de adhesión y se las utiliza para evitar efectivamente el acceso a tribunales, en particular a mecanismos de demanda colectiva para enjuiciar y resolver pequeñas demandas judiciales acumuladas. Sin embargo, el artículo 3.5 parece excluir el uso de disposiciones que garanticen el acceso a los tribunales y mecanismos de demanda colectiva, ya que esto podría constituir una interferencia con los mecanismos de solución de controversias determinados mutuamente, a pesar del hecho que el "acuerdo" de los consumidores se establece en una cláusula no negociable en un contrato de adhesión más amplio.

Artículo 4: Protección de la información personal

Artículo 4: Protección de la información personal
1. [AU/CA/CL/TW/CO/IL/JP/KR/MX/NZ/NO/PA/PE proponen: Las Partes reconocen los beneficios económicos y sociales de proteger la información personal de los usuarios de comercio electrónico y cómo esto contribuye a mejorar la confianza de los consumidores de comercio electrónico.]
2. [AU/CA/CL/TW/CO/IL/KR/MX/NZ/NO/PA/PE proponen: Con este fin, cada Parte adoptará o mantendrá un marco jurídico nacional que establezca la protección de la información personal de los usuarios de comercio electrónico. En el desarrollo de estos marcos jurídicos de protección de la información personal, cada parte debería tener en cuenta los principios y directrices de los organismos internacionales relevantes.]
[CA propone: Cada parte deberá garantizar que su marco jurídico nacional para la protección de la información personal de los usuarios de comercio electrónico se aplique de forma no discriminatoria].
3. [AU/CA/CL/TW/CO/IL/JP/KR/MX/NZ/NO/PA/PE proponen: Cada parte debería publicar información sobre las medidas de protección de la información personal que ofrecen a los usuarios de comercio electrónico, incluyendo: (a) cómo los usuarios pueden hacer reclamaciones; y (b) cómo las empresas pueden cumplir con cualesquier obligaciones legales.]

Las Partes reconocen los beneficios económicos y sociales de proteger la información personal de los usuarios de comercio electrónico y se las obliga a adoptar o mantener un marco jurídico nacional que establezca la protección de la información personal de los usuarios de comercio electrónico. Con este fin, una mayoría de las Partes que están negociando el acuerdo proponen que las leyes nacionales que protegen la información personal deben seguir los principios y directrices de los organismos internacionales relevantes. Estados Unidos, por ejemplo,

probablemente no adopte una "ley" o serie de leyes sobre privacidad, sino que continuará siguiendo las reglamentaciones generales de la Comisión Federal de Comercio y las normas de conducta voluntarias.

Canadá propone una base no discriminatoria para la protección de la información personal. Estados Unidos está notoriamente ausente. Estados Unidos no asume ninguna posición sobre la protección de información personal. Esto puede deberse a que Estados Unidos no tiene ningún sistema general para proteger la información personal. En su lugar, tiene una combinación de leyes federales y estaduales, además de reglamentaciones sobre la recopilación y uso de datos personales, que pueden superponerse, coincidir e incluso contradecirse entre sí.

Artículo 5: Comunicaciones electrónicas comerciales no solicitadas

Artículo 5: [AU/CO/NZ proponen: Mensajes] [UE propone; NO considera: Comunicaciones] electrónicas comerciales no solicitadas.]

1. **[AU/CA/CL/CO/CR/UE/IL/JP/KR/MX/NZ/NO/PE proponen**: Cada parte deberá [**TW/TR proponen:** esforzarse a] adoptar o mantener medidas relativas a los [mensajes] [**UE propone**: comunicaciones] electrónicas comerciales no solicitadas que:]
(a) obliguen a los proveedores de mensajes electrónicos comerciales no solicitados a facilitar la capacidad de los destinatarios de elegir detener tales mensajes; o [**UE/NO proponen**; **AU se opone**: a]

(b) requerir el consentimiento, tal como se especifique en las leyes y reglamentaciones de cada Parte, de los destinatarios de recibir mensajes electrónicos comerciales; [**UE/NO se oponen**: o

(c) de otra forma ofrecer la minimización de los mensajes electrónicos comerciales no solicitados.]]

2. [**AU/CA/CL/CO/IL/JP/KR/NZ/NO/PE proponen**: Cada Pate deberá [**TW/TR proponen**: esforzarse por] ofrecer recursos contra los proveedores de mensajes electrónicos comerciales no solicitados que no cumplan con sus medidas implementadas de acuerdo con el párrafo 1.]

3. [**AU/CA/CL/CO/CR/UE/IL/KR/JP/NZ/NO/PE proponen**: Las Partes deberán esforzarse por cooperar en casos de preocupación mutua sobre la reglamentación de los mensajes electrónicos comerciales no solicitados.]

El artículo 5 obliga a las Partes a adoptar medidas para reglamentar las comunicaciones electrónicas comerciales no solicitadas. El inciso (a) propone una salida en la cual el destinatario puede elegir detener los mensajes. El inciso (b) propone que las comunicaciones comerciales no solicitadas requieran el consentimiento del usuario o que este opte por recibir los mensajes. Además, el inciso (c) propone la adopción de otras medidas que minimizarían la cantidad de mensajes comerciales no solicitados.

Actualmente, estas tres medidas se presentan como opciones alternativas, dejándole a los signatarios bastante amplitud respecto de cómo eligen reglamentar los correos basura electrónicos (*spam*). La propuesta de la UE de hacer que los incisos (a) a (c) se consideren

obligaciones superpuestas que coexisten fortalecería significativamente la disposición que, en su forma actual, solo obliga realmente a las Partes a "ofrecer la minimización de la cantidad de mensajes electrónicos comerciales no solicitados" de cualquier forma que consideren adecuada. Si se adopta la propuesta de la UE, sin embargo, se van a tener que ajustar varios regímenes *anti-spam* para imponer una obligación de consentimiento previo.
Además, el TISA cedería cierto nivel de control sobre cómo se interpretan a nivel internacional las palabras clave en el control del *spam*.

Si bien el artículo 5 deja expresamente a los gobiernos nacionales la decisión de cómo definir el "consentimiento", no hace lo mismo respecto de determinar qué significa en este contexto otorgarles a los usuarios finales el derecho de detener los mensajes.

Artículo 6: Transferencia o acceso al código fuente

Artículo 6: [JP propone; CO se opone: Transferencia o acceso al código fuente
1. Ninguna de las Partes podrá requerir la transferencia o acceso al código fuente de un *software* de propiedad de una persona de otra Parte, como condición para el suministro de servicios relacionados con dicho *software* en su territorio.
2. A efectos de este artículo, el *software* sujeto al párrafo 1 se limita a *software* de mercado masivo, y no incluye *software* utilizado para infraestructuras críticas.]

La propuesta de Japón pretende prohibir que los gobiernos puedan exigirle a una empresa que proporciona un servicio relacionado con *software* que transfiera o proporcione acceso al código fuente del *software*. Se exceptúan categóricamente de esta prohibición las infraestructuras críticas.

Al igual que en muchos otros puntos de este anexo sobre comercio electrónico del TISA, esta disposición está mal pensada y es al mismo tiempo demasiado incluyente y muy poco incluyente. Hay muchas situaciones más allá del contexto de infraestructura crítica en las que podría ser deseable desde una perspectiva de política pública requerir el acceso al *software*, como en el caso de los enrutadores (*routers)* domésticos, cuya seguridad tan débil representa un problema permanente para las redes domésticas. Una prohibición tan categórica y general requisito de acceso al código fuente puede perjudicar la transparencia y el uso de ofrecimientos de código abierto en los contratos gubernamentales. Cualquier proveedor de servicios que quiera mantener los derechos de propiedad sobre sus códigos fuente podría fácilmente argumentar que es una violación del artículo 6 que un gobierno exija que se publique un código fuente como condición esencial en una propuesta de servicio -un mecanismo que mejoraría la transparencia pública de los servicios gubernamentales, así como que alentaría en general la producción de códigos abiertos.

Por otro lado, la prohibición del artículo 6 es también poco incluyente. Podría haber muy buenas razones para evitar que un gobierno determinado tenga acceso al código fuente de *software* utilizado en infraestructuras críticas. Por ejemplo, una autoridad regulatoria podría querer imponer obligaciones de auditoría para comprobar las capacidades de filtrado o monitoreo de un equipamiento de Inspección a fondo de los paquetes (*Deep Packet Inspection*) instalado en una red de un proveedor de servicios de telefonía móvil o por cable. Esto puede ser necesario para entender posibles actividades invasivas de la privacidad o de censura en la red.

Un enfoque más sutil de la reglamentación de las obligaciones de transferencia o acceso al código fuente evitaría la prohibición categórica del TISA y en su lugar codificaría los objetivos o propósitos bajo los cuales es o no aceptable que se impongan tales condiciones.

Artículo 7: Interoperabilidad

Artículo 7: [CO propone: Interoperabilidad]
[**CO propone**: Cada Parte deberá esforzarse por promover la interoperabilidad entre los procedimientos electrónicos de su gobierno a través de la Internet y los servicios provistos por medios electrónicos.]

La propuesta de Colombia tiene por objetivo garantizar la interoperabilidad entre los procedimientos electrónicos de los gobiernos a través de la Internet y los servicios provistos por medios electrónicos. Lograr esta interoperabilidad requiere de liderazgo y dedicación en términos de la implementación práctica de los servicios a niveles operativos entre los sectores. Debido a que los "Auténticos Buenos Amigos" de la industria de servicios carecen de la infraestructura cooperativa de otros organismos de gobernanza tales como la OCDE, APEC y el Foro de la Gobernanza de Internet, no queda claro a través de qué mecanismos pretenden cumplir con este mandato.

Artículo 8: Redes abiertas, acceso y uso de redes

Artículo 8: Redes abiertas, acceso y uso de redes

1. [AU/CA/CL/CO/IL/JP/NO/PE/EEUU proponen: Cada Parte reconoce que los consumidores de su territorio, de conformidad con las leyes y reglamentaciones aplicables, deberían poder:

(a) acceder a y utilizar los servicios y aplicaciones de su elección que estén disponibles en Internet, siempre y cuando hagan un manejo razonable de la red;

(b) conectar a Internet los dispositivos que elijan, siempre y cuando tales dispositivos no dañen la red; y

(c) tener acceso a información sobre las prácticas de gestión de redes de sus proveedores de servicios de acceso a Internet.]

2. [**KR se opone: [CO/CH proponen**: Las Partes, preferentemente a través de autoridades relevantes, deberían promover la capacidad de los consumidores de acceder, compartir y distribuir información legítimamente, así como de ejecutar aplicaciones y utilizar los servicios que elijan.] **[CO/JP proponen:** Cada parte se deberá esforzar para no] [**TR propone**: Sin perjuicio de la legislación aplicable,] [**CH propone**: Las partes no deberían] [**CO/JP/CH proponen:** restringir la capacidad] [**JP propone**: de los proveedores de servicios de suministrar servicios] [**CO/CH propone**: de suministrar servicios] [**CO/JP/CH proponen**: por Internet] [**CH propone:** incluyendo] [**CO/JP/CH proponen**: de forma transfronteriza y tecnológicamente neutral, y] [**JP propone**: se deberán esforzar por] [**CO/CH proponen**: deberían] [**CO/JP/CH proponen**: promover la interoperabilidad de los servicios y tecnologías, cuando corresponda.] [JP propone: Cada Parte deberá esforzarse para garantizar que lo proveedores de acceso a Internet eviten discriminar de forma no razonable al transmitir tráfico legal de redes.]]

Esta disposición es muy similar al artículo X.5 de la propuesta de Estados Unidos de fecha 25 de abril de 2014. Representa una obligación débil formulada en un lenguaje de "reconocimiento" de que los consumidores deberían tener acceso a cualquier servicio o aplicación de Internet, siempre y cuando hagan un manejo razonable de la red; conectarse a cualquier dispositivo que quieran, siempre y cuando al hacerlo no dañen la red; y tener acceso a información sobre las prácticas de gestión de redes de quienes les suministran acceso a Internet.

La disposición aborda la neutralidad de las redes de telecomunicaciones de manera minimalista, pero de todos modos problemática. El inciso 1(a) del artículo 8 impone la prohibición de impedir el acceso a contenidos. El inciso 1(a) les permite a los proveedores impedir el acceso a contenidos por motivos de "manejo razonable de la red". El "manejo razonable de la red" es un estándar más permisivo que el adoptado por otras jurisdicciones y quizás requiera cambios en los marcos existentes sobre la neutralidad de las redes de telecomunicaciones. No queda claro como el organismo de control que se elija en el TISA para

aplicar sus obligaciones interpretará finalmente la excepción referida al "manejo razonable de la red". Es interesante que el término "manejo razonable de la red" no se utiliza en la disposición equivalente en el artículo 15.7 del Tratado de Libre Comercio entre Corea del Sur y Estados Unidos (KORUS, por su sigla en inglés). El inciso 1(b), que prohíbe que se impida el acceso a las redes a los dispositivos no perjudiciales, no exime el "manejo razonable de la red".

Los incisos 1(a) y (b) del artículo 8 del TISA reproducen un conjunto de normas sobre "Internet abierta" adoptadas recientemente por la Comisión Federal de Conminación (FCC, por su sigla en inglés), un conjunto enfocado en proteger contra el bloqueo del acceso de usuarios finales a contenidos y servicios, así como el uso de dispositivos finales no perjudiciales.[2]

La neutralidad de las redes de telecomunicaciones como principio protegido por ley está evolucionando rápidamente en muchas jurisdicciones y sus parámetros completos no se han establecido aún. Desafortunadamente, el TISA no aborda efectivamente los problemas existentes de neutralidad de las redes de telecomunicaciones. Solo aborda de manera significativa las violaciones de neutralidad más atroces (aquellas relacionadas con impedir el acceso a contenidos) e incluso aquí exime de manera general el "manejo razonable de la red". Si este enfoque del TISA de convertirse en norma internacional sobre el acceso abierto neutral llega a consagrarse como norma internacional, ésta será incapaz de garantizar la neutralidad de las redes de telecomunicaciones de hoy en día, mucho menos las de mañana. Por cierto, los marcos jurídicos de neutralidad de las redes de telecomunicaciones que existen actualmente en Brasil, Canadá y otros países adoptan restricciones más estrictas para los proveedores de servicios que quieran impedir el acceso de los clientes a servicios o contenidos de bajada.

El inciso 1(a) del artículo 8 del TISA también es problemático ya que sólo se aplica a situaciones en las que se impide el acceso a aplicaciones o servicios. No incluye los casos en que el tráfico se degrada injustificada o discriminativamente en términos económicos. Sin embargo, la mayoría de las inquietudes relativas a la neutralidad de las redes de telecomunicaciones están asociadas a la discriminación económica o técnica contra el tráfico de bajada.

El inciso 2 del artículo 8 del TISA reconoce que las Partes deberían "esforzarse" por evitar una "discriminación no razonable" de manos de los proveedores de servicios de Internet en la transmisión de tráfico legal en redes. Sin embargo, no sólo se permite una "discriminación razonable" (reproduciendo el estándar de "razonabilidad" adoptado por la FCC que, tal como se mencionó anteriormente, es más permisivo que los adoptados por otras jurisdicciones tales como Brasil y Canadá), sino que el TISA no impone ninguna obligación de acción regulatoria respecto de tal discriminación. "Esforzarse" no implica al aparato estatal de aplicación de las

[2] FCC, In the Matter of Protecting and Promoting the Open Internet, FCC 15-24, 26

leyes y bien puede también excluir su utilización. Debido a estas limitaciones, el marco de acceso abierto del TISA deja abierto un gran abanico de actividad discriminatoria y perjudicial para la innovación que los proveedores de tráfico pueden aprovechar, pero que las autoridades regulatorias consideran objetable.

Si llegase a convertirse en la norma internacional para encarar las afrentas contra la neutralidad de las redes de comunicaciones o el acceso abierto, lo hará de manera verdaderamente deficiente.

Artículo 9: Infraestructura local / Presencia local

Artículo 9: [JP/CH/EEUU proponen: Infraestructura local] [JP propone: y Presencia local] [KR propone: 1]

1 **[KR propone**: El artículo 9 no se aplica a los proveedores de redes o servicios públicos de telecomunicaciones.]

1. **[CO/EEUU proponen:** Ninguna de las Partes puede exigirle a un proveedor de servicios, como condición para suministrar un servicio o invertir en su territorio, que:

a) use instalaciones informáticas ubicadas en territorio de la Parte;

(b) utilice servicios de procesamiento o almacenamiento informático suministrados desde el territorio de la Parte;

o

(c) almacene o procese datos de cualquier otro modo en su territorio.]

[**CO propone**: Sin embargo, nada de lo dispuesto en el párrafo 1 deberá impedir que una Parte condicione el otorgamiento de ventajas o su continuidad al cumplimiento del requisito de usar, establecer o ampliar las instalaciones informáticas en su territorio, incluyendo las necesarias para el procesamiento o almacenamiento de datos.]

[KR: Respecto al párrafo 1 (infraestructura local), Corea tiene reservas para aceptar el texto actual, teniendo en cuenta nuestro marco regulatorio de telecomunicaciones. Corea está dispuesta a discutir limitaciones o la definición del alcance de aplicación de esta disposición.]

2. **[Estados Unidos propone; KR/CO se oponen**: Este artículo deberá aplicarse a los proveedores de servicios financieros transfronterizos únicamente en la medida que las Partes hayan incluido los servicios financieros transfronterizos en su lista de compromisos específicos.]

[**JP** querría aclarar el significado del párrafo 2]. [**KR**: Respecto al párrafo 2, Corea considera que esto puede abordarse en el anexo sobre Servicios Financieros. Corea sugiere que se elimine este párrafo y al mismo tiempo apoya la propuesta de Suiza/Japón de excluir de este anexo a los servicios financieros, así como del artículo III.X de las Disposiciones Generales.]

3. [**KR se opone**: [**JP propone**: Ninguna de las Partes deberá] [**CH propone**: Las partes no deberían] [**JP/CH proponen**: requerirle] [**JP propone**: a los proveedores de servicios de tecnología de la información y comunicaciones] **[CH propone**: a los proveedores de comercio electrónico] [**JP/CH**

proponen: usar] [**CH propone**: o establecer ninguna] [**JP/CH proponen**: infraestructura local como condición para] [**JP propone**: suministrar]
[**CH propone:** el suministro de] [**JP/CH proponen**: servicios.]]
4. [**KR se opone**: [**JP propone**: Ninguna de las Partes deberá requerirle a los proveedores de servicios de tecnología de la información y comunicaciones establecer una presencia local como condición para el suministro transfronterizo de servicios.]]
[**JP** querría eliminar el párrafo 4 de este artículo si se establece la presencia local en el texto central del TISA.] [**KR** tiene reservas sobre el artículo de Presencia Local (párrafo 4 del artículo 9 que propone Japón).]
5. [**KR se opone: [JP propone**: Ninguna de las Partes deberá] [**CH propone**: Además, las Partes no deberían] [**JP/CH proponen**: dar prioridad o trato especial a] **[JP propone**: sus propios proveedores de servicios] [**CH propone**: proveedores nacionales de comercio electrónico] [**JP/CH proponen**: en el uso de infraestructura local] [**JP propone**: nacional] recursos [**CH propone**: terrestres] [**JP/CH proponen**: de espectro] [**JP propone**:,] [**JP/CH proponen**: orbitales]].
[CO querría excluir de esta disposición los asuntos relacionados con las compras públicas.]

La propuesta de Estados Unidos y Colombia sobre la localización de los datos establece que "ninguna de las Partes puede exigirle a un proveedor de servicios utilizar instalaciones informáticas ubicadas en su territorio para procesar y almacenar datos como condición para suministrar el servicio o invertir en el país". Esta obligación se aplica a todos los proveedores de servicios (actuales y futuros), inclusive las empresas privadas nacionales y las empresas estatales. Las restricciones se aplican a "suministrar un servicio o invertir en su territorio", lo cual es de gran alcance ya que se aplica a todos los elementos directos e indirectos de la cadena de suministro de un servicio.

El Representante de Comercio de Estados Unidos considera desde hace ya bastante tiempo que cualesquier obligaciones de utilizar la infraestructura local de redes o los servidores locales constituyen una barrera no arancelaria y una restricción discriminatoria contra los derechos de comercialización, argumentando a tal efecto que los requisitos de localización son estrategias proteccionistas que dejan en desventaja a los bienes, servicios o proveedores de Internet extranjeros frente a los bienes nacionales. Estados Unidos también considera que los requisitos de localización socavarían las ventajas de los servicios estadounidenses basados en la nube, ya que la mayoría, si no todas las empresas que utilizan servicios basados en la nube están ubicadas actualmente en Estados Unidos.

Requerir siempre y sin excepciones el uso de servidores locales es desproporcionado y puede repercutir negativamente en la economía digital. Sin embargo, la informática basada en la nube está ganando popularidad rápidamente entre los proveedores de servicios, lo cual plantea serias inquietudes e interrogantes respecto a la responsabilidad y la rendición de cuentas de los

proveedores de servicios. Es importante destacar los riesgos que esto representa para las leyes nacionales sobre privacidad y protección de la información médica, información personal no relacionada con el comercio y protección del consumidor. El marco legislativo actual sobre privacidad está lejos de ser el ideal. Existen distintas leyes y reglamentaciones sobre privacidad. La ubicación de los datos a menudo determina las leyes aplicables sobre cómo se almacenan y procesan los datos. La mayoría de las empresas estadounidenses de tecnología de la información y comunicaciones almacenan datos en Estados Unidos, lo que hace que sean las normas de Estados Unidos las aplicables en términos de almacenamiento, procesamiento y transferencia de datos. El nivel inadecuado de protección de los datos en Estados Unidos podría ser considerado una barrera comercial por otras Partes negociadoras con leyes nacionales fuertes sobre privacidad y almacenamiento de datos.

Estados Unidos quiere que en la aplicación de este artículo se establezca una limitación referida a los proveedores de servicios financieros transfronterizos, de modo tal que sólo abarque los servicios financieros transfronterizos de las Partes que han incluido esos servicios en su lista de compromisos específicos. Suiza y Japón quieren que los servicios financieros sean excluidos de esta anexo, y Corea apoya esa propuesta. El articulo X.11 del capítulo del TISA sobre servicios financieros que se filtró habilita la transferencia transfronteriza de información.[3] También vale la pena mencionar que el anteproyecto de "Ley de Comercio Digital" que se introdujo en el Senado estadounidense en diciembre de 2013 le daría mandato vinculante al Representante de Comercio de Estados Unidos para cualesquier negociaciones internacionales en el área del comercio electrónico. Ese mandato incluye prohibir las reglamentaciones sobre "localización" y consagrar las normas sobre la "interoperabilidad" en el procesamiento de datos como un principio fundamental. Esta ley por supuesto también se aplicaría a las negociaciones sobre el capítulo correspondiente del TLC Transatlántico (TTIP por su sigla en inglés).

Japón y Suiza proponen que los gobiernos no puedan obligar a un proveedor de servicios (de comercio electrónico o tecnologías de la información y comunicaciones) a usar o establecer una infraestructura local como condición para el suministro de un servicio (se aplica a todos los elementos directos e indirectos en la cadena de suministro de un servicio). Esta disposición no permite que los gobiernos obliguen a que las instalaciones informáticas, incluyendo los servidores, estén ubicados dentro de su territorio.

Según el párrafo 4 que propuso Japón, la presencia local no puede transformarse en una "condición" para el suministro transfronterizo de un servicio. Japón quiere poder suministrar servicios de tecnología de la información y comunicaciones sin que se le requiera tener una oficina física en los países del TISA. La norma sólo afectará a los servicios que exijan algún tipo

[3] https://wikileaks.org/tisa-financial/

de aprobación y se aplicará a los servicios que sólo puedan suministrarse dentro del país por proveedores registrados o autorizados u operadores con licencias, como en el caso de las empresas que brindan servicios de contabilidad, jurídicos, médicos, de ingeniería, etc.

Japón, sin embargo, quiere eliminar el párrafo si se aborda el tema de la presencia local en el texto central del TISA.

Artículo 10: Autenticación electrónica y firmas electrónicas

Artículo 10: Autenticación electrónica y firmas electrónicas

1. [**AU/CA/TW/CO/UE/IS/KR/MX/NO/PA/PE/TR/EEUU proponen**: Excepto cuando esta ley disponga lo contrario, una Parte no podrá negar la validez o legalidad de una firma sólo por el hecho que la firma se consigne en formato electrónico.]

[**JP** querría aclarar el significado de "excepto cuando esta ley disponga lo contrario" en el párrafo 1.]

2. **[AU/CA/TW/CO/UE/IS/JP/KR/MX/PE/TR/EEUU proponen**: Ninguna de las Partes podrá adoptar o mantener medidas sobre autenticación electrónica que:

(a) prohíban a las partes de una transacción electrónica determinar mutuamente los métodos apropiados de autenticación de la transacción o

(b) no permitan que las partes tengan la oportunidad de establecer ante autoridades judiciales o administrativas que su transacción electrónica cumple con todos los requisitos legales relativos a la autenticación.]

3. **[AU/CA/TW/CO/UE/IS/JP/KR/MX/PE/TR/EEUU proponen**: Sin perjuicio del párrafo 2, una Parte puede requerir que, en el caso de una categoría particular de transacciones, el método de autenticación cumpla con determinados estándares de desempeño o sea certificada por una autoridad acreditada de conformidad con las leyes de la Parte.]

Esta disposición tiene por objetivo minimizar las restricciones al uso de firmas electrónicas. Se basa en la propuesta de Estados Unidos de fecha 25 de abril de 2014. Según ella, un gobierno no puede negar la validez o legalidad de una firma sólo por el hecho de que sea electrónica. Incluso aunque la norma suene fuerte, se sigue sometiendo a la legislación nacional. Las leyes nacionales pueden impedir o limitar el reconocimiento legal de las firmas electrónicas como válidas.

Según esta bien fundamentada disposición, un gobierno no puede introducir o mantener requisitos existentes de autenticación que no permitan a las partes de una transacción electrónica decidir por sí mismas cuál es la mejor manera de autenticar la transacción. Un gobierno tampoco puede prohibir que las partes de una transacción electrónica den pruebas ante organismos administrativos o judiciales de que su transacción cumple con la ley en materia de autenticación.

El párrafo 3 permite que se establezcan estándares de desempeño para la autenticación y que se pueda requerir la certificación de una autoridad acreditada, pero sólo cuando una medida esté relacionada en su contenido con lograr un "objetivo gubernamental legitimo". Un gobierno puede de todas maneras requerir que una "categoría particular de transacción" cumpla con ciertos estándares de desempeño o esté certificada por una autoridad acreditada de conformidad con la legislación nacional. No se indica cuáles pueden ser estas categorías y por lo tanto no se limita su alcance o cantidad.

Artículo 11: Derechos aduaneros sobre los envíos electrónicos

Artículo 11: [AU/CO/UE/IS/NO/PE/CH/TW proponen: Derechos aduaneros sobre los envíos electrónicos

[UE/NO proponen: Las Partes acuerdan que los envíos electrónicos no estarán sujetos al pago de derechos aduaneros, [TW se opone: derechos, tasas o cargos]]. [CO/CR/JP/PE proponen: Ninguna de las Partes puede imponer derechos aduaneros [TW se opone: derechos, tasas o cargos] sobre las transmisiones electrónicas.]

2. Para mayor claridad, el párrafo 1 no prohíbe que una Parte imponga impuestos internos u otros cargos internos sobre [UE/NO proponen: un envío transmitido por medio electrónico] [CO/MX/PE proponen: las transmisiones electrónicas], siempre y cuando tales impuestos o cargos se impongan de manera compatible con este acuerdo.]

Si bien la disposición establece que los servicios suministrados mediante transmisión electrónica no están sujetos al pago de derechos, tasas o cargos aduaneros, la disposición no prohíbe que un gobierno pueda imponer impuestos internos u otros cargos internos para el suministro electrónico, siempre y cuando tales impuestos y cargos se impongan de manera compatible con el Acuerdo.

Si se exime a los envíos electrónicos del pago de derechos aduaneros, se perderán los derechos aduaneros sobre esas importaciones. Los países, especialmente los países en desarrollo donde los ingresos aduaneros juegan un papel significativo en el presupuesto nacional deberían considerar cuidadosamente la dificultad de sustituir esos ingresos perdidos, antes de comprometerse para siempre a exonerar de impuestos los envíos mediante medios electrónicos.

Artículo 12: Cooperación internacional

Artículo 12: [JP/CH proponen: Cooperación internacional]

1. [CO/JP/NO proponen: Cada parte deberá esforzarse por cooperar con las otras Partes para aumentar el nivel de alfabetización digital a nivel mundial y reducir la "brecha digital".]
2. [CO/CH proponen: Las partes intercambiarán [CO propone: en la medida de lo posible] información en el área del comercio electrónico y los servicios de telecomunicaciones. Esto puede incluir información sobre, entre otros:
   (a) avances e investigaciones tecnológicas en el área del comercio electrónico y los servicios de telecomunicaciones;
   (b) aspectos comerciales y técnicos sobre el suministro de comercio electrónico y servicios de telecomunicaciones a través de todos los modos de suministro;
   c) las posibilidades disponibles para el intercambio de comercio electrónico y tecnologías relacionadas con las telecomunicaciones; y
   (d) leyes y reglamentaciones aplicables, procesos legislativos y avances legislativos recientes; normas técnicas aplicables.]
3. [CO/NO/CH proponen: Las Partes intercambiarán sus visiones sobre los avances relacionados con el comercio electrónico y los servicios de telecomunicaciones a nivel internacional.]
4. CH propone: Promoción
   Las Partes afirman su intención de:
   (a) promover estas disposiciones para contribuir a la expansión y difusión del comercio electrónico y los servicios de telecomunicaciones;
   (b) trabajar juntos y cooperar en foros internacionales para aumentar el nivel de alfabetización digital y reducir la brecha digital a nivel mundial;
   (c) cooperar con terceros países con el objetivo de mejorar la capacidad regulatoria nacional y contribuir a la difusión del comercio electrónico y los servicios de telecomunicaciones, que son herramientas poderosas para promover el desarrollo económico.]

La alfabetización digital puede definirse como la capacidad de utilizar tecnología digital, herramientas de comunicaciones o redes para ubicar, evaluar, utilizar o crear información. La alfabetización digital está supeditada al uso de métodos digitales de comunicación y facilita la colaboración e intercambio de conocimiento. Por otro lado, la brecha digital es un concepto dinámico y complejo que describe las diferencias en el acceso a las tecnologías de la información y las comunicaciones. Sin embargo, no existe una única brecha sino múltiples, y por lo tanto hay numerosas maneras de medir la brecha digital.

Incluso aunque el comercio electrónico ofrezca nuevas oportunidades de negocios a nivel mundial, es muy probable que estos avances amplíen la brecha digital y que los países en desarrollo queden rezagados y pierdan en esa carrera. Por lo tanto, la coordinación internacional y el intercambio de información se tornan importantes. Esta disposición

promueve la cooperación y el intercambio de información entre los gobiernos, pero no impone ninguna obligación.

Artículo 14

[EEUU propone: Nada de lo dispuesto en la Sección III (Comercio electrónico) debe considerarse como un impedimento para que las Partes emprendan cualesquier acciones que estimen necesarias para la protección de sus propios intereses esenciales de seguridad.]
[CO/JP querrían aclarar el significado de "intereses esenciales de seguridad" en el párrafo 1 de este artículo.] [KR: A Corea le gustaría tener una discusión más amplia sobre lo que significan los "intereses esenciales de seguridad" en este artículo.]

Esta excepción propuesta por Estados Unidos protege el derecho de un gobierno a emprender cualquier acción que considere necesaria para proteger sus intereses esenciales de seguridad. Esta disposición no incluye ninguna limitación o reserva. Al aplicar estas excepciones, los gobiernos deberían sopesar el daño que le hacen al interés público.

La excepción de seguridad nacional es discrecional. Estados Unidos se ha negado a someterse a ninguna controversia que impugne su uso de una disposición similar pero más débil en el marco del GATT y en la OMC.

Artículo 15: Definiciones

A los efectos de este anexo:
[AU/CO proponen: **autenticación** implica el proceso o acto de establecer la identidad de una parte en una comunicación o transacción electrónica o garantizar la integridad de una comunicación electrónica;]

[CO propone: **comercio electrónico** implica toda transacción comercial o empresarial transfronteriza realizada por medios electrónicos; incluyendo, entre otros, los contratos de distribución de servicios, de obras de construcción, de servicios de consultoría, servicios de ingeniería y servicios empresariales**.**]

[UE/TR: **firma electrónica** son datos en formato electrónico que se adjuntan o asocian lógicamente con otros datos electrónicos y que cumplen con los siguientes requisitos:

(i) La utiliza una persona para establecer su acuerdo con los datos electrónicos a los cuales se refiere;
(ii) (ii) se vincula con los datos electrónicos a los cuales se refiere, de forma tal que toda alteración futura de los datos sea detectable.]

AU/CO/NZ proponen: **información personal** implica toda información, incluyendo los datos, sobre una persona física identificada o identificable.]

[Los proponentes harán consultas sobre esta definición de información personal.]

[AU propone: **mensaje electrónico comercial no solicitado** implica un mensaje electrónico que se envía con fines comerciales a una dirección electrónica sin el consentimiento del destinatario o haciendo caso omiso del rechazo explícito del destinatario, utilizando un proveedor de servicios de acceso a Internet y, en la medida que lo dispongan las leyes nacionales y reglamentaciones de cada Parte, otro servicio de telecomunicaciones.]

Autenticación: Aunque la noción de autenticación cumple distintas funciones en diferentes sistemas jurídicos, se entiende generalmente que refiere a la autenticidad de un documento o registro, que refiere a la originalidad de un documento, al respaldo de la información que contiene, en la forma que se registró y sin ninguna alteración. Las distintas definiciones jurídicas de autenticación en diversos sistemas legales pueden generar confusión sobre los procedimientos particulares o requisitos formales. La definición propuesta por Australia y Colombia es la misma que se incluye en el Tratado de Libre Comercio entre Australia y Estados Unidos.[4]

Firma electrónica: La definición que se propone replica la definición de "firma electrónica

[4] Artículo 16.8, TLC entre Australia – US (https://ustr.gov/sites/default/files/uploads/agreements/fta/australia/asset_upload_file508_5156.pdf)

avanzada" provista en la Directiva. Debe hacerse referencia al hecho que a medida que se desarrollan nuevas formas de tecnología, disponer una forma tecnológicamente específica de firma electrónica en la legislación no es deseable. Una definición amplia de firma electrónica ayudará a los gobiernos a determinar su uso para cada forma de firma y coordinar la autenticidad con otros aparceros.

Datos personales: Cómo se define el término "datos personales" determina la aplicabilidad y alcance de las leyes sobre privacidad. La definición propuesta por Australia, Colombia y Nueva Zelanda replica la definición de datos personales de la Directiva Europea de Protección de Datos: "información relativa a una persona física identificada o identificable". En vista de las diversas definiciones que contempla la legislación estadounidense, esta disposición puede ser considerada expansionista para Estados Unidos.

La transferencia transfronteriza de datos depende en gran medida de la coordinación entre sistemas legales, y las definiciones divergentes del término 'datos personales' muy probablemente sea fuente de problemas para la protección de la privacidad.

Nuevas disposiciones aplicables a todos los servicios

[La inclusión en este documento de trabajo de los siguientes artículos de la propuesta de Estados Unidos para la Parte III del texto central del TISA pretende facilitar la discusión, sin perjuicio de la inclusión o no y la disposición final de tales artículos en el texto central del TISA o en un anexo.]

El análisis de la propuesta de Estados Unidos filtrada previamente (Propuesta de nuevas disposiciones aplicables a todos los servicios en el Acuerdo de Comercio de Servicios, fechada 25 de abril de 2014) está disponible aquí.